#A44 INTEGERS 10 (2010), 523-529

ON THE FROBENIUS PROBLEM FOR $\{a^k, a^k+1, a^k+a, \ldots, a^k+a^{k-1}\}$

Amitabha Tripathi
Dept. of Mathematics, Indian Institute of Technology, New Delhi, India
atripath@maths.iitd.ac.in

Received: 11/14/09, Revised: 5/7/10, Accepted: 5/13/10, Published: 10/8/10

Abstract

For positive integers a, k, let $\mathcal{A}_k(a)$ denote the sequence $a^k, a^k+1, a^k+a, \ldots, a^k+a^{k-1}$. Let $\Gamma\big(\mathcal{A}_k(a)\big)$ denote the set of integers that are expressible as a linear combination of elements of $\mathcal{A}_k(a)$ with non-negative integer coefficients. We determine $\mathtt{g}\big(\mathcal{A}_k(a)\big)$ and $\mathtt{n}\big(\mathcal{A}_k(a)\big)$ which denote the *largest* (respectively, the *number* of) positive integer(s) not in $\Gamma\big(\mathcal{A}_k(a)\big)$. We also determine the set $\mathcal{S}^\star\big(\mathcal{A}_k(a)\big)$ of positive integers not in $\Gamma\big(\mathcal{A}_k(a)\big)$ which satisfy $n+\Gamma^\star\big(\mathcal{A}_k(a)\big) \subset \Gamma^\star\big(\mathcal{A}_k(a)\big)$, where $\Gamma^\star\big(\mathcal{A}_k(a)\big) = \Gamma\big(\mathcal{A}_k(a)\big) \setminus \{0\}$.

1. Introduction

For a sequence of relatively prime positive integers $A = a_1, \ldots, a_k$, let $\Gamma(A)$ denote the set of all integers of the form $\sum_{i=1}^k a_i x_i$ where each $x_i \geq 0$. It is well-known and not difficult to show that $\Gamma^c(A) := \mathbb{N} \setminus \Gamma(A)$ is a *finite* set. The *Coin Exchange Problem* of Frobenius is to determine the *largest* integer in $\Gamma^c(A)$. This is denoted by $\mathtt{g}(A)$, and called the Frobenius number of A. The Frobenius number is known in the case $k=2$ to be $\mathtt{g}(a_1, a_2) = a_1a_2 - a_1 - a_2$. A related problem is the determination of the number of integers in $\Gamma^c(A)$, which is denoted by $\mathtt{n}(A)$ and known in the case $k=2$ to be given by $\mathtt{n}(a_1, a_2) = \frac{1}{2}(a_1-1)(a_2-1)$. Various aspects of the Frobenius Problem may be found in [4].

The purpose of this article is to determine both the Frobenius number $\mathtt{g}\big(\mathcal{A}_k(a)\big)$ and $\mathtt{n}\big(\mathcal{A}_k(a)\big)$ when $\mathcal{A}_k(a) = \{a^k, a^k+1, a^k+a, \ldots, a^k+a^{k-1}\}$. Moreover, we determine the set $\mathcal{S}^\star\big(\mathcal{A}_k(a)\big)$, introduced in [7], of positive integers not in $\Gamma\big(\mathcal{A}_k(a)\big)$ which satisfy $n + \Gamma^\star\big(\mathcal{A}_k(a)\big) \subset \Gamma^\star\big(\mathcal{A}_k(a)\big)$, where $\Gamma^\star\big(\mathcal{A}_k(a)\big) = \Gamma\big(\mathcal{A}_k(a)\big) \setminus \{0\}$. In particular, this determines the Frobenius number since $\mathtt{g}\big(\mathcal{A}_k(a)\big)$ is the largest integer in $\mathcal{S}^\star\big(\mathcal{A}_k(a)\big)$. Hujter in [2] determined the Frobenius number $\mathtt{g}\big(\mathcal{A}_k(a)\big)$ (see p.70 in [4]) as a special case of a more general result. We give simpler and direct proofs of this result, employing three methods to determine not only the Frobenius number $\mathtt{g}(\cdot)$ but also $\mathtt{n}(\cdot)$. First, we use a reduction formula due to Johnson [3] for $\mathtt{g}(\cdot)$, and due to Rødseth [5] for $\mathtt{n}(\cdot)$. Next, we again determine these values using results due to Brauer and Shockley [1] for $\mathtt{g}(\cdot)$, and to Selmer [6] for $\mathtt{n}(\cdot)$. We determine $\mathtt{n}\big(\mathcal{A}_k(a)\big)$ from this by showing that exactly half of the nonnegative integers less than or equal to $\mathtt{g}\big(\mathcal{A}_k(a)\big)$ belong to $\Gamma\big(\mathcal{A}_k(a)\big)$.

2. Main Results

Throughout this section, for positive integers a, k, we denote by $\mathcal{A}_k$ the sequence $a^k, a^k+1, a^k+a, \ldots, a^k+a^{k-1}$. For the sake of convenience, we state without proof, two results that are crucial in the determination of exact values for both $\mathtt{g}(\cdot)$ and $\mathtt{n}(\cdot)$. The following reduction formulae for $\mathtt{g}(A)$, due to Johnson [3], and for $\mathtt{n}(A)$ due to Rødseth [5], are useful in cases when all but one member of A have a common factor greater than 1.

Lemma 1. [3, 5] *Let $a \in A$, let $d = \gcd\big(A \setminus \{a\}\big)$, and define $A' := \frac{1}{d}\big(A \setminus \{a\}\big)$. Then*

(i) $\mathtt{g}(A) = d \cdot \mathtt{g}\big(A' \cup \{a\}\big) + a(d-1)$;

(ii) $\mathtt{n}(A) = d \cdot \mathtt{n}\big(A' \cup \{a\}\big) + \frac{1}{2}(a-1)(d-1)$.

Fix $a \in A$, and let $\mathbf{m_C}$ denote the smallest integer in $\Gamma(A) \cap \mathbf{C}$, where $\mathbf{C}$ denotes a nonzero residue class mod a. The functions $\mathtt{g}(\cdot)$ and $\mathtt{n}(\cdot)$ are easily determined from the values of $\mathbf{m_C}$. The following result, part (i) of which is due to Brauer & Shockley [1] and part (ii) to Selmer [6], shows that both $\mathtt{g}(\cdot)$ and $\mathtt{n}(\cdot)$ can be determined from the values of $\mathbf{m_C}$.

Lemma 2. *[1, 6] Let $a \in A$. Then*

(i) $\mathtt{g}(A) = \max\limits_{\mathbf{C}} \mathbf{m_C} - a$, *the maximum taken over all nonzero classes $\mathbf{C}$ mod a;*

(ii) $\mathtt{n}(A) = \dfrac{1}{a}\sum\limits_{\mathbf{C}} \mathbf{m_C} - \frac{1}{2}(a-1)$, *the sum taken over all nonzero classes $\mathbf{C}$ mod a.*

The following variation of the Frobenius Problem was introduced by the author [7]. Observe that $n + \Gamma(A) \subset \Gamma(A)$ for $n \in \Gamma^\star(A) = \Gamma(A) \setminus \{0\}$. Let

$$\mathcal{S}^\star(A) := \{n \in \Gamma^c(A) : n + \Gamma^\star(A) \subset \Gamma^\star(A)\}.$$

For the sake of convenience, we recall the following essential result regarding $\mathcal{S}^\star(A)$ from [7]. If $\mathcal{C}$ denotes the set of all nonzero residue classes mod a, then

$$\mathcal{S}^\star(A) \subseteq \{\mathbf{m_C} - a : \mathbf{C} \in \mathcal{C}\}. \tag{1}$$

Moreover, if (x) denotes the residue class of x mod a and $\mathbf{m}_x$ the least integer in $\Gamma(A) \cap (x)$, then

$$\mathbf{m}_j - a \in \mathcal{S}^\star(A) \Longleftrightarrow \mathbf{m}_j - a \geq \mathbf{m}_{j+i} - \mathbf{m}_i \ \text{ for } \ 1 \leq i \leq a-1. \tag{2}$$

Observe that $\mathcal{S}^\star(A) \neq \emptyset$; in fact, $\mathtt{g}(A)$ is the largest integer in $\mathcal{S}^\star(A)$. A complete description of $\mathcal{S}^\star(A)$ would therefore lead to the determination of $\mathtt{g}(A)$.

2.1. The Reduction Formulae

We first determine $\mathtt{g}\big(\mathcal{A}_k(a)\big)$ and $\mathtt{n}\big(\mathcal{A}_k(a)\big)$ by using the reduction formulae of Lemma 1. This is particularly useful because the integers in $\mathcal{A}_k(a) \setminus \{a^k+1\}$ share a common divisor a.

Theorem 3. *For positive integers a and k,*

(i) $\mathtt{g}\big(a^k, a^k+1, a^k+a, \ldots, a^k+a^{k-1}\big) = k(a-1)a^k - 1$;

(ii) $\mathtt{n}\big(a^k, a^k+1, a^k+a, \ldots, a^k+a^{k-1}\big) = \frac{1}{2}k(a-1)a^k$.

First Proof. We use the reduction formulae given in Lemma 1 and the identity $a^k + 1 = (a-1)a^{k-1} + (a^{k-1}+1)$. Note that the identity implies $a^k+1 \in \Gamma\big(\{a^{k-1}, a^{k-1}+1\}\big)$. We fix a and induct on k.

(i)
$$\begin{aligned}
&\mathtt{g}\big(a^k, a^k+1, a^k+a, \ldots, a^k+a^{k-1}\big)\\
&= a \cdot \mathtt{g}\big(a^k+1, a^{k-1}, a^{k-1}+1, \ldots, a^{k-1}+a^{k-2}\big) + (a-1)(a^k+1)\\
&= a \cdot \mathtt{g}\big(a^{k-1}, a^{k-1}+1, \ldots, a^{k-1}+a^{k-2}\big) + (a-1)(a^k+1)\\
&= a\big\{(k-1)(a-1)a^{k-1} - 1\big\} + (a-1)(a^k+1)\\
&= k(a-1)a^k - 1
\end{aligned}$$

(ii)
$$\begin{aligned}
&\mathtt{n}\big(a^k, a^k+1, a^k+a, \ldots, a^k+a^{k-1}\big)\\
&= a \cdot \mathtt{n}\big(a^k+1, a^{k-1}, a^{k-1}+1, \ldots, a^{k-1}+a^{k-2}\big) + \tfrac{1}{2}(a-1)a^k\\
&= a \cdot \mathtt{n}\big(a^{k-1}, a^{k-1}+1, \ldots, a^{k-1}+a^{k-2}\big) + \tfrac{1}{2}(a-1)a^k\\
&= \tfrac{1}{2}(k-1)(a-1)a^k + \tfrac{1}{2}(a-1)a^k\\
&= \tfrac{1}{2}k(a-1)a^k.
\end{aligned}$$

□

2.2. The Calculation of $\mathbf{m_C}$

For the second proof, we determine $\mathbf{m_C}$ for each nonzero residue class $\mathbf{C}$ mod a^k. In addition to providing a method to determine $\mathtt{g}\big(\mathcal{A}_k(a)\big)$ and $\mathtt{n}\big(\mathcal{A}_k(a)\big)$, it also provides an expression for $\mathcal{S}^\star\big(\mathcal{A}_k(a)\big)$. Now $\mathtt{g}\big(\mathcal{A}_k(a)\big)$ denotes the largest N such that

$$\begin{aligned} a^k y + (a^k+1)x_0 + (a^k+a)x_1 + \cdots + (a^k+a^{k-1})x_{k-1} \\ = a^k \left(y + \textstyle\sum_{i=0}^{k-1} x_i\right) + \textstyle\sum_{i=0}^{k-1} a^i x_i = N \end{aligned} \tag{3}$$

has no solution in nonnegative integers x_i, and $\mathtt{n}\big(\mathcal{A}_k(a)\big)$ the number of such N.

Lemma 4. *Let $\mathbf{s}_a(x)$ denote the sum of digits in the base a representation of x. For each x, $1 \le x \le a^k - 1$, the least positive integer of the form given by (3) in the class x mod a^k is given by $a^k\mathbf{s}_a(x) + x$.*

Proof. Let $\mathbf{m}_x$ denote the least positive integer in $\Gamma(A_k(a))$, which is in the class (x) mod a^k. Then $\mathbf{m}_x$ is the minimum value attained by the expression on the left in (3) subject to $\sum_{i=0}^{k-1} a^i x_i = x$ and each $x_i \ge 0$. The values of x_i are uniquely determined by the base a representation of x mod a^k, and we must choose $y = 0$ in order to minimize the sum in (3) subject to the constraints. Thus $\mathbf{m}_x = a^k\mathbf{s}_a(x) + x$. □

Lemma 4 allows us to provides another proof of Theorem 3.

Second Proof. Let $\mathcal{C}$ denote the set of nonzero residue classes mod a^k. We use Lemma 4.

$$\begin{aligned} \text{(i)}\quad \mathtt{g}\big(a^k, a^k+1, a^k+a, \ldots, a^k+a^{k-1}\big) &= \max_{\mathbf{C}\in\mathcal{C}} m_{\mathbf{C}} - a^k \\ &= \max_{1\le x\le a^k-1} \left\{a^k\mathbf{s}_a(x) + x\right\} - a^k \\ &= \Big(a^k\mathbf{s}_a(a^k-1) + (a^k-1)\Big) - a^k \\ &= k(a-1)a^k - 1. \end{aligned}$$

(ii) $\mathtt{n}\big(a^k, a^k+1, a^k+a, \ldots, a^k+a^{k-1}\big)$

$$\begin{aligned}
&= \frac{1}{a^k}\sum_{\mathbf{C}\in\mathcal{C}} m_{\mathbf{C}} - \tfrac{1}{2}(a^k-1)\\
&= \frac{1}{a^k}\sum_{1\le x\le a^k-1}\Big(a^k\mathbf{s}_a(x)+x\Big) - \tfrac{1}{2}(a^k-1)\\
&= \sum_{1\le x\le a^k-1}\mathbf{s}_a(x)\\
&= \tfrac{1}{2}\sum_{0\le x\le a^k-1}\Big(\mathbf{s}_a(x)+\mathbf{s}_a(a^k-1-x)\Big)\\
&= \tfrac{1}{2}\sum_{0\le x\le a^k-1}\mathbf{s}_a(a^k-1)\\
&= \tfrac{1}{2}k(a-1)a^k. \qquad \square
\end{aligned}$$

2.3. The Determination of $\mathcal{S}^\star\big(a^k, a^k+1, a^k+a, \ldots, a^k+a^{k-1}\big)$

Theorem 5. *For positive integers a and k,*

$$\mathcal{S}^\star\big(a^k, a^k+1, a^k+a, \ldots, a^k+a^{k-1}\big) = \big\{k(a-1)a^k-1\big\}.$$

Proof. Let $\mathcal{A}_k(a) = \{a^k, a^k+1, a^k+a, \ldots, a^k+a^{k-1}\}$. By (1) and Lemma 4,

$$\mathcal{S}^\star\big(\mathcal{A}_k(a)\big) \subseteq \big\{a^k\big(\mathbf{s}_a(x)-1\big)+x : 1\le x\le a^k-1\big\}.$$

By (2), $a^k\big(\mathbf{s}_a(x)-1\big)+x \in \mathcal{S}^\star$ if and only if for each y with $1\le y\le a^k-1$,

$$a^k\Big(\mathbf{s}_a\big((x+y) \bmod a^k\big)+1\Big) + (x+y) \bmod a^k \le a^k\Big(\mathbf{s}_a(x)+\mathbf{s}_a(y)\Big)+x+y. \quad (4)$$

Since $\mathbf{s}_a(x)+\mathbf{s}_a(a^k-1-x) = \mathbf{s}_a(a^k-1)$, the inequality (4) fails to hold for the pair $\{x, a^k-1-x\}$ whenever $x < a^k-1$. Thus the only element in $\mathcal{S}^\star\big(\mathcal{A}_k(a)\big)$ is $a^k\big(\mathbf{s}_a(a^k-1)-1\big)+(a^k-1) = k(a-1)a^k-1$. $\square$

Corollary 6. *For positive integers a and k,*

$$\mathtt{g}\big(a^k, a^k+1, a^k+a, \ldots, a^k+a^{k-1}\big) = k(a-1)a^k-1.$$

2.4. A Connection Between $\mathtt{g}\big(\mathcal{A}_k(a)\big)$ and $\mathtt{n}\big(\mathcal{A}_k(a)\big)$

If m, n are integers with sum $\mathtt{g}\big(\mathcal{A}_k(a)\big)$, then it is easy to see that *at most* one of m, n can belong to $\Gamma\big(\mathcal{A}_k(a)\big)$. On the other hand, if for some such pair m, n, neither belongs to $\Gamma\big(\mathcal{A}_k(a)\big)$, there would be less than $\frac{1}{2}\big\{1+\mathtt{g}\big(\mathcal{A}_k(a)\big)\big\}$ integers in $\Gamma^c\big(\mathcal{A}_k(a)\big)$. Thus, for every pair of non-negative integers m, n with sum $\mathtt{g}\big(\mathcal{A}_k(a)\big)$, *exactly* one of m, n belong to $\Gamma^c\big(\mathcal{A}_k(a)\big)$. We use this to derive $\mathtt{n}\big(\mathcal{A}_k(a)\big)$, giving a third derivation for $\mathtt{n}\big(\mathcal{A}_k(a)\big)$.

Theorem 7. *For positive integers a and k, let $\mathcal{A}_k(a)$ denote the sequence $a^k, a^k+1, a^k+a, \ldots, a^k+a^{k-1}$. If $m+n=\mathtt{g}(\mathcal{A}_k(a))$, then $m \in \Gamma\big(\mathcal{A}_k(a)\big)$ if and only if $n \notin \Gamma\big(\mathcal{A}_k(a)\big)$.*

Proof. Let $m+n=\mathtt{g}(\mathcal{A}_k(a))$. If $m \in \Gamma\big(\mathcal{A}_k(a)\big)$, then $n \notin \Gamma\big(\mathcal{A}_k(a)\big)$, for otherwise $m+n=\mathtt{g}(\mathcal{A}_k(a)) \in \Gamma\big(\mathcal{A}_k(a)\big)$, which is false.

Conversely, suppose $n \notin \Gamma\big(\mathcal{A}_k(a)\big)$. If $n<0$, then $m>\mathtt{g}(\mathcal{A}_k(a))$ and so $m \in \Gamma\big(\mathcal{A}_k(a)\big)$. We may therefore assume that $1 \le n \le \mathtt{g}(\mathcal{A}_k(a))$ since both 0 and any integer greater than $\mathtt{g}(\mathcal{A}_k(a))$ belong to $\Gamma\big(\mathcal{A}_k(a)\big)$. Suppose $n \equiv x \pmod{a^k}$; then $n \le \mathbf{m}_x - a^k = a^k\big(\mathbf{s}_a(x)-1\big)+x$. Since $m+n=\mathtt{g}\big(\mathcal{A}_k(a)\big)=a^k\mathbf{s}_a(a^k-1)-1 \equiv -1 \pmod{a^k}$, we have $m \equiv a^k-1-x \pmod{a^k}$. Using $\mathbf{s}_a(x)+\mathbf{s}_a(a^k-1-x)=\mathbf{s}_a(a^k-1)$, we have

$$m=\mathtt{g}\big(\mathcal{A}_k(a)\big)-n \ge a^k\big(\mathbf{s}_a(a^k-1)-\mathbf{s}_a(x)\big)+(a^k-1-x)=a^k\mathbf{s}_a(a^k-1-x)+(a^k-1-x)$$
$$=\mathbf{m}_{a^k-1-x}.$$

Hence $m \in \Gamma\big(\mathcal{A}_k(a)\big)$. This completes the proof. □

Corollary 8. *For positive integers a and k,*

$$\mathtt{n}\big(\mathcal{A}_k(a)\big)=\tfrac{1}{2}\left\{1+\mathtt{g}\big(\mathcal{A}_k(a)\big)\right\}.$$

Proof. Consider pairs $\{m,n\}$ of integers in the interval $[0, \mathtt{g}\big(\mathcal{A}_k\big)]$ with $m+n = g\big(\mathcal{A}_k(a)\big)$. By Theorem 7, *exactly* one integer from each such pair is in $\Gamma^c\big(\mathcal{A}_k(a)\big)$. This completes the proof since no integer greater than $\mathtt{g}\big(\mathcal{A}_k(a)\big)$ is in $\Gamma^c\big(\mathcal{A}_k(a)\big)$. □

Acknowledgement. The author wishes to thank the referee for his comments.

References

[1] A. Brauer and J. E. Shockley, On a problem of Frobenius, *Crelle* **211** (1962), 215–220.

[2] M. Hujter, On a sharp upper and lower bounds for the Frobenius problem, Technical Report MO/32, Computer and Automation Institute, Hungarian Academy of Sciences, 1982.

[3] S. M. Johnson, A Linear Diophantine Problem, *Canad. J. Math.* **12** (1960), 390–398.

[4] J. L. Ramírez Alfonsín, The Frobenius Diophantine Problem, Oxford Lecture Series in Mathematics and its Applications, no. 30, Oxford University Press, 2005.

[5] Ø. J. Rødseth, On a linear Diophantine problem of Frobenius, *Crelle* **301** (1978), 171–178.

[6] E. S. Selmer, On the linear Diophantine problem of Frobenius, *Crelle* **293/294** (1977), 1–17.

[7] A. Tripathi, On a variation of the Coin Exchange Problem for Arithmetic Progressions, *Integers* **3**, Article A01 (2003), 5 pp.