RAMANUJAN'S METHOD IN q-SERIES CONGRUENCES

BY

George E. Andrews[1] and Ranjan Roy

Written in honor of Herb Wilf's 65^{th} birthday

Abstract. We show that the method developed by Ramanujan to prove $5|p(5n+4)$ and $7|p(7n+5)$ may, in fact, be extended to a wide variety of q-series and products including some with free parameters.

1. Introduction.

Ramanujan [11] is the discoverer of the surprising fact that the partition function, $p(n)$, satisfies numerous congruences. Among the infinite family of such congruences, the two simplest examples are

$$p(5n+4) \equiv 0 \pmod 5 \tag{1.1}$$

and

$$p(7n+5) \equiv 0 \pmod 7. \tag{1.2}$$

Ramanujan used an ingenious and elementary argument to prove these congruences which relied on Jacobi's famous formula [10; last eqn. p.5]:

$$(q;q)_\infty^3 = \prod_{n=1}^{\infty}(1-q^n)^3 = \sum_{j=0}^{\infty}(-1)^j(2j+1)q^{j(j+1)/2}, \tag{1.3}$$

where

$$(A)_N = (A;q)_N = \prod_{j=0}^{N-1}(1-Aq^j). \tag{1.4}$$

[1] Partially supported by National Science Foundation Grant DMS-8702695-04

A rather more general result of this nature was proved in [3; p. 27, Th. 10.1] to account for certain congruences connected with generalized Frobenius partitions.

Indeed J. M. Gandhi [7], [8], [9], J. Ewell [5], L. Winquist [12] and many others (cf., Gupta [10; Sec. 6.3]) have proved partition function congruences based on this idea. In all these theorems, the underlying generating functions were either modular forms or simple linear combinations thereof.

The point of this paper is to show that Ramanujan's original method is applicable to an infinite number of congruence theorems including many non-modular functions defined by q-series.

Our main result is:

Theorem 1. *Suppose p is a prime > 3, and $0 < a < p$ and b are integers. Also, $-a$ must be a quadratic nonresidue mod p. Suppose $\{\alpha_n\}_{n=-\infty}^{\infty} = \{\alpha_n(z_1, z_2, \dots, z_j)\}$ is a doubly infinite sequence of Laurent polynomials over $\mathbb{Z}$ with variables $z_1, \dots, z_j$ independent of q. Then there is an integer c such that the coefficient of $z_1^{m_1} z_2^{m_2} \cdots z_j^{m_j}$ q^{pN} in*

$$\frac{q^c \sum_{n=-\infty}^{\infty} \alpha_n q^{a\binom{n}{2}+bn}}{(q;q)_\infty^{p-3}} \tag{1.5}$$

is divisible by p. For each integer m, we shall denote by $\overline{m}$ the multiplicative inverse of m mod p. The integer $c = c_p(a,b)$ may be chosen as the least nonnegative integer congruent to $\bar{8}(a(2b\bar{a}-1)^2+1)$ mod p.

In Section 2, we shall prove this result. In Section 3, we examine the implications of Theorem 1 for a variety of modular forms. In Section 4, we collect a number of congruences for the coefficients in several q-series.

2. The Proof of Theorem 1.

With the various hypotheses of the theorem, we note that

$$(2.1) \qquad \frac{q^c \sum_{n=-\infty}^{\infty} \alpha_n q^{a\binom{n}{2}+bn}}{(q;q)_\infty^{p-3}}$$

$$= \frac{q^c \sum_{n=-\infty}^{\infty} \sum_{j=0}^{\infty} (-1)^j (2j+1) \alpha_n q^{a\binom{n}{2}+bn+j(j+1)/2}}{(q;q)_\infty^p}$$

$$\equiv \frac{q^c \sum_{n=-\infty}^{\infty} \sum_{j=0}^{\infty} (-1)^j (2j+1) \alpha_n q^{a\binom{n}{2}+bn+j(j+1)/2}}{(q^p;q^p)_\infty} \pmod p.$$

We see that in this last expression the denominator is a function of q^p. Let us now examine the exponent of q in the numerator; for ease of computation we multiply by 8:

$$(2.2) \qquad 8\left(c + a\binom{n}{2} + bn + j(j+1)/2\right)$$

$$= 8c + a(4n^2 - 4n) + 8bn + 4j^2 + 4j$$

$$\equiv a(2n + 2b\bar{a} - 1)^2 + (2j+1)^2 \pmod p$$

Now we observe (by the definition of c) that if $j \equiv (p-1)/2 \bmod p$ (i.e. $(2j+1) \equiv 0 \pmod p$), then the last expression above is congruent to 0 mod p precisely when

$$n \equiv (1 - 2b\overline{a})\overline{2} \equiv \frac{p+1}{2} - b\overline{a} \pmod p.$$

If $j \not\equiv \frac{p-1}{2} \pmod p$, then the last expression in (2.2) can never be congruent to zero mod p because by the conditions on a

$$-a(2n + 2b\overline{a} - 1)^2$$

is either 0 or a quadratic nonresidue mod p and so cannot be congruent to a quadratic residue (i.e. $(2j+1)^2$) mod p.

Hence the coefficients of q^{pN} in (2.1) will all be linear combinations over $p\mathbb{Z}$ of various α_n (which are Laurent polynomials in several variables over $\mathbb{Z}$). $\square$

3. Modular Forms.

Ramanujan, Ewell, Gandhi (and probably many others) have proved instances of Theorem 1 (as mentioned in Section 1).

Congruence (1.1) follows from Theorem 1 with $p = 5, a = 3, b = 1, c_5(3,1) = 1$ and $\alpha_m = (-1)^m$. Congruence (1.2) follows from Theorem 1 with $p = 7, a = b = 1, c_7(1,1) = 2$ and $\alpha_m = (-1)^m(2m+1)$ if $m \geqq 0, \alpha_m = 0$ if $m < 0$.

Gandhi's Theorem IV in [7] corresponds to $\alpha_m = \delta_{m,0}$, while Theorem 2 in [8] corresponds to $a = b = 1$ and $\alpha_m = (-1)^m(2m+1)$ if $m \geqq 0$, $\alpha_m = 0$ if $m < 0$. Finally, Theorem 4 in [8] corresponds to $a = 3, b = 1$ and $\alpha_m = (-1)^m$.

Theorem 10.1 of [3] is the case $p = 5, a = 2, b = 1, c_5(2,1) = 2$; in that result the α_m were assumed to be 0 if $m < 0$ and to be integers otherwise.

The generality of Theorem 1 allows for a variety of other modular forms. To illustrate, we consider

$$\sum_{n=0}^{\infty} V_n q^n = \frac{\sum_{n=0}^{\infty} p(n) q^n}{\sum_{n=0}^{\infty} (-1)^n r_2(n) q^n},$$

where $r_2(n)$ is the number of representations of n as a sum of two squares. We note that

$$\begin{aligned}
\sum_{n=0}^{\infty} V_n q^n &= \frac{1}{(q)_\infty \left(\sum_{n=-\infty}^{\infty} (-1)^n q^{n^2} \right)^2} \\
&= \frac{(-q)_\infty^2}{(q)_\infty^3} \\
&= \frac{(q^2;q^2)_\infty}{(q)_\infty^4 (q;q^2)_\infty} \\
&= \frac{\sum_{m=0}^{\infty} q^{m(m+1)/2}}{(q)_\infty^4}.
\end{aligned}$$

Now by Theorem 1 with $p = 7, a = b = 1, c_7(1,1) = 2, \alpha_m = 1$ if $m \geq 0$, and 0 if $m < 0$, we see that

$$V_{7m+5} \equiv 0 \pmod{7}.$$