JP Jour. Algebra, Number Theory & Appl. **5**(1) (2005), 147-161

THE LINEAR DIOPHANTINE PROBLEM OF FROBENIUS

JOSEPH BAK

Department of Mathematics, City College of New York
138*th Street and Convent Avenue, New York, N. Y.* 10031, *U.S.A.*

Abstract

If $S = \{a_1, a_2, ..., a_n\}$ is a set of relatively prime positive integers, it is well known that any sufficiently large integer can be expressed as a nonnegative integral combination of the elements of S. The Frobenius problem consists of determining how large is sufficiently large. That is, find the smallest possible integer $L(a_1, a_2, ..., a_n)$ with the property that any number greater than or equal to it can be expressed as a nonnegative integral combination of $a_1, a_2, ..., a_n$. We review two classical approaches to the problem, and offer a third one. We then apply this latter approach to obtain simplified proofs for several known results and to obtain some new results.

1. Introduction

Suppose a and b are relatively prime positive integers. We will say that an integer is *representable by a and b* if it can be expressed in the form $xa + yb$, where x and y are nonnegative integers. It has been known for at least a century, and probably much longer, that all sufficiently large positive integers are representable by a and b. (Thus, a post-office with only two different stamps can still give exact postage as long as the stamps have relatively prime values and the postage exceeds a certain minimum.) To be more precise, and for future reference, let

2000 Mathematics Subject Classification: 11A07, 11D04.

Key words and phrases: Frobenius number.

Received November 9, 2004

$g(a, b)$ = the largest integer *not* representable by a and b;

$L(a, b) = 1 + g(a, b)$ = the smallest number such that all numbers greater than or equal to it are representable;

$N(a, b)$ = the total number of positive integers not representable by a and b.

Then

$$L(a, b) = (a - 1)(b - 1) \tag{1}$$

and

$$N(a, b) = (a - 1)(b - 1)/2. \tag{2}$$

It is difficult to identify the first known proof of (1). Many authors have credited Sylvester, citing [16, p. 21]. In the cited article, however, Sylvester simply poses the question of proving (2), and a solution is given by W. J. Curran Sharp. Neither the question nor the solution makes any reference to (1), in spite of the obvious connection between the two formulae. Still, (1) has been known for some time. In fact, Frobenius (1849-1917) repeatedly raised in his lectures the question of generalizing the result to a collection of relatively prime positive integers $a_1, a_2, ..., a_n$ with $n > 2$ [3, p. 215]. This has come to be known as the linear diophantine problem of Frobenius.

We will indicate two proofs of (1) in Sections 3 and 4. We begin, however, by reviewing some of the classical results regarding the Frobenius problem.

Suppose then that $S = \{a_1, a_2, ..., a_n\}$, $n > 2$, represents a set of relatively prime integers. As before, we will say that m is representable by S if there exist nonnegative integers $x_1, x_2, ..., x_n$ such that $m = x_1a_1 + x_2a_2 + \cdots + x_na_n$. Based on the known result for $n = 2$, it is fairly easy to prove that all sufficiently large integers are representable by S. The Frobenius problem consists of finding $L(S)$, the smallest integer such that all integers greater or equal to it are representable by S.

We will refer to $L(S)$ as the Frobenius number, although some authors use this term to refer to $g(S) = L(S) - 1$, the greatest integer *not* representable by S.

Note that if any element of S can be expressed as a nonnegative integral combination of the other elements, its presence in S has no effect on the Frobenius number $L(S)$. For that reason, we will assume that S is *independent* in the following sense:

Definition. $S = \{a_1, a_2, ..., a_n\}$ is *independent* if no element of S can be expressed as a nonnegative integral combination of the other elements.

The Frobenius problem has not been completely solved, and the available results suggest that no simple formula may be possible, even for $n = 3$. Still, there have been many partial results.

Several authors ([5], [17]) obtained upper and/or lower bounds for $L(S)$. Still others ([6], [14]) devised efficient algorithms to determine $L(S)$ for a given set S. Finally, explicit formulae have been obtained for $L(S)$ under certain additional hypotheses. In the next section, we consider Johnson's approach, which yields both a general algorithm and certain explicit formulae for $n = 3$. We then consider the approach of Brauer and Shockley, which has led to some of the most general results to date for arbitrary n. Each of the two approaches hinges on a characterization for $g(S)$. The remainder of the paper deals with the implications of a third approach, which rests on an extremely simple characterization for $L(S)$.

2. Johnson's Algorithm for $n = 3$

Before obtaining his algorithm for $g(S)$, Johnson first proved the following lemma (adapted to our notation) [9, p. 391].

Lemma 1. *Suppose* $S = \{a_1, a_2, a_3\}$ *is relatively prime and* $(a_2, a_3) = d$, *so that* $a_2 = db_2$, $a_3 = db_3$, *and* $(b_2, b_3) = 1$. *Then*

$$g(S) = dg(a_1, b_2, b_3) + (d - 1)a_1.$$

By applying the lemma three times (at most) one can reduce the problem of finding $g(S)$ for any set of relatively prime integers to the corresponding problem for a set of *pairwise* relatively prime integers.

To find $g(S)$ for independent, pairwise relatively prime sets S, Johnson focused on the following characterization of $g(S)$.

Proposition 1. *With S as above, there are at most two positive integers, x, not representable by S, but such that $x + a_i$ is representable for $i = 1, 2$ and 3. Hence, if g_1 and g_2 are those two integers, $g(S) = \max\{g_1, g_2\}$.*

Johnson also presented the following algorithm to find g_1 and g_2:

For each $i = 1, 2$ and 3, let $L_i a_i$ be the smallest multiple of a_i which is a nonnegative integral combination of the other two elements of S. Find the unique coefficients L_i, x_{ij} and x_{ik} satisfying

$$L_i a_i = x_{ij} a_j + x_{ik} a_k, \text{ for } (ijk) = \text{ a cyclic permutation of (123).} \tag{3}$$

Then g_1 and g_2 are given by

$$g_1 = L_i a_i + x_{jk} a_k - a_1 - a_2 - a_3; \quad g_2 = L_i a_i + x_{kj} a_j - a_1 - a_2 - a_3, \tag{4}$$

for any value of i.

As an example, suppose $S = \{a_1, a_2, a_3\} = \{7, 11, 24\}$. Then the matrix of nonzero coefficients for the system of equations (3), written in homogeneous form, is

7	11	24
– 5	1	1
1	– 5	2
4	4	– 3

Applying (4) with $i = 1$, $g(S) = \max\{g_1, g_2\} = \max\{35 + 48 - 42, 35 + 44 - 42\} = 41$. Note that the same result could have been obtained using $i = 2$ or $i = 3$.

Johnson also described an efficient algorithm for finding all the coefficients in equations (3).

Finally, Johnson noted that the algorithm described in (3) and (4) can be applied to obtain explicit formulae for $g(S)$ in certain special cases. In particular, he showed that if $S = \{a, a + 1, a + b\}$, and if the unique

representation of a in the form $a = kb - u$, $0 \le u < b$ has $u \le k + 1$, then

$$g(S) = \begin{cases} (k + b - 2 - u)a - 1 & \text{if } u \le 1 \\ [(a + 1)/b](a + b) + (b - 3)a - 1 & \text{if } u > 1 \end{cases}$$

[9, p. 398]. This improved a similar result of Roberts [13], obtained under stronger hypotheses.

3. The Approach of Brauer and Shockley

In place of Johnson's characterization for $g(S)$, given in Proposition 1, Brauer and Shockley offered the following: As before, assume that $S = \{a_1, a_2, ..., a_n\}$ is a set of relatively prime positive integers.

Proposition 2. *For each residue class w modulo a_1 there are numbers representable by $S - \{a_1\}$. Denote the minimum for each w by r_w, and let r be the maximum of these minima. Then $g(S) = r - a_1$* [3, p. 217].

The proof of the proposition is almost immediate. Numbers in each residue class $w \pmod{a_1}$ are representable by S if and only if they are greater than or equal to r_w. Hence the largest nonrepresentable number is $r - a_1$.

Brauer and Shockley also proved the following generalization of Lemma 1:

Lemma 2. *Suppose $S = \{a_1, a_2, ..., a_n\}$ is a set of relatively prime integers and $T = \{a_1, ca_2, ca_3, ..., ca_n\}$, with c relatively prime to a_1. Then*

$$g(T) = cg(S) + (c - 1)a_1 \quad \text{[3, p. 216].} \tag{5}$$

As in Proposition 2, a_1 does not necessarily have to be the smallest element of S, although it is often applied to that situation. Also, while the lemma was actually stated for the case where $\gcd(a_2, a_3, ..., a_n) = 1$, this is not a necessary hypothesis.

Interestingly, although Brauer and Shockley proved the above result without any reference to Proposition 2, it can be derived as a corollary of

that proposition. For suppose that the set of values r_w representing the smallest members of each residue class mod a_1 are given by linear combinations of the form $\sum x_{iw}a_i$, $(w = 1, 2, ..., a_1 - 1; i = 2, 3, ..., n)$. Then the corresponding values using elements of $T - \{a_1\}$ would be the set of linear combinations of the form $\sum cx_{iw}a_i$. Thus $g(T) = c[g(S) + a_1] - a_1$.

In a truly seminal article, Selmer [15] showed how Proposition 2 can be applied to obtain elegant derivations of the Frobenius number under a variety of hypotheses. The following three examples show the wide range of these applications.

(i) The fundamental result of formula (1): $L(a, b) = (a - 1)(b - 1)$ can be proven by observing that the minimum representatives of each nonzero residue class mod a, expressible as positive integral combinations of b, are obviously given by $b, 2b, ..., (a - 1)b$. Hence $g(S) = (a - 1)b - a$, and $L(a, b) = (a - 1)(b - 1)$.

(ii) Johnson's formula for $L(S)$, for $S = \{a, a + 1, a + b\}$, can be extended to obtain explicit formulae for more general sets of three elements [15, p. 4]. In fact, Selmer's method serves as the foundation for a very elegant algorithm which determines $L(S)$, for all sets of three elements, and also provides simple explicit formulae under additional hypotheses [14, pp. 172-173].

(iii) Suppose $S = \{a_0, a_1, ..., a_k\} = \{a, ma + d, ma + 2d, ..., ma + kd\}$. Then $L(S) = ma(1 + [(a - 2)/k]) + (d - 1)(a - 1)$. This result, due originally to Lewin [11], generalized earlier results regarding arithmetic sequences. We offer an alternative proof and a further generalization in Section 5.

4. A Uniquely Simple Characterization of $L(S)$

While Proposition 2 offers a simple and fruitful characterization of $g(S)$, the following characterization of $L(S)$ is even more obvious, and offers an additional approach in the pursuit of the Frobenius number.

We will say that a number m, representable by S, is *reducible* if $m - 1$ is also representable by S. Then the following proposition is immediately obvious:

Proposition 3. *$L(S)$ is the largest integer representable by S which is not reducible.*

Surprisingly, this elementary proposition affords both simplified proofs and extensions of solutions to the Frobenius problem in many cases. Examples of these are given in the next three sections. First, however, we will show how Proposition 3 leads to a straightforward proof of the basic formula (1). To that end, we will also use what may be called a "descent algorithm", and the following variation of ordinary mathematical induction:

Lemma 3. *Suppose a proposition $P(n)$ is true for an infinite number of positive integers n. We will denote this as $P(\infty)$. Suppose, moreover, that for $n > n_0$, $P(n) \Rightarrow P(n-1)$. Then $P(n)$ is true for all integers $n \geq n_0$.*

To prove formula (1), suppose a and b are relatively prime, and let $P(n)$ denote the proposition that n is representable by a and b. $P(\infty)$ is obviously true. By the Euclidean algorithm, there exist integers j and k such that

$$ja + kb = 1.$$

Since j and k cannot both be positive (nor both negative), it follows that there exist positive integers r, s, t, and u such that

$$ra - sb = 1; \quad 0 < r < b,\ 0 < s < a \tag{6}$$

and

$$tb - ua = 1; \quad 0 < t < a,\ 0 < u < b. \tag{7}$$

Note that the double inequality for r implies the corresponding one for s and the double inequality for t implies the one for u. With the given restrictions, it is easy to see that r, s, t, and u are uniquely determined. Finally, note that (6) and (7) are equivalent. For example, (6) implies that $(r-b)a - (s-a)b = 1$, giving the following reformulation of (7):

$$(a-s)b - (b-r)a = 1; \quad r \text{ and } s \text{ as in (6).} \tag{8}$$

Identities (6) and (8) can be viewed as equations for "trading down". Suppose we think of a and b as the denominations of certain stamps.

Then (6) shows that ra-stamps can be exchanged for sb-stamps with a net value exactly one cent less. Similarly (8) shows that $(a-s)b$-stamps can be traded down one cent for $(b-r)a$-stamps.

To complete the proof of (1), let $n_0 = (a-1)(b-1)$, and assume $P(n)$ for some $n > n_0$, i.e., assume

$$n = xa + yb; \quad x, y \geq 0.$$

If $x \geq r$, $P(n-1)$ follows from (6):

$$n - 1 = (x - r)a + (y + s)b.$$

Similarly, if $y \geq a - s$, $P(n-1)$ follows from (8):

$$n - 1 = (x + b - r)a + (y - a + s)b.$$

Moreover, since $n > n_0$, either $x \geq r$ or $y \geq a - s$. Otherwise,

$$n = xa + yb \leq (r-1)a + (a - s - 1)b = ra - sb + ab - a - b = n_0.$$

Thus, by Lemma 3, $P(n)$ is true for all $n \geq n_0$. Finally, to show that $n_0 = L(a, b)$, we need to show that $n_0 - 1$ is not representable by a and b. Assuming then that

$$n_0 - 1 = xa + yb$$

and subtracting from the identity

$$n_0 = (r-1)a + (a - s - 1)b$$

would yield

$$1 = (r - 1 - x)a + (a - s - 1 - y)b,$$

which is impossible since the coefficients in (6) and (8) are unique.

5. Almost Arithmetic Sequences and Arithmetic Sequences of Residues

One of the first sets, with more than 2 elements, for which the Frobenius number was determined, was a set of consecutive integers

[2, p. 301]. This result was later extended to arithmetic sequences [1, 13]. Finally, a formula for the Frobenius number was given for all sets of the form $S = \{a, ma + d, ma + 2d, ..., ma + kd\}$, denoted *almost arithmetic sequences* ([10], [15]). Using Proposition 3, we obtain a very straightforward proof of this result, along with further extensions.

Theorem 1. *Suppose* $S = \{a_0, a_1, ..., a_k\} = \{a, m_1a + d, m_2a + 2d, ..., m_ka + kd\}$, *where all the variables are positive integers such that* $\gcd(a, d) = 1$, $k \le a - 1$ *and* $m_1 \le m_2 \le \cdots \le m_k$.

I. *If* $m_k/m_j < k/j$ *for all* $j < k$, *and if* k *divides* $a - 1$, *then*

$$L(S) = a_k(a - 1)/k - a + 1. \tag{9}$$

II. (Lewin) *If* $m_1 = m_2 = \cdots = m_k = m$,

$$L(S) = ma(1 + [(a - 2)/k]) + (d - 1)(a - 1). \tag{10}$$

Note that the condition $\gcd(a, d) = 1$ is necessary to insure that S forms a set of relatively prime integers. The second condition: $k \le a - 1$ is necessary to assure that S is independent [15, p. 2]. *If* j *divides* k, the first condition in Case I is also necessary to insure that a_k is not superfluous. Otherwise, we could obtain a_k as $(k/j)(m_ja + jd) +$ a nonnegative integral multiple of a.

In Case I, our methods yield a simplified method for finding $L(S)$ even if k does not divide $a - 1$, but the condition is necessary to obtain the very compact formula (9). This will be discussed in the examples following the proof. In Case II, S forms an almost arithmetic sequence.

Proof of Theorem 1. Since $(a, d) = 1$, there exists c, $0 < c < a$, such that $cd \equiv 1 \pmod{a}$. Suppose $cd = ea + 1$. Then $cjd = jea + j$, for $j = 1, 2, ..., k$ and if $b_j = ca_j$,

$$b_j = cm_ja + jea + j.$$

Let $T = \{a, b_1, ..., b_k\}$. Since b_j is exactly one more than $b_{j-1} +$ a multiple of a if $j > 1$, and b_1 is one more than $(cm_1 + e)a$, the only

irreducible elements of T are multiples of a. Hence, $L(T)$ is a multiple of a, and $g(T)$ is the largest number congruent to $a-1 \pmod a$ which is not representable by T. It follows that $h = g(T) + a$ is the smallest number congruent to $a-1 \pmod a$ which is representable by T. To find h, note that $h = \min\{\sum x_j b_j \mid \sum x_j b_j \equiv a-1 \pmod a\}$, or

$$h = \min\{ca\sum m_j x_j + (ea+1)\sum jx_j \mid \sum jx_j \equiv a-1 \pmod a\}.$$

We now consider our two cases.

Case I. If k divides $a-1$, then h is obtained by taking $x_k = (a-1)/k$, and all other $x_j = 0$. This follows since $\sum jx_j \equiv a-1 \pmod a$ implies

$$\sum jx_j \geq a-1,$$

and because of the conditions on the coefficients m_j,

$$\sum m_j x_j \geq \sum (j/k) m_k x_j \geq (m_k/k)\sum jx_j \geq m_k(a-1)/k.$$

Hence

$$g(T) = b_k(a-1)/k - a = ca_k(a-1)/k - a.$$

According to (5), then, $g(S) = [g(T) - (c-1)a]/c = a_k(a-1)/k - a$, and Case I is proven.

Case II. In this case, since all the coefficients m_j are equal, h is obtained by taking $\sum jx_j = a-1$, with $\sum x_j$ as small as possible. Since $a-1 \geq k$,

$$a-1 = qk + r, \quad 0 \leq r < k,\ q \geq 1,$$

and h is found by taking $x_k = q = [(a-1)/k]$, $x_r = 1$ (if $r > 0$) and all other $x_i = 0$. The case $r = 0$ has already been covered in Case I, so we may assume $r > 1$. Hence

$$h = c(q+1)ma + ea(a-1) + a - 1,$$
$$g(T) = h - a = cm(q+1)a + cd(a-1) - a$$

and, according to Lemma 2,

$$g(S) = m(q+1)a + d(a-1) - a.$$

Note, then, that since $a-1 = qk + r$, $r > 0$,

$$q = [(a-1)/k] = [(a-2)/k]$$

which establishes (10) in a form which, according to (9), is also valid if $r = 0$. That is, if $a-1 = qk$, $[(a-2)/k] = q-1$, and if all $m_j = m$, both (9) and (10) give $L(S) = maq + (d-1)(a-1)$, so that (10) is valid in all cases.

Example 1. By a direct application of (9), if $S = \{13, 41, 56, 84\}$, $L(S) = 4(84) - 12 = 324$.

Example 2. Let $S = \{14, 45, 76, 93\}$. Note that in this case, k does *not* divide $a-1$. Nevertheless, since $d = 3$ and $5(3) \equiv 1 \pmod{14}$, we consider $T = \{14, 5(45), 5(76), 5(93)\}$. Using our previous ideas, then, $L(T)$ is a multiple of 14 and $g(T) = h - 14$, where

$$h = \min\{14(16x + 27y + 33z) + (x + 2y + 3z) \mid x + 2y + 3z = 13\}.$$

h is obtained by taking $z = 4$ and $x = 1$, so that

$$g(T) = 4(5)(93) + 5(45) - 14.$$

Finally, by Lemma 2, $g(S) = 4(93) + 45 - 14$, and $L(S) = 404$.

Example 3. Suppose S is any independent triple of the form $\{a, b, c\}$, where a and b are relatively prime, $a < b < c$, and $c \equiv 2b \pmod{a}$. If a is odd, then formula (9) is applicable, and if a is even, we can use an analogous argument to obtain

$$L(S) = \begin{cases} c(a-1)/2 - a + 1, & \text{if } a \text{ is odd} \\ b + c[(a-1)/2] - a + 1, & \text{if } a \text{ is even.} \end{cases}$$

We now consider sets more closely related to geometric sequences.

6. A Direct Calculation of $L(S)$, for $S = \{a, a+1, a+2, a+4\}$

Dulmage and Mendelsohn proved several interesting results concerning the relationship between the exponent of a primitive graph and the Frobenius number for the lengths of its circuits [4]. As an

application, using graph-theoretic methods, they determined $L(S)$ when S is of the form $\{a, a+1, a+2, a+k\}$; $k = 4,\ 5$, or 6. The results were later proven by purely number-theoretic arguments [15, pp. 7-9]. Again, the method of Proposition 3 offers a uniquely simple proof. We include the details for $k = 4$, although analogous proofs can also be given for $k = 5$ and $k = 6$.

Theorem 2 (Dulmage and Mendelsohn)**.** *If* $S = \{a, a+1, a+2, a+4\}$, *then*

$$L(S) = [a/4](a+1) + [(a+1)/4] + 2[(a+2)/4]. \tag{11}$$

Proof. Assume that n is representable by S and irreducible. Then, if

$$n = c_1a + c_2(a+1) + c_3(a+2) + c_4(a+4) \tag{12}$$

it follows that

(i) $c_2 = c_3 = 0$, and

(ii) either $c_1 = 0$ or $c_4 = 0$.

The latter derives from the observation that $a + (a+4)$ can be exchanged down for $(a+1) + (a+2)$. Hence n is either a multiple of a or a multiple of $(a+4)$, and $L(S) = \max\{n_1, n_2\}$, where n_1 is the largest irreducible multiple of a, and n_2 is the largest irreducible multiple of $(a+4)$.

As in the previous section, n_1 and n_2 can be determined as

$$n_1 = m_1 - a + 1, \quad n_2 = m_2 - a - 3,$$

where

m_1 is the smallest representable number congruent to $a - 1 \pmod a$;

m_2 is the smallest representable number congruent to $a + 3 \pmod{(a+4)}$.

According to (12), then,

$$m_1 = \min\{(c_2 + c_3 + c_4)a + (c_2 + 2c_3 + 4c_4) \mid c_2 + 2c_3 + 4c_4 \equiv (a-1) \bmod a\}$$

and, setting $a = (a + 4) - 4$, etc.,

$$m_2 = \min\{(c_1 + c_2 + c_3)(a + 4) - (4c_1 + 3c_2 + 2c_3) \mid$$
$$4c_1 + 3c_2 + 2c_3 \equiv 1 \bmod (a + 4)\}.$$

Since all the coefficients c_i must be nonnegative, m_1 is found by solving $c_2 + 2c_3 + 4c_4 = (a - 1)$, with c_4 as large as possible. Similarly, m_2 is found by solving $4c_1 + 3c_2 + 2c_3 = (a + 5)$, with c_1 as large as possible. The results, for the different possible values of $a \bmod 4$ are summarized in the chart below:

a mod 4	m_1	$n_1 = m_1 - a + 1$	m_2	$n_2 = m_2 - a - 3$	$L(S) = \max\{n_1, n_2\}$
0	$(a+1)+(a+2)$ $+((a-4)/4)(a+4)$	$a(a+4)/4$	$(a/4)a+(a+1)$ $+(a+2)$	$(a+4)a/4$	$a(a+4)/4$
1	$((a-1)/4)(a+4)$	$a(a-1)/4$	$((a+3)/4)a$ $+(a+2)$	$(a+4)(a-1)/4$	$(a+4)(a-1)/4$
2	$(a+1)$ $+((a-2)/4)(a+4)$	$a(a+2)/4$	$((a+2)/4)a$ $+(a+1)$	$(a+4)(a-2)/4$	$a(a+2)/4$
3	$(a+2)$ $+((a-3)/4)(a+4)$	$a(a+1)/4$	$((a+5)/4)a$	$(a+4)(a-3)/4$	$a(a+1)/4$

The expression for $L(S)$ in (11) derives from graph-theoretic considerations. Our formulae highlight the fact that $L(S)$ is always an integral multiple of either a or $a + 4$ (or both). A simple check shows, however, that the two expressions are equal in all four cases, and the proof is complete.

7. Sets of the form $\{a\} \cup \{m_j a + 2^j\}$ and of the form $\{a\} \cup \{a + 2^j d\}$

Theorem 3. *Let* $S = \{a, m_0 a + 1, m_1 a + 2, \ldots, m_k a + 2^k\}$, *and assume that*

$$m_0 + m_1 + \cdots + m_{j-1} \le m_j < 2m_{j-1} \quad \text{for } j = 1, \ldots, k. \tag{13}$$

Then $L(S) = (b_0 m_0 + b_1 m_1 + \cdots + b_k m_k)a$, *where* $b_k = [(a-1)/2^k]$ *and* $b_{k-1} b_{k-2} \cdots b_0$ *is the binary representation of* $a - 1 \pmod{2^k}$.

Proof. Since $2^j = (1 + 2 + \cdots + 2^{j-1}) + 1$, it follows from the first inequality in (13) that every element of S, other than a, is reducible. Hence $L(S)$ must be a multiple of a. It follows that

$$L(S) = m - a + 1, \tag{14}$$

where $m = \min\{\sum c_j(m_j a + 2^j) | \sum c_j 2^j = a - 1\}$, or $m = \min\{\sum c_j m_j a + a - 1 | \sum c_j 2^j = a - 1\}$. According to the second inequality in (13), m is found by taking the coefficients c_j, for large j, as big as possible. Hence $c_k = b_k = [(a-1)/k]$ and $c_j = b_j$ for $j < k$. According to (14), then, the proof is complete.

Corollary. *Let* $S = \{a, a + d, a + 2d, ..., a + 2^k d\}$, *with* $\gcd(a, d) = 1$. *If* $d/a \geq k$, *then* $L(S) = (a-1)(d-1) + a\sum b_j$, *with* b_j *defined as above.*

Proof. As before, choose c so that $cd \equiv 1 \pmod a$, and assume $cd = ea + 1$. Then, $c(a + 2^j d) = (c + 2^j e)a + 2^j$. Let $n_j = c + 2^j e$. Then $n_j < 2n_{j-1}$ and $n_j - (n_0 + n_1 + \cdots + n_{j-1}) = e - (j-1)c \geq e - (k-1)c$. Since $ea = cd - 1$, $e/c = d/a - 1/(ac)$. Hence if $d/a \geq k$, $e/c \geq k - 1$, and $n_j \geq (n_0 + n_1 + \cdots + n_{j-1})$. According to Theorem 2, then, if

$$T = \{a, c(a + d), c(a + 2d), ..., c(a + 2^k d)\},$$

$$L(T) = (b_0 n_0 + b_1 n_1 + \cdots + b_k n_k)a = [\sum b_j(c + 2^j e)]a$$

$$= (a-1)(cd - 1) + (\sum b_j)ca,$$

$$g(S) = (1/c)[L(T) - 1 - (c-1)a] = (a-1)d - a + (\sum b_j)a, \text{ and}$$

$$L(S) = (a-1)(d-1) + (\sum b_j)a.$$

Example 1. If $S = \{17, 52, 87, 157\}$, then a direct application of the Corollary shows $L(S) = 16(34) + 4(17) = 612$.

Example 2. Let $S = \{14, 57, 157, 429\} = \{14, 4(14) + 1, 11(14) + 3, 30(14) + 9\}$. Then, arguing as in the proof of Theorem 3, $g(S) + 14 = 57c_0 + 157c_1 + 429c_2$, where $13 = c_2c_1c_0$ (base 3), and $L(S) = 630$.

References

[1] P. T. Bateman, Remark on a recent note on linear forms, Amer. Math. Monthly 65 (1958), 517-518.

[2] A. Brauer, On a problem of partitions, Amer. J. Math. 64 (1942), 299-312.

[3] A. Brauer and J. E. Shockley, On a problem of Frobenius, J. Reine Angew. Math. 211 (1962), 215-220.

[4] A. L. Dulmage and N. S. Mendelsohn, Gaps in the exponent set of primitive matrices, Illinois J. Math. 8 (1964), 642-656.

[5] P. Erdos and R. L. Graham, On a linear diophantine problem of Frobenius, Acta Arithm. 21 (1972), 399-408.

[6] H. Greenberg, Solution to a linear diophantine equation for nonnegative integers, J. Algorithms 9 (1988), 343-353.

[7] G. R. Hofmeister, Zu einem Problem von Frobenius, Norske Videnskabers Selskabs Skrifter 5 (1966), 1-37.

[8] M. Hujter and B. Vizvari, The exact solution to the Frobenius problem with three variables, J. Ramanujan Math. Soc. 2 (1987), 117-143.

[9] S. M. Johnson, A linear diophantine problem, Canad. J. Math. 12 (1960), 390-398.

[10] M. Lewin, On a problem of Frobenius for an almost consecutive set of integers, J. Reine Angew. Math. 273 (1975), 134-137.

[11] M. Lewin, An algorithm for a solution of a problem of Frobenius, J. Reine Angew. Math. 276 (1975), 68-82.

[12] J. B. Roberts, Interaction of cycles, Bulletin of Mathematical Biophysics 10 (1948), 123-129.

[13] J. B. Roberts, Note on linear forms, Proc. Amer. Math. Soc. 7 (1956), 465-469.

[14] O. J. Rodseth, On a linear diophantine problem of Frobenius, J. Reine Angew. Math. 301 (1978), 171-178.

[15] E. S. Selmer, On the linear diophantine problem of Frobenius, J. Reine Angew. Math. 293/294 (1977), 1-17.

[16] J. J. Sylvester, Mathematical questions with their solutions, Educational Times 41 (1884), 21.

[17] Y. Vitek, Bounds for a linear diophantine problem of Frobenius, II, Canad. J. Math. 28 (1976), 1280-1288.

■