

On m -ary Partition Function Congruences: A Fresh Look at a Past Problem

Øystein J. Rødseth

Department of Mathematics, University of Bergen, Johs. Brunsgt. 12, N-5008 Bergen, Norway
E-mail: rodseth@mi.uib.no

and

James A. Sellers

*Department of Science and Mathematics, Cedarville University, 251 N. Main St.,
Cedarville, Ohio 45314*
E-mail: sellersj@cedarville.edu

Communicated by A. Granville

Received February 22, 2000; published online March 14, 2001

Let $b_m(n)$ denote the number of partitions of n into powers of m . Define $\sigma_r = \varepsilon_2 m^2 + \varepsilon_3 m^3 + \dots + \varepsilon_r m^r$, where $\varepsilon_i = 0$ or 1 for each i . Moreover, let $c_r = 1$ if m is odd, and $c_r = 2^{r-1}$ if m is even. The main goal of this paper is to prove the congruence $b_m(m^{r+1}n - \sigma_r - m) \equiv 0 \pmod{m^r/c_r}$. For $\sigma_r = 0$, the existence of such a congruence was conjectured by R. F. Churchhouse some 30 years ago, and its truth was proved by Ø. J. Rødseth, G. E. Andrews, and H. Gupta soon after. © 2001 Academic Press

Key Words: partitions; congruences.

1. INTRODUCTION

In 1968, while working with the best in contemporary computing technology at the Atlas Computer Laboratory, R. F. Churchhouse [2] discovered the following facts about the binary partition function $b(n)$: For all $k, n \geq 1$,

$$b(2^{2k+2}n) \equiv b(2^{2k}n) \pmod{2^{3k+2}}$$

and

$$b(2^{2k+1}n) \equiv b(2^{2k-1}n) \pmod{2^{3k}},$$

where $b(n)$ is the number of ways to represent n as

$$n = 2^{a_0} + 2^{a_1} + \dots$$

with $0 \leq a_0 \leq a_1 \leq \dots$.

Within months, several mathematicians expanded on Churchhouse's original results. Indeed, Rødseth [5] proved Churchhouse's congruences, and also proved, among other things, that for all odd primes p and all r , $n \geq 1$,

$$b_p(p^{r+1}n) \equiv b_p(p^r n) \pmod{p^r}. \quad (1)$$

The function $b_m(n)$ is the number of m -ary partitions of n , or the number of representations of n as

$$n = m^{a_0} + m^{a_1} + \dots$$

with $0 \leq a_0 \leq a_1 \leq \dots$.

Andrews [1] extended (1) by proving that, for all $m \geq 2$ and all r , $n \geq 1$,

$$b_m(m^{r+1}n) \equiv b_m(m^r n) \pmod{\frac{m^r}{c_r}}, \quad (2)$$

where $c_r = 1$ if m is odd and $c_r = 2^r$ if m is even. Finally, Gupta [4] sharpened Andrews' result by showing that (2) holds with $c_r = 2^{r-1}$ when m is even.

It is easy to see that the generating function for $b_m(n)$ is given by

$$B_m(q) = \sum_{n=0}^{\infty} b_m(n) q^n = \prod_{i=0}^{\infty} \frac{1}{1 - q^{m^i}},$$

which clearly satisfies $(1 - q) B_m(q) = B_m(q^m)$. Thus,

$$b_m(mn) - b_m(n) = b_m(mn - 1),$$

and

$$b_m(mn - 1) = b_m(mn - 2) = \dots = b_m(mn - m).$$

This allows (2) to be rewritten in the form

$$b_m(m^{r+1}n - m) \equiv 0 \pmod{\frac{m^r}{c_r}}. \quad (3)$$

The intent of this paper is to prove a family of congruences of which (3) is simply one subset. Indeed, we will see that a binary tree of congruences holds, for which (3) is simply one branch.

Our main goal is to prove the following:

THEOREM 1. *Let $r \geq 1$ and suppose that σ_r can be expressed as*

$$\sigma_r = \sum_{i=2}^r \varepsilon_i m^i,$$

where $\varepsilon_i = 0$ or 1 for each i . Finally, let $c_r = 1$ if m is odd, and $c_r = 2^{r-1}$ if m is even. Then, for all $n \geq 1$,

$$b_m(m^{r+1}n - \sigma_r - m) \equiv 0 \pmod{\frac{m^r}{c_r}}. \quad (4)$$

Note that (4) is Gupta's result in the case when $\sigma_r = 0$. Moreover, note that the presence of σ_r implies that (4) gives 2^{r-1} different congruences for each value of r . This is in contrast with (3), where only one congruence is proven for each r .

In order to prove Theorem 1, we will actually prove a stronger theorem by studying a specific restricted m -ary partition function. Let $b_{m,k}(n)$ be the number of representations of n of the form

$$n = m^{a_0} + m^{a_1} + \dots + m^{a_j}$$

with $0 \leq a_0 \leq a_1 \leq \dots \leq a_j < k$. If we denote the generating function for $b_{m,k}(n)$ by $B_{m,k}(q)$, then we have

$$B_{m,k}(q) = \prod_{i=0}^{k-1} \sum_{j=0}^{\infty} q^{jm^i} = \prod_{i=0}^{k-1} \frac{1}{1 - q^{m^i}},$$

and it is easily seen that $b_{m,k}(n)$ also equals the number of representations of n of the form

$$n = c_0 + c_1 m + c_2 m^2 + \dots, \quad 0 \leq c_i < m^k.$$

We now state our stronger theorem.

THEOREM 2. *Let $r \geq 1$, $k \geq 2$, and $s = \min(r, k-1)$. Moreover, let σ_s and c_s be defined as in Theorem 1. Then*

$$b_{m,k}(m^{r+1}n - \sigma_s - m) \equiv 0 \pmod{\frac{m^r}{c_s}}.$$

Two remarks are in order before moving to the proof of Theorem 2. First, we note that the case $\sigma_s = 0$ of Theorem 2 was proven by Dirdal [3, Theorem 2]. Second, it is clear that, for a given n , $b_m(n) = b_{m,k}(n)$ for a

sufficiently large value of k . Therefore, Theorem 1 must follow once Theorem 2 is proven.

In Section 2 below, we briefly mention some preliminaries needed throughout the remainder of the paper. We provide the bulk of the mathematical work needed, including several crucial lemmata, in Section 3. We close the paper in Section 4 by incorporating the various results in Section 3 to complete the proof of Theorem 2.

2. PRELIMINARIES

Let $\mathbf{Z}[[q]]$ be the ring of formal power series in q with coefficients in \mathbf{Z} . We define a \mathbf{Z} -linear operator $U: \mathbf{Z}[[q]] \rightarrow \mathbf{Z}[[q]]$ by putting

$$U \sum_n a(n) q^n = \sum_n a(mn) q^n. \quad (5)$$

Notice that

$$U \sum_n a(n) q^{n+1} = \sum_n a(mn-1) q^n, \quad (6)$$

and if $f(q), g(q) \in \mathbf{Z}[[q]]$, then

$$U(f(q) g(q^m)) = (Uf(q)) g(q). \quad (7)$$

Finally, if $f(q) = \sum_n a(n) q^n$, $g(q) = \sum_n c(n) q^n \in \mathbf{Z}[[q]]$ and M is a positive integer, then we know

$$f(q) \equiv g(q) \pmod{M} \quad (\text{in } \mathbf{Z}[[q]])$$

if and only if, for all n ,

$$a(n) \equiv c(n) \pmod{M} \quad (\text{in } \mathbf{Z}).$$

3. THE LEMMATA

We open this section with a lemma concerning binomial coefficients.

LEMMA 1. *If $n, r \geq 1$, then there exist $\alpha_r(i) \in \mathbf{Z}$ such that*

$$\binom{mn+r-1}{r} = \sum_{i=1}^r \alpha_r(i) \binom{n+i-1}{i}. \quad (8)$$

Proof. We consider the binomial coefficients involved as polynomials in n over \mathbf{Q} . Since $\binom{mn+r-1}{r}$ is a polynomial of degree r in n , and $\binom{n+i-1}{i}$ is a polynomial of degree i in n , $i=0, 1, \dots, r$, there exist $\alpha_r(i) \in \mathbf{Q}$ such that

$$\binom{mn+r-1}{r} = \sum_{i=0}^r \alpha_r(i) \binom{n+i-1}{i}.$$

Putting $n=0$, we see that $\alpha_r(0)=0$. Putting $n=-j$, we get

$$(-1)^j \alpha_r(j) = (-1)^r \binom{mj}{r} - \sum_{i=1}^{j-1} (-1)^i \binom{j}{i} \alpha_r(i), \quad j=1, 2, \dots, r.$$

By induction on i , it follows that all the $\alpha_r(i)$ are integers. ■

Comparing the coefficients of n^r in (8), we get

$$\alpha_r(r) = m^r, \quad (9)$$

and comparing the coefficients of n^{r-1} , we get

$$\alpha_r(r-1) = -\frac{1}{2}(r-1)(m-1)m^{r-1}. \quad (10)$$

We also have

$$\alpha_r(j) = 0 \quad \text{for } mj < r \quad \left(\text{i.e., if } j \leq \left\lfloor \frac{r-1}{m} \right\rfloor \right).$$

Next, let

$$h_i = h_i(q) = \frac{q}{(1-q)^{i+1}}, \quad i \geq 0.$$

Then

$$h_i = \sum_{n=1}^{\infty} \binom{n+i-1}{i} q^n, \quad (11)$$

so that

$$Uh_r = U \sum_{n=1}^{\infty} \binom{n+r-1}{r} q^n = \sum_{n=1}^{\infty} \binom{mn+r-1}{r} q^n.$$

It follows from Lemma 1 and (11) that

$$Uh_r = \sum_{i=1}^r \alpha_r(i) h_i, \quad r \geq 1. \quad (12)$$

Let

$$H_0 = h_0 \quad \text{and} \quad H_{i+1} = U\left(\frac{1}{1-q} H_i\right), \quad i \geq 0. \tag{13}$$

Then we have

$$H_1 = mh_1 \quad \text{and} \quad H_2 = m^3 h_2 - \binom{m}{2} H_1.$$

We can prove analogous results for H_r for each $r \geq 1$.

LEMMA 2. *Let $c_2 = 1$ if m is odd and $c_2 = 2$ if m is even (as in the statement of Theorem 1). Then, for $r \geq 1$, there exist $\beta_r(i) \in \mathbf{Z}$ such that*

$$H_r = m^{(1/2)r(r+1)} h_r - \sum_{i=1}^{r-1} \beta_r(i) H_i, \tag{14}$$

where

$$\beta_r(i) \equiv 0 \pmod{\frac{m^{r-i}}{c_2}}, \quad i = 1, 2, \dots, r-1. \tag{15}$$

Note. In the following we set $\beta_r(r) = 1$ and $\beta_r(0) = 0$ for all $r \geq 1$.

Proof. We use induction on r . The lemma is true for $r = 1$. Suppose that for some $r > 1$, we have

$$H_j = m^{(1/2)j(j+1)} h_j - \sum_{i=1}^{j-1} \beta_j(i) H_i, \quad j = 1, 2, \dots, r-1, \tag{16}$$

where all the $\beta_j(i)$ are integers satisfying

$$\beta_j(i) \equiv 0 \pmod{\frac{m^{j-i}}{c_2}}, \quad i = 1, 2, \dots, j-1. \tag{17}$$

Then

$$H_r = U\left(\frac{1}{1-q} H_{r-1}\right) = m^{(1/2)(r-1)r} U h_r - \sum_{i=1}^{r-2} \beta_{r-1}(i) H_{i+1},$$

and, by (12),

$$H_r = m^{(1/2)(r-1)r} \sum_{j=1}^r \alpha_r(j) h_j - \sum_{i=2}^{r-1} \beta_{r-1}(i-1) H_i.$$

Using (9) and (16), we further get

$$\begin{aligned}
 H_r &= m^{(1/2)r(r+1)}h_r + \sum_{j=1}^{r-1} m^{(1/2)(r-1)r-(1/2)j(j+1)}\alpha_r(j) \sum_{i=1}^j \beta_j(i) H_i \\
 &\quad - \sum_{i=1}^{r-1} \beta_{r-1}(i-1) H_i \\
 &= m^{(1/2)r(r+1)}h_r + \sum_{i=1}^{r-1} \sum_{j=i}^{r-1} m^{(1/2)(r-1)r-(1/2)j(j+1)}\alpha_r(j) \beta_j(i) H_i \\
 &\quad - \sum_{i=1}^{r-1} \beta_{r-1}(i-1) H_i.
 \end{aligned}$$

Thus (14) holds with

$$\beta_r(i) = \beta_{r-1}(i-1) - \sum_{j=i}^{r-1} m^{(1/2)(r-1)r-(1/2)j(j+1)}\alpha_r(j) \beta_j(i),$$

so that $\beta_r(i) \in \mathbf{Z}$. Since $\frac{1}{2}(r-1)r - \frac{1}{2}j(j+1) \geq r-1$ for $j \leq r-2$, we further have

$$\beta_r(i) \equiv \beta_{r-1}(i-1) - \alpha_r(r-1) \beta_{r-1}(i) \pmod{m^{r-1}},$$

and, by (17) and (10), we see that (15) holds. ■

LEMMA 3. *Let c_s be defined as in Theorem 1. For $r \geq 1$, there exists $\gamma_r(i) \in \mathbf{Z}$ such that*

$$UH_r = \sum_{i=1}^r \gamma_r(i) H_i, \tag{18}$$

where

$$\gamma_r(i) \equiv 0 \pmod{\frac{m^{r+1-i}}{c_{r+1-i}}}, \quad i = 1, 2, \dots, r. \tag{19}$$

Proof. We use induction on r . We have $UH_1 = mH_1$, so the lemma is true for $r = 1$. Suppose that for some $r > 1$, we have

$$UH_j = \sum_{i=1}^j \gamma_j(i) H_i, \quad j = 1, 2, \dots, r-1, \tag{20}$$

where all the $\gamma_j(i)$ are integers satisfying

$$\gamma_j(i) \equiv 0 \pmod{\frac{m^{j+1-i}}{c_{j+1-i}}}. \quad (21)$$

Applying U to (14), and using (12) and (20), we have

$$\begin{aligned} UH_r &= m^{(1/2)r(r+1)}Uh_r - \sum_{j=1}^{r-1} \beta_r(j)UH_j \\ &= m^{(1/2)r(r+1)} \sum_{j=1}^r \alpha_r(j)h_j - \sum_{j=1}^{r-1} \beta_r(j) \sum_{i=1}^j \gamma_j(i)H_i \\ &= \sum_{j=1}^r m^{(1/2)r(r+1)-(1/2)j(j+1)}\alpha_r(j) \sum_{i=1}^j \beta_j(i)H_i \\ &\quad - \sum_{i=1}^{r-1} \sum_{j=i}^{r-1} \beta_r(j)\gamma_j(i)H_i \\ &= \sum_{i=1}^r \sum_{j=i}^r m^{(1/2)r(r+1)-(1/2)j(j+1)}\alpha_r(j)\beta_j(i)H_i \\ &\quad - \sum_{i=1}^{r-1} \sum_{j=i}^{r-1} \beta_r(j)\gamma_j(i)H_i. \end{aligned}$$

Thus (18) holds with

$$\gamma_r(i) = \sum_{j=i}^r m^{(1/2)r(r+1)-(1/2)j(j+1)}\alpha_r(j)\beta_j(i) - \sum_{j=i}^{r-1} \beta_r(j)\gamma_j(i),$$

which shows that all the $\gamma_r(i)$ are integers. For $1 \leq j \leq r-1$, we have $\frac{1}{2}r(r+1) - \frac{1}{2}j(j+1) \geq r$, so that, using (9),

$$\gamma_r(i) \equiv - \sum_{j=i}^{r-1} \beta_r(j)\gamma_j(i) \pmod{m^r},$$

and by (15) and (21), we obtain (19). ■

LEMMA 4. For $r \geq 1$ and $t \geq 0$, there exist $\gamma_{r,t}(i) \in \mathbf{Z}$ such that

$$U^t H_r = \sum_{i=1}^r \gamma_{r,t}(i) H_i, \quad (22)$$

where

$$\gamma_{r,t}(i) \equiv 0 \pmod{\frac{m^{r+t-i}}{c_{r+1-i}}}, \quad i = 1, 2, \dots, r. \quad (23)$$

Proof. We use induction on t . The lemma is trivially true for $t=0$. Suppose that the lemma is true for t replaced by $t-1$ for some $t \geq 1$. Using Lemma 3, we have

$$\begin{aligned} U^t H_r &= \sum_{j=1}^r \gamma_{r,t-1}(j) UH_j = \sum_{j=1}^r \gamma_{r,t-1}(j) \sum_{i=1}^j \gamma_j(i) H_i \\ &= \sum_{i=1}^r \sum_{j=i}^r \gamma_{r,t-1}(j) \gamma_j(i) H_i, \end{aligned}$$

and we see that (22) holds with

$$\gamma_{r,t}(i) = \sum_{j=i}^r \gamma_{r,t-1}(j) \gamma_j(i).$$

Thus, all the $\gamma_{r,t}(i)$ are integers. By the induction hypothesis and (19), we have

$$\gamma_{r,t-1}(j) \gamma_j(i) \equiv 0 \pmod{\frac{m^{r+t-1-j}}{c_{r+1-j}} \cdot \frac{m^{j+1-i}}{c_{j+1-i}}}$$

or

$$\gamma_{r,t-1}(j) \gamma_j(i) \equiv 0 \pmod{\frac{m^{r+t-i}}{c_{r+1-i}}}.$$

Therefore, (23) is satisfied and the proof is complete. ■

We now define $K_i = K_i(q)$ by

$$K_1 = H_1, \quad K_i = U \left(\frac{q^{\varepsilon_i}}{1-q} K_{i-1} \right) \quad \text{for } i \geq 2, \quad (24)$$

where $\varepsilon_i = 0$ or 1 for each i (as in the statement of Theorem 1). Then we have the following lemma.

LEMMA 5. For $r \geq 1$, there exist $\kappa_r(i) \in \mathbf{Z}$ such that

$$K_r = \sum_{i=1}^r \kappa_r(i) H_i, \quad (25)$$

where $\kappa_r(r) = 1$, and

$$\kappa_r(i) \equiv 0 \pmod{\frac{m^{r-i}}{c_{r-i}}}, \quad i = 1, 2, \dots, r-1. \quad (26)$$

Proof. We use induction on r . The lemma is trivially true for $r = 1$. Suppose the lemma is true for r replaced by $r-1$ for some $r \geq 2$. Putting $\kappa_r(0) = 0$ for all r , we have

$$\begin{aligned} U\left(\frac{1}{1-q} K_{r-1}\right) &= \sum_{i=1}^{r-1} \kappa_{r-1}(i) U\left(\frac{1}{1-q} H_i\right) \\ &= \sum_{i=1}^{r-1} \kappa_{r-1}(i) H_{i+1} = \sum_{i=1}^r \kappa_{r-1}(i-1) H_i. \end{aligned}$$

Moreover, using Lemma 3, we get

$$\begin{aligned} UK_{r-1} &= \sum_{j=1}^{r-1} \kappa_{r-1}(j) UH_j = \sum_{j=1}^{r-1} \kappa_{r-1}(j) \sum_{i=1}^j \gamma_j(i) H_i \\ &= \sum_{i=1}^{r-1} \sum_{j=i}^{r-1} \kappa_{r-1}(j) \gamma_j(i) H_i. \end{aligned}$$

Now we have

$$\begin{aligned} K_r &= U\left(\frac{q^{\varepsilon_r}}{1-q} K_{r-1}\right) = U\left(\frac{1}{1-q} K_{r-1} - \varepsilon_r K_{r-1}\right) \\ &= \sum_{i=1}^r \kappa_{r-1}(i-1) H_i - \varepsilon_r \sum_{i=1}^{r-1} \sum_{j=i}^{r-1} \kappa_{r-1}(j) \gamma_j(i) H_i. \end{aligned}$$

Thus (25) holds with

$$\kappa_r(i) = \kappa_{r-1}(i-1) - \varepsilon_r \sum_{j=i}^{r-1} \kappa_{r-1}(j) \gamma_j(i).$$

Then all the $\kappa_r(i)$ are integers, and in particular $\kappa_r(r) = \kappa_{r-1}(r-1) = 1$. Using the induction hypothesis and (19), we also see that (26) holds. ■

LEMMA 6. For $r = 1, 2, \dots, k-1$, we have

$$\sum_{n=1}^{\infty} b_{m,k}(m^{r+1}n - \sigma_r - m) q^n = K_r(q) B_{m,k-r-1}(q). \quad (27)$$

Proof. It is clear that, for $k \geq 1$,

$$B_{m,k}(q) = \frac{1}{1-q} B_{m,k-1}(q^m). \quad (28)$$

Suppose that $k \geq 2$. Because

$$B_{m,k}(q) = \sum_{n=0}^{\infty} b_{m,k}(n) q^n,$$

we see from (28) that

$$\sum_{n=0}^{\infty} b_{m,k}(n) q^n = \frac{1}{1-q} B_{m,k-1}(q^m).$$

Since $U_{\frac{1}{1-q}} = \frac{1}{1-q}$, (7) and (28) imply that

$$\sum_{n=0}^{\infty} b_{m,k}(mn) q^{n+1} = H_0(q) B_{m,k-1}(q) = \frac{1}{1-q} H_0(q) B_{m,k-2}(q^m).$$

By (6), (7), (13), and (24), it follows that (27) is true for $r = 1$.

Suppose that (27) holds for r replaced by $r - 1$ for some r in the interval $2 \leq r \leq k - 1$. By (28), we then have

$$\sum_{n=1}^{\infty} b_{m,k}(m^r n - \sigma_{r-1} - m) q^{n+\varepsilon_r} = \frac{q^{\varepsilon_r}}{1-q} K_{r-1}(q) B_{m,k-r-1}(q^m).$$

Now use (5) if $\varepsilon_r = 0$ and (6) if $\varepsilon_r = 1$. Then, by (7) and (24), we obtain (27), which completes the proof. \blacksquare

4. PROOF OF THEOREM 2

With the various lemmata provided in the previous section, we can now quickly prove Theorem 2. Using Lemma 2, we get by induction on r that

$$H_r(q) \equiv 0 \pmod{\frac{m^r}{c_r}}, \quad r \geq 1. \quad (29)$$

It follows by Lemma 5 that

$$K_r(q) \equiv 0 \pmod{\frac{m^r}{c_r}}, \quad r \geq 1.$$

Thus, by Lemma 6, Theorem 2 holds for $1 \leq r \leq k - 1$.

Next, suppose that $r \geq k-1 \geq 1$. Let $r = k-1 + t$, $t \geq 0$. By Lemma 6 (with $r = k-1$) and Lemma 5,

$$\sum_{n=1}^{\infty} b_{m,k}(m^{kn} - \sigma_{k-1} - m) q^n = K_{k-1}(q) = \sum_{j=1}^{k-1} \kappa_{k-1}(j) H_j(q).$$

Applying U^t and using Lemma 4, we get

$$\begin{aligned} \sum_{n=1}^{\infty} b_{m,k}(m^{r+1}n - \sigma_{k-1} - m) q^n &= \sum_{j=1}^{k-1} \kappa_{k-1}(j) U^t H_j \\ &= \sum_{j=1}^{k-1} \kappa_{k-1}(j) \sum_{i=1}^j \gamma_{j,t}(i) H_i \\ &= \sum_{i=1}^{k-1} \sum_{j=i}^{k-1} \kappa_{k-1}(j) \gamma_{j,t}(i) H_i. \end{aligned}$$

By Lemma 5, (23) and (29), it follows that

$$\kappa_{k-1}(j) \gamma_{j,t}(i) H_i \equiv 0 \pmod{\frac{m^{k-1+t}}{c_{k-1}}}.$$

Thus

$$b_{m,k}(m^{r+1}n - \sigma_{k-1} - m) \equiv 0 \pmod{\frac{m^r}{c_{k-1}}} \quad \text{if } 1 \leq k-1 \leq r.$$

This completes the proof of Theorem 2.

REFERENCES

1. G. E. Andrews, Congruence properties of the m -ary partition function, *J. Number Theory* **3** (1971), 104–110.
2. R. F. Churchhouse, Congruence properties of the binary partition function, *Math. Proc. Cambridge Philos. Soc.* **66** (1969), 371–376.
3. G. Dirdal, Congruences for m -ary partitions, *Math. Scand.* **37** (1975), 76–82.
4. H. Gupta, On m -ary partitions, *Math. Proc. Cambridge Philos. Soc.* **71** (1972), 343–345.
5. Ø. J. Rødseth, Some arithmetical properties of m -ary partitions, *Math. Proc. Cambridge Philos. Soc.* **68** (1970), 447–453.