ELECTRONIC RESEARCH ANNOUNCEMENTS
OF THE AMERICAN MATHEMATICAL SOCIETY
Volume **1**, Issue 1, 1995

PARITY OF THE PARTITION FUNCTION

KEN ONO

(Communicated by Don Zagier)

Abstract. Let $p(n)$ denote the number of partitions of a non-negative integer n. A well-known conjecture asserts that every arithmetic progression contains infinitely many integers M for which $p(M)$ is odd, as well as infinitely many integers N for which $p(N)$ is even (see Subbarao [22]). From the works of various authors, this conjecture has been verified for every arithmetic progression with modulus t when $t = 1, 2, 3, 4, 5, 10, 12, 16$, and 40. Here we announce that there indeed are infinitely many integers N in every arithmetic progression for which $p(N)$ is even; and that there are infinitely many integers M in every arithmetic progression for which $p(M)$ is odd so long as there is at least one such M. In fact if there is such an M, then the smallest such $M \leq 10^{10}t^7$. Using these results and a fair bit of machine computation, we have verified the conjecture for every arithmetic progression with modulus $t \leq 100,000$.

1. Introduction

A partition of a non-negative integer n is a non-increasing sequence of positive integers whose sum is n. Euler's generating function for $p(n)$, the number of partitions of an integer n, is:

$$\sum_{n=0}^{\infty} p(n)q^n = \prod_{n=1}^{\infty} \frac{1}{1-q^n}. \tag{1}$$

Ramanujan discovered various surprising congruences for $p(n)$ when n is in certain special arithmetic progressions; for example:

$$p(5n+4) \equiv 0 \mod 5,$$

$$p(7n+5) \equiv 0 \mod 7,$$

and

$$p(11n+6) \equiv 0 \mod 11.$$

There are now many proofs of these congruences (and their generalizations) in the literature (see [1, 2, 3, 4, 5, 6, 7, 11, 12, 23] for instance). Surprisingly there do

Received by the editors February 28, 1995, and, in revised form, May 3, 1995.
1991 *Mathematics Subject Classification.* Primary 05A17; Secondary 11P83.
Key words and phrases. Parity conjecture, partitions, modular forms.
The author is supported by NSF grant DMS-9508976.

not seem to be any such congruences modulo 2 or 3. In fact the parity of $p(n)$ seems to be quite random, and it is believed that the partition function is 'equally often' even and odd; that is, that $p(n)$ is even for $\sim \frac{1}{2}x$ positive integers $n \le x$ (see Parkin and Shanks [19]).

In [22] Subbarao made the following conjecture on the parity of $p(n)$, for those integers n belonging to any given arithmetic progression:

Conjecture. *For any arithmetic progression $r \pmod{t}$, there are infinitely many integers $M \equiv r \pmod{t}$ for which $p(M)$ is odd, and there are infinitely many integers $N \equiv r \pmod{t}$ for which $p(N)$ is even.*

From the works of Garvan, Kolberg, Hirschhorn, Stanton, and Subbarao (see [6, 9, 10, 13, 16, 22],), this conjecture has been proved for every arithmetic progression with modulus t when $t = 1, 2, 3, 4, 5, 10, 12, 16$ and 40.

Using very different methods, we go some way towards a proof of the conjecture. Using the theory of modular forms, we announce:

Main Theorem 1. *For any arithmetic progression $r \pmod{t}$, there are infinitely many integers $N \equiv r \pmod{t}$ for which $p(N)$ is even.*

Main Theorem 2. *For any arithmetic progression $r \pmod{t}$, there are infinitely many integers $M \equiv r \pmod{t}$ for which $p(M)$ is odd, provided there is one such M. Furthermore, if there does exist an $M \equiv r \pmod{t}$ for which $p(M)$ is odd, then the smallest such M is less than $C_{r,t}$, where*

$$C_{r,t} := \frac{2^{23}A \cdot 3^7 t^6}{d^2} \prod_{p \mid 6t} \left(1 - \frac{1}{p^2}\right) - A,$$

with $d := \gcd(24r - 1, t)$ and $A > \frac{t}{24}$ is a power of 2.

From the two theorems we obtain an algorithm to determine the truth of our parity conjecture for any given arithmetic progression $r \pmod{t}$: Compute $p(N) \pmod{2}$ for $N = r, r + t, r + 2t, \ldots$ for all such N up to $C_{r,t}$. As soon as we find one odd number we have verified the conjecture. If all these numbers are even then we have proved that the conjecture is false.

Ken Burrell (Universal Analytics, Inc.) ran an efficient version of this algorithm on a CRAY C-90, giving the following result:

Main Corollary. *For all $0 \le r < t \le 10^5$, there are infinitely many integers $M \equiv r \pmod{t}$ for which $p(M)$ is odd.*

2. The main ideas

First we briefly recall essential preliminaries concerning modular forms. For more on the theory of modular forms see [15].

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ act on $\mathfrak{H}$, the upper half of the complex plane, by the linear fractional transformation $Az = \frac{az+b}{cz+d}$. If N is a positive integer, then we define the following *congruence subgroups* of $SL_2(\mathbb{Z})$ of *level* N:

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc = 1,\ c \equiv 0 \mod N \right\}.$$

and

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \ ad - bc = 1, \ a \equiv d \equiv 1 \mod N, \text{ and } c \equiv 0 \mod N \right\}.$$

A meromorphic function $f(z)$ on $\mathfrak{H}$ is called a *modular function* with positive integer weight k with respect to congruence subgroup Γ if

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

for all $z \in \mathfrak{H}$ and all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. If $f(z)$ is holomorphic on $\mathfrak{H}$ and at the cusps of Γ (i.e. the rationals), then $f(z)$ is known as a *modular form* of weight k with respect to Γ. If $f(z)$ vanishes at the cusps of Γ, then $f(z)$ is known as a *cusp form.*

We denote the finite dimensional space of modular forms (resp. cusp forms) of weight k with respect to $\Gamma_1(N)$ by $M_k(N)$ (resp. $S_k(N)$). In the variable $q = e^{2\pi i z}$, a holomorphic modular form $f(z) \in M_k(N)$ admits a Fourier expansion of the form

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

Of particular interest are certain modular forms in $M_k(N)$ with nice modular transformation properties with respect to $\Gamma_0(N)$. If χ is a Dirichlet character mod N, then we say that a form $f(z) \in M_k(N)$ (resp. $S_k(N)$) is modular form of weight k with Nebentypus character χ if

$$f\left(\frac{az+b}{cz+d}\right) = \chi(d)(cz+d)^k f(z)$$

for all $z \in \mathfrak{H}$ and all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$. The space of such modular forms (resp. cusp forms) is denoted by $M_k(N,\chi)$ (resp. $S_k(N,\chi)$).

The Dedekind eta-function is the principal modular form of interest in this paper; it is defined by the infinite product

$$\eta(z) := q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 - q^n).$$

A function $f(z)$ is called an *eta-product* if it is expressible as a finite product of the form

$$f(z) = \prod_{\delta \mid N} \eta^{r_\delta}(\delta z)$$

where N and each r_δ is an integer. Probably the most famous of all eta-products is Ramanujan's $\Delta-$function, defined by $\Delta(z) := \eta^{24}(z) = q \prod_{n=1}^{\infty}(1-q^n)^{24}$. This is the unique normalized weight 12 cusp form on $SL_2(\mathbb{Z})$. More generally, Gordon, Hughes, and Newman (see [8,17,18]) examined the general *modular* properties of eta-products.

We construct modular forms that are eta-products whose Fourier expansions modulo 2 are determined by the values of $p(n)$ modulo 2.

Proposition 1. *For a given positive integer t, let $A > \frac{t}{24}$ be a power of 2. Define $f_{t,A}(z)$ by*

$$f_{t,A}(z) := \frac{\eta(24z)}{\eta(48z)}\Delta^A(24tz) = \sum_{n\geq 1} a_t(n)q^{24n-1}.$$

Then $f_{t,A}(z)$ is a cusp form in $S_{12A}(1152t, \left(\frac{2}{d}\right))$. Moreover the Fourier expansion of $f_{t,A}(z) \mod 2$ can be factored as:

$$(2) \quad f_{t,A}(z) = \sum_{n=0}^{\infty} a_t(n)q^{24n-1} \equiv \left(\sum_{n=0}^{\infty} p(n)q^{24n-1}\right)\left(\sum_{n=0}^{\infty} q^{24At(2n+1)^2}\right) \mod 2.$$

Proof. Using the well known properties of the Dedekind eta-function, it is relatively straightforward to deduce that $f_{t,A}(z)$ is a modular form of weight $12A$. It is also straightforward to deduce that $f_{t,A}(z)$ is a cusp form.

The essential feature of the cusp form $f_{t,A}(z)$ is the convenient fact that $f_{t,A}(z)$ is *essentially* the product of the generating function for $p(n)$ and a theta function $\mod 2$.

Since $\frac{1}{1-X^n} = \frac{1+X^n}{1-X^{2n}} \equiv \frac{1-X^n}{1-X^{2n}} \mod 2$, it follows that

$$\sum_{n=0}^{\infty} p(n)q^n \equiv \prod_{n=1}^{\infty} \frac{1-q^n}{1-q^{2n}} \mod 2.$$

In terms of the eta-functions, we find that

$$(3) \qquad \frac{\eta(24z)}{\eta(48z)} = \frac{1}{q}\prod_{n=1}^{\infty}\frac{1-q^{24n}}{1-q^{48n}} \equiv \sum_{n=0}^{\infty} p(n)q^{24n-1} \mod 2.$$

The following infinite product identity was proved by Jacobi:

$$\frac{\eta^2(16z)}{\eta(8z)} = q\prod_{n=1}^{\infty}\frac{(1-q^{16n})^2}{(1-q^{8n})} = \sum_{n=0}^{\infty} q^{(2n+1)^2}.$$

Therefore since $(1-X)^2 \equiv (1-X^2) \mod 2$, we find that

(4)

$$\Delta(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = q\prod_{n=1}^{\infty}\frac{(1-q^n)^{32}}{(1-q^n)^8} \equiv q\prod_{n=1}^{\infty}\frac{(1-q^{16n})^2}{(1-q^{8n})} \equiv \sum_{n=0}^{\infty} q^{(2n+1)^2} \mod 2.$$

The factorization of $f_{t,A}(z)$ now follows easily from (3) and (4). □

Serre [20] proved the following remarkable theorem regarding the divisibility of Fourier coefficients of holomorphic integer weight modular forms.

Theorem. (Serre) *Let $f(z)$ be a holomorphic modular form of positive integer weight k on some congruence subgroup of $SL_2(\mathbb{Z})$ with Fourier expansion*

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

where $a(n)$ are algebraic integers in some number field. If m is a positive integer, then there exists a positive constant α such that the set of integers $n \leq x$ for which $a(n)$ is not divisible by m has cardinality $\ll \frac{x}{\log^\alpha x}$.

With this theorem we obtain

Main Theorem 1. *For any arithmetic progression $r \pmod t$, there are infinitely many integers $N \equiv r \pmod t$ for which $p(N)$ is even.*

Proof. Comparing coefficients in (2), it is easy to deduce that

$$a_t(Atk^2+n) \equiv \sum_{i\geq 1,\ i \text{ odd}} p(At(k^2-i^2)+n) \mod 2. \tag{5}$$

Now suppose every $N \geq n_0$ for which $N \equiv r \pmod t$ has the property that $p(N)$ is odd. If $k \equiv 1 \mod 4$, then every integer $n \equiv r \pmod t$ in the interval $[Atk^2+n_0, At(k+2)^2+r-t]$ has the property that $a_t(n)$ is odd since there are $\frac{k+1}{2}$ many odd summands in (5). After combining all such intervals, we find a set of positive integers with positive density for which $a_t(n) \not\equiv 0 \mod 2$. This would contradict Serre's theorem. □

Now we need to establish that there are infinitely many $M \equiv r \pmod t$ where $p(M)$ is odd provided that there is at least one M. To do this we first deduce a technical lemma about the reduction modulo m of the Fourier expansions of holomorphic modular forms. Main Theorem 2 follows as a consequence, for if there were only finitely many $M \equiv r \pmod t$ for which $p(M)$ is odd, then the reduction $\mod 2$ of the relevant modular form contradicts the lemma.

For a given positive integer m and formal power series $f := \sum_{n\in\mathbb{Z}} a(n)q^n$ with algebraic integer coefficients, we define $\mathrm{Ord}_m(f)$ to be the smallest integer n for which $a(n)$ is not divisible by m. A special case of a theorem of Sturm [21] allows us to computationally determine whether m divides $a(n)$ for every integer n (that is, to determine whether $\mathrm{Ord}_m(f) = \infty$).

If $f(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_k(N)$ for some positive integer N with algebraic integer Fourier coefficients from a fixed number field and m is a positive integer, then Sturm proved that if

$$\mathrm{Ord}_m(f) > \frac{k}{12} N^2 \prod_{p|N} (1-\frac{1}{p^2}),$$

then $\mathrm{Ord}_m(f) = \infty$ (i.e. $a(n) \equiv 0 \mod m$ for all n). Now we prove the essential lemma about the reduction of a holomorphic modular form $\mod m$.

Lemma 1. *Let $f(z) = \sum_{n=0}^{\infty} a(n)q^n$ where the coefficients $a(n)$ are algebraic integers in some number field. Let s and w be positive integers and $b_1, b_2, \dots b_s$ distinct non-zero integers. If m is a positive integer and*

$$f(z) \equiv \sum_{1\leq i\leq s} \sum_{n=0}^{\infty} a_i(n) q^{wn^2+b_i} \mod m$$

where $a_i(n) \not\equiv 0 \mod m$ for infinitely many $n \geq 0$, then $f(z)$ is not in $M_k(N)$ for any pair of positive integers k, and N.

Proof. Suppose that $f \in M_k(N)$ for some k and N. If $p \equiv 1 \pmod N$ is prime, then the image of f under the Hecke operator T_p satisfies

$$\begin{aligned} f(z)|T_p &= \sum_{n\geq 0} (a(pn) + p^{k-1}a(n/p))\, q^n \\ &\equiv \sum_{\substack{i,n \\ p|wn^2+b_i}} a_i(n)\, q^{(wn^2+b_i)/p} + p^{k-1} \sum_{i,n} a_i(n)\, q^{(wn^2+b_i)p} \qquad \pmod m, \end{aligned} \tag{6}$$

and $f|T_p$ again belongs to $M_k(N)$. We claim that $\mathrm{Ord}_m(f|T_p) < \infty$ for every sufficiently large prime p and $\mathrm{Ord}_m(f|T_p) > C$ for almost every p, for any given constant C. Taking $C = \frac{kN^2}{12}\prod_{l|N}(1-l^{-2})$ gives a contradiction to Sturm's theorem.

To see that $\mathrm{Ord}_m(f|T_p) < \infty$, we observe that only finitely many of the infinitely many exponents on the right-hand side of (6) can coincide, so that the expression cannot vanish identically modulo m. Indeed, if $(wn^2+b_i)p^{\pm 1} = (wl^2+b_j)p^{\pm 1}$ for some $n \neq l$, then $w(n+l)(n-l) = b_j - b_i$ implies that both n and l are bounded, while if $(wn^2+b_i)p = (wl^2+b_j)p^{-1}$ then $w(pn+l)(pn-l) = b_j - p^2 b_i$ gives the same conclusion if no b_j is divisible by p^2.

For the reverse direction, we observe that if $C < p < x$ and $\mathrm{Ord}_m(f|T_p) = h < C$, then we must have $h = (wn^2+b_i)/p$ for some n and i and that this n is then bounded by $\sqrt{Cx - b_i}$. Since each triple (n,i,h) gives at most one prime $p = (wn^2+b_i)/h$ and the number of i's and h's is bounded, this shows that for $x \to \infty$ there are $\mathrm{O}(\sqrt{x})$ primes $p < x$ and congruent to 1 modulo N with $\mathrm{Ord}_m(f|T_p) < C$, and this proves the claim since the total number of primes $< x$ in this congruence class is $\gg x/\log x$ by Dirichlet's theorem.

□

The following lemma follows from the standard fact that if $f(z) \in M_k(N)$, then $f\left(z+\frac{s}{t}\right) \in M_k(Nt^2)$.

Lemma 2. *Let $f(z) = \sum_{n=0}^{\infty} a(n)q^n$ be a modular form in $M_k(N,\chi)$ and let $d :=$* $\gcd(r,t)$. *Then*

$$f_{r,t}(z) = \sum_{n\equiv r \mod t} a(n)q^n$$

is the Fourier expansion of a modular form in $M_k\left(\frac{Nt^2}{d}\right)$.

We now combine these facts to establish the main theorem of this section.

Main Theorem 2. *For any arithmetic progression $r \pmod t$, there are infinitely many integers $M \equiv r \pmod t$ for which $p(M)$ is odd, provided there is one such M. Furthermore, if there does exist an $M \equiv r \pmod t$ for which $p(M)$ is odd, then the smallest such M is less than $C_{r,t}$. where*

$$C_{r,t} := \frac{2^{23}A\cdot 3^7 t^6}{d^2}\prod_{p|6t}\left(1-\frac{1}{p^2}\right) - A.$$

where $d := \gcd(24r-1,t)$ and $A > \frac{t}{24}$ is a power of 2.

Proof. Recall from Proposition 1 that

$$f_{t,A}(z) := \frac{\eta(24z)}{\eta(48z)}\Delta^A(24tz) = \sum_{n\geq 1} a_t(n)q^{24n-1} \in S_{12A}(1152t,\chi).$$

and

$$f_{t,A}(z) \equiv \sum_{n=0}^{\infty} p(n)q^{24n-1}\sum_{n=0}^{\infty} q^{24At(2n+1)^2} \mod 2.$$

Let $d := \gcd(24r-1, t)$. Therefore by Lemma 2 we define

$$f_{24r-1,24t}(z) = \sum_{n \equiv 24r-1 \mod 24t} a_t(n)q^n \in S_{12A}\left(\frac{2^{13} \cdot 3^4 t^3}{d}\right),$$

which when reduced $\mod 2$ is:

$$f_{24r-1,24t}(z) \equiv \sum_{n \equiv r \mod t} p(n)q^{24n-1} \sum_{n=0}^{\infty} q^{24At(2n+1)^2} \mod 2.$$

Note that the arithmetic progression $r \mod t$ corresponds to the arithmetic progression $24r-1 \mod 24t$. If $p(M)$ is odd for at least one $M \equiv r \pmod t$ but only finitely many, then the $\mod 2$ factorization above contradicts Lemma 1. This proves that if $p(M)$ is odd for at least one $M \equiv r \pmod t$, then $p(M)$ is odd for infinitely many such M.

The computation of the constant $C_{r,t}$ follows easily from the bound in Sturm's theorem.

□

This theorem then proves that if $0 \leq r < t$, and if $p(M)$ is ever odd for an $M \equiv r \pmod t$ (hence infinitely often), then the first odd value must occur where $M < C_{r,t}$. It is easy to verify that $C_{r,t} < 10^{10}t^7$ since $\frac{t}{12} > 2^j$ when we choose the minimal j such that $2^j > \frac{t}{24}$. As a consequence of the two main theorems we find that the conjecture holds for an arithmetic progression $r \pmod t$ provided there is at least one $N \equiv r \mod t$ for which $p(N)$ is odd. By computing $p(n) \mod 2$ for all $n \leq 5,000,000$ we found that every arithmetic progression with modulus $t \leq 100,000$ contains an integer M for which $p(M)$ is odd. Therefore we obtain:

Main Corollary. *For all* $0 \leq r < t \leq 10^5$, *there are infinitely many integers* $M \equiv r \pmod t$ *for which* $p(M)$ *is odd.*

3. Acknowledgements

I am indebted Ken T. Burrell (Universal Analytics, Inc.) whose computations are the content of the Main Corollary. The computations were completed on a CRAY C-90 at the San Diego Supercomputing Center. I am indebted to Andrew Granville for his advice regarding this research. I also thank the referee whose comments improved the paper in many ways. In particular, the proof of Lemma 1 is an improved version of the original proof as suggested by the referee.

References

1. G. Andrews, *The Theory of Partitions*, Addison-Wesley, 1976.
2. G. Andrews and F. Garvan, *Dyson's crank of a partition*, Bull. Am. Math. Soc. **18** (1988), 167-171.
3. A.O.L. Atkin, *Proof of a conjecture of Ramanujan*, Glasgow Math. J. **8** (1967), 14-32.
4. F. Garvan, *A simple proof of Watson's partition congruence for powers of 7*, J. Australian Math. Soc. (A) **36** (1984), 316-334.
5. F. Garvan, *New combinatorial interpretations of Ramanujan's partition congruences* mod *5, 7 and* 11, Trans. Am. Math. Soc. **305** (1988), 47-77.
6. F. Garvan and D. Stanton, *Sieved partition functions and q−binomial coefficients*, Math. Comp. **55** **191** (1990), 299-311.

7. F. Garvan and D. Stanton, *Cranks and $t-$cores*, Invent. Math. **101** (1990), 1-17.
8. B. Gordon and K. Hughes, *Multiplicative properties of $\eta-$products II*, A tribute to Emil Grosswald: Number Theory and related analysis, Cont. Math. **143** (1993), Amer. Math. Soc., 415-430.
9. M. Hirschhorn, *On the residue mod 2 and mod 4 of $p(n)$*, Acta Arithmetica **38** (1980), 105-109.
10. ______, *On the parity of $p(n)$ II*, J. Combin. Theory (A) **62** (1993), 128-138.
11. ______, *Ramanujan's partition congruences*, Discrete Math. **131** (1994), 351-355.
12. M. Hirschhorn and D.C. Hunt, *A simple proof of the Ramanujan conjecture for powers of* 5, J. Reine Angew. Math. **336** (1981), 1-17.
13. M. Hirschhorn and M. Subbarao, *On the parity of $p(n)$*, Acta Arith. **50** **4** (1988), 355-356.
14. M. Knopp, *Modular functions in analytic number theory*, Markham, 1970.
15. N. Koblitz, *Introduction to elliptic curves and modular forms*, Springer-Verlag, 1984.
16. O. Kolberg, *Note on the parity of the partition function*, Math. Scand. **7** (1959), 377-378.
17. M. Newman, *Construction and application of a certain class of modular functions*, Proc. London Math. Soc. (3) **7** (1956), 334-350.
18. M. Newman, *Construction and application of a certain class of modular functions II*, Proc. London Math. Soc. (3) **9** (1959), 373-387.
19. T. R. Parkin and D. Shanks, *On the distribution of parity in the partition function*, Math. Comp. **21** (1967), 466-480.
20. J.-P. Serre, *Divisibilité des coefficients des formes modulaires de poids entier*, C.R. Acad. Sci. Paris (A) **279** (1974), 679-682.
21. J. Sturm, *On the congruence of modular forms*, Springer Lect. Notes **1240** (1984), Springer-Verlag.
22. M. Subbarao, *Some remarks on the partition function*, Amer. Math. Monthly **73** (1966), 851-854.
23. G.N. Watson, *Ramanujan's Vermutung über Zerfällungsanzahlen*, J. Reine Angew. Math. vol 179 (1938), 97-128.

Department of Mathematics, The University of Illinois, Urbana, Illinois 61801
E-mail address: ono@symcom.math.uiuc.edu