PARTITION IDENTITIES AND THE COIN EXCHANGE PROBLEM

ALEXANDER E. HOLROYD

ABSTRACT. The number of partitions of n into parts divisible by a or b equals the number of partitions of n in which each part and each difference of two parts is expressible as a non-negative integer combination of a and b. This generalizes identities of MacMahon and Andrews. The analogous identities for three or more integers (in place of a, b) hold in certain cases.

1. INTRODUCTION

A **partition** of n is an unordered multiset of positive integers (called **parts**) whose sum is n. For positive integers $a_1, \ldots, a_m$ we denote the set of non-negative integer combinations

$$S = S(a_1, \ldots, a_m) := \left\{ \sum_{i=1}^m x_i a_i : x_1, \ldots, x_m \in \mathbb{N}_0 \right\},$$

where $\mathbb{N}_0 := \{0, 1, 2, \ldots\}$.

Theorem 1. *For positive integers n, a_1 and a_2, the following are all equinumerous:*

(i) partitions of n in which each part and each difference between two parts lies in $S(a_1, a_2)$;

(ii) partitions of n in which each part appears with multiplicity lying in $S(a_1, a_2)$;

(iii) partitions of n in which each part is divisible by a_1 or a_2.

For example, when $(n, a_1, a_2) = (13, 3, 4)$, the three sets of partitions are: (i) $\{(13), (10, 3), (7, 3, 3)\}$; (ii) $\{(3, 3, 3, 1, 1, 1, 1)\}, (2, 2, 2, 1, \ldots, 1), (1, \ldots, 1)\}$; (iii) $\{(9, 4), (6, 4, 3), (4, 3, 3, 3)\}$.

We also establish the following partial extension to three or more integers $a_1, \ldots, a_m$. Let $\sqcap$ and $\sqcup$ denote greatest common divisor and least common multiple respectively.

Date: June 15, 2007; revised December 8, 2007.

2000 *Mathematics Subject Classification.* 05A17; 11P81; 11P83.

Key words and phrases. partition identity, coin problem, Frobenius problem.

Funded in part by an NSERC Discovery Grant and by Microsoft Research.

Theorem 2. *For any positive integers n and $a_1, \ldots, a_m$, the following are equinumerous:*

(i) partitions of n in which each part and each difference between two parts lies in $S(a_1, \ldots, a_m)$;
(ii) partitions of n in which each part appears with multiplicity lying in $S(a_1, \ldots, a_m)$.

If $a_1, \ldots, a_m$ can be ordered such that

$$\forall i = 2, \ldots, m, \ \exists j < i \text{ such that } (a_1 \sqcap \cdots \sqcap a_{i-1}) \sqcup a_i = a_j \sqcup a_i. \qquad (*)$$

then in addition the following are equinumerous with (i) and (ii):

(iii) partitions of n in which each part is divisible by some a_i.

Note that (*) holds automatically when $m = 2$, so Theorem 1 is a special case of Theorem 2.

2. Remarks

To avoid uninteresting cases, $a_1, \ldots, a_m$ should be coprime, and none should be a multiple of another. (Indeed, if the greatest common divisor is $g > 1$ then Theorem 2 reduces easily to the case $(n', a'_1, \ldots, a'_m) = g^{-1}(n, a_1, \ldots, a_m)$, while if a_j is a multiple of a_i then the statements of the theorem are unchanged by removing a_j from $a_1, \ldots, a_m$).

The set S is sometimes interpreted as describing sums of money that can be formed using coins of given denominations. When $a_1, \ldots, a_m$ are coprime, the complement $S^{\mathrm{C}} := \mathbb{N}_0 \setminus S$ is finite; see e.g. [10]. The case $m = 2$ was studied by Sylvester [11], who proved for a_1, a_2 coprime that $|S^{\mathrm{C}}| = \frac{1}{2}(a_1 - 1)(a_2 - 1)$ and $\max S^{\mathrm{C}} = (a_1 - 1)(a_2 - 1) - 1$. The case $m \geq 3$ was proposed by Frobenius, and is much less well understood in general. An exception is when $a_1, \ldots, a_m$ satisfy a certain condition which is implied by our condition (*); see [9]. For more information see [10].

When $m = 2$ we have for example $S(2,3)^{\mathrm{C}} = \{1\}$; $S(3,4)^{\mathrm{C}} = \{1,2,5\}$; $S(2,5)^{\mathrm{C}} = \{1,3\}$; $S(3,5)^{\mathrm{C}} = \{1,2,4,7\}$; $S(4,5)^{\mathrm{C}} = \{1,2,3,6,7,11\}$. Larger sets $\{a_1, \ldots, a_m\}$ satisfying condition (*) include $\{4,6,9\}$; $\{6,8,9\}$; $\{6,9,10\}$; $\{p^{m-1}, p^{m-2}q, \ldots, q^{m-1}\}$ for p, q coprime; $\{\pi/p_1, \ldots, \pi/p_m\}$ for $p_1, \ldots, p_m$ pairwise coprime and $\pi := \prod_i p_i$. We have for instance $S(4,6,9)^{\mathrm{C}} = \{1,2,3,5,7,11\}$.

In the case $\{a_1, a_2\} = \{2, 3\}$, the equality between (i) and (iii) in Theorem 1 gives the following partition identity due to MacMahon [8, §299–300] (see also [3, p. 14, Examples 9–10]).

The number of partitions of n into parts not congruent to ± 1 modulo 6 equals the number of partitions of n with no consecutive integers and no ones as parts.

The generalization to $\{a_1, a_2\} = \{2, 2r+1\}$, $r \in \mathbb{N}_0$ was proved (in a form similar to that above) by Andrews [2]. The other cases of Theorems 1 and 2 appear to be new. Other recent work related to MacMahon's identity appears in [1, 4, 7]. Somewhat similar identities are proved in [5]. For more information on partitions and partition identities see e.g. [3].

Finally we note that the second assertion in Theorem 2 cannot hold for arbitrary $a_1, \dots, a_m$ with $m \geq 3$. For example, it does not hold for $\{a_1, a_2, a_3\} = \{2, 3, 5\}$: we have $S(2,3,5) = S(2,3)$, but allowing multiples of 5 in addition to multiples of 2 and 3 clearly increases the number of partitions of type (iii) for some n.

3. Proofs

As remarked above, Theorem 1 is the $m = 2$ case of Theorem 2. We will prove the two assertions of Theorem 2 separately. The proofs are simpler when $m = 2$, and the reader may find it helpful to bear this case in mind throughout.

Proof of Theorem 2 (first equality). Fix $a_1, \dots, a_m$, and let F_n and M_n be the sets of partitions in (i) and (ii) respectively. We will show that $|F_n| = |M_n|$.

For a partition $\lambda = (\lambda_1, \dots, \lambda_r)$ (where $n = \sum_i \lambda_i$ and $\lambda_1 \geq \dots \geq \lambda_r$), the **conjugate** partition $\lambda' = (\lambda'_1, \dots, \lambda'_{r'})$ is defined as usual by $r' = \lambda_1$ and $\lambda'_i = \max\{j : \lambda_j \geq i\}$. Since the set S is closed under addition, the condition that λ has all parts and differences between parts in S is equivalent to the condition that each *adjacent* pair in the sequence $\lambda_1, \lambda_2, \dots, \lambda_r, 0$ differs by an element of S. On the other hand, it is readily seen that the latter condition is equivalent to the condition that λ' has all multiplicities in S (indeed this holds for any set S). Hence conjugation is a bijection between F_n and M_n. $\square$

Our proof of the second assertion in Theorem 2 relies on the two simple lemmas below. Given integers $a_1, \dots, a_m$ we write

$$\ell_i := (a_1 \sqcap \dots \sqcap a_{i-1}) \sqcup a_i.$$

Lemma 3. *If $a_1 \dots, a_m$ satisfy condition (*) then we have the formal power series identity*

$$\sum_{k \in S(a_1, \dots, a_m)} q^k = \frac{\prod_{i=2}^m (1 - q^{\ell_i})}{\prod_{i=1}^m (1 - q^{a_i})}.$$

In the case when $m = 2$ and a_1, a_2 are coprime, the above expression has the appealing form $(1 - q^{a_1 a_2})(1 - q^{a_1})^{-1}(1 - q^{a_2})^{-1}$, as noted in

[12]. Expressions for the left side for $m = 3$ and arbitrary a_1, a_2, a_3, are derived in [6, 12].

Proof of Lemma 3. We use induction on m. When $m = 1$ we have

$$\sum_{k \in S(a_1)} q^k = 1 + q^{a_1} + q^{2a_1} + \cdots = \frac{1}{1 - q^{a_1}}$$

as required.

For $m \geq 2$, clearly any $k \in S(a_1, \ldots, a_m)$ can be expressed as

$$k = xa_m + y, \qquad \text{where } x \in \mathbb{N}_0 \text{ and } y \in S(a_1, \ldots, a_{m-1}). \tag{1}$$

We claim that under condition (*), each such k has a *unique* such representation subject to the additional constraint

$$x < \ell_m / a_m. \tag{2}$$

Once this is proved we obtain

$$\sum_{k \in S(a_1, \ldots, a_m)} q^k = (1 + q^{a_m} + q^{2a_m} + \cdots + q^{\ell_m - a_m}) \sum_{k \in S(a_1, \ldots, a_{m-1})} q^k.$$

By the inductive hypothesis this equals

$$\frac{1 - q^{\ell_m}}{1 - q^{a_m}} \times \frac{\prod_{i=2}^{m-1}(1 - q^{\ell_i})}{\prod_{i=1}^{m-1}(1 - q^{a_i})},$$

which is the required expression.

To check the above claim, let $j = j(m)$ be as in condition (*), and write $d = a_1 \sqcap \cdots \sqcap a_{m-1}$, so that $\ell_m = d \sqcup a_m = a_j \sqcup a_m$. Now note that any representation $k = xa_m + y$ as in (1) that violates (2) may be re-expressed as $k = (x - \ell_m/a_m)a_m + (y + \ell_m)$, where $x - \ell_m/a_m \in \mathbb{N}_0$, and $y + \ell_m \in S(a_1, \ldots, a_{m-1})$ (since ℓ_m is a multiple of a_j). By repeatedly applying this we can reduce x until (2) is satisfied, as required. To check uniqueness, note that all elements of $S(a_1, \ldots, a_{m-1})$ are divisible by d, while the ℓ_m/a_m quantities $0, a_m, 2a_m, \ldots, \ell_m - a_m$ are all distinct modulo d (since $\ell_m = d \sqcup a_m$). Hence we see that no two distinct expressions $xa_m + y$ satisfying (1),(2) can be equal. $\square$

Let $\mathbf{1}[\cdot]$ denote an indicator function and let $|$ denote "divides".

Lemma 4. *If $a_1 \ldots, a_m$ satisfy condition (*) then for any positive integer k,*

$$\mathbf{1}\big[a_i | k \text{ for some } i\big] = \sum_{i=1}^{m} \mathbf{1}[a_i | k] - \sum_{i=2}^{m} \mathbf{1}[\ell_i | k].$$

When $m = 2$ and a_1, a_2 are coprime, the lemma is the familiar inclusion/exclusion formula $\mathbf{1}[a_1 | k \text{ or } a_2 | k] = \mathbf{1}[a_1 | k] + \mathbf{1}[a_2 | k] - \mathbf{1}[a_1 a_2 | k]$.

Proof of Lemma 4. We use induction on m. The case $m = 1$ is trivial. For $m \geq 2$ we have

$$\begin{aligned}\mathbf{1}\big[a_i|k \text{ for some } i\big] =&\mathbf{1}[a_m|k] + \mathbf{1}\big[a_i|k \text{ for some } i < m\big]\\ &- \mathbf{1}\big[a_m|k, \text{ and } a_i|k \text{ for some } i < m\big]\end{aligned}$$

We claim that the last condition "$a_m|k$, and $a_i|k$ for some $i < m$" is equivalent to $\ell_m|k$. Once this is established, the result follows by substituting the inductive hypothesis and the claim into the above equation.

Turning to the proof of the claim, if the given condition holds then $a_m|k$ and $d|k$, where $d = a_1 \sqcap \cdots \sqcap a_{m-1}$. So k is divisible by $a_m \sqcup d = \ell_m$. For the converse, recall from (*) that $\ell_m = a_m \sqcup a_j$ for some $j < m$, so $\ell_m|k$ implies $a_m|k$ and $a_j|k$. □

Proof of Theorem 2 (second equality). Suppose (*) holds, and let M_n and D_n denote the sets of partitions in (ii) and (iii) respectively. We will show $|M_n| = |D_n|$.

Using Lemma 3, the generating function for $|M_n|$ is

$$G(q) := \sum_{n=0}^{\infty} |M_n|\, q^n = \prod_{t=1}^{\infty} \Big[\sum_{k\in S} q^{kt}\Big] = \prod_{t=1}^{\infty} \frac{\prod_{i=2}^{m}(1-q^{\ell_i t})}{\prod_{i=1}^{m}(1-q^{a_i t})}.$$

When the product over t is expanded, the factor $(1 - q^{\ell_i t})$ contributes a factor $(1 - q^k)$ in the numerator for each k that is a non-negative multiple of ℓ_i; similarly for the factors in the denominator. Thus

$$\begin{aligned}G(q) &= \prod_{k=1}^{\infty}\Big(1-q^k\Big)^{-\sum_{i=1}^{m}\mathbf{1}[a_i|k] + \sum_{i=2}^{m}\mathbf{1}[\ell_i|k]}\\ &= \prod_{k=1}^{\infty}\Big(1-q^k\Big)^{-\mathbf{1}[a_i|k \text{ for some } i]} = \prod_{\substack{k\geq 1:\\ a_i|k \text{ for some } i}} \frac{1}{1-q^k}.\end{aligned}$$

(In the second equality we have used Lemma 4.) But the last expression is the generating function for $|D_n|$. □

Questions

Can Theorems 1 and 2 be given simple bijective proofs? Dan Romik has found an affirmative answer for Theorem 1 (personal communication). Is condition (*) necessary and sufficient for the identity between (i) and (iii) in Theorem 2? For those $a_1, \ldots, a_m$ not satisfying this identity, are the partitions of type (i) or type (iii) equinumerous with partitions in some other natural classes? Can condition (*) be expressed in a more natural form?

Acknowledgments

I thank Dan Romik, George Andrews and the referees for valuable comments and encouragement.

References

[1] G. Andrews, H. Eriksson, F. Petrov, and D. Romik. Integrals, partitions and MacMahon's theorem. *J. Combinatorial Theory A*, 114:545–554, 2007.

[2] G. E. Andrews. A generalization of a partition theorem of MacMahon. *J. Combinatorial Theory*, 3:100–101, 1967.

[3] G. E. Andrews. *The theory of partitions*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1998. Reprint of the 1976 original.

[4] G. E. Andrews. Partitions with short sequences and mock theta functions. *Proc. Natl. Acad. Sci. USA*, 102(13):4666–4671 (electronic), 2005.

[5] G. E. Andrews and R. P. Lewis. An algebraic identity of F. H. Jackson and its implications for partitions. *Discrete Math.*, 232(1-3):77–83, 2001.

[6] G. Denham. Short generating functions for some semigroup algebras. *Electron. J. Combin.*, 10:Research Paper 36, 7 pp. (electronic), 2003.

[7] A. E. Holroyd, T. M. Liggett, and D. Romik. Integrals, partitions, and cellular automata. *Trans. Amer. Math. Soc.*, 356(8):3349–3368, 2004.

[8] P. A. MacMahon. *Combinatory analysis*. Two volumes (bound as one). Chelsea Publishing Co., New York, 1960.

[9] A. Nijenhuis and H. S. Wilf. Representations of integers by linear forms in nonnegative integers. *J. Number Theory*, 4:98–106, 1972.

[10] J. L. Ramírez Alfonsín. *The Diophantine Frobenius problem*, volume 30 of *Oxford Lecture Series in Mathematics and its Applications*. Oxford University Press, Oxford, 2005.

[11] J. J. Sylvester. On subinvariants, i.e. semi-invariants to binary quantities of an unlimited order. *Am. J. Math.*, 5:119–136, 1882.

[12] L. A. Székely and N. C. Wormald. Generating functions for the Frobenius problem with 2 and 3 generators. *Math. Chronicle*, 15:49–57, 1986.

Department of Mathematics, University of British Columbia, 121-1984 Mathematics Rd., Vancouver, BC V6T 1Z2, Canada

E-mail address: holroyd(at)math.ubc.ca