Internat. J. Math. & Math. Sci.
Vol. 23, No. 7 (2000) 493–496
S0161171200002829

ON CONGRUENCE PROPERTIES OF THE PARTITION FUNCTION

JAYCE GETZ

(Received 1 March 1999)

ABSTRACT. Some congruence properties of the partition function are proved.

Keywords and phrases. Partition function and congruences.

2000 Mathematics Subject Classification. Primary 11P83.

1. Introduction and statement of results. A partition of n is defined to be a non-increasing set of positive integers whose sum is n. The unrestricted partition function, or $p(n)$, is defined to be the number of partitions of n.

EXAMPLE 1.1. The partitions of 3 are 3, 2+1, 1+1+1, and so

$$p(3) = 3. \tag{1.1}$$

This function has been of interest since *S*. Ramanujan first studied it 80 years ago. He proved that for any non-negative integer n that

$$\begin{aligned} p(5n+4) &\equiv 0 \pmod 5, \\ p(7n+5) &\equiv 0 \pmod 7, \\ p(11n+6) &\equiv 0 \pmod{11}. \end{aligned} \tag{1.2}$$

If one were to examine in any detail the values of $p(n)$ for any set of n, it would become obvious that these congruences are unexpected and rare. In fact, K. Ono has begun the process of quantifying their rarity (see [4] and [3]).

The first to show that there are infinitely many even and odd values of the partition function was Kolberg [1]. However, other conjectures exist regarding the parity of the partition function.

CONJECTURE 1.2 [5]**.** *In every arithmetic progression* $r \pmod t$ *there are infinitely many integers* $N \equiv r \pmod t$ *for which* $p(N)$ *is even, and there are infinitely many integers* $M \equiv r \pmod t$ *for which* $p(M)$ *is odd.*

In [3], Ono went some way towards resolving Subbarao's conjecture.

THEOREM 1.3. *For any arithmetic progression* $r \pmod t$ *there are infinitely many integers* $N \equiv r \pmod t$ *for which* $p(N)$ *is even.*

THEOREM 1.4. *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.

As is seen in Theorem 1.4, the odd case of Subbarao's conjecture remains open.

The first result we obtain in this paper is the following theorem. This theorem provides us, for the first time, with an explicit infinite set of non-trivial cases of Subbarao's conjecture in the odd case.

Theorem 1.5. *For all primes $l > 3$, in any progression $kl \pmod{l^n}$, where $0 \leq k \leq l^{n-1}-1$ and n is any positive integer, there are infinitely many $M \equiv kl \pmod{l^n}$ where $p(M)$ is odd.*

However, we are interested in more than just the parity of the partition function. As shown in [4], congruences like Ramanujan's are indeed rare, but there are few concrete results that detail precise infinite families of progressions that do not possess similar congruence properties. Our next result, the following theorem, gives us an example of such a family of progressions.

Theorem 1.6. *For all primes $l > 3$ in any progression $kl \pmod{l^{n-1}}$, where $0 \leq k \leq l^n - 1$ and n is any positive integer, there are infinitely many $M \equiv kl \pmod{l^n}$ where $p(M)$ is not congruent to $0 \pmod{l}$.*

Example 1.7. In order to illustrate the conclusions of Theorems 1.5 and 1.6, let $l = 5$ and $n = 3$. Now let r be any of the numbers $0, 5, 10, 15, 20, \ldots, 120$. By Theorem 1.5, we know that there are infinitely many non-negative integers n for which $p(125n+r)$ is odd. By Theorem 1.6, there are infinitely many non-negative integers n for which $p(125n+r)$ is not divisible by 5.

2. Proof of Theorems 1.5 and 1.6. Before we begin the discussion of the two main theorems of this paper, we must present the following three theorems that will be used in their proofs. First it is necessary to discuss Hensel's lemma [2].

Hensel's Lemma. *Suppose $f(x)$ is a polynomial with integral coefficients. If there is an integer a and a prime p such that $f(a) \equiv 0 \pmod{p^j}$ and $f'(a)$ is not congruent to $0 \pmod{p}$, then there is a unique $t \pmod{p}$ such that $f(a+tp^j) \equiv 0 \pmod{p^{j+1}}$.*

This theorem allows us to establish the solvability of a congruence $\pmod{p^{j+1}}$ by its solvability $\pmod{p^j}$.

In [4], Ono proves the following two theorems.

Theorem 2.1. *Let $0 \leq r < t$ be integers for which $\gcd(24r-1, t) = 1$. If an integer n exists such that $n \equiv r \pmod{t}$ for which $p(n)$ is odd, then for every integer s coprime to $24t$ there are infinitely many $M \equiv s^2(r-24^{-1})+24^{-1} \pmod{t}$ for which $p(M)$ is odd.*

Theorem 2.2. *Let $0 \leq r < t$ be integers for which $\gcd(24r-1, t) = 1$ and let l be an odd prime. If an integer n exists such that $n \equiv r \bmod t$ for which $p(n)$ is not congruent to $0 \pmod{l}$ then for every integer s coprime to $24t$ there exists infinitely many $M \equiv s^2(r-24^{-1})+24^{-1} \pmod{t}$ for which $p(M)$ is not congruent to $0 \pmod{l}$.*

These theorems relate directly to the question of the parity and congruences of the partition function. As explained in the preceding section, it is known that there are infinitely many integers $n \equiv r \pmod{t}$ where $p(n)$ is even and infinitely many $n \equiv r \pmod{t}$ for which $p(n)$ is odd, providing that there is at least one such n. Theorem 1.5 allows us to determine some cases where such an odd $p(n)$ exists.

Proof of Theorem 1.5. In Theorem 2.1, first note that $p(0) = 1$. Let $n, r = 0$ and let $t = l^n$. Then for any l^n, $\gcd(-1, t) = 1$, so the first condition is fulfilled. Now, we know that for every s coprime to $24t$, there exists infinitely many $M \equiv s^2(r - 24^{-1}) + 24^{-1} \pmod{t}$ for which M is odd. Substituting values, we see that there exists infinitely many $M \equiv -24^{-1}(s^2 - 1) \pmod{l^n}$ for s coprime to $24l^n$. To prove the trivial case of $k = 0$, take $s = 1$. The proof for the other cases is more complicated. Our goal is to prove that for s coprime to $24l^n$, $-24^{-1}(s^2 - 1)$ covers the values $1l, 2l, \ldots, (l^{n-1} - 1)l$.

The first step in this process is to eliminate the -24^{-1} coefficient. Multiply the congruence by -24. We obtain $s^2 - 1 \equiv -24kl \pmod{l^n}$. Since $-24kl$ is still a multiple of l, the question is now reduced to whether or not we can find s coprime to $24l^n$ such that $s^2 - 1 \equiv kl \pmod{l^n}$ for all k and n.

There are two different methods of proving that this congruence is solvable. First, we use a constructive method. Take the congruence $s^2 - 1 \equiv kl \pmod{l}$, or equivalently, $s^2 - 1 - kl \equiv 0 \pmod{l}$. The solutions s to this congruence are of the form $ml \pm 1$.

If we input $ml + 1$ into the congruence $\pmod{l^2}$ we find another solution.

$$\begin{aligned} (ml+1)^2 - 1 - kl &\equiv 0 \pmod{l^2}, \\ m^2l^2 + 2ml + 1 - 1 - kl &\equiv 0 \pmod{l^2}, \\ (2m - k)l &\equiv 0 \pmod{l^2}. \end{aligned} \tag{2.1}$$

We can pick m so that $ml + 1$ is coprime to $24t$. In fact, it is easy to see that

$$m \equiv \frac{k}{2} \pmod{l}. \tag{2.2}$$

If we input $(ml^2 + (kl/2) + 1) = s$ into the congruence

$$s^2 - 1 - kl \equiv 0 \pmod{l^3}, \tag{2.3}$$

we obtain

$$\left(ml^2 + \frac{kl}{2} + 1\right)^2 - 1 - kl \equiv \left(2m + \frac{k^2}{4}\right)l^2 \equiv 0 \pmod{l^3}. \tag{2.4}$$

Therefore, by letting $m = (-k^2/8) \pmod{l}$ we obtain a solution to the congruence.

This process can be repeated, and therefore tells us that the congruence is always solvable for each n. □

Remark 2.3. In an alternate proof, we can use Hensel's lemma to reduce the question of this congruence's solvability to the solvability of $s^2 - 1 - kl \equiv 0 \bmod l$. By taking $s = \pm 1$, this congruence can be solved in all cases. Note also that for $s = \pm 1$, $\gcd(s, 24l^n) = 1$. The derivative of $s^2 - 1 - kl$ is equal to $2s$, which is not congruent to $0 \pmod{l}$.

Suppose there is a solution to $s^2 - 1 - kl \equiv 0 \pmod{l^n}$. As before, since $f' = 2s$ which is not congruent to $0 \pmod{l}$, Hensel's lemma tells us that there is a set of s that are solutions to the congruence $\pmod{l^{n+1}}$. By induction, this gives us another proof of Theorem 1.5.

A similar method can be used to prove Theorem 1.6.

PROOF OF THEOREM 1.6. In Theorem 2.2, let $r, n = 0$. Since $\gcd(-1, t) = 1$ and $p(0) = 1$ is not congruent to 0 $(\mathrm{mod}\, l)$ we know that there are infinitely many $M \equiv s^2(r - 24^{-1}) + 24^{-1} \pmod{t}$ such that M is not congruent to 0 $(\mathrm{mod}\, l)$. From the proof of Theorem 1.5, we know that if we let $t = l^n$, $s^2(r - 24^{-1}) + 24^{-1}$ covers the values kl where $0 \le k \le l^{n-1} - 1$, so the theorem is proved. □

ACKNOWLEDGEMENTS. I would like to thank K. Ono at Pennsylvania State University for suggesting this project and for his continued aid in helping me decipher the language and concepts of number theory. I would also like to thank J. Harkins, the teacher of my Junior class advanced problems in science course, for suggesting a number theory project and helping me to make the right contacts to support me in this endeavor.

REFERENCES

[1] O. Kolberg, *Note on the parity of the partition function*, Math. Scand. **7** (1959), 377–378. MR 22#7995. Zbl 091.04402.

[2] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*, John Wiley & Sons Inc., New York, 1991. MR 91i:11001. Zbl 742.11001.

[3] K. Ono, *Parity of the partition function in arithmetic progressions*, J. Reine Angew. Math. **472** (1996), 1–15. MR 97e:11131. Zbl 835.11038.

[4] ———, *The partition function in arithmetic progressions*, Math. Ann. **312** (1998), no. 2, 251–260. CMP 1 671 788. Zbl 914.11054.

[5] M. V. Subbarao, *Some remarks on the partition function*, Amer. Math. Monthly **73** (1966), 851–854. MR 34#1293. Zbl 173.01803.

GETZ: BIG SKY HIGH SCHOOL, 3100 SOUTH AVENUE WEST MISSOULA, MONTANA 59804, USA
E-mail address: getz@bigsky.net