Congruences of the Partition Function

Yifan Yang
Department of Applied Mathematics, National Chiao Tung University
and National Center for Theoretical Sciences, Hsinchu, Taiwan 300

Correspondence to be sent to: yfyang@math.nctu.edu.tw

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

\[
p(m \ell^k n + B) \equiv 0 \pmod{m} \quad \text{for all } n \geq 0
\]

exist for all primes \( m \) and \( \ell \) satisfying \( m \geq 13 \) and \( \ell \neq 2, 3, m \), where \( B \) is a suitably chosen integer depending on \( m \) and \( \ell \). 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 with a properly chosen \( B \) the congruence

\[
p(m^i \ell^k n + B) \equiv 0 \pmod{m^i}
\]

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 unordered sums of positive integers. For convenience, we also set \( p(0) = 1 \), \( p(n) = 0 \) for \( n < 0 \), and \( p(\alpha) = 0 \) if \( \alpha \not\in \mathbb{Z} \). A remarkable discovery of Ramanujan [14] is that the partition function \( p(n) \)
satisfies the congruences
\[ p(An + B) \equiv 0 \mod m, \] (1)
for all nonnegative 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 [18] for the cases of powers of 5 and 7 and Atkin [4] for the cases of powers of 11. (Apparently, Ramanujan actually found a proof of the congruences modulo powers of 5 himself. The proof was contained in an unpublished manuscript, which was hidden from the public until 1988. It appeared that Ramanujan intended to prove congruences modulo powers of 7 along the same line of attack, but his ailing health prevented him from working out the details. See the commentary at the end of [8] for more details.) 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 [5, 7]. In those examples, the integer \( A \) is no longer a prime power.

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 nonprime power, a surprising result of Ono [13] shows that for each prime \( m \geq 5 \) and each positive integer \( k, \) a positive proportion of prime \( \ell \) has the property
\[ p \left( \frac{m^k \ell^3 n + 1}{24} \right) \equiv 0 \mod m \] (2)
for all nonnegative integers \( n \) relatively prime to \( \ell. \) This result was later extended to composite \( m, (m, 6) = 1, \) by Ahlgren [1]. The results of [1, 13] were further extended by Ahlgren and Ono [3].

Neither of [1, 13] 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 [19]. In effect, she found 76,065 new congruences. (However, we should remark that some congruences listed in [19, Theorem 2] were already discovered by Atkin [5]. Had Atkin had the computing power of the present day, he would have undoubtedly discovered many more congruences.) For primes \( m \geq 37, \) this was addressed by Chua [9], although no explicit examples were given therein.
Another remarkable discovery of Ono [13, Theorem 5] is that the partition function possesses a 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

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

for all nonnegative integers $n$ and all $i \geq N(m)$. Note that the bound $m^{48(m^3-2m+1)}$ can be improved greatly using a result of Garvan [10]. See Corollary 3.3 in Section 3 for details.

In this paper, 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

$$p(m\ell^k n + B) \equiv 0 \mod m$$

for all primes $m$ and $\ell$ such that $m \geq 13$ and $\ell$ not equal to 2, 3, and $m$, where $B$ is a suitably chosen integer depending on $m$ and $\ell$.

**Theorem 1.1.** 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

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

for all nonnegative integers $n$ relatively prime to $m$. □

For instance, in Section 5, we will find that for $m = 37$, congruences (4) hold with

<table>
<thead>
<tr>
<th>$\ell$</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
<th>29</th>
<th>31</th>
<th>41</th>
<th>43</th>
<th>47</th>
<th>53</th>
<th>59</th>
<th>61</th>
</tr>
</thead>
<tbody>
<tr>
<td>$k$</td>
<td>228</td>
<td>57</td>
<td>18</td>
<td>684</td>
<td>38</td>
<td>38</td>
<td>684</td>
<td>684</td>
<td>228</td>
<td>171</td>
<td>18</td>
<td>333</td>
<td>18</td>
<td>12</td>
<td>684</td>
</tr>
</tbody>
</table>

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 1.1 is in fact a simplified version of one of the main results. (See Theorem 3.6.) In the full version, we will see that the integer $k$ in Theorem 1.1 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 \( \chi_{12} = (\frac{12}{-}) \). This invariant subspace of \( S_{m/2-1}(\Gamma_0(576), \chi_{12}) \) was first discovered by Garvan [10] and rediscovered by the author of the present paper. 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 [13] and other subsequent papers [9, 19]. 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 6, we will see that for each prime power \( m^i \) and a prime \( \ell \neq 2, 3, m \), there always exists a positive integer \( k \) such that

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

for all positive integers \( n \) not divisible by \( \ell \). One example worked out in Section 6 is

\[
p\left( \frac{13^2 \cdot 56783n + 1}{24} \right) \equiv 0 \mod 13^2.
\]

In the same section, we will also discuss congruences of type \( p(5^j \ell^k n + B) \equiv 0 \mod 5^{j+1} \).

### 1.1 Notation

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 matrix \( \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}(2, \mathbb{Q}) \) and a modular form \( f(\tau) \) of an even weight \( k \), the slash operator is defined by

\[
f(\tau)|_{k \gamma} := (\det \gamma)^{k/2}(c\tau + d)^{-k} f\left( \frac{a\tau + b}{c\tau + d} \right).
\]

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

\[
U_N : f(q) \mapsto f(q)|_{U_N} := \sum_{n=0}^{\infty} a_f(Nn)q^n,
\]

\[
V_N : f(q) \mapsto f(q)|_{V_N} := \sum_{n=0}^{\infty} a_f(n)q^{Nn}.
\]
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

$$F_{m,j} = \sum_{n \geq 0, m/n \equiv -1 \mod 24} p\left(\frac{m^j n + 1}{24}\right)q^n.$$ 

Note that we have

$$F_{m,j}|U_m = F_{m,j+1}. \quad (5)$$

2 Works of Ono [13], Weaver [19], and Chua [9]

In this section, we will review the ideas in [9, 13, 19].

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 [13] considered the function $\eta(m^k\tau)^m / \eta(\tau)$. On the one hand, one has

$$\frac{\eta(m^k\tau)^m}{\eta(\tau)} \bigg| U_m = \prod_{n=1}^{\infty} (1 - q^n)^{m^k} \cdot \left(\sum_{n=0}^{\infty} p(n)q^{n+(m^{2k} - 1)/24}\right) \bigg| U_m.$$ 

On the other hand, one has

$$\frac{\eta(m^k\tau)^m}{\eta(\tau)} \equiv \eta(\tau)^{m^2 - 1} = \Delta(\tau)^{(m^{2k} - 1)/24} \mod m.$$
where \( \Delta(\tau) = \eta(\tau)^{24} \) is the normalized cusp form of weight 12 on \( \text{SL}(2, \mathbb{Z}) \). From these, Ono [13, 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 \( \chi_{12} = (\frac{12}{m}) \). Then by (5) and the fact that \( U_m \) defines a linear map

\[
U_m : S_{k+1/2}(\Gamma_0(4Nm), \psi) \to S_{k+1/2}(\Gamma_0(4Nm), \psi\chi_m),
\]

where \( \chi_m \) is the Kronecker character attached to \( \mathbb{Q}(\sqrt{m}) \), one sees that

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

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

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

\[
T_{\ell^2} : f(\tau) \mapsto \sum_{n=1}^{\infty} \left( a_f(\ell^2n) + \psi(\ell) \left( \frac{n}{\ell^2} \right) \ell^\lambda a_f(n) + \psi(\ell^2)\ell^{2\lambda} a_f \left( \frac{n}{\ell^2} \right) \right) q^n
\]

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

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

\[
= \sum_{n=1}^{\infty} \left( a_{m,k}(\ell^2n) + \psi(\ell^2)\ell^{m^2-m-3} a_{m,k} \left( \frac{n}{\ell} \right) \right) q^n
\]
Congruences of the Partition Function

since \( \left( \frac{\ell n}{\tau} \right) = 0 \). 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 [16] and a result of Serre [15, 6.4].

As mentioned earlier, Ono [13] did not address the issue of finding explicit congruences of the form (2). However, [13, Section 4] 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 [17] Ono verified that

\[ F_{13,2k+1} \equiv G_{13,2k+1} \equiv 11 \cdot 6^k \eta(24\tau)^{11} \mod 13, \]

\[ F_{13,2k+2} \equiv G_{13,2k+2} \equiv 10 \cdot 6^k \eta(24\tau)^{23} \mod 13 \]

for all nonnegative 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. It has been known since Morris Newman’s work in the 1950s that for odd \( r \) with \( 0 < r < 24 \), the function \( \eta(24\tau)^r \) is a Hecke eigenform.) More generally, for \( m \in \{13, 17, 19, 23, 29, 31\} \), it is shown in [13, Section 4], [11, Proposition 6] and [19, Proposition 5] that \( G_{m,1} \) is congruent to a Hecke eigenform of weight \( m/2 - 1 \). Using this observation, Weaver [19] then devised an algorithm to find explicit congruences of the form (2) for \( m \in \{13, 17, 19, 23, 29, 31\} \).

The proof of congruences (6) given in [11, 19] is essentially “verification” in the sense that they all used Sturm’s criterion [17]. That is, by Sturm’s theorem to show that two modular forms on a congruence subgroup \( \Gamma \) are congruent to each other modulo a prime \( m \), it suffices to compare sufficiently many coefficients, depending on the weight.
and index \((\text{SL}(2, \mathbb{Z}) : \Gamma)\). Naturally, this kind of argument will not be very useful in proving general results.

In [9], instead of the congruence
\[
\eta(m\tau)^m \equiv \eta(\tau)^{m^2 - 1} \mod m
\]
used by Ono, Chua considered the congruence
\[
\eta(m\tau)^m \equiv \eta(m\tau)^{m-1}\eta(\tau)^{m-1} \mod m
\]
as the starting point. The function on the right is a modular form of weight \(m - 1\) on \(\Gamma_0(m)\). Thus, by the level reduction lemma of Atkin and Lehner [6, Lemma 7], one has
\[
\eta(m\tau)^{m-1}\eta(\tau)^{m-1}|(U_m + m^{(m-1)/2 - 1} W_m) \in S_{m-1}(\text{SL}(2, \mathbb{Z})),
\]
where for a modular form \(f(\tau)\) of an even integral weight \(k\) on \(\Gamma_0(m)\), the Atkin–Lehner operator \(W_m\) is defined by
\[
W_m : f(\tau) \rightarrow f(\tau)|_k \begin{pmatrix} 0 & -1 \\ m & 0 \end{pmatrix} = (\sqrt{m}\tau)^{-k} f \left( -\frac{1}{m\tau} \right).
\]

It follows that
\[
F_{m,1} = \frac{1}{\eta(24\tau)} \left| U_m \equiv \frac{f_m(24\tau)}{\eta(24\tau)^m} \mod m \right.
\]
for some cusp form \(f_m(\tau) \in S_{m-1}(\text{SL}(2, \mathbb{Z}))\). (Incidently, this also proves Ramanujan’s congruences for \(m = 5, 7,\) and \(11,\) since there are no nontrivial cusp forms of weight \(4, 6,\) and \(10\) on \(\text{SL}(2, \mathbb{Z})\).) By examining the order of vanishing of \(f_m(\tau)\) at \(\infty\), Chua [9, 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
\[
F_{m,1} \equiv \eta(24\tau)^r \phi_{m,1}(24\tau) \mod m
\]
for some modular form \(\phi_{m,1}\) on \(\text{SL}(2, \mathbb{Z})\) of weight \((m - r_m - 2)/2\). More generally, one has the following proposition.
Proposition 2.1. 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

$$F_m, j \equiv \eta(24\tau)^{r_m, j} \phi_{m, j}(24\tau) \mod m$$

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.

□

Proof. Consider the function $f_{m, j}(\tau) = \eta(m^j \tau)^{m^j}/\eta(\tau)$. It is a modular form of weight $(m^j - 1)/2$ on $\Gamma_0(m^j)$ with character $(\cdot / m^j)$. Consider also the auxiliary function

$$h_{m, j}(\tau) = \begin{cases} 
  \frac{\eta(\tau)^m}{\eta(m\tau)} & \text{if } j \text{ is odd,} \\
  \left(\frac{\eta(\tau)^m}{\eta(m\tau)}\right)^2 & \text{if } j \text{ is even.}
\end{cases}$$

It is a modular form on $\Gamma_0(m)$ with character $(\cdot / m)^j$ and satisfies

$$h_{m, j}(\tau) \equiv 1 \mod m. \quad (8)$$

By the level reduction lemma of Atkin and Lehner [6, Lemma 7], if we apply $U_m$ to $f_{m, j}$ $j - 1$ times and then multiply the resulting function by $h_{m, j}$, we get a modular form on $\Gamma_0(m)$ with trivial character. That is,

$$f_{m, j}(\tau)|U_m^{j-1} \cdot h_{m, j}(\tau)$$

is a modular form on $\Gamma_0(m)$ with trivial character. The weight is

$$\lambda_{m, j} = \begin{cases} 
  \frac{(m^j - 1)}{2} + \frac{(m - 1)}{2} & \text{if } j \text{ is odd,} \\
  \frac{(m^j - 1)}{2} + m - 1 & \text{if } j \text{ is even.}
\end{cases}$$
Then by the level reduction lemma again

\[(f_{m,j}(\tau)|U_m^{j-1} \cdot h_{m,j}(\tau))(U_m + m^{\lambda_{m,j}/2} W_m)\]

is a modular form on \(SL(2, \mathbb{Z})\), where \(W_m\) is the Atkin–Lehner operator defined in (7). Considering the order of vanishing at \(\infty\), we see that this modular form on \(SL(2, \mathbb{Z})\) is

\[\Delta(\tau)^{\mu_{m,j}} \phi_{m,j}(\tau),\]

where \(\Delta(\tau) = \eta(\tau)^{24},\)

\[\mu_{m,j} = \frac{m^{2j} + 24m_{\lambda_{m,j}} - 1}{24m_j}\]

with \(v_{m,j}\) being the unique integer satisfying \(0 < v_{m,j} < m^j\) and \(24v_{m,j} \equiv 1 \mod m^j\), and \(\phi_{m,j}\) is a modular form of weight \(\lambda_{m,j} - 12\mu_{m,j}\) on \(SL(2, \mathbb{Z})\).

Now observe that \(h_{m,j} | m^{\lambda_{m,j}/2} W_m\) is congruent to 0 modulo a high power of \(m\). Then, by (8), we have

\[\Delta(24\tau)^{\mu_{m,j}} \phi_{m,j}(24\tau) \equiv f_{m,j}(\tau)|U_m| V_{24} = \eta(24\tau)^{m_j} F_{m,j} \mod m.\]

In other words, we have

\[F_{m,j} \equiv \eta(24\tau)^{2\mu_{m,j} - m_j} \phi_{m,j}(24\tau) = \eta(24\tau)^{(24v_{m,j} - 1)/m_j} \phi_{m,j}(24\tau) \mod m.\]

The integer \((24v_{m,j} - 1)/m_j\) is in the range between 0 and 24. Also, it is congruent to \(-1/m_j\) modulo 24. Thus, we have

\[\frac{24v_{m,j} - 1}{m_j} = r_{m,j} = \begin{cases} r_m & \text{if } j \text{ is odd}, \\ 23 & \text{if } j \text{ is even}. \end{cases}\]

From this, we get

\[\lambda_{m,j} - 12\mu_{m,j} = \begin{cases} \frac{(m - r_m - 2)}{2} & \text{if } j \text{ is odd}, \\ m - 13 & \text{if } j \text{ is even}. \end{cases}\]

This proves the proposition. \(\blacksquare\)
Remark 2.2. Proposition 2.1 was stated as [9, Conjecture 1]. The proof sketched here was suggested by one of the referees and was adapted from the proof of [2, Theorem 3]. Alternatively, one can combine Proposition 3.1 with an induction step proved in [9] to get the same conclusion. See the arxiv version arXiv:0904.2530 of the present paper for more details. □

3 Main results

In this section, we will state our main results. Before doing so, let us first recall a property about the subspace

\[ \{ \eta(24\tau)^r f(24\tau) : f \in M_{s}(\text{SL}(2, \mathbb{Z})) \} \]

of \( S_{s+r/2}(\Gamma_0(576), \chi_{12}) \), in which the function \( \eta(24\tau)^{r_{m,j}}\phi_{m,j}(24\tau) \) in Proposition 2.1 lies.

Proposition 3.1 ([10, Proposition 3.1]). Let \( r \) be an odd integer with \( 0 < r < 24 \). Let \( s \) be a nonnegative even integer. Then the space

\[ S_{r,s} := \{ \eta(24\tau)^r f(24\tau) : f(\tau) \in M_{s}(\text{SL}(2, \mathbb{Z})) \} \quad (9) \]

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 \( \ell \neq 2, 3 \) and all \( f \in S_{r,s} \), we have \( f|T_{\ell^2} \in S_{r,s} \). □

Remark 3.2. This property of \( S_{r,s} \) was first discovered by Garvan [10], and later rediscovered by the author of the present paper. (See the arxiv version arXiv:0904.2530 of the present paper.) Garvan stated the proposition under the assumption that \( (r, 6) = 1 \) instead of \( 2 \mid r \), but it can be easily checked that his proof also works for the cases \( r = 3, 9, 15, \) and \( 21 \) as well. The author’s proof is more complicated, but can be applied in other similar situations. However, at the hindsight, the invariance of \( S_{r,s} \) under the action of Hecke algebra is best explained (and proved) as follows.

The usual definition of modular forms of half-integral weights, as per Shimura [16], is given in terms of the theta function \( \theta(\tau) = \sum_{n \in \mathbb{Z}} q^{n^2} \). Specifically, we say a holomorphic function \( f : \mathbb{H} \to \mathbb{C} \) is a modular form of half-integral weight \( \lambda + \frac{1}{2} \) on \( \Gamma_0(4N) \) with character \( \chi \), where \( \chi \) is a Dirichlet character modulo \( 4N \), if \( f(\tau) \) is holomorphic at each cusp and satisfies

\[ \frac{f(\gamma \tau)}{f(\tau)} = \chi(d) \frac{\theta(\gamma \tau)^{2\lambda+1}}{\theta(\tau)^{2\lambda+1}} \]
for all \( \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4N) \). It is in this sense we say \( \eta(24\tau) \) is a modular form of weight \( 1/2 \) on \( \Gamma_0(576) \) with character \( \chi_{12} \).

Now the choice of \( \theta \) in the definition of half-integral modular forms is perhaps the most natural and simplest from the view point of Weil representations, but one drawback of this choice is that the levels of the modular forms have to be a multiple of 4. On the other hand, if we define modular forms of half-integral weights in terms of \( \eta(\tau) \), then the levels can be taken all the way down to 1. Explicitly, let \( \Gamma \) be a congruence subgroup of \( \text{SL}(2, \mathbb{Z}) \) for an odd integer \( r \) with \( 0 < r < 24 \) and a nonnegative even integer \( s \), we say a function \( f : \mathbb{H} \to \mathbb{C} \) is a modular form of \( (\eta^r, s) \)-type on \( \Gamma \) if it is holomorphic in \( \mathbb{H} \) and at each cusp such that

\[
\frac{f(\gamma \tau)}{f(\tau)} = (c\tau + d)^s \frac{\eta(\gamma \tau)^r}{\eta(\tau)^r}
\]

for all \( \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \). Let \( S_{r,s}(\Gamma) \) be the space of all such modular forms on \( \Gamma \).

Consider the case \( \Gamma = \text{SL}(2, \mathbb{Z}) \). On the space \( S_{r,s}(\text{SL}(2, \mathbb{Z})) \), we can also define Hecke operators \( T_{\ell^2} \) for primes \( \ell \neq 2, 3 \) and show that their actions on \( f(\tau) = \sum a_f(n)q^{n/24} \in S_{r,s}(\text{SL}(2, \mathbb{Z})) \) is

\[
T_{\ell^2} : f(\tau) \mapsto \sum_{n=1}^{\infty} \left( a_f(\ell^2n) + \frac{12}{\ell} \right) \left( \frac{(-1)^{\lambda}n}{\ell} \right) \ell^{\lambda-1} a_f(n) + \ell^{2\lambda-1} a_f \left( \frac{n}{\ell^2} \right) q^{n/24}
\]

with \( \lambda = (r + 2s - 1)/2 \). Now observe that if \( g(\tau) \in S_{r,s}(\text{SL}(2, \mathbb{Z})) \), then \( g(\tau + 1) = e^{2\pi i r/24} g(\tau) \), which implies that \( g(\tau) = q^{r/24}(c_0 + c_1 q + \cdots) \), \( c_i \in \mathbb{C} \). Therefore, \( f(\tau) = \frac{g(\tau)}{\eta(\tau)^r} \) is a function holomorphic on \( \mathbb{H} \) and at each cusp and satisfies \( f(\gamma \tau) = (c\tau + d)^s f(\tau) \) for all \( \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z}) \). In other words,

\[
S_{r,s}(\text{SL}(2, \mathbb{Z})) = \{ \eta(\tau)^r f(\tau) : f \in M_s(\text{SL}(2, \mathbb{Z})) \}
\]

and

\[
S_{r,s} = \{ g(24\tau) : g \in S_{r,s}(\text{SL}(2, \mathbb{Z})) \}.
\]

This explains why \( S_{r,s} \) is an invariant subspace of \( S_{7/2+s}(\Gamma_0(576), \chi_{12}) \).

Using the pigeonhole principle, one can see that Propositions 2.1 and 3.1 yield Ono’s periodicity result (3), with an improved bound.
Corollary 3.3. Let \( m \geq 5 \) be a prime. Then there exist integers \( N(m) \) and \( P(m) \) with 
\[ 0 \leq (N(m) - 1)/2 \leq m^{A(m)} \] and \( 0 \leq P(m) \leq m^{A(m)} \) such that 
\[ p \left( \frac{m^i n + 1}{24} \right) \equiv p \left( \frac{m^{2P(m)+i} n + 1}{24} \right) \mod m \] 
for all nonnegative integers \( n \) and all \( i \geq N(m) \), where 
\[ A(m) = \dim M_{(m-r_m-2)/2}(\text{SL}(2, \mathbb{Z})) = \left\lfloor \frac{m}{12} \right\rfloor - \left\lfloor \frac{m}{24} \right\rfloor \] (10) 
and \( r_m \) is the integer satisfying \( 0 < r_m < 24 \) and \( m \equiv -r_m \mod 24 \). \( \square \)

From Proposition 3.1, we can deduce the following corollary, which will be proved in the next section.

Corollary 3.4. Let \( r \) be an odd integer satisfying \( 0 < r < 24 \) and \( s \) be a nonnegative even integer. Let \( S_{r,s} \) be defined as (9) 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 
\[ \begin{pmatrix} f_1 \\ \vdots \\ f_t \end{pmatrix} \begin{pmatrix} f_1 \\ \vdots \\ f_t \end{pmatrix}^T = A \begin{pmatrix} f_1 \\ \vdots \\ f_t \end{pmatrix} \]
Then we have 
\[ \begin{pmatrix} f_1 \\ \vdots \\ f_t \end{pmatrix} V^{k}_{\ell^2} = A_k \begin{pmatrix} f_1 \\ \vdots \\ f_t \end{pmatrix} + B_k \begin{pmatrix} g_1 \\ \vdots \\ g_t \end{pmatrix} + C_k \begin{pmatrix} f_1 \\ \vdots \\ f_t \end{pmatrix} \]
where \( g_j = f_j \otimes (\bar{\ell}) \), and for nonnegative integers \( k \), \( A_k \), \( B_k \), and \( C_k \) are \( t \times t \) matrices satisfying 
\[ \begin{pmatrix} A_k \\ A_{k-1} \end{pmatrix} = \begin{pmatrix} A & -\ell^r + 2s - 2 I_t \\ I_t & 0 \end{pmatrix}^{k} \begin{pmatrix} I_t \\ 0 \end{pmatrix} \] 
with \( I_t \) being the \( t \times t \) identity matrix, and 
\[ B_k = -\ell^{s+(r-3)/2} \left( \frac{(-1)^{(r-1)/2} 12}{\ell} \right) A_{k-1}, \quad C_k = -\ell^r + 2s - 2 A_{k-1}. \] \( \square \)
Remark 3.5. It is well known that for nonnegative even integer $s$, the space $M_s(\text{SL}(2, \mathbb{Z}))$ has a basis consisting of $g_1, \ldots, g_d$ satisfying $g_i \in \mathbb{Z}[q]$ and $g_i = q^{i-1} + \cdots$, where $d = \dim M_s(\text{SL}(2, \mathbb{Z}))$. (Usually, $g_i$ are chosen to be products of $\Delta(\tau)$ and Eisenstein series.) Then it can be easily verified that the functions $f_i(\tau) = \eta(24\tau)^r g_i(24\tau)$ form a $\mathbb{Z}$-basis of the $\mathbb{Z}$-module $\mathbb{Z}[q] \cap S_{r,s}$. In particular, the rank of the $\mathbb{Z}$-module $\mathbb{Z}[q] \cap S_{r,s}$ is the same as the dimension of $S_{r,s}$.

Note also that if $r + 2s \geq 3$, then the Hecke operator $T_{\ell^2}$ maps $\mathbb{Z}[q] \cap S_{r,s}$ into $\mathbb{Z}[q] \cap S_{r,s}$. Therefore, the matrix $A$ in the above corollary has entries in $\mathbb{Z}$. This property is crucial in our subsequent discussion when we need to take $A$ modulo a prime. \hfill \Box

Now we can state our main results. The first one is a more precise version of Theorem 1.1. The proof utilizes the corollary above and will be given in the next section.

Theorem 3.6. Let $m \geq 13$ be a prime. Set $r_m$ to be the integer satisfying $0 < r_m < 24$ and $m \equiv -r_m \mod 24$. 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

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

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

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

(12)

for all positive integers $u$ and all positive integers $n$ not divisible by $\ell$. 
Also, if the order of the matrix (11) in $GL(2t, \mathbb{F}_m)$ is $M$, then we have

$$p\left(\frac{m^i n + 1}{24}\right) \equiv p\left(\frac{m^{2M-i} n + 1}{24}\right) \mod m \tag{13}$$

for all nonnegative integer $i$ and all positive integers $n$. \hfill \Box

**Remark 3.7.** Note that if the matrix $A$ in the above theorem vanishes modulo $m$, then the matrix in (11) has order 2 in $PGL(2t, \mathbb{F}_m)$, and the conclusion of the theorem asserts that

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

This is the congruence appearing in Ono’s theorem. \hfill \Box

**Remark 3.8.** In general, the integer $K$ in Theorem 3.6 may not be the smallest positive integer such that congruence (4) holds. We choose to state the theorem in the current form because of its simplicity. See the remark following the proof of Theorem 3.6. \hfill \Box

4 Proof of Corollary 3.4 and Theorem 3.6

**Proof of Corollary 3.4.** By the definition of $T_{\ell^2}$, we have

$$
\begin{pmatrix}
  f_1 \\
  \vdots \\
  f_t
\end{pmatrix}
\quad U_{\ell^2} = A_1
\begin{pmatrix}
  f_1 \\
  \vdots \\
  f_t
\end{pmatrix}
+ B_1
\begin{pmatrix}
  g_1 \\
  \vdots \\
  g_t
\end{pmatrix}
+ C_1
\begin{pmatrix}
  f_1 \\
  \vdots \\
  f_t
\end{pmatrix}
\quad V_{\ell^2},
$$

where $g_j = f_j \otimes (\bar{\ell})$ and

$$A_1 = A, \quad B_1 = -\ell^{s+(r-3)/2} \left(\frac{(-1)^{(r-1)/2}2}{\ell}\right) I_t, \quad C_1 = -\ell^{r+2s-2} I_t.$$

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

\[
\begin{pmatrix}
  f_1 \\
  \vdots \\
  f_t
\end{pmatrix}
\begin{pmatrix}
  f_1 \\
  \vdots \\
  f_t
\end{pmatrix} = (A_1^2 + C_1)
\begin{pmatrix}
  f_1 \\
  \vdots \\
  f_t
\end{pmatrix} + A_1 B_1
\begin{pmatrix}
  g_1 \\
  \vdots \\
  g_t
\end{pmatrix} + A_1 C_1
\begin{pmatrix}
  f_1 \\
  \vdots \\
  f_t
\end{pmatrix} \quad V_{1^2}.
\]

Iterating, we see that in general if

\[
\begin{pmatrix}
  f_1 \\
  \vdots \\
  f_t
\end{pmatrix} = A_k
\begin{pmatrix}
  f_1 \\
  \vdots \\
  f_t
\end{pmatrix} + B_k
\begin{pmatrix}
  g_1 \\
  \vdots \\
  g_t
\end{pmatrix} + C_k
\begin{pmatrix}
  f_1 \\
  \vdots \\
  f_t
\end{pmatrix} \quad V_{1^2},
\]

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 corollary.

\[\blacksquare\]

**Proof of Theorem 3.6.** 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 Proposition 2.1, \(F_{m,1}\) is congruent to a modular form in \(S_{r,s}\), where \(S_{r,s}\) is defined by (9). Now let \(\{f_1, \ldots, f_t\}\) be a \(\mathbb{Z}\)-basis for \(\mathbb{Z}[q] \cap S_{r,s}\) and \(A\) be given as in the statement of the theorem. (Note that \(A\) has entries in
Z. See Remark 3.5.) Then by Corollary 3.4, we know that

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

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

$$\begin{pmatrix} A_k \\ A_{k-1} \end{pmatrix} = X^k \begin{pmatrix} I_t \\ 0 \end{pmatrix},$$

$$B_k = -\ell^{(m-5)/2} \left( \frac{(r-1/2)12}{\ell} \right) A_{k-1},$$

$$C_k = -\ell^{m-4} A_{k-1}$$

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 $X \bmod m$ in $\text{PGL}(2t, \mathbb{F}_m)$ is $K$, then we have, for all positive integers $u$,

$$\begin{pmatrix} A_{uK-1} \\ A_{uK-2} \end{pmatrix} = X^{uK-1} \begin{pmatrix} I_t \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ U \end{pmatrix} \bmod m$$

for some $t \times t$ matrix $U$, that is, $A_{uK-1} \equiv 0 \bmod m$. The rest of proof follows Ono’s argument.

We have

$$\begin{pmatrix} f_1 \\ \vdots \\ f_t \end{pmatrix} U_{\ell^2}^{uK-1} \equiv B_{uK-1} \begin{pmatrix} g_1 \\ \vdots \\ g_t \end{pmatrix} + C_{uK-1} \begin{pmatrix} f_1 \\ \vdots \\ f_t \end{pmatrix} V_{\ell^2} \bmod m$$
and
\[
\begin{pmatrix}
  f_1 \\
  \vdots \\
  f_t
\end{pmatrix}
U_{\ell^2}^{uK-1} U_\ell \equiv C_{uK-1} \begin{pmatrix}
  f_1 \\
  \vdots \\
  f_t
\end{pmatrix}
V_\ell \mod m.
\]

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 $(\ell^{2uK-1}n)$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 (12).

Finally, if the matrix $X$ has order $M$ in $GL(2t, F_m)$, then from the recursive relations (14) and (15), it is obvious that (13) holds. This completes the proof. ■

**Remark 4.1.** In general, the integer $K$ in Theorem 3.6 may not be the smallest positive integer such that congruence (4) holds. For example, consider the case where $S_{r,s}$ has dimension $t \geq 2$ and the reduction of $\mathcal{Z}[q] \cap S_{r,s}$ modulo $m$ has a basis consisting of Hecke eigenforms $f_1, \ldots, f_t$ defined over $F_m$. Suppose that the eigenvalues of $T_\ell^2$ for $f_i$ modulo $m$ are $a_{\ell}^{(1)}, \ldots, a_{\ell}^{(t)} \in F_m$. Let $k_i$ denote the order of \( \left(\frac{a_{\ell}^{(i)} - \ell^m - 4}{1 \cdot 0}\right) \) in $PGL(2, F_m)$. Let $k$ be the least common multiple of $k_i$. Then we can show that
\[
f_i | U_{\ell^2}^{2k-1} \equiv c_i f_i | V_\ell \mod m
\]
for some $c_i \in F_m$ and consequently congruence (4) holds. Of course, the least common multiple of $k_i$ may be smaller than the integer $K$ in Theorem 3.6 in general. □

5 Examples

**Example 5.1.** Let $m = 13$. According to Proposition 2.1, we have
\[
F_{13,1} \equiv c\eta(24\tau)^{11} \mod 13
\]
for some $c \in F_{13}$. (In fact, $c = 11$. See [13, page 303].) The eigenvalues $a_\ell$ modulo $13$ of $T_\ell^2$ for the first few primes $\ell$ are...
For $\ell = 5$, the matrix
\[
X = \begin{pmatrix} a_\ell & -\ell^9 \\ 1 & 0 \end{pmatrix} \equiv \begin{pmatrix} 10 & 8 \\ 1 & 0 \end{pmatrix} \mod 13
\]
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
\[
p\left(\frac{13 \cdot 5^{28u-1} n + 1}{24}\right) \equiv 0 \mod 13
\]
for all positive integers $u$ and all positive integers $n$ not divisible by 5. Likewise, we find that congruence (4) holds with $\square$.

<table>
<thead>
<tr>
<th>$\ell$</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>17</th>
<th>19</th>
<th>23</th>
<th>29</th>
<th>31</th>
<th>37</th>
<th>41</th>
<th>43</th>
<th>47</th>
<th>53</th>
<th>59</th>
<th>61</th>
<th>67</th>
<th>73</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a_\ell$</td>
<td>10</td>
<td>8</td>
<td>5</td>
<td>1</td>
<td>8</td>
<td>8</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>9</td>
<td>12</td>
<td>6</td>
<td>10</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>$\ell^9$</td>
<td>5</td>
<td>8</td>
<td>8</td>
<td>12</td>
<td>5</td>
<td>12</td>
<td>1</td>
<td>5</td>
<td>8</td>
<td>5</td>
<td>12</td>
<td>8</td>
<td>1</td>
<td>8</td>
<td>1</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

Example 5.2. Let $m = 37$. By Proposition 2.1, we know that $F_{37,1}$ is congruent to a cusp form in $S_{11,12}$ modulo 37. In fact, according to [9, 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 $S_{11,12} \cap \mathbb{Z}[[q]]$ 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 $a_\ell^{(i)}$ denote the eigenvalue of $T_{\ell^2}$ associated to $f_i$. We have the following data.

<table>
<thead>
<tr>
<th>$\ell$</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
<th>29</th>
<th>31</th>
<th>37</th>
<th>41</th>
<th>43</th>
<th>47</th>
<th>53</th>
<th>59</th>
<th>61</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a_\ell^{(1)}$</td>
<td>1</td>
<td>33</td>
<td>22</td>
<td>7</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>9</td>
<td>35</td>
<td>11</td>
<td>28</td>
<td>14</td>
<td>30</td>
<td>24</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>$a_\ell^{(2)}$</td>
<td>32</td>
<td>10</td>
<td>0</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>31</td>
<td>36</td>
<td>9</td>
<td>10</td>
<td>1</td>
<td>35</td>
<td>9</td>
<td>3</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>$\ell^{33}$</td>
<td>8</td>
<td>26</td>
<td>36</td>
<td>8</td>
<td>23</td>
<td>8</td>
<td>6</td>
<td>31</td>
<td>31</td>
<td>11</td>
<td>6</td>
<td>1</td>
<td>10</td>
<td>23</td>
<td>29</td>
<td></td>
</tr>
</tbody>
</table>
Let
\[ X_i = \begin{pmatrix} a^{(i)}_\ell & -\ell^3 \\ 1 & 0 \end{pmatrix}. \]

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
\[ p \left( \frac{37 \cdot 5^{456u-1}n + 1}{24} \right) \equiv 0 \mod 37 \]
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 3.6 is not optimal. (Here we have \( K = 456 \).)

For other small primes \( \ell \), we find that the congruence
\[ p \left( \frac{37\ell^{2uk-1}n + 1}{24} \right) \equiv 0 \mod 37 \]
holds for all \( n \) not divisible by \( \ell \) with
\[
\begin{array}{ccccccccccccccc}
\ell & 5 & 7 & 11 & 13 & 17 & 19 & 23 & 29 & 31 & 41 & 43 & 47 & 53 & 59 & 61 \\
k & 228 & 57 & 18 & 684 & 38 & 38 & 684 & 684 & 228 & 171 & 18 & 333 & 18 & 12 & 684 \\
\end{array}
\]

6 Generalizations

There are several directions in which one may generalize Theorem 3.6. 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 \( m = 5 \) and 7, Watson [18, 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
\[
\begin{align*}
  c_{j,i} &
  = \begin{cases} 
    3^{j-1} 5^j \mod 5^{j+1} & \text{if } i = 1, \\
    0 \mod 5^{j+1} & \text{if } i \geq 2.
  \end{cases}
\end{align*}
\]

From the identity, one deduces that

\[
F_{5,j} \equiv 3^{j-1} 5^j \begin{cases} 
  \eta(24\tau)^{19} \mod 5^{j+1} & \text{if } j \text{ is odd}, \\
  \eta(24\tau)^{23} \mod 5^{j+1} & \text{if } j \text{ is even}.
\end{cases}
\tag{16}
\]

Then Lovejoy and Ono \cite{12} used this formula to study congruences of the partition function modulo higher powers of 5. One distinct feature of \cite{12} is the following lemma.

**Lemma 6.1** (Lovejoy and Ono \cite[Theorem 2.2]{12}). 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
\[
a, b \equiv \left( \frac{15}{\ell} \right) (1 + \ell) \mod 5. \tag*{\square}
\]

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 6.2.** 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

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

for all positive integers \( j \) and \( u \) and all integers \( n \) not divisible by \( \ell \). \tag*{\square}
Proof. In view of (16), 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 3.4 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 \( a_1 = a \), \( b_1 = -\ell^6(-12/\ell) \), \( c_1 = -\ell^{17} \), 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 3.6, if the order of \( (a - \ell^{17}) \mod 5 \) (18) in \( \text{PGL}(\mathbb{F}_5) \) is \( k \), then

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

for all positive integers \( u \). Now by Lemma 6.1 the characteristic polynomial of (18) 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 (18) 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, (19) holds with \( k = K_\ell \). This yields the congruence

\[
p \left( 5j^{2uK_{\ell^{-1}}n + 1} \right) \equiv 0 \mod 5^{j+1}
\]

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

The proof of the case \( j \) even is exactly the same because \( \ell^{21} \equiv \ell^{17} \mod 5 \).  

Remark 6.3. Watson [18] 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 6.1 in this case, we do not have a result as precise as Theorem 6.2.  

\[\square\]
The next congruence result is an analog of [19, Theorem 2], which in turn originates from the argument outlined in [13, page 301].

**Theorem 6.4.** Let $\ell \geq 7$ be a prime. Assuming one of the three situations below occurs, we set $k_\ell$ and $m_\ell$ to be

1. $k_\ell = 2$ and $m_\ell = 5$ if $\ell \equiv 1 \text{ mod } 5$, $(-n/\ell) = -1$,
2. $k_\ell = 2$ and $m_\ell = 4$ if $\ell \equiv 2 \text{ mod } 5$, $(-n/\ell) = -1$, and
3. $k_\ell = 1$ and $m_\ell = 4$ if $\ell \equiv 3 \text{ mod } 5$, $(-n/\ell) = -1$.

Then

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

for all nonnegative integers $u$ and all positive integers $i$. \qed

**Proof.** Assume first that $i$ is odd. Again, in view of (16), 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 $a$ be the eigenvalue of $T_{\ell^2}$ associated to $\ell$. By (17), we have

$$f|U^{k}_{\ell^2} = a_k f + b_k f \otimes \left(\frac{-1}{\ell}\right) + c_k f|V^{k}_{\ell^2}, \tag{20}$$

where $a_k$, $b_k$, and $c_k$ satisfy

$$\begin{pmatrix} a_k \\ a_{k-1} \end{pmatrix} = \begin{pmatrix} a & -\ell^{17} \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad b_k \equiv -\left(\frac{-12}{\ell}\right) a_{k-1}, \quad c_k \equiv -a_{k-1} \text{ mod } 5.$$

From Lemma 6.1, we know that for $\ell \equiv 1 \text{ mod } 5$, we have $a_1 \equiv 2\epsilon$ and thus the values of $a_k$ modulo 5 are

<table>
<thead>
<tr>
<th>$a_1$</th>
<th>$a_2$</th>
<th>$a_3$</th>
<th>$a_4$</th>
<th>$a_5$</th>
<th>$a_6$</th>
<th>$a_7$</th>
<th>$a_8$</th>
<th>$a_9$</th>
<th>$a_{10}$</th>
<th>$a_{11}$</th>
<th>$a_{12}$</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2\epsilon$</td>
<td>3</td>
<td>$4\epsilon$</td>
<td>0</td>
<td>$\epsilon$</td>
<td>2</td>
<td>$3\epsilon$</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>$2\epsilon$</td>
<td>3</td>
<td>...</td>
</tr>
</tbody>
</table>

where $\epsilon = (15/\ell)$. Now assume that $f(\tau) = \sum c(n)q^n$. Comparing the $n$th Fourier coefficients of the two sides of (20) for integers $n$ relatively prime to $\ell$, we obtain

$$c(\ell^{2k}n) = \left(a_k + b_k \left(\frac{n}{\ell}\right)\right) c(n) \equiv \left(a_k - a_{k-1} \left(\frac{-12n}{\ell}\right)\right) c(n) \text{ mod } 5.$$
When $k = 5u + 2$ for a nonnegative integer $u$, we have
\[
\begin{align*}
c(\ell^{2(5u+2)} n) &\equiv 3 \left( \frac{15}{\ell} \right)^u \left( 1 + \left( \frac{15}{\ell} \right) \left( -\frac{12n}{\ell} \right) \right) c(n) \\
&= 3 \left( \frac{15}{\ell} \right)^u \left( 1 + \left( -\frac{n}{\ell} \right) \right) c(n) \mod 5.
\end{align*}
\]

Thus, if $(-n/\ell) = -1$, then $c(\ell^{2(5u+2)} n) \equiv 0 \mod 5$. This translates to the congruence
\[
p \left( \frac{5^i \ell^{2(5u+2)} n + 1}{24} \right) \equiv 0 \mod 5^{i+1}.
\]

This proves the first case of the theorem. The proof of the other cases is similar.  \[\square\]

**Remark 6.5.** Note that the case $\ell \equiv 4 \mod 5$ is missing in Theorem 6.4. This is because in this case, by Lemma 6.1, the Hecke eigenvalues of $T_{\ell^2}$ for $\eta(24\tau)^{19}$ and $\eta(24\tau)^{23}$ are both multiples of 5. Then the numbers $a_k$ in (20) satisfy
\[
\begin{pmatrix} a_k \\ a_{k-1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}.
\]

From this, we see that $a_k \pm a_{k-1}$ can never vanish modulo 5. \[\square\]

**Example 6.6.** We now give some examples of congruences predicted in Theorem 6.4.

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 (21) 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 \( p(4) = 5, \)

\[ p(57954) = 37834 \ldots \ldots 45055, \]

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

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

which is indeed a multiple of 5³.

\[ \square \]

**Theorem 6.7.** Let \( m \geq 13 \) be a prime and \( \ell \) be a prime different from 2, 3, and \( m. \) For each positive integer \( i, \) there exists a positive integer \( K \) such that for all \( u \geq 1 \) and all positive integers \( n \) not divisible by \( \ell, \) the congruence

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

holds. There is also another positive integer \( M \) such that

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

holds for all nonnegative integers \( n \) and \( r. \)

\[ \square \]

**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

\[ k_{m,i} = \begin{cases} \frac{(m^{i-1} + 1)(m - 1)}{2} - 12 & \text{if } i \text{ is odd}, \\ m^{i-1}(m - 1) - 12 & \text{if } i \text{ is even}. \end{cases} \]

By [2, Theorem 3], 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 3.6.
Example 6.8. Consider the case $m = 13$ and $i = 2$ of Theorem 6.7 and assume that $\ell$ is a prime different from 2, 3, and 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

$$f_i = \eta(24\tau)^{23}E_4(24\tau)^{3(13-i)}\Delta(24\tau)^{i-1}, \quad i = 1, \ldots, 13,$$

for $\mathbb{Z}[q] \cap S_{23,144}$ and let $A$ be the matrix of $T_{\ell^2}$ with respect to this basis. If the order of the matrix

$$\begin{pmatrix} A & -\ell^{309}I_{13} \\ I_{13} & 0 \end{pmatrix} \mod 169$$

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

$$A = \begin{pmatrix}
20 & 101 & 52 & 52 & 166 & 148 & 46 & 135 & 96 & 51 & 73 & 49 & 128 \\
166 & 164 & 159 & 66 & 123 & 50 & 144 & 85 & 29 & 116 & 22 & 93 & 10 \\
158 & 152 & 90 & 65 & 20 & 167 & 27 & 96 & 109 & 154 & 127 & 164 & 76 \\
120 & 154 & 132 & 110 & 22 & 113 & 115 & 51 & 25 & 104 & 108 & 82 & 33 \\
134 & 23 & 151 & 120 & 151 & 44 & 30 & 1 & 76 & 32 & 60 & 132 & 165 \\
121 & 40 & 83 & 4 & 56 & 88 & 3 & 134 & 100 & 85 & 88 & 18 & 3 \\
23 & 20 & 20 & 31 & 66 & 24 & 41 & 126 & 47 & 137 & 33 & 112 & 49 \\
143 & 18 & 44 & 26 & 89 & 109 & 118 & 148 & 35 & 16 & 35 & 122 & 150 \\
144 & 51 & 47 & 143 & 109 & 164 & 52 & 38 & 92 & 50 & 98 & 60 & 104 \\
70 & 165 & 89 & 80 & 28 & 75 & 19 & 110 & 101 & 41 & 155 & 78 & 67 \\
123 & 147 & 54 & 4 & 60 & 133 & 49 & 151 & 30 & 32 & 157 & 108 & 82 \\
95 & 139 & 50 & 70 & 124 & 168 & 87 & 63 & 13 & 104 & 58 & 107 & 113
\end{pmatrix} \mod 169,$$}

modulo 169, and the order $K$ is 28, 392, which yields

$$p\left(\frac{13^2 \cdot 5^{56.783}n + 1}{24}\right) \equiv 0 \mod 13^2$$

for all $n$ not divisible by 5. □
Acknowledgements

The author would like to thank the referees for thorough reading of the manuscript and providing many invaluable comments. In particular, the author is very grateful to one of the referees for giving a more accurate account of the history of the partition congruence problem and to another referee for bringing his attention to a very recent paper of Garvan [10]. Also, the proof of Proposition 2.1 presented here was suggested by the second referee.

This paper was dedicated to Prof. B. C. Berndt on the occasion of his 70th birthday.

Funding

This work was partially supported by the National Science Council of Taiwan, grant no. 98-2115-M-009-001 (to Y.Y.). This work was also supported by the National Center for Theoretical Sciences.

References


