

ON A LINEAR DIOPHANTINE PROBLEM OF FROBENIUS

Amitabha Tripathi

Department of Mathematics, Indian Institute of Technology, Hauz Khas, New Delhi - 110016, India
atripath@maths.iitd.ac.in

Received: 11/21/05, Revised: 4/17/06, Accepted: 1/1/06, Published: 1/2/06

Abstract

Let a_1, a_2, \dots, a_k be positive and pairwise coprime integers with product P . For each i , $1 \leq i \leq k$, set $A_i = P/a_i$. We find closed form expressions for the functions $g(A_1, A_2, \dots, A_k)$ and $n(A_1, A_2, \dots, A_k)$ that denote the *largest* (respectively, the *number of*) N such the equation

$$A_1x_1 + A_2x_2 + \dots + A_kx_k = N$$

has no solution in nonnegative integers x_i . This is a special case of the well-known *Coin Exchange Problem* of Frobenius.

1. Introduction

Given positive integers a_1, a_2, \dots, a_k , relatively prime, it is well-known that for all sufficiently large N the equation

$$a_1x_1 + a_2x_2 + \dots + a_kx_k = N \tag{1}$$

has a solution with nonnegative integers x_i . If we denote by $g(a_1, a_2, \dots, a_k)$ the *largest* integer N such that (1) has no solution in nonnegative integers, then it is a well-known result of Sylvester that $g(a_1, a_2) = a_1a_2 - a_1 - a_2$. The related functions $n(a_1, a_2, \dots, a_k)$ and $s(a_1, a_2, \dots, a_k)$ denote the number of positive integers N for which (1) has no solution and the sum of such integers, respectively. While it is well-known that $n(a_1, a_2) = (a_1 - 1)(a_2 - 1)/2$, the corresponding result $s(a_1, a_2) = (a_1 - 1)(a_2 - 1)(2a_1a_2 - a_1 - a_2 - 1)/12$ is more recent and less known [4]. Except when the a_i 's are in arithmetic progression [1, 5, 9, 15] or in certain other particular cases with three or more variables [2, 3, 7, 10, 11, 12, 13, 14], there is no closed form expression for either g or n . More information on this problem may be found in the recently published monograph [8].

The purpose of this note is to obtain a formula for the functions g and n in a special case. More specifically, we shall henceforth assume that the a_i 's are *pairwise* coprime with product P , and set $A_i = P/a_i$ for $1 \leq i \leq k$. We determine $g(A_1, A_2, \dots, A_k)$ and $n(A_1, A_2, \dots, A_k)$ by two methods. The first method uses a reduction formula while the second method is direct. We note that $g(A_1, A_2) = g(a_1, a_2)$ and $n(A_1, A_2) = n(a_1, a_2)$.

2. Main Results

For the sake of completeness, we prove two well-known results that help in evaluating the functions g and n in the general case.

Lemma 1 [3, 13]. Let $\gcd(a_1, a_2, \dots, a_k) = 1$, and for $1 \leq j \leq k - 1$, let m_j denote the *least* positive integer N congruent to $j \pmod{a_1}$ such that (1) has a solution in nonnegative integers. Then

$$(a) \quad g(a_1, a_2, \dots, a_k) = \max_{1 \leq j \leq a_1 - 1} m_j - a_1;$$

$$(b) \quad n(a_1, a_2, \dots, a_k) = \frac{1}{a_1} \sum_{j=1}^{a_1 - 1} (m_j - j) = \frac{1}{a_1} \sum_{j=1}^{a_1 - 1} m_j - \frac{a_1 - 1}{2}.$$

Proof.

- (a) From the definition of m_i it follows that $m_i - a_1$ is not representable by a_1, \dots, a_k in nonnegative integers for each i , $1 \leq i \leq k$. On the other hand, any N greater than each $m_i - a_1$ and congruent to $j \pmod{a_1}$ must be at least m_j , and hence representable by a_1, \dots, a_k in nonnegative integers.
- (b) Since the numbers congruent to $j \pmod{a_1}$ and not representable by a_1, \dots, a_k in nonnegative integers form an arithmetic progression with first term j , last term $m_j - a_1$ and common difference a_1 , their number is given by $(m_j - j)/a_1$. The second part of the lemma now easily follows. □

Lemma 2 [6, 11]. Let a_1, a_2, \dots, a_k be positive integers. If $\gcd(a_2, \dots, a_k) = d$ and $a_j = da'_j$ for each $j > 1$, then

$$(a) \quad g(a_1, a_2, \dots, a_k) = dg(a_1, a'_2, \dots, a'_k) + a_1(d - 1);$$

$$(b) \quad n(a_1, a_2, \dots, a_k) = dn(a_1, a'_2, \dots, a'_k) + \frac{1}{2}(a_1 - 1)(d - 1);$$

Proof. As in Lemma 1, for each j , $1 \leq j \leq a_1 - 1$, let m_j and m'_j denote the *least* positive integer congruent to $j \pmod{a_1}$ representable as a nonnegative linear combination of a_1, a_2, \dots, a_k and a_1, a'_2, \dots, a'_k , respectively. Since each such m_j and m'_j must also be representable as a nonnegative linear combination of a_2, \dots, a_k and of a'_2, \dots, a'_k , respectively, it follows that $\{m_j : 1 \leq j \leq a_1 - 1\} = \{dm'_j : 1 \leq j \leq a_1 - 1\}$. We now apply Lemma 1.

(a)

$$\begin{aligned} g(a_1, a_2, \dots, a_k) &= \max_{1 \leq j \leq a_1-1} m_j - a_1 \\ &= d \left(\max_{1 \leq j \leq a_1-1} m'_j - a_1 \right) + a_1(d-1) \\ &= d g(a_1, a'_2, \dots, a'_k) + a_1(d-1). \end{aligned}$$

(b)

$$\begin{aligned} n(a_1, a_2, \dots, a_k) &= \frac{1}{a_1} \sum_{j=1}^{a_1-1} m_j - \frac{1}{2}(a_1-1) \\ &= d \left(\frac{1}{a_1} \sum_{j=1}^{a_1-1} m'_j - \frac{1}{2}(a_1-1) \right) + \frac{1}{2}(a_1-1)(d-1) \\ &= d n(a_1, a'_2, \dots, a'_k) + \frac{1}{2}(a_1-1)(d-1). \end{aligned}$$

□

Theorem 1. Let a_1, a_2, \dots, a_k be pairwise coprime, positive integers with product P . Let $A_i = P/a_i$ for $1 \leq i \leq k$. Let σ_r denote the sum of the products of the a_i 's taken r at a time, so that $\sigma_k = P$ and $\sigma_{k-1} = A_1 + A_2 + \dots + A_k$. Then

- (a) $g(A_1, A_2, \dots, A_k) = (k-1)\sigma_k - \sigma_{k-1}$;
- (b) $n(A_1, A_2, \dots, A_k) = \frac{1}{2}\{(k-1)\sigma_k - \sigma_{k-1} + 1\}$.

Proof. This is a direct consequence of Lemma 2. We induct on k . If $k = 2$, these are just the well-known results cited above. We observe that A_k is a multiple of $A_j/a_k = A'_j$ for each $j \neq k$ since $A_j|a_k A_k = \sigma_k$ and $a_k|A_j$ if $j \neq k$.

(a)

$$\begin{aligned} g(A_1, A_2, \dots, A_k) &= a_k g \left(\frac{A_1}{a_k}, \frac{A_2}{a_k}, \dots, \frac{A_{k-1}}{a_k}, A_k \right) + A_k(a_k-1) \\ &= a_k g \left(\frac{A_1}{a_k}, \frac{A_2}{a_k}, \dots, \frac{A_{k-1}}{a_k} \right) + \sigma_k - A_k \\ &= a_k g(A'_1, A'_2, \dots, A'_{k-1}) + \sigma_k - A_k \\ &= (k-2)\sigma_k - (\sigma_{k-1} - A_k) + \sigma_k - A_k \text{ by Induction Hypothesis} \\ &= (k-1)\sigma_k - \sigma_{k-1}. \end{aligned}$$

(b)

$$\begin{aligned}
 n(A_1, A_2, \dots, A_k) &= a_k n\left(\frac{A_1}{a_k}, \frac{A_2}{a_k}, \dots, \frac{A_{k-1}}{a_k}, A_k\right) + \frac{1}{2}(a_k - 1)(A_k - 1) \\
 &= a_k n\left(\frac{A_1}{a_k}, \frac{A_2}{a_k}, \dots, \frac{A_{k-1}}{a_k}\right) + \frac{1}{2}\sigma_k - \frac{1}{2}a_k - \frac{1}{2}A_k + \frac{1}{2} \\
 &= a_k n(A'_1, A'_2, \dots, A'_{k-1}) + \frac{1}{2}\sigma_k - \frac{1}{2}a_k - \frac{1}{2}A_k + \frac{1}{2} \\
 &= \frac{1}{2}\{(k - 2)\sigma_k - (\sigma_{k-1} - A_k) + a_k + \sigma_k - a_k - A_k + 1\} \\
 &\quad \text{by Induction Hypothesis} \\
 &= \frac{1}{2}\{(k - 1)\sigma_k - \sigma_{k-1} + 1\}.
 \end{aligned}$$

□

The proof of Theorem 1 given above is based on Lemma 2. It is indeed possible to give an independent proof. Using the notation of Theorem 1, we give a

Second proof of Theorem 1. Let a_1, a_2, \dots, a_k be pairwise coprime, positive integers. Let σ_r denote the sum of the products of the a_i 's taken r at a time, and let $A_j = \sigma_k/a_j$ for $1 \leq j \leq k$. Then

$$g(A_1, A_2, \dots, A_k) = (k - 1)\sigma_k - \sigma_{k-1}.$$

Proof. If each $x_j \geq 0$ and

$$A_1x_1 + A_2x_2 + \dots + A_kx_k = (k - 1)\sigma_k - \sigma_{k-1}, \tag{2}$$

$A_jx_j \equiv -A_j \pmod{a_j}$, so that $x_j \geq a_j - 1$ since $\gcd(a_j, A_j) = 1$. But then

$$\sum_{j=1}^k A_jx_j \geq \sum_{j=1}^k A_j(a_j - 1) \geq k\sigma_k - \sigma_{k-1},$$

and (2) has no solution in nonnegative integers.

Since the $A_ix_i + A_jx_j = A_i(x_i + a_i) + A_j(x_j - a_j)$, and since $\gcd(A_1, A_2, \dots, A_k) = 1$, we can always write any N in the form $A_1x_1 + A_2x_2 + \dots + A_kx_k$ with $0 \leq x_j \leq a_j - 1$ for $1 \leq j \leq k - 1$. Now, if $N > (k - 1)\sigma_k - \sigma_{k-1}$ and we choose x_j as above, then

$$x_k = \frac{N - \sum_{j=1}^{k-1} A_jx_j}{A_k} > \frac{\sum_{j=1}^{k-1} A_j(a_j - x_j - 1)}{A_k} - 1 \geq -1.$$

Thus $x_k \geq 0$, and every N greater than $(k - 1)\sigma_k - \sigma_{k-1}$ is expressible as a nonnegative linear combination of the A_j 's. □

Lemma 3. Let a_1, a_2, \dots, a_k be pairwise coprime, positive integers, and let $A_j = \sigma_k/a_j$ for $1 \leq j \leq k$. If $p + q = g(A_1, A_2, \dots, A_k)$, then exactly one of the equations

$$A_1x_1 + A_2x_2 + \dots + A_kx_k = p \quad \text{and} \quad A_1x_1 + A_2x_2 + \dots + A_kx_k = q$$

is solvable in nonnegative integers x_j .

Proof. If both the equations had a solution, so would $g(A_1, A_2, \dots, A_k)$, contradicting its definition. Suppose $A_1x_1 + A_2x_2 + \dots + A_kx_k = p$ has no solution in nonnegative integers. Choose x_j such that $0 \leq x_j \leq a_j - 1$ for $1 \leq j \leq k - 1$. But then $x_k < 0$, and

$$q = (k - 1)\sigma_k - \sigma_{k-1} - p = \sum_{j=1}^{k-1} A_j(a_j - x_j - 1) + A_k(-x_k)$$

is expressible in the given form, proving the lemma. □

Corollary 1. Let a_1, a_2, \dots, a_k be pairwise coprime, positive integers. Let σ_r denote the sum of the products of the a_i 's taken r at a time, and let $A_j = \sigma_k/a_j$ for $1 \leq j \leq k$. Then

$$n(A_1, A_2, \dots, A_k) = \frac{1}{2}\{(k - 1)\sigma_k - \sigma_{k-1} + 1\}.$$

Proof. If we pair p with q whenever $p + q = g(A_1, A_2, \dots, A_k)$ and $p, q \geq 0$, by Lemma 1,

$$n(A_1, A_2, \dots, A_k) = \frac{1}{2}\{1 + g(A_1, A_2, \dots, A_k)\}.$$

The corollary now follows from Theorem 1. □

The evaluation of g given in Theorem 1 can also be derived by explicitly determining the set \mathcal{S}^* , introduced in [16], since $g(a_1, a_2, \dots, a_k)$ is the largest element in $\mathcal{S}^*(a_1, a_2, \dots, a_k)$. For positive and coprime integers a_1, a_2, \dots, a_k , let Γ^* denote the positive integers in the set $\{a_1x_1 + a_2x_2 + \dots + a_kx_k : x_j \geq 0\}$. Then

$$\mathcal{S}^*(a_1, a_2, \dots, a_k) := \{n \notin \Gamma^* : n + \Gamma^*\} \subseteq \{m_j - a_1 : 1 \leq j \leq a_1 - 1\}.$$

Moreover,

$$m_j - a_1 \in \mathcal{S}^*(a_1, a_2, \dots, a_k) \iff m_j + m_i > m_{j+i} \text{ for } 1 \leq i \leq a_1 - 1. \tag{3}$$

We refer to [16] for the more notations and results. With the notations above, we show that $\mathcal{S}^*(A_1, A_2, \dots, A_k) = \{(k - 1)\sigma_k - \sigma_{k-1}\}$ for each $k \geq 2$. Since $g(a_1, a_2, \dots, a_k) \in \mathcal{S}^*(a_1, a_2, \dots, a_k)$, this further verifies the first result of Theorem 1.

Theorem 2. Let a_1, a_2, \dots, a_k be pairwise coprime, positive integers. Let σ_r denote the sum of the products of the a_i 's taken r at a time, and let $A_j = \sigma_k/a_j$ for $1 \leq j \leq k$. Then

$$\mathcal{S}^*(A_1, A_2, \dots, A_k) = \{(k - 1)\sigma_k - \sigma_{k-1}\}$$

for $k \geq 2$.

Proof. We prove the result by inducting on k . The case $k = 2$ is a special case of the main result in [16]. Given pairwise coprime, positive integers a_1, a_2, \dots, a_k , define integers A_1, A_2, \dots, A_k as above. As in the proof of Lemma 2, for each j , $1 \leq j \leq A_k - 1$, let M_j and M'_j denote the *least* positive integer congruent to $j \pmod{A_k}$ representable as a nonnegative linear combination of A_1, A_2, \dots, A_k and $A'_1, A'_2, \dots, A'_{k-1}, A_k$, respectively, where $A'_j = A_j/a_k$ for $1 \leq j \leq k-1$. Then $\{M_j : 1 \leq j \leq A_k - 1\} = \{a_k M'_j : 1 \leq j \leq A_k - 1\}$. Observe that each A'_i divides A_k , and that $\{A'_1, A'_2, \dots, A'_{k-1}\}$ is just the set of A_i 's corresponding to a_1, a_2, \dots, a_{k-1} . From (3), $M_j - A_k \in \mathcal{S}^*(A_1, A_2, \dots, A_k)$ if and only if $M_j + M_i > M_{j+i}$ for $1 \leq i \leq A_k - 1$, which holds precisely when $M'_j + M'_i > M'_{j+i}$ for $1 \leq i \leq A_k - 1$. Thus $M_j - A_k \in \mathcal{S}^*(A_1, A_2, \dots, A_k)$ if and only if $M'_j - A_k \in \mathcal{S}^*(A'_1, A'_2, \dots, A'_{k-1}, A_k) = \mathcal{S}^*(A'_1, A'_2, \dots, A'_{k-1})$, which is the set $\{(k-2)a_1 a_2 \cdots a_{k-1} - (A'_1 + \cdots + A'_{k-1})\}$, by induction hypothesis. It now follows that $\mathcal{S}^*(A_1, A_2, \dots, A_k) = \{a_k M'_j - A_k\} = \{(k-2)a_1 a_2 \cdots a_k - a_k(A'_1 + \cdots + A'_{k-1}) + a_k A_k - A_k\} = \{(k-1)a_1 a_2 \cdots a_k - (A_1 + A_2 + \cdots + A_k)\}$, as desired. \square

Acknowledgements

The author wishes to thank the referee for some valuable comments and for pointing out the eighth reference.

References

- [1] Bateman, P. T., Remark on a Recent Note on Linear Forms, *American Mathematical Monthly* **65** (1958), 517-518.
- [2] Brauer, A., On a Problem of Partitions, *American Journal of Mathematics* **64** (1942), 299-312.
- [3] Brauer, A. and Shockley, J. E., On a problem of Frobenius, *Crelle* **211** (1962), 215-220.
- [4] Brown, T. C. and Shiue, P. J., A remark related to the Frobenius problem, *Fibonacci Quarterly* **31** (1993), 31-36.
- [5] Grant, D. D., On linear forms whose coefficients are in Arithmetic progression, *Israel Journal of Mathematics* **15** (1973), 204-209.
- [6] Johnson, S. M., A Linear Diophantine Problem, *Canadian Journal of Mathematics* **12** (1960), 390-398.

- [7] Nijenhuis, A. and Wilf, H. S., Representations of integers by linear forms in non negative integers, *Journal of Number Theory* **4** (1972), 98-106.
- [8] Ramirez Alfonsin, J. L., *The Frobenius Diophantine Problem*, Oxford University Press, 2006.
- [9] Roberts, J. B., Note on Linear Forms, *Proceedings of the American Mathematical Society* **7** (1956), 465-469.
- [10] Roberts, J. B., On a Diophantine problem, *Canadian Journal of Mathematics* **9** (1957), 219-222.
- [11] Rödseth, Ö. J., On a linear Diophantine problem of Frobenius, *Crelle* **301** (1978), 171-178.
- [12] Rödseth, Ö. J., On a linear Diophantine problem of Frobenius II, *Crelle* **307/308** (1979), 431-440.
- [13] Selmer, E. S., On the linear Diophantine problem of Frobenius, *Crelle* **293/294** (1977), 1-17.
- [14] Selmer, E. S. and Beyer, Ö, On the linear Diophantine problem of Frobenius in three variables, *Crelle* **301** (1978), 161-170.
- [15] Tripathi, A., The Coin Exchange Problem for Arithmetic Progressions, *American Mathematical Monthly* (1994), no. 10, 779-781.
- [16] Tripathi, A., On a variation of the Coin Exchange Problem for Arithmetic Progressions, *Integers: Electronic Journal of Combinatorial Number Theory* (2003), **3**, no. A01, 1-5.