Congruence properties for the partition function

Scott Ahlgren* and Ken Ono†‡

*Department of Mathematics, University of Illinois, Urbana, IL 61801; and †Department of Mathematics, University of Wisconsin, Madison, WI 53706

Communicated by Richard A. Askey, University of Wisconsin, Madison, WI, September 17, 2001 (received for review August 15, 2000)

Eighty years ago, Ramanujan conjectured and proved some striking congruences for the partition function modulo powers of 5, 7, and 11. Until recently, only a handful of further such congruences were known. Here we report that such congruences are much more widespread than was previously known, and we describe the theoretical framework that appears to explain every known Ramanujan-type congruence.

1. Introduction and Statement of Results.

Let $p(n)$ denote the usual partition function; $p(n)$ is the number of ways to write a positive integer n as the sum of a nonincreasing sequence of positive integers. As usual, we agree that $p(0) = 1$ and that $p(t) = 0$ if $t \notin \mathbb{Z}_{\geq 0}$. Many of the most interesting arithmetic properties of this function were suggested (and often proved) by Ramanujan. Notice that if δ_ℓ is defined by

$$\delta_\ell := \frac{\ell^2 - 1}{24}, \qquad [1.1]$$

then the celebrated Ramanujan congruences may be written succinctly in the form

$$p(\ell n - \delta_\ell) \equiv 0 \pmod{\ell}.$$

Countless papers have been written on these three congruences and their extensions (already conjectured, and in some cases proved, by Ramanujan) to arbitrary powers of 5, 7, and 11 [see the fundamental works of Andrews, Atkin, Dyson, Garvan, Kim, Ramanujan, Stanton, and Swinnerton-Dyer (1–10)]. Each of these extensions lies within the class $-\delta_\ell \pmod{\ell}$. The important role that this class plays in the theory is illustrated by the work of Kiming and Olsson (ref. 11, theorem 1), who proved that if $\ell \geq 5$ is prime and $p(\ell n + \beta) \equiv 0 \pmod{\ell}$ for all n, then $\beta \equiv -\delta_\ell \pmod{\ell}$.

Work of Atkin, Newman, O'Brien, and Swinnerton-Dyer (12, 14, 15, 16) produced further congruences modulo ℓ^m for primes $\ell \leq 31$ and small m. The examples discovered by Atkin and Newman in refs. 12 and 16 show that not every congruence lies within the progression $-\delta_\ell \pmod{\ell}$. For example, we have

$$p(17303n + 237) \equiv 0 \pmod{13}. \qquad [1.2]$$

We have shown (13, 17) that if $\ell \geq 5$ is prime and m is any positive integer, then there are infinitely many congruences of the form

$$p(An + B) \equiv 0 \pmod{\ell^m}.$$

As in the case of Ramanujan's congruences, all of these arithmetic progressions lie within the class $-\delta_\ell \pmod{\ell}$. To summarize, the current state of knowledge consists of a systematic theory of congruences within the progressions $-\delta_\ell \pmod{\ell}$, as well as some sporadic examples of congruences that fall outside of this class. In view of this, it is natural to wonder what role the class $-\delta_\ell \pmod{\ell}$ truly plays.

In this paper, we show that in general this class is not as distinguished as might have been expected. In fact, we prove that it is only one of $(\ell + 1)/2$ classes modulo ℓ in which the partition function enjoys similar congruence properties. The results in this paper include the main results in refs. 13 and 17 as special cases and provide a theoretical framework that (to our knowledge) explains every known congruence for the partition function.

For each prime $\ell \geq 5$, define the integer $\varepsilon_\ell \in \{\pm 1\}$ by

$$\varepsilon_\ell := \left(\frac{-6}{\ell}\right), \qquad [1.3]$$

and let S_ℓ denote the set of $(\ell + 1)/2$ integers

$$S_\ell := \left\{\beta \in \{0, 1, \ldots, \ell - 1\} : \left(\frac{\beta + \delta_\ell}{\ell}\right) = 0 \text{ or } -\varepsilon_\ell\right\}. \qquad [1.4]$$

THEOREM 1. *If $\ell \geq 5$ is prime, m is a positive integer, and $\beta \in S_\ell$, then a positive proportion of the primes $Q \equiv -1 \pmod{24\ell}$ have the property that*

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

for all $n \equiv 1 - 24\beta \pmod{24\ell}$ with $\gcd(Q, n) = 1$.

Note that the case when $\beta \equiv -\delta_\ell \pmod{\ell}$ already contains the main results in refs. 13 and 17.

In general, there is no simple description of the set of primes Q occurring in *Theorem 1.* However, as Atkin (12) showed, when $\ell = 5$, 7, or 13, the situation can be made quite explicit. For example, Atkin proved the following (see ref. 12 for analogous results when $\ell = 7$ or 13).

THEOREM 2 [Atkin (12)].

(1) *Suppose $\ell \equiv 4 \pmod 5$ is prime and n is a positive integer with $\ell \nmid n$. If $n \equiv 23\ell \pmod{120}$ or $n \equiv 47\ell \pmod{120}$, then*

$$p\left(\frac{\ell^3 n + 1}{24}\right) \equiv 0 \pmod 5.$$

(2) *Suppose $\ell \equiv 3 \pmod 5$ is a prime exceeding 3, and n* is a positive integer with $(-n/\ell) = -1$. *If $n \equiv 23 \pmod{120}$ or $n \equiv 47 \pmod{120}$, then*

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

We should remark that Newman (16) discovered the simplest example of the congruences described in the first part of *Theorem 2* (i.e., the case where $\ell = 19$). Notice that in either part of *Theorem 2*, fixing n in an appropriate residue class modulo 120ℓ yields a Ramanujan-type congruence. For example, if $\ell = 13$, then the second part of *Theorem 2* implies, for every integer n, that

$$p(10985n + 2697) \equiv 0 \pmod 5. \qquad [1.5]$$

Arguing in this manner from *Theorem 1*, we obtain

THEOREM 3. *If $\ell \geq 5$ is prime, m is a positive integer, and $\beta \in S_\ell$, then there are infinitely many non-nested arithmetic progressions $\{An + B\} \subseteq \{\ell n + \beta\}$, such that for every integer n we have*

$$p(\mathcal{A}n + \mathcal{B}) \equiv 0 \pmod{\ell^m}.$$

‡To whom reprint requests should be addressed. E-mail: ono@math.wisc.edu.

www.pnas.org/cgi/doi/10.1073/pnas.191488598

If M is an integer coprime to 6, then *Theorem 3* and the Chinese Remainder Theorem guarantee the existence of congruences modulo $\mathcal{M}$.

In Section 2, we construct half integral weight cusp forms whose coefficients capture the relevant values of the partition function, and in Section 3 we prove *Theorem 1*. The proof requires certain facts arising from the theory of Galois representations associated to modular forms and Shimura's theory of half integral weight modular forms. In Section 4, we consider those progressions $\ell n + \beta$ for $\beta \notin \mathcal{S}_\ell$. We give heuristics that cast doubt on the existence of congruences within these progressions.

2. Half integral weight cusp forms and the partition function.

We assume familiarity with standard notation and facts from the theory of integral and half integral weight modular forms. Throughout, we agree that $q := e^{2\pi iz}$, and we identify a modular form $f(z)$ with its Fourier expansion $f(z) = \Sigma_{n=0}^{\infty} a(n)q^n$. Recall Dedekind's eta-function

$$\eta(z) := q^{1/24} \prod_{n=1}^{\infty} (1 - q^n). \qquad [2.1]$$

THEOREM 2.1. *Suppose $\ell \geq 5$ is prime and m is a positive integer. If $\beta \in S_\ell$, then there is an integer $\lambda_{\ell,m}$ and a modular form $F_{\ell,m,\beta}(z) \in S_{(2\lambda_{\ell,m}+1)/2}(\Gamma_1(576\ell^5)) \cap \mathbb{Z}[[q]]$ such that*

$$F_{\ell,m,\beta}(z) \equiv \sum_{n=0}^{\infty} p(\ell n + \beta) q^{24\ell n + 24\beta - 1} \pmod{\ell^m}.$$

Proof: If $\ell \geq 5$ is prime and t is a positive integer, then

$$E_{\ell,t}(z) := \frac{\eta^{\ell^t}(z)}{\eta(\ell^t z)} \in M_{(\ell^t-1)/2}(\Gamma_0(\ell^t), \chi_{\ell,t}), \qquad [2.2]$$

where $\chi_{\ell,t} := ((-1)^{(\ell^t-1)/2}\ell^t/\bullet)$. By using standard facts, it can be shown that if $\ell \nmid a$ and $0 \leq b < t$, then $\mathrm{ord}_{a/\ell^b}(E_{\ell,t}(z)) > 0$. Hence, $E_{\ell,t}(z)$ vanishes at those cusps of $\Gamma_0(\ell^t)$, which are not equivalent to ∞. Also, because $(1 - X)^\ell \equiv (1 - X^\ell) \pmod{\ell}$, for every $m > 0$ we have

$$E_{\ell,t}^{\ell^{m-1}}(z) \equiv 1 \pmod{\ell^m}. \qquad [2.3]$$

If $\ell \geq 5$ is prime, then define $f_\ell(z) = \Sigma_{n=1}^{\infty} a_\ell(n)q^n$ by

$$f_\ell(z) = \sum_{n=1}^{\infty} a_\ell(n)q^n := \frac{\eta^\ell(\ell z)}{\eta(z)} \in M_{(\ell-1)/2}(\Gamma_0(\ell), (\tfrac{\bullet}{\ell})). \qquad [2.4]$$

Because $\Sigma_{n=0}^{\infty} p(n)q^n = \Pi_{n=1}^{\infty}(1-q^n)^{-1}$, **2.1** and **2.4** imply that

$$\sum_{n=1}^{\infty} a_\ell(n)q^n = \left(\sum_{n=0}^{\infty} p(n)q^{n+\delta_\ell}\right) \cdot \prod_{n=1}^{\infty}(1 - q^{\ell n})^\ell. \qquad [2.5]$$

Define $\tilde{f}_\ell(z)$ by

$$\tilde{f}_\ell(z) := \sum_{n=1}^{\infty} (1 - \varepsilon_\ell(\tfrac{n}{\ell}))a_\ell(n)q^n. \qquad [2.6]$$

By standard facts, we have $\tilde{f}_\ell(z) \in M_{(\ell-1)/2}(\Gamma_0(\ell^3), (\tfrac{\bullet}{\ell}))$. By **2.3** and **2.6**, if m' is sufficiently large, then $f_{\ell,m'}(z) := E_{\ell,3}^{\ell^{m'}}(z)\tilde{f}_\ell(z)$ is a cusp form on $\Gamma_0(\ell^3)$ with character $\chi_{\ell,t}\cdot(\tfrac{\bullet}{\ell})$ for which

$$f_{\ell,m'}(z) \equiv \tilde{f}_\ell(z) \pmod{\ell^m}, \qquad [2.7]$$

and

$$\mathrm{ord}_\infty(f_{\ell,m'}(z)) \geq \delta_\ell + 1. \qquad [2.8]$$

By **2.5** and **2.7**, we have

$$\frac{f_{\ell,m'}(z)}{\eta^\ell(\ell z)} \equiv \sum_{n \equiv 0 \pmod{\ell}} p(n - \delta_\ell)q^{n - \frac{\ell^2}{24}} + 2 \sum_{\left(\frac{n}{\ell}\right) = -\varepsilon_\ell} p(n - \delta_\ell)q^{n - \frac{\ell^2}{24}} \pmod{\ell^m}. \qquad [2.9]$$

Now **2.8** shows that $(f_{\ell,m'}(z)/\eta^\ell(\ell z))^{24}$ vanishes at ∞. Therefore, if m' is sufficiently large, then this form vanishes at every cusp. It follows that $f_{\ell,m'}(24z)/\eta^\ell(24\ell z)$ is a cusp form on $\Gamma_0(576\ell^3)$. We have the general fact that if $f(z) = \Sigma_{n=1}^{\infty} a(n)q^n \in S_{\lambda+\frac{1}{2}}(\Gamma_1(N))$, and r and t are positive integers, then $\Sigma_{n \equiv r \pmod{t}} a(n)q^n \in S_{\lambda+\frac{1}{2}}(\Gamma_1(Nt^2))$. *Theorem 2.1* follows by applying this fact to $f_{\ell,m'}(24z)/\eta^\ell(24\ell z)$. □

3. Proof of *Theorems 1* and *2*.

We begin with some general facts. Suppose that $\lambda \in \mathbb{Z}$, and that $f(z) = \Sigma_{n=1}^{\infty} a(n)q^n \in S_{\lambda+\frac{1}{2}}(\Gamma_1(N))$ has algebraic coefficients. We have a decomposition

$$S_{\lambda+\frac{1}{2}}(\Gamma_1(N)) = \bigoplus_{\chi \text{ even}} S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi); \qquad [3.1]$$

further, we may write $f(z) = \Sigma_{\chi \text{ even}} \alpha_{f_\chi} f_\chi(z)$, where each α_{f_χ} is algebraic, and each form $f_\chi(z) \in S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi)$ has algebraic integer coefficients. Suppose that the Fourier expansion of such a form is given by $f_\chi(z) = \Sigma_{n=1}^{\infty} a_\chi(n)q^n$. If p is prime, then the action of the usual Hecke operator $T_\chi(p^2)$ on f_χ is described by

$$f_\chi | T_\chi(p^2) = \sum_{n=1}^{\infty} \left(a_\chi(p^2 n) + \chi(p)\left(\frac{(-1)^\lambda n}{p}\right)p^{\lambda-1}a_\chi(n) + \chi(p^2)p^{2\lambda-1}a_\chi(n/p^2)\right)q^n. \qquad [3.2]$$

Using **3.1** and **3.2**, we define the operator $T(p^2)$ on $S_{\lambda+\frac{1}{2}}(\Gamma_1(N))$ via linearity. In particular, if $f(z) = \Sigma_{n=1}^{\infty} a(n)q^n \in S_{\lambda+\frac{1}{2}}(\Gamma_1(N))$ and $p \equiv -1 \pmod{N}$ is prime, then

$$f | T(p^2) = \sum_{n=1}^{\infty} \left(a(p^2 n) + p^{\lambda-1}\left(\frac{(-1)^\lambda n}{p}\right)a(n) + p^{2\lambda-1}a(n/p^2)\right)q^n. \qquad [3.3]$$

LEMMA 3.1. *Suppose that $f(z) = \Sigma_{n=1}^{\infty} a(n)q^n \in S_{\lambda+\frac{1}{2}}(\Gamma_1(N))$ has algebraic integer coefficients. If M is a positive integer, then a positive proportion of the primes $p \equiv -1 \pmod{MN}$ have the property that $f(z) \mid T(p^2) \equiv 0 \pmod{M}$.*

Proof: Write $f(z) = \Sigma_{\chi \text{ even}} \alpha_{f_\chi} f_\chi(z)$ as above and choose a positive integer $\mathcal{D}$ such that each $D\alpha_{f_\chi}$ is an algebraic integer. After replacing M by DM, we see that it will suffice to prove that a positive proportion of the primes $p \equiv -1 \pmod{MN}$ have the property that $f_\chi(z) \mid T(p^2) \equiv 0 \pmod{M}$ for every character χ.

Fix a number field K such that the coefficients of each form f_χ and the values of each character χ belong to the ring of integers $\mathcal{O}_K$. If t is an integer, then let χ_t denote the usual Kronecker character for $\mathbb{Q}(\sqrt{t})$. For each form f_χ and for every positive squarefree integer t, we have the Shimura lift (18)

$$S_t(f_\chi)(z) \in S_{2\lambda}(\Gamma_0(N), \chi^2) \subseteq S_{2\lambda}(\Gamma_1(N)) \qquad [3.4]$$

MATHEMATICS

defined by $S_t(f_\chi)(z) := \Sigma_{n=1}^{\infty} A_{\chi,t}(n)q^n$, where the $A_{\chi,t}(n)$ are given by

$$\sum_{n=1}^{\infty} \frac{A_{\chi,t}(n)}{n^s} = L(s-\lambda+1, \chi\chi_t\chi^{\lambda-1}) \sum_{n=1}^{\infty} \frac{a_\chi(tn^2)}{n^s}. \qquad [3.5]$$

If M, k, and N are positive integers, then let $S_k(\Gamma_1(N))_{\mathbb{O}_K/M}$ [respectively (resp) $S_k(\Gamma_0(N), \chi)_{\mathbb{O}_K/M}$] denote the reductions modulo M of those forms in $S_k(\Gamma_1(N))$ [*resp* $S_k(\Gamma_0(N), \chi)$] with coefficients in $\mathbb{O}_K$, and let $T(p)$ [resp $T_\chi(p)$] denote the usual integral-weight Hecke operator. Serre (ref. 19, 6.4) proved that a positive proportion of the primes $p \equiv -1 \pmod{MN}$ have

$$F_\chi(z)|T_\chi(p) \equiv 0 \pmod{M} \text{ for all } F_\chi \in S_k(\Gamma_0(N), \chi)_{\mathbb{O}_K/M}.$$

By using a straightforward modification of the same argument, one can show that a positive proportion of the primes $p \equiv -1 \pmod{MN}$ have

$$F(z)|T(p) \equiv 0 \pmod{M} \text{ for all } F \in S_k(\Gamma_1(N))_{\mathbb{O}_K/M}.$$

After **3.4**, we conclude that a positive proportion of the primes $p \equiv -1 \pmod{MN}$ have

$$S_t(f_\chi)|T(p) \equiv 0 \pmod{M} \text{ for all } \chi \text{ and } t.$$

Because the Shimura correspondence commutes with the action of the Hecke algebra, it follows that if p is such a prime, then

$$S_t(f_\chi|T(p^2)) \equiv 0 \pmod{M} \text{ for all } \chi \text{ and } t. \qquad [3.6]$$

Lemma 3.1 follows from **3.5** and **3.6**. □

Proof of Theorem 1: We apply *Lemma 3.1* to the forms $F_{\ell,m,\beta}(z)$ given in *Theorem 2.1.* Fix a prime ℓ and an integer $\beta \in S_\ell$ and write

$$F_{\ell,m,\beta}(z) = \sum_{n=1}^{\infty} a_{\ell,m,\beta}(n)q^n \equiv \sum_{n \equiv 24\beta-1 \pmod{24\ell}} p\left(\frac{n+1}{24}\right)q^n \pmod{\ell^m}.$$

By *Lemma 3.1*, a positive proportion of the primes $Q \equiv -1 \pmod{24\ell}$ have the property that $F_{\ell,m,\beta}(z) \mid T(Q^2) \equiv 0 \pmod{\ell^m}$. After replacing n by Qn in definition **3.3**, we see that if $n \equiv 1 - 24\beta \pmod{24\ell}$ and $\gcd(Q, n) = 1$, then

$$0 \equiv a_{\ell,m,\beta}(Q^3n) \equiv p\left(\frac{Q^3n+1}{24}\right) \pmod{\ell^m},$$

because $Q^3n \equiv 24\beta - 1 \pmod{24\ell}$. *Theorem 1* follows. □

4. Final Remarks.

One naturally questions whether *Theorem 1* can be extended to the remaining residue classes modulo ℓ. Suppose that $\beta \in \{0, \ldots, \ell-1\}$. If we could produce a cusp form $F_{\ell,m,\beta}(z)$ as in *Theorem 2.1*, then we would obtain the statment of *Theorem 1* for β. Because $F_{\ell,m,0}(z)$ would necessarily have a pole at infinity, this approach seems hopeless when $\beta = 0$. The situation, however, is less clear when $\beta \neq 0$. For every prime $\ell \geq 5$ and every m, it is straightforward to show that there exists an integral weight modular form $H_{\ell,m}(z)$ such that

$$\sum_{n \not\equiv \delta_\ell \pmod{\ell}} p(n - \delta_\ell)q^{24n-\ell^2} \equiv H_{\ell,m}(24z)/\eta^\ell(24\ell z) \pmod{\ell^m}.$$

However, to construct $H_{\ell,m}(z)$ requires the twists of $f_\ell(z)$ by all of the Dirichlet characters modulo ℓ; it results that $H_{\ell,m}(z)$ is a form on $\Gamma_1(\ell^3)$. By contrast, the form that we constructed in **2.6** required only a single quadratic twist and so remained on $\Gamma_0(\ell^3)$.

It is clear that if we had the analog for $\Gamma_1(\ell^t)$ of the form $E_{\ell,t}(z)$ used in the proof of *Theorem 2.1*, then we could prove *Theorem 1* for all nonzero β. By using the work of Hecke, it is possible to construct an Eisenstein series on $\Gamma_1(\ell^t)$ that has the proper cusp conditions (in fact, up to scalar multiplication, exactly one such series exists). It remains to determine whether this series can be defined over the algebraic numbers, and, if so, to determine the ℓ-adic nature of its coefficients. Unfortunately, the answers to both of these problems seem to depend on the arithmetic of certain unknown values of Dirichlet L-functions at positive integral arguments. Although many of these values can be described in terms of generalized Bernoulli numbers, the remaining values are (up to unknown algebraic factors) values of certain regulators defined via canonical maps from higher K-groups into Minkowski-type spaces (20).

We conclude by remarking that computer calculations seem to cast some doubt on whether such forms exist in general. If they did, this evidence suggests a contradiction to Serre's famous result (ref. 19, theorem 4.7) that if M is any given integer, then almost all of the coefficients of an integral weight modular form with integer coefficients are multiples of M.

S.A. is supported by a National Science Foundation grant. K.O. is supported by a National Science Foundation Presidential Early Career Award, an Alfred P. Sloan Foundation Research Fellowship, and a David and Lucile Packard Research Fellowship.

1. Andrews, G. E. & Garvan, F. (1988) *Bull. Am. Math. Soc. (N.S.)* **18,** 167–171.
2. Atkin, A. O. L. (1967) *Glasgow Math. J.* **8,** 14–32.
3. Atkin, A. O. L. & Swinnerton-Dyer, H. P. F. (1954) *Proc. London Math. Soc.* **4,** 84–106.
4. Berndt, B. C. & Ono, K. (1999) *Sem. Lothar. Comb.* **42,** B42.
5. Dyson, F. J. (1944) *Eureka (Cambridge)* **8,** 10–15.
6. Garvan, F., Kim, D. & Stanton, D. (1990) *Invent. Math.* **101,** 1–17.
7. Ramanujan, S. (1916) *Trans. Cambridge Philos. Soc.* **22,** 159–184.
8. Ramanujan, S. (1919) *Proc. Cambridge Philos. Soc.* **19,** 207–210.
9. Ramanujan, S. (1920) *Proc. London Math. Soc.* **18,** xix.
10. Ramanujan, S. (1921) *Math. Z.* **9,** 147–153.
11. Kiming, I. & Olsson, J. (1992) *Arch. Math. (Basel)* **59,** 348–360.
12. Atkin, A. O. L. (1968) *Proc. London Math. Soc.* **18,** 563–576.
13. Ahlgren, S. (2000) *Math. Ann.* **318,** 795–803.
14. Atkin, A. O. L. & O'Brien, J. N. (1967) *Trans. Am. Math. Soc.* **126,** 442–459.
15. Atkin, A. O. L. & Swinnerton-Dyer, H. P. F. (1971) *Proc. Sympos. Pure Math.* **19,** 1–25.
16. Newman, M. (1967) *Math. Comp.* **21,** 481–482.
17. Ono, K. (2000) *Ann. Math.* **151,** 293–307.
18. Shimura, G. (1973) *Ann. Math.* **97,** 440–481.
19. Serre, J.-P. (1976) *L'Enseign. Math.* **22,** 227–260.
20. Beilinson, A. A. (1984) *Current Problems in Mathematics, Itogi Nauki i Tekhniki Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow* **24,** 181–238.