An extension of the Frobenius coin-exchange problem [1]

Matthias Beck and Sinai Robins[2]

Dedicated to the memory of Robert F. Riley

1 Introduction

Given a set of positive integers $A = \{a_1, \dots, a_d\}$ with $\gcd(a_1, \dots, a_d) = 1$, we call an integer n *representable* if there exist nonnegative integers $m_1, \dots, m_d$ such that

$$n = m_1 a_1 + \cdots + m_d a_d \, .$$

In this paper, we discuss the *linear diophantine problem of Frobenius*: namely, find the largest integer which is not representable. We call this largest integer the *Frobenius number* $g(a_1, \dots, a_d)$.

One fact which makes this problem attractive is that it can be easily described, for example, in terms of coins of denominations $a_1, \dots, a_d$; the Frobenius number is the largest amount of money which cannot be formed using these coins.

The following "folklore" theorem has long been known (probably at least since Sylvester [9]).

Theorem 1. *$g(a, b) = ab - a - b$.*

For $d \geq 3$, the quest for general formulas has so far been unsuccessful. For the case $d = 2$, Sylvester [9] proved the following result.

Theorem 2 (Sylvester). *For $A = \{a, b\}$, exactly half of the integers between 1 and $(a-1)(b-1)$ are representable.*

Here we introduce and study a more general problem, a natural extension of the Frobenius problem, which seems to be new.

Definition 1. *We say that n is* k-representable *if n can be represented in the form*

$$n = m_1 a_1 + \cdots + m_d a_d$$

(where $m_1, \dots, m_d$ are again nonnegative integers) in exactly k ways.

In terms of coins, we can exchange the n pennies in exactly k different ways in terms of the given coin denominations. It is not hard to convince ourselves that—because the numbers in A are relatively prime—eventually every integer can be represented in more than k ways, for any k. Our extension of the Frobenius number is captured by the following definition:

[1] Revised version of 6/13/2002.

[2] The second author is supported by the NSA Young Investigator Grant MSPR-OOY-196.

Definition 2. *$g_k(a_1, \ldots, a_d)$ is the smallest integer beyond which every integer is represented more than k times.*

This is a natural generalization of the concept of the Frobenius number, as

$$g(a_1, \ldots, a_d) = g_0(a_1, \ldots, a_d) \ .$$

As to be expected, the study of g_k is extremely complicated for $d \geq 3$. There is an analogy here with k-representable integers and the classic problem of finding the number of representations of an integer as a sum of 4 squares, for example. However, the methods here are different. In this paper we concentrate on the case $d = 2$, that is, $A = \{a, b\}$, and present the following results.

Theorem 3. *$g_k(a, b) = (k + 1)ab - a - b$.*
Theorem 4. *Given $k \geq 2$, the smallest k-representable integer is $ab(k - 1)$.*
Theorem 5. *There are exactly $ab - 1$ integers which are uniquely representable. Given $k \geq 2$, there are exactly ab k-representable integers.*

Theorem 3 is a direct generalization of Theorem 1. Theorem 4 is meaningless for $k = 0$ and trivial for $k = 1$: the smallest representable integer is $\min(a, b)$. Theorem 5 extends Theorem 2 for $k > 0$.

2 The restricted partition function

One approach to the Frobenius problem and its generalizations is through the study of the *restricted partition function*

$$p_A(n) = \# \left\{ (m_1, \ldots, m_d) \in \mathbb{Z}^d : \ \text{all } m_j \geq 0, \ m_1a_1 + \cdots + m_da_d = n \right\} \ ,$$

the number of partitions of n using only the elements of A as parts. In view of this function, $g_k(a_1, \ldots, a_d)$ is the smallest integer such that for every $n > g_k(a_1, \ldots, a_d)$ we have $p_A(n) > k$.

It is well known [3, 5] that

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

In particular,

$$p_{\{a,b\}}(n) = \frac{n}{ab} + c(n) \ ,$$

where $c(n) = O(1)$. In fact, [11, p. 99] gives a nice argument that $c(n)$ is periodic in n with period ab, based on the generating function

$$\frac{1}{(1 - x^a)(1 - x^b)} \ ,$$

the coefficient of x^n of which is equal to $p_{\{a,b\}}(n)$. This argument can be carried even further to give the following little-known formula.

Theorem 6 (Popoviciu). *Suppose a and b are relatively prime positive integers, and n is a positive integer. Then*

$$p_{\{a,b\}}(n) = \frac{n}{ab} - \left\{ \frac{b^{-1}n}{a} \right\} - \left\{ \frac{a^{-1}n}{b} \right\} + 1 \ .$$

Here $\{x\} = x - \lfloor x \rfloor$ denotes the fractional part of x, $a^{-1}a \equiv 1 (\operatorname{mod} b)$, and $b^{-1}b \equiv 1 (\operatorname{mod} a)$.

The earliest reference to this result that we are aware of is [7]; the formula has since been resurrected at least twice [8, 10].

Instead of giving another proof of this theorem, we invite the reader to a scenic tour through the following modularized set of exercises, which lead to a—as far as we are aware of—new proof of Theorem 6. Consider the function

$$f(z) = \frac{1}{(1-z^a)\,(1-z^b)\,z^{n+1}} \ .$$

1. Compute the residues at all non-zero poles of f, and verify that $\operatorname{Res}(f(z), z=0) = p_{\{a,b\}}(n)$.
2. Use the residue theorem to derive an identity for $p_{\{a,b\}}(n)$. (Integrate f around a circle with center 0 and radius R, and show that this integral vanishes as $R \to \infty$.)
3. Verify that for $b = 1$,
$$\begin{aligned} p_{\{a,1\}}(n) &= \# \left\{ (m_1, m_2) \in \mathbb{Z} : m_1, m_2 \geq 0, \ m_1 a + m_2 = n \right\} \\ &= \# \left(\left[0, \frac{n}{a} \right] \cap \mathbb{Z} \right) = \frac{n}{a} - \left\{ \frac{n}{a} \right\} + 1 \ . \end{aligned}$$
4. Use this together with the identity found in 2. to obtain
$$\frac{1}{a} \sum_{\lambda^a = 1 \neq \lambda} \frac{1}{(1-\lambda)\lambda^n} = - \left\{ \frac{n}{a} \right\} + \frac{1}{2} - \frac{1}{2a} \ .$$
5. Verify that
$$\sum_{\lambda^a = 1 \neq \lambda} \frac{1}{(1-\lambda^b)\lambda^n} = \sum_{\lambda^a = 1 \neq \lambda} \frac{1}{(1-\lambda)\lambda^{b^{-1}n}}$$
and use this together with 4. above to simplify the identity found in 2.

Popoviciu's beautiful and simple formula leads to very short proofs of the results stated in the introduction.

Proof of Theorems 1 and 3. We will show that $p_{\{a,b\}}((k+1)ab - a - b) = k$ and that $p_{\{a,b\}}(n) > k$

for every $n > (k+1)ab - a - b$. First, by the periodicity of $\{x\}$,

$$\begin{aligned} &p_{\{a,b\}}((k+1)ab-a-b) = \\ &\quad = \frac{(k+1)ab-a-b}{ab} - \left\{\frac{b^{-1}((k+1)ab-a-b)}{a}\right\} - \left\{\frac{a^{-1}((k+1)ab-a-b)}{b}\right\} + 1 \\ &\quad = k+2-\frac{1}{b}-\frac{1}{a}-\left\{\frac{-b^{-1}b}{a}\right\}-\left\{\frac{-a^{-1}a}{b}\right\} \\ &\quad = k+2-\frac{1}{b}-\frac{1}{a}-\left\{\frac{-1}{a}\right\}-\left\{\frac{-1}{b}\right\} \\ &\quad = k+2-\frac{1}{b}-\frac{1}{a}-\left(1-\frac{1}{a}\right)-\left(1-\frac{1}{b}\right) = k\ . \end{aligned}$$

For any integer m, $\left\{\frac{m}{a}\right\} \le 1 - \frac{1}{a}$. Hence for any positive integer n,

$$p_{\{a,b\}}((k+1)ab-a-b+n) \ge \frac{(k+1)ab-a-b+n}{ab} - \left(1-\frac{1}{a}\right) - \left(1-\frac{1}{b}\right) + 1 = k + \frac{n}{ab} > k.$$

□

Proof of Theorem 2. We first claim that, if $n \in [1, ab-1]$ is not a multiple of a or b,

$$p_{\{a,b\}}(n) + p_{\{a,b\}}(ab-n) = 1\ . \tag{1}$$

This identity follows directly from Theorem 6:

$$\begin{aligned} p_{\{a,b\}}(ab-n) &= \frac{ab-n}{ab} - \left\{\frac{b^{-1}(ab-n)}{a}\right\} - \left\{\frac{a^{-1}(ab-n)}{b}\right\} + 1 \\ &= 2 - \frac{n}{ab} - \left\{\frac{-b^{-1}n}{a}\right\} - \left\{\frac{-a^{-1}n}{b}\right\} \\ &\overset{(\star)}{=} -\frac{n}{ab} + \left\{\frac{b^{-1}n}{a}\right\} + \left\{\frac{a^{-1}n}{b}\right\} \\ &= 1 - p_{\{a,b\}}(n)\ . \end{aligned}$$

Here, $(\star)$ follows from the fact that $\{-x\} = 1 - \{x\}$ if $x \notin \mathbb{Z}$. This shows that, for n between 1 and $ab-1$ and not divisible by a or b, exactly one of n and $ab-n$ is not representable. There are

$$ab - a - b + 1 = (a-1)(b-1) = g(a,b) + 1$$

integers between 1 and $ab-1$ which are not divisible by a or b. Finally, we note that $p_{\{a,b\}}(n) > 0$ if n is a multiple of a or b, by the very definition of $p_{\{a,b\}}(n)$. Hence the number of non-representable integers is $\frac{1}{2}(a-1)(b-1)$. □

Note that we proved even more. By (1), every positive integer less than ab has at most one representation. Hence, the representable integers in the above theorem are *uniquely* representable.

Proof of Theorem 4. Let n be a nonnegative integer. Then

$$\begin{aligned} p_{\{a,b\}}(ab(k-1)-n) &= \\ &= \frac{ab(k-1)-n}{ab} - \left\{ \frac{b^{-1}(ab(k-1)-n)}{a} \right\} - \left\{ \frac{a^{-1}(ab(k-1)-n)}{b} \right\} + 1 \\ &= k - \frac{n}{ab} - \left\{ \frac{-b^{-1}n}{a} \right\} - \left\{ \frac{-a^{-1}n}{b} \right\} . \end{aligned} \tag{2}$$

If $n=0$, (2) equals k. If n is positive, we use $\{x\} \geq 0$ to see that

$$p_{\{a,b\}}(ab(k-1)-n) \leq k - \frac{n}{ab} < k . \qquad \square$$

All nonrepresentable positive integers lie, by definition, in the interval $[1, g(a,b)]$. It is easy to see that the smallest interval containing all uniquely representable integers is $[\min(a,b), g_1(a,b)]$. For $k \geq 2$, the corresponding interval always has length $2ab-a-b+1$, and the precise interval is given next.

Corollary. *Given $k \geq 2$, the smallest interval containing all k-representable integers is*

$$[g_{k-2}(a,b)+a+b, g_k(a,b)] .$$

Proof. By Theorems 3 and 4, the smallest integer in the interval is

$$ab(k-1) = g_{k-2}(a,b)+a+b .$$

The upper bound of the interval follows from the proof of Theorem 3. □

Proof of Theorem 5. First, in the interval $[1, ab]$, there are, by Theorems 2 and 4,

$$ab - \frac{(a-1)(b-1)}{2} - 1$$

1-representable integers. Because of the almost periodic behavior of the partition function

$$p_{\{a,b\}}(n+ab) = p_{\{a,b\}}(n) + 1 , \tag{3}$$

which follows directly from Theorem 6, we see that there are

$$\frac{(a-1)(b-1)}{2}$$

1-representable integers above ab. For $k \geq 2$, the statement follows by similar reasoning. □

3 Final remarks

Although the proofs we have given so far are simple, they rely on Popoviciu's formula (Theorem 6). It is worth mentioning that there exist even more "elementary" proofs of Theorems 3, 4, and 5.

We note that for all $d > 2$, generalized Dedekind sums [4] appear in the formulas for $p_A(n)$, which increases the complexity of the problem. The full details of these connections to Dedekind sums appear in [2].

We conclude with a few remarks regarding extensions of the above theorems to $d > 2$. Although no 'nice' formula similar to the one appearing in Theorem 1 is known for $d > 2$, there has been a huge effort devoted to giving bounds and algorithms for the Frobenius number [1]. Secondly, we remark that Theorem 2 does not extend in general; however, [6] gives necessary and sufficient conditions on the a_j's under which Theorem 2 does extend. The almost periodic behavior (3) of the partition function extends easily to higher dimensions [2]. We leave the reader with the following "exercise":

Unsolved problems. *Extend Theorems 3, 4, and 5 to* $d \geq 3$.

Acknowledgements. The authors are grateful to Mel Nathanson and Herb Wilf for helpful remarks and references on partition functions, and to Olivier Bordellès for pointing out the reference [7].

References

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

[2] Matthias Beck, Ricardo Diaz, and Sinai Robins, *The Frobenius problem, rational polytopes, and Fourier–Dedekind sums*, J. Number Theory (to appear 2002).

[3] Paul Erdös and Joseph Lehner, *The distribution of the number of summands in the partitions of a positive integer*, Duke Math. J. **8** (1941), 335–345. MR 3,69a

[4] Ira M. Gessel, *Generating functions and generalized Dedekind sums*, Electron. J. Combin. **4** (1997), no. 2, Research Paper 11, approx. 17 pp. (electronic), The Wilf Festschrift (Philadelphia, PA, 1996). MR 98f:11032

[5] Melvyn B. Nathanson, *Partitions with parts in a finite set*, Proc. Amer. Math. Soc. **128** (2000), no. 5, 1269–1273. MR 2000j:11152

[6] Albert Nijenhuis and Herbert S. Wilf, *Representations of integers by linear forms in nonnegative integers.*, J. Number Theory **4** (1972), 98–106. MR 44 #5274

[7] Tiberiu Popoviciu, *Asupra unei probleme de patitie a numerelor*, Acad. Republicii Populare Romane, Filiala Cluj, Studii si cercetari stiintifice **4** (1953), 7–58.

[8] Sinan Sertoz, *On the number of solutions of the Diophantine equation of Frobenius*, Diskret. Mat. **10** (1998), no. 2, 62–71. MR 2000a:11049

[9] J. J. Sylvester, *Mathematical questions with their solutions*, Educational Times **41** (1884), 171–178.

[10] Amitabha Tripathi, *The number of solutions to $ax + by = n$*, Fibonacci Quart. **38** (2000), no. 4, 290–293. MR 2001d:11036

[11] Herbert S. Wilf, *generatingfunctionology*, second ed., Academic Press Inc., Boston, MA, 1994. MR 95a:05002

Department of Mathematical Sciences
Binghamton University
Binghamton, NY 13902-6000
matthias@math.binghamton.edu

Department of Mathematics
Temple University
Philadelphia, PA 19122
srobins@math.temple.edu