Mathematical
Inequalities
& Applications
Volume 11, Number 2 (2008), 203–212

THE SMALLEST POSITIVE INTEGER THAT IS SOLUTION OF A PROPORTIONALLY MODULAR DIOPHANTINE INEQUALITY

J. C. ROSALES AND P. VASCO

(*communicated by J. Pečarić*)

Abstract. A proportionally modular Diophantine inequality is an expression of the form $ax \bmod b \leqslant cx$, where a, b and c are positive integers. In this paper we present an algorithm that allows us to calculate the smallest positive integer that is solution of an inequality of this type. We also obtain an algorithm that computes the Frobenius number and the number of gaps of a numerical semigroup generated by three positive integers.

1. Introduction

Given two integers m and n with $n \neq 0$, we denote by $m \bmod n$ the remainder of the division of m by n. Following the notation of [8], a proportionally modular Diophantine inequality is an expression of the form $ax \bmod b \leqslant cx$, where a, b and c are positive integers. Our principal aim in this paper is to give an algorithm that allows us to calculate the smallest positive integer that is solution of an inequality of this type. This algorithm as we will see has a great similarity with the Euclides algorithm for computing the greatest common divisor of two integers.

Given a subset A of $\mathbb{N}$ (here $\mathbb{N}$ denotes the set of nonnegative integers), then we will denote by $\langle A \rangle$ the submonoid of $(\mathbb{N}, +)$ generated by A. That is, $\langle A \rangle = \{s_1a_1 + \cdots + s_na_n \mid n \in \mathbb{N}\setminus\{0\}, s_1, \ldots, s_n \in \mathbb{N} \text{ and } a_1, \ldots, a_n \in A\}$. In this paper, and as an application of the above mentioned algorithm, we also give an algorithmic method that, given three positive integers n_1, n_2 and n_3, calculates the smallest positive multiple of n_3 that belongs to $\langle n_1, n_2 \rangle$.

Finally, combining these results with those obtained in [7] we will obtain an algorithm that computes the Frobenius number and the number of gaps (see [4]) of a numerical semigroup generated by three positive integers.

Mathematics subject classification (2000): 20M14, 13H10.

Key words and phrases: numerical semigroup,Diophantine inequality, multiplicity, Frobenius number, gaps.

The first author is supported by the project MTM2004-01446 and FEDER funds. This paper has been supported by the Luso-Espanhola action HP2004-0056.

Paper MIA-11-14

2. Preliminaries

Given the proportionally modular Diophantine inequality $ax \bmod b \leqslant cx$, we denote by $\mathrm{S}(a,b,c)$ the set of integer solutions of this inequality, $\mathrm{S}(a,b,c) = \{x \in \mathbb{N} \mid ax \bmod b \leqslant cx\}$.

A numerical semigroup is a subset S of $\mathbb{N}$, that is closed under addition, $0 \in S$ and such that $\mathbb{N}\backslash S$ is finite. In [8] we saw that $\mathrm{S}(a,b,c)$ is a numerical semigroup. Not all numerical semigroups are of this form. We will refer to these type of semigroups as proportionally modular numerical semigroups.

If S is a numerical semigroup, then the smallest positive integer that belongs to S is an important invariant of S called the multiplicity of S and we denote it by $\mathrm{m}(S)$ (see for example [1]). Our principal aim in this paper is to give an algorithm that allows us to calculate the multiplicity of $\mathrm{S}(a,b,c)$. It is an open problem to give a formula for the multiplicity of $\mathrm{S}(a,b,c)$, from the integers a, b and c. This problem is still open in the case $c = 1$.

Let $\alpha < \beta$ be two positive rational numbers and let T be the submonoid of $\left(\mathbb{Q}_0^+, +\right)$ (here $\mathbb{Q}_0^+$ denotes the set of nonnegative rational numbers) generated by the closed interval $[\alpha,\beta] = \{x \in \mathbb{Q} \mid \alpha \leqslant x \leqslant \beta\}$. In [8] we saw that $T \cap \mathbb{N}$ is a proportionally modular numerical semigroup and that all proportionally modular numerical semigroup can be obtained in this way. The following result is a reformulation of [8, Corollary 9].

PROPOSITION 1.

(1) Let a, b and c be positive integers such that $c < a < b$ and let T be the submonoid of $\mathbb{Q}_0^+$ generated by $\left[\frac{b}{a}, \frac{b}{a-c}\right]$. Then $T \cap \mathbb{N} = \{x \in \mathbb{N} \mid ax \bmod b \leqslant cx\}$.

(2) Conversely, let a_1, b_1, a_2 and b_2 be positive integers such that $\frac{b_1}{a_1} < \frac{b_2}{a_2}$ and let T be the submonoid of $\mathbb{Q}_0^+$ generated by $\left[\frac{b_1}{a_1}, \frac{b_2}{a_2}\right]$. Then $T \cap \mathbb{N} = \{x \in \mathbb{N} \mid a_1b_2x \bmod b_1b_2 \leqslant (a_1b_2 - a_2b_1)x\}$.

Following the notation of (2) of the above proposition we will refer to $T \cap \mathbb{N}$ as the proportionally modular numerical semigroup associated to the interval $\left[\frac{b_1}{a_1}, \frac{b_2}{a_2}\right]$ and we will denote it by $\mathrm{S}\left(\left[\frac{b_1}{a_1}, \frac{b_2}{a_2}\right]\right)$. Since the inequality $ax \bmod b \leqslant cx$ has the same solutions of the inequality $(a \bmod b)x \bmod b \leqslant cx$, we can assume that $a < b$. Moreover, if $c \geqslant a$, then $\mathrm{S}(a,b,c) = \mathbb{N}$. Therefore we can suppose that a, b and c are positive integers such that $c < a < b$. Consequently the condition imposed in (1) of the above proposition is not restrictive.

The following result is a reformulation of [8, Lemma 1] and will be used several times in this paper.

LEMMA 2. *Let $\alpha < \beta$ be positive rational numbers. Then a positive integer x belongs to $\mathrm{S}([\alpha,\beta])$ if and only if there exists a positive integer y such that $\alpha \leqslant \frac{x}{y} \leqslant \beta$.*

3. The algorithm

In this section, assume that α and β denote positive rational numbers such that $\alpha < \beta$. Our aim is to give an algorithm that allows us to compute the multiplicity of $\mathrm{S}([\alpha,\beta])$.

LEMMA 3. *If* $\mathrm{S}([\alpha,\beta])$ *has multiplicity* $\mathrm{m} \neq 1$, *then there exists a unique positive integer* t *such that* $\alpha \leqslant \frac{\mathrm{m}}{t} \leqslant \beta$.

Proof. Since $\mathrm{m} \in \mathrm{S}([\alpha,\beta])$, by Lemma 2, we deduce that there exists a positive integer t such that $\alpha \leqslant \frac{\mathrm{m}}{t} \leqslant \beta$. Let us see that t in this setting is unique. Assume to the contrary that there exists an integer $a \geqslant 2$ such that $\alpha \leqslant \frac{\mathrm{m}}{a} < \frac{\mathrm{m}}{a-1} \leqslant \beta$. As $\left[\frac{\mathrm{m}}{a}, \frac{\mathrm{m}}{a-1}\right] \subseteq [\alpha,\beta]$, in view of Lemma 2, we have that $\mathrm{S}\left(\left[\frac{\mathrm{m}}{a}, \frac{\mathrm{m}}{a-1}\right]\right) \subseteq \mathrm{S}([\alpha,\beta])$. By Proposition 1 we know that $\mathrm{S}\left(\left[\frac{\mathrm{m}}{a}, \frac{\mathrm{m}}{a-1}\right]\right) = \{x \in \mathbb{N} \mid a\mathrm{m}x \bmod \mathrm{m}^2 \leqslant \mathrm{m}x\} = \{x \in \mathbb{N} \mid ax \bmod \mathrm{m} \leqslant x\}$. Since $\mathrm{m} \neq 1$, $1 \notin \mathrm{S}([\alpha,\beta])$ and therefore $1 \notin \mathrm{S}\left(\left[\frac{\mathrm{m}}{a}, \frac{\mathrm{m}}{a-1}\right]\right)$. Thus $a \cdot 1 \bmod \mathrm{m} > 1$. Then $a(\mathrm{m}-1) \bmod \mathrm{m} = \mathrm{m} - (a \bmod \mathrm{m}) \leqslant \mathrm{m} - 1$ and consequently $\mathrm{m} - 1 \in \mathrm{S}\left(\left[\frac{\mathrm{m}}{a}, \frac{\mathrm{m}}{a-1}\right]\right)$, which contradicts the fact that m is the multiplicity of $\mathrm{S}([\alpha,\beta])$. □

Observe that asserting that $\mathrm{S}([\alpha,\beta])$ has multiplicity different from 1 is equivalent to saying that $\mathrm{S}([\alpha,\beta]) \neq \mathbb{N}$. Lemma 3 allows us to give the following definition. If I is a closed interval of $\mathbb{Q}_0^+$ such that $\mathrm{S}(I) \neq \mathbb{N}$, then we call the "small point" of I, and denote it by $P(I)$, the fraction $\frac{\mathrm{m}}{t}$, where m is the multiplicity of $\mathrm{S}(I)$ and t is the unique positive integer such that $\frac{\mathrm{m}}{t} \in I$.

LEMMA 4. *Assume that* $\mathrm{S}([\alpha,\beta]) \neq \mathbb{N}$ *and* $P([\alpha,\beta]) = \frac{\mathrm{m}}{t}$. *If* $\frac{s}{x} \in [\alpha,\beta]$, *then* $t \leqslant x$.

Proof. If $\frac{s}{x} \in [\alpha,\beta]$, then by applying Lemma 2 we know that $s \in \mathrm{S}([\alpha,\beta])$ and therefore $\mathrm{m} \leqslant s$. If $t > x$, then $\frac{\mathrm{m}}{t} < \frac{\mathrm{m}}{x} \leqslant \frac{s}{x}$. Thus $\alpha \leqslant \frac{\mathrm{m}}{t} < \frac{\mathrm{m}}{x} \leqslant \beta$, which contradicts Lemma 3. □

Observe that as a consequence of the previous lemma we have that $P(I)$ is the fraction of I with the smallest numerator and also with the smallest denominator.

LEMMA 5. *Let us assume that* $\mathrm{S}([\alpha,\beta]) \neq \mathbb{N}$, $a \in \mathbb{N}$ *and* $P([\alpha,\beta]) = \frac{\mathrm{m}}{t}$. *Then* $\mathrm{S}([a+\alpha, a+\beta]) \neq \mathbb{N}$ *and* $P([a+\alpha, a+\beta]) = \frac{\mathrm{m}+ta}{t}$.

Proof. If $a = 0$, then $\mathrm{S}([a+\alpha, a+\beta]) = \mathrm{S}([\alpha,\beta]) \neq \mathbb{N}$. If $a \geqslant 1$ then $a + \alpha > 1$ and in view of Lemma 2 we easily deduce that $1 \notin \mathrm{S}([a+\alpha, a+\beta])$. Therefore $\mathrm{S}([a+\alpha, a+\beta]) \neq \mathbb{N}$. Since $\alpha \leqslant \frac{\mathrm{m}}{t} \leqslant \beta$, we have that $a + \alpha \leqslant a + \frac{\mathrm{m}}{t} \leqslant a + \beta$, that is, $a + \alpha \leqslant \frac{\mathrm{m}+ta}{t} \leqslant a + \beta$. To conclude the proof we only have to see that $\mathrm{m} + ta$ is the multiplicity of $\mathrm{S}([a+\alpha, a+\beta])$. Suppose that there exists a positive integer $x \in \mathrm{S}([a+\alpha, a+\beta])$ such that $x < \mathrm{m} + ta$. By applying Lemma 2 we have that there exists a positive integer y such that $a + \alpha \leqslant \frac{x}{y} \leqslant a + \beta$. Therefore $\alpha \leqslant \frac{x-ay}{y} \leqslant \beta$, and thus in view of Lemma 2, $x - ay \in \mathrm{S}([\alpha,\beta])$. By applying

Lemma 4 we know that $t \leqslant y$. Consequently $x - ay \leqslant x - at < \mathrm{m} + ta - ta = \mathrm{m}$, which contradicts the fact that m is the multiplicity of $\mathrm{S}([\alpha,\beta])$. $\square$

Given a rational number x we denote by $\lfloor x \rfloor$ the integer $\max\{z \in \mathbb{Z} \mid z \leqslant x\}$ and by $\lceil x \rceil$ the integer $\min\{z \in \mathbb{Z} \mid x \leqslant z\}$. The following two results follow easily.

LEMMA 6. *If* $\mathrm{S}([\alpha,\beta]) \neq \mathbb{N}$ *and* $[\alpha,\beta]$ *contains an integer, then* $P([\alpha,\beta]) = \frac{\lceil \alpha \rceil}{1}$.

LEMMA 7. *If* $[\alpha,\beta]$ *does not contain an integer, then* $\lfloor \alpha \rfloor = \lfloor \beta \rfloor$.

The next result is the key to give the announced algorithm.

PROPOSITION 8. *Let* a_1, b_1, a_2 *and* b_2 *be positive integers such that* $\frac{b_1}{a_1} < \frac{b_2}{a_2}$, $\mathrm{S}\left(\left[\frac{b_1}{a_1}, \frac{b_2}{a_2}\right]\right) \neq \mathbb{N}$ *and* $\left[\frac{b_1}{a_1}, \frac{b_2}{a_2}\right]$ *contains no integers. Then* $\frac{a_2}{b_2 \bmod a_2} < \frac{a_1}{b_1 \bmod a_1}$ *and* $\mathrm{S}\left(\left[\frac{a_2}{b_2 \bmod a_2}, \frac{a_1}{b_1 \bmod a_1}\right]\right) \neq \mathbb{N}$. *Moreover, if* $P\left(\left[\frac{a_2}{b_2 \bmod a_2}, \frac{a_1}{b_1 \bmod a_1}\right]\right) = \frac{\mathrm{m}}{t}$, *then* $P\left(\left[\frac{b_1}{a_1}, \frac{b_2}{a_2}\right]\right) = \frac{t + \left\lfloor \frac{b_1}{a_1} \right\rfloor \mathrm{m}}{\mathrm{m}}$.

Proof. By Lemma 7, we have that $\left\lfloor \frac{b_1}{a_1} \right\rfloor = \left\lfloor \frac{b_2}{a_2} \right\rfloor$. If $\frac{b_1}{a_1} < \frac{b_2}{a_2}$, then $\frac{b_1}{a_1} - \left\lfloor \frac{b_1}{a_1} \right\rfloor < \frac{b_2}{a_2} - \left\lfloor \frac{b_2}{a_2} \right\rfloor$ and therefore $\frac{b_1 \bmod a_1}{a_1} < \frac{b_2 \bmod a_2}{a_2}$. Observe that as $\left[\frac{b_1}{a_1}, \frac{b_2}{a_2}\right]$ does not contain an integer, both $\frac{b_1}{a_1}$ and $\frac{b_2}{a_2}$ are not integers, and consequently $b_1 \bmod a_1 \neq 0$ and $b_2 \bmod a_2 \neq 0$. Thus we have $\frac{a_2}{b_2 \bmod a_2} < \frac{a_1}{b_1 \bmod a_1}$.

Notice that $b_2 \bmod a_2 < a_2$ and therefore $1 < \frac{a_2}{b_2 \bmod a_2}$. In view of Lemma 2 we easily deduce that $1 \notin \mathrm{S}\left(\left[\frac{a_2}{b_2 \bmod a_2}, \frac{a_1}{b_1 \bmod a_1}\right]\right)$. Hence $\mathrm{S}\left(\left[\frac{a_2}{b_2 \bmod a_2}, \frac{a_1}{b_1 \bmod a_1}\right]\right) \neq \mathbb{N}$.

If $P\left(\left[\frac{a_2}{b_2 \bmod a_2}, \frac{a_1}{b_1 \bmod a_1}\right]\right) = \frac{\mathrm{m}}{t}$, then $\frac{\mathrm{m}}{t} \in \left[\frac{a_2}{b_2 \bmod a_2}, \frac{a_1}{b_1 \bmod a_1}\right]$ and therefore $\frac{t}{\mathrm{m}} \in \left[\frac{b_1 \bmod a_1}{a_1}, \frac{b_2 \bmod a_2}{a_2}\right]$. Hence $\frac{t}{\mathrm{m}} + \left\lfloor \frac{b_1}{a_1} \right\rfloor \in \left[\frac{b_1 \bmod a_1}{a_1} + \left\lfloor \frac{b_1}{a_1} \right\rfloor, \frac{b_2 \bmod a_2}{a_2} + \left\lfloor \frac{b_1}{a_1} \right\rfloor\right]$. Since $\left\lfloor \frac{b_1}{a_1} \right\rfloor = \left\lfloor \frac{b_2}{a_2} \right\rfloor$ we have that $\frac{t + \left\lfloor \frac{b_1}{a_1} \right\rfloor \mathrm{m}}{\mathrm{m}} \in \left[\frac{b_1}{a_1}, \frac{b_2}{a_2}\right]$. To conclude the proof it suffices to prove that $t + \left\lfloor \frac{b_1}{a_1} \right\rfloor \mathrm{m}$ is the multiplicity of $\mathrm{S}\left(\left[\frac{b_1}{a_1}, \frac{b_2}{a_2}\right]\right)$. Assume to the contrary that there exists a positive integer $x \in \mathrm{S}\left(\left[\frac{b_1}{a_1}, \frac{b_2}{a_2}\right]\right)$ such that $x < t + \left\lfloor \frac{b_1}{a_1} \right\rfloor \mathrm{m}$. As $x \in \mathrm{S}\left(\left[\frac{b_1}{a_1}, \frac{b_2}{a_2}\right]\right)$, by applying Lemma 2, there exists a positive integer y such that $\frac{x}{y} \in \left[\frac{b_1}{a_1}, \frac{b_2}{a_2}\right]$. Thus $\frac{x}{y} - \left\lfloor \frac{b_1}{a_1} \right\rfloor \in \left[\frac{b_1 \bmod a_1}{a_1}, \frac{b_2 \bmod a_2}{a_2}\right]$ and consequently $\frac{y}{x - \left\lfloor \frac{b_1}{a_1} \right\rfloor y} \in \left[\frac{a_2}{b_2 \bmod a_2}, \frac{a_1}{b_1 \bmod a_1}\right]$. Since $P\left(\left[\frac{a_2}{b_2 \bmod a_2}, \frac{a_1}{b_1 \bmod a_1}\right]\right) = \frac{\mathrm{m}}{t}$, we deduce that $\mathrm{m} \leqslant y$ and by applying Lemma 4 also $t \leqslant x - \left\lfloor \frac{b_1}{a_1} \right\rfloor y$. Thus $t \leqslant x - \left\lfloor \frac{b_1}{a_1} \right\rfloor y < t + \left\lfloor \frac{b_1}{a_1} \right\rfloor \mathrm{m} - \left\lfloor \frac{b_1}{a_1} \right\rfloor y$. Therefore $t < t + (\mathrm{m} - y)\left\lfloor \frac{b_1}{a_1} \right\rfloor$, which is absurd since $\mathrm{m} \leqslant y$. $\square$

The previous lemma allows us to give the following definition. Let I be a closed interval of positive rational numbers not containing any integer. We define its "reduced

interval", and denote it by $R(I)$, in the following way. If $I = \left[\frac{b_1}{a_1}, \frac{b_2}{a_2}\right]$ with a_1, b_1, a_2 and b_2 positive integers, then $R(I) = \left[\frac{a_2}{b_2 \bmod a_2}, \frac{a_1}{b_1 \bmod a_1}\right]$.

Notice that the above mentioned definition does not depend on the chosen fractions as extremes of the interval I. In fact, it suffices to observe that if m and n are positive integers, then $I = \left[\frac{nb_1}{na_1}, \frac{mb_2}{ma_2}\right]$ and $\frac{ma_2}{(mb_2) \bmod (ma_2)} = \frac{ma_2}{m(b_2 \bmod a_2)} = \frac{a_2}{b_2 \bmod a_2}$. Similarly, $\frac{na_1}{(nb_1) \bmod (na_1)} = \frac{a_1}{b_1 \bmod a_1}$.

Given a closed interval I of positive rational numbers we define recursively the following sequence of closed intervals:

$I_1 = I$

$I_{n+1} = R(I_n)$ if I_n contains no integers, otherwise $I_{n+1} = I_n$.

We will refer to $\{I_n\}_{n \in \mathbb{N} \setminus \{0\}}$ as the sequence of intervals associated to I. Observe that if I_k contains an integer, then $I_n = I_k$, for every $n \geqslant k$.

Before we state the following result, let us remember the Euclides algorithm for calculating the greatest common divisor of two positive integers (see [3]).

Input: b and a positive integers.

Output: the greatest common divisor of b and a.

Begin

$(x, y) := (b, a)$

While $y \neq 0$ do $(x, y) := (y, x \bmod y)$

Return x

End.

LEMMA 9. *Let I be a closed interval and let $\{I_n\}_{n \in \mathbb{N} \setminus \{0\}}$ be the sequence of intervals associated to I. Then there exists a positive integer k such that I_k contains an integer.*

Proof. Let a_1, b_1, a_2 and b_2 be positive integers such that $I = \left[\frac{b_1}{a_1}, \frac{b_2}{a_2}\right]$. Let (x_1, y_1), (x_2, y_2), ... be the values of the variable (x, y) in the Euclides algorithm for calculating the greatest common divisor of b_1 and a_1. In view of the definition of the sequence $\{I_n\}_{n \in \mathbb{N} \setminus \{0\}}$, we deduce that if I_n does not contain any integer, then $\frac{x_n}{y_n}$ is an end of the interval I_n. To conclude the proof we only need to observe that the Euclides algorithm stops in a finite number of steps. □

Next, we give an example that illustrates the previous lemma.

EXAMPLE 10. Let $I = \left[\frac{33}{13}, \frac{66}{25}\right]$. Let us construct the sequence of intervals associated to I.

$$I_1 = \left[\frac{33}{13}, \frac{66}{25}\right], \quad I_2 = \left[\frac{25}{16}, \frac{13}{7}\right], \quad I_3 = \left[\frac{7}{6}, \frac{16}{9}\right], \quad I_4 = \left[\frac{9}{7}, \frac{6}{1}\right].$$

Observe that I_4 already contains an integer. Therefore $I_n = I_4$ for all $n \geqslant 4$.

If I is a closed interval with no integers in it, then as a consequence of Lemma 7, we have that $\lfloor x \rfloor = \lfloor y \rfloor$, for all $x, y \in I$. This integer is denoted by $\lfloor I \rfloor$.

The next result establishes a relation between the "small points" of the elements of the sequence of intervals associated to a closed interval of positive rational numbers without integers.

LEMMA 11. *Let I be a closed interval such that $\mathrm{S}(I) \neq \mathbb{N}$ and let $\{I_n\}_{n\in\mathbb{N}\setminus\{0\}}$ be the sequence of intervals associated to I. Let l be the smallest positive integer such that I_l contains an integer. For $k \in \{2,\ldots,l\}$, $P(I_{k-1}) = \frac{1}{P(I_k)} + \lfloor I_{k-1} \rfloor$.*

Proof. It suffices to observe that from Proposition 8 we know that if $P(I_k) = \frac{\mathrm{m}}{t}$, then $P(I_{k-1}) = \frac{t+\lfloor I_{k-1}\rfloor \mathrm{m}}{\mathrm{m}} = \frac{t}{\mathrm{m}} + \lfloor I_{k-1} \rfloor$. □

We are now ready to give the algorithm announced in the beginning of this section.

ALGORITHM 12. Input: I a closed interval of positive rational numbers such that $\mathrm{S}(I) \neq \mathbb{N}$.

Output: The multiplicity of the semigroup $\mathrm{S}(I)$.

1. Compute the sequence of intervals associated to I until we find the first interval of the sequence that contains an integer. Let us denote such intervals by $I_1, I_2, \ldots, I_l$.
2. If $I_l = [\alpha, \beta]$, then $P(I_l) = \frac{\lceil \alpha \rceil}{1}$.
3. Calculate $P(I_1)$ by applying successively that $P(I_{n-1}) = \frac{1}{P(I_n)} + \lfloor I_{n-1} \rfloor$.
4. The multiplicity of $\mathrm{S}(I)$ is the numerator of $P(I_1)$.

EXAMPLE 13. Let us calculate the multiplicity of the semigroup $\mathrm{S}\left(\left[\frac{33}{13}, \frac{66}{25}\right]\right)$ by applying the results given so far. First of all, let us calculate the sequence of intervals associated to $I = \left[\frac{33}{13}, \frac{66}{25}\right]$ until we find the first term of the sequence that contains an integer. We already made the computation in the Example 10:

$$I_1 = \left[\frac{33}{13}, \frac{66}{25}\right], \quad I_2 = \left[\frac{25}{16}, \frac{13}{7}\right], \quad I_3 = \left[\frac{7}{6}, \frac{16}{9}\right], \quad I_4 = \left[\frac{9}{7}, \frac{6}{1}\right].$$

By applying Lemma 6, we know that $P(I_4) = \frac{2}{1}$. Now successively applying Lemma 11 we have:

$$P(I_3) = \frac{1}{2} + 1 = \frac{3}{2}, \quad P(I_2) = \frac{2}{3} + 1 = \frac{5}{3}, \quad P(I_1) = \frac{3}{5} + 2 = \frac{13}{5}.$$

Therefore, 13 is the multiplicity of $\mathrm{S}\left(\left[\frac{33}{13}, \frac{66}{25}\right]\right)$.

REMARK 14.

1. In this note we intend to show how, given a closed interval I, we can decide if $\mathrm{S}(I) \neq \mathbb{N}$. Assume that a_1, b_1, a_2 and b_2 are positive integers such that $I = \left[\frac{b_1}{a_1}, \frac{b_2}{a_2}\right]$. In view of Proposition 1 we know that $\mathrm{S}(I) = \{x \in \mathbb{N} \mid a_1 b_2 x \bmod b_1 b_2 \leqslant (a_1 b_2 - a_2 b_1)\, x\}$. Observe that $\mathrm{S}(I) = \mathbb{N}$ if and only if $1 \in \mathrm{S}(I)$, which is equivalent to $a_1 b_2 \bmod b_1 b_2 \leqslant a_1 b_2 - a_2 b_1$.
2. Also observe that if $c < a < b$, then $\mathrm{S}(a,b,c) = \mathrm{S}\left(\left[\frac{b}{a}, \frac{b}{a-c}\right]\right)$. As $\frac{b}{a} > 1$, by applying Lemma 2 we deduce that $\mathrm{S}(a,b,c) \neq \mathbb{N}$.

In the following example, we apply Algorithm 12 to calculate the smallest positive integer that is solution of a proportionally modular Diophantine inequality.

EXAMPLE 15. We find the smallest positive integer that satisfies the inequality $231x \bmod 938 \leqslant 3x$. To this end, by using Proposition 1, it suffices to calculate the multiplicity of $\mathrm{S}\left(\left[\frac{938}{231}, \frac{938}{228}\right]\right)$, which can be obtained by applying Algorithm 12.

1. $I_1 = \left[\frac{938}{231}, \frac{938}{228}\right]$, $I_2 = \left[\frac{228}{26}, \frac{231}{14}\right]$.
2. As I_2 contains an integer, $P(I_2) = \frac{9}{1}$.
3. $P(I_1) = \frac{1}{9} + 4 = \frac{37}{9}$.
4. 37 is the multiplicity of $\mathrm{S}\left(\left[\frac{938}{231}, \frac{938}{228}\right]\right)$.

Therefore 37 is the smallest positive integer that is solution of the inequality $231x \bmod 938 \leqslant 3x$.

4. An application

Let n_1, n_2 and n_3 be three positive integers. Our aim in this section will be to give an algorithm that allows us to calculate the smallest positive multiple of n_3 that belongs to $\langle n_1, n_2 \rangle$.

We start by introducing two lemmas that will tell us that we can focus on the case where n_1 and n_2 are relatively prime.

LEMMA 16. *Let n_1, n_2 and n_3 be positive integers and let $d = \gcd\{n_1, n_2, n_3\}$. If $\xi \frac{n_3}{d}$ is the smallest positive multiple of $\frac{n_3}{d}$ that belongs to $\left\langle \frac{n_1}{d}, \frac{n_2}{d} \right\rangle$, then ξn_3 is the smallest positive multiple of n_3 that belongs to $\langle n_1, n_2 \rangle$.*

Proof. It suffices to observe that if k is a positive integer, then $k\frac{n_3}{d} \in \left\langle \frac{n_1}{d}, \frac{n_2}{d} \right\rangle$ if and only if $kn_3 \in \langle n_1, n_2 \rangle$. □

LEMMA 17. *Let n_1, n_2 and n_3 be positive integers such that $\gcd\{n_1, n_2, n_3\} = 1$ and let $d = \gcd\{n_1, n_2\}$. If ξn_3 is the smallest positive multiple of n_3 that belongs to $\left\langle \frac{n_1}{d}, \frac{n_2}{d} \right\rangle$, then $\xi d n_3$ is the smallest positive multiple of n_3 that belongs to $\langle n_1, n_2 \rangle$.*

Proof. Let $\overline{\xi} n_3$ be the smallest positive multiple of n_3 that belongs to $\langle n_1, n_2 \rangle$. Let us see that $\overline{\xi} = \xi d$. Since $\xi n_3 \in \left\langle \frac{n_1}{d}, \frac{n_2}{d} \right\rangle$, $\xi n_3 = \lambda \frac{n_1}{d} + \mu \frac{n_2}{d}$, for some $\lambda, \mu \in \mathbb{N}$. Therefore $\xi d n_3 = \lambda n_1 + \mu n_2 \in \langle n_1, n_2 \rangle$. Consequently $\overline{\xi} \leqslant \xi d$. As $\overline{\xi} n_3 \in \langle n_1, n_2 \rangle$, $\overline{\xi} n_3 = s n_1 + t n_2$, for some $s, t \in \mathbb{N}$. Thus $d | \overline{\xi} n_3$. As $\gcd\{n_1, n_2, n_3\} = 1$, $\gcd\{d, n_3\} = 1$ and in consequence $d | \overline{\xi}$. Then we have that $\frac{\overline{\xi}}{d} n_3 = s\frac{n_1}{d} + t\frac{n_2}{d}$ and therefore $\xi \leqslant \frac{\overline{\xi}}{d}$. □

The following result is a reformulation of [9, Lemma 4].

LEMMA 18. *Let n_1 and n_2 be relatively prime positive integers and let u be a positive integer such that $un_2 \equiv 1 \pmod{n_1}$. Then $\langle n_1, n_2 \rangle = \{x \in \mathbb{N} \mid un_2 x \bmod n_1 n_2 \leqslant x\}$.*

Observe that if n_1 and n_2 are relatively prime, then by Bézout's lemma, there exist positive integers u and v such that $un_2 - vn_1 = 1$. Moreover these integers are calculable by the so called extended Euclides algorithm (see for example [3]).

PROPOSITION 19. *Let n_1, n_2 and n_3 be positive integers such that* $\gcd\{n_1, n_2\} = 1$ *and let u be a positive integer such that* $un_2 \equiv 1 \pmod{n_1}$. *If* m *is the multiplicity of the semigroup* $\mathrm{S}(un_2n_3, n_1n_2, n_3)$, *then* $\mathrm{m}n_3$ *is the smallest positive multiple of n_3 that belongs to* $\langle n_1, n_2 \rangle$.

Proof. Let k be a positive integer. In view of Lemma 18 we deduce that $kn_3 \in \langle n_1, n_2 \rangle$ if and only if $un_2n_3k \bmod n_1n_2 \leqslant n_3k$ and this is equivalent to $k \in \mathrm{S}(un_2n_3, n_1n_2, n_3)$. □

Now we will present the algorithm announced at the beginning of this section.

ALGORITHM 20. Input: n_1, n_2 and n_3 positive integers such that $\gcd\{n_1, n_2\} = 1$.

Output: $\xi = \min\{k \in \mathbb{N}\backslash\{0\} \mid kn_3 \in \langle n_1, n_2 \rangle\}$.

1. Calculate, using the extended Euclides algorithm, a positive integer u such that $un_2 \equiv 1 \pmod{n_1}$.
2. Calculate by applying Algorithm 12 the multiplicity m of

$$\mathrm{S}(un_2n_3, n_1n_2, n_3) = \mathrm{S}(un_2n_3 \bmod n_1n_2, n_1n_2, n_3).$$

3. Return m.

We finish this paper by illustrating the steps of this algorithm with an example.

EXAMPLE 21. Let us calculate the smallest positive multiple of 37 that belongs to $\langle 68, 79 \rangle$.

1. By applying the extended Euclides algorithm we calculate a positive integer u such that $79 \cdot u \equiv 1 \pmod{68}$. Consider $u = 31$.
2. Let us calculate the multiplicity of

$$\mathrm{S}(31 \cdot 79 \cdot 37, 68 \cdot 79, 37) = \mathrm{S}(90613, 5372, 37) = \mathrm{S}(4661, 5372, 37).$$

The sequence of intervals associated to $I = \left[\frac{5372}{4661}, \frac{5372}{4624}\right]$ is

$$I_1 = \left[\frac{5372}{4661}, \frac{5372}{4624}\right], \quad I_2 = \left[\frac{4624}{748}, \frac{4661}{711}\right], \quad I_3 = \left[\frac{711}{395}, \frac{748}{136}\right].$$

As I_3 contains an integer, we have that $P(I_3) = \frac{2}{1}$. Then $P(I_2) = \frac{1}{2} + 6 = \frac{13}{2}$ and $P(I_1) = \frac{2}{13} + 1 = \frac{15}{13}$. Therefore the multiplicity of $\mathrm{S}(4661, 5372, 37)$ is 15.

3. Thus $15 \cdot 37$ is the smallest positive multiple of 37 that belongs to $\langle 68, 79 \rangle$.

5. The Frobenius number and the number of gaps of a numerical semigroup generated by three positive integers

Let S be a numerical semigroup. Since $\mathbb{N}\backslash S$ is finite, the set $\mathbb{Z}\backslash S$ has a maximum. This integer is called the Frobenius number of S (see [4]) and we will denote it by $\mathrm{g}(S)$. For a set A, we write $\#A$ for its cardinality. The elements of $\mathbb{N}\backslash S$ are the so called gaps of S. The set of gaps of S is denoted by $\mathrm{H}(S)$.

It is well-known (see for example [6]) that every numerical semigroup S is finitely generated and therefore there exists a finite subset A of $\mathbb{N}$ such that $S = \langle A \rangle$. We say that A is a minimal system of generators of S if no proper subset of A generates S. It is also well-known (see for instance [6]) that $S^* \setminus (S^* + S^*)$ is the unique minimal system of generators of S, with $S^* = S \setminus \{0\}$.

Let S be a numerical semigroup minimally generated by $\{n_1, n_2\}$. Then Sylvester proved in [10, 11] that $\mathrm{g}(S) = n_1 n_2 - n_1 - n_2$ and $\#\mathrm{H}(S) = \frac{(n_1-1)(n_2-1)}{2}$. If S is minimally generated by $\{n_1, \ldots, n_p\}$, with $p > 2$, then it is still an open problem to find formulas for $\mathrm{g}(S)$ and $\#\mathrm{H}(S)$ in terms of $n_1, \ldots, n_p$. Particulary, the case $p = 3$ is not solved. In this section, and as an application of the results presented in the previous section, we give an algorithm that computes the Frobenius number and the number of gaps of a numerical semigroup minimally generated by $\{n_1, n_2, n_3\}$. The complexity of this algorithm is the same of the Euclides algorithm, and therefore of $O(\log n)$ complexity (see [3]). In this sense is at the same level of the best existing algorithms to solve this problem (see [4]).

Along this paragraph we shall suppose that S is a numerical semigroup minimally generated by $\{n_1, n_2, n_3\}$. In the study of $\mathrm{g}(S)$ and $\#\mathrm{H}(S)$ we can assume that $\gcd\{n_i, n_j\} = 1$, for $i \neq j$ with $i, j \in \{1, 2, 3\}$. This is due to the following. If $d = \gcd\{n_1, \ldots, n_{p-1}\}$, then Johnson showed in [2] that

$$\mathrm{g}(\langle n_1, \ldots, n_{p-1}, n_p \rangle) = d \cdot \mathrm{g}\left(\left\langle \frac{n_1}{d}, \ldots, \frac{n_{p-1}}{d}, n_p \right\rangle\right) + (d-1)\, n_p$$

and Rödseth gives in [5] the formula

$$\#\mathrm{H}(\langle n_1, \ldots, n_{p-1}, n_p \rangle) = d \cdot \#\mathrm{H}\left(\left\langle \frac{n_1}{d}, \ldots, \frac{n_{p-1}}{d}, n_p \right\rangle\right) + \frac{1}{2}(n_p - 1)(d-1).$$

Hence, we can suppose that $\gcd\{n_1, n_2\} = \gcd\{n_1, n_3\} = \gcd\{n_2, n_3\} = 1$. Denote by c_i the positive integer $\min\{x \in \mathbb{N}\setminus\{0\} \mid x n_i \in \langle n_j, n_k \rangle\}$, with $\{i, j, k\} = \{1, 2, 3\}$. In [7, Proposition 15] it is proved that

$$\mathrm{g}(S) = \frac{1}{2}\left((c_1 - 2)n_1 + (c_2 - 2)n_2 + (c_3 - 2)n_3 + \Delta\right)$$

with

$$\Delta = \sqrt{(c_1 n_1 + c_2 n_2 + c_3 n_3)^2 - 4(c_1 n_1 c_2 n_2 + c_1 n_1 c_3 n_3 + c_2 n_2 c_3 n_3 - n_1 n_2 n_3)}$$

and in [7, Proposition 17] that

$$\#\mathrm{H}(S) = \frac{1}{2}((c_1 - 1)n_1 + (c_2 - 1)n_2 + (c_3 - 1)n_3 - c_1 c_2 c_3 + 1).$$

Observe that, by applying Algorithm 20, we obtain c_1, c_2 and c_3. Now, using the previous formulas, we have $\mathrm{g}(S)$ and $\#\mathrm{H}(S)$.

Acknowledgement. The authors want to thank P. A. Garcĺa-Sánchez and the referee for their wise comments and suggestions.

REFERENCES

[1] V. BARUCCI, D. E. DOBBS AND M. FONTANA, *Maximality Properties in Numerical Semigroups and Applications to One-Dimensional Analytically Irreducible Local Domains*, Memoirs of the Amer. Math. Soc. 598 (1997).
[2] S. M. JOHNSON, *A linear Diophantine problem*, Can. J. Math. 12 (1960), 390–398.
[3] J. D. LIPSON, *Elements of algebra and algebraic computing*, Addison-Wesley, 1981.
[4] J. L. RAMÍREZ ALFONSÍN, *The diophantine Frobenius problem*, Oxford Univ. Press, 2005.
[5] Ö. J. RÖDSETH, *On a linear Diophantine problem of Frobenius*, J. Reine Angew. Math. 301 (1978), 171–178.
[6] J. C. ROSALES AND P. A. GARCÍA-SÁNCHEZ, *Finitely generated commutative monoids*, Nova Science Publishers, New York, 1999.
[7] J. C. ROSALES AND P. A. GARCÍA-SÁNCHEZ, *Numerical semigroups with embedding dimension three*, Archiv Math (Basel) 83 (2004), 488–496.
[8] J. C. ROSALES, P. A. GARCÍA-SÁNCHEZ, J. I. GARCÍA-GARCÍA AND J. M. URBANO-BLANCO, *Proportionally modular Diophantine inequalities*, J. Number Theory 103 (2003), 281–294.
[9] J. C. ROSALES, AND J. M. URBANO-BLANCO, *Proportionally modular Diophantine inequalities and full semigroups*, Semigroup Forum 72 (2006), 362–374.
[10] J. J. SYLVESTER, *Excursus on rational fractions and partitions*, Amer J. Math. 5 (1882), 119–136.
[11] J. J. SYLVESTER, *Mathematical questions with their solutions*, Educational Times 41 (1884), 21.

(Received October 16, 2006)

J. C. Rosales
Departamento de Álgebra
Universidad de Granada
E-18071 Granada
Spain
e-mail: jrosales@ugr.es

P. Vasco
Departamento de Matemática
Universidade de Trás-os-Montes e Alto Douro
5001-801 Vila Real
Portugal
e-mail: pvasco@utad.pt