#A75 INTEGERS 20 (2020)

ON NUMERICAL SEMIGROUPS GENERATED BY PRIMITIVE PYTHAGOREAN TRIPLETS

Edgar Federico Elizeche
Department of Mathematics, Indian Institute of Technology, Hauz Khas, New Delhi, India
maz188235@maths.iitd.ac.in

Amitabha Tripathi[1]
Department of Mathematics, Indian Institute of Technology, Hauz Khas, New Delhi, India
atripath@maths.iitd.ac.in

Received: 2/13/19, Revised: 6/11/20, Accepted: 8/29/20, Published: 9/11/20

Abstract

For any set of positive integers A with $\gcd A = 1$, let $S = \langle A \rangle$ denote the numerical semigroup generated by A. Let $\mathrm{F}(S)$, $\mathrm{g}(S)$, and $\mathrm{PF}(S)$ denote the Frobenius number, genus, and the set of pseudo-Frobenius numbers of S, respectively. For a set A of primitive Pythagorean triplets, we determine $\mathrm{F}(S)$, $\mathrm{g}(S)$, and $\mathrm{PF}(S)$.

1. Introduction

By $\mathbb{Z}_{\geq 0}$ and $\mathbb{N}$ we mean the set of non-negative integers and the set of positive integers, respectively. A numerical semigroup is a subset S of $\mathbb{Z}_{\geq 0}$ that is closed under addition, $0 \in S$ and $\mathbb{N} \setminus S$ is a finite set. The semigroup generated by a list of positive integers $a_1, \ldots, a_k$ is

$$\langle a_1, \ldots, a_k \rangle = \Big\{ a_1x_1 + \cdots + a_kx_k : x_i \in \mathbb{Z}_{\geq 0} \Big\}.$$

It is not difficult to show that $\langle a_1, \ldots, a_k \rangle$ is a numerical semigroup if and only if $\gcd(a_1, \ldots, a_k) = 1$.

The set $A = \{a_1, \ldots, a_k\}$ is called a system of generators of the semigroup $S = \langle a_1, \ldots, a_k \rangle$. For a semigroup S, A is a minimal system of generators if A generates S and no proper subset of A generates S. Every numerical semigroup has a unique minimal system of generators. This system of generators is finite, and the cardinality of this minimal system of generators is called the *embedding*

[1] Corresponding author

dimension of S, and is denoted by $\mathrm{e}(S)$. The smallest positive integer in S is called the *multiplicity* of S, and denoted by $\mathrm{m}(S)$. It is not difficult to show that $\mathrm{e}(S) \leq \mathrm{m}(S)$. We say that S has *maximal embedding dimension* if $\mathrm{e}(S) = \mathrm{m}(S)$.

The set $\mathbb{Z}_{\geq 0} \setminus S$ is called the *gap set* of S, and is denoted by $\mathrm{G}(S)$. The *Frobenius number* of S, denoted by $\mathrm{F}(S)$, is the largest element in $\mathrm{G}(S)$. The *genus* of S, denoted by $\mathrm{g}(S)$, is the cardinality of $\mathrm{G}(S)$.

Although the origins of the problem of determining $\mathrm{F}(S)$ is attributed to Sylvester [15], an apparent reason for associating the name of Frobenius with this problem is possibly due to the fact that he was largely instrumental in popularizing this problem in his lectures. The Frobenius problem has a rich and long history, with several applications and extensions, and connections to several areas of research; refer [10] for a comprehensive survey of the Frobenius problem. Exact determination of the Frobenius number is a difficult problem in general. In the absence of exact results, research on the Frobenius problem has often focused on sharpening bounds on the Frobenius number and on algorithmic aspects. Although running time of these algorithms is superpolynomial, it is known that the Frobenius problem can be solved in polynomial time for fixed number of variables, and that the problem is NP-hard under Turing reduction; see [7]. For more results on algorithmic aspects and on complexity, refer [3, 9, 10, 11]. Corresponding results for $\mathrm{g}(S)$ have been much rarer, even in special cases.

A very useful tool in the study of numerical semigroups is the determination of an Apéry set of the semigroup. Given a numerical semigroup S, and $a \in S$, the Apéry set of S corresponding to a is given by

$$\mathrm{Ap}(S, a) = \big\{\mathbf{m}_x : 0 \leq x \leq a-1\big\},$$

where $\mathbf{m}_x$ denotes the least positive integer in S congruent to x modulo a; see [1].

A well known result of Brauer & Shockley [2] shows how $\mathrm{F}(S)$ can be determined from the Apéry set of S corresponding to any $a \in S$; see Proposition 1.

The set $S = \langle A \rangle$ is closed under addition, and so $n + S \subseteq S$ whenever $n \in S$. It is conceivable that $n \in \mathrm{G}(S)$ satisfy a slightly modified condition, replacing S by $S^\star = S \setminus \{0\}$. In fact, $\mathrm{F}(S)$ is clearly the largest number satisfying such a condition. Thus we study the set given by

$$\mathrm{PF}(S) = \big\{n \,\in\, \mathrm{G}(S) : n + S^\star \subset S^\star\big\}.$$

Members of $\mathrm{PF}(S)$ are called *pseudo-Frobenius* numbers. The size of $\mathrm{PF}(S)$ is called the *type* of S and denoted by $\mathrm{t}(S)$.

A numerical semigroup $S = \langle A \rangle$ is *irreducible* if S cannot be expressed as the intersection of two numerical semigroups properly containing it, *symmetric* if S is irreducible and $\mathrm{F}(S)$ is odd, and *pseudo-symmetric* if S is irreducible and $\mathrm{F}(S)$ is even. The following result characterizes symmetric and pseudo-symmetric semigroups.

Lemma 1. *([13, Corollary 4.11, 4.16]) Let S be the numerical semigroup. Then*

(i) *S is symmetric if and only if $PF(S) = \{F(S)\}$.*

(ii) *S is pseudo-symmetric if and only if $PF(S) = \left\{F(S), \frac{1}{2}F(S)\right\}$.*

We say that a numerical semigroup S has the *Arf* property if, for any $x, y, z \in S$ with $x \geq y \geq z$, we have $x + y - z \in S$. We say that S is *saturated* if whenever $s, s_1, \ldots, s_k \in S$, $s_i \leq s$ for each i, and $n_1, \ldots, n_k \in Z$ with $n_1 s_1 + \cdots + n_k s_k \geq 0$, then $s + n_1 s_1 + \cdots + n_k s_k \in S$. It is evident that every saturated numerical semigroup has the Arf property. Moreover, every numerical semigroup with Arf property has maximal embedding dimension; see [13, p. 23].

In this paper, we determine the Frobenius number $\mathrm{F}(S)$, the genus $\mathrm{g}(S)$, and the set $\mathrm{PF}(S)$ of pseudo-Frobenius numbers when $A = \{a, b, c\}$, with $a^2 + b^2 = c^2$, $\gcd(a, b, c) = 1$. The basis of our results is the determination of the Apéry set $\mathrm{Ap}(S, c)$ in Theorem 1. We use this to determine $\mathrm{F}(S)$, $\mathrm{g}(S)$, and the set $\mathrm{PF}(S)$ in Theorem 2. These formulae also follow from a result of Kraft [8], cited by Fel [4], using the algorithm given by Johnson [6]. Our proof uses basic results of Brauer & Shockley [2], Selmer [14], and Tripathi [16]. We also discuss whether or not S is symmetric, pseudo-symmetric, saturated, has the Arf property, and has maximal embedding dimension in Remarks 1, 2, and 3. For the case $e(S) = 3$, $\mathrm{F}(S)$, $\mathrm{g}(S)$ and $\mathrm{PF}(S)$ can also be determined by computing the entries of a 3×3 matrix with integer entries; see Proposition 3. We close this paper by determining these entries in Theorem 5, thereby finding another set of proofs for our main results.

2. Preliminary Results

Suppose A is any set of positive integers with $\gcd A = 1$, and let $S = \langle A \rangle$. Fix $a \in A$. For each residue class $\mathbf{C}$ modulo a, let $\mathbf{m_C}$ denote the least integer in $S \cap \mathbf{C}$. It is well known that $\mathrm{F}(S)$ and $\mathrm{g}(S)$ are easily determined from the values of $\mathbf{m_C}$. The following result, part (i) of which is due to Brauer & Shockley [2] and part (ii) to Selmer [14], is often a key step in this determination.

Proposition 1. *([2], [14]) Let A be any set of positive integers with* $\gcd(A) = 1$, *and let $S = \langle A \rangle$. Let $a \in A$, and let $\mathbf{m}_x$ denote the least integer in S congruent to x modulo a, $0 \leq x \leq a - 1$. Then*

(i)

$$F(S) = \left(\max_{1 \leq x \leq a-1} \mathbf{m}_x \right) - a.$$

(ii)

$$g(S) = \frac{1}{a} \sum_{x=1}^{a-1} \mathbf{m}_x - \frac{1}{2}(a-1).$$

The set $\mathrm{PF}(S)$ consists of positive integers n in $\mathrm{G}(S)$ such that translating the set of positive integers in S by n results in a subset of S. Since $\mathrm{F}(S) = \max \mathrm{PF}(S)$, determining $\mathrm{PF}(S)$ ensures that $\mathrm{F}(S)$ is also determined. The following result is due to Tripathi [16].

Proposition 2. *([16]) Let A be any set of positive integers with $\gcd(A) = 1$, and let $S = \langle A \rangle$. Let $a \in A$, and let $\mathbf{m}_x$ denote the least integer in S congruent to x modulo a, $0 \le x \le a-1$. Then*

$$PF(S) = \big\{ \mathbf{m}_x - a : \mathbf{m}_x + \mathbf{m}_y \ge \mathbf{m}_{x+y} + a \text{ for } 1 \le y \le a-1 \big\}.$$

For the case where $|A| = 3$, Johnson [6] determined $\mathrm{F}(S)$ in terms of the entries of a 3×3 matrix with integer entries. The entries from this matrix were later used by Rosales and García-Sánchez [12] to determine $\mathrm{g}(S)$ and $\mathrm{PF}(S)$.

Proposition 3. *([6, 12]) Let $A = \{a, b, c\}$ be a set of positive integers, with $\gcd(a, b, c) = 1$. Define c_1, c_2, c_3 by*

$$\begin{aligned} c_1 &= \min \big\{ m \in \mathbb{N} : ma \in \langle b, c \rangle \big\}, \\ c_2 &= \min \big\{ m \in \mathbb{N} : mb \in \langle a, c \rangle \big\}, \\ c_3 &= \min \big\{ m \in \mathbb{N} : mc \in \langle a, b \rangle \big\}. \end{aligned}$$

Then there exist nonnegative integers $r_{12}, r_{13}, r_{21}, r_{23}, r_{31}, r_{32}$ such that

$$c_1 a = r_{12} b + r_{13} c, \quad c_2 b = r_{21} a + r_{23} c, \quad c_3 c = r_{31} a + r_{32} b.$$

Moreover, if the elements in A are pairwise coprime, then each $r_{ij} \ge 1$ and each $c_i = r_{ji} + r_{ki}$. Further,

(i)
$$F(S) = \max \big\{ (c_3 - 1)c + (r_{12} - 1)b - a, (c_2 - 1)b + (r_{13} - 1)c - a \big\}.$$

(ii)
$$g(S) = \frac{1}{2}\big((c_1 - 1)a + (c_2 - 1)b + (c_3 - 1)c - c_1 c_2 c_3 + 1 \big).$$

(iii)
$$PF(S) = \big\{ (c_3 - 1)c + (r_{12} - 1)b - a, (c_2 - 1)b + (r_{13} - 1)c - a \big\}.$$

3. Main Results

Let $A = \{a, b, c\}$ be a set of primitive Pythagorean triplets. Then there exist positive integers r, s with $r > s$, $\gcd(r, s) = 1$, and with r, s of opposite parity, such that

$$a = r^2 - s^2, \quad b = 2rs, \quad c = r^2 + s^2.$$

In this section, we give explicit formula for $\mathrm{F}(S)$ and $\mathrm{g}(S)$, and determine $\mathrm{PF}(S)$, where $S = \langle A \rangle$. To do this, we first determine the set of the minimum representative integers $\mathbf{m}_x$ in $\langle a, b \rangle$ as x runs through all non-zero residue classes modulo c (Theorem 1). We then use Propositions 1 and 2 to determine $\mathrm{F}(S)$ and $\mathrm{g}(S)$, and $\mathrm{PF}(S)$, respectively (Theorem 2).

Johnson [6] showed that the positive integers c_1, c_2, c_3 and $r_{12}, r_{13}, r_{21}, r_{23}, r_{31}, r_{32}$ which form the entries in the 3×3 matrix (refer Proposition 3) may be characterized by properties that do not require the computation of the minimum elements of the three sets in Proposition 3. Kraft [8] determined these nine entries in the case where A is a Pythagorean triple, and verified his result via the characterization given in [6]. We close this section by determining the nine entries given by Proposition 5 directly, without using the characterization in [6].

Gil et al. [5] have also determined the Frobenius number $\mathrm{F}(S)$. They have shown that $(r-1)(a+b)-c$ is the largest integer not representable by the form $ax+by+cz$ with $x, y, z \in \mathbb{Z}_{\geq 0}$, but how they arrive at their formula remains a mystery.

We begin by describing a complete residue system modulo c.

Proposition 4. *Let r, s be coprime positive integers of opposite parity, $r > s$. Let $a = r^2 - s^2$, $b = 2rs$, and $c = r^2 + s^2$. Then*

$$\big\{\lambda a + \mu b : 0 \leq \lambda < r+s, 0 \leq \mu < s\big\} \bigcup \big\{\lambda a + \mu b : 0 \leq \lambda < r, s \leq \mu < r\big\}$$

is a complete residue system modulo c.

Proof. Let $X = \big\{\lambda a + \mu b : 0 \leq \lambda < r+s, 0 \leq \mu < s\big\}$ and $Y = \big\{\lambda a + \mu b : 0 \leq \lambda < r, s \leq \mu < r\big\}$. Since $a \equiv 2r^2 \pmod{c}$ and $\gcd(2r, c) = 1$, $\lambda_1 a + \mu_1 b \equiv \lambda_2 a + \mu_2 b \pmod{c}$ is equivalent to $\lambda_1 r + \mu_1 s \equiv \lambda_2 r + \mu_2 s \pmod{c}$, or to $\lambda r + \mu s \equiv 0 \pmod{c}$ with $\lambda = \lambda_1 - \lambda_2$ and $\mu = \mu_1 - \mu_2$. Now

$$\max\big\{\lambda r + \mu s\big\} = \begin{cases} r(r+s-1) + s(s-1) & \text{if } \lambda_1 a + \mu_1 b,\ \lambda_2 a + \mu_2 b \in X; \\ r(r-1) + s(r-s-1) & \text{if } \lambda_1 a + \mu_1 b,\ \lambda_2 a + \mu_2 b \in Y; \\ (r-1)(r+s) & \text{if } \lambda_1 a + \mu_1 b,\ \lambda_2 a + \mu_2 b \\ & \text{are in different sets.} \end{cases}$$

By interchanging $\lambda_1 a + \mu_1 b$ and $\lambda_2 a + \mu_2 b$ if necessary, we may assume $\lambda r + \mu s \geq 0$. In each case $\lambda r + \mu s < 2(r^2 + s^2) = 2c$, and so $\lambda r + \mu s \in \{0, c\}$.

Case (i). If $\lambda r + \mu s = 0$, then $r \mid \mu$ since $\gcd(r, s) = 1$. Since $|\mu| < r$, this is only possible when $\mu = 0$. But then $\lambda = 0$ as well, so that $\lambda_1 a + \mu_1 b = \lambda_2 a + \mu_2 b$.

Case (ii). If $\lambda r + \mu s = c = r^2 + s^2$, then $\lambda = r - st$ and $\mu = s + rt$ for some $t \in \mathbb{Z}$. From $|\lambda| < r + s$ we have $t \geq 0$ and from $|\mu| < r$ we have $t \leq 0$. Therefore, $t = 0$, so that $\lambda = \lambda_1 - \lambda_2 = r$ and $\mu = \mu_1 - \mu_2 = s$. But then $\lambda_1 \geq r$ and $\mu_1 \geq s$, which is impossible.

To complete the proof, note that $|X \cup Y| = |X| + |Y| = s(r+s) + r(r-s) = c$ since $X \cap Y = \emptyset$. □

The following result describes the set of minimum representatives in $\langle a, b\rangle$ modulo c.

Theorem 1. *Let $a = r^2 - s^2$, $b = 2rs$, $c = r^2 + s^2$ be a set of primitive Pythagorean triplets. Let $\mathbf{m}_x$ denote the least positive integer in $\langle a, b\rangle$ congruent to x modulo c. Then*

$$\begin{aligned}&\big\{\mathbf{m}_x : 0 \le x < r^2 + s^2\big\}\\ &= \big\{\lambda a + \mu b : 0 \le \lambda < r + s, 0 \le \mu < s\big\} \bigcup \big\{\lambda a + \mu b : 0 \le \lambda < r, s \le \mu < r\big\}.\end{aligned}$$

Proof. The set $\{2rx : 0 \le x \le c - 1\}$ is a complete residue system modulo c since $\gcd(2r, c) = 1$. Fix $x \in \{0, \ldots, c - 1\}$, and consider the residue class $2rx$ modulo c. Thus, for $x > 0$, $\mathbf{m}_{2rx}$ is the least positive integer of the form $ax_1 + bx_2$, with $x_1 \ge 0$ and $x_2 \ge 0$, that is congruent to $2rx$ modulo c. Since $a \equiv 2r^2 \pmod{c}$,

$$\mathbf{m}_{2rx} = \min_{x_1 \ge 0, x_2 \ge 0} \big(ax_1 + bx_2\big) \text{ such that } rx_1 + sx_2 \equiv x \pmod{c}. \tag{1}$$

Set $rx_1 + sx_2 = x + ct$, $t \in \mathbb{Z}$. If $ry_1 + sy_2 = x + ct$, then $x_1 - y_1 = ks$ and $x_2 - y_2 = -kr$, with $k \in \mathbb{Z}$ since $\gcd(r, s) = 1$. Set $F(x_1, x_2) = ax_1 + bx_2$, $x_1 \ge 0$, $x_2 \ge 0$. Then $F(x_1 - s, x_2 + r) - F(x_1, x_2) = cs > 0$. Hence the minimum in Equation (1) is obtained at $x_2 = (x + ct)s^{-1} \pmod{r}$, $0 \le x_2 < r$.

We must now determine

$$x_1 = \min_{t \in \mathbb{Z}} \frac{x + ct - sx_2}{r} \tag{2}$$

subject to $x + ct - sx_2 \ge 0$. This restriction implies $t \ge 0$ since $x < c$ and $x_2 \ge 0$.

Let $f(t) = x + ct - s\big((x + ct)s^{-1} \pmod{r}\big)$, $t \ge 0$. Since

$$f(t+1) - f(t) = c - s\big((x + c(t+1))s^{-1} \pmod{r} - (x + ct)s^{-1} \pmod{r}\big) \ge c - (r-1)s > 0,$$

the minimum in Equation (2) is attained at the least nonnegative integer t_0 for which $f(t_0) = x + ct_0 - sx_2 = x + ct_0 - s\big((x + ct_0)s^{-1} \pmod{r}\big) \ge 0$.

Since $\gcd(r, s) = 1$, there exist integers u, v such that $x = ru + sv$, with $v \in \{0, \ldots, r - 1\}$. From $x > 0$ we conclude that $-ru < sv < rs$, and so $-u < s < r$.

If $u \ge 0$, then $f(0) = x - s\big(xs^{-1} \pmod{r}\big) = (ru + sv) - sv = ru \ge 0$. If $u < 0$, then $f(0) = ru < 0$ and $f(1) = x + c - s\big((x + c)s^{-1} \pmod{r}\big) = (ru + sv) + c - s\big((v + s) \pmod{r}\big) \ge (ru + sv) + c - s(v + s) = r(u + r) > 0$. Therefore,

$$\min_{t \ge 0} f(t) = \begin{cases} f(0) & \text{if } x \in \langle r, s\rangle; \\ f(1) & \text{if } x \notin \langle r, s\rangle. \end{cases}$$

From Equation (2) and the argument immediately preceding, we thus have

$$\begin{aligned}(x_1,x_2) &= \begin{cases}\left(\frac{f(0)}{r}, xs^{-1} \pmod r\right) & \text{if } u \geq 0;\\ \left(\frac{f(1)}{r}, (x+c)s^{-1} \pmod r\right) & \text{if } u < 0\end{cases}\\ &= \begin{cases}(u,v) & \text{if } u \geq 0;\\ (u+r, v+s) & \text{if } u<0,\ v+s<r;\\ (u+r+s, v+s-r) & \text{if } u<0,\ v+s \geq r.\end{cases}\end{aligned}$$

Since $0 \leq x = ru+sv < r^2+s^2$ is equivalent to $u < \frac{r^2+s(s-v)}{r}$, the first case yields the set

$$\begin{aligned}&\left\{au+bv : 0 \leq u < \tfrac{r^2+s(s-v)}{r}, 0 \leq v < r\right\}\\ &= \left\{\lambda a + \mu b : 0 \leq \lambda < \tfrac{r^2+s(s-\mu)}{r}, 0 \leq \mu < r\right\}.\end{aligned}$$

Since $0 \leq ru+sv < r^2+s^2$ is equivalent to $u \geq -\frac{sv}{r}$, the second case yields the set

$$\begin{aligned}&\left\{a(u+r)+b(v+s) : \tfrac{r^2-sv}{r} \leq u+r < r, s \leq v+s < r\right\}\\ &= \left\{\lambda a + \mu b : \tfrac{r^2+s(s-\mu)}{r} \leq \lambda < r, s \leq \mu < r\right\}.\end{aligned}$$

Since $0 \leq ru+sv < r^2+s^2$ is equivalent to $u \geq -\frac{sv}{r}$, the third case yields the set

$$\begin{aligned}&\left\{a(u+r+s)+b(v+s-r) : \tfrac{r^2+rs-sv}{r} \leq u+r+s < r+s, 0 \leq v+s-r < s\right\}\\ &= \left\{\lambda a + \mu b : \tfrac{r^2+s(s-\mu)}{r} \leq \lambda < r+s, 0 \leq \mu < s\right\}.\end{aligned}$$

Putting the three sets together describes the set of all minimum representatives. □

Theorem 2. *Let $a = r^2-s^2$, $b = 2rs$, $c = r^2+s^2$ be a set of primitive Pythagorean triplets. If $S = \langle a,b,c\rangle$, then*

(i)
$$F(S) = (r-1)(a+b)-c;$$

(ii)
$$g(S) = \frac{1}{2}\big((r^2-s^2+rs-2r)(r+s)+1\big);$$

(iii)
$$PF(S) = \big\{(r+s-1)a+(s-1)b-c, (r-1)(a+b)-c\big\}.$$

Proof. We use Proposition 1 and Theorem 1 for parts (i) and (ii), and Proposition 2 and Theorem 1 for part (iii). Note that $\{2rx : 0 \leq x < c\}$ represents a complete residue system modulo c since $\gcd(2r,c) = 1$.

(i)

$$\begin{aligned}
\mathrm{F}(S)+c &= \max_{0\le x\le c-1} \mathbf{m}_{2rx} \\
&= \max\left\{ \max_{\substack{0\le\lambda<r+s\\ 0\le\mu<s}} \big(\lambda a+\mu b\big), \max_{\substack{0\le\lambda<r\\ s\le\mu<r}} \big(\lambda a+\mu b\big) \right\} \\
&= \max\big\{(r+s-1)a+(s-1)b, (r-1)(a+b)\big\} \\
&= (r-1)(a+b),
\end{aligned}$$

since $(r-1)(a+b)-\big((r+s-1)a+(s-1)b\big)=(r-s)b-sa=s(r-s)^2>0$.

(ii)

$$\begin{aligned}
\mathrm{g}(S) &= \frac{1}{c}\sum_{x=1}^{c-1}\mathbf{m}_{2rx}-\frac{c-1}{2} \\
&= \frac{1}{c}\left(\sum_{\substack{0\le\lambda<r+s\\ 0\le\mu<s}}(\lambda a+\mu b)+\sum_{\substack{0\le\lambda<r\\ s\le\mu<r}}(\lambda a+\mu b)\right)-\frac{c-1}{2} \\
&= \frac{1}{c}\left(\sum_{\substack{0\le\lambda<r\\ 0\le\mu<r}}(\lambda a+\mu b)+\sum_{\substack{r\le\lambda<r+s\\ 0\le\mu<s}}(\lambda a+\mu b)\right)-\frac{c-1}{2} \\
&= \frac{1}{2}\big((r+s)(r^2-s^2+rs-2r)+1\big).
\end{aligned}$$

(iii) Write $T_1=[0,r+s)\times[0,s)$, $T_2=[0,r)\times[s,r)$, and $T=T_1\cup T_2$. Let $\mathbf{m}_{(\lambda,\mu)}$ denote the least positive integer in the congruence class $\lambda a+\mu b$ modulo c. Then $\{\lambda a+\mu b : (\lambda,\mu)\in T\}$ is a complete residue system modulo c, $\mathbf{m}_{(\lambda,\mu)}\le\lambda a+\mu b$, with equality if and only if $(\lambda,\mu)\in T$, and

$$\mathrm{PF}(S)=\big\{\mathbf{m}_{(\lambda_0,\mu_0)}-c\big\},$$

where

$$(\lambda_0,\mu_0)\in T, \mathbf{m}_{(\lambda_0,\mu_0)}>\mathbf{m}_{(\lambda+\lambda_0,\mu+\mu_0)}-\mathbf{m}_{(\lambda,\mu)}\ \forall\ (\lambda,\mu)\in T\setminus\{(0,0)\}.$$

For $(\lambda_0,\mu_0)\in T_1\setminus\{(0,0),(r+s-1,s-1)\}$, we have

$$\big(\lambda_0 a+\mu_0 b\big)+\big((r+s-1-\lambda_0)a+(s-1-\mu_0)b\big)=(r+s-1)a+(s-1)b.$$

Since $(r+s-1-\lambda_0,s-1-\mu_0)\in T_1$ and $(r+s-1,s-1)\in T_1$, $\lambda_0 a+\mu_0 b-c\notin\mathrm{PF}(S)$.

For $(\lambda_0, \mu_0) \in T_2 \setminus \{(r-1, r-1)\}$, we have

$$\big(\lambda_0 a + \mu_0 b\big) + \big((r-1-\lambda_0)a + (r-1-\mu_0)b\big) = (r-1)a + (r-1)b.$$

Since $(r-1-\lambda_0, r-1-\mu_0) \in T_2$ and $(r-1, r-1) \in T_2$, $\lambda_0 a + \mu_0 b - c \notin \mathrm{PF}(S)$.

Thus, $\mathrm{PF}(S) \subseteq \big\{(r+s-1)a + (s-1)b - c, (r-1)a + (r-1)b - c\big\}$. We show that both $(r+s-1)a + (s-1)b - c$ and $(r-1)a + (r-1)b - c$ belong to $\mathrm{PF}(S)$.

We note that $rc = ra + sb$ and $sc = -sa + rb$.

Let $(\lambda_0, \mu_0) = (r+s-1, s-1)$ and let $(\lambda, \mu) \in T \setminus \{(0,0)\}$.

If $\lambda = 0$, then $\mu > 0$ and

$$\begin{aligned}(\lambda a + \mu b) + \big((r+s-1)a + (s-1)b\big) - c &= (s-1)a + (\mu-1)b + (r-1)c \\ &= \mathbf{m}_{(s-1,\mu-1)} + (r-1)c.\end{aligned}$$

If $\lambda > 0$, then

$$\begin{aligned}(\lambda a + \mu b) + \big((r+s-1)a + (s-1)b\big) - c &= (\lambda-1)a + (\mu+r-1)b + (r-s-1)c \\ &\geq \mathbf{m}_{(\lambda-1,\mu+r-1)} + (r-s-1)c.\end{aligned}$$

Hence $(r+s-1)a + (s-1)b - c \in \mathrm{PF}(S)$.

We know that $\mathrm{F}(S) = (r-1)(a+b) - c \in \mathrm{PF}(S)$. However, we also give a direct proof. Let $(\lambda_0, \mu_0) = (r-1, r-1)$ and let $(\lambda, \mu) \in T \setminus \{(0,0)\}$.

If $\lambda = 0$, then $\mu > 0$ and

$$\begin{aligned}(\lambda a + \mu b) + \big((r-1)a + (r-1)b\big) - c &= (r+s-1)a + (\mu-1)b + (s-1)c \\ &\geq \mathbf{m}_{(r+s-1,\mu-1)} + (s-1)c.\end{aligned}$$

If $\lambda > 0$, then

$$\begin{aligned}(\lambda a + \mu b) + \big((r-1)a + (r-1)b\big) - c &= (\lambda-1)a + (\mu+r-s-1)b + (r-1)c \\ &\geq \mathbf{m}_{(\lambda-1,\mu+r-s-1)} + (r-1)c.\end{aligned}$$

Hence $(r-1)a + (r-1)b - c \in \mathrm{PF}(S)$.

□

Various properties of the numerical semigroup S generated by primitive Pythagorean triplets, e.g., symmetricity, pseudo-symmetricity, Arf property, and saturation, follow easily from Theorem 2. In the remarks that follow, we take $S = \langle a, b, c\rangle$, where $a = r^2 - s^2$, $b = 2rs$, $c = r^2 + s^2$, with $r > s$, $\gcd(r, s) = 1$, with r, s of opposite parity.

Remark 1. We have that $(r-1)(a+b)-\big((r+s-1)a+(s-1)b\big)=(r-s)b-sa=s(r-s)^2>0$, as in the proof of Theorem 2, part (i). From Lemma 1 and Theorem 2, part (iii), we conclude that S is not symmetric.

Remark 2. From Theorem 2, part (iii), $\mathrm{F}(S)=(r-1)(a+b)-c$ is even if and only if r is even. So by Lemma 1 and Theorem 2, part (iii), S is pseudo-symmetric if and only if r is even and

$$2\big((r+s-1)a+(s-1)b-c\big)=(r-1)(a+b)-c.$$

This is equivalent to $r^3-2s^3+3rs^2-2r^2-2rs=0$. Hence, $r \mid 2s^3$, and so $r=2$ since $\gcd(r,s)=1$ and r is even. The only possibility for $s=1$, and we may verify that $(r,s)=(2,1)$ satisfies the above equation. We conclude that S is pseudo-symmetric only when $A=\{3,4,5\}$.

Remark 3. Recall that S is saturated implies S has the Arf property, which in turn implies S has maximal embedding dimension. Now S has maximal embedding dimension if and only if $\mathrm{m}(S)=3$, which is the same as $A=\{3,4,5\}$. Therefore, the only possibility for S to be saturated, or to have the Arf property, is when $A=\{3,4,5\}$. It is easy to see that S is saturated from the fact that $S=[3,\infty)\cup\{0\}$ when $A=\{3,4,5\}$. We conclude that S is saturated, has the Arf propery, or has maximal embedding dimension if and only if $S=\langle 3,4,5\rangle$.

We close this section by determining the nine entries of the matrix in Proposition 3.

Proposition 5. *Let $a=r^2-s^2$, $b=2rs$, $c=r^2+s^2$ be a set of primitive Pythagorean triplets. With the notations of Proposition 3, we have*

$$\begin{array}{lll} c_1=r+s, & r_{12}=r-s, & r_{13}=r-s,\\ c_2=r, & r_{21}=s, & r_{23}=s,\\ c_3=r, & r_{31}=r, & r_{32}=s. \end{array}$$

Proof. We use the notations of Proposition 3.
(i) Suppose $a \mid (by+cz)$ with $y,z\in\mathbb{Z}_{\geq 0}$, $y+z>0$. Since $c\equiv 2s^2 \pmod{a}$ and $\gcd(2s,a)=1$, we have $a\mid(ry+sz)$ and so both $r\pm s$ divide $ry+sz$. From $ry+sz=(r+s)y-s(y-z)$ and $\gcd(s,r+s)=1$ we have $(r+s)\mid(y-z)$.

If $y>z$, then $y\geq r+s$, and we have $a\mid\big(b(y-r)+c(z+s)\big)$ and $b(y-r)+c(z+s)<by+cz$.

If $y<z$, then $z\geq r+s$, and we have $a\mid\big(b(y+s)+c(z-r)\big)$ and $b(y+s)+c(z-r)<by+cz$.

So if y,z are such that $\frac{1}{a}(by+cz)$ is minimized, then $y=z$. Thus, $r_{12}=r_{13}$.

From $ry+sz=(r-s)y+s(y+z)$ and $\gcd(s,r-s)=1$ we have $(r-s)\mid(y+z)$. With $y=z=r_{12}$, this gives $(r-s)\mid r_{12}$. Thus $r_{12}=r-s$, and $c_1=\frac{1}{a}r_{12}(b+c)=r+s$.

(ii) Suppose $b \mid (ax + cz)$ with $x, z \in \mathbb{Z}_{\geq 0}$, $x + z > 0$. Note that $ax + cz = r^2(x+z) - s^2(x-z)$. If r is even, then $2r \mid (x-z)$ and $s \mid (x+z)$. If s is even, then $2s \mid (x+z)$ and $r \mid (x-z)$. Therefore, in any case, $2r \mid (x-z)$ and $2s \mid (x+z)$.

If $x > z$, then $x \geq 2r$, and we have $b \mid \big(a(x-r-s) + c(z+r-s)\big)$ and $a(x-r-s) + c(z+r-s) < ax + cz$.

If $x < z$, then $z \geq 2r$, and we have $b \mid \big(a(x+r)+c(z-r)\big)$ and $a(x+r)+c(z-r) < ax + cz$.

So if x, z are such that $\frac{1}{b}(ax + cz)$ is minimized, then $x = z$. Thus, $r_{21} = r_{23}$.

From $2s \mid (x+z)$, with $x = z = r_{21}$, we have $s \mid r_{21}$. Thus $r_{21} = s$, and $c_2 = \frac{1}{b} r_{21}(a+c) = r$.

From Proposition 3, $c_3 = r_{13} + r_{23} = (r-s) + s = r$, $r_{31} = c_1 - r_{21} = (r+s) - s = r$, and $r_{32} = c_2 - r_{12} = r - (r-s) = s$. □

We note that the results in Proposition 3 and Proposition 5 lead to the results in Theorem 2.

Acknowledgment. The authors wish to thank the anonymous referee for his suggestions.

References

[1] R. Apéry, Sur les branches superlinéaires des courbes algébriques, *C. R. Acad. Sci. Paris* **222** (1946), 1198–1200.

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

[3] F. Curtis, On formulas for the Frobenius number of a numerical semigroup, *Math. Scand.* **67** (1990), 190–192.

[4] L. G. Fel, Frobenius problem for semigroups $S(d_1, d_2, d_3)$, *Funct. Anal. Other Math.* **1**, no. 2 (2006), 119–157.

[5] B. K. Gil, J.-W. Han, T. H. Kim, R. H. Koo, B. W. Lee, J. Lee, K. S. Nam, H. W. Park, and P.-S. Park, Frobenius numbers of Pythagorean triples, *Int. J. of Number Theory* **11**, no. 2 (2015), 613–619.

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

[7] R. Kannan, Lattice translates of a polytope and the Frobenius problem, *Combinatorica* **12**, no. 2 (1992), 161–177.

[8] J. Kraft, Singularity of monomial curves in $\mathbf{A}^3$ and Gorenstein monomial curves in $\mathbf{A}^4$, *Canad. J. Math.* **37**, Issue 5 (1985), 872–892.

[9] J. L. Ramírez Alfonsín, Complexity of the Frobenius problem, *Combinatorica* **16** (1996), 143–147.

[10] J. L. Ramírez Alfonsín, The Diophantine Frobenius Problem, Oxford Lecture Series in Mathematics and Its Applications **30**, Oxford University Press, 2005.

[11] Ø. J. Rødseth, On a linear diophantine problem of Frobenius, *J. Reine Angew. Math.* **301** (1978), 171–178.

[12] J. C. Rosales and P. A. García-Sánchez, Numerical semigroups with embedding dimension three, *Arch. Math.* (Basel) **83**, no. 6 (2004), 488–496.

[13] J. C. Rosales and P. A. García-Sánchez, Numerical Semigroups, Developments in Mathematics, vol. 20, *Springer*, 2009.

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

[15] J. J. Sylvester, 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.

[16] A. Tripathi, On a variation of the coin exchange problem for arithmetic progressions, *Integers* **3** (2003), Article A01, 5 pages.