The polynomial part of a restricted partition function related to the Frobenius problem

Matthias Beck
Department of Mathematical Sciences
State University of New York
Binghamton, NY 13902–6000, USA
matthias@math.binghamton.edu

Ira M. Gessel *
Department of Mathematics
Brandeis University
Waltham, MA 02454–9110, USA
gessel@brandeis.edu

Takao Komatsu
Faculty of Education
Mie University
Mie, 514–8507, Japan
komatsu@edu.mie-u.ac.jp

August 17, 2001

MR Subject Classifications: Primary 05A15; Secondary 11P81, 05A17

Abstract

Given a set of positive integers $A = \{a_1, \dots, a_n\}$, we study the number $p_A(t)$ of nonnegative integer solutions $(m_1, \dots, m_n)$ to $\sum_{j=1}^n m_j a_j = t$. We derive an explicit formula for the polynomial part of p_A.

Let $A = \{a_1, \dots, a_n\}$ be a set of positive integers with $\gcd(a_1, \dots, a_n) = 1$. The classical *Frobenius problem* asks for the largest integer t (the *Frobenius number*) such that

$$m_1 a_1 + \cdots + m_n a_n = t$$

has no solution in nonnegative integers $m_1, \dots, m_n$. For $n = 2$, the Frobenius number is $(a_1 - 1)(a_2 - 1) - 1$, as is well known, but the problem is extremely difficult for $n > 2$. (For surveys of the Frobenius problem, see [R, Se].) One approach [BDR, I, K, SÖ] is to study the restricted partition function $p_A(t)$, the number of nonnegative integer solutions $(m_1, \dots, m_n)$ to $\sum_{j=1}^n m_j a_j = t$, where t is a nonnegative integer. The Frobenius number is the largest integral zero of $p_A(t)$. Note that, in contrast to the Frobenius problem, in the definition of p_A we do not require $a_1, \dots, a_n$ to be relatively prime. In the following, $a_1, \dots, a_n$ are *arbitrary* positive integers.

*Research partially supported by NSF grant DMS-9972648.

It is clear that $p_A(t)$ is the coefficient of z^t in the generating function

$$G(z) = \frac{1}{(1-z^{a_1})\cdots(1-z^{a_n})}.$$

If we expand $G(z)$ by partial fractions, we see that $p_A(t)$ can be written in the form

$$\sum_{\lambda} P_{A,\lambda}(t)\lambda^t,$$

where the sum is over all complex numbers λ such that $\lambda^{a_i}=1$ for some i, and $P_{A,\lambda}(t)$ is a polynomial in t. The aim of this paper is to give an explicit formula for $P_{A,1}(t)$, which we denote by $P_A(t)$ and call the *polynomial part* of $p_A(t)$. It is easy to see that $P_A(t)$ is a polynomial of degree $n-1$. (More generally, the degree of $P_{A,\lambda}(t)$ is one less than the number of values of i for which $\lambda^{a_i}=1$.) It is well known [PS, Problem 27] that

$$p_A(t) = \frac{t^{n-1}}{(n-1)!\,a_1\cdots a_n} + O\left(t^{n-2}\right).$$

Our theorem is a refinement of this statement. We note that Israilov derived a more complicated formula for $P_A(t)$ in [I].

Let us define $Q_A(t)$ by $p_A(t) = P_A(t) + Q_A(t)$. From the partial fraction expansion above, it is clear that Q_A (and hence also p_A) is a *quasi-polynomial*, that is, an expression of the form

$$c_d(t)t^d + \cdots + c_1(t)t + c_0(t),$$

where $c_0,\ldots,c_d$ are periodic functions in t. (See, for example, Stanley [St, Section 4.4], for more information about quasi-polynomials.) In the special case in which the a_i are pairwise relatively prime, each $P_{A,\lambda}(t)$ for $\lambda \neq 1$ is a constant, and thus $Q_A(t)$ is a periodic function with average value 0, and this property determines $Q_A(t)$, and thus $P_A(t)$. Discussions of $Q_A(t)$ can be found, for example, in [BDR, I, K].

We define the *Bernoulli numbers* B_j by

$$\frac{z}{e^z-1} = \sum_{j\geq 0} B_j \frac{z^j}{j!} \tag{1}$$

(so $B_0=1, B_1=-\frac{1}{2}, B_2=\frac{1}{6}, B_4=-\frac{1}{30}$, and $B_n=0$ if n is odd and greater than 1.)

Theorem.

$$P_A(t) = \frac{1}{a_1\cdots a_n}\sum_{m=0}^{n-1}\frac{(-1)^m}{(n-1-m)!}\sum_{k_1+\cdots+k_n=m} a_1^{k_1}\cdots a_n^{k_n}\frac{B_{k_1}\cdots B_{k_n}}{k_1!\cdots k_n!}t^{n-1-m} \tag{2}$$

$$= \frac{1}{a_1\cdots a_n}\sum_{m=0}^{n-1}\frac{(-1)^m}{(n-1-m)!}$$

$$\times \sum_{k_1+2k_2\cdots+mk_m=m}\frac{(-1)^{k_2+\cdots+k_m}}{k_1!\cdots k_m!}\left(\frac{B_1 s_1}{1\cdot 1!}\right)^{k_1}\cdots\left(\frac{B_m s_m}{m\cdot m!}\right)^{k_m} t^{n-1-m}, \tag{3}$$

where $s_i = a_1^i + \cdots + a_n^i$.

Proof. As noted earlier, $p_A(t)$ is the coefficient of z^t in the generating function

$$G(z) = \frac{1}{(1-z^{a_1})\cdots(1-z^{a_n})}.$$

Hence if we let $f(z) = G(z)/z^{t+1}$ then $p_A(t) = \operatorname{Res}(f(z), z=0)$. As in [BDR], we use the residue theorem to derive a formula for $p_A(t)$. Since clearly $\lim_{R\to\infty} \int_{|z|=R} f(z)\,dz = 0$,

$$p_A(t) = -\operatorname{Res}(f(z), z=1) - \sum \operatorname{Res}(f(z), z=\lambda).$$

Here the sum is over all nontrivial $a_1, \ldots, a_n$th roots of unity λ. It is not hard to see that $\operatorname{Res}(f(z), z=\lambda)$ may be expressed in the form $u_\lambda(t)\lambda^{-t}$ for some polynomial $u_\lambda(t)$, and thus it follows from our earlier discussion that $-\operatorname{Res}(f(z), z=\lambda) = P_{A,\lambda^{-1}}(t)\lambda^{-t}$. In particular,

$$P_A(t) = -\operatorname{Res}(f(z), z=1).$$

To compute this residue, note that

$$\operatorname{Res}(f(z), z=1) = \operatorname{Res}(e^z f(e^z), z=0),$$

so that

$$P_A(t) = -\operatorname{Res}\left(\frac{e^{-tz}}{(1-e^{a_1 z})\cdots(1-e^{a_n z})}, z=0\right). \tag{4}$$

The coefficient of t^{n-1-m} in $P_A(t)$ is by (4) the coefficient of z^{-n+m} in

$$\frac{(-1)^{n-m}}{(n-1-m)!} \cdot \frac{1}{(1-e^{a_1 z})\cdots(1-e^{a_n z})},$$

which is the coefficient of z^m in

$$\frac{(-1)^m}{(n-1-m)!\,a_1\cdots a_n} B(a_1 z)\cdots B(a_n z), \tag{5}$$

where $B(z) = z/(e^z-1)$, and this implies (2).

To prove (3), we first note that

$$\log\left(\frac{z}{e^z-1}\right) = \sum_{j\geq 1} (-1)^{j-1} \frac{B_j}{j} \frac{z^j}{j!},$$

as can easily be proved by differentiating both sides. Then

$$\begin{aligned} B(a_1 z)\cdots B(a_n z) &= \exp \sum_{j\geq 1} (-1)^{j-1} \frac{B_j s_j}{j} \frac{z^j}{j!} \\ &= \prod_{j\geq 1} \exp\left((-1)^{j-1} \frac{B_j s_j}{j} \frac{z^j}{j!}\right). \end{aligned} \tag{6}$$

Since $B_{2i+1} = 0$ for $i > 0$, $(-1)^{j-1}B_j = -B_j$ for $j > 1$, and (3) follows from (5) and (6). □

Remark. It is possible to avoid the use of complex analysis and give a purely formal power series proof of the theorem. We indicate here how this can be done. We work with formal Laurent series, which are power series with finitely many negative powers of the variable. If $F(z) = \sum_i u_i z^i$ is a formal Laurent series (u_i is nonzero for only finitely many negative values of i) then the *residue* of $F(z)$ is $\operatorname{res} F(z) = u_{-1}$. An elementary fact about formal Laurent series is the change of variables formula for residues: If $g(z)$ is a formal power series with $g(0) = 0$ and $g'(0) \neq 0$ then

$$\operatorname{res} F(z) = \operatorname{res} F(g(z))g'(z).$$

(See, for example, Goulden and Jackson [GJ, p. 15].)

By partial fractions, we have

$$G(z) = \frac{1}{(1 - z_1^a) \cdots (1 - z^{a_m})} = \frac{c_1}{1-z} + \cdots + \frac{c_m}{(1-z)^m} + R(z),$$

where $R(z)$ is a rational function of z with denominator not divisible by $1 - z$. It follows from our earlier discussion that

$$\sum_{t=0}^{\infty} P_A(t) z^t = \frac{c_1}{1-z} + \cdots + \frac{c_m}{(1-z)^m}$$

and thus

$$P_A(t) = \sum_{l=1}^{\infty} c_l \binom{t+l-1}{l-1},$$

where we take c_l to be 0 for $l > m$. Now let $U(z) = G(1 - z)$. Then

$$\begin{aligned} U(z) &= \frac{1}{(1 - (1-z)^{a_1}) \cdots (1 - (1-z)^{a_m})} \\ &= \frac{c_1}{z} + \cdots + \frac{c_m}{z^m} + R(1 - z), \end{aligned}$$

where $R(1-z)$ has a formal power series expansion (with no negative powers of z), and thus $c_l = \operatorname{res} z^{l-1}U(z)$. Note that this holds for all $l \geq 1$, since for $l > m$, $c_l = \operatorname{res} z^{l-1}U(z) = 0$.

Then

$$P_A(t) = \sum_{l=1}^{\infty} c_l \binom{t+l-1}{l-1} = \operatorname{res} \frac{U(z)}{z} \sum_{l=1}^{m} z^l \binom{t+l-1}{l-1} = \operatorname{res} \frac{U(z)}{(1-z)^{t+1}}.$$

We now apply the change of variables formula with $g(z) = 1 - e^z$ and we obtain

$$\begin{aligned} P_A(t) &= -\operatorname{res} \frac{U(1 - e^z)}{e^{tz}} \\ &= -\operatorname{res} \frac{e^{-tz}}{(1 - e^{a_1 z}) \cdots (1 - e^{a_m z})}, \end{aligned}$$

which is (4), and the proof continues as before.

References

[BDR] M. Beck, R. Diaz, S. Robins, The Frobenius problem, rational polytopes, and Fourier–Dedekind sums, to appear in *J. Number Theory.*

[GJ] I. P. Goulden and D. M. Jackson, *Combinatorial Enumeration*, Wiley, New York, 1983.

[I] M. I. Israilov, Numbers of solutions of linear Diophantine equations and their applications in the theory of invariant cubature formulas, *Sibirsk. Mat. Zh.* **22** (1981), no. 2, 121–136, 237. English translation: *Siberian Math. J.* **22** (1981), no. 2, 260–273.

[K] T. Komatsu, The number of solutions of the Diophantine equation of Frobenius, to appear in *J. Théor. Nombres Bordeaux.*

[PS] G. Pólya and G. Szegő, *Aufgaben und Lehrsätze aus der Analysis*, Springer-Verlag, Berlin, 1925.

[R] J. L. Ramirez Alfonsin, The diophantine Frobenius problem, *Report No. 00893*, Forschungsinstitut für diskrete Mathematik, Universität Bonn (2000).

[Se] E. S. Selmer, On the linear diophantine problem of Frobenius, *J. reine angew. Math.* **293/294** (1977), 1–17.

[SÖ] S. Sertöz, A. Özlük, On the number of representations of an integer by a linear form, *İstanbul Üniv. Fen Fak. Mat. Derg.* **50** (1991), 67–77.

[St] R. P. Stanley, *Enumerative Combinatorics, Vol. 1*, Wadsworth & Brooks/Cole, Monterey, California, 1986.