Mathematical
Inequalities
& Applications
Volume 8, Number 4 (2005), 565–570

PSEUDO–SYMMETRIC MODULAR DIOPHANTINE INEQUALITIES

J. C. ROSALES

(*communicated by J. Pečarić*)

Abstract. In this paper we study and characterize those Diophantine inequalities $ax \bmod b \leqslant x$ whose set of solutions is a pseudo-symmetric numerical semigroup.

Following the notation used in [11], a *modular Diophantine inequality* is an expression of the form $ax \bmod b \leqslant x$. The set $\mathrm{S}(a,b)$ of integer solutions of this inequality is a numerical semigroup, that is, it is a subset of $\mathbb{N}$ (the set of nonnegative integers) closed under addition, $0 \in \mathrm{S}(a,b)$ and $\mathbb{N} \setminus \mathrm{S}(a,b)$ has finitely many elements. We say that a numerical semigroup is *modular* if it is the set of solutions to a modular Diophantine inequality. As shown in [11], not every numerical semigroup is of this form.

If S is a numerical semigroup, then the greatest integer not in S is the Frobenius number of S, denoted by $\mathrm{g}(S)$. We say that S is *irreducible* (see [5]) if it cannot be expressed as an intersection of two numerical semigroups that contain it properly. The numerical semigroup S is *symmetric* (respectively *pseudo-symmetric*) if it is irreducible with odd (respectively even) Frobenius number. These semigroups have been widely studied (see for instance [2] and the references given there). An inequality $ax \bmod b \leqslant x$ is *symmetric* (respectively *pseudo-symmetric*) if $\mathrm{S}(a,b)$ is a symmetric (respectively pseudo-symmetric) numerical semigroup. In [6] we initiated the study of symmetric modular Diophantine inequalities, in this paper we focus on pseudo-symmetric modular Diophantine inequalities.

Every numerical semigroup S is finitely generated and thus there exist positive integers $n_1, \ldots, n_p$ such that $S = \langle n_1, \ldots, n_p \rangle = \{a_1 n_1 + \ldots + a_p n_p \mid a_1, \ldots, a_p \in \mathbb{N}\}$. If no proper subset of $\{n_1, \ldots, n_p\}$ generates S, then we say that $\{n_1, \ldots, n_p\}$ is a minimal system of generators of S. The minimal system of generators of a numerical semigroup is unique (see [7]) and its cardinality is known as the *embedding dimension* of S, denoted by $\mathrm{e}(S)$.

Observe that $\mathrm{S}(1,b) = \mathbb{N}$ and that the inequality $ax \bmod b \leqslant x$ has the same solutions as the inequality $(a \bmod b)x \bmod b \leqslant x$. Thus we will assume that a and

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

Key words and phrases: numerical semigroups, symmetric, pseudo-symmetric, modular Diophantine inequalities, Frobenius number.

The author is supported by the project BFM2000-1469 and wants to thank P. A. García-Sánchez for his comments and suggestions.

b are integers such that $2 \leqslant a < b$. In the rest of the paper we will use d and d' to denote the integers $\gcd\{a,b\}$ and $\gcd\{a-1,b\}$, respectively.

In Theorem 10 we will explicitly describe a minimal system of generators of $\mathrm{S}(a,b)$ when this semigroup is pseudo-symmetric. As a consequence of this result we will obtain that these numerical semigroups have embedding dimension three. Theorem 14 characterizes pseudo-symmetric modular numerical semigroups in terms of its generators and Frobenius number. We finish this paper by describing those positive integers that are the Frobenius numbers of pseudo-symmetric modular numerical semigroup.

The following result is a consequence of Corollaries 6, 16 and 17, and Lemma 11 in [11].

LEMMA 1.

1) *If* $x \in \mathbb{Z} \setminus \mathrm{S}(a,b)$*, then* $b - x \in \mathrm{S}(a,b)$.
2) *Let* x *be a positive integer. Then* $x \in \mathrm{S}(a,b)$ *and* $b - x \in \mathrm{S}(a,b)$ *if and only if*

$$x \in \left\{ k\frac{b}{d} \mid 0 \leqslant k \leqslant d-1 \} \cup \{ k\frac{b}{d'} \mid 0 \leqslant k \leqslant d'-1 \right\}.$$

3) $b - d - d' \geqslant \mathrm{g}(\mathrm{S}(a,b))$.
4) $\mathrm{S}(a,b)$ *is symmetric if and only if* $\mathrm{g}(\mathrm{S}(a,b)) = b - d - d'$.
5) $\mathrm{S}(a,b)$ *is pseudo-symmetric if and only if* $\mathrm{g}(\mathrm{S}(a,b)) = b - d - d' - 1$.

As an immediate consequence of 3) and 4) in Lemma 1, we obtain the following result.

LEMMA 2. $\mathrm{S}(a,b)$ *is symmetric if and only if* $b - d - d' \notin \mathrm{S}(a,b)$.

In the literature one can find several characterizations of the concept of symmetric numerical semigroup. The most common is the following (see for instance [1]).

LEMMA 3. *A numerical semigroup* S *is symmetric if and only if* $x \in \mathbb{Z} \setminus S$ *implies* $\mathrm{g}(S) - x \in S$.

LEMMA 4. $\mathrm{S}(a,b)$ *is pseudo-symmetric if and only if* $b - d - d' - 1 \notin \mathrm{S}(a,b)$.

Proof. If $\mathrm{S}(a,b)$ is pseudo-symmetric, then by 5) in Lemma 1, we have that $b - d - d' - 1 \notin \mathrm{S}(a,b)$. In order to prove the converse, it suffices to show that $\mathrm{g}(\mathrm{S}(a,b)) = b - d - d' - 1$ and then use 5) in Lemma 1. We first see that $b - d - d' \in \mathrm{S}(a,b)$. If this were not the case, then in view of Lemma 2, $\mathrm{S}(a,b)$ would be symmetric and by 4) in Lemma 1, $\mathrm{g}(\mathrm{S}(a,b)) = b - d - d'$. As $2 \leqslant a < b$, we have that $1 \notin \mathrm{S}(a,b)$. From Lemma 3, we deduce that $b - d - d' - 1 \in \mathrm{S}(a,b)$, in contradiction with the hypothesis. Hence $b - d - d' \in \mathrm{S}(a,b)$ and by 3) in Lemma 1, we deduce that $\mathrm{g}(\mathrm{S}(a,b)) = b - d - d' - 1$. □

As with symmetric numerical semigroups, one can find in the literature several characterizations of the pseudo-symmetric property. The following appears in [3].

LEMMA 5. *A numerical semigroup* S *is pseudo-symmetric if and only if* $\mathrm{g}(S)$ *is even and* $\{x, \mathrm{g}(S) - x\} \subseteq \mathbb{Z} \setminus S$ *implies that* $x = \frac{\mathrm{g}(S)}{2}$.

LEMMA 6. *If* $\mathrm{S}(a,b)$ *is pseudo-symmetric, then*

$$\mathrm{S}(a,b)=\left\langle \frac{b}{d},\frac{b}{d'},d+d'+1,\frac{b+d+d'+1}{2}\right\rangle .$$

Proof. By 5) in Lemma 1, we know that $\mathrm{g}(\mathrm{S}(a,b))=b-d-d'-1$. Hence $\frac{b-d-d'-1}{2}\notin \mathrm{S}(a,b)$, which in view of 1) in Lemma 1 implies that $\frac{b+d+d'+1}{2}=b-\frac{b-d-d'-1}{2}\in \mathrm{S}(a,b)$. As $b-d-d'-1\notin \mathrm{S}(a,b)$, by using again 1) in Lemma 1, we have that $d+d'+1\in \mathrm{S}(a,b)$. Besides, $a\frac{b}{d} \bmod b=0$ and $a\frac{b}{d'} \bmod b\leqslant \frac{b}{d'}$, and consequently $\{\frac{b}{d},\frac{b}{d'}\}\subseteq \mathrm{S}(a,b)$. This proves that $\{\frac{b}{d},\frac{b}{d'},d+d'+1,\frac{b+d+d'+1}{2}\}\subseteq \mathrm{S}(a,b)$ and consequently $\langle \frac{b}{d},\frac{b}{d'},d+d'+1,\frac{b+d+d'+1}{2}\rangle \subseteq \mathrm{S}(a,b)$. For the other inclusion, let $x\in \mathrm{S}(a,b)$ and $t=\max\{k\in\mathbb{N}\mid x-k(d+d'+1)\in \mathrm{S}(a,b)\}$. Then $x-(t+1)(d+d'+1)\notin \mathrm{S}(a,b)$. By using Lemma 5, we have one of the following two cases.

1) If $b-d-d'-1-(x-(t+1)(d+d'+1))\in \mathrm{S}(a,b)$, then $b-(x-t(d+d'+1))\in \mathrm{S}(a,b)$. As $x-t(d+d'+1)\in \mathrm{S}(a,b)$, by 2) in Lemma 1, we deduce that $x\in\langle \frac{b}{d},\frac{b}{d'},d+d'+1\rangle$.

2) If $x-(t+1)(d+d'+1)=\frac{b-d-d'-1}{2}$, then $x=t(d+d'+1)+\frac{b+d+d'+1}{2}\in \langle d+d'+1,\frac{b+d+d'+1}{2}\rangle$. □

This result is telling us that if $\mathrm{S}(a,b)$ is pseudo-symmetric, then $\mathrm{e}(\mathrm{S}(a,b))\leqslant 4$. We do not highlight this result, since in Corollary 11 we will see that $\mathrm{e}(\mathrm{S}(a,b))=3$.

LEMMA 7. $\mathrm{S}(a,b)$ *is pseudo-symmetric if and only if* $0<a(d+d'+1) \bmod b<d+d'+1$.

Proof. If $\mathrm{S}(a,b)$ is pseudo-symmetric, then by Lemma 6, we know that $d+d'+1\in \mathrm{S}(a,b)$ and thus $0\leqslant a(d+d'+1) \bmod b\leqslant d+d'+1$. If $a(d+d'+1) \bmod b=0$, then $a(b-d-d'-1) \bmod b=0$, which implies that $b-d-d'-1\in \mathrm{S}(a,b)$, in contradiction with what we obtained in Lemma 4. If $a(d+d'+1) \bmod b=d+d'+1$, then $a(b-d-d'-1) \bmod b=b-d-d'-1$. Again this leads to $b-d-d'-1\in \mathrm{S}(a,b)$, which is impossible.

If $0<a(d+d'+1) \bmod b<d+d'+1$, then $a(b-d-d'-1) \bmod b=b-(a(d+d'+1) \bmod b)>b-d-d'-1$, meaning that $b-d-d'-1\notin \mathrm{S}(a,b)$. By Lemma 4, we can assert that $\mathrm{S}(a,b)$ is pseudo-symmetric. □

The following result is a reformulation of [11, Lemma 4].

LEMMA 8. $\mathrm{S}(a,b)=S(b+1-a,b)$.

The following result is the key to understand that the condition imposed in Theorem 10 is not restrictive.

LEMMA 9. *If* $\mathrm{S}(a,b)$ *is pseudo-symmetric, then* $1\in\{d,d'\}$.

Proof. Assume that $d\neq 1\neq d'$. As $\gcd\{a,a-1\}=1$, we deduce that $d\neq d'$. We distinguish two cases.

1) Assume that $d > d' \geqslant 2$. Observe that there exist positive integers u, v and k such that $a = ud$, $a-1 = vd'$, $b = kdd'$ and (thus) $ud - vd' = 1$. Hence $\mathrm{S}(a,b) = \mathrm{S}(ud, kdd')$. By Lemma 7 we know that $0 < ud(d+d'+1) \bmod kdd' < d+d'+1$ and consequently $0 < d(u(d+d'+1) \bmod kd') < d+d'+1$. Thus $0 < u(d+d'+1) \bmod kd' < \frac{d+d'+1}{d} \leqslant 2$. This implies that $u(d+d'+1) \bmod kd' = 1$. Then there exists $q \in \mathbb{N}$ such that $u(d+d'+1) = qkd'+1$. Hence $qkd'+1 = ud+ud'+u = 1+vd'+ud'+u = 1+u+(u+v)d'$. This leads to $qkd' = u+(u+v)d'$, which implies that d' divides u, in contradiction with $ud - vd' = 1$ and $d' \geqslant 2$.

2) Assume that $d' > d \geqslant 2$. By Lemma 8, we know that $\mathrm{S}(a,b) = \mathrm{S}(b+1-a,b)$. Moreover, $\gcd\{a,b\} = \gcd\{b+1-a-1,b\}$ and $\gcd\{a-1,b\} = \gcd\{b+1-a,b\}$. Hence $\mathrm{S}(b+1-a,b)$ is under the conditions of case 1), and we obtain again a contradiction. □

REMARK 1. Observe that as a consequence of Lemmas 8 and 9, every pseudo-symmetric modular numerical semigroup is of the form $\mathrm{S}(a,b)$ with $2 \leqslant a < b$ and $\gcd\{a-1,b\} = 1$.

THEOREM 10. *Let a and b be positive integers such that $2 \leqslant a < b$ and $\gcd\{a-1,b\} = 1$. Let $d = \gcd\{a,b\}$. Then $\mathrm{S}(a,b)$ is pseudo-symmetric if and only if $0 < a(d+2) \bmod b < d+2$. Moreover, if this is the case, then $\mathrm{S}(a,b) = \langle \frac{b}{d}, d+2, \frac{b+d+2}{2} \rangle$ and $\mathrm{g}(\mathrm{S}(a,b)) = b-d-2$.*

Proof. The first part is a consequence of Lemma 7; the second of Lemma 6 and 5) in Lemma 1. □

It is well known (see for instance [3]) that if S is a numerical semigroup with $\mathrm{e}(S) \leqslant 2$, then it is symmetric and thus it is not pseudo-symmetric. As a consequence of Theorem 10 we obtain the following result.

COROLLARY 11. *If $\mathrm{S}(a,b)$ is pseudo-symmetric, then $\mathrm{e}(\mathrm{S}(a,b)) = 3$.*

In the following examples we highlight the results obtained so far.

EXAMPLE 1.

- Observe that $\gcd\{6,20\} \neq 1 \neq \gcd\{5,20\}$. Hence by Lemma 9, $\mathrm{S}(6,20)$ is not pseudo-symmetric.
- Observe that $\mathrm{S}(5,8)$ does not fulfill the conditions to apply Theorem 10. However, by Lemma 8, $\mathrm{S}(5,8) = \mathrm{S}(4,8)$ and we can use Theorem 10 with $\mathrm{S}(4,8)$. As $(4 \times 6) \bmod 8 = 0$, we can assert that $\mathrm{S}(5,8)$ ($= \mathrm{S}(4,8)$) is not pseudo-symmetric.
- Observe that $\mathrm{S}(6,9)$ is under the conditions of Theorem 10. Moreover, $(6 \times 5) \bmod 9 = 3$, which in view of Theorem 10 implies that $\mathrm{S}(6,9)$ is pseudo-symmetric, $\mathrm{S}(6,9) = \langle 3,5,7 \rangle$ and $\mathrm{g}(\mathrm{S}(6,9)) = 4$.

Note that by Theorem 10 we know that every modular pseudo-symmetric numerical semigroup S has the form $\langle \frac{n}{t}, t+2, \frac{n+t+2}{2} \rangle$ and with $\mathrm{g}(S) = n-t-2$. Our next goal will be Theorem 14 in which we give the conditions that a couple of integers n and t must fulfill so that $\langle \frac{n}{t}, t+2, \frac{n+t+2}{2} \rangle$ is a pseudo-symmetric modular numerical semigroup with Frobenius number $n-t-2$.

The following result can be deduced from [4].

LEMMA 12. *Let* $S = \langle n_1, n_2, n_3 \rangle$ *be a numerical semigroup. If* $\gcd\{n_1, n_2\} n_3 \in \langle n_1, n_2 \rangle$ *, then* S *is symmetric.*

LEMMA 13. *Let* n *and* t *be positive integers such that* t *divides* n*. If* $S = \langle \frac{n}{t}, t+2, \frac{n+t+2}{2} \rangle$ *is a pseudo-symmetric numerical semigroup and* $\mathrm{g}(S) = n-t-2$*, then* $\frac{n}{t}$ *is odd.*

Proof. Since S is pseudo-symmetric, we have that $\mathrm{g}(S) = n-t-2$ is even. If $\frac{n}{t}$ is even, then so is $t+2$. As $2\frac{n+t+2}{2} = t\frac{n}{t} + t + 2 \in \langle \frac{n}{t}, t+2 \rangle$, from Lemma 12 we deduce that S is symmetric, contradicting that S is pseudo-symmetric. □

THEOREM 14. *Let* $t < n$ *be two positive integers such that* t *divides* n*. Then* $S = \langle \frac{n}{t}, t+2, \frac{n+t+2}{2} \rangle$ *is a pseudo-symmetric modular numerical semigroup with Frobenius number* $n-t-2$ *if and only if* $\frac{n}{t}$ *is odd and* $\gcd\{t+2, \frac{n}{t}\} = 1$*.*

Proof. Necessity. By Lemma 13 we know that $\frac{n}{t}$ is odd. Since S is a numerical semigroup $\gcd\{\frac{n}{t}, t+2, \frac{n+t+2}{2}\} = 1$. From the equality $2\frac{n+t+2}{2} = t\frac{n}{t} + t + 2$, we deduce that $\gcd\{\frac{n}{t}, t+2\} = 1$.

Sufficiency. If $\gcd\{t+2, \frac{n}{t}\} = 1$, then there exists $u \in \{1, \ldots, \frac{n}{t} - 1\}$ such that $u(t+2) \equiv 1 \bmod \frac{n}{t}$. Note that $\gcd\{u, \frac{n}{t}\} = 1$. We prove that $S = \mathrm{S}(ut, n)$ and that $\mathrm{S}(ut, n)$ is a pseudo-symmetric modular numerical semigroup with Frobenius number $n-t-2$. Observe that $\gcd\{ut, n\} = t \gcd\{u, \frac{n}{t}\} = t$. Moreover, $u(t+2) = q\frac{n}{t} + 1$ for some $q \in \mathbb{N}$, whence $ut - 1 + 2u = q\frac{n}{t}$. We deduce that $\gcd\{ut-1, \frac{n}{t}\} = 1$, since otherwise $\gcd\{2u, \frac{n}{t}\} \neq 1$, and as $\frac{n}{t}$ is odd, this would lead to $\gcd\{u, \frac{n}{t}\} \neq 1$, which contradicts what we have seen above. Since $\gcd\{ut-1, \frac{n}{t}\} = 1$, we have that $\gcd\{ut-1, n\} = 1$. Observe now that $ut(t+2) \bmod n = ut(t+2) \bmod t\frac{n}{t} = t(u(t+2) \bmod \frac{n}{t}) = t$ and thus $0 < ut(t+2) \bmod n < t+2$. By using Theorem 10, we conclude that $S = \mathrm{S}(ut, n)$, S is pseudo-symmetric and $\mathrm{g}(S) = n-t-2$. □

EXAMPLE 2. If we apply the preceding theorem to $n = 20$ and $t = 4$, we have that $\langle 5, 6, 13 \rangle$ is a modular pseudo-symmetric numerical semigroup with Frobenius number 14.

In [9] it is shown that every positive integer is the Frobenius number of a numerical semigroup of embedding dimension less than or equal to three. In [8] the same result is achieved for irreducible numerical semigroups, but imposing that the embedding dimension is less than or equal to four. Moreover, in this last paper it is pointed out that there exists no irreducible numerical with embedding dimension three and Frobenius number twelve. Thus one might wonder for which positive integers g there exists an irreducible numerical semigroup with Frobenius number g and embedding dimension three. The following result gives a partial answer to this problem.

COROLLARY 15. *Let* g *be a positive integer. Then there exists a pseudo-symmetric modular numerical semigroup with Frobenius number* g *if and only if there exist positive integers* k *and* k' *such that* k *is odd,* $k \geqslant 3$*,* $\gcd\{k'+2, k\} = 1$ *and* $g = kk' - k' - 2$*.*

Proof. By using Remark 1 and Theorems 10 and 14, we deduce that there exists a pseudo-symmetric modular numerical semigroup with Frobenius number g if and only if $g = n - t - 2$ with $t < n$ positive integers such that $\frac{n}{t}$ is an odd integer and $\gcd\{t+2, \frac{n}{t}\} = 1$. We conclude the proof by taking $t = k'$ and $n = kk'$.

We finish this work with an example in which we give some families of positive integers g for which there exist a pseudo-symmetric modular numerical semigroup with Frobenius number g (and thus with embedding dimension three).

EXAMPLE 3.

(1) If we apply Corollary 15 with $k = 3$, then the condition $\gcd\{k'+2, 3\} = 1$ is equivalent to $k' \not\equiv 1 \bmod 3$.

• If $k' = 3t$ with $t \in \mathbb{N} \setminus \{0\}$, then Corollary 15 states that there exist pseudo-symmetric modular numerical semigroups with Frobenius number g, for all $g \in \{4 + 6t \mid t \in \mathbb{N}\}$.

• If $k' = 2+3t$, with $t \in \mathbb{N}$, then we can say the same for all $g \in \{2+6t \mid t \in \mathbb{N}\}$.

(2) If we use Corollary 15 with $k = 5$, then • for $k' = 5t$ with $t \in \mathbb{N} \setminus \{0\}$, we obtain $g \in \{18 + 20t \mid t \in \mathbb{N}\}$,

• for $k' = 1 + 5t$ with $t \in \mathbb{N}$, we get $g \in \{2 + 20t \mid t \in \mathbb{N}\}$,

• for $k' = 2 + 5t$ with $t \in \mathbb{N}$, $g \in \{6 + 20t \mid t \in \mathbb{N}\}$,

• for $k' = 4 + 5t$ with $t \in \mathbb{N}$, we have that $g \in \{14 + 20t \mid t \in \mathbb{N}\}$.

REFERENCES

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

[2] 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).

[3] R. FRÖBERG, G. GOTTLIEB AND R. HÄGGKVIST, *On numerical semigroups*, Semigroup Forum, **35**, (1987), 63–83.

[4] J. HERZOG, *Generators and relations of abelian semigroups and semigroup rings*, Manuscripta Math., **3**, (1970), 175–193.

[5] J. C. ROSALES, M. B. BRANCO, *Irreducible numerical semigroups*, Pacific J. Math. **209**, (2003), 131–143.

[6] J. C. ROSALES, *Symmetric modular Diophantine inequalities*, to appear in Proc. Amer. Math. Soc.

[7] J. C. ROSALES, P. A. GARCÍA-SÁNCHEZ, *Finitely generated commutative monoids*, Nova Science Publishers, New York, 1999.

[8] J. C. ROSALES, P. A. GARCÍA-SÁNCHEZ, *Every positive integer is the Frobenius number of an irreducible numerical semigroup with at most four generators*, Arkiv Mat., **42**, (2004), 301–306.

[9] J. C. ROSALES, P. A. GARCÍA-SÁNCHEZ AND J. I. GARCÍA-GARCÍA, *Every positive integers is the Frobenius number of a numerical semigroup with three generators*, Math. Scandinavica., **94**, (2004), 5–12.

[10] 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.

[11] J. C. ROSALES, P. A. GARCÍA-SÁNCHEZ AND J. M. URBANO-BLANCO, *Modular Diophantine inequalities and numerical semigroups*, Pacific J. Math. **218** (2005), 379-398.

(Received April 22, 2004)

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