Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
Vol. 24, 2018, No. 2, 71–73
DOI: 10.7546/nntdm.2018.24.2.71-73

A note on the Frobenius and the Sylvester numbers

Amitabha Tripathi

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

Received: 30 March 2017 **Accepted:** 7 May 2018

Abstract: Positive integers that cannot be represented by a linear form with relatively prime coefficients and over nonnegative integers are finite in number. We describe a connection between the largest number in this set and the cardinality of this set. We also describe a connection with a subset related to this set.
Keywords: Representable, Frobenius number.
2010 Mathematics Subject Classification: 11D07.

The Frobenius Coin Exchange problem revolves around the set $\Gamma^c(\{a_1,\ldots,a_k\})$ of positive integers that are not representable by the linear form $a_1x_1+\cdots+a_kx_k$. For brevity, let us call $A=\{a_1,\ldots,a_k\}$. For the set $\Gamma^c(A)$ to be a finite set it is necessary and sufficient that $\gcd A=1$. The Frobenius problem operates under this assumption. Two classical problems involving the set $\Gamma^c(A)$ are the determination of the functions $\mathtt{g}(A)$ and $\mathtt{n}(A)$, both due to Sylvester [2], given by

$$\mathtt{g}(A) := \max \Gamma^c(A), \quad \mathtt{n}(A) := \big|\Gamma^c(A)\big|. \tag{1}$$

The number $\mathtt{g}(A)$ is often called the *Frobenius number* of A and the number $\mathtt{n}(A)$ sometimes called the *Sylvester number* of A, the former due to the fact that Frobenius popularized the problem posed by Sylvester in his lectures.

The set $\Gamma(A)=\{a_1x_1+\cdots+a_kx_k : x_i\geq 0\}$ is closed under addition. So at most one of n, $\mathtt{g}(A)-n$ can belong to $\Gamma(A)$. By pairing the integers n and $\mathtt{g}(A)-n$ in $\{0,\ldots,\mathtt{g}(A)\}$, we see that at least one integer in each pair belongs to $\Gamma^c(A)$. Hence $\mathtt{n}(A)\geq\frac{1}{2}\big(1+\mathtt{g}(A)\big)$. Equality occurs precisely when exactly one of n, $\mathtt{g}(A)-n$ belongs to $\Gamma^c(A)$, for each $n\in\{0,\ldots,\mathtt{g}(A)\}$.

This inequality, together with different conditions under which equality may occur, appear in [1]. However, the equivalence we state and prove next is very easy to see and possibly has the status of folklore.

Theorem 1. *Let A be a set of positive integers with* $\gcd A = 1$. *The following are equivalent:*

(i) $n \in \Gamma^c(A)$ *implies* $\mathtt{g}(A) - n \in \Gamma(A)$ *for each* $n \in \{0, \ldots, \mathtt{g}(A)\}$.

(ii) $\mathtt{n}(A) = \frac{1}{2}\big(1 + \mathtt{g}(A)\big)$.

Proof. Condition (ii) holds exactly when one of n, $\mathtt{g}(A) - n$ belongs to $\Gamma(A)$ and the other to $\Gamma^c(A)$, for each $n \in \{0, \ldots, \mathtt{g}(A)\}$. Since we already have this situation to hold when $n \in \Gamma(A)$, the remaining condition, given by (i), is equivalent to condition (ii). □

The fact that $\Gamma(A)$ is closed under addition implies $n + \Gamma(A) \subseteq \Gamma(A)$ whenever $n \in \Gamma(A)$. What if we asked for the same property to hold for $n \in \Gamma^c(A)$? We will need to modify the condition a little, since $0 \in \Gamma(A)$ and $n + 0 \notin \Gamma(A)$. To exclude this trivial possibility, we define

$$\mathcal{S}^\star(A) := \big\{n \in \Gamma^c(A) : n + \Gamma^\star \subset \Gamma^\star\big\}, \tag{2}$$

where $\Gamma^\star(A) = \Gamma(A) \setminus \{0\}$.

The set $\mathcal{S}^\star(A)$ is never empty, for $\mathtt{g}(A) \in \mathcal{S}^\star(A)$. Is it ever possible for $\mathcal{S}^\star(A) = \{\mathtt{g}(A)\}$? To answer this question, fix $a \in A$, and let $\mathbf{m}_x$ denote the smallest integer in $\Gamma(A) \cap (x)$, where (x) denotes the residue class of x modulo a. Thus $\Gamma^c(A) \cap (x)$ consists of the nonnegative integers of the form $\mathbf{m}_x - \lambda a$, with $\lambda \geq 1$. Since $\big(\mathbf{m}_x - \lambda a\big) + a \notin \Gamma(A)$ for $\lambda > 1$, we have

$$\mathcal{S}^\star(A) \subseteq \big\{\mathbf{m}_x - a : 1 \leq x \leq a - 1\big\}. \tag{3}$$

In order that $\mathbf{m}_x - a \in \mathcal{S}^\star(A)$ for some $x \in \{1, \ldots, a-1\}$, it is necessary that $\big(\mathbf{m}_x - a\big) + \mathbf{m}_y \in \Gamma(A)$ for each $y \in \{1, \ldots, a-1\}$. This condition is also sufficient since any $n \in \Gamma(A)$ is of the form $\mathbf{m}_y + \lambda a$ with $y \in \{0, \ldots, a-1\}$ and $\lambda \geq 1$. Since $\big(\mathbf{m}_x - a\big) + \mathbf{m}_y \equiv x + y \mod a$, we must have $\big(\mathbf{m}_x - a\big) + \mathbf{m}_y \geq \mathbf{m}_{x+y}$, for each $y \in \{1, \ldots, a-1\}$. Hence we have shown that

$$\mathbf{m}_x - a \in \mathcal{S}^\star(A) \iff \mathbf{m}_x + \mathbf{m}_y \geq \mathbf{m}_{x+y} + a \quad \text{for} \quad 1 \leq y \leq a - 1. \tag{4}$$

The definition in Eqn. (2) and results in Eqn. (3) and Eqn. (4) are from [3].

We are now in position to partially answer the question about when $\mathcal{S}^\star(A) = \{\mathtt{g}(a, b)\}$. The connection is due to the fact that the largest integer in $\Gamma^c(A)$ is the largest among $\mathbf{m}_x - a$, with $x \in \{1, \ldots, a-1\}$.

Theorem 2. *Let A be a set of positive integers with* $\gcd A = 1$. *If* $n \in \Gamma^c(A)$ *implies* $\mathtt{g}(A) - n \in \Gamma(A)$ *for each* $n \in \{0, \ldots, \mathtt{g}(A)\}$, *then*

$$\mathcal{S}^\star(A) = \{\mathtt{g}(A)\}.$$

Proof. Note that $\mathtt{g}(A) \in \mathcal{S}^\star(A)$ because any integer greater than $\mathtt{g}(A)$ belongs to $\Gamma(A)$. Fix $a \in A$, and let $\mathtt{g}(A) = \mathbf{m}_r - a$ with $r \in \{1, \ldots, a-1\}$.

Suppose condition (i) of Theorem 1 holds. Then exactly one of n, $\mathtt{g}(A) - n$ belongs to $\Gamma^c(A)$, for each $n \in \{0, \ldots, \mathtt{g}(A)\}$. Suppose $n \in \mathcal{S}^\star(A)$, $n \neq \mathtt{g}(A)$. Then $n = \mathbf{m}_x - a$ for some $x \in \{1, \ldots, a-1\} \setminus \{r\}$. Since $n \in \Gamma^c(A)$, $\mathtt{g}(A) - n = \mathbf{m}_r - \mathbf{m}_x \in \Gamma(A)$, and must therefore be at least as much as the least integer in $\Gamma(A)$ in its congruence class. Therefore $\mathbf{m}_r - \mathbf{m}_x \geq \mathbf{m}_{r-x}$, so that $\mathbf{m}_x + \mathbf{m}_{r-x} \leq \mathbf{m}_r$. It follows from (4) that $n = \mathbf{m}_x - a \notin \mathcal{S}^\star(A)$ for $x \neq r$. □

Corollary 1. *Let A be a set of positive integers with* $\gcd A = 1$. *Then*

$$\mathtt{n}(A) = \frac{1}{2}\big(1 + \mathtt{g}(A)\big) \ \textit{implies} \ \mathcal{S}^\star(A) = \{\mathtt{g}(A)\}.$$

There are many instances where the converse of Theorem 2 (or to Corollary 1) holds. One such instance is the case of the geometric sequence $A = \{a^k, a^{k-1}b, \ldots, b^k\}$, where $\gcd(a, b) = 1$. However, for the arithmetic sequence $A = \{a, a+d, \ldots, a+kd\}$, where $\gcd(a, d) = 1$, it turns out that whereas $\mathtt{n}(A) > \frac{1}{2}\big(1 + \mathtt{g}(A)\big)$, we have $\mathcal{S}^\star(A) = \{\mathtt{g}(A)\}$ when $k \mid (a-2)$; refer [3].

References

[1] Nijenhuis, M. & Wilf, H. S. (1972) Representation of integers by linear forms in nonnegative integers, *J. Number Theory*, 4, 98–106.

[2] Sylvester, J. J. (1884) Problem 7382, in W. J. C. Miller, ed., *Mathematical Questions*, with their Solutions, from the "Educational Times", 41, 1884, p. 21. Solution by W. J. Curran Sharp.

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