DIVISIBILITY AND DISTRIBUTION OF PARTITIONS INTO DISTINCT PARTS

JEREMY LOVEJOY

Abstract. We study the generating function for $Q(n)$, the number of partitions of a natural number n into distinct parts. Using the arithmetic properties of Fourier coefficients of integer weight modular forms, we prove several theorems on the divisibility and distribution of $Q(n)$ modulo primes $p \geq 5$.

1. Introduction

A partition of n into distinct parts is a decreasing sequence of positive integers whose sum is n. The number of such partitions of n is denoted by $Q(n)$, and it is an easy combinatorial exercise [2] to determine the generating function for $Q(n)$

$$\sum_{n=0}^{\infty} Q(n)q^n = \prod_{n=1}^{\infty} (1+q^n) = 1 + q + q^2 + 2q^3 + 2q^4 + 3q^5 + ... \tag{1}$$

A problem that naturally arises in the study of a combinatorial function such as $Q(n)$ is that of divisibility and distribution. Given a natural number M, describe the behavior of $Q(n)$ modulo M. In the absence of any combinatorial intuition, the naive assumption is that such a function is randomly distributed among the congruence classes modulo M, although this is not necessarily the case. For example, Gordon and Ono [5] have shown that almost all of the values of $Q(n)$ are divisible by 2^k for any natural number k. Except in a few cases [1], it seems hopeless that combinatorial arguments will settle these problems in general, and so we must turn to the analysis of generating functions.

Using an asymptotic formula for $Q(n)$ derived using the Hardy - Ramanujan - Rademacher circle method, Rickert [12] has shown that the number of primes $p < X$ which divide some value of $Q(n)$ is $\gg \log\log X$. Since the number of primes $p < X$ is asymptotically $X/\log X$, this is a sparse subset of the prime numbers. Moreover, Rickert's theorem does not preclude the possibility that every prime p dividing $Q(n)$ does so only once. Using the theory of modular forms, we will establish the following:

Theorem 1. *For any prime number $p \geq 5$,*

$$\liminf_{N\to\infty} \frac{\#\{n < N : Q(n) \equiv 0 \pmod{p}\}}{N} \geq \frac{1}{p} \tag{2}$$

Since the discovery by Ramanujan of congruences in arithmetic progressions for the ordinary partition function, there has been extensive interest in such congruences for combinatorial functions. For partitions into distinct parts, Gordon and Hughes [4] established congruences of the

Date: January 21, 2004.

1991 *Mathematics Subject Classification.* Primary 11P83; Secondary 05A17.

Ramanujan type modulo powers of 5 and 7 using methods based on Atkin's work on the classical partition function $p(n)$. Here we use a decidedly different technique to demonstrate

Theorem 2. *For any prime $p \geq 5$, there are infinitely many distinct arithmetic progressions $an+b$ such that for all nonnegative integers n*

$$Q(an+b) \equiv 0 \pmod{p} \tag{3}$$

It turns out that the values of a guaranteed by Theorem 2 are typically quite large, and in §4 we present a few of the simplest such congruences. These *extracombinatorial* congruences arise from an inherent regularity of the generating function rather than some combinatorial property of partitions with distinct parts.

In the 1960's Newman [9] made a famous conjecture about the distribution of the ordinary partition function $p(n)$ modulo M. He predicted that for any r there will be infinitely many n such that $p(n) \equiv r \pmod{M}$. Although this question remains open, Ono [10] has found a computational technique for verifying that a given prime larger than 5 satisfies Newman's conjecture, and subsequently the conjecture has been proven for all primes M below 1000. In the case of partitions into distinct parts, Ono and Penniston [11] have shown that the answer to Newman's question is affirmative if M is any power of 2. We consider $Q(n)$ modulo primes $p \geq 5$ and prove the following

Theorem 3. *Let $p \geq 5$ be prime. Suppose there is one $n_0 \equiv -24^{-1} \pmod{p}$ such that $p \nmid Q(n_0)$. Then*

$$\#\{n < N : Q(n) \equiv r \pmod{p}\} \gg_p \begin{cases} N & \text{if } r \equiv 0 \pmod{p} \\ \frac{N}{\log N} & \text{if } r \not\equiv 0 \pmod{p} \end{cases}$$

Moreover, if such an n_0 exists then $n_0 \leq 32p(p-1)$.

2. Preliminaries

In many instances the generating functions for combinatorial objects turn out to be closely related to modular forms, particularly to products of η functions (Recall that $\eta(z) := q^{1/24}(q;q)_\infty$ where $(q;q)_\infty := \prod_{n=1}^{\infty}(1-q^n)$ and $q := e^{2\pi i z}$). For this reason, we often make use the following fact recorded in [3, 7, 8]:

Theorem 4 (Gordon, Hughes, Ligozat, Newman)**.** *Let*

$$f(z) = \prod_{1 \leq \delta | N} \eta^{r_\delta}(\delta z)$$

be a product of η functions which satisfies the following criteria

(*i*)

$$\sum_{\delta | N} \delta r_\delta \equiv 0 \pmod{24}$$

(*ii*)

$$\sum_{\delta | N} \frac{N}{\delta} r_\delta \equiv 0 \pmod{24}$$

(iii)

$$\sum r_\delta \in 2\mathbb{Z}^+$$

(iv) For each $d|N$,

$$\sum_{\delta|N} \frac{(\gcd(d,\delta))^2 r_\delta}{\delta} \geq 0$$

Then, $f(z) \in M_k(\Gamma_0(N), \chi)$ where $k = \frac{1}{2}\sum r_\delta$ and

$$\chi(\ell) = \left(\frac{(-1)^k \prod \delta^{r_\delta}}{\ell}\right).$$

Here $M_k(\Gamma_0(N), \chi)$ is the finite dimensional $\mathbb{C}$ - vector space of holomorphic modular forms of weight k, level N, and character χ. The condition *(iv)* ensures that f has nonnegative orders at the cusps. If f actually has positive orders at all cusps, then it is a cusp form, and we denote the corresponding space of cusp forms by $S_k(\Gamma_0(N), \chi)$. We use the notation $M_k(\Gamma_0(N), \chi)_m$ and $S_k(\Gamma_0(N), \chi)_m$ to denote the same spaces except the coefficients in the Fourier expansions of the relevant forms with integer coefficients are reduced modulo m. Before proving a key theorem, we record some useful facts about modular forms and their Fourier coefficients, and refer the interested reader to [6] for a more detailed overview of modular forms.

Proposition 5. *Suppose that $f(z) = \sum_{n=0}^{\infty} a(n)q^n$ is a modular form in $M_k(\Gamma_0(N), \chi)$.*

(i) For any positive integer t,

$$f(tz) = \sum_{n=0}^{\infty} a(n)q^{tn}$$

is the Fourier expansion of a modular form in $M_k(\Gamma_0(tN), \chi)$

(ii) For any prime p,

$$f(z) \mid T(p) := \sum_{n=0}^{\infty} \left(a(pn) + \chi(p)p^{k-1}a(n/p)\right) q^n$$

is the Fourier expansion of a modular form in $M_k(\Gamma_0(N), \chi)$

Moreover, both statements remain true if $M_k(\Gamma_0(N), \chi)$ is replaced by $S_k(\Gamma_0(N), \chi)$.

The operator $T(p)$ is the Hecke operator for the prime p. Notice that modulo p, $f(z) \mid T(p) \equiv f(z) \mid U(p)$ on $M_k(\Gamma_0(N), \chi)_p$, where the operator $U(p)$ acts on series expansions by

$$\sum_{n=0}^{\infty} a(n)q^n \mid U(p) := \sum_{n \equiv 0 \pmod{p}} a(n)q^{\frac{n}{p}}$$

The following useful criterion allows us to check congruences for modular forms with a finite computation.

Proposition 6 (Sturm). *Suppose $f(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_k(\Gamma_0(N), \chi)$ satisfies*

(i) $a(n) \in \mathbb{Z}$ for all n

(ii) $a(n) \equiv 0 \pmod{m}$ for all $n \leq 1 + \frac{kN}{12}\prod_{p|N}(1 + \frac{1}{p})$

Then, $a(n) \equiv 0 \pmod{m}$ for all n.

We wish to study the function $\sum_{n=0}^{\infty} Q(n)q^n$ in the context of modular forms, but unfortunately this is almost certainly not the Fourier expansion of a modular form modulo any prime $p \neq 2$. However, for primes $p \geq 5$, it turns out that for a properly chosen function $h_p(n)$,

$$\sum_{n=0}^{\infty} Q((h_p(n))q^n$$

is the Fourier expansion of a cusp form modulo p. This is the content of Theorem 8, whose proof depends on the following observation.

Lemma 7. *If $f(z)$ is a cusp form in $S_k(\Gamma_0(2))$, then*

$$g(z) := \frac{f(z)}{\eta^8(z)\eta^8(2z)}$$

is a holomorphic modular form in $M_{k-8}(\Gamma_0(2))$

Proof: By Theorem 4, $\eta^8(z)\eta^8(2z)$ is a cusp form of weight 8 and level 2 and has the minimal order of vanishing of 1 at the two cusps of $\Gamma_0(2)$. Also, $\eta^8(z)\eta^8(2z)$ can have no zeroes in the upper half plane. Therefore,

$$\frac{f(z)}{\eta^8(z)\eta^8(2z)}$$

is a modular function which is holomorphic for $Im\ z > 0$ and has nonnegative orders at the cusps. That is, $g(z)$ is in $M_{k-8}(\Gamma_0(2), \chi)$. □

Theorem 8. *Let $p \geq 5$ be prime and let χ be the quadratic character defined by $\chi(d) = \left(\frac{2}{d}\right)$. Then,*

$$F_p(z) := \sum_{n=0}^{\infty} Q\left(\frac{pn-1}{24}\right) q^n \in S_{4(p-1)}(\Gamma_0(1152), \chi)_p$$

Proof: For a prime $p \geq 5$, let

$$\begin{aligned} a &:= 16 - (p \mod 24) \\ b &:= (p \mod 24) - 8 \end{aligned}$$

and

$$f_p(z) := \frac{\eta(2z)}{\eta(z)}\eta^a(2pz)\eta^b(pz).$$

Using Theorem 4 we can check that

$$\eta^{pa+1}(2z)\eta^{pb-1}(z) \in S_{4p}(\Gamma_0(2))$$

and therefore

$$f_p(z) \mid U(p) \equiv_p f_p(z) \mid T(p) \in S_{4p}(\Gamma_0(2))_p$$

By Lemma 7,

$$f_p(z) \mid U(p) \equiv \eta^8(z)\eta^8(2z)g_p(z) \pmod p$$

where $g_p(z) \in M_{4p-8}(\Gamma_0(2))$. To prove the theorem we will write $f_p(z) \mid U(p) \pmod{p}$ in a second way.

$$\begin{aligned} f_p(z) \mid U(p) &= \frac{\eta(2z)}{\eta(z)}\eta^a(2pz)\eta^b(pz) \mid U(p) \\ &= \left(\sum_{n=0}^{\infty} Q(n)q^{n+\frac{p(2a+b)+1}{24}} \mid U(p)\right)\prod_{n=1}^{\infty}(1-q^{2n})^a(1-q^n)^b \end{aligned}$$

Therefore,

$$\begin{aligned} \sum Q(n)q^{\frac{n}{p}+\frac{p(2a+b)+1}{24p}} &= \frac{f_p(z) \mid U(p)}{\prod_{n=1}^{\infty}(1-q^{2n})^a(1-q^n)^b} \\ &\equiv q^{\frac{(2a+b)}{24}}\eta^{8-a}(2z)\eta^{8-b}(z)g_p(z) \pmod{p} \end{aligned}$$

and so

$$\sum Q(n)q^{\frac{24n+1}{24p}} \equiv \eta^{8-a}(2z)\eta^{8-b}(z)g_p(z) \pmod{p} \tag{4}$$

One can verify using Theorem 4 that

$$\eta^{8-a}(48z)\eta^{8-b}(24z) \in S_4(\Gamma_0(1152),\chi)$$

and so replacing q by q^{24} in (4) gives the result. □

Remark 9. *Let*

$$\begin{aligned} \sigma_p &= -24^{-1} \pmod{p} \\ r_p &= p \pmod{24} \end{aligned}$$

Then we also have the following representation for $F_p(z)$:

$$F_p(z) = \sum_{n=0}^{\infty} Q\left(pn+\sigma_p\right)q^{24n+r_p}.$$

3. Divisibility and Distribution of $Q(n)$

Theorem 8 reveals that for any prime $p \geq 5$ certain values of $Q(n)$ are actually Fourier coefficients modulo p of modular forms. The role of modular forms in number theory is deep and detailed, and in particular there have been many observations on the arithmetic properties of their Fourier coefficients. Theorem 1 is now an immediate corollary of the following result of Serre [13]:

Theorem 10. *Suppose that*

$$f(z) = \sum_{n=0}^{\infty} a(n)q^n$$

is an integral weight holomorphic modular form with integer coefficients. For any positive integers m and N, let $\delta_m(N)$ denote the proportion of $n \leq N$ for which $a(n) \equiv 0 \pmod{m}$. Then

$$\lim_{N\to\infty}\delta_m(N) = 1$$

Although Theorem 10 makes it clear that $Q(n)$ is divisible by p for almost every n in a certain arithmetic progression modulo p, notice that it says nothing about $Q(n)$ outside of this progression.

Since $Q(pn+\sigma_p) \equiv 0 \pmod{p}$ for almost all n, it is not surprising that congruences in arithmetic subprogressions are eventually common. In [13], Serre proved the following wonderful result about the behavior of the Fourier coefficients modulo M of integer weight cusp forms, which yields the proof of Theorem 2.

Theorem 11. *Suppose that $F(z) := \sum_{n=1}^{\infty} a(n)q^n$ is an integer weight cusp form with coefficients in $\mathbb{Z}$. If m is a positive integer, then there is a set of primes S_m of positive density with the property that*

$$a(n\ell^r) \equiv (r+1)a(n) \pmod{m}$$

whenever $\ell \in S_m$, r is a positive integer, and n is coprime to ℓ.

Proof of Theorem 2: Apply Theorem 11 with $m = p$ and $r = p-1$ to the form $F_p(z)$. Then, a positive proportion of the primes ℓ satisfy

$$Q\left(\frac{pn\ell^{p-1}-1}{24}\right) \equiv 0 \pmod{p} \tag{5}$$

whenever $\gcd(n,\ell) = 1$ and $n \equiv p \pmod{24}$. To construct congruences in arithmetic progressions modulo p, we simply let $n = 24\ell k + p$. Then equation (5) becomes

$$Q\left(p\ell^p k + \frac{p^2\ell^{p-1}-1}{24}\right) \equiv 0 \pmod{p} \tag{6}$$

for all nonnegative integers k. □

Since the vector space of reductions mod M of integral weight cusp forms contains no nonzero polynomials [5], we can already say that if there is one $n \equiv -24^{-1} \pmod{p}$ for which $Q(n)$ is not a multiple of p, then there are infinitely many such n. We can do better, however, by using Theorem 11 to prove Theorem 3.

Proof of Theorem 3: Fix $p \geq 5$ and let S_p denote the set of primes for $F_p(z)$ guaranteed by Theorem 11. The case $r \equiv 0 \pmod{p}$ follows from Theorem 1. Otherwise recall the assumption that there is some $n_0 = (n-1)/24$ such that

$$Q(n_0) \equiv a \neq 0 \pmod{p}$$

Hence there exists a prime $\ell \in S_p$ such that for $1 \leq b \leq p$ the p numbers

$$Q\left(\frac{n\ell^b-1}{24}\right) \equiv (b+1)a \pmod{p}$$

cover all of the residue classes modulo p. Because p is odd, for all but possibly finitely many primes $m \in S_p$ we know that that the p numbers

$$Q\left(\frac{n\ell^b m-1}{24}\right) \equiv 2Q\left(\frac{n\ell^b-1}{24}\right) \equiv 2(b+1)a \pmod{p}$$

cover all of the residue classes modulo p. Since S_p contains a positive proportion of the primes m, we have

$$\#\{n \leq N : Q(n) \equiv r \pmod{p}\} \gg \pi(N) \gg \frac{N}{\log N}$$

The upper bound on n_0 follows easily from Sturm's criterion. □

For primes $p \geq 5$, Theorem 3 provides an easy computational technique for verifying Newman's question, and it has been checked for all such primes $p < 1000$. It is likely true for all primes $p \geq 5$. In fact, unless there is a congruence $Q(pn + \sigma_p) \equiv 0 \pmod{p}$ for *all* natural numbers n, Newman's conjecture is true for $Q(n)$ modulo p.

4. Examples

In view of the small dimensions of spaces of cusp forms with low weight, it is possible in some cases to write down $F_p(z)$ modulo p explicitly in terms of well known modular forms.

Proposition 12.

$$\sum_{n=0}^{\infty} Q(5n+1)q^n \equiv \frac{(q;q)_\infty^{11}}{(q^2;q^2)_\infty^3} \pmod{5}$$

Proof: Using Sturm's theorem, we find that

$$\begin{aligned} \frac{\eta^{56}(2z)}{\eta^{16}(z)} | U(5) &\equiv \frac{\eta^{38}(z)\eta^8(2z)}{\eta^6(5z)} \pmod{5} \\ &\equiv \eta^8(z)\eta^8(2z) \pmod{5} \end{aligned}$$

and therefore

$$F_5(z) \equiv \frac{\eta^{11}(24z)}{\eta^3(48z)} \pmod{5}.$$

□

Using similar computations, we discover nice expressions for $F_7(z)$ and $F_{11}(z)$. We employ the classical weight k Eisenstein series $E_k(z)$ defined by

$$E_k(z) := 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

where B_k is the kth Bernoulli number and

$$\sigma_{k-1}(n) := \sum_{d|n} d^{k-1}.$$

Proposition 13.

$$\sum_{n=0}^{\infty} Q(7n+2)q^n \equiv \frac{(q;q)_\infty^9}{(q^2;q^2)_\infty}(2E_8(z) - E_8(2z)) \pmod{7}.$$

Proposition 14.

$$\sum_{n=0}^{\infty} Q(11n+5)q^n \equiv 7(q;q)_\infty^5 (q^2;q^2)_\infty^3 (E_6(2z) + E_6(z)) \pmod{11}.$$

Applying the theory of Hecke operators allows one to explicitly identify congruences in arithmetic progressions for $Q(n)$. For example, we find that

$$F_p(z) \mid T(\ell) \equiv 0 \pmod{p}$$

for the pairs $(p,\ell) = (5,73),(5,97),(5,193),(5,313),(5,337),(7,673)$. Hence for these pairs (p,ℓ) we have

$$Q\left(\frac{pn\ell-1}{24}\right) + \ell^{-1}Q\left(\frac{\frac{pn}{\ell}-1}{24}\right) \equiv 0 \pmod{p} \tag{7}$$

for all nonnegative integers n with $n \equiv p \pmod{24}$. Replacing n by $24\ell n + p$ in (7) yields the follwing congruences:

Theorem 15. *For all nonnegative integers n we have*

$$\begin{aligned}
Q(26645n+76) &\equiv 0 \pmod{5}\\
Q(47045n+101) &\equiv 0 \pmod{5}\\
Q(186245n+201) &\equiv 0 \pmod{5}\\
Q(489845n+326) &\equiv 0 \pmod{5}\\
Q(567845n+351) &\equiv 0 \pmod{5}\\
Q(3170503n+1374) &\equiv 0 \pmod{7}
\end{aligned}$$

References

[1] K. Alladi, Partition identities involving gaps and weights, *Trans. Amer. Math. Soc.* **349** (1997), 5001-5019.

[2] G.E. Andrews, "The Theory of Partitions," Cambridge Univ. Press, Cambridge, 1998.

[3] B. Gordon and K. Hughes, Multiplicative properties of η-products II, *Cont. Math.* **143** (1993), 415-430.

[4] B. Gordon and K. Hughes, Ramanujan congruences for $q(n)$, "Analytic Number Theory," Lecture Notes in Math. **899** Springer, New York, 1981, pp. 333-359.

[5] B. Gordon And K. Ono, Divisibility of certain partition functions by powers of primes, *Ramanujan J.* **1** (1997), 25-34

[6] N. Koblitz, "Introduction to Elliptic Curves and Modular Forms," Springer-Verlag, New York, 1984.

[7] G. Ligozat, Courbes modulaires de genre 1, *Bull. Soc. Math. France*, [Memoire 43] (1972), 1-80.

[8] M. Newman, Construction and application of a certain class of modular functions II, *Proc. London Math. Soc.* **9** (1959), 353-387.

[9] M. Newman, Periodicity modulo m and divisibility properties of the partition function, *Trans. Amer. Math. Soc.* **97** (1960), 225-236.

[10] K. Ono, Distribution of the partition function modulo m, *Ann. of Math.* **151** (2000), 1-15.

[11] K. Ono and D. Penniston, The 2-adic behavior of the number of partitions into distinct parts, *J. Comb. Th. Ser. A*, accepted for publication.

[12] J. Rickert, Divisibility of restricted partition functions, preprint.

[13] J.P. Serre, Divisibilité de certaines fonctions arithmétiques, *L'Ensign. Math.* **22** (1976), 227-260.

[14] J. Sturm, On the Congruence Properties of Modular Forms, "Number Theory," Lecture Notes in Math. **1240** (1984), Springer-Verlag, New York, 1984, pp. 275-280.

Department of Mathematics, University of Wisconsin, Madison, WI 53706
E-mail address: `lovejoy@math.wisc.edu`