The smallest positive integer that is solution of a proportionally modular Diophantine inequality

P. Vasco

Iberian meeting on numerical semigroups, Porto 2008

J. C. Rosales and P. Vasco, The smallest positive integer that is solution of a proportionally modular Diophantine inequality, Mathematical Inequalities and Applications, to appear.

AIM

Given two integers m and n with $n \neq 0$, we denote by $m \mod n$ the remainder of the division of m by n. A proportionally modular Diophantine inequality is an expression of the form $ax \mod b \leq cx$, where a, b and c are positive integers.

Our principal aim is

To give an algorithm that allows us to calculate the smallest positive integer that is solution of a proportionally modular Diophantine inequality.

Given the proportionally modular Diophantine inequality $ax \mod b \leq cx$, we denote by $\mathrm{S}(a,b,c)$ the set of integer solutions of this inequality, $\mathrm{S}(a,b,c) = \{x \in \mathbb{N} \mid ax \mod b \leq cx\}$. We will refer to these type of semigroups as proportionally modular numerical semigroups.

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.

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 $T \cap \mathbb{N} = \{x \in \mathbb{N} \mid ax \mod b \leq cx\}$.
2. 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 $T \cap \mathbb{N} = \{x \in \mathbb{N} \mid a_1 b_2 x \mod b_1 b_2 \leq (a_1 b_2 - a_2 b_1) x\}$.

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.

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 $T \cap \mathbb{N} = \{x \in \mathbb{N} \mid ax \mod b \leq cx\}$.
2. 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 $T \cap \mathbb{N} = \{x \in \mathbb{N} \mid a_1 b_2 x \mod b_1 b_2 \leq (a_1 b_2 - a_2 b_1) x\}$.

- $T \cap \mathbb{N}$ is 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 $\mathrm{S}\left(\left[\frac{b_1}{a_1}, \frac{b_2}{a_2}\right]\right)$.

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.

Lemma 2

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

Lemma 3

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

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 $\frac{\mathrm{m}}{t} \in I$.

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 $t \leq x$.

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 $t \leq x$.

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 $P([a+\alpha, a+\beta]) = \frac{\mathrm{m}+ta}{t}$.

Given a rational number x we denote by $\lfloor x \rfloor$ the integer $\max\{z \in \mathbb{Z} \mid z \leq x\}$ and by $\lceil x \rceil$ the integer $\min\{z \in \mathbb{Z} \mid x \leq z\}$. 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 $\lfloor \alpha \rfloor = \lfloor \beta \rfloor$.

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 $\frac{a_2}{b_2 \mod a_2} < \frac{a_1}{b_1 \mod a_1}$ and $\mathrm{S}\left(\left[\frac{a_2}{b_2 \mod a_2}, \frac{a_1}{b_1 \mod a_1}\right]\right) \neq \mathbb{N}$. Moreover, if $P\left(\left[\frac{a_2}{b_2 \mod a_2}, \frac{a_1}{b_1 \mod a_1}\right]\right) = \frac{\mathrm{m}}{t}$, then $P\left(\left[\frac{b_1}{a_1}, \frac{b_2}{a_2}\right]\right) = \frac{t + \left\lfloor \frac{b_1}{a_1} \right\rfloor \mathrm{m}}{\mathrm{m}}$.

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 $\frac{a_2}{b_2 \mod a_2} < \frac{a_1}{b_1 \mod a_1}$ and $\mathrm{S}\left(\left[\frac{a_2}{b_2 \mod a_2}, \frac{a_1}{b_1 \mod a_1}\right]\right) \neq \mathbb{N}$. Moreover, if $P\left(\left[\frac{a_2}{b_2 \mod a_2}, \frac{a_1}{b_1 \mod a_1}\right]\right) = \frac{\mathrm{m}}{t}$, then $P\left(\left[\frac{b_1}{a_1}, \frac{b_2}{a_2}\right]\right) = \frac{t + \left\lfloor \frac{b_1}{a_1} \right\rfloor \mathrm{m}}{\mathrm{m}}$.

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 $R(I) = \left[\frac{a_2}{b_2 \mod a_2}, \frac{a_1}{b_1 \mod a_1}\right]$.

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 $n \geq k$.

The Euclides algorithm for calculating the greatest common divisor of two positive integers.
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 $(x, y) := (y, x \mod y)$
Return x
End.

The Euclides algorithm for calculating the greatest common divisor of two positive integers.
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 $(x,y) := (y, x \mod y)$
- Return x

End.

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 $R(I) = \left[\frac{a_2}{b_2 \mod a_2}, \frac{a_1}{b_1 \mod a_1}\right]$.

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.

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 $n \geq 4$.

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 $n\geq 4$.

(33,13), (13,7), (7,6), (6,1), (1,0)

(66,25), (25,16), (16,9), (9,7), (7,2), (2,1), (1,0)

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 $R(I)=\left[\frac{a_2}{b_2 \mod a_2},\frac{a_1}{b_1 \mod a_1}\right]$.

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 $\lfloor I \rfloor$.

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 $k \in \{2, \ldots, l\}$, $P(I_{k-1}) = \frac{1}{P(I_k)} + \lfloor I_{k-1} \rfloor$.

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 $S\left(\left[\frac{33}{13},\frac{66}{25}\right]\right)$. We already made the computation 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 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 $S\left(\left[\frac{33}{13},\frac{66}{25}\right]\right)$.

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 $T \cap \mathbb{N} = \{x \in \mathbb{N} \mid ax \mod b \leq cx\}$.

Example 15

We find the smallest positive integer that satisfies the inequality $231x \mod 938 \leq 3x$. To this end, by using Proposition 1, it suffices to calculate the multiplicity of $\mathrm{S}\left(\left[\frac{938}{231}, \frac{938}{228}\right]\right)$.

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 $231x \mod 938 \leq 3x$.

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 $\langle n_1, n_2\rangle$.

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
$$\mathrm{S}(un_2n_3, n_1n_2, n_3) = \mathrm{S}(un_2n_3 \mod n_1n_2, n_1n_2, n_3).$$
3. Return m.

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 $u \in \mathbb{N}$ such that $79 \cdot u \equiv 1 \pmod{68}$. Consider $u = 31$.
2. Let us calculate the multiplicity of $S(31 \cdot 79 \cdot 37, 68 \cdot 79, 37) = S(90613, 5372, 37) = S(4661, 5372, 37)$.
   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, $P(I_3) = \frac{2}{1}$. 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 $S(4661, 5372, 37)$ is 15.
3. Thus $15 \cdot 37$ is the smallest positive multiple of 37 that belongs to $\langle 68, 79\rangle$.

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

J. C. Rosales and P. A. García-Sánchez, Numerical semigroups with embedding dimension three, Archiv Math (Basel) 83 (2004), 488-496.

J. C. Rosales, M. Bullejos, Proportionally modular Diophantine inequalities and Stern-Brocot tree.