THE RESIDUE OF $p(N)$ MODULO SMALL PRIMES

Ken Ono

Dedicated to the memory of Paul Erdös

Abstract. For primes ℓ we obtain a simple formula for $p(N) \pmod{\ell}$ as a weighted sum over ℓ-square affine partitions of N. When $\ell \in \{3, 5, 7, 11\}$ the weights are explicit divisor functions. The Ramanujan congruences modulo 5,7, 11, 25, 49, and 121 follow immediately from these formulae.

On several occasions Professor Erdös asked me whether or not anyone has proved a good theorem regarding the parity of $p(N)$, the unrestricted partition function. Although there are numerous papers on the subject (see for instance [5, 6, 7, 9, 14, 15, 20]), including two of my own, I must confess that little is really known. He was interested in the conjecture [18] that the number of $N \leq X$ for which $p(N)$ is even is $\sim \frac{1}{2}X$, and more generally he was interested in the distribution of $p(N) \pmod{\ell}$ for primes ℓ. The difficulty of such problems appears to be that there is no known good method of computing $p(N) \pmod{\ell}$ apart from mild variations of Euler's recurrence. Here we give an alternate method for computing $p(N) \pmod{\ell}$ which does not depend on recurrences. Perhaps these formulae shed light on these difficult questions.

A partition of N is called a *t-core* if none of the hook numbers of the associated Ferrers-Young diagram are multiples of t, and their number is denoted $C(t, N)$. These partitions are important in the representation theory of permutation groups and finite general linear groups (see [2, 4, 8, 10, 11, 12, 13, 17]). Its generating function is

$$f(t,q) := \sum_{N=0}^{\infty} C(t,N) q^N = \prod_{n=1}^{\infty} \frac{(1-q^{tn})^t}{(1-q^n)}. \tag{1}$$

If ℓ is prime, then a partition $\Lambda = (\lambda_1, \lambda_2, \dots)$ of N is called *ℓ-affine* (also ℓ-ary) if each λ_i is a power of ℓ. Such partitions are important in representation theory, and are

The author is supported by National Science Foundation grants DMS-9304580 and DMS-9508976, and NSA grant MSPR-Y012.

used to compute McKay numbers of certain classical groups (see [11, 12, 13]). Here we will need a subclass of these partitions, the *ℓ-square affine* partitions. A partition Λ is ℓ-square affine if each λ_i is an even power of ℓ.

Throughout this note a_i and n_i will denote non-negative integers, d a positive integer, p a prime, and $\left(\frac{\bullet}{p}\right)$ the Legendre symbol modulo p where $\left(\frac{n}{p}\right) = 0$ if $n \equiv 0 \pmod{p}$. Furthermore we recall that $\eta(z) := q^{1/24}\prod_{n=1}^{\infty}(1-q^n)$ with $q := e^{2\pi i z}$ is Dedekind's weight $1/2$ modular cusp form.

Proposition 1. *If ℓ is prime and $N < \ell^{2s+2}$, then*

$$p(N) \equiv \sum_{a_0+a_1\ell^2+\cdots+a_s\ell^{2s}=N} C(\ell,a_0)C(\ell,a_1)\cdots C(\ell,a_s) \pmod{\ell}.$$

Proof. If k is a non-negative integer, then

$$f(\ell^{k+1},q) = \prod_{n=1}^{\infty}\frac{(1-q^{\ell^k n})^{\ell^k}}{(1-q^n)}\cdot\frac{(1-q^{\ell^{k+1}n})^{\ell^{k+1}}}{(1-q^{\ell^k n})^{\ell^k}} \equiv f(\ell^k,q)\cdot\prod_{n=1}^{\infty}\frac{(1-q^{\ell^{2k+1}n})^{\ell}}{(1-q^{\ell^{2k}n})} \pmod{\ell}$$
$$= f(\ell^k,q)\cdot f(\ell,q^{\ell^{2k}}).$$

Therefore $f(\ell^{k+1},q) \equiv f(\ell,q)\cdot f(\ell,q^{\ell^2})\cdots f(\ell,q^{\ell^{2k}}) \pmod{\ell}$, and so by (1) we obtain

$$\sum_{N=0}^{\infty} C(\ell^{k+1},N)q^N \equiv \prod_{n=1}^{\infty}\frac{(1-q^{\ell^{2k+2}n})}{(1-q^n)}$$
$$\equiv \left(\sum_{N=0}^{\infty} C(\ell,N)q^N\right)\cdot\left(\sum_{N=0}^{\infty} C(\ell,N)q^{\ell^2 N}\right)\cdots\left(\sum_{N=0}^{\infty} C(\ell,N)q^{\ell^{2k}N}\right) \pmod{\ell}. \tag{2}$$

Therefore if $N < \ell^{2k+2}$, then

$$p(N) \equiv \sum_{a_0+a_1\ell^2+\cdots a_k\ell^{2k}=N} C(\ell,a_0)C(\ell,a_1)\cdots C(\ell,a_k) \pmod{\ell}.$$

It is easy to see that the indices consist precisely of the ℓ-square affine partitions of N.

□

The following result was obtained earlier by Hirschhorn in [5].

Theorem 1. *If $N < 4^{s+1}$, then*

$$p(N) \equiv \#\left\{(n_0,n_1,\ldots,n_s) \mid \frac{1}{2}\sum_{i=0}^{s} 4^i(n_i^2+n_i) = N\right\} \pmod{2}.$$

Proof. The result follows from Proposition 1 and the following well known $q-$series identity:

$$\sum_{N=0}^{\infty} C(2,N)q^N = \prod_{n=1}^{\infty} \frac{(1-q^{2n})^2}{(1-q^n)} = \sum_{n=0}^{\infty} q^{\frac{n^2+n}{2}}.$$

□

Theorem 2. *If $N < 9^{s+1}$, then*

$$p(N) \equiv \sum_{a_0+9a_1+\cdots+9^s a_s = N} \sigma_3(a_0)\sigma_3(a_1)\cdots\sigma_3(a_s) \pmod 3,$$

where $\sigma_3(n) := \sum_{d|3n+1} d$.

Proof. The result follows from Proposition 1 and the following Eisenstein series identity [4]:

$$\frac{\eta^3(9z)}{\eta(3z)} = \sum_{N=0}^{\infty} C(3,N)q^{3N+1} = \sum_{n=0}^{\infty} \sum_{d|3n+1} \left(\frac{d}{3}\right) q^{3n+1}.$$

□

Theorem 3. *If $N < 25^{s+1}$, then*

$$p(N) \equiv \sum_{a_0+25a_1+\cdots+25^s a_s = N} \sigma_5(a_0)\sigma_5(a_1)\cdots\sigma_5(a_s) \pmod 5$$

where $\sigma_5(n) := (n+1)\sum_{d|n+1} d$.

Proof. The result follows from Proposition 1 and the identity (see [3,4])

$$\frac{\eta^5(5z)}{\eta(z)} = \sum_{N=0}^{\infty} C(5,N)q^{N+1} = \sum_{n=1}^{\infty} \sum_{d|n} \left(\frac{d}{5}\right) \cdot \frac{n}{d} \cdot q^n.$$

□

Theorem 4. *If $N < 49^{s+1}$, then*

$$p(N) \equiv \sum_{a_0+49a_1+\cdots+49^s a_s = N} \sigma_7(a_0)\sigma_7(a_1)\cdots\sigma_7(a_s) \pmod 7$$

where $\sigma_7(n) := (n+2)\sum_{d|n+2} \left(2d + nd + 6d^3\right)$.

Proof. It is well known that [3]

$$\frac{\eta^7(7z)}{\eta(z)} = \sum_{N=0}^{\infty} C(7,N)q^{N+2} = \frac{1}{8}\sum_{n=1}^{\infty}\sum_{d|n}\left(\frac{d}{7}\right)\cdot\frac{n^2}{d^2}q^n - \frac{1}{8}\eta^3(z)\eta^3(7z).$$

Since $\eta^3(z)\eta^3(7z) \equiv \sum_{n=1}^{\infty}\tau(n)q^n \pmod 7$ where $\tau(n)$ is Ramanujan's tau-function, the result now follows by Proposition 1 and the Lehmer congruence [21]

$$\tau(n) \equiv n\sum_{d|n} d^3 \pmod 7.$$

□

Theorem 5. *If* $N < 121^{s+1}$, *then*

$$p(N) \equiv \sum_{a_0+121a_1+\cdots 121^s+a_s=N} \sigma_{11}(a_0)\sigma_{11}(a_1)\cdots\sigma_{11}(a_s) \pmod{11}$$

where

$$\sigma_{11}(n) := A(n+5) + 3(n+5)\sum_{d|n+5}\left(2d^7 + (n+5)^5d^7 + 7(n+5)^3d\right),$$

and

$$A(m) := \begin{cases} 0 & \text{if } \mathrm{ord}_{11}(m) \geq 1, \\ 0 & \text{if } \mathrm{ord}_p(m) \equiv 1 \pmod 2 \text{ for some } \left(\frac{p}{11}\right) = -1, \\ 3m^2\prod_j(\delta_j+1) & \text{if } m = \prod_{\left(\frac{p_i}{11}\right)=-1} p^{2\delta_i}\prod_{\left(\frac{p_j}{11}\right)=1} p_j^{\delta_j}. \end{cases}$$

Proof. Here $\eta^{11}(11z)/\eta(z)$ is a weight 5 holomorphic modular form with respect to $\Gamma_0(11)$ with Nebentypus character $\left(\frac{-11}{\bullet}\right)$. Define the cusp forms $C_1(z), C_2(z)$ and $C_3(z)$ by

$$C_1(z) := \sum_{n=1}^{\infty}\sum_{d|n}\left(\frac{d}{11}\right)\cdot\frac{n^4}{d^4}\cdot q^n - 1275\frac{\eta^{11}(11z)}{\eta(z)},$$

$C_2(z) := C_1(z)|T_3$, and $C_3(z) := C_1(z)|T_2$. Here T_p is the usual Hecke operator with Nebentypus $\left(\frac{-11}{\bullet}\right)$. The three newforms in $S_5\left(11, \left(\frac{-11}{\bullet}\right)\right)$ are

$$N_1(z) := \sum_{n=1}^{\infty} a(n)q^n = \frac{3}{85}C_1(z) + \frac{1}{85}C_2(z) = q + 7q^3 + 16q^4 - 49q^5 - \cdots,$$

$$N_2(z) := \frac{15-\sqrt{-30}}{1275}\cdot\left(-7C_1(z) + C_2(z) + \frac{\sqrt{-30}}{3}C_3(z)\right) = q + \sqrt{-30}q^2 - 3q^3 - \cdots,$$

$$N_3(z) := \frac{15+\sqrt{-30}}{1275}\cdot\left(-7C_1(z) + C_2(z) - \frac{\sqrt{-30}}{3}C_3(z)\right) = q - \sqrt{-30}q^2 - 3q^3 - \cdots.$$

Furthermore it turns out that

$$\frac{\eta^{11}(11z)}{\eta(z)} = \sum_{N=0}^{\infty} C(11,N)q^{N+5}$$

(3)

$$= \frac{1}{1275}\sum_{n=1}^{\infty}\sum_{d|n}\left(\frac{d}{11}\right)\cdot\frac{n^4}{d^4}\cdot q^n - \frac{1}{150}N_1(z) + \frac{15+\sqrt{-30}}{5100}N_2(z) + \frac{15-\sqrt{-30}}{5100}N_3(z).$$

The forms $N_2(z)$ and $N_3(z)$ are complex conjugates and if $B(z) = \sum_{n=1}^{\infty} b(n)q^n$ is

$$B(z) := \frac{15+\sqrt{-30}}{30}N_2(z) + \frac{15-\sqrt{-30}}{30}N_3(z) = q - 2q^2 - 3q^3 - 14q^4 + \ldots,$$

then using the methods of Sturm and Swinnerton-Dyer [19,21] we obtain

$$b(n) \equiv \left(8n + 4n\left(\frac{n}{11}\right)\right)\sum_{d|n} d^7 \pmod{11}.$$

Therefore by (3) we obtain

$$C(11,N)$$

$$\equiv 3a(N+5) + 3(N+5)\sum_{d|N+5}\left(2d^7 + \left(\frac{N+5}{11}\right)d^7 + 7(N+5)^3\left(\frac{d}{11}\right)d^6\right) \pmod{11}.$$

Completing the proof simply requires formulae for $a(n) \pmod{11}$. Since $N_1(z)$ is a newform it turns out that $a(1) = 1$ and

(4) $$a(n)a(m) = a(nm) \quad \text{if } \gcd(n,m) = 1,$$

(5) $$a(p^{k+1}) = a(p)a(p^k) - \left(\frac{-11}{p}\right)p^4 a(p^{k-1}) \quad \text{if } k \geq 1.$$

The form $N_1(z)$ has complex multiplication by $\mathbb{Q}(\sqrt{-11})$, and we find that for primes p

$$a(p) = \begin{cases} 121 & \text{if } p = 11, \\ 0 & \text{if } p \equiv 2,6,7,8,10 \pmod{11}, \\ \frac{2x^4 - 132x^2y^2 + 242y^4}{16} & \text{if } p \equiv 1,3,4,5,9 \pmod{11} \text{ and } 4p = x^2 + 11y^2. \end{cases}$$

Therefore if $p \equiv 0,2,6,7,8,10 \pmod{11}$, then $a(p) \equiv 0 \pmod{11}$. If $p \equiv 1,3,4,5,9 \pmod{11}$ and $4p = x^2 + 11y^2$, then $a(p) \equiv 7x^4 \pmod{11}$. Since $x^2 \equiv 4p \pmod{11}$, we find that $a(p) \equiv 2p^2 \pmod{11}$. Using (4) and (5) it is now an easy exercise to verify that $A(n) \equiv 3a(n) \pmod{11}$ for every $n > 1$. The result follows from Proposition 1.

□

Corollary 1. *For every non-negative integer n*

$$p(5n+4) \equiv 0 \pmod{5},$$
$$p(7n+5) \equiv 0 \pmod{7},$$
$$p(11n+6) \equiv 0 \pmod{11}.$$

Proof. The congruences modulo 5 and 7 follow from the observation that $(n+1)|\sigma_5(n)$ and $(n+2)|\sigma_7(n)$. The congruence modulo 11 follows from the fact that $\sigma_{11}(n) \equiv A(n+5) \pmod{n+5}$ and $A(n) \equiv 0 \pmod{11}$ if $\mathrm{ord}_{11}(n) \geq 1$.

□

It also turns out that the Ramanujan congruences modulo 25, 49, and 121 follow easily from the proofs of Theorems 3,4 and 5.

Theorem 6. *For every non-negative integer n*

$$p(25n+24) \equiv 0 \pmod{25},$$
$$p(49n+47) \equiv 0 \pmod{49},$$
$$p(121n+116) \equiv 0 \pmod{121}.$$

Proof. If $\ell = 5, 7$, or 11, and $\delta(\ell) := \frac{\ell^2-1}{24}$, then it is easy to verify using the information from the proofs of Theorems 3, 4, and 5 that

$$C(\ell, \ell^2 N - \delta(\ell)) \equiv 0 \pmod{\ell^2} \tag{6}$$

for every positive integer N. Moreover it is easy to see that the above Ramanujan congruences are equivalent to the assertion that

$$C(\ell^2, \ell^2 N - \delta(\ell)) \equiv 0 \pmod{\ell^2} \tag{7}$$

for every positive integer N. Define integers $B(\ell, N)$ by

$$\sum_{N=0}^{\infty} B(\ell, N) q^{\ell N} := \left(\sum_{N=0}^{\infty} C(\ell, N) q^{\ell N} \right)^{\ell}.$$

Since

$$\sum_{N=0}^{\infty} C(\ell^2, N) q^N = \left(\sum_{N=0}^{\infty} C(\ell, N) q^N \right) \cdot \left(\sum_{N=0}^{\infty} B(\ell, N) q^{\ell N} \right),$$

we find that

$$C(\ell^2, \ell^2 N - \delta(\ell)) = \sum_{k \geq 0} C(\ell, \ell^2 N - \delta(\ell) - \ell k) B(\ell, k). \tag{8}$$

Since $C(\ell, \ell^2 N - \delta(\ell) - \ell k) \equiv 0 \pmod{\ell}$, and $B(\ell, k) \equiv 0 \pmod{\ell}$ if $k \not\equiv 0 \pmod{\ell}$, we find that

$$C(\ell^2, \ell^2 N - \delta(\ell)) \equiv \sum_{k \geq 0} C(\ell, \ell^2 N - \delta(\ell) - \ell^2 k) B(\ell, \ell k) \pmod{\ell^2}.$$

However by (6) we obtain the Ramanujan congruences mod 25, 49, and 121.

□

Concluding remarks

There are analogs of these results where ℓ-affine partitions replace ℓ-square affine partitions. I chose to use the ℓ-square affine partitions because the weighted sums involve fewer terms, and the formulae for $3 \leq \ell \leq 11$ only involve divisor sums rather than values of Hecke Grössencharacters. Nevertheless there is some interest in working out formulae for $p(N) \pmod{\ell}$ via ℓ-affine partitions.

Recently there has been a lot of interest in the *method of weighted words* as developed by Alladi and Gordon. These works, some joint with Andrews, lead to combinatorial explanations of identities where two seemingly unrelated partition functions are shown to be equal (see [1]). Here we exhibited $p(N) \pmod{\ell}$ as a *weighted* sum over ℓ-square affine partitions of N where the weights are products of values of the ℓ-core partition function. Perhaps this resonates with the Alladi-Gordon method and can be viewed as an example of a mod ℓ theory.

References

1. K. Alladi, *The method of weighted words and applications to partitions*, Number Theory (Paris, 1992-1993), London Math. Soc. Lect. Notes 215 (1995), 1-36.
2. P. Fong and B. Srinivasan, *The blocks of finite general linear groups and unitary groups*, Invent. Math. **69** (1982), 109-153.
3. F. Garvan, D. Kim and D. Stanton, *Cranks and $t-$cores*, Invent. Math. **101** (1990), 1-17.
4. A. Granville and K. Ono, *Defect zero $p-$blocks for finite simple groups*, Trans. Amer. Math. Soc., **348, 1** (1996), 331-347.
5. M. Hirschhorn, *On the residue mod 2 and mod 4 of $p(n)$*, Acta Arith. **38** (1980), 105-109.
6. ______, *On the parity of $p(n)$ II*, J. Combin. Theory (A) **62** (1993), 128-138.
7. M. Hirschhorn and M. Subbarao, *On the parity of $p(n)$*, Acta Arith. **50 4** (1988), 355-356.
8. G. James and A. Kerber, *The representation theory of the symmetric group*, Addison-Wesley, Reading, 1979.
9. O. Kolberg, *Note on the parity of the partition function*, Math. Scand. **7** (1959), 377-378.

10. A. Klyachko, *Modular forms and representations of symmetric groups, integral lattices and finite linear groups*, Zap. Nauchn. Sem. Leningrad Otdel. Mat. Inst. Steklov **116** (1982).
11. H. Nakamura, *On some generating functions for McKay numbers - prime power divisibilities of the hook products of Young diagrams*, J. Math. Sci., U. Tokyo **1** (1994), 321-337.
12. J. Olsson, *Remarks on symbols, hooks and degrees of unipotent characters*, J. Comb. Th. (A) **42** (1986), 223-238.
13. ———, *Combinatorics and representations of finite groups*, Univ. Essen Lect. Notes 20, 1993.
14. K. Ono, *Parity of the partition function in arithmetic progressions*, J. reine angew. Math. **472** (1996), 1-15.
15. ———, *Odd values of the partition function*, Disc. Math., **169** (1997), 263-268.
16. ———, *On the positivity of the number of partitions that are $t-$cores*, Acta Arith. **66,3** (1994), 221-228.
17. K. Ono and L. Sze, 4-*core partitions and class numbers*, Acta. Arith., **65** (1997), 249-272.
18. T. R. Parkin and D. Shanks, *On the distribution of parity in the partition function*, Math. Comp. **21** (1967), 466-480.
19. J. Sturm, *On the congruence of modular forms*, Springer Lect. Notes **1240** (1984), Springer-Verlag.
20. M. Subbarao, *Some remarks on the partition function*, Amer. Math. Monthly **73** (1966), 851-854.
21. H.P.F. Swinnerton-Dyer, *On ℓ-adic Galois representations and congruences for coefficients of modular forms*, Springer Lect. Notes 350 (1973).

School of Mathematics, Institute for Advanced Study, Princeton, New Jersey 08540
E-mail address: ono@math.ias.edu

Department of Mathematics, Penn State University, University Park, Pennsylvania 16802
E-mail address: ono@math.psu.edu