CONGRUENCES OF THE PARTITION FUNCTION

YIFAN YANG

Dedicated to Professor B. C. Berndt on the occasion of his 70th birthday

ABSTRACT. Let \( p(n) \) denote the partition function. In this article, we will show that congruences of the form

\[ p(m^j \ell^k n + B) \equiv 0 \mod m \]

exist for all primes \( m \) and \( \ell \) satisfying \( m \geq 13 \) and \( \ell \neq 2, 3, m \). Here the integer \( k \) depends on the Hecke eigenvalues of a certain invariant subspace of \( S_{m/2-1}(\Gamma_0(576), \chi_{12}) \) and can be explicitly computed.

More generally, we will show that for each integer \( i > 0 \) there exists an integer \( k \) such that for every non-negative integers \( j \geq i \) with a properly chosen \( B \) the congruence

\[ p(m^j \ell^k n + B) \equiv 0 \mod m^i \]

holds for all integers \( n \) not divisible by \( \ell \).

1. INTRODUCTION

Let \( p(n) \) denote the number of ways to write a positive integer \( n \) as sums of positive integers. For convenience, we also set \( p(0) = 1 \), \( p(n) = 0 \) for \( n < 0 \), and \( p(\alpha) = 0 \) if \( \alpha \notin \mathbb{Z} \). A remarkable discovery of Ramanujan \([13]\) is that the partition function \( p(n) \) satisfies the congruences

\[ p(An + B) \equiv 0 \mod m, \]

for all non-negative integers \( n \) for the triples

\[ (A, B, m) = (5, 4, 5), (7, 5, 7), (11, 6, 11). \]

Ramanujan also conjectured that congruences \( (1) \) exist for the cases \( A = 5^j, 7^j, \) or \( 11^j \). This conjecture was proved by Watson \([17]\) for the cases of powers of 5 and 7 and Atkin \([3]\) for the cases of powers of 11. Since then, the problem of finding more examples of such congruences has attracted a great deal of attention. However, Ramanujan-type congruences appear to be very sparse. Prior to the late twentieth century, there are only a handful of such examples \([4, 6]\). In those examples, the integers \( A \) are no longer prime powers.

It turns out that if we require the integer \( A \) to be a prime, then the congruences proved or conjectured by Ramanujan are the only ones. This was proved recently in a remarkable paper of Ahlgren and Boylan \([2]\). On the other hand, if \( A \) is allowed to be a non-prime power, a surprising result of Ono \([12]\) shows that for each prime \( m \geq 5 \) and each positive integer \( k \), a positive proportion of primes \( \ell \) have the property

\[ p \left( \frac{m^k \ell^k n + 1}{24} \right) \equiv 0 \mod m \]

Date: April 16, 2009.

2000 Mathematics Subject Classification. Primary 11P83; Secondary 11F25, 11F37, 11P82.
for all non-negative integers \( n \) relatively prime to \( \ell \). This result was later extended to composite \( m \), \((m, 6) = 1\), by Ahlgren [12]. Neither of [12] and [11] addressed the algorithmic aspect of finding congruences of the form (2). For the cases \( m \in \{13, 17, 19, 23, 29, 31\} \) this was done by Weaver [18]. In effect, she found 76,065 new congruences. For primes \( m \geq 37 \), this was addressed by Chua [8]. Although no explicit examples of congruences (2) for \( m \geq 37 \) were given in [8], in principle, if one is patient enough, one will eventually find such congruences.

Another remarkable discovery of Ono [12, Theorem 5] is that the partition function possesses certain periodic property modulo a prime \( m \). Specifically, he showed that for every prime \( m \geq 5 \), there exist integers \( 0 \leq N(m) \leq m^{48(m^3 - 2m + 1)} \) and \( 1 \leq P(m) \leq m^{48(m^3 - 2m + 1)} \) such that

\[
p\left(\frac{m^n + 1}{24}\right) \equiv p\left(\frac{m^{P(m)} n + 1}{24}\right) \mod m
\]

for all non-negative integers \( n \) and all \( i \geq N(m) \). In [8], Chua raised a conjecture (Conjecture 2.1 in Section 3 below), which, if is true, will greatly improve Ono’s bound. (See Corollary 5 below.)

In this note, we will obtain new congruences for the partition function and discuss related problems. In particular, we will show that there exist congruences of the form

\[
p(m^j \ell^k n + B) \equiv 0 \mod m
\]

for all primes \( m \) and \( \ell \) such that \( m \geq 13 \) and \( \ell \) not equal to 2, 3, \( m \).

**Theorem 1.** Let \( m \) and \( \ell \) be primes such that \( m \geq 13 \) and \( \ell \neq 2, 3, m \). Then there exists an explicitly computable positive integer \( k \geq 2 \) such that

\[
p\left(\frac{m^j \ell^k n + 1}{24}\right) \equiv 0 \mod m
\]

for all non-negative integers \( n \) relatively prime to \( m \) and all positive integers \( j \).

For instance, in Section 6 we will find that for \( m = 37 \) and arbitrary \( j \), congruences (4) hold with

| \( \ell \) | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 41 | 43 | 47 | 53 | 59 | 61 |
|-----|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| \( k \) | 228 | 57 | 18 | 684 | 38 | 38 | 684 | 684 | 228 | 171 | 18 | 333 | 18 | 12 | 684 |

As far as we know, this is the first example in literature where a congruence (1) modulo a prime \( m \geq 37 \) is explicitly given.

**Theorem 1** is in fact a simplified version of one of the main results. (See Theorem 7). In the full version, we will see that the integer \( k \) in Theorem 1 can be determined quite explicitly in terms of the Hecke operators on a certain invariant subspace of the space \( S_{m/2-1} (\Gamma_0(576), \chi_{12}) \) of cusp forms of level 576 and weight \( m/2 - 1 \) with character \( \chi_{12} = (42) \). To describe this invariant subspace and to see how it comes into play with congruences of the partition function, perhaps we should first review the work of Ono [12] and other subsequent papers [8] [18]. Thus, we will postpone giving the statements of our main results until Section 3.

Our method can be easily extended to obtain congruences of \( p(n) \) modulo a prime power. In Section 7 we will see that for each prime power \( m^j \) and a prime \( \ell \neq 2, 3, m \), there always exists a positive integer \( k \) such that

\[
p\left(\frac{m^j \ell^k n + 1}{24}\right) \equiv 0 \mod m^j
\]
for all positive integers \( n \) not divisible by \( \ell \). One example worked out in Section\(^7\) is
\[
p\left(\frac{13^2 \cdot 5 \cdot 6783 \cdot n + 1}{24}\right) \equiv 0 \mod 13^2.
\]
In the same section, we will also discuss congruences of type \( p(5^j \ell^n + B) \equiv 0 \mod 5^{j+1} \).

**Notations.** Throughout the paper, we let \( S_\lambda(\Gamma_0(N), \chi) \) denote the space of cusp forms of weight \( \lambda \) and level \( N \) with character \( \chi \). By an invariant subspace of \( S_\lambda(\Gamma_0(N), \chi) \) we mean a subspace that is invariant under the action of the Hecke algebra on the space.

For a power series \( f(q) = \sum a_f(n)q^n \) and a positive integer \( N \), we let \( U_N \) and \( V_N \) denote the operators
\[
U_N : f(q) \mapsto f(q)|_{n=0}^{\infty} a_f(Nn)q^n,
\]
\[
V_N : f(q) \mapsto f(q)|_{n=0}^{\infty} a_f(n)q^{Nn}.
\]
Moreover, if \( \psi \) is a Dirichlet character, then \( f \otimes \psi \) denotes the twist \( f \otimes \psi := \sum a_f(n)\psi(n)q^n \).

Finally, for a prime \( m \geq 5 \) and a positive integer \( j \), we write
\[
F_{m,j} = \sum_{n \geq 0, m \mid n = -1 \mod 24} p\left(\frac{m^j n + 1}{24}\right) q^n.
\]

Note that we have
\[
(5) \quad F_{m,j} |_{U_m} = F_{m,j+1}.
\]

2. **Works of Ono [12], Weaver [18], and Chua [8]**

In this section, we will review the ideas in [12, 18, 8].

First of all, by a classical identity of Euler, we know that the generating function of \( p(n) \) has an infinite product representation
\[
\sum_{n=0}^{\infty} p(n)q^n = \prod_{n=1}^{\infty} \frac{1}{1 - q^n}.
\]

If we set \( q = e^{2\pi i \tau} \), then we have
\[
q^{-1/24} \sum_{n=0}^{\infty} p(n)q^n = \eta(\tau)^{-1},
\]
where \( \eta(\tau) \) is the Dedekind eta function. Now assume that \( m \) is a prime greater than 3.

Ono [12] considered the function \( \frac{\eta(m^k \tau m^k)}{\eta(\tau)} \). On the one hand, one has
\[
\frac{\eta(m^k \tau m^k)}{\eta(\tau)} |_{U_{m^k}} = \prod_{n=1}^{\infty} (1 - q^n)^{m^k} \cdot \left(\sum_{n=0}^{\infty} p(n)q^{n+(m^{2k} - 1)/24}\right) |_{U_{m^k}}.
\]

On the other hand, one has
\[
\frac{\eta(m^k \tau m^k)}{\eta(\tau)} \equiv \eta(\tau)^{m^{2k} - 1} = \Delta(\tau)^{(m^{2k} - 1)/24} \mod m,
\]
where $\Delta(\tau) = \eta(\tau)^{24}$ is the normalized cusp form of weight 12 on $SL(2, \mathbb{Z})$. From this, Ono [12, Theorem 6] deduced that

$$F_{m,k} \equiv \frac{(\Delta(\tau^{m^2-1})/24|U_{m,k})|V_{24}}{\eta(24\tau^{m^k})} \mod m.$$ 

Now it can be verified that for $k = 1$, the right-hand side of the above congruence is contained in the space $S(m^2-m-1)/2(\Gamma_0(576m), \chi_{12})$ of cusp forms of level 576m and weight $(m^2 - m - 1)/2$ with character $\chi_{12} = \left(\frac{12}{m}\right)$. Then by (5) and the fact that $U_m$ defines a linear map

$$U_m : S_{\lambda+1/2}(\Gamma_0(4Nm), \psi) \rightarrow S_{\lambda+1/2}(\Gamma_0(4Nm), \psi \chi_m), \quad \chi_m = \left(\frac{m}{\ell}\right),$$

one sees that

$$F_{m,k} \equiv G_{m,k} = \sum a_{m,k}(n)q^n \mod m$$

for some $G_{m,k} \in S(m^2-m-1)/2(\Gamma_0(576m), \chi_{12}\chi_{m}^{k-1})$.

Now recall the general Hecke theory for half-integral weight modular forms states that if $f(\tau) = \sum_{n=1}^{\infty} a_f(n)q^n \in S_{\lambda+1/2}(\Gamma_0(4N), \psi)$ and $\ell$ is a prime not dividing $4N$, then the Hecke operator defined by

$$T_{\ell^2} : f(\tau) \rightarrow \sum_{n=1}^{\infty} \left( a_f(\ell^2n) + \psi(\ell) \left(\frac{(-1)^{\lambda}n}{\ell}\right) \ell^{\lambda-1}a_f(n) + \psi(\ell^2)\ell^{2\lambda-1}a_f(n/\ell^2) \right) q^n$$

sends $f(\tau)$ to a cusp form in the same space. In the situation under consideration, if $\ell$ is a prime not dividing 576m such that

$$G_{m,k}|T_{\ell^2} \equiv 0 \mod m,$$

then we have

$$0 \equiv (G_{m,k}|T_{\ell^2})|U_{\ell} \mod m$$

$$= \sum_{n=1}^{\infty} \left( a_{m,k}(\ell^3n) + \psi(\ell^2)\ell^{m^2-m-3}a_{m,k}(n/\ell) \right) q^n$$

since $\left(\frac{\ell}{m}\right) = 0$. In particular, if $n$ is not divisible by $\ell$, then

$$a_{m,k}(\ell^3n) \equiv 0 \mod m,$$

which implies

$$p \left( \frac{m^k\ell^3n+1}{24} \right) \equiv 0 \mod m.$$ 

Finally, to show that there is a positive proportion of primes $\ell$ such that $G_{m,k}|T_{\ell^2} \equiv 0 \mod m$, Ono invoked the Shimura correspondence between half-integral weight modular forms and integral weight modular forms [15] and a result of Serre [14, 6.4].

As mentioned earlier, Ono [12] did not address the issue of finding explicit congruences of the form (2). However, Section 4 of [12] did give us some hints on how one might proceed to discover new congruences, at least for small primes $m$. The key observation is the following.

The modular form $G_{m,k}$ itself is in a vector space of big dimension, so to determine whether $G_{m,k}|T_{\ell^2}$ vanishes modulo $m$, one needs to compute the Fourier coefficients of $G_{m,k}$ for a huge number of terms. However, it turns out that $F_{m,k}$ is congruent to another
half-integral weight modular form of a much smaller weight. For example, using Sturm’s theorem \[16\] Ono verified that

\begin{align*}
F_{13,2k+1} &\equiv G_{13,2k+1} \equiv 11 \cdot 6^k \eta(24\tau)^{11} \mod 13, \\
F_{13,2k+2} &\equiv G_{13,2k+2} \equiv 10 \cdot 6^k \eta(24\tau)^{23} \mod 13
\end{align*}

for all non-negative integers \(k\). The modular form \(\eta(24\tau)^{11}\) is in fact a Hecke eigenform. (The modular form \(\eta(24\tau)^{23}\) is also a Hecke eigenform as we shall see in Section 5.) More generally, for \(m \in \{13, 17, 19, 23, 29, 31\}\), it is shown in [12 Section 4], [9 Proposition 6] and [18 Proposition 5] that \(G_{m,1}\) is congruent to a Hecke eigenform of weight \(m/2 - 1\).

Using this observation, Weaver [18] then devised an algorithm to find explicit congruences of the form (2) for \(m\) in the range\(r\) such that \(24\tau\) is congruent to a modular form of weight \(m\) modulo 24. (Incidently, this also proves Ramanujan’s congruences for \(m = 5, 7, 11\), since there are no non-trivial cusp forms of weight 4, 6, 10.) By examining the order of vanishing of \(f_m(\tau)\) at \(\infty\), Chua [8 Theorem 1.1] then concluded that if we let \(r_m\) denote the integer in the range \(0 < r_m < 24\) such that \(m \equiv -r_m \mod 24\), then

\[F_{m,1} \equiv \eta(24\tau)^{r_m} \phi_m(24\tau) \mod 13\]

for some modular form \(\phi_m\) on \(SL(2, \mathbb{Z})\) of weight \((m - r_m - 2)/2\). Furthermore, based on an extensive numerical computation, Chua made the following conjecture.

**Conjecture 2.1** (Chua [8 Conjecture 1]). Let \(m \geq 13\) be a prime and \(r_m\) be the integer in the range \(0 < r_m < 24\) such that \(m \equiv -r_m \mod 24\). Set

\[r_{m,j} = \begin{cases} r_m, & \text{if } j \text{ is odd,} \\ 23, & \text{if } j \text{ is even.} \end{cases}\]
Then
\[ F_{m,j} = \eta(24\tau)^{m-j} \phi_{m,j}(24\tau) \mod m \]
for some modular form \( \phi_{m,j}(\tau) \) on \( \text{SL}(2, \mathbb{Z}) \), where the weight of \( \phi_{m,j} \) is \((m - r_m - 2)/2\) if \( j \) is odd and is \( m - 13 \) if \( j \) is even.

In [8] Section 4, Chua established the induction step for the case of even \( j \) assuming the conjecture holds for odd \( j - 1 \). However, as remarked by Chua, it appears difficult to prove the induction step from cases of even \( j - 1 \) to cases of odd \( j \). In the next section, we will see that this conjecture is a simple consequence of our Theorem 2.

Remark 2.2. Professor H. H. Chan has kindly informed us that Serre has indicated to him an argument to establish Conjecture 2.1. The argument will be given in a forthcoming article [7].

3. Statements of main results

The functions \( \eta(24\tau)^{m+k} \phi_{m,k}(24\tau) \) appearing in Chua’s conjecture (Conjecture 2.1) are all half-integral weight modular forms of level 576 and character \( \chi_{12} \). Thus, our first main result is concerned with the space \( S_{\lambda+1/2}(\Gamma_0(576), \chi_{12}) \).

Theorem 2. Let \( r \) be an odd integer with \( 0 < r < 24 \). Let \( s \) be a non-negative even integer. Then the space
\[ S_{r,s} := \{ \eta(24\tau)^r f(24\tau) : f(\tau) \in M_s(\text{SL}(2, \mathbb{Z})) \} \]
is an invariant subspace of \( S_{s+r/2}(\Gamma_0(576), \chi_{12}) \) under the action of the Hecke algebra. That is, for all primes \( l \neq 2, 3 \) and all \( f \in S_{r,s} \), we have \( f|T_l^r \in S_{r,s} \).

The following corollary is immediate.

Corollary 3. Let \( r \) be an odd integer with \( 0 < r < 24 \). Let \( E_4(\tau) \) and \( E_6(\tau) \) be the Eisenstein series of weights 4 and 6 on \( \text{SL}(2, \mathbb{Z}) \) and \( f(\tau) \) be one of the function \( 1, E_4(\tau), E_6(\tau), E_4(\tau)^2, E_4(\tau)E_6(\tau), \) and \( E_4(\tau)^2E_6(\tau) \). Then the function \( \eta(24\tau)^r f(24\tau) \) is a Hecke eigenform. In particular, for \( m \in \{ 13, 17, 19, 23, 29, 31 \} \), the function
\[ \eta(24\tau)^m \phi_{m,1}(24\tau) \]
in Conjecture 2.1 is a Hecke eigenform.

Note that the assertion about \( g_m := \eta(24\tau)^m \phi_{m,1} \) was already proved in Proposition 6 of [9]. In the same proposition, it was also proved that the image of \( g_m \) under the Shimura correspondence is \( G_m \otimes \chi_{12} \), where \( G_m \) is the unique normalized newform of weight \( m-3 \) on \( \Gamma_0(6) \) whose eigenvalues for the Atkin-Lehner involutions \( W_2 \) and \( W_3 \) are \( -\left( \frac{2}{m} \right) \) and \( -\left( \frac{3}{m} \right) \), respectively.

We now apply Theorem 2 to study congruences of the partition function. We first consider Conjecture 2.1. Observe that the Hecke operator \( T_{m^2} \) is the same as the operator \( U_{m^2} \mod m \). Also, the case \( j = 1 \) and the induction step from \( j = 1 \) to \( j = 2 \) have already been proved in [8]. Thus, from Theorem 2 we immediately conclude that Chua’s conjecture indeed holds in general.

Corollary 4 (Conjecture of Chua). Let \( m \geq 13 \) be a prime and \( r_m \) be the integer in the range \( 0 < r_m < 24 \) such that \( m \equiv -r_m \mod 24 \). Set
\[ r_{m,j} = \begin{cases} r_m, & \text{if } j \text{ is odd}, \\ 23, & \text{if } j \text{ is even}. \end{cases} \]
Then

\[ F_{m,j} = \eta(24\tau)^{r_{m,j}} \phi_{m,j}(24\tau) \mod m \]

for some modular form \( \phi_{m,j}(\tau) \) on \( \text{SL}(2, \mathbb{Z}) \), where the weight of \( \phi_{m,j} \) is \((m - r_m - 2)/2\) if \( j \) is odd and is \( m - 13 \) if \( j \) is even.

**Remark 3.1.** Note that for odd \( j \), we have

\[ \dim S_{m,n}(\mathbb{Z}) = \left\lfloor \frac{m}{12} \right\rfloor - \left\lfloor \frac{m}{24} \right\rfloor. \]

To see this, we observe that \( \dim \mathcal{M}_n(\text{SL}(2, \mathbb{Z})) \) is periodic of period 12. Thus, to show (8), we only need to verify case by case according to the residue of \( m \) modulo 24.

Using the pigeonhole principle, one can see that Theorem 2 also yields Ono’s periodicity result (5), with an improved bound.

**Corollary 5.** Let \( m \geq 5 \) be a prime. Then there exist integers \( 0 \leq N(m) \leq m A(m) \) and \( 0 \leq P(m) \leq m A(m) \) such that

\[ p \left( \frac{m^{n+1} / 24}{24} \right) \equiv p \left( \frac{m^{P(m)+1} / 24}{24} \right) \mod m \]

for all non-negative integers \( n \), where

\[ A(m) = 2 \dim \mathcal{M}_{m,2} \text{SL}(2, \mathbb{Z}) \]

and \( r_m \) is the integer satisfying \( 0 < r_m < 24 \) and \( m = -r_m \mod 24 \).

**Corollary 6.** Let \( r \) be an odd integer satisfying \( 0 < r < 24 \) and \( s \) be a non-negative even integer. Let \( S_{r,s} \) be defined as (7) and \( \{f_1, \ldots, f_t\} \) be a \( \mathbb{Z} \)-basis for the \( \mathbb{Z} \)-module \( \mathbb{Z}[q] \cap S_{r,s} \). Given a prime \( \ell \geq 5 \), assume that \( A \) is the \( t \times t \) matrix such that

\[ \begin{pmatrix} f_1 \\ \vdots \\ f_t \end{pmatrix} | T_{\ell^2} = A \begin{pmatrix} f_1 \\ \vdots \\ f_t \end{pmatrix}. \]

Then we have

\[ \begin{pmatrix} f_k \\ \vdots \\ f_t \end{pmatrix} | U_{\ell^2}^k = A_k \begin{pmatrix} f_1 \\ \vdots \\ f_t \end{pmatrix} + B_k \begin{pmatrix} g_1 \\ \vdots \\ g_t \end{pmatrix} + C_k \begin{pmatrix} f_1 \\ \vdots \\ f_t \end{pmatrix} | V_{\ell^2}, \]

where \( g_j = f_j \otimes (\frac{r}{\ell}) \), and \( A_k, B_k, \) and \( C_k \) are \( t \times t \) matrices satisfying

\[ \begin{pmatrix} A_k \\ A_{k-1} \end{pmatrix} = \begin{pmatrix} A & -\ell r + 2s - 2I_t \\ I_t & 0 \end{pmatrix}^k \begin{pmatrix} I_t \\ 0 \end{pmatrix}, \]

and

\[ B_k = -\ell^{s+(r-3)/2} \begin{pmatrix} -1 \end{pmatrix}^{(r-1)/2} A_k^{-1}, \quad C_k = -\ell r + 2s - 2A_k^{-1}. \]

**Theorem 7.** Let \( m \geq 13 \) be a prime and \( j \) be a positive integer. Set \( r_m \) to be the integer satisfying \( 0 < r_m < 24 \) and \( m = -r_m \mod 24 \). Let

\[ t = \left\lfloor \frac{m}{12} \right\rfloor - \left\lfloor \frac{m}{24} \right\rfloor \]
be the dimension of \( S_{r_m, (m-r_m-2)/2} \) and assume that \( \{ f_1, \ldots, f_t \} \) is a \( \mathbb{Z} \)-basis for the \( \mathbb{Z} \)-module \( \mathbb{Z}[q] \cap S_{r_m, (m-r_m-2)/2} \). Let \( \ell \) be a prime different from 2, 3, and \( m \), and assume that \( A \) is the \( t \times t \) matrix such that

\[
\begin{pmatrix}
  f_1 \\
  \vdots \\
  f_t
\end{pmatrix}
= A
\begin{pmatrix}
  f_1 \\
  \vdots \\
  f_t
\end{pmatrix}.
\]

Assume that the order of the square matrix

\[
\begin{pmatrix}
  A & -\ell^{m-4}I_t \\
  I_t & 0
\end{pmatrix}
\mod m
\]

in \( \text{PGL}(2t, \mathbb{F}_m) \) is \( K \), then we have

\[
p \left( \frac{m^j \ell^u K - 1}{24} \right) \equiv 0 \mod m
\]

for all positive integers \( j \) and \( u \) and all positive integers \( n \) not divisible by \( \ell \).

Also, if the order of the matrix \( \text{(10)} \) in \( \text{GL}(2t, \mathbb{F}_m) \) is \( M \), then we have

\[
p \left( \frac{m^j \ell^i n + 1}{24} \right) \equiv p \left( \frac{m^j \ell^{2M+4} n + 1}{24} \right) \mod m
\]

for all non-negative integer \( i \) and all positive integers \( j \) and \( n \).

**Remark 3.2.** Note that if the matrix \( A \) in the above theorem vanishing modulo \( m \), then the matrix in \( \text{(10)} \) has order 2 in \( \text{PGL}(2t, \mathbb{F}_m) \), and the conclusion of the theorem asserts that

\[
p \left( \frac{m^j \ell^3 n + 1}{24} \right) \equiv 0 \mod m.
\]

This is the congruence appearing in Ono’s theorem.

**Remark 3.3.** In general, the integer \( K \) in Theorem 7 may not be the smallest positive integer such that congruence \( \text{(4)} \) holds. We choose to state the theorem in the current form because of its simplicity. See the remark following the proof of Theorem 7.

### 4. Proof of Theorem 2

We first recall the following lemma of Atkin and Lehner.

**Lemma 4.1** ([5, Lemma 7]). Let \( f \) be a cusp form of weight \( s \) on \( \Gamma_0(N) \) and \( \ell \) be a prime. Then

(a) If \( \ell \mid N \), then \( f \mid U_\ell \) is a cusp form on \( \Gamma_0(N) \). Furthermore, if \( \ell^2 \mid N \), then \( f \mid U_\ell \) is modular on \( \Gamma_0(N/\ell) \).

(b) If \( \ell \nmid N \) but \( \ell^2 \nmid N \), then \( f \mid (U_\ell + \ell^{s/2-1}W_\ell) \) is a cusp form on \( \Gamma_0(N/\ell) \).

The following transformation formula for \( \eta(\tau) \) is frequently used.

**Lemma 4.2** ([19, pp.125–127]). For

\[
\gamma = \begin{pmatrix}
  a & b \\
  c & d
\end{pmatrix} \in \text{SL}_2(\mathbb{Z}),
\]

the transformation formula for \( \eta(\tau) \) is given by, for \( c = 0 \),

\[
\eta(\tau + b) = e^{\pi ib/12} \eta(\tau),
\]
and, for \( c > 0 \),

\[
\eta(\gamma \tau) = \epsilon(a, b, c, d) \sqrt{\frac{c \tau + d}{i}} \eta(\tau)
\]

with

\[
\epsilon(a, b, c, d) = \begin{cases} \left( \frac{d}{c} \right) e^{(1-c)/2} e^{\pi i (bd(1-c^2) + c(a+d))/12}, & \text{if } c \text{ is odd}, \\
\left( \frac{c}{d} \right) e^{\pi i (ac(1-d^2) + (b+c+1))/12}, & \text{if } d \text{ is odd},
\end{cases}
\]

where \( \left( \frac{d}{c} \right) \) is the Legendre-Jacobi symbol.

We now prove Theorem 2. Assume that \( g(\tau) \in S_{r,s} \), say \( g(\tau) = \eta(24\tau)^r f(24\tau) \) for some \( f(\tau) \in M_s(\text{SL}(2, \mathbb{Z})) \). Assume \( g(\tau) = q^{-s} \sum_{n=0}^{\infty} a(n)q^{24n} \). Then by the definition of \( T_{\ell^2} \), we have

\[
g|T_{\ell^2} = \sum_{n \geq 0, n \equiv -r/24 \mod \ell^2} a(n)q^{(24n+r)/\ell^2}
\]

\[
+ \ell^s+e^{(r-3)/2} \sum_{n=0}^{\infty} \left( \frac{-1}{\ell} \right)^{r-1}/212 \sum_{n=0}^{24n+r} \left( \frac{24n+r}{\ell} \right) a(n)q^{24n+r}
\]

\[
+ \ell^{r+2s-2} \sum_{n=0}^{\infty} a(n)q^{\ell^2(24n+r)}.
\]

We now consider the function

\[
h(\tau) = \eta(\ell^2 \tau)^{24-r} g(\tau/24) = \eta(\ell^2 \tau)^{24-r} \eta(\tau)^r f(\tau).
\]

Using Newman’s criterion \[^{11} \text{Theorem } 1\], we see that \( h(\tau) \) is a cusp form of weight \( s + 12 \) on \( \Gamma_0(\ell^2) \). Then by Lemma \[^{4} \text{Lemma } 4\], \( h|U_{\ell^2} + \ell^{s/2+5} U_{\ell^2} \) is a cusp form on \( \text{SL}(2, \mathbb{Z}) \), that is,

\[
h|U_{\ell^2} + \ell^{s/2+5} U_{\ell^2} = \eta(\tau)^{24} h(\tau)
\]

for some modular form \( \tilde{h}(\tau) \) of weight \( s \) on \( \text{SL}(2, \mathbb{Z}) \). We claim that

\[
h|U_{\ell^2} + \ell^{s/2+5} U_{\ell^2} = \eta(\tau)^{24-r} (g|T_{\ell^2})(\tau/24).
\]

Once this is proved, by comparing (14) and (15), we immediately get Theorem 2. We now verify (15).

By the definition of \( U_{\ell^2} \) we have

\[
h|U_{\ell^2} = \left( \prod_{n=1}^{\infty} (1 - q^{e^2 n})^{24-r} \sum_{n=0}^{\infty} a(n)q^{(24n-\ell(\ell^2-1))/24+n} \right) |U_{\ell^2}
\]

\[
= q \prod_{n=1}^{\infty} (1 - q^n)^{24-r} \sum_{n \geq 0, n \equiv -r/24 \mod \ell^2} a(n)q^{(24n-r(\ell^2-1))/24\ell^2}
\]

\[
= \eta(\tau)^{24-r} \sum_{n \geq 0, n \equiv -r/24 \mod \ell^2} a(n)q^{(24n+r)/24\ell^2}.
\]

The term involving \( U_{\ell^2} \) is more complicated. We have

\[
h|U_{\ell^2} = \left( \frac{1}{\ell} \sum_{k=0}^{\ell-1} h \begin{pmatrix} 1 & k \\ 0 & \ell \end{pmatrix} \right) |W_{\ell} = \ell^{-s/2-7} \tau^{-s-12} \sum_{k=0}^{\ell-1} h \begin{pmatrix} 1 & k \\ 0 & \ell \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.
\]
The term $k = 0$ gives us
\[ \ell^{-s/2} \tau^{-s-12} h(-1/\ell^2 \tau) = \ell^{-s/2} \tau^{-s-12} \eta(-1/\ell^2 \tau)^24-r \eta(-1/\ell^2 \tau)^{r} f(-1/\ell^2 \tau). \]

Using the formula $\eta(-1/\tau) = \sqrt{(\tau/i)}\eta(\tau)$ and the assumption that $f(\tau) \in M_n(\text{SL}(2, \mathbb{Z}))$, this reduces to
\[ e^{3s/2} \tau^{-r} \eta(\tau)^{24-r} f(\ell^2 \tau) = \ell^{3s/2} \tau^{-r} \eta(\tau)^{24-r} \sum_{n=0}^{\infty} a(n) q^{(24n+r)/24}. \]

We now consider the contribution from the cases $k \neq 0$.

We have
\[ \eta(\ell^2 \tau) \left( \begin{array}{c} k \ell \\ \ell^2 \end{array} \right) = \eta \left( \frac{k \ell \tau - 1}{\tau} \right). \]

By Lemma 4.2, this is equal to
\[ \eta(\ell^2 \tau) \left( \begin{array}{c} k \ell \\ \ell^2 \end{array} \right) = e^{2\pi ik\ell/24} \sqrt{\frac{\tau}{i}} \eta(\tau). \]

For $\eta(\tau)$ and $f(\tau)$, we observe that
\[ \frac{k \ell \tau - 1}{\ell^2 \tau} = \left( \frac{k}{\ell} - \frac{u}{k'} \right) (\tau - k'/\ell), \]

where $k'$ denotes the multiplicative inverse of $k$ modulo $\ell$ and $u = (kk' - 1)/\ell$. Thus, by Lemma 4.2
\[ \eta(\tau) \left( \begin{array}{c} k \ell \\ \ell^2 \end{array} \right) = \eta \left( \frac{k'}{\ell} - 1 \right) \eta^{(1-\ell)/2} e^{2\pi i(k+k')/24} \sqrt{\frac{\ell \tau}{i}} \eta \left( \tau - \frac{k'}{\ell} \right). \]

Also,
\[ f(\tau) \left( \begin{array}{c} k \ell \\ \ell^2 \end{array} \right) = (\ell \tau)^{r} f \left( \tau - \frac{k'}{\ell} \right). \]

Combining (18), (19), and (20), we obtain
\[ \ell^{-s/2} \tau^{-s-12} h \left| \frac{k \ell}{\ell^2} \right| \left( \begin{array}{c} -1 \\ 0 \end{array} \right) = \ell^{s+2} \tau^{-24} \eta^{(1-\ell)/2} e^{2\pi i k \ell / 24} \eta(\tau)^{24-r} \eta \left( \tau - \frac{k'}{\ell} \right) f \left( \tau - \frac{k'}{\ell} \right), \]

and
\[ \ell^{-s/2} \tau^{-s-12} \sum_{k=1}^{\ell-1} h \left| \frac{k \ell}{\ell^2} \right| \left( \begin{array}{c} -1 \\ 0 \end{array} \right) = \ell^{s+2} \tau^{-24} \eta^{(1-\ell)/2} \eta(\tau)^{24-r} \sum_{k=1}^{\ell-1} \left( \frac{k}{\ell} \right) e^{2\pi i k \ell / 24} g \left( \frac{\tau - k/\ell}{24} \right). \]

The sum in the last expression is equal to
\[ \sum_{k=1}^{\ell-1} \left( \frac{k}{\ell} \right) e^{2\pi ik (\ell^2 - 1)/24 \ell} \sum_{n=0}^{\infty} e^{-2\pi i kn/\ell} a(n) q^{n+r}/24. \]

With the well-known evaluation
\[ \sum_{k=1}^{\ell-1} \left( \frac{k}{\ell} \right) e^{2\pi ikn/\ell} = \left( \frac{n}{\ell} \right) i^{(\ell-1)^2/4} \sqrt{\ell}. \]
of the Gaussian sum, (22) can be simplified to
\[ i^{(\ell-1)/4} \sqrt{\ell} \sum_{n=0}^{\infty} \left( \frac{r(\ell^2 - 1) / 24 - n}{\ell} \right) a(n) q^{n+r/24} \]
\[ = i^{(\ell-1)/4} \sqrt{\ell} \left( \frac{-24}{\ell} \right) \sum_{n=0}^{\infty} \left( \frac{24n + r}{\ell} \right) a(n) q^{n+r/24}. \]
Substituting this into (21) and using
\[ (\ell - s) \frac{1}{2} = 2 - A, \]
we arrive at
\[ (\frac{1}{2}) \ell = (-1)^{(\ell-1)/2}, \quad (\frac{2}{\ell}) = (-1)^{(\ell^2-1)/8}, \]
we have
\[ \ell^{-s/2-7} \tau^{-s-12} \sum_{k=1}^{\ell-1} \left| \begin{array}{cc} kl \ell & -1 \\ \ell^2 & 0 \end{array} \right| \]
\[ = \ell^{(s+r+1)/2-7} \tau^{(1-\ell)/2+(\ell-1)/4} \left( -\frac{24}{\ell} \right) \eta(\tau)^{24-r} \sum_{n=0}^{\infty} \left( \frac{24n + r}{\ell} \right) a(n) q^{n+r/24} \]
\[ = \ell^{(s+r+1)/2-7} \left( \frac{-1}{\ell} \right)^{(r-1)/2} \left( \frac{12}{\ell} \right) \eta(\tau)^{24-r} \sum_{n=0}^{\infty} \left( \frac{24n + r}{\ell} \right) a(n) q^{n+r/24}. \]
Together with (17), (23) implies that
\[ \ell^{s/2+5} h \mid U_{\ell} W_{\ell} = \ell^{2s+r-2} \eta(\tau)^{24-r} \sum_{n=0}^{\infty} a(n) q^{\ell^2(24n+r)/24} \]
\[ + \ell^{s+(r-3)/2} \eta(\tau)^{24-r} \left( \frac{-1}{\ell} \right)^{(r-1)/2} \frac{12}{\ell} \sum_{n=0}^{\infty} \left( \frac{24n + r}{\ell} \right) a(n) q^{n+r/24}. \]
Comparing (16) and (24) with (13), we see that (15) indeed holds. The proof of Theorem 2 is now complete.

5. PROOF OF COROLLARY 6 AND THEOREM 7

Proof of Corollary 6 By the definition of \( T_{\ell^2} \), we have
\[ \left( \begin{array}{c} f_1 \\ \vdots \\ f_{\ell} \end{array} \right) | U_{\ell^2} = A_1 \left( \begin{array}{c} f_1 \\ \vdots \\ f_{\ell} \end{array} \right) + B_1 \left( \begin{array}{c} g_1 \\ \vdots \\ g_{\ell} \end{array} \right) + C_1 \left( \begin{array}{c} f_1 \\ \vdots \\ f_{\ell} \end{array} \right) | V_{\ell^2}, \]
where \( g_t = f_t \otimes (\tau) \) and
\[ A_1 = A, \quad B_1 = -\ell^{s+(r-3)/2} \left( \frac{(-1)^{(r-1)/2} \tau^{12}}{\ell} \right) I_{\ell^2}, \quad C_1 = -\ell^{r+2s-2} I_{\ell^2}. \]
Now we make the key observation
\[ g_j | U_{\ell^2} = 0, \quad f_j | V_{\ell^2} | U_{\ell^2} = f_j, \]
from which we obtain
\[ \left( \begin{array}{c} f_1 \\ \vdots \\ f_{\ell} \end{array} \right) | U_{\ell^2} = (A_1^2 + C_1) \left( \begin{array}{c} f_1 \\ \vdots \\ f_{\ell} \end{array} \right) + A_1 B_1 \left( \begin{array}{c} g_1 \\ \vdots \\ g_{\ell} \end{array} \right) + A_1 C_1 \left( \begin{array}{c} f_1 \\ \vdots \\ f_{\ell} \end{array} \right) | V_{\ell^2}. \]
Iterating, we see that in general if
\[
\begin{pmatrix}
f_1 \\ \\
\vdots \\ \\
f_t
\end{pmatrix}
\begin{pmatrix}
f_1 \\ \\
\vdots \\ \\
f_t
\end{pmatrix}
= A_k
\begin{pmatrix}
f_1 \\ \\
\vdots \\ \\
f_t
\end{pmatrix}
+ B_k
\begin{pmatrix}
g_1 \\ \\
\vdots \\ \\
g_t
\end{pmatrix}
+ C_k
\begin{pmatrix}
f_1 \\ \\
\vdots \\ \\
f_t
\end{pmatrix}
\end{pmatrix}
\begin{pmatrix}
V_\ell \\ \\
V_\ell \\
V_\ell
\end{pmatrix},
\]
then the coefficients satisfy the recursive relation
\[
A_{k+1} = A_k A_1 + C_k, \quad B_{k+1} = A_k B_1, \quad C_{k+1} = A_k C_1.
\]
(Note that \(B_1\) and \(C_1\) are scalar matrices. Thus, all coefficients are polynomials in \(A\).)
Finally, we note that the relation \(A_{k+1} = A_k A_1 + C_k = A_k A_1 + C_1 A_{k-1}\) can be written as
\[
\begin{pmatrix}
A_{k+1} \\ \\
A_k
\end{pmatrix} = \begin{pmatrix}
A & C_1 \\ I_t & 0
\end{pmatrix}
\begin{pmatrix}
A_k \\ A_{k-1}
\end{pmatrix},
\]
which yields
\[
\begin{pmatrix}
A_{k+1} \\ \\
A_k
\end{pmatrix} = \begin{pmatrix}
A & C_1 \\ I_t & 0
\end{pmatrix}^k
\begin{pmatrix}
A \\ I_t
\end{pmatrix} = \begin{pmatrix}
A & C_1 \\ I_t & 0
\end{pmatrix}^{k+1}
\begin{pmatrix}
I_t \\ 0
\end{pmatrix}.
\]
This proves the theorem. \(\Box\)

**Proof of Theorem** Let \(m \geq 13\) be a prime. Let \(r\) be the integer satisfying \(0 < r < 24\) and \(m \equiv -r \mod 24\) and set \(s = (m - r - 2)/2\). By Corollary 4, \(F_{m,1}\) is congruent to a modular form in \(S_{r,s}\), where \(S_{r,s}\) is defined by (7). Now let \(\{f_1, \ldots, f_t\}\) be a basis for \(S_{r,s}\) and \(A\) be given as in the statement of the theorem. Then by Corollary 5 we know that
\[
\begin{pmatrix}
f_1 \\ \\
\vdots \\ \\
f_t
\end{pmatrix}
\begin{pmatrix}
f_1 \\ \\
\vdots \\ \\
f_t
\end{pmatrix}
= A_k
\begin{pmatrix}
f_1 \\ \\
\vdots \\ \\
f_t
\end{pmatrix}
+ B_k
\begin{pmatrix}
g_1 \\ \\
\vdots \\ \\
g_t
\end{pmatrix}
+ C_k
\begin{pmatrix}
f_1 \\ \\
\vdots \\ \\
f_t
\end{pmatrix}
\end{pmatrix}
\begin{pmatrix}
V_\ell \\ \\
V_\ell \\
V_\ell
\end{pmatrix},
\]
where \(g_j = f_j \otimes (7)\), and \(A_k, B_k,\) and \(C_k\) are \(t \times t\) matrices satisfying
\[
\begin{pmatrix}
A_k \\ A_{k-1}
\end{pmatrix} = X^k
\begin{pmatrix}
I_t \\ 0
\end{pmatrix},
\]
\[
B_k = -\ell^{(m-5)/2} \left( \frac{(-1)^{(r-1)/2}12}{\ell} \right) A_{k-1}, \quad C_k = -\ell^{m-4} A_{k-1}
\]
with
\[
X = \begin{pmatrix}
A & -\ell^{m-4} I_t \\ I_t & 0
\end{pmatrix}
\]
for all \(k \geq 1\). Now we have
\[
X^{-1} = \ell^{-(m-4)} \begin{pmatrix}
0 & \ell^{m-4} I_t \\ -I_t & A
\end{pmatrix}
\]
Therefore, if the order of \(X \mod m\) in \(\text{PGL}(2t, \mathbb{F}_m)\) is \(K\), then we have
\[
\begin{pmatrix}
A_{uK-1} \\ A_{uK-2}
\end{pmatrix} = X^{uK-1}
\begin{pmatrix}
I_t \\ 0
\end{pmatrix} \equiv \begin{pmatrix}
0 \\ U
\end{pmatrix} \mod m.
\]
for some \(t \times t\) matrix \(U\), that is, \(A_{uK-1} \equiv 0 \mod m\). The rest of proof follows Ono’s argument.
We have
\[
\begin{pmatrix}
 f_1 \\
 \vdots \\
 f_t
\end{pmatrix} \big|_{U_{\ell^2}^{nK-1}} \equiv B u_{K-1} \begin{pmatrix}
 g_1 \\
 \vdots \\
 g_t
\end{pmatrix} + C u_{K-1} \begin{pmatrix}
 f_1 \\
 \vdots \\
 f_t
\end{pmatrix} \big|_{V_{\ell^2}} \mod m
\]
and
\[
\begin{pmatrix}
 f_1 \\
 \vdots \\
 f_t
\end{pmatrix} \big|_{U_{\ell^2}^{nK-1}} U_{\ell^2} \equiv C u_{K-1} \begin{pmatrix}
 f_1 \\
 \vdots \\
 f_t
\end{pmatrix} \big|_{V_{\ell^2}} \mod m.
\]
This implies that the $\ell^{2uK-1}$th Fourier coefficients of $f_j$ vanishes modulo $m$ for all $j$ and all $n$ not divisible by $\ell$. Since $F_{m,1}$ is a linear combination of $f_j$ modulo $m$, the same thing is true for the $\ell^{2uK-1}$th Fourier coefficients of $F_{m,1}$. This translates to
\[
p \left( \frac{m\ell^{2uK-1}n + 1}{24} \right) \equiv 0 \mod m
\]
for all $n$ not divisible by $\ell$. This proves (11) for the case $j = 1$.

For the case $j > 1$, we note that the operators $U_{\ell^2}$ and $U_m$ commutes. Thus,
\[
\begin{pmatrix}
 f_1 \\
 \vdots \\
 f_t
\end{pmatrix} \big|_{U_{m}^{j}} U_{\ell^2} = A_k \begin{pmatrix}
 f_1 \\
 \vdots \\
 f_t
\end{pmatrix} \big|_{U_{m}^{j}} + B_k \begin{pmatrix}
 g_1 \\
 \vdots \\
 g_t
\end{pmatrix} \big|_{U_{m}^{j}} + C_k \begin{pmatrix}
 f_1 \\
 \vdots \\
 f_t
\end{pmatrix} \big|_{V_{\ell^2}} U_{m}^{j},
\]
where $A_k$, $B_k$, and $C_k$ satisfy the same relations (25) and (26). Taking the fact (5) into account, we see that the same argument in the case $j = 1$ gives us the general congruence.

Finally, if the matrix $X$ has order $M$ in $\text{GL}(2t, \mathbb{F}_m)$, then from the recursive relations (25) and (26), it is obvious that (12) holds. This completes the proof. \qed

**Remark 5.1.** In general, the integer $K$ in Theorem 7 may not be the smallest positive integer such that congruence (4) hold. To see this, for simplicity, we assume that $S_{r,s}$ has dimension $t$ and its reduction modulo $m$ has a basis consisting of Hecke eigenforms $f_1, \ldots, f_t$ defined over $\mathbb{F}_m$. If the eigenvalues of $T_{r^2}$ for $f_i$ modulo $m$ are $a_{\ell^i}^{(1)}, \ldots, a_{\ell^i}^{(t)} \in \mathbb{F}_m$. Let $k_i$ denote the order of \( \left( a_{\ell^i}^{(1)} - \ell^{m-4} \right) \) in $\text{PGL}(2, \mathbb{F}_m)$. Let $k$ be the least common multiple of $k_i$. Then we can show that
\[
f_i | U_{\ell^2}^{2k-1} \equiv c_i f_i | V_{\ell^2} \mod m
\]
for some $c_i \in \mathbb{F}_m$ and consequently congruence (4) holds. Of course, the least common multiple of $k_i$ may be smaller than the integer $K$ in Theorem 7 in general.

6. **Examples**

**Example 6.1.** Let $m = 13$. According to Corollary 4 we have
\[
F_{13,1} \equiv c \eta(24\tau)^{11} \mod 13
\]
for some $c \in \mathbb{F}_{13}$. (In fact, $c = 11$. See page 303.) The eigenvalues $a_\ell$ modulo 13 of $T_{r^2}$ for the first few primes $\ell$ are

| $\ell$ | 5  | 7  | 11 | 17 | 19 | 23 | 29 | 31 | 37 | 41 | 43 | 47 | 53 | 59 | 61 | 67 | 73 |
|-------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| $a_\ell$ | 10 | 8  | 5  | 1  | 8  | 4  | 4  | 5  | 9  | 12 | 6  | 10 | 0  | 2  | 4  | 0  |
| $\ell^a$ | 5  | 8  | 12 | 5  | 12 | 1  | 5  | 8  | 5  | 12 | 8  | 1  | 8  | 1  | 5  | 5  |
For $\ell = 5$, the matrix

$$X = \begin{pmatrix} a_5 - \ell^9 & -\ell^9 \\ 1 & 0 \end{pmatrix} \equiv \begin{pmatrix} 10 & 8 \\ 1 & 0 \end{pmatrix} \mod 13$$

has eigenvalues $5 \pm \sqrt{7}$ over $\mathbb{F}_{13}$. Now the order of $(5 + \sqrt{7})/(5 - \sqrt{7})$ in $\mathbb{F}_{169}$ is 14. This implies that $14$ is the order of $X$ in $\text{PGL}(2, \mathbb{F}_{13})$ and we have

$$p\left( \frac{13 \cdot 5^{2u-1} n + 1}{24} \right) \equiv 0 \mod 13$$

for all positive integers $u$ and all positive integers $n$ not divisible by 5. Likewise, we find congruence (4) holds with

| $\ell$ | 5  | 7  | 11 | 17 | 19 | 23 | 29 | 31 | 37 | 41 | 43 | 47 | 53 | 59 | 61 | 67 | 73 |
|-------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| $k$   | 14 | 14 | 14 | 7  | 14 | 3  | 6  | 12 | 14 | 12 | 7  | 12 | 7  | 2  | 13 | 12 | 2  |

**Example 6.2.** Let $m = 37$. By Corollary [3] we know that $F_{37,1}$ is congruent to a cusp form in $S_{11,12}$ modulo 37. In fact, according to [3] Table 3.1,

$$F_{37,1} \equiv \eta(24\tau)^{11}(E_4(24\tau)^3 + 17\Delta(24\tau)) \mod 37.$$ 

The two eigenforms of $S_{11,12}$ are defined over a certain real quadratic number field, but the reduction of $S_{11,12} \cap \mathbb{Z}[\eta]$ modulo 37 has eigenforms defined over $\mathbb{F}_{37}$. They are

$$f_1 = \eta(24\tau)^{11}(E_4(24\tau)^3 + 24\Delta(24\tau)), \quad f_2 = \eta(24\tau)^{11}\Delta(24\tau).$$

Let $a_i^{(i)}$ denote the eigenvalue of $T_\ell^2$ associated to $f_i$. We have the following data.

| $\ell$ | 5  | 7  | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 41 | 43 | 47 | 53 | 59 | 61 |
|-------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| $a_\ell^{(1)}$ | 1  | 33 | 22 | 7  | 11 | 0  | 1  | 9  | 35 | 11 | 28 | 14 | 30 | 24 | 12 |
| $a_\ell^{(2)}$ | 32 | 10 | 0  | 6  | 7  | 8  | 31 | 36 | 9  | 10 | 1  | 35 | 9  | 3  | 16 |
| $a_\ell^{33}$ | 8  | 26 | 38 | 6  | 23 | 8  | 6  | 31 | 31 | 11 | 6  | 1  | 10 | 23 | 29 |

Let

$$X_i = \begin{pmatrix} a_i^{(i)} & -a_i^{33} \\ 1 & 0 \end{pmatrix}.$$ 

For $\ell = 5$, we find the orders of $X_1$ and $X_2$ in $\text{PGL}(2, \mathbb{F}_{37})$ are 38 and 12, respectively. The least common multiple of the orders is 228. Thus, we have

$$p\left( \frac{37 \cdot 5^{2u-1} n + 1}{24} \right) \equiv 0 \mod 37$$

for all positive integers $u$ and all positive integers $n$ not divisible by 5. Note that this is an example showing that the integer $K$ in the statement of Theorem 7 is not optimal. (Here we have $K = 456$.)

For other small primes $\ell$, we find congruence

$$p\left( \frac{37\ell^{2u-1} n + 1}{24} \right) \equiv 0 \mod 37$$

holds for all $n$ not divisible by $\ell$ with

| $\ell$ | 5  | 7  | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 41 | 43 | 47 | 53 | 59 | 61 |
|-------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| $k$   | 228 | 57 | 18 | 684 | 38 | 38 | 684 | 684 | 228 | 171 | 18 | 333 | 18 | 12 | 684 |
7. Generalizations

There are several directions one may generalize Theorem 7. Here we only consider congruences of the partition function modulo prime powers. The case \( m = 5 \) will be dealt with separately because in this case we have a very precise congruence result.

In his proof of Ramanujan’s conjecture for the cases \( m = 5, 7 \), Watson [17, page 111] established a formula

\[
F_{5,j} = \begin{cases} 
\sum_{i \geq 1} c_{j,i} \frac{\eta(120\tau)^{6i-1}}{\eta(24\tau)^{6i}}, & \text{if } j \text{ is odd,} \\
\sum_{i \geq 1} c_{j,i} \frac{\eta(120\tau)^{6i}}{\eta(24\tau)^{6i+1}}, & \text{if } j \text{ is even,}
\end{cases}
\]

where

\[
c_{j,i} \equiv \begin{cases} 
3j - 1 \mod 5, & \text{if } i = 1, \\
0 \mod 5, & \text{if } i \geq 2.
\end{cases}
\]

From the identity, one deduces that

\[
(27) 
F_{5,j} \equiv 3^{j-1} 5^j \mod 5^{j+1}, \quad \text{if } j \text{ is odd,}
\]

\[
(27) 
F_{5,j} \equiv \eta(24\tau)^{19} \mod 5^{j+1}, \quad \text{if } j \text{ is even.}
\]

Then Lovejoy and Ono [10] used this formula to study congruences of the partition function modulo higher powers of 5. One distinct feature of [10] is the following lemma.

**Lemma 7.1** (Lovejoy and Ono [10, Theorem 2.2]). Let \( \ell \geq 5 \) be a prime. Let \( a \) and \( b \) be the eigenvalues of \( \eta(24\tau)^{19} \) and \( \eta(24\tau)^{23} \) for the Hecke operator \( T_{\ell^2} \), respectively. Then we have

\[
a, b \equiv \left( \frac{15}{\ell} \right) (1 + \ell) \mod 5.
\]

With this lemma, Lovejoy and Ono obtained congruences of the form

\[
p \left( \frac{5^j \ell^k n + 1}{24} \right) \equiv 0 \mod 5^{j+1}
\]

for primes \( \ell \) congruent to 3 or 4 modulo 5. Here we shall deduce new congruences using our method.

**Theorem 8.** Let \( \ell \geq 7 \) be a prime. Set

\[
K_\ell = \begin{cases} 
5, & \text{if } \ell \equiv 1 \mod 5, \\
4, & \text{if } \ell \equiv 2, 3 \mod 5, \\
2, & \text{if } \ell \equiv 4 \mod 5.
\end{cases}
\]

Then we have

\[
p \left( \frac{5^j \ell^k n + 1}{24} \right) \equiv 0 \mod 5^{j+1}
\]

for all positive integers \( j \) and \( u \) and all integers \( n \) not divisible by \( \ell \).

**Proof.** In view of (27), We need to study when a Fourier coefficient of \( \eta(24\tau)^{19} \) or \( \eta(24\tau)^{23} \) vanishes modulo 5.

Let \( f = \eta(24\tau)^{19} \). Let \( \ell \geq 7 \) be a prime and \( a \) be the eigenvalue of \( T_{\ell^2} \) associated to \( f \).

By Corollary [6] we have

\[
f | U^{k}_{\ell^2} = a_k f + b_k f \otimes \left( \frac{1}{\ell^2} \right) + c_k f | V_{\ell^2},
\]

\[
(28)
\]

\[
\]
where \( a_1 = a, b_1 = -\ell^8 \left( \frac{-12}{\ell} \right), c_1 = -\ell^{17}, \) and \( a_k = a_{k-1} a_1 + c_{k-1}, b_k = a_{k-1} b_1, \) \( c_k = a_{k-1} c_1. \) According to the proof of Theorem 7, if the order of

\[
\begin{pmatrix}
a & -\ell^{17} \\
1 & 0
\end{pmatrix}
\mod 5
\]

in \( \text{PGL}(\mathbb{F}_5) \) is \( k, \) then

\[
f|U_{\ell^2 u_k^{-1}} \equiv f|V_{\ell} \mod 5
\]

for all positive integers \( u. \) Now by Lemma 7.1 the characteristic polynomial of (29) has a factorization

\[
\left( x - \left( \frac{15}{\ell} \right) \right) \left( x - \left( \frac{15}{\ell} \right) \ell \right)
\]

modulo 5. From this we see that the order of (29) in \( \text{PGL}(\mathbb{F}_5) \) is

\[
K_\ell = \begin{cases} 
5, & \text{if } \ell \equiv 1 \mod 5, \\
4, & \text{if } \ell \equiv 2, 3 \mod 5, \\
2, & \text{if } \ell \equiv 4 \mod 5.
\end{cases}
\]

Thus, (30) holds with \( k = K_\ell. \) This yields the congruence

\[
p \left( \frac{5^i \ell^{2 u K_{\ell^{-1}} n + 1}}{24} \right) \equiv 0 \mod 5^{i+1}
\]

for odd \( j, \) positive integer \( u, \) and all positive integers \( n \) not divisible by \( \ell. \)

The proof of the case \( j \) even is similar to the above and is omitted. \( \square \)

**Remark 7.2.** In [17], Watson also had an identity for \( F_{7,j}, \) with which one can study congruences modulo higher powers of 7. However, because there does not seem to exist an analog of Lemma 7.1 in this case, we do not have a result as precise as Theorem 8.

The next congruence result is an analog of Theorem 2 of [18], which in turn is originated from the argument outlined in [12, page 301].

**Theorem 9.** Let \( \ell \geq 7 \) be a prime. Assume that one of the following situations occurs.

1. \( \ell \equiv 1 \mod 5, \left( \frac{-1}{\ell} \right) = -1 \) with \( k_\ell = 2 \) and \( m_\ell = 5, \) or
2. \( \ell \equiv 2 \mod 5, \left( \frac{-n}{\ell} \right) = (-1)^{t-1} \) with \( k_\ell = 2 \) and \( m_\ell = 4, \) or
3. \( \ell \equiv 3 \mod 5, \left( \frac{-n}{\ell} \right) = (-1)^{t-1} \) with \( k_\ell = 1 \) and \( m_\ell = 4. \)

Then

\[
p \left( \frac{5^i \ell^{2 (um_\ell + k_\ell) n + 1}}{24} \right) \equiv 0 \mod 5^{i+1}
\]

for all non-negative integers \( u. \)

**Proof.** Assume first that \( i \) is odd. Again, in view of (27), we need to study when the Fourier coefficients of \( f(\tau) = \eta(24 \tau)^{19} \) vanish modulo 5.

Let \( \ell \geq 7 \) be a prime and \( \alpha \) be the eigenvalue of \( T_{\ell^2} \) associated to \( \ell. \) By (28), we have

\[
f|U_{\ell^2}^k = a_k f + b_k f \otimes \left( \frac{\cdot}{\ell} \right) + c_k f|V_{\ell^2},
\]

where \( a_k, b_k, c_k \) satisfy

\[
\begin{pmatrix} a_k \\ a_{k-1} \end{pmatrix} = \begin{pmatrix} a & -\ell^{17} \\ 1 & 0 \end{pmatrix}^k \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad b_k \equiv -\left( -\frac{12}{\ell} \right) a_{k-1}, \quad c_k \equiv -\ell a_{k-1} \mod 5.
\]
From Lemma 7.1, we know that for $\ell \equiv 1 \mod 5$, we have $a_1 \equiv 2\epsilon$ and thus the values of $a_k$ modulo 5 are

| $a_1$ | $a_2$ | $a_3$ | $a_4$ | $a_5$ | $a_6$ | $a_7$ | $a_8$ | $a_9$ | $a_{10}$ | $a_{11}$ | $a_{12}$ |
|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| $2\epsilon$ | $3$ | $4\epsilon$ | $0$ | $\epsilon$ | $2$ | $3\epsilon$ | $4$ | $0$ | $1$ | $2\epsilon$ | $3$ |

where $\epsilon = (\frac{15}{\ell})$. Now assume that $f(\tau) = \sum c(n)q^n$. Comparing the $n$th Fourier coefficients of the two sides of (31) for integers $n$ relatively prime to $\ell$, we obtain

$$c(\ell^{2k}n) = (a_k + b_k \left(\frac{n}{\ell}\right)) c(n) \equiv (a_k - a_{k-1} \left(\frac{-12n}{\ell}\right)) c(n) \mod 5.$$ (32)

Thus, if $\left(\frac{-n}{\ell}\right) = -1$, then $c(\ell^{2(5u+2)}n) \equiv 0 \mod 5$. This translates to the congruence

$$p \left(\frac{5\ell^{2(5u+2)}n + 1}{24}\right) \equiv 0 \mod 5.$$ (32)

This proves the first case of the theorem. The proof of the other cases is similar.

**Example 7.3.**

(1) Let $\ell = 11$, $i = 1$, and $n = 67$. Then the first situation occurs. We find

$$p \left(\frac{5 \cdot 11^4 \cdot 67 + 1}{24}\right) = p(204364) = 28469 \ldots \ldots 24450,$$

which is a multiple of 25.

(2) Let $\ell = 11$, $i = 1$, and $n = 19$. The condition in the theorem is not fulfilled, but (32) implies that

$$p \left(\frac{5 \cdot 11^4 \cdot 19 + 1}{24}\right) \equiv p \left(\frac{5 \cdot 19 + 1}{24}\right) \mod 25.$$

Indeed, we have $p(4) = 5,$

$$p(57954) = 37834 \ldots \ldots \ldots 45055,$$

and they are congruent to each other modulo 25.

(3) Let $\ell = 7$, $i = 2$, and $n = 23$. Then the second situation occurs. We have

$$p \left(\frac{5^2 \cdot 7^4 \cdot 23 + 1}{24}\right) = p(57524) = 38402 \ldots \ldots \ldots 43875,$$

which is indeed a multiple of 53.

**Theorem 10.** Let $m \geq 13$ be a prime and $\ell$ be a prime different from 2, 3, $m$. For each positive integer $i$, there exists a positive integer $K$ such that for all $j \geq i$, all $u \geq 1$ and all positive integers $n$ not divisible by $\ell$, the congruence

$$p \left(\frac{m^j\ell^{2uK-1}n + 1}{24}\right) \equiv 0 \mod m^i$$
holds. There is also another positive integer $M$ such that
\[
p \left( \frac{m^j \ell^r n + 1}{24} \right) \equiv p \left( \frac{m^j \ell^{M+r} n + 1}{24} \right) \mod m^i
\]
holds for all $n$.

**Proof.** Let $\beta_{m,i}$ be the integer satisfying $1 \leq \beta_{m,i} \leq m^i - 1$ and $24\beta_{m,i} \equiv 1 \mod m^i$. Define
\[
k_{m,i} = \begin{cases} 
(m^{i-1} + 1)(m - 1)/2 - 12\lfloor m/24 \rfloor - 12, & \text{if } i \text{ is odd}, \\
m^{i-1}(m - 1) - 12, & \text{if } i \text{ is even}.
\end{cases}
\]
By Theorem 3 of [2], for all $i \geq 1$, there is a modular form $f \in M_{k_{m,i}}(\text{SL}(2,\mathbb{Z}))$ such that
\[
F_{m,i} \equiv \eta(24\tau)^{(24\beta_{m,i} - 1)/m^i} f(24\tau) \mod m^i.
\]
The rest of proof is parallel to that of Theorem 7. □

**Example 7.4.** Consider the case $m = 13$ and $i = 2$ of Theorem 10 and assume that $\ell$ is a prime different from 2, 3, 13. By [2, Theorem 3], $F_{13,2}$ is congruent to a modular form in the space $S_{23,144}$ of dimension 13. Choose a $\mathbb{Z}$-basis
\[
f_i = \eta(24\tau)^{23} E_i(24\tau)^{3(i+1-i)} \Delta(24\tau)^{i-1}, \quad i = 1, \ldots, 13,
\]
for $\mathbb{Z}[[q]] \cap S_{23,144}$ and let $A$ be the matrix of $T_{22}$ with respect to this basis. If the order of the matrix
\[
\begin{pmatrix} A & -\ell^{309}I_{13} \\ I_{13} & 0 \end{pmatrix}
\]
in $\text{PGL}(26,\mathbb{Z}/169)$ is $K$, then we have
\[
p \left( \frac{169\ell^{2K-1}n + 1}{24} \right) \equiv 0 \mod 169
\]
for all integers $n$ not divisible by $\ell$. For instance, for $\ell = 5$, we find
\[
A = \begin{pmatrix} 20 & 101 & 52 & 52 & 166 & 148 & 46 & 135 & 96 & 51 & 73 & 49 & 128 \\ 166 & 164 & 159 & 66 & 123 & 50 & 144 & 85 & 29 & 116 & 22 & 93 & 10 \\ 158 & 152 & 90 & 65 & 20 & 167 & 27 & 96 & 109 & 154 & 127 & 164 & 76 \\ 120 & 154 & 132 & 110 & 22 & 113 & 115 & 51 & 25 & 104 & 108 & 82 & 33 \\ 43 & 148 & 131 & 45 & 81 & 2 & 164 & 145 & 117 & 157 & 4 & 108 & 61 \\ 134 & 23 & 151 & 120 & 151 & 44 & 30 & 1 & 76 & 32 & 60 & 132 & 165 \\ 121 & 40 & 83 & 4 & 56 & 88 & 3 & 134 & 109 & 85 & 88 & 18 & 3 \\ 23 & 20 & 20 & 31 & 66 & 24 & 41 & 126 & 47 & 137 & 33 & 112 & 49 \\ 143 & 18 & 44 & 26 & 89 & 109 & 118 & 148 & 35 & 16 & 35 & 122 & 150 \\ 144 & 51 & 47 & 143 & 109 & 164 & 52 & 38 & 92 & 50 & 98 & 60 & 104 \\ 70 & 165 & 89 & 80 & 28 & 75 & 19 & 110 & 101 & 41 & 155 & 78 & 67 \\ 123 & 147 & 54 & 4 & 60 & 133 & 49 & 151 & 30 & 32 & 157 & 108 & 82 \\ 95 & 139 & 50 & 70 & 124 & 168 & 87 & 63 & 13 & 104 & 58 & 107 & 113 \end{pmatrix}
\]
modulo 169, and the order $K$ is 28392, which yields
\[
p \left( \frac{13^2 \cdot 5^{56783} n + 1}{24} \right) \equiv 0 \mod 13^2
\]
for all $n$ not divisible by 5.
REFERENCES

[1] Scott Ahlgren. Distribution of the partition function modulo composite integers. *Math. Ann.*, 318(4):795–803, 2000.
[2] Scott Ahlgren and Matthew Boylan. Arithmetic properties of the partition function. *Invent. Math.*, 153(3):487–502, 2003.
[3] A. O. L. Atkin. Proof of a conjecture of Ramanujan. *Glasgow Math. J.*, 8:14–32, 1967.
[4] A. O. L. Atkin. Multiplicative congruence properties and density problems for $p(n)$. *Proc. London Math. Soc. (3)*, 18:563–576, 1968.
[5] A. O. L. Atkin and J. Lehner. Hecke operators on $\Gamma_0(m)$. *Math. Ann.*, 185:134–160, 1970.
[6] A. O. L. Atkin and J. N. O’Brien. Some properties of $p(n)$ and $c(n)$ modulo powers of 13. *Trans. Amer. Math. Soc.*, 126:442–459, 1967.
[7] Heng Huat Chan. *Serre’s proof of Ramanujan’s claim (15.6) in “Ramanujan’s unpublished manuscript on the partition and tau functions with proofs and commentary” by Bruce C. Berndt and Ken Ono*. written for Ramanujan’s Lost Notebook by George E. Andrews and Bruce C. Berndt.
[8] Kok Seng Chua. Explicit congruences for the partition function modulo every prime. *Arch. Math. (Basel)*, 81(1):11–21, 2003.
[9] Li Guo and Ken Ono. The partition function and the arithmetic of certain modular $L$-functions. *Internat. Math. Res. Notices*, (21):1179–1197, 1999.
[10] Jeremy Lovejoy and Ken Ono. Extension of Ramanujan’s congruences for the partition function modulo powers of 5. *J. Reine Angew. Math.*, 542:123–132, 2002.
[11] Morris Newman. Construction and application of a class of modular functions. II. *Proc. London Math. Soc. (3)*, 9:373–387, 1959.
[12] Ken Ono. Distribution of the partition function modulo $m$. *Ann. of Math. (2)*, 151(1):293–307, 2000.
[13] Srinivasa Ramanujan. *Collected papers of Srinivasa Ramanujan*. AMS Chelsea Publishing, Providence, RI, 2000. Edited by G. H. Hardy, P. V. Seshu Aiyar and B. M. Wilson, Third printing of the 1927 original, With a new preface and commentary by Bruce C. Berndt.
[14] Jean-Pierre Serre. Divisibilité de certaines fonctions arithmétiques. *Enseignement Math. (2)*, 22(3-4):227–260, 1976.
[15] Goro Shimura. On modular forms of half integral weight. *Ann. of Math. (2)*, 97:440–481, 1973.
[16] Jacob Sturm. On the congruence of modular forms. In *Number theory (New York, 1984–1985)*, volume 1240 of *Lecture Notes in Math.*, pages 275–280. Springer, Berlin, 1987.
[17] G. N. Watson. Ramanujans Vermutung über Zerfallzahlen. *J. Reine Angew. Math.*, 179:97–128, 1938.
[18] Rhiannon L. Weaver. New congruences for the partition function. *Ramanujan J.*, 5(1):53–63, 2001.
[19] Heinrich Weber. *Lehrbuch der Algebra, Vol. III*. Chelsea, New York, 1961.

DEPARTMENT OF APPLIED MATHEMATICS, NATIONAL CHIAO TUNG UNIVERSITY, 1001 TA HSUEH ROAD, HSINCHU, TAIWAN 300

E-mail address: yfyang@math.nctu.edu.tw