Journal of Number Theory 162 (2016) 212–223

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On the Frobenius problem for $\{a, ha + d, ha + bd, ha + b^2d, \ldots, ha + b^kd\}$

Amitabha Tripathi

Department of Mathematics, Indian Institute of Technology, Hauz Khas, New Delhi 110016, India

ARTICLE INFO

Article history:
Received 29 June 2015
Received in revised form 27 September 2015
Accepted 3 October 2015
Available online 14 December 2015
Communicated by Steven J. Miller

MSC:
11D07

Keywords:
Frobenius problem
Frobenius number

ABSTRACT

For positive and relatively prime set of integers A, let $\Gamma(A)$ denote the set of integers that is formed by taking nonnegative integer linear combinations of integers in A. Then there are finitely many positive integers that do not belong to $\Gamma(A)$. For $A = \{a, ha + d, ha + bd, ha + b^2d, \ldots, ha + b^kd\}$, $\gcd(a, d) = 1$, we determine the largest integer $\mathtt{g}(A)$ that does not belong to $\Gamma(A)$, and the number of integers $\mathtt{n}(A)$ that does not belong to $\Gamma(A)$, both for all sufficiently large values of d. This extends a result of Selmer, and corrects a result of Hofmeister, both given in special cases.

1. Introduction

Given a finite set $A = \{a_1, \ldots, a_k\}$ of positive integers with gcd $A := \gcd(a_1, \ldots, a_k) = 1$, let $\Gamma(A) := \{a_1x_1 + \cdots + a_kx_k : x_i \geq 0\}$ and $\Gamma^\star(A) = \Gamma(A) \setminus \{0\}$. It is well known that $\Gamma^c(A) := \mathbb{N} \setminus \Gamma(A)$ is finite. Although it was Sylvester [9] who first asked to determine

$$\mathtt{g}(A) := \max \Gamma^c(A),$$

E-mail address: atripath@maths.iitd.ac.in.

http://dx.doi.org/10.1016/j.jnt.2015.10.020

and who showed that $\mathtt{g}(a_1, a_2) = (a_1 - 1)(a_2 - 1) - 1$, it was Frobenius who was largely instrumental in giving this problem the early recognition and it is after him that the problem is also named. The monograph on the Frobenius problem [6] gives an extensive survey. Related to the Frobenius problem is the problem of determining $\mathtt{n}(A) := |\Gamma^c(A)|$. As in the case of determining $\mathtt{g}(A)$, it was Sylvester who showed that $\mathtt{n}(a_1, a_2) = \frac{1}{2}(a_1 - 1)(a_2 - 1)$.

Exact determination of the $\mathtt{g}(A)$ and $\mathtt{n}(A)$ is a difficult problem in general; there is no general formula for $|A| > 2$. There are only a few cases other than when $|A| = 2$ where $\mathtt{g}(A)$ or $\mathtt{n}(A)$ have been determined. Among those few cases are those where the elements of A are in arithmetic progression, and generalizations thereof. Brauer [2] found $\mathtt{g}(A)$ for consecutive integers, Roberts [7] extended this result to numbers in arithmetic progression (see also [1,12,10]), and Selmer [8] further generalized this to the determination of $\mathtt{g}(a, ha + d, ha + 2d, \ldots, ha + kd)$ (see also [11]). Grant [4] determined $\mathtt{n}(A)$ where the elements of A are in arithmetic progression, and this was extended by Tripathi [11] to the determination of $\mathtt{n}(a, ha + d, ha + 2d, \ldots, ha + kd)$.

Selmer [8] determined both $\mathtt{g}(A)$ and $\mathtt{n}(A)$ for $A = \{a, a+1, a+2, a+2^2, \ldots, a+2^k\}$. However, his result is valid only for sufficiently large values of a, and fails for values not covered by the statement of Theorem 1.

Theorem 1 *(Selmer). (See [8].) For positive integers a and k with $a > (k-3)2^k + 1$,*

(i)

$$\mathtt{g}\big(a, a+1, a+2, a+2^2, \ldots, a+2^k\big) = (a+1)\left\lfloor \frac{a}{2^k} \right\rfloor + \sum_{i=0}^{k-1} 2^i \left\lfloor \frac{a+2^i}{2^k} \right\rfloor + (k-2)a - 1.$$

(ii)

$$\mathtt{n}\big(a, a+1, a+2, a+2^2, \ldots, a+2^k\big) = \left(2^{k-1}\left(k - 1 - \left\lfloor \frac{a}{2^k} \right\rfloor\right) + a\right)\left\lfloor \frac{a}{2^k} \right\rfloor + B\left(a - 2^k \left\lfloor \frac{a}{2^k} \right\rfloor\right),$$

where $B(n)$ denotes the total number of ones in the binary representations of $0, 1, \ldots, n-1$.

Hofmeister [5] extended Selmer's result for $\mathtt{g}(A)$ to the case where $A = \{a, a+d, a+bd, \ldots, a+b^k d\}$. As with the case of Selmer's result, Hofmeister's result is valid only for sufficiently large values of d. Moreover, there appears to be no explicit expression for this bound for d in Hofmeister's result.

Theorem 2 *(Hofmeister). (See [5].) Let a, d, k, b be positive integers, with $b > 1$ and $\gcd(a, d) = 1$. For all sufficiently large d,*

$$\mathtt{g}\big(a, a+d, a+bd, \dots, a+b^k d\big) = \left\lfloor \frac{a-2}{b^k} \right\rfloor a + d(a-1).$$

For positive integers a, h, k, d, b, where $\gcd(a, d) = 1$ and $b > 1$, let $A = \{a, ha + d, ha + bd, ha + b^2 d, \dots, ha + b^k d\}$. In Section 2, we study the sum of digits function $\mathtt{w}_b$ that plays a crucial role in the determination of both $\mathtt{g}(A)$ and $\mathtt{n}(A)$ in the latter part of this paper. In Section 3, we give exact results for both $\mathtt{g}(A)$ and $\mathtt{n}(A)$ that hold for all sufficiently large values of d in Theorem 3. This not only generalizes Hofmeister's result in Theorem 2 but also gives an explicit value to the lower bound for d for validity of the result. In particular, in the special case $h = 1$ this provides a contradiction to the result in Theorem 2. In Section 4, we consider the case $b = 2$ and $h = 1$ in our main result, verifying Selmer's result in Theorem 1. Our main result is as follows.

Theorem 3. *Let a, h, k, d, b be positive integers, with $\gcd(a, d) = 1$ and $b > 1$. Let $q = \lfloor \frac{a-1}{b^k} \rfloor$ and $r \equiv a - 1 \pmod{b^k}$, $0 \le r < b^k$. Let $\mathtt{w}_b(x)$ denote the sum of the digits in the base b representation of x. If $A = \{a, ha + d, ha + bd, ha + b^2 d, \dots, ha + b^k d\}$ and $d \ge h\big(k(b-1) - \lfloor \frac{a}{b^k} \rfloor\big)$, then*

(i)

$$\begin{aligned}\mathtt{g}(A) = {} & a(hq-1) + d(qb^k - 1) \\ & + \max\left\{ ha\big(k(b-1)-1\big), \max_{0 \le x \le r} \Big(ha \cdot \mathtt{w}_b(x) + d(x+1)\Big) \right\}.\end{aligned}$$

In particular, for all sufficiently large values of d,

$$\mathtt{g}(A) = ha\big(q + \mathtt{w}_b(r)\big) + d(a-1) - a. \tag{1}$$

(ii)

$$\mathtt{n}(A) = h\left(\frac{1}{2}q\big(q - 1 + k(b-1)\big)b^k + q(r+1) + \sum_{x=0}^{r} \mathtt{w}_b(x)\right) + \frac{1}{2}(a-1)(d-1).$$

Remark 1. The particular case in Theorem 3, part (i) for $h = 1$ is not consistent with the result of Theorem 2. If $b^k \mid (a-1)$, the two results are identical. However, if $b^k \nmid (a-1)$, our result exceeds that of Hofmeister's by $a\big(\mathtt{w}_b(r) - 1\big)$.

Remark 2. Let $f(x) := ha \cdot \mathtt{w}_b(x) + d(x+1)$ for $x \in \{0, \dots, r\}$. Equation (1) holds provided $\max_{0 \le x \le r} f(x) = f(r)$. Since $\mathtt{w}_b(x) \le k(b-1)$, $d \ge hak(b-1)$ ensures both $f(r) > f(x)$ for all $x \in \{0, \dots, r-1\}$ and $f(r) > ha\big(k(b-1) - 1\big)$. This gives an explicit lower bound for d for validity of (1).

Remark 3. The results in Theorem 3 can be made more precise by using Proposition 1 in Section 2. The maximum in part (i) to compute $\mathtt{g}(A)$ may be taken over the subset $[\overline{r}, r]$ instead of $[0, r]$. Here $\overline{r}$ denotes the largest integer m not exceeding r for which $\mathtt{w}_b(m)$ is the largest among $\mathtt{w}_b(0), \mathtt{w}_b(1), \dots, \mathtt{w}_b(r)$. The definition of $\overline{r}$ appears in the statement of Proposition 1. The sum in part (ii) to compute $\mathtt{n}(A)$ is explicitly given in the proposition.

For each nonzero residue class $\mathbf{C}$ modulo a, let $\mathbf{m_C}$ denote the least positive integer in $\Gamma(A) \cap \mathbf{C}$. The functions $\mathtt{g}$ and $\mathtt{n}$ are easily determined from the values of $\mathbf{m_C}$ by Lemma 1. We employ the results in Lemma 1 to evaluate both $\mathtt{g}(A)$ and $\mathtt{n}(A)$.

Lemma 1 *(Brauer and Shockley; Selmer). (See [3] and [8].) Let $a \in A$. Then*

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

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

2. The sum of digits functions $\mathtt{w}_b$

Fix $b > 1$. For $n \in \mathbb{N} \cup \{0\}$, let $n = c_0 + c_1 b + c_2 b^2 + \cdots + c_s b^s$, $0 \le c_i \le b-1$, be the representation of n in base b. Define the sum of digits function $\mathtt{w}_b : \mathbb{N} \cup \{0\} \to \mathbb{N} \cup \{0\}$ by

$$\mathtt{w}_b\big(c_0 + c_1 b + c_2 b^2 + \cdots + c_s b^s\big) = c_0 + c_1 + c_2 + \cdots + c_s.$$

Proposition 1. *Let $b > 1$, and let $n = c_0 + c_1 b + c_2 b^2 + \cdots + c_s b^s$, $0 \le c_i \le b-1$. Let $\overline{n} = \max\{m : \mathtt{w}_b(m) = \max_{0 \le x \le n} \mathtt{w}_b(x), m \le n\}$.*

(i) *For $b > 1$, $\big(\overline{1}, \mathtt{w}_b(\overline{1})\big) = (1, 1)$. For $b > 2$, $\big(\overline{2}, \mathtt{w}_b(\overline{2})\big) = (2, 2)$ and $\big(\overline{2}, \mathtt{w}_2(\overline{2})\big) = (2, 1)$. If $b > 2$ and $n > 2$, then*

$$\big(\overline{n}, \mathtt{w}_b(\overline{n})\big) = \begin{cases} \big(n, (b-1)s + c_s\big) & \text{if } c_0 + \cdots + c_{s-1} \ge (b-1)s - 1; \\ \big(c_s b^s - 1, (b-1)s + c_s - 1\big) & \text{otherwise.} \end{cases}$$

If $b = 2$ and $n > 2$, then

$$\big(\overline{n}, \mathtt{w}_2(\overline{n})\big) = \begin{cases} \big(n, s+1\big) & \text{if } c_0 + \cdots + c_{s-1} \ge s - 1; \\ \big(2^{s+1} - 2^t - 1, s\big) & \text{otherwise,} \end{cases}$$

where t is the unique nonnegative integer satisfying $2^{s+1} - 1 - 2^t \le n < 2^{s+1} - 1 - 2^{t-1}$.

(ii) *Let c_1, c_2 be positive integers. If $f(x) = c_1 \cdot \mathtt{w}_b(x) + c_2 x$ for $0 \le x \le n$, then*

$$\max_{0 \le x \le n} f(x) = \max_{\overline{n} \le x \le n} f(x).$$

(iii) *Let* $n = c_s b^s + c_{s_1} b^{s_1} + \cdots + c_{s_k} b^{s_k}$*, where* $s = s_0 > s_1 > \cdots > s_k > 0$*. Then*

$$\sum_{x=0}^{n} \mathtt{w}_b(x) = \left(\frac{1}{2}c_{s_k}(c_{s_k}-1)b^{s_k} + \frac{1}{2}c_{s_k}b^{s_k}(b-1)s_k + 1\right) + \frac{1}{2}\sum_{i=0}^{k-1} c_{s_i}(c_{s_i}-1)b^{s_i}$$

$$+ \frac{b-1}{2}\sum_{i=0}^{k-1} c_{s_i}b^{s_i}s_i + \sum_{i=1}^{k} c_{s_i}\big(c_{s_0}+c_{s_1}+\cdots+c_{s_{i-1}}\big)b^{s_i} + \sum_{i=0}^{k-1} c_{s_i}.$$

In particular, if $n = 2^s + 2^{s_1} + 2^{s_2} + \cdots + 2^{s_k}$*, with* $s = s_0 > s_1 > s_2 > \cdots > s_k \geq 0$*, then*

$$\sum_{x=0}^{n} \mathtt{w}_2(x) = \sum_{i=0}^{k} 2^{s_i-1}(s_i + 2i) + k + 1.$$

Proof.

(i) The cases $n \leq 2$ are easily verified. Henceforth we assume $n > 2$. Let $\overline{n} = \overline{c_0} + \overline{c_1}b + \overline{c_2}b^2 + \cdots + \overline{c_s}b^s$, where $0 \leq \overline{c_i} \leq b-1$ for $i < s$ and $\overline{c_s} \leq c_s$, and let $\mathtt{w}_b(\overline{n}) = \overline{\mathtt{w}}$. Since $(b-1)(1+b+b^2+\cdots+b^{s-1})+(c_s-1)b^s < n$, we have $(b-1)s+c_s-1 \leq \overline{\mathtt{w}} \leq (b-1)s+c_s$. Suppose $c_0+\cdots+c_{s-1} = (b-1)s$. Then $c_i = b-1$ for $i < s$ and $\mathtt{w}_b(n) = (b-1)s+c_s$. Since $\mathtt{w}_b(n) \leq \overline{\mathtt{w}} \leq (b-1)s + c_s$, we must have $(b-1)s + c_s = \overline{\mathtt{w}} = \sum_{i=0}^{s-1} \overline{c_i} + \overline{c_s}$. Thus $\overline{c_i} = b-1 = c_i$ for $i < s$ and $\overline{c_s} = c_s$, so that $\overline{n} = n$. In particular, note that $\overline{\mathtt{w}} = (b-1)s + c_s$ implies $\overline{n} = n$.
Henceforth suppose $\overline{\mathtt{w}} = (b-1)s + c_s - 1$. If $c_0 + \cdots + c_{s-1} = (b-1)s - 1$, then $\mathtt{w}_b(n) = (b-1)s-1+c_s = \overline{w}$, so that $\overline{n} = n$. Thus $\overline{n} = n$ whenever $c_0+\cdots+c_{s-1} \geq (b-1)s-1$.
Finally suppose $c_0+\cdots+c_{s-1} < (b-1)s-1$. We consider the cases $b > 2$ and $b = 2$ separately.
Suppose $b > 2$. If $\overline{c_s} = c_s$, then $\sum_{i=1}^{s-1} \overline{c_i} = (b-1)s-1$, so that all but one of the $\overline{c_i}$'s equals $b-1$ and the remaining one equals $b-2$. Since at least two of the c_i's are less than $b-1$, $\sum_{i=0}^{s} \overline{c_i}b^i > n$, contradicting the definition of $\overline{n}$. Hence $\overline{c_s} = c_s - 1$ and $\overline{c_i} = b-1$ for $i < s$, so that $\overline{n} = (b-1)\sum_{i=0}^{s-1} b^i + (c_s-1)b^s = c_s b^s - 1$.
Suppose $b = 2$. Since $c_s = 1$, we have $\overline{\mathtt{w}} = s$ so that exactly one of the $\overline{c_i}$'s equals 0. Hence $\overline{n} = (2^{s+1}-1)-2^j$ with $j \in \{0, \ldots, s-1\}$. Since the least such j that satisfies the inequality $\overline{n} \leq n$ is $j = t$, we have the desired result.

(ii) If $x < \overline{n}$, then $\mathtt{w}_b(x) \leq \mathtt{w}_b(\overline{n})$, so that $f(x) = c_1 \cdot \mathtt{w}_b(x)+c_2 x < c_1 \cdot \mathtt{w}_b(\overline{n})+c_2\overline{n} = f(\overline{n})$.

(iii) Let $S(n) := \sum_{x=0}^{n} \mathtt{w}_b(x)$. Consider the set of integers $\{0, \ldots, b^s - 1\}$. Pair x, y such that $x+y = b^s-1$. If b is even, there are $\frac{1}{2}b^s$ such pairs $\{x, y\}$; note that $x \neq y$ and $\mathtt{w}_b(x) + \mathtt{w}_b(y) = (b-1)s$. If b is odd, there are $\frac{1}{2}(b^s - 1)$ such pairs $\{x, y\}$; note that $x \neq y$ and $\mathtt{w}_b(x) + \mathtt{w}_b(y) = (b-1)s$. The remaining integer m is $\frac{1}{2}(b-1)\sum_{i=0}^{s} b^i$, and $\mathtt{w}_b(m) = \frac{1}{2}(b-1)s$. In either case

$$S(b^s-1)=\frac{1}{2}b^s(b-1)s. \tag{2}$$

The set $\{0,\ldots,c_sb^s-1\}$ can be partitioned into sets $S_\lambda := \{0,\ldots,b^s-1\}+\lambda b^s$, $\lambda \in \{0,\ldots,c_s-1\}$. Since $\sum_{x\in S_\lambda}\mathtt{w}_b(x)=\lambda b^s+S(b^s-1)$, we have using (2)

$$\begin{aligned} S(c_sb^s-1) &= \sum_{\lambda=0}^{c_s-1}\left(\lambda b^s+S(b^s-1)\right)=\frac{1}{2}c_s(c_s-1)b^s+c_sS(b^s-1)\\ &= \frac{1}{2}c_s(c_s-1)b^s+\frac{1}{2}c_sb^s(b-1)s. \end{aligned} \tag{3}$$

Since the base b representations of the $n-c_sb^s+1$ integers in the interval $[c_sb^s,n]$ all have leading coefficient c_s, using (3) we have the reduction formula

$$\begin{aligned} S(n) &= \sum_{x=0}^{c_sb^s-1}\mathtt{w}_b(x)+\sum_{x=c_sb^s}^{n}\mathtt{w}_b(x)\\ &= S(c_sb^s-1)+\sum_{x=0}^{n-c_sb^s}\mathtt{w}_b(x)+c_s(n-c_sb^s+1)\\ &= S(c_sb^s-1)+S(n-c_sb^s)+c_s(n-c_sb^s+1)\\ &= S(n-c_sb^s)+\frac{1}{2}c_s(c_s-1)b^s+\frac{1}{2}c_sb^s(b-1)s+c_s(n-c_sb^s+1). \end{aligned} \tag{4}$$

Let $T=\{i : c_i\neq 0\}$, and arrange the integers in T in decreasing order: $s=s_0>s_1>s_2>\cdots>s_k>0$. For $i\in\{0,1,\ldots,k\}$, write $n_i=c_{s_i}b^{s_i}+c_{s_{i+1}}b^{s_{i+1}}+\cdots+c_{s_k}b^{s_k}$; note that $n_0=n$. So for $i\in\{0,1,\ldots,k-1\}$, (4) can be rewritten as

$$S(n_i)=S(n_{i+1})+\frac{1}{2}c_{s_i}(c_{s_i}-1)b^{s_i}+\frac{1}{2}c_{s_i}b^{s_i}(b-1)s_i+c_{s_i}(n_{i+1}+1). \tag{5}$$

Summing over $i\in\{0,1,\ldots,k-1\}$ and using (3) gives

$$\begin{aligned} S(n) &= S(n_k)+\frac{1}{2}\sum_{i=0}^{k-1}c_{s_i}(c_{s_i}-1)b^{s_i}+\frac{b-1}{2}\sum_{i=0}^{k-1}c_{s_i}b^{s_i}s_i+\sum_{i=0}^{k-1}c_{s_i}n_{i+1}+\sum_{i=0}^{k-1}c_{s_i}\\ &= \left(\frac{1}{2}c_{s_k}(c_{s_k}-1)b^{s_k}+\frac{1}{2}c_{s_k}b^{s_k}(b-1)s_k+1\right)+\frac{1}{2}\sum_{i=0}^{k-1}c_{s_i}(c_{s_i}-1)b^{s_i}\\ &\quad+\frac{b-1}{2}\sum_{i=0}^{k-1}c_{s_i}b^{s_i}s_i+\sum_{i=0}^{k-1}c_{s_i}\left(\sum_{j=i+1}^{k}c_{s_j}b^{s_j}\right)+\sum_{i=0}^{k-1}c_{s_i}\\ &= \left(\frac{1}{2}c_{s_k}(c_{s_k}-1)b^{s_k}+\frac{1}{2}c_{s_k}b^{s_k}(b-1)s_k+1\right)+\frac{1}{2}\sum_{i=0}^{k-1}c_{s_i}(c_{s_i}-1)b^{s_i} \end{aligned}$$

$$+\frac{b-1}{2}\sum_{i=0}^{k-1}c_{s_i}b^{s_i}s_i+\sum_{j=1}^{k}c_{s_j}b^{s_j}\left(\sum_{i=0}^{j-1}c_{s_i}\right)+\sum_{i=0}^{k-1}c_{s_i}$$

$$=\left(\frac{1}{2}c_{s_k}(c_{s_k}-1)b^{s_k}+\frac{1}{2}c_{s_k}b^{s_k}(b-1)s_k+1\right)+\frac{1}{2}\sum_{i=0}^{k-1}c_{s_i}(c_{s_i}-1)b^{s_i}$$

$$+\frac{b-1}{2}\sum_{i=0}^{k-1}c_{s_i}b^{s_i}s_i+\sum_{i=1}^{k}c_{s_i}\big(c_{s_0}+c_{s_1}+\cdots+c_{s_{i-1}}\big)b^{s_i}+\sum_{i=0}^{k-1}c_{s_i}. \tag{6}$$

For $b = 2$ we may write $n = 2^s + 2^{s_1} + 2^{s_2} + \cdots + 2^{s_k}$, with $s = s_0 > s_1 > s_2 > \cdots > s_k > 0$. The formula for $S(n)$ given by (6) simplifies significantly since each $c_{s_i} = 1$.

$$S(n)=2^{s_k-1}s_k+1+\sum_{i=0}^{k-1}2^{s_i-1}s_i+\sum_{i=1}^{k}i2^{s_i}+k=\sum_{i=0}^{k}2^{s_i-1}s_i+\sum_{i=1}^{k}i2^{s_i}+k+1. \tag{7}$$

Note that the last term $\sum_{i=0}^{k-1}c_{s_i}$ in (6) equals $\mathtt{w}_b(n)$. In particular, $k+1$ in (7) equals $\mathtt{w}_2(n)$, so that $S(n-1)=\sum_{i=0}^{k}2^{s_i-1}s_i+\sum_{i=1}^{k}i2^{s_i}=\sum_{i=0}^{k}2^{s_i-1}(s_i+2i)$. □

3. The general case $\{a, ha + d, ha + bd, ha + b^2d, \ldots, ha + b^kd\}$

Let $A = \{a, ha + d, ha + bd, ha + b^2d, \ldots, ha + b^kd\}$, where a, h, k, d, b are positive integers, with $\gcd(a, d) = 1$ and $b > 1$. Thus $\mathtt{g}(A)$ denotes the largest N such that

$$ax_{-1}+(ha+d)x_0+(ha+bd)x_1+\cdots+(ha+b^kd)x_k$$
$$=a\left(x_{-1}+h\sum_{i=0}^{k}x_i\right)+d\left(\sum_{i=0}^{k}b^ix_i\right)=N \tag{8}$$

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

Proposition 2. *Let a, h, k, d, b be positive integers, with $\gcd(a, d) = 1$ and $b > 1$. Then the least positive integer of the form given by (8) in the class (dx) modulo a is*

$$\mathbf{m}_{dx}=\min_{t\ge 0}\left\{ha\left(\left\lfloor\frac{x+at}{b^k}\right\rfloor+\mathtt{w}_b\big((x+at) \bmod b^k\big)\right)+d(x+at)\right\},$$

where $\mathtt{w}_b(r)$ is the sum of digits in the base b representation of r. Moreover, if $d \ge h\big(k(b-1)-\lfloor\frac{a}{b^k}\rfloor\big)$ with $\gcd(a, d) = 1$, then

$$\mathbf{m}_{dx}=ha\left(\left\lfloor\frac{x}{b^k}\right\rfloor+\mathtt{w}_b\big(x \bmod b^k\big)\right)+dx.$$

Proof. Let $\mathbf{m}_{dx}$ denote the least positive integer in the class (dx) modulo a. By (8), $\mathbf{m}_{dx}$ is obtained by minimizing $x_{-1} + h\sum_{i=0}^{k} x_i$ subject to $\sum_{i=0}^{k} b^i x_i \equiv x \pmod{a}$, with each $x_i \geq 0$. This is the same as minimizing $\sum_{i=0}^{k} x_i$ subject to $\sum_{i=0}^{k} b^i x_i = x + at$, with each $x_i \geq 0$ and over all $t \geq 0$.

Fix $t \geq 0$. Let $x + at = qb^k + r$, $0 \leq r \leq b^k - 1$, and let $r = \sum_{i=0}^{k-1} \epsilon_i b^i$, $\epsilon_i \in \{0, 1, \dots, b-1\}$. Then $\sum_{i=0}^{k} x_i$ is minimized by choosing $x_k = q$, $x_i = \epsilon_i$ for $i \in \{0, \dots, k-1\}$. Thus the minimum value for $x_{-1} + h\sum_{i=0}^{k} x_i$ is $h\big(q + \mathtt{w}_b(r)\big)$, and the corresponding value for the LHS of (8) is

$$f(t) := ha\left(\left\lfloor \tfrac{x+at}{b^k} \right\rfloor + \mathtt{w}_b\big((x+at) \bmod b^k\big)\right) + d(x+at).$$

Hence $\mathbf{m}_{dx} = \min_{t\geq 0} f(t)$.

To obtain the special form for sufficiently large d, note that $f(t+1) - f(t)$ equals

$$\begin{aligned} &ha\left(\left\lfloor \tfrac{x+a(t+1)}{b^k} \right\rfloor - \left\lfloor \tfrac{x+at}{b^k} \right\rfloor\right) + ha\left(\mathtt{w}_b\big((x+a(t+1)) \bmod b^k\big)\right. \\ &\quad \left. - \mathtt{w}_b\big((x+at) \bmod b^k\big)\right) + ad. \end{aligned}$$

This is a sum of three terms. The first term equals one of $ha\lfloor \frac{a}{b^k} \rfloor$, $ha\lceil \frac{a}{b^k} \rceil$, and the second lies between $-hak(b-1)$ and $hak(b-1)$. So $f(t+1) \geq f(t)$ whenever $d \geq h\big(k(b-1) - \lfloor \frac{a}{b^k} \rfloor\big)$, implying $\min_{t\geq 0} f(t) = f(0)$ for these values of d. □

Remark 4. The results in Proposition 2 can be made more precise. If $\gcd(a, b^k) = \ell$, then

$$\big\{(x+at) \bmod b^k : t \geq 0\big\} = \big\{(x+\ell t) \bmod b^k : 0 \leq t < b^k/\ell\big\} = \big\{x' + \ell t : 0 \leq t < b^k/\ell\big\},$$

where $x' \equiv x \pmod{\ell}$. Therefore the minimum used to define $\mathbf{m}_{dx}$ is over the set of nonnegative integers less than b^k/ℓ. Moreover, if x is a multiple of ℓ, there is a value of t for which $x + at \equiv 0 \pmod{b^k}$. Fix such an x, and let t_0 denote a solution to $x + at \equiv 0 \pmod{b^k}$. Note that solutions to this congruence are uniquely determined modulo b^k/ℓ. Since $\mathtt{w}_b\big(x + at_0\big) = 0$ and the other two terms that define $f(t)$ are increasing in t, the minimum used to define $\mathbf{m}_{dx}$ can be further reduced to over the set $t \in \{0, \dots, t_0\}$.

Proof of Theorem 3. Let $a - 1 = qb^k + r$, where $0 \leq r \leq b^k - 1$. We use Lemma 1 and Proposition 2 to determine $\mathtt{g}(A)$ and $\mathtt{n}(A)$ when $d \geq h\big(k(b-1) - \lfloor \frac{a}{b^k} \rfloor\big)$ with $\gcd(a, d) = 1$.

(i)

$$\begin{aligned} \mathtt{g}(A) &= \max_{\mathbf{C}\in\mathscr{C}} \mathbf{m}_{\mathbf{C}} - a \\ &= \max_{1\leq x\leq a-1} \left(ha\left(\left\lfloor \frac{x}{b^k} \right\rfloor + \mathtt{w}_b\big(x \bmod b^k\big)\right) + dx\right) - a \\ &= \max\left\{ha\left(\left\lfloor \frac{qb^k - 1}{b^k} \right\rfloor + \mathtt{w}_b\big((qb^k - 1) \bmod b^k\big)\right) + d(qb^k - 1),\right. \end{aligned}$$

$$\max_{qb^k \le x \le qb^k+r} \Big(ha\left(q + \mathtt{w}_b\big(x \bmod b^k\big)\right) + dx\Big)\Big\} - a$$

$$= \max\Big\{ha\big((q-1) + k(b-1)\big) + d(qb^k - 1),$$

$$\max_{0 \le x \le r} \big(ha\big(q + \mathtt{w}_b(x)\big) + d(qb^k + x)\big)\Big\} - a$$

$$= haq + d(qb^k - 1) + \max\Big\{ha\big(k(b-1) - 1\big),$$

$$\max_{0 \le x \le r} \Big(ha \cdot \mathtt{w}_b(x) + d(x+1)\Big)\Big\} - a.$$

Let $f(x) := ha \cdot \mathtt{w}_b(x) + d(x+1)$ for $x \in \{0, \ldots, r\}$. Since $ha \cdot \mathtt{w}_b(x)$ is bounded for bounded x, $\max_{0 \le x \le r} f(x) = f(r)$ and $f(r) > ha\big(k(b-1) - 1\big)$ for all sufficiently large values of d. Hence, for all sufficiently large values of d,

$$\mathtt{g}(A) = haq + d(qb^k - 1) + ha \cdot \mathtt{w}_b(r) + d(r+1) - a = ha\big(q + \mathtt{w}_b(r)\big) + d(a-1) - a.$$

(ii) Observe that $\mathtt{w}_b(x) + \mathtt{w}_b(y) = k(b-1)$ if $x + y = b^k - 1$, so that $\sum_{x=0}^{b^k-1} \mathtt{w}_b(x) = \frac{1}{2}k(b-1)b^k$.

$$\mathtt{n}(A) = \frac{1}{a}\sum_{\mathbf{C} \in \mathscr{C}} \mathbf{m}_{\mathbf{C}} - \frac{1}{2}(a-1)$$

$$= \frac{1}{a}\sum_{x=1}^{a-1} \Big(ha\left(\left\lfloor \frac{x}{b^k} \right\rfloor + \mathtt{w}_b\big(x \bmod b^k\big)\right) + dx\Big) - \frac{1}{2}(a-1)$$

$$= h\sum_{x=1}^{a-1} \left\lfloor \frac{x}{b^k} \right\rfloor + h\left(\sum_{x=1}^{a-1} \mathtt{w}_b\big(x \bmod b^k\big)\right) + \frac{1}{2}d(a-1) - \frac{1}{2}(a-1)$$

$$= h\sum_{m=0}^{q-1} \sum_{x=mb^k}^{(m+1)b^k-1} \left\lfloor \frac{x}{b^k} \right\rfloor + h\sum_{x=qb^k}^{qb^k+r} \left\lfloor \frac{x}{b^k} \right\rfloor + h\sum_{m=0}^{q-1} \sum_{x=mb^k}^{(m+1)b^k-1} \mathtt{w}_b\big(x \bmod b^k\big)$$

$$+ h\sum_{x=qb^k}^{qb^k+r} \mathtt{w}_b\big(x \bmod b^k\big) + \frac{1}{2}(a-1)(d-1)$$

$$= h\sum_{m=0}^{q-1} \sum_{x=mb^k}^{(m+1)b^k-1} m + h\sum_{x=qb^k}^{qb^k+r} q + h\sum_{m=0}^{q-1} \sum_{x=0}^{b^k-1} \mathtt{w}_b(x) + h\sum_{x=0}^{r} \mathtt{w}_b(x)$$

$$+ \frac{1}{2}(a-1)(d-1)$$

$$= h\left(\frac{1}{2}q(q-1)b^k + q(r+1) + \frac{1}{2}qk(b-1)b^k + \sum_{x=0}^{r} \mathtt{w}_b(x)\right)$$

$$+\frac{1}{2}(a-1)(d-1)$$
$$= \quad h\left(\frac{1}{2}q\big(q-1+k(b-1)\big)b^k + q(r+1) + \sum_{x=0}^{r} \mathtt{w}_b(x)\right) + \frac{1}{2}(a-1)(d-1).$$

We note that $\gcd(a,d) = 1$ implies that at least one of a, d is odd, and hence that $\frac{1}{2}(a-1)(d-1)$ is an integer. □

4. The special case $\{a, a+1, a+2, a+2^2, \ldots, a+2^k\}$

The special case $h = 1$ of Theorem 3 was first studied by Hofmeister [5], who gave an exact formula for $\mathtt{g}(A)$ which holds for all sufficiently large d; see Theorem 2 in the Introduction. However, there appears to be a mistake in this result, as discussed in Remark 1. Selmer [8] additionally considered the special case $d = 1$ and $b = 2$ considered by Hofmeister, and determined both $\mathtt{g}(A)$ and $\mathtt{n}(A)$ when $a > (k-3)2^k+1$; see Theorem 1 in the Introduction. We use the result in Theorem 3 to show that Selmer's two results hold for $\lfloor \frac{a}{2^k} \rfloor \geq k-1$, which is slightly weaker than Selmer's bound for validity. Theorem 3 reduces to the following result when $h = d = 1$ and $b = 2$. The expressions for both $\mathtt{g}(A)$ and $\mathtt{n}(A)$ involve a term that depends on the residue class of $a-1$ modulo 2^k. In the case of $\mathtt{g}(A)$, that term is $f(r)$ and this is given as a maximum of two explicitly computable expressions. In the case of $\mathtt{n}(A)$, that term is the one involving a sum that depends on this residue class.

Theorem 4. *Let a, k be positive integers. Let $q = \lfloor \frac{a-1}{2^k} \rfloor$ and $r \equiv a-1 \pmod{2^k}$, $0 \leq r < 2^k$. If $A = \{a, a+1, a+2, a+2^2, \ldots, a+2^k\}$ and $\lfloor \frac{a}{2^k} \rfloor \geq k-1$, then*

(i) $\mathtt{g}(A) = qa - r - 2 + f(r)$, *where*

$$f(r) = \begin{cases} \max\left\{a(k-1), ak_0 + 2^{k_0}\right\} & \text{if } r = 2^{k_0}-1; \\ \max\left\{a(k-1), a(k_0-1) + 2^{k_0} - 2^{j_0}\right\} & \text{if } (2^{k_0}-1) - 2^{j_0} \\ & \quad \leq r < (2^{k_0}-1) - 2^{j_0-1}. \end{cases}$$

(ii) $\mathtt{n}(A) = \frac{1}{2}q\big(a + r + 1 + (k-1)2^k\big) + \sum_{x=0}^{r} \mathtt{w}_2(x)$.

Proof. This is a special case of Theorem 3, and follows easily by putting $h = d = 1$ and $b = 2$ at the appropriate places. The result for $\mathtt{g}(A)$ can be further simplified since we can determine the maximum, which involves the expression

$$f(r) := \max_{0 \leq x \leq r} \big(a \cdot \mathtt{w}_2(x) + x + 1\big)$$

for $r \in \{0, 1, \ldots, 2^k - 1\}$. By Proposition 1, part (ii), the maximum may be taken over the set $\{\overline{r}, \ldots, r\}$.

If $r = 2^{k_0} - 1$ for $k_0 \in \{0, 1, \dots, k\}$, then $\overline{r} = r$ by Proposition 1, part (i). Hence $f(r) = a \cdot \mathtt{w}_2(r) + r + 1 = ak_0 + 2^{k_0}$.

Otherwise $(2^{k_0} - 1) - 2^{j_0} \le r < (2^{k_0} - 1) - 2^{j_0 - 1}$, with $j_0 \in \{1, \dots, k_0 - 1\}$. In this case, $\overline{r} = (2^{k_0} - 1) - 2^{j_0}$ by Proposition 1, part (i).

For $x \in \{\overline{r} + 1, \dots, r\}$, $\mathtt{w}_2(x) < \mathtt{w}_2(\overline{r})$ and $x - \overline{r} \le r - \overline{r} < 2^k < a$. Hence $f(\overline{r}) - f(x) = a\big(\mathtt{w}_2(\overline{r}) - \mathtt{w}_2(x)\big) + (\overline{r} - x) > 0$, so that $f(r) = f(\overline{r}) = a \cdot \mathtt{w}_2(\overline{r}) + \overline{r} + 1 = a(k_0 - 1) + 2^{k_0} - 2^{j_0}$. □

Proof of equivalence of Theorem 1 and Theorem 4.

(i) To see that the formula for $\mathtt{g}(A)$ in Theorem 4, part (i) matches the result in Theorem 1, part (i), write $a = q2^k + r + 1$, $0 \le r < 2^k$. Then the sum in Theorem 1, part (i) simplifies to

$$\sum_{i=0}^{k-1} 2^i \left\lfloor \frac{a + 2^i}{2^k} \right\rfloor = q(2^k - 1) + \sum_{i=0}^{k-1} 2^i \left\lfloor \frac{r + 1 + 2^i}{2^k} \right\rfloor .$$

If $r = 2^k - 1$, then $2^k \mid a$, and Theorem 1, part (i) gives $\mathtt{g}(A) = (q + 1)(a + 1) + q(2^k - 1) + (2^k - 1) + (k - 2)a - 1 = (q + k - 1)a + (q + 1)2^k - 1 = (q + k)a - 1$. The result of Theorem 4, part (i) gives $\mathtt{g}(A) = qa - r - 2 + (ak + 2^k) = (q + k)a - 1$, as desired.

If $r = 2^{k-1} - 1$, Theorem 1, part (i) gives $\mathtt{g}(A) = q(a + 1) + q(2^k - 1) + 2^{k-1} + (k - 2)a - 1 = (q + k - 2)a + q2^k + 2^{k-1} - 1 = (q + k - 1)a - r - 2 + 2^{k-1}$. The result of Theorem 4, part (i) gives $\mathtt{g}(A) = qa - r - 2 + \big(a(k - 1) + 2^{k-1}\big) = (q + k - 1)a - r - 2 + 2^{k-1}$, as desired.

If $r = 2^{k_0} - 1$ for some $k_0 < k - 1$, Theorem 1, part (i) gives $\mathtt{g}(A) = q(a + 1) + q(2^k - 1) + (k - 2)a - 1 = (q + k - 2)a + q2^k - 1 = (q + k - 1)a - r - 2$. The result of Theorem 4, part (i) gives $\mathtt{g}(A) = qa - r - 2 + a(k - 1) = (q + k - 1)a - r - 2$, as desired.

Otherwise $(2^{k_0} - 1) - 2^{j_0} \le r < (2^{k_0} - 1) - 2^{j_0 - 1}$ for some j_0, k_0 with $1 \le j_0 < k_0 \le k$. Two cases arise: (i) $k_0 = k$, and (ii) $k_0 < k$. In case (i), $r + 1 + 2^{j_0 - 1} < 2^k \le r + 1 + 2^i < 2^{k+1}$ for $i \ge j_0$. Therefore Theorem 1, part (i) gives $\mathtt{g}(A) = q(a + 1) + q(2^k - 1) + (2^{j_0} + 2^{j_0 + 1} + \dots + 2^{k-1}) + (k - 2)a - 1 = (q + k - 1)a - r - 2 + (2^k - 2^{j_0})$. The result of Theorem 4, part (i) gives $\mathtt{g}(A) = qa - r - 2 + a(k - 1) + (2^k - 2^{j_0}) = (q + k - 1)a - r - 2 + (2^k - 2^{j_0})$, as desired. In case (ii), $r + 1 + 2^{k-1} < 2^k$. Therefore Theorem 1, part (i) gives $\mathtt{g}(A) = q(a+1) + q(2^k - 1) + (k - 2)a - 1 = (q + k - 1)a - r - 2$. The result of Theorem 4, part (i) gives $\mathtt{g}(A) = qa - r - 2 + a(k - 1) = (q + k - 1)a - r - 2$, as desired. Thus the results of Theorem 4, part (i) and Theorem 1, part (i) are identical when $a \ge (k - 1)2^k$.

(ii) To see that the formula for $\mathtt{n}(A)$ in Theorem 4, part (ii) matches the result in Theorem 1, part (ii), we use $r = (a - 1) - \lfloor \frac{a-1}{2^k} \rfloor 2^k$ to get

$$\mathtt{n}(A) = \left\lfloor \frac{a - 1}{2^k} \right\rfloor \left(a + 2^{k-1} \left(k - 1 - \left\lfloor \frac{a - 1}{2^k} \right\rfloor \right) \right) + \sum_{x=0}^{r} \mathtt{w}_2(x).$$

Recall that $B(n)$ denotes the total number of ones in the binary representations of $0, 1, \ldots, n-1$, so that it is given by the expression $\sum_{x=0}^{n-1} \mathtt{w}_2(x)$. If $2^k \nmid a$, then $\lfloor \frac{a-1}{2^k} \rfloor = \lfloor \frac{a}{2^k} \rfloor$ and $\sum_{x=0}^{r} \mathtt{w}_2(x) = B(a - \lfloor \frac{a}{2^k} \rfloor 2^k)$. If $2^k \mid a$, then $\lfloor \frac{a-1}{2^k} \rfloor = \lfloor \frac{a}{2^k} \rfloor - 1$ and $\sum_{x=0}^{r} \mathtt{w}_2(x) = k2^{k-1}$ while $B(a - \lfloor \frac{a}{2^k} \rfloor 2^k) = 0$. In both cases, we easily verify this reduces to the formula in Theorem 1, part (ii). Thus the results of Theorem 4, part (ii) and Theorem 1, part (ii) are identical when $a \geq (k-1)2^k$.

This completes the proof of the equivalence. □

Concluding remarks. The results of Theorems 2 and 3 hold only for sufficiently large values of d, and that of Theorem 1 holds only for sufficiently large values of a. In fact, Theorem 1 fails to hold when $a = (k-3)2^k + 1$. When $h = d = 1$ and $b = 2$, the computation of $\mathbf{m}_x$ in Proposition 2 may be possible even when $a \leq (k-3)2^k + 1$. Lemma 1 may then be applied to determine both $\mathtt{g}(A)$ and $\mathtt{n}(A)$ in the remaining cases.

Acknowledgment

The author gratefully acknowledges the many varied comments of the referee that has contributed to a cleaner and clearer exposition of this manuscript.

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, J.E. Shockley, On a problem of Frobenius, J. Reine Angew. Math. 211 (1962) 215–220.
[4] D.D. Grant, On linear forms whose coefficients are in arithmetic progression, Israel J. Math. 15 (1973) 204–209.
[5] G.R. Hofmeister, Zu einem Problem von Frobenius, Nor. Vidensk. Selsk. Skr. 5 (1966) 1–37.
[6] J.L. Ramírez Alfonsín, The Diophantine Frobenius Problem, Oxford Lecture Series in Mathematics and Its Applications, vol. 30, Oxford University Press, 2005.
[7] J.B. Roberts, Note on linear forms, Proc. Amer. Math. Soc. 7 (1956) 465–469.
[8] E.S. Selmer, On the linear Diophantine problem of Frobenius, J. Reine Angew. Math. 293/294 (1977) 1–17.
[9] J.J. Sylvester, Problem 7382, in: W.J.C. Miller (Ed.), Mathematical Questions, with Their Solutions, from the “Educational Times”, vol. 41, 1884, p. 21. Solution by W.J. Curran Sharp.
[10] A. Tripathi, The coin exchange problem for arithmetic progressions, Amer. Math. Monthly 101 (10) (1994) 779–781.
[11] A. Tripathi, The Frobenius problem for modified arithmetic progressions, J. Integer Seq. 16 (7) (2013) 13.7.4.
[12] D.X. Zheng, A note on the Frobenius problem for linear forms, Sichuan Daxue Xuebao 29 (2) (1992) 188–192 (in Chinese).