Semigrupos numéricos proporcionalmente modulares

Tesis Doctoral

Juan Manuel Urbano Blanco

Departamento de Álgebra
Universidad de Granada
Granada (España)

Marzo de 2005

Editor: Editorial de la Universidad de Granada
Autor: Juan Manuel Urbano Blanco
D.L.: Gr. 559 - 2005
ISBN: 84-338-3310-3

Semigrupos numéricos proporcionalmente modulares

Memoria realizada por

D. Juan Manuel Urbano Blanco

en el Departamento de Álgebra de la Universidad de Granada bajo la dirección del Profesor Dr. José Carlos Rosales González, profesor titular de dicho departamento, para obtener el grado de Doctor en Ciencias Matemáticas por la Universidad de Granada.

V.B. Director

Aspirante

Quisiera agradecer a mi director, José Carlos Rosales González así como a los restantes compañeros del Departamento de Álgebra, y en especial a los profesores Dr. Pedro A. García Sánchez y Dr. Juan I. García García, por toda la ayuda recibida, el interés que más que de sobra han mostrado en que todo salga bien y todo lo que he aprendido de ellos.

Deseo también agradecer a mi familia todo el apoyo y ayuda que he recibido en todo momento.

A mi madre, Antonia
y a mi padre, Juan Manuel

Índice general

Introducción

En esta memoria estudiamos semigrupos numéricos, es decir, subconjuntos de números naturales que son cerrados para la suma y que contienen a todos los naturales salvo posiblemente a un número finito. Es muy importante la forma cómo se describe o se representa un semigrupo numérico S, principalmente a la hora de dar respuesta a determinadas cuestiones como son el problema de pertenencia de un elemento a S, el cálculo del número de Frobenius de S, denotado como $\mathrm{g}(S)$, el cálculo del número de huecos de S, etc. Las descripciones más usuales para semigrupos numéricos son los sistemas de generadores (minimales) y las presentaciones en términos de generadores y relatores. Siempre con la idea de la representación en mente, este trabajo comenzó cuando nos encontramos con las inecuaciones de la forma $ax \bmod b \leq x$, siendo a y b números naturales con $a < b$ y x variando en los números enteros. Observamos que dichas inecuaciones definen subconjuntos de números naturales que son semigrupos numéricos, pues éstos son cerrados para la suma y además todo elemento mayor o igual que b pertenece a dichos subconjuntos. Denominamos pues a tales semigrupos numéricos simplemente semigrupos modulares y los representamos como $\mathrm{S}(a,b)$. Tras deducir algunas propiedades aritméticas básicas para $\mathrm{S}(a,b)$, obtenemos una fórmula para el número de huecos en términos de a y b. Concretamente,

$$\#\mathrm{H}(\mathrm{S}(a,b)) = \frac{b+1-(a,b)-(a-1,b)}{2},$$

donde (α,β) denota el máximo común divisor de α y β. Como consecuencia, deducimos que si $\mathrm{S}(a_1,b_1) = \mathrm{S}(a_2,b_2)$, entonces

$$b_1-(a_1,b_1)-(a_1-1,b_1) = b_2-(a_2,b_2)-(a_2-1,b_2),$$

lo que nos lleva a definir el peso de $\mathrm{S}(a,b)$ como $\mathrm{w}(\mathrm{S}(a,b)) = b-(a,b)-(a-1,b)$. Obtenemos que si S es un semigrupo modular, entonces $\mathrm{w}(S) \geq \mathrm{g}(S)$. Los casos particulares $\mathrm{w}(S) = \mathrm{g}(S)$ y $\mathrm{w}(S) = \mathrm{g}(S)+1$ curiosamente corresponden a los semigrupos modulares simétricos y pseudo-simétricos, respectivamente.

Seguidamente nos planteamos el problema de decidir cuándo un semigrupo numérico S dado mediante un sistema de generadores es o no modular. Damos un algoritmo el cual resuelve este problema de decisión. Destacamos que no es tan importante el algoritmo en sí, el cual se puede mejorar usando los resultados del capítulo séptimo, sino las propiedades previas al mismo. Aplicando este algoritmo obtenemos los primeros ejemplos de semigrupos que no son modulares.

Decimos que un semigrupo numérico es un sistema modular si éste puede ser expresado como la intersección de un número finito de semigrupos modulares. Un semigrupo numérico se denomina irreducible si no se puede representar como intersección de dos semigrupos numéricos que lo contengan de forma propia. Como existen semigrupos irreducibles que no son modulares, vemos que no todo semigrupo numérico es un sistema modular.

Por otra parte, de la definición de peso para un semigrupo modular $S = \mathrm{S}(a,b)$, es inmediato que $b \geq \mathrm{w}(S)+2$. Caracterizamos los semigrupos modulares que verifican $b = \mathrm{w}(S)+2$ en términos de los llamados UESY-semigrupos, es decir, semigrupos numéricos que se obtienen añadiendo un elemento a un semigrupo numérico simétrico. Cerramos el primer capítulo haciendo un estudio similar para el caso $b = \mathrm{w}(S)+3$, caracterizando estos semigrupos modulares en términos de los PEPSY-semigrupos los cuales son semigrupos numéricos que se obtienen añadiendo los pseudo-números de Frobenius a un semigrupo numérico pseudo-simétrico.

Para un intervalo I incluido en $\mathbb{R}_0^+$, si T es el subsemigrupo de $\mathbb{R}_0^+$ generado por I, definimos $\mathrm{S}(I) = T \cap \mathbb{N}$. En el capítulo segundo comenzamos estudiando los subsemigrupos de $\mathbb{R}_0^+$ generados por un intervalo cerrado de la forma $I = [\alpha, \beta]$, con $\alpha < \beta$. Entonces $\mathrm{S}(I)$ es un semigrupo numérico y a los semigrupos numéricos que se obtienen de esta forma los denominamos semigrupos proporcionalmente modulares. Probamos que los extremos del intervalo I pueden ser elegidos de modo que ambos sean números racionales, y cuando $S \neq \mathbb{N}$ existen enteros positivos $c < a < b$ tales que $S = \mathrm{S}([\frac{b}{a}, \frac{b}{a-c}])$. Por otra parte, definimos $\mathrm{S}(a,b,c) = \{x \in \mathbb{N} \mid ax \bmod b \leq cx\}$. Entonces probamos que $\mathrm{S}(a,b,c) = \mathrm{S}([\frac{b}{a}, \frac{b}{a-c}])$. Resulta por tanto que todo semigrupo modular es un semigrupo proporcionalmente modular, pues $\mathrm{S}(a,b) = \mathrm{S}(a,b,1)$. Además los semigrupos modulares son aquellos semigrupos proporcionalmente modulares que pueden ser definidos por un intervalo de la forma $[\frac{b}{a}, \frac{b}{a-1}]$.

Dado un semigrupo numérico S y un número entero positivo p, definimos el conjunto

$$\frac{S}{p} = \{x \in \mathbb{N} \mid px \in S\}.$$

Es fácil comprobar que S/p es de nuevo un semigrupo numérico que contiene a S. Decimos que $\frac{S}{p}$ es el cociente de S por el entero p. Esta construcción nos permite caracterizar a los semigrupos proporcionalmente modulares como aquellos que se obtienen como el cociente, por un entero positivo, de un semigrupo aritmético, es decir, un semigrupo numérico generado por un conjunto de la forma $\{n, n+1, \ldots, n+d\}$.

A continuación damos un algoritmo para decidir cuándo un semigrupo numérico S definido mediante un sistema de generadores es o no proporcionalmente modular.

Decimos que un semigrupo numérico S es un sistema proporcionalmente modular, si S se puede escribir como una intersección de semigrupos proporcionalmente modulares. Recurriendo de nuevo a los semigrupos numéricos irreducibles vemos que no todo semigrupo numérico es un sistema proporcionalmente modular. Damos un algoritmo para decidir cuándo un semigrupo numérico definido mediante un sistema de

generadores es o no un sistema proporcionalmente modular. Finalizamos este segundo capítulo estudiando una familia de semigrupos proporcionalmente modulares, la cual contiene a aquellos semigrupos numéricos generados por una progresión aritmética y en particular a los semigrupos numéricos de dos generadores.

El capítulo tercero está dedicado al estudio de los semigrupos modulares $\mathrm{S}(a,b)$ en los cuales a divide a b. Éste en realidad se puede considerar una continuación del capítulo primero. Obtenemos la multiplicidad para estos semigrupos y el conjunto de Apéry con respecto a la multiplicidad. Ello nos permite deducir fórmulas para el número de Frobenius y para el número de huecos. A continuación obtenemos el sistema minimal de generadores así como los pseudo-números de Frobenius para estos semigrupos. También caracterizamos cuándo el semigrupo $\mathrm{S}(a,b)$, con b múltiplo de a, es simétrico así como cuándo es pseudo-simétrico. Acabamos este capítulo dando varias subfamilias de semigrupos del tipo que estamos considerando y para cada una de ellas mostramos de forma explícita su sistema minimal de generadores y sus pseudo-números de Frobenius.

Una secuencia de Bézout es una secuencia creciente formada por dos o más números racionales $\frac{a_1}{b_1} < \frac{a_2}{b_2} < \cdots < \frac{a_p}{b_p}$ tal que $a_1,\ldots,a_p,b_1,\ldots,b_p$ son números enteros positivos y $b_i a_{i+1} - b_{i+1}a_i = 1$ para todo $i \in \{1,\ldots,p-1\}$. Este concepto ha resultado ser fundamental para el estudio de los semigrupos proporcionalmente modulares. La mayor parte del capítulo cuarto está dedicada al estudio de las secuencias de Bézout y a su relación con los semigrupos proporcionalmente modulares. Comenzamos probando que dos fracciones positivas dadas siempre se pueden "conectar"mediante una secuencia de Bézout. A continuación asociamos a cada secuencia de Bézout un semigrupo proporcionalmente modular. Exactamente le asociamos el semigrupo S definido por el intervalo cerrado dado por los extremos de dicha secuencia. Probamos que si $\frac{a_1}{b_1} < \frac{a_2}{b_2} < \cdots < \frac{a_p}{b_p}$ es una secuencia de Bézout, entonces

$$\langle a_1,\ldots,a_p\rangle = \mathrm{S}\Big(\Big[\frac{a_1}{b_1},\frac{a_p}{b_p}\Big]\Big),$$

es decir, los numeradores que aparecen en la secuencia de Bézout constituyen un sistema de generadores para el semigrupo correspondiente. Como consecuencia, este resultado nos proporciona un método para resolver inecuaciones diofánticas del tipo $ax \bmod b \leq cx$, con a, b y c números enteros positivos.

A continuación estudiamos condiciones que al imponerlas a una secuencia de Bézout garanticen que los numeradores de la misma formen un sistema minimal de generadores para el semigrupo asociado a dicha secuencia. Decimos que una secuencia de Bézout $\frac{a_1}{b_1} < \frac{a_2}{b_2} < \cdots < \frac{a_p}{b_p}$ es propia, si $a_{i+h}b_i - a_i b_{i+h} \geq 2$ para todo $h \geq 2$ tal que $i, i+h \in \{1,\ldots,p\}$. Dos fracciones $0 < \frac{a_1}{b_1} < \frac{a_2}{b_2}$ decimos que son adyacentes, si

$$\frac{a_2}{b_2+1} < \frac{a_1}{b_1}, \text{ y si } b_1 \neq 1, \text{ entonces } \frac{a_2}{b_2} < \frac{a_1}{b_1-1}.$$

Con estos elementos demostramos que los numeradores de una secuencia de Bézout constituyen el sistema minimal de generadores para el semigrupo proporcionalmente modular asociado si y sólo si dicha secuencia de Bézout es propia y tiene como extremos dos fracciones adyacentes.

Seguidamente caracterizamos los semigrupos proporcionalmente modulares en términos de los generadores minimales del semigupo. Concretamente probamos que un semigrupo numérico S minimalmente generado por el conjunto $\{n_1,\ldots,n_p\}$ es proporcionalmente modular si y sólo si existe una ordenación, digamos $n_1,\ldots,n_p$, para sus generadores minimales de modo que

1. $(n_i,n_{i+1})=1$ para todo $i\in\{1,\ldots,p-1\}$,
2. $n_{i-1}+n_{i+1}\equiv 0 \bmod n_i$ para todo $i\in\{2,\ldots,p-1\}$.

Como aplicación estudiamos los semigrupos proporcionalmente modulares con tres generadores, deduciendo expresiones para el número de Frobenius y para el número de huecos en términos de dichos generadores.

En el capítulo quinto damos una nueva caracterización para los semigrupos proporcionalmente modulares como cocientes por un número natural de semigrupos numéricos de dos generadores. Ello nos permite relacionar los semigrupos proporcionalmente modulares con los semigrupos afines completos contenidos en $\mathbb{N}^2$. Concretamente, para a_1,a_2 y a_3 enteros positivos, defininos el semigrupo afín completo

$$\mathrm{A}(a_1,a_2,a_3)=\{(x_1,x_2)\in\mathbb{N}^2 \mid a_1x_1+a_2x_2\equiv 0 \bmod a_3\}.$$

Entonces, si n_1,n_2 y d son enteros positivos tales que n_1 y n_2 son primos relativos, probamos que

$$\frac{\langle n_1,n_2\rangle}{d}=\left\{\frac{n_1x_1+n_2x_2}{d} \mid (x_1,x_2)\in \mathrm{A}(n_1,n_2,d)\right\}.$$

Por consiguiente, resulta interesante conocer cómo son los sistemas de generadores para los semigrupos afines $\mathrm{A}(n_1,n_2,d)$. En este capítulo obtenemos una descripción detallada de los sistemas minimales de generadores para dichos semigrupos.

En el capítulo sexto vemos que los intervalos I no necesariamente cerrados de números reales positivos también definen semigrupos $\mathrm{S}(I)$ proporcionalmente modulares. Nos centramos en el estudio de los semigrupos proporcionalmente modulares de la forma $\mathrm{S}(]\frac{b}{a},\frac{b}{a-1}[)$ determinando su número de Frobenius y su número de huecos. Ésto nos permite estudiar los semigrupos proporcionalmente modulares irreducibles. En concreto vemos que un semigrupo S proporcionalmente modular es simétrico si y sólo si $S=\mathbb{N}$, $S=\langle 2,3\rangle$ ó $S=\mathrm{S}(]\frac{b}{a},\frac{b}{a-1}[)$ para ciertos números enteros a y b verificando que $2\leq a<b$ y $\mathrm{mcd}\{a,b\}=\mathrm{mcd}\{a-1,b\}=1$. De manera similar, S es pseudo-simétrico si y sólo si $S=\langle 3,4,5\rangle$ ó $S=\mathrm{S}(]\frac{b}{a},\frac{b}{a-1}[)$ para ciertos números enteros a y b verificando que $2\leq a<b$ y $\{\ \mathrm{mcd}\ \{a,b\},\mathrm{mcd}\{a-1,b\}\}=\{1,2\}$.

Al programar el algoritmo del capítulo primero ya mencionado para decidir cuándo un semigrupo numérico es modular, lo hicimos de forma que en caso de que la respuesta fuese afirmativa, se obtuviesen todas las representaciones modulares para el

semigrupo dado. Cuando aplicábamos dicho algoritmo a un semigrupo distinto de $\mathbb{N}$, observábamos que siempre devolvía a lo sumo seis representaciones modulares, alcanzándose dicho máximo sólo para semigrupos numéricos de dos generadores. Estos resultados motivaron nuestro estudio de las representaciones modulares $\mathrm{S}(a,b)$ el cual se recoge en el capítulo séptimo, en el que además se pone de manifiesto que existe una relación muy estrecha entre las representaciones modulares para un semigrupo modular S y las secuencias de Bézout cuyos numeradores son los generadores minimales de S. Probamos que cuando S es un semigrupo numérico de dimensión de inmersión igual a dos, éste puede tener sólo cinco o seis representaciones modulares. Además, damos dichas representaciones modulares de forma explícita. Seguidamente demostramos que un semigrupo modular con dimensión de inmersión mayor o igual que tres, puede tener a lo sumo cuatro representaciones modulares. Finalmente damos un nuevo algoritmo el cual nos permite obtener fácilmente todas las representaciones modulares para cualquier semigrupo numérico S distinto de $\mathbb{N}$.

Conocemos por el capítulo segundo que todo semigrupo numérico generado por una progresión aritmética, digamos $S = \langle m, m+c, m+2c, \ldots, m+kc \rangle$, es siempre proporcionalmente modular. Sin embargo, al aplicar el algoritmo dado en el capítulo primero a varios ejemplos, observamos que no todo semigrupo numérico generado por una progresión aritmética es modular. En el capítulo octavo probamos que S es modular si y sólo si $(m \bmod k) \in \{0,1\}$, obteniendo además las expresiones para las correspondientes representaciones modulares.

Terminamos esta memoria con un último capítulo en el que planteamos algunos problemas abiertos.

Preliminares

Un **semigrupo numérico** es un subconjunto S del conjunto de los números naturales $\mathbb{N}$, que es cerrado para la suma, contiene al cero y verifica que $\mathbb{N} \setminus S$ es finito.

Sea S un semigrupo numérico. Un **sistema de generadores** para S es un conjunto finito $\{n_0, n_1, \ldots, n_p\}$ de números naturales tales que para todo $x \in S$, existen naturales $\lambda_0, \lambda_1, \ldots, \lambda_p$ verificando que $x = \lambda_0 n_0 + \lambda_1 n_1 + \cdots + \lambda_p n_p$. Claramente, el máximo común divisor de $n_0, n_1, \ldots, n_p$ ha de ser igual a 1, por lo que a veces un semigrupo numérico se define también como un subconjunto S de $\mathbb{N}$ que es cerrado para la suma, contiene al cero y el máximo común divisor de todos sus elementos es igual a 1.

Para denotar que $A = \{n_0, n_1, \ldots, n_p\}$ es un conjunto de generadores para S, se escribe $S = \langle A \rangle$, o bien, $S = \langle n_0, n_1, \ldots, n_p \rangle$. Con la misma notación anterior, decimos que la igualdad $x = \lambda_0 n_0 + \lambda_1 n_1 + \cdots + \lambda_p n_p$ es una **expresión** o una **representación** para x. Además x es de **expresión única** si no existe $(\lambda'_0, \ldots, \lambda'_p) \in \mathbb{N}^{p+1}$ tal que $x = \lambda'_0 n_0 + \cdots + \lambda'_p n_p$ y $(\lambda_0, \ldots, \lambda_p) \neq (\lambda'_0, \ldots, \lambda'_p)$.

Un **sistema de generadores** $\{n_0, n_1, \ldots, n_p\}$ para S se dice **minimal** si para cualquier i tal que $0 \leq i \leq p$, no existen números naturales $\lambda_0, \ldots, \lambda_{i-1}, \lambda_{i+1}, \ldots, \lambda_p$ verificando que $n_i = \lambda_0 n_0 + \cdots + \lambda_{i-1} n_{i-1} + \lambda_{i+1} n_{i+1} + \cdots + \lambda_p n_p$, es decir, cuando ningún subconjunto propio suyo genera a S.

Es un hecho bien conocido que todo semigrupo numérico admite un único sistema minimal de generadores (véase [**36**]) cuyo cardinal se denomina la **dimensión de inmersión** de S y se denota por $\mathrm{e}(S)$.

Decimos que un conjunto finito B de números naturales es **independiente** cuando ninguno de sus elementos tiene una representación en términos de los elementos restantes de B. Es evidente que si B es el sistema minimal de generadores de un semigrupo numérico S, entonces B es un conjunto independiente.

Sea S un semigrupo numérico minimalmente generado por $n_0 < n_1 < \cdots < n_p$. Decimos que n_0 es la **multiplicidad** de S y la denotamos como $\mathrm{m}(S)$.

Un semigrupo numérico S es un **MED-semigrupo** si $\mathrm{e}(S) = \mathrm{m}(S)$, es decir, cuando S tiene la máxima dimensión de inmersión que puede tener un semigrupo con multiplicidad $\mathrm{m}(S)$. Un **semigrupo aritmético** es un semigrupo numérico generado por un conjunto de números naturales de la forma $\{n, n+1, \ldots, n+d\}$.

El conjunto $\mathbb{N} \setminus S$, que claramente determina al semigrupo S, será denotado por $\mathrm{H}(S)$ y sus elementos se denominan los **huecos** de S.

Tal y como se pone de manifiesto en varios trabajos entre los que citamos [**8**], [**16**], [**20**], [**22**], los semigrupos numéricos son de interés en el campo de la Geometría Algebraica. Como consecuencia, gran parte de la terminología empleada para los semigrupos numéricos ha sido heredada de la Geometría Algebraica.

El cardinal de $\mathrm{H}(S)$ se llama el **género** o **grado de singularidad** de S (véase [**2, 19**]). El **número de Frobenius** de S es el mayor entero no perteneciente a S, y se denota por $\mathrm{g}(S)$. Observar que $\mathrm{g}(\mathbb{N}) = -1$. Fué demostrado por J. J. Sylvester en 1884 (véase [**48**]) que si n_1 y n_2 son dos enteros positivos los cuales son además primos relativos, entonces $\mathrm{g}(\langle n_1, n_2\rangle) = n_1 n_2 - n_1 - n_2$. En algunas ocasiones nos referiremos a esta fórmula como la fórmula de **Sylvester** para el número de Frobenius. Sigue siendo un problema abierto el encontrar una fórmula para $\mathrm{g}(S)$ para tres o más generadores minimales (véase [**23**], [**24**]).

Para un conjunto finito A, denotamos por $\#A$ el número de elementos en A. Además, si $a_1 < a_2 < \ldots < a_n$ son números enteros, definimos

$$\{a_1, a_2, \ldots, a_n, \rightarrow\} = \{a_1, a_2, \ldots, a_n\} \cup \{x \in \mathbb{Z} \mid x > a_n\}.$$

Diremos que un semigrupo numérico S es una **semirecta**, si existe $m \in \mathbb{N}$ tal que $S = \{0, m, \rightarrow\}$.

El **conductor** de S, denotado por $\mathrm{c}(S)$ es $\mathrm{g}(S)+1$, es decir, $\mathrm{c}(S)$ es el menor número natural tal que $\{\mathrm{c}(S), \rightarrow\} \subseteq S$.

Dado un semigrupo numérico S, definimos

$$\mathrm{Pg}(S) = \{x \in \mathbb{Z} \setminus S \mid x + s \in S \text{ para todo } s \in S \setminus \{0\}\}.$$

Cada elemento de $\mathrm{Pg}(S)$ es un **pseudo-número de Frobenius** de S (véase [**34**]). El cardinal del conjunto $\mathrm{Pg}(S)$ se denomina el **tipo** de S y se representa por $\mathrm{t}(S)$ (véase [**2, 11**]).

Para cualquier semigrupo numérico S y cualquier subconjunto no vacío de números enteros A, siempre podemos definir la siguiente relación de orden sobre A:

$$a_1 \leq_S a_2 \quad \text{si y sólo si} \quad a_2 - a_1 \in S.$$

Claramente los elementos minimales de $S \setminus \{0\}$ con respecto de la relación $\leq_S$ constituyen el sistema minimal de generadores de S. Además, si representamos el conjunto de los elementos maximales de A con respecto de la relación de orden $\leq_S$ por $\mathrm{Max}_{\leq_S} A$, entonces $\mathrm{Max}_{\leq_S}\mathrm{H}(S) = \mathrm{Pg}(S)$ siempre que $S \neq \mathbb{N}$.

Para un semigrupo numérico S y un elemento $n \in \mathrm{S} \setminus \{0\}$, el **conjunto de Apéry** de n en S (véase [**1**]) es

$$\mathrm{Ap}(S, n) = \{s \in S \mid s - n \notin S\}.$$

Obsérvese que $\mathrm{Ap}(S, n)$ puede ser descrito como el conjunto $\{w(0) = 0, w(1), \ldots, w(n-1)\}$, siendo $w(i)$ el menor elemento en S que es congruente con i módulo n. Claramente $\mathrm{Ap}(S, n) \cup \{n\}$ es un sistema de generadores para S y además se verifica que $x \in \mathbb{Z}$ es un elemento de S si y sólo si $x \geq w(x \bmod n)$, donde $x \bmod n$ como es usual denota el resto de la división de x entre n. A veces los elementos de $\mathrm{Ap}(S, n)$ también se denominan **los restos primarios** de S respecto del elemento

n. Si $S \neq \{0\}$ y $\{n_0, n_1, \ldots, n_p\}$ es el sistema minimal de generadores de S, cualquier elemento $x \in S$ puede ser expresado de manera única como $x = k_0 n_0 + \cdots + k_p n_p$ con $k_{i+1} n_{i+1} + \cdots + k_p n_p \in \bigcap_{j=0}^{i} \mathrm{Ap}(S, n_j)$ para todo $i \in \{0, \ldots, p-1\}$. La expresión $x = k_0 n_0 + \cdots + k_p n_p$ se denomina la **representación primaria** para x con respeco a la ordenación $n_0, n_1, \ldots, n_p$ de los generadores (véase [**36**]).

En el siguiente resultado se recogen dos hechos bien conocidos los cuales pueden ser encontrados en [**46**].

LEMA 0.1. *Sea S un semigrupo numérico, sea $m \in S \setminus \{0\}$ y $\mathrm{Ap}(S,m) = \{0, w(1), \ldots, w(m-1)\}$. Entonces*

$$\mathrm{g}(S) = \max(\mathrm{Ap}(S,n)) - n \quad y \quad \#\mathrm{H}(S) = \frac{1}{m}(w(1) + \cdots + w(m-1)) - \frac{m-1}{2}.$$

Sean $n_1 < n_2$ dos enteros positivos primos relativos y llamemos $S = \langle n_1, n_2 \rangle$. Entonces es inmediato probar que $\mathrm{Ap}(S, n_1) = \{0, n_2, 2n_2, \ldots, (n_1 - 1)n_2\}$. Como consecuencia, se obtiene el siguiente resultado el cual es bien conocido (véase [**47**]).

LEMA 0.2. *Sean n_1 y n_2 enteros positivos primos relativos y sea $S = \langle n_1, n_2 \rangle$. Entonces*

$$\#\mathrm{H}(S) = \frac{1}{2}(n_1 - 1)(n_2 - 1).$$

Es un problema abierto el encontrar una fórmula general para $\#\mathrm{H}(S)$ (véase [**24**]).

Además existe una relación entre conjuntos de Apéry y pseudo-números de Frobenius para semigrupos numéricos como indica el siguiente resultado (véase [**34**]).

LEMA 0.3. *Sea S un semigrupo numérico con multiplicidad m. Si*

$$\mathrm{Max}_{\leq_S}(\mathrm{Ap}(S,m)) = \{w_{i_1}, \ldots, w_{i_t}\},$$

entonces

$$\mathrm{Pg}(S) = \{w_{i_1} - m, \ldots, w_{i_t} - m\}.$$

Un semigrupo numérico se denomina **irreducible** si no puede escribirse como la intersección de dos semigrupos numéricos que lo contienen propiamente. El siguiente resultado aparece en [**35**].

LEMA 0.4. *Para un semigrupo numerico S, las siguientes condiciones son equivalentes:*

1. *S es irreducible,*
2. *S es maximal en el conjunto de todos los semigrupos numericos con número de Frobenius $\mathrm{g}(S)$,*
3. *S es maximal en el conjunto de todos los semigrupos numericos que no contienen a $\mathrm{g}(S)$.*

Un semigrupo numérico se dice que es **simétrico** si para cualquier $x \in \mathbb{Z} \setminus S$ se verifica que $\mathrm{g}(S) - x \in S$. Es inmediato que el número de Frobenius de cualquier semigrupo

numérico simétrico ha de ser un número impar. Además es un hecho bien conocido que todo semigrupo numérico generado por dos elementos es simétrico (véase [**2**]).

Un semigrupo numérico se dice que es **pseudo-simétrico** si $\mathrm{g}(S)$ es par y para cualquier $x \in \mathbb{Z} \setminus S$ se verifica que $x = \mathrm{g}(S)/2$ ó $\mathrm{g}(S) - x \in S$

En [**34**] se demuestra que un semigrupo numérico S es irreducible si y sólo si S es simétrico o pseudo-simétrico, según la paridad de $\mathrm{g}(S)$.

Existen varias caracterizaciones en la literatura para los semigrupos simétricos así como para los semigrupos pseudo-simétricos. Nosotros emplearemos principalmente las siguientes (véase [**2, 11**]).

LEMA 0.5. *Un semigrupo numérico S es simétrico si y sólo si* $\mathrm{g}(S)$ *es impar y* $\#\mathrm{H}(S) = \frac{1}{2}(\mathrm{g}(S)+1)$.

LEMA 0.6. *Un semigrupo numérico S es pseudo-simétrico si y sólo si* $\mathrm{g}(S)$ *es par y* $\#\mathrm{H}(S) = \frac{1}{2}(\mathrm{g}(S)+2)$.

Además, para un semigrupo numérico S, es conocido que S es pseudo-simétrico si y sólo si $\mathrm{Pg}(S) = \{\frac{1}{2}\mathrm{g}(S), \mathrm{g}(S)\}$, y que S es simétrico si y sólo si $\mathrm{Pg}(S) = \{\mathrm{g}(S)\}$ (véase [**2, 11**]).

CAPÍTULO 1

Semigrupos modulares

En este capítulo introducimos el concepto de semigrupo modular, el cual será generalizado en el capítulo siguiente. En la Sección 1 recogemos las propiedades aritméticas básicas para los semigrupos modulares. Además para dichos semigrupos definimos un invariante al que llamamos peso y estudiamos su relación con el número de Frobenius. En la Sección 2, basándonos en los resultados anteriores, obtenemos un algorítmo para decidir cuándo un semigrupo numérico dado es o no modular. En la sección siguiente estudiamos los semigrupos modulares cuyo módulo es igual a su peso más dos. Caracterizamos esta clase de semigrupos modulares en términos de los UESY-semigrupos así como en términos de los semigrupos numéricos simétricos. En la última sección hacemos un estudio similar para los semigrupos modulares cuyo módulo es igual a su peso más tres, y caracterizamos dicha clase de semigrupos modulares en términos de los PEPSY-semigrupos así como en términos de los semigrupos numéricos pseudo-simétricos. Los resultados de este capítulo pueden ser encontrados en [**41**].

1. Propiedades básicas

Una **inecuación diofántica modular** es una expresión de la forma $ax \bmod b \leq x$, siendo a y b números enteros, con $b \neq 0$.

PROPOSICIÓN 1.1. *El conjunto de soluciones enteras de una inecuación diofántica modular es un semigrupo numérico.*

DEMOSTRACIÓN. Sean a y b dos enteros, con $b \neq 0$, y sea $S = \{x \in \mathbb{N} \mid ax \bmod b \leq x\}$. Claramente $0 \in S$, y si x es un entero mayor o igual que b, entonces $x \in S$. Por tanto $\mathbb{N} \setminus S$ es un conjunto finito. Dados $x, y \in S$, se verifica que $a(x+y) \bmod b \leq ax \bmod b + ay \bmod b \leq x+y$, lo que significa que $x+y \in S$, y por tanto S también es cerrado para la suma. □

Denotamos el semigrupo numérico $\{x \in \mathbb{N} \mid ax \bmod b \leq x\}$ por $\mathrm{S}(a,b)$ y denominamos a a y a b el **factor** y el **módulo**, respectivamente. Un **semigrupo modular** es un semigrupo numérico S para el cual existen dos números enteros a y b, con $b \neq 0$, tales que $S = \mathrm{S}(a,b)$. En tal caso decimos que $\mathrm{S}(a,b)$ es una **representación modular** para S. La inecuación $ax \bmod b \leq x$ tiene las mismas soluciones que $(a \bmod b)x \bmod b \leq x$. Además, si $a \in \{0,1\}$, entonces $\mathrm{S}(a,b) = \mathbb{N}$ para cualquier módulo $b \neq 0$. En consecuencia podemos suponer que $2 \leq a < b$.

El siguiente ejemplo pone de manifiesto que un semigrupo modular puede tener varias representaciones modulares.

EJEMPLO 1.2. $\{0,2,3,\rightarrow\} = \mathrm{S}(2,3) = \mathrm{S}(2,4)$. □

LEMA 1.3. *Sean a y b dos enteros tales que $0 \leq a < b$. Entonces $ax \bmod b \leq x$ si y sólo si $(b+1-a)x \bmod b \leq x$, es decir,* $\mathrm{S}(a,b) = \mathrm{S}(b+1-a,b)$.

DEMOSTRACIÓN. Si $ax \bmod b \leq x$, entonces existen $q,r \in \mathbb{N}$ tales que $ax = qb+r$ con $0 \leq r \leq x$. Tenemos entonces que $(b+1-a)x = (b+1)x - ax = bx - qb + x - r$ y como consecuencia $(b+1-a)x \bmod b \leq x-r \leq x$. Para probar la otra implicación es suficiente observar que $(b+1-(b+1-a)) = a$. □

LEMA 1.4. *Sea S un semigrupo modular con módulo $b \geq 2$. Entonces existe un entero positivo a tal que $a \leq \frac{1}{2}(b+1)$ y $S = \mathrm{S}(a,b)$.*

DEMOSTRACIÓN. Por hipótesis existen enteros positivos $a < b$ tales que $S = \mathrm{S}(a,b)$. Además según el Lema 1.3 también tenemos que $S = \mathrm{S}(b+1-a,b)$. Para concluir la demostración basta observar que a o bien $b+1-a$ es siempre menor o igual que $\frac{1}{2}(b+1)$. □

El siguiente resultado se demuestra fácilmente.

LEMA 1.5. *Sean a y b dos números enteros tales que $0 \leq a < b$ y sea $x \in \mathbb{N}$. Entonces*

$$a(b-x) \bmod b = \begin{cases} 0 & \text{si } ax \bmod b = 0, \\ b - (ax \bmod b) & \text{si } ax \bmod b \neq 0. \end{cases}$$

Además, si $ax \bmod b > x$, entonces $a(b-x) \bmod b < b-x$.

Como consecuencia inmediata de este resultado, obtenemos la siguiente propiedad que será utilizada muy a menudo en este capítulo.

COROLARIO 1.6. *Si S es un semigrupo modular con módulo b y $x \in \mathbb{N} \setminus S$, entonces $b-x \in S$.*

COMENTARIO 1.7. Supongamos que $S = \mathrm{S}(a,b)$ para ciertos enteros positivos a y b. Si $S \neq \mathbb{N}$, entonces $b-1$ no puede pertenecer a $\mathrm{H}(S)$, pues de lo contrario aplicando el Corolario 1.6 tendríamos que $b-(b-1) = 1$ pertenecería a S. Aparte, como ya hemos observado más arriba, para todo $x \in \mathbb{N}$ tal que $x \geq b$, se verifica que $x \in S$. Obtenemos pues que si S es un semigrupo modular tal que $S \neq \mathbb{N}$, entonces $\mathrm{g}(S) \leq b-2$. □

Vamos a caracterizar ahora el caso en el cual $\mathrm{g}(S) = b-2$.

LEMA 1.8. *Sea S un semigrupo numérico distinto de $\mathbb{N}$. Entonces S es un semigrupo modular con módulo b y $\mathrm{g}(S) = b-2$ si y sólo si b es impar y $S = \langle 2,b \rangle$.*

DEMOSTRACIÓN. Supongamos que $S = \mathrm{S}(a,b)$ siendo a y b enteros positivos tales que $1 < a < b$. Si $\mathrm{g}(S) = b-2$, entonces $b-2 \notin S$, y aplicando el Corolario 1.6 resulta que $b-(b-2) = 2 \in S$. Por consiguiente b ha de ser impar y $S = \langle 2,b \rangle$.

Recíprocamente, si b es impar y $S = \langle 2, b\rangle$, entonces claramente $g(S) = b-2$. Además, si $2 \in S$, entonces se verifica que $2a \bmod b \leq 2$ y ésto implica que $2a > b$, es decir, $a > b/2$. Además por el Lema 1.4 podemos elegir a de modo que sea menor o igual que $\frac{1}{2}(b+1)$. Ambas condiciones implican que $a = \frac{1}{2}(b+1)$. Así pues, $S = S(\frac{1}{2}(b+1), b)$, lo que prueba que S es modular. □

Para un número real x, representamos por $\lceil x \rceil$ el mínimo del conjunto $\{z \in \mathbb{Z} \mid z \geq x\}$, y por $\lfloor x \rfloor$ el máximo del conjunto $\{z \in \mathbb{Z} \mid z \leq x\}$.

EJEMPLO 1.9. Veamos que para cualquier entero positivo b se verifica $S(2,b) = \{0, \lfloor \frac{b+1}{2} \rfloor, \rightarrow\}$.

Llamemos $S = \{0, \lfloor \frac{b+1}{2} \rfloor, \rightarrow\}$. Claramente $\{b, \rightarrow\} \subseteq S \cap S(a,b)$. Sea $0 < x < b$. Tenemos que $2x < b$ si y sólo si $2x \bmod b = 2x$, lo que significa que $x \notin S$. Además $b \leq 2x$ si y sólo si $2x \bmod b = 2x - b \leq x$, es decir, $x \in S$. □

LEMA 1.10. *Sean a y b números enteros tales que $0 \leq a < b$, $S = S(a,b)$ y sea x un número entero verificando que $0 \leq x \leq b-1$. Entonces $x \in S$ y $b - x \in S$ si y sólo si $ax \bmod b \in \{0, x\}$.*

DEMOSTRACIÓN.

Condición necesaria. Sea $x \in S$ y supongamos que $ax \bmod b \neq 0$. Entonces $ax \bmod b \leq x$. Si $ax \bmod b < x$, entonces por el Lema 1.5, deducimos que $a(b-x) \bmod b = b - (ax \bmod b) > b - x$. Por tanto $b - x \notin S$, lo cual contradice la hipótesis. Concluimos pues que $ax \bmod b = x$.

Condición suficiente. Si $ax \bmod b = 0$, entonces está claro que $x \in S$. Además, por el Lema 1.5, obtenemos que $a(b-x) \bmod b = 0$ con lo cual $b - x$ es un elemento de S.

Si $ax \bmod b = x \neq 0$, de nuevo $x \in S$, y de nuevo por el Lema 1.5 obtenemos $a(b - x) \bmod b = b - (ax \bmod b) = b - x$, lo que implica que $b - x \in S$. □

Si x e y son dos números enteros, con al menos uno de ellos distinto de cero, denotamos por (x,y), así como por $\text{mcd}\{x,y\}$, el máximo común divisor de a y de b. El siguiente lema es fácil de demostrar.

LEMA 1.11. *Sean a y b dos enteros positivos y sea x un entero tal que $0 \leq x \leq b-1$. Entonces*

1. *$ax \mod b = 0$ si y sólo si x es un múltiplo de $b/(a,b)$,*
2. *$ax \mod b = x$ si y sólo si x es un múltiplo de $b/(b, a-1)$.*

LEMA 1.12. *Sea $S = S(a,b)$ para ciertos enteros $0 < a < b$. Sean $d = (b,a)$, $d' = (b, a-1)$, y x un entero tal que $0 \leq x \leq b-1$. Entonces $x \in S$ y $b - x \in S$ si y sólo si*

$$x \in X = \left\{0, \frac{b}{d'}, 2\frac{b}{d'}, \ldots (d'-1)\frac{b}{d'}, \frac{b}{d}, 2\frac{b}{d}, \ldots, (d-1)\frac{b}{d}\right\}.$$

Además, el cardinal de X es $d + d' - 1$.

DEMOSTRACIÓN. Por el Lema 1.10 ya sabemos que $x \in S$ y que $b-x \in S$ si y sólo si $ax \bmod b \in \{0,x\}$. Utilizando ahora el Lema 1.11, ésto último equivale a que $x \in X$.

Observar que $(a-1,a)=1$ y por tanto $(d,d')=1$. Si $sb/d' = tb/d$ para ciertos números $s,t \in \mathbb{N}$, entonces $sd = td'$ y ya que $(d,d')=1$, deducimos que existe $k \in \mathbb{N}$ tal que $sd = td' = kdd'$. Por tanto $s = kd'$ y $t = kd$. Como consecuencia, la cardinalidad de X es igual a $d+d'-1$. □

Recordemos que si S es un semigrupo numérico, entonces $\mathrm{H}(S) = \mathbb{N} \setminus S$ es el conjunto de los huecos de S.

TEOREMA 1.13. *Sea $S = \mathrm{S}(a,b)$ para ciertos enteros a y b tales que $0 \leq a < b$. Entonces*

$$\#\mathrm{H}(S) = \frac{b+1-(a,b)-(a-1,b)}{2}.$$

DEMOSTRACIÓN. Sean d, d' y X como en el Lema 1.12. Utilizando el Corolario 1.6 y el Lema 1.12, si llamamos $Y = \{0,\ldots,b-1\} \setminus X$, deducimos que $\#(Y \cap S) = \#(Y \setminus S)$, con lo cual $\#Y = 2 \cdot \#\mathrm{H}(S)$. Empleando de nuevo el Lema 1.12, obtenemos que $2 \cdot \#\mathrm{H}(S) = b-(d+d'-1)$ y por tanto la fórmula propuesta. □

COMENTARIO 1.14. Por la demostración del teorema anterior podemos afirmar que para $S = \mathrm{S}(a,b)$, la aplicación de $\{x \in S | b-x \notin S\}$ en $\mathrm{H}(S)$ definida por $x \mapsto b-x$, es biyectiva. □

EJEMPLO 1.15.

Si p es un número primo impar, entonces $\#\mathrm{H}(\mathrm{S}(a,p)) = \frac{1}{2}(p+1-1-1) = \frac{1}{2}(p-1)$ para todo a tal que $1 < a < p$. □

Como una consecuencia inmediata del Teorema 1.13, deducimos el siguiente resultado.

COROLARIO 1.16. *Sean a_1,a_2,b_1 y b_2 enteros positivos tales que $\mathrm{S}(a_1,b_1) = \mathrm{S}(a_2,b_2)$. Entonces*

$$b_1-(a_1,b_1)-(a_1-1,b_1) = b_2-(a_2,b_2)-(a_2-1,b_2).$$

EJEMPLO 1.17. El recíproco del Corolario 1.16 es falso. Basta considerar $\langle 4,5,6\rangle = \mathrm{S}(3,12) \neq \mathrm{S}(2,10) = \langle 5,6,7,8,9\rangle$. □

Si $S = \mathrm{S}(a,b)$ para ciertos enteros $0 \leq a < b$, definimos el **peso** de S como $\mathrm{w}(S) = b-(a,b)-(a-1,b)$. Según el Corolario 1.16, $\mathrm{w}(S)$ es un invariante de S, pues dicho valor no depende de la elección de a y de b. Observar también que $\mathrm{w}(\mathbb{N}) = -1$. Si $S \neq \mathbb{N}$, entonces podemos elegir a y b de manera que $2 \leq a < b$. Ésto implica que $(a,b)+(a-1,b) \leq b/2+b/3 < b$, y por tanto que $\mathrm{w}(S) \geq 1$. Observamos pues que de manera similar a como ocurre para el número de Frobenius de un semigrupo numérico, el peso de un semigrupo modular es siempre mayor o igual que 1, excepto para el caso $S = \mathbb{N}$ en el cual $\mathrm{w}(S) = \mathrm{g}(S) = -1$.

Es un hecho bien conocido que para cualquier semigrupo numérico S se verifica que $\#\mathrm{H}(S) \geq \frac{1}{2}(\mathrm{g}(S)+1)$ (véase por ejemplo [**11**]).

COROLARIO 1.18. *Si S es un semigrupo modular, entonces* $\mathrm{w}(S)$ *es impar y* $\mathrm{w}(S) \geq \mathrm{g}(S)$.

DEMOSTRACIÓN. Por el Teorema 1.13 deducimos que $\mathrm{w}(S) = 2 \cdot \#\mathrm{H}(S) - 1$, por lo que $\mathrm{w}(S)$ es impar y además $\mathrm{w}(S) \geq 2(\frac{1}{2}(\mathrm{g}(S)+1)) - 1 = \mathrm{g}(S)$. □

En vista del Corolario 1.18, aquellos semigrupos modulares S con $\mathrm{w}(S) = \mathrm{g}(S)$ y $\mathrm{g}(S)$ impar, o bien $\mathrm{w}(S) = \mathrm{g}(S)+1$ y $\mathrm{g}(S)$ par, son los semigrupos numéricos modulares para los cuales el peso toma su valor más pequeño posible con respecto a su número de Frobenius. El siguiente resultado caracteriza este tipo de semigrupos. Pero antes, recordemos que un semigrupo numérico es irreducible si éste no puede ser expresado como la intersección de dos semigrupos numéricos que lo contienen propiamente. Además en [**35**] se prueba que S es irreducible si y sólo si S es simétrico ó pseudo-simétrico, según la paridad de $\mathrm{g}(S)$.

COROLARIO 1.19. *Sea S un semigrupo modular. Entonces*

1. *S es simétrico si y sólo si* $\mathrm{w}(S) = \mathrm{g}(S)$,
2. *S es pseudo-simétrico si y sólo si* $\mathrm{w}(S) = \mathrm{g}(S)+1$.

DEMOSTRACIÓN.

1. S es simétrico si y sólo si $\#\mathrm{H}(S) = \frac{1}{2}(\mathrm{g}(S)+1)$. Por el Teorema 1.13 sabemos que $\#\mathrm{H}(S) = \frac{1}{2}(\mathrm{w}(S)+1)$, por lo cual S es simétrico si y sólo si $\mathrm{g}(S) = \mathrm{w}(S)$.
2. Es similar al caso anterior, usando ahora que S es pseudo-simétrico si y sólo si $\#\mathrm{H}(S) = \frac{1}{2}(\mathrm{g}(S)+2)$.

□

EJEMPLO 1.20. Para cualquier entero positivo impar b, siempre existe un semigrupo modular S para el cual $\mathrm{w}(S) = b$. Es suficiente considerar $S = \mathrm{S}(2, b+2)$, pues $\mathrm{w}(\mathrm{S}(2,b+2)) = b+2-(2,b+2)-(1,b+2) = b+2-1-1 = b$. □

2. Un algorítmo para determinar si un semigrupo numérico es o no modular

Tal y como indica el título, en esta sección damos un algorítmo para decidir si un semigrupo numérico S es modular, y en caso afirmativo encontramos una representación modular para S.

Comenzamos con un primer resultado que es consecuencia del Teorema 1.13 y que limita superiormente los posibles módulos que pueden aparecer en una representación modular para S. En particular nos dice que el número de representaciones modulares para un semigrupo modular es siempre finito.

LEMA 1.21. *Sea $S \neq \mathbb{N}$ un semigrupo modular con módulo b. Entonces*

$$b \leq 12 \cdot \#\mathrm{H}(S) - 6.$$

DEMOSTRACIÓN. Sean a y b dos enteros positivos tales que $2 \leq a < b$ y sea $S = \mathrm{S}(a,b)$. Puesto que (a,b) y $(a-1,b)$ son divisores propios de b, y además $((a,b),(a-1,b)) = 1$, resulta que $(a,b)+(a-1,b) \leq b/2 + b/3 = 5b/6$. Por el Teorema 1.13, $\#\mathrm{H}(S) \geq \frac{1}{2}(b+1-\frac{5}{6}b)$ y por tanto $b \leq 12 \cdot \#\mathrm{H}(S) - 6$. □

Recordar que para un semigrupo numérico S, la multiplicidad de S, denotada por $\mathrm{m}(S)$, es el menor entero positivo perteneciente a S.

LEMA 1.22. *Sea $S = \mathrm{S}(a,b)$ un semigrupo modular. Entonces*

$$b - \mathrm{m}(S) \in S \quad \textit{si y sólo si} \quad \mathrm{m}(S) = \mathrm{mín}\{\frac{b}{(a,b)}, \frac{b}{(a-1,b)}\}.$$

DEMOSTRACIÓN. Es inmediata a partir del Lema 1.12. □

El siguiente lema establece una cota inferior para los posibles módulos b que pueden aparecer en cualquier represenstación modular para un semigrupo modular S.

LEMA 1.23. *Sea S un semigrupo modular con módulo b. Entonces*

$$b \geq \mathrm{g}(S) + \mathrm{m}(S).$$

DEMOSTRACIÓN. Como $\{1,2,\ldots,\mathrm{m}(S)-1\} \cap S$ es igual al conjunto vacío, por el Corolario 1.6 deducimos que $\{b-\mathrm{m}(S)+1,\ldots,b-1\} \subseteq S$. Además, $\{b, \mathrm{m}(S)\} \subset S$ y por tanto $\{b-\mathrm{m}(S)+1, \rightarrow\} \subseteq S$. Ésto implica que $\mathrm{g}(S) \leq b - \mathrm{m}(S)$. □

Ahora determinamos cuándo se alcanza el menor valor posible para b.

LEMA 1.24. *Sea $S = \mathrm{S}(a,b)$ un semigrupo modular. Entonces*

$$b = \mathrm{g}(S) + \mathrm{m}(S) \quad \textit{si y sólo si} \quad \mathrm{m}(S) \neq \mathrm{mín}\{\frac{b}{(a,b)}, \frac{b}{(a-1,b)}\}.$$

DEMOSTRACIÓN. Es consecuencia de los Lemas 1.22 y 1.23. □

Ya tenemos todos los elementos necesarios para dar el algorítmo anunciado al comienzo de la sección.

ALGORITMO 1.25.
ENTRADA: un semigrupo numérico S, con $S \neq \mathbb{N}$.
SALIDA: "S es modular con módulo b y factor a" ó "S no es modular".

(1) Calcular $\#\mathrm{H}(S)$, $\mathrm{g}(S)$ y $\mathrm{m}(S)$.
(2) Sea $b = \mathrm{g}(S) + \mathrm{m}(S)$. Obtener todos los elementos del conjunto

$$A = \left\{ a \in \mathbb{N} \;\middle|\; \begin{array}{l} 2 \leq a \leq \frac{b+1}{2}, \\ b = 2 \cdot \#\mathrm{H}(S) + (a,b) + (a-1,b) - 1, \\ \mathrm{m}(S) < \mathrm{mín}\{b/(a,b), b/(a-1,b)\} \end{array} \right\}.$$

(3) Para todo $a \in A$, calcular $\mathrm{S}(a,b)$.
(4) Si $S = \mathrm{S}(a,b)$ para algún $a \in A$, entonces devolver como respuesta "*S es modular con módulo b y factor a*" y finalizar.
(5) Calcular todos los elementos del conjunto

$$C = \{c \in \{k \cdot \mathrm{m}(S) \mid k \in \mathbb{N}\} \mid 2 \cdot \#\mathrm{H}(S) + 1 \leq c \leq 12 \cdot \#\mathrm{H}(S) - 6\}.$$

(6) Para cada $c \in C$, obtener el conjunto

$$A_c = \left\{ a \in \mathbb{N} \;\middle|\; \begin{array}{l} 2 \leq a \leq \frac{c+1}{2}, \\ c = 2 \cdot \#\mathrm{H}(S) + (a,c) + (a-1,c) - 1, \\ \mathrm{m}(S) = \mín\{c/(a,c), c/(a-1,c)\} \end{array} \right\}.$$

(7) Para cada $c \in C$ y cada $a \in A_c$, calcular $\mathrm{S}(a,c)$.
(8) Si $S = \mathrm{S}(a,c)$ para algún $c \in C$ y algún $a \in A_c$, entonces devolver como respuesta "*S es modular con módulo c y factor a*" y finalizar.
(9) Devolver como respuesta "*S no es modular*".

Argumentamos a continuación brevemente que el Algorítmo 1.25 es correcto. Aunque no se ha indicado explícitamente, podemos suponer que el semigrupo S viene dado en términos de un sistema de generadores a partir de los cuales se obtienen $\#\mathrm{H}(S)$, $\mathrm{g}(S)$ y $\mathrm{m}(S)$ en el paso (1). En los pasos (2), (3) y (4) estamos comprobando si S es o no un semigrupo numérico modular con módulo $\mathrm{g}(S) + \mathrm{m}(S)$. La justificación teórica de los mismos viene dada por los Lemas 1.4 y 1.24, y el Teorema 1.13. Si S no es modular con módulo $\mathrm{g}(S) + \mathrm{m}(S)$, entonces por el Lema 1.24, tenemos que $\mathrm{m}(S) = \mín\{b/(a,b), b/(a-1,b)\}$, lo cual en particular implica que $\mathrm{m}(S)$ divide a b. Por el Teorema 1.13 sabemos que $b = 2 \cdot \#\mathrm{H}(S) + (a,b) + (a-1,b) - 1$, y por tanto $b \geq 2 \cdot \#\mathrm{H}(S) + 1$. Finalmente, por el Lema 1.21 sabemos que b ha de ser menor o igual que $12 \cdot \#\mathrm{H}(S) - 6$. Por consiguiente, vemos que los pasos (5)–(8) cubren el caso en que $b \neq \mathrm{g}(S) + \mathrm{m}(S)$. Para concluir, decir que las comprobaciones de igualdad $S = \mathrm{S}(x,y)$ en los pasos (4) y (8) pueden llevarse a cabo calculando un sistema minimal de generadores para cada semigrupo y viendo si éstos coinciden, o bien comprobando si $S \subseteq \mathrm{S}(x,y)$ y $\#\mathrm{H}(S) = \#\mathrm{H}(\mathrm{S}(x,y))$.

EJEMPLO 1.26. Para $S = \langle 3,5 \rangle$, calculamos $\#\mathrm{H}(S) = 4$, $\mathrm{g}(S) = 7$ y $\mathrm{m}(S) = 3$. Así, en el paso (2) obtenemos $b = 10$ y $A = \{2,3,4\}$. En el paso (3) resulta

$$\mathrm{S}(2,10) = \langle 5,6,7,8,9 \rangle,\ \mathrm{S}(3,10) = \langle 4,5,7 \rangle,\ \mathrm{S}(4,10) = \langle 3,5 \rangle.$$

Por tanto el Algorítmo 1.25 dedulve como respuesta "$\langle 3,5 \rangle$ es un semigrupo modular con módulo 10 y factor 4". □

EJEMPLO 1.27. Sea $S = \langle 3,8,10 \rangle$. En este caso $\#\mathrm{H}(S) = 5$, $\mathrm{g}(S) = 7$ y $\mathrm{m}(S) = 3$. En el paso (2) obtenemos $b = 10$ y $A = \emptyset$. En el paso (5) resulta $C = \{12,15,18,21,24,27,30,33,36,39,42,45,48,51,54\}$. El único conjunto A_c, con $c \in C$, el cual no es vacío es $A_{15} = \{5\}$. Puesto que $S \neq \mathrm{S}(5,15) = \langle 3,7,11 \rangle$, el algorítmo devuelve como respuesta que "$\langle 3,8,10 \rangle$ no es un semigrupo modular.". □

EJEMPLO 1.28. Sea $S = \langle 10,11,12 \rangle$. Entonces $\#\mathrm{H}(S) = 25$, $\mathrm{g}(S) = 49$ y $\mathrm{m}(S) = 10$. En el paso (2) obtenemos $b = 59$ y $A = \emptyset$. Al calcular C en el paso (5), obtenemos

$$C = \{60,70,80,90,100,110,120,130,140,150,160,170,180,$$
$$190,200,210,220,230,240,250,260,270,280,290\}.$$

El único conjunto A_c con $c \in C$ el cual es no vacío es $A_{60} = \{6\}$. Por tanto $S = \mathrm{S}(6,60)$.

COMENTARIO 1.29. Es posible incluir algunas mejoras en el Algorítmo 1.25 si éste lo aplicamos a ciertos tipos conocidos de semigrupos. Por ejemplo, si sabemos a priori que un semigrupo numérico S es simétrico y ocurre que $S = \mathrm{S}(a,b)$, entonces b ha de ser igual a $\mathrm{g}(S)+(a,b)+(a-1,b)$, pues según el Corolario 1.19 en este caso se verifica que $\mathrm{w}(S) = \mathrm{g}(S)$. Se pueden realizar optimizaciones similares para semigrupos numéricos pseudo-simétricos. □

COMENTARIO 1.30. Tal y como ya hemos comentado, no todo semigrupo numérico es modular. Si $a_1, b_1, \ldots, a_n, b_n$, $n > 0$, son enteros positivos, entonces

$$S = \left\{x \in \mathbb{N} \mid a_i x \bmod b_i \leq x, \text{ para todo } i \in \{1,\ldots,n\}\right\} = \bigcap_{i=1}^{n} \{x \in \mathbb{N} \mid a_i x \bmod b_i \leq x\}$$

es un semigrupo numérico. Decimos que S es un **sistema modular**. Claramente todo semigrupo modular es un sistema modular, aunque el recíproco es falso. Sea el semigrupo $S = \langle 3,8,10\rangle$. Se puede comprobar fácilmente que $S = \langle 3,4\rangle \cap \langle 3,5\rangle$. Puesto que $\langle 3,4\rangle = \mathrm{S}(3,8) = \mathrm{S}(3,9)$ y $\langle 3,5\rangle = \mathrm{S}(4,10)$, vemos que S es un sistema modular. Sin embargo, en vista del Ejemplo 1.27, tenemos que S no es modular.

Aparte, no todo semigrupo numérico es un sistema modular. Por ejemplo el semigrupo $S = \langle 7,8,10,13\rangle$ es irreducible por lo que no puede ser expresado como una intersección de semigrupos numéricos que lo contengan de forma propia. Por tanto si S fuese un sistema modular, entonces tendría que ser modular. Pero al aplicarle el Algorítmo 1.25 obtenemos que S no es un semigrupo numérico modular. □

3. Semigrupos modulares cuyo módulo es igual a su peso más dos

Si $S = \mathrm{S}(a,b)$, entonces sabemos que $b = \mathrm{w}(S)+(a,b)+(a-1,b) \geq \mathrm{w}(S)+2$. De aquí deducimos que $b = \mathrm{w}(S)+2$ si y sólo si $(a,b) = (a-1,b) = 1$. Claramente esta condición implica que b ha de ser impar. Por tanto en esta sección estudiaremos aquellos semigrupos modulares cuyo módulo es mínimo con respecto a su peso.

PROPOSICIÓN 1.31. *Sea $S = \mathrm{S}(a,b)$ tal que $2 \leq a < b$ y $(a,b) = (a-1,b) = 1$. Entonces*

1. $b = \mathrm{g}(S)+\mathrm{m}(S)$,
2. $\#\mathrm{H}(S) = \frac{1}{2}(\mathrm{g}(S)+\mathrm{m}(S)-1)$,
3. *b es el mayor generador minimal de S.*

DEMOSTRACIÓN.

1. La hipótesis $2 \leq a < b$ implica que $1 \notin S$. Por el Corolario 1.6, obtenemos que $b-1 \in S$. Por tanto $\mathrm{m}(S) \neq b$. Usando el Lema 1.24 deducimos que $b = \mathrm{g}(S)+\mathrm{m}(S)$.
2. Es una consecuencia inmediata del Teorema 1.13.
3. En primer lugar demostramos que las hipótesis implican que b es un generador minimal de S. Supongamos por reducción al absurdo que $b = x+y$ con $x,y \in S \setminus \{0\}$. Entonces $ax \bmod b \leq x$ y $ay \bmod b \leq y$, y como consecuencia $(ax \bmod b)+(ay \bmod b) \leq x+y = b$. Por tanto ha de cumplirse

que $(ax \bmod b) + (ay \bmod b) = a(x+y) \bmod b$, y ya que $a(x+y) \bmod b = ab \bmod b = 0$, deducimos que $(ax \bmod b) + (ay \bmod b) \in \{0, b\}$. Tenemos dos casos posibles:

- $ax \bmod b = x$ y $ay \bmod b = y$, ó
- $ax \bmod b = 0$ y $ay \bmod b = 0$.

Pero la hipótesis $(a,b) = (a-1,b) = 1$ hace que cada uno de estos casos sea contradictorio con el Lema 1.11. Por tanto b ha de ser un generador minimal de S. Para cualquier $x \in S$, con $x > b$, aplicando el apartado (1) resulta que $x > \mathrm{g}(S) + \mathrm{m}(S)$, lo cual en particular implica que $x - \mathrm{m}(S) > \mathrm{g}(S)$, y ésto a su vez lleva a que $x - \mathrm{m}(S)$ pertenece a S. Ya que $x = \mathrm{m}(S) + (x - \mathrm{m}(S))$, deducimos que x no puede ser un generador minimal de S.

□

Esta proposición nos permite relacionar el tipo de semigrupos numéricos que estamos estudiando en esta sección con los llamados UESY-semigrupos. Decimos que un semigrupo numérico S es un **UESY-semigrupo** (o bien un semigrupo UESY), si existe un semigrupo numérico simétrico S' tal que $S' \subseteq S$ y $\#(S \setminus S') = 1$. El término UESY es el acrónimo de "unitary extension of a symmetric numerical semigroup"(véase [**29**]).

Los siguientes resultados también aparecen en [**29**].

LEMA 1.32. *Un semigrupo numérico S es un UESY-semigrupo si y sólo si existe un semigrupo numérico simétrico S' tal que $S = S' \cup \{\mathrm{g}(S')\}$.*

PROPOSICIÓN 1.33. *Sea $S \neq \mathbb{N}$ un semigrupo numérico. Las siguientes condiciones son equivalentes:*

1. *S es un UESY-semigrupo,*
2. *$\#\mathrm{H}(S) = \frac{1}{2}(\mathrm{g}(S) + \mathrm{m}(S) - 1)$ y $\mathrm{g}(S) + \mathrm{m}(S)$ es un generador minimal de S.*

Para un semigrupo numérico S, recordemos que un pseudo-número de Frobenius para S es un número entero x tal que $x \notin S$ y $x + s \in S$ para todo $s \in S \setminus \{0\}$. Denotamos por $\mathrm{Pg}(S)$ el conjunto de todos los pseudo-números de Frobenius de S, y por $\mathrm{t}(S)$ el cardinal de $\mathrm{Pg}(S)$ (véase [**2, 11**]). En [**29**] se prueba además que si $S \neq \mathbb{N}$ es un UESY-semigrupo, entonces $\mathrm{t}(S) = \mathrm{e}(S) - 1$.

Como consecuencia de las Proposiciones 1.31 y 1.33, obtenemos el siguiente resultado.

COROLARIO 1.34. *Sea $S = \mathrm{S}(a,b)$ tal que $2 \leq a < b$ y $(a,b) = (a-1,b) = 1$. Entonces $\mathrm{t}(S) = \mathrm{e}(S) - 1$ y existe un semigrupo numérico simétrico S' tal que $S = S' \cup \{\mathrm{g}(S')\}$.*

TEOREMA 1.35. *Sea $S = \mathrm{S}(a,b)$. Entonces $b = \mathrm{w}(S) + 2$ si y sólo si S es un UESY-semigrupo y b es un generador minimal de S.*

DEMOSTRACIÓN.

Condición necesaria. Si $b = \mathrm{w}(S) + 2$, entonces tal y como observamos al comienzo de esta sección, se verifica que $(a,b) = (a-1,b) = 1$. Por el Corolario 1.34 y el

Lema 1.32, deducimos que S es un UESY-semigrupo, y por la Proposición 1.31 que b es un generador minimal de S.

Condición suficiente. Recordar de la demostración de la Proposición 1.31 que si $x > \mathrm{g}(S) + \mathrm{m}(S)$, entonces x no puede ser un generador minimal de S. Por el Lema 1.23 sabemos que $b \geq \mathrm{g}(S) + \mathrm{m}(S)$, y ya que estamos suponiendo que b es un generador minimal de S, deducimos que $b = \mathrm{g}(S) + \mathrm{m}(S)$. Por la Proposición 1.33 sabemos que $\#\mathrm{H}(S) = \frac{1}{2}(\mathrm{g}(S) + m(S) - 1)$ y por el Teorema 1.13 que $\#\mathrm{H}(S) = \frac{1}{2}(\mathrm{w}(S) + 1)$, de lo cual deducimos que $b = \mathrm{w}(S) + 2$. □

COROLARIO 1.36. *Sea S un semigrupo modular con módulo b. Entonces $b = \mathrm{w}(S) + 2$ si y sólo si $S \setminus \{b\}$ es un semigrupo numérico simétrico. Además, si b es un número primo, entonces $S \setminus \{b\}$ es un semigrupo numérico simétrico.*

DEMOSTRACIÓN.

Condición necesaria. Por el Teorema 1.35 sabemos que b es un generador minimal de S (de hecho es el mayor de todos), lo cual implica que $S' = S \setminus \{b\}$ es un semigrupo numérico y $\mathrm{g}(S') = b$. Por el Corolario 1.6 deducimos que S' es simétrico.

Condición suficiente. Si $S \setminus \{b\}$ es un semigrupo numérico simétrico, entonces estamos diciendo que S es un UESY-semigrupo y que b es un generador minimal de S. Por el Teorema 1.35 deducimos que $b = \mathrm{w}(S) + 2$.

Por último, si b es primo, entonces $(a,b) = (a-1,b) = 1$ y por tanto $\mathrm{w}(S) = b - 2$. □

COROLARIO 1.37. *Sea b un número entero mayor o igual que 3. Entonces b es primo si y sólo si b es el mayor generador minimal de $\mathrm{S}(a,b)$ para todo a tal que $2 \leq a \leq \sqrt{b}$.*

DEMOSTRACIÓN.

Condición necesaria. Es consecuencia de la Proposición 1.31.

Condición suficiente. Si b no es primo, entonces $b = ac$ con $a, c \in \mathbb{N} \setminus \{0,1\}$. Podemos suponer sin pérdida de generalidad que $a \leq \sqrt{b}$). Entonces si $S = \mathrm{S}(a,b)$, tenemos que $ac \bmod b = 0 \leq c$ y por tanto $c \in S$. Ya que $b = ac$, deducimos que b no puede ser un generador minimal de S. □

4. Semigrupos modulares cuyo módulo es igual a su peso más tres

Si $S = \mathrm{S}(a,b)$, entonces $b = \mathrm{w}(S) + 3$ si y sólo si $(a,b) + (a-1,b) = 3$. Vemos que existen dos casos posibles:

- $(a,b) = 1$ y $(a-1,b) = 2$,
- $(a,b) = 2$ y $(a-1,b) = 1$.

De cualquier manera, b ha de ser par y por el Corolario 1.6 deducimos que $b/2 \in S$.

PROPOSICIÓN 1.38. *Sea $S = \mathrm{S}(a,b)$ tal que $2 \leq a < b$ y $(a,b) + (a-1,b) = 3$. Entonces:*

1. *las siguientes afirmaciones son equivalentes:*

a) $\mathrm{m}(S) \neq b/2$,
b) $S \neq \{0, b/2, \rightarrow\}$,
c) $b = \mathrm{g}(S) + \mathrm{m}(S)$,
d) $\#\mathrm{H}(S) = \frac{1}{2}(\mathrm{g}(S) + \mathrm{m}(S) - 2)$,

2. *$b/2$ es un generador minimal de S,*
3. *b es un elemento de S de expresión única.*

DEMOSTRACIÓN.

1. La demostración de este apartado se obtiene fácilmente del Corolario 1.6, del Lema 1.24 y del Teorema 1.13.
2. Supongamos que existen $x, y \in S$ tales que $x + y = b/2$. Como $x, y \in S$, sabemos que $ax \bmod b \leq x$ y $ay \bmod b \leq y$, de donde $ax \bmod b + ay \bmod b \leq x + y = b/2$. Por tanto $ab/2 \bmod b = a(x+y) \bmod b = ax \bmod b + ay \bmod b$. Distinguimos dos casos:
   - si $(a, b) = 2$, entonces $ab/2 \bmod b = 0$, lo cual implica que $ax \bmod b$ y $ay \bmod b$ son ambos iguales a 0; por el Lema 1.11 deducimos que x e y son ambos múltiplos de $b/2$, de donde $x = 0$ ó $y = 0$;
   - si $(a-1, b) = 2$, entonces $ab/2 \bmod b = b/2$ lo cual implica que $ax \bmod b = x$ y $ay \bmod b = y$. Al igual que en el apartado anterior, en vista del Lema 1.11 deducimos que x e y son ambos múltiplos de $b/2$, y por consiguiente $x = 0$ ó $y = 0$.
3. Por último probamos que si $x, y \in S \setminus \{0\}$ y $x + y = b$, entonces $x = y = b/2$. Procediendo de manera similar a como se hizo en la demostración del apartado (3) de la Proposición 1.31, obtenemos que o bien $(ax \bmod b, ay \bmod y) = (x, y)$ ó $ax \bmod b = ay \bmod y = 0$. De nuevo por el Lema 1.11 deducimos que x e y son ambos múltiplos de $b/2$, y puesto que $x \neq 0 \neq y$, finalmente concluimos que $x = y = b/2$.

□

Esta última proposición nos va a permitir relacionar los semigrupos numéricos que estamos considerando en esta sección con los llamados PEPSY-semigrupos (esta relación será similar a la que establecimos en la sección anterior mediante el Teorema 1.35 usando los UESY-semigrupos).

Sabemos que si S' es un semigrupo numérico pseudo-simétrico, entonces el conjunto de los pseudo-números de Frobenius de S' es $\mathrm{Pg}(S') = \{\frac{1}{2}\mathrm{g}(S'), \mathrm{g}(S')\}$ (véase [**2, 11**]). Un semigrupo numérico S es un **PEPSY-semigrupo** (o bien un semigrupo PEPSY), si existe un semigrupo numérico pseudo-simétrico S' tal que $S = S' \cup \{\frac{1}{2}\mathrm{g}(S'), \mathrm{g}(S')\}$, es decir, S se obtiene añadiéndole a S' sus pseudo-números de Frobenius. El término PEPSY es el acrónimo de "pseudo-Frobenius number extension of a pseudo-symmetric numerical semigroup"(véase [**25**]). Recuérdese también que un semigrupo numérico S es una semirecta cuando es de la forma $S = \{0, m, \rightarrow\}$.

El siguiente resultado aparece en [**25**].

PROPOSICIÓN 1.39. *Sea S un semigrupo numérico que no es una semirecta. Las siguientes afirmaciones son equivalentes:*

1. *S es un PEPSY-semigrupo,*
2. *$\#\mathrm{H}(S) = \frac{1}{2}(\mathrm{g}(S)+\mathrm{m}(S)-2)$, $\frac{1}{2}(\mathrm{g}(S)+\mathrm{m}(S))$ es un generador minimal de S y $\mathrm{g}(S)+\mathrm{m}(S)$ es un elemento de S de expresión única.*

Como consecuencia inmediata de las Proposiciones 1.38 y 1.39 obtenemos lo siguiente.

COROLARIO 1.40. *Sea $S = \mathrm{S}(a,b)$ tal que $2 \leq a < b$, $(a,b)+(a-1,b) = 3$ y S no es una semirecta. Entonces S es un PEPSY-semigrupo.*

En [**25**] se demuestra que si S es un PEPSY-semigrupo que no es una semirecta, entonces $\mathrm{t}(S) = \mathrm{e}(S)-1$. Ésto nos permite enunciar un nuevo resultado.

COROLARIO 1.41. *Sea $S = \mathrm{S}(a,b)$ tal que $2 \leq a < b$, $(a,b)+(a-1,b) = 3$ y S no es una semirecta. Entonces $\mathrm{t}(S) = \mathrm{e}(S)-1$.*

COMENTARIO 1.42. Los semigrupos que son semirectas también son MED-semigrupos, es decir, semigrupos numéricos de máxima dimensión de inmersión, lo cual significa que su multiplicidad es igual a su dimensión de inmersión. Es un hecho bien conocido (véase por ejemplo [**2**]) que si S es un MED-semigrupo, entonces $\mathrm{t}(S) = \mathrm{m}(S)-1$, y por tanto $\mathrm{t}(S) = \mathrm{e}(S)-1$. Como consecuencia, la hipótesis de que "S no es una semirecta" puede ser suprimida en el Corolario 1.41. □

TEOREMA 1.43. *Supongamos que $S = \mathrm{S}(a,b)$ no es una semirecta. Entonces $b = \mathrm{w}(S)+3$ si y sólo si S es un PEPSY-semigrupo, $b/2$ es un generador minimal de S y b es un elemento de S de expresión única.*

DEMOSTRACIÓN.

Condición necesaria. Es una consecuencia inmediata del Corolario 1.40 y de la Proposición 1.38.

Condición suficiente. Por el Corolario 1.6, si $\mathrm{m}(S) = b/2$, entonces S es una semirecta, con lo cual $\mathrm{m}(S) \neq b/2$. Por el Lema 1.23 además sabemos que $b \geq \mathrm{g}(S)+\mathrm{m}(S)$. Si $b > \mathrm{g}(S)+\mathrm{m}(S)$, entonces $b = \mathrm{m}(S)+(b-\mathrm{m}(S))$ con $\mathrm{m}(S)$ y $b-\mathrm{m}(S)$ ambos pertenecientes a S. Puesto que $\mathrm{m}(S) \neq b/2$, entonces tenemos dos expresiones diferentes de b, contradiciendo el hecho de que b es un elemento de S de expresión única. Por consiguiente $b = \mathrm{g}(S)+\mathrm{m}(S)$. Por la Proposición 1.39 sabemos que $\#\mathrm{H}(S) = \frac{1}{2}(\mathrm{g}(S)+\mathrm{m}(S)-2)$ y por el Teorema 1.13 que $\#\mathrm{H}(S) = \frac{1}{2}(\mathrm{w}(S)+1)$. Igualando ambas fórmulas, deducimos que $b = \mathrm{g}(S)+\mathrm{m}(S) = \mathrm{w}(S)+3$. □

COROLARIO 1.44. *Sea S un semigrupo modular de módulo b. Entonces $b = \mathrm{w}(S)+3$ si y sólo si $S \setminus \{b/2, b\}$ es un semigrupo numérico pseudo-simétrico. Si p es un número primo, $b = 2p$ y $a < p$, entonces $S \setminus \{b/2, b\}$ es un semigrupo numérico pseudo-simétrico.*

DEMOSTRACIÓN.

Condición necesaria. Por el Teorema 1.43 sabemos que $b/2$ es un generador minimal de S y b es un elemento de S de expresión única. Ésto en particular implica que $S' = S \setminus \{b/2, b\}$ es un semigrupo numérico y además $\mathrm{g}(S') = b$. Usando el Corolario 1.6 deducimos que S' es un semigrupo numérico pseudo-simétrico.

Condición suficiente. Si $S \setminus \{b/2, b\}$ es un semigrupo numérico pseudo-simétrico, entonces por definición S es un PEPSY-semigrupo, $b/2$ es un generador minimal de S y $b = b/2 + b/2$ es la única expresión de b en S. Por el Teorema 1.43 concluimos que $b = \mathrm{w}(S) + 3$. □

CAPÍTULO 2

Semigrupos numéricos y desigualdades diofánticas proporcionalmente modulares

En este capítulo introducimos el concepto de semigrupo proporcionalmente modular el cual generaliza al de semigrupo modular que fué introducido en el capítulo anterior. Seguidamente deducimos varias caracterizaciones para semigrupos proporcionalmente modulares. A continuación damos algoritmos para decidir cuando un semigrupo numérico es o no proporcionalmente modular, y para dedicir si es o no una intersección de semigrupos proporcionalmente modulares. En la última sección introducimos una familia de semigrupos proporcionalmente modulares en la cual están englobados los semigrupos numéricos de dos generadores y más generalmente los semigrupos numéricos generados por progresiones aritméticas.

Los contenidos de este capítulo aparecen en [**40**].

1. Submonoides de $\mathbb{R}_0^+$ generados por intervalos cerrados

En esta sección, salvo que se indique lo contrario, α y β serán dos números reales no negativos tales que $\alpha < \beta$, y T denotará el submonoide de $\mathbb{R}_0^+$ generado por el intervalo cerrado $[\alpha, \beta]$.

LEMA 2.1. *Sea $x \in \mathbb{R}_0^+$. Entonces $x \in T$ si y sólo si existe $k \in \mathbb{N}$ tal que $x \in [k\alpha, k\beta]$.*

DEMOSTRACIÓN. Si $x \in T$, entonces existen $t_1, \ldots, t_k \in [\alpha, \beta]$ y $a_1, \ldots, a_k \in \mathbb{N}$ tal que $x = a_1 t_1 + \cdots + a_k t_k$, y por tanto $(a_1 + \cdots + a_k)\alpha \leq x \leq (a_1 + \cdots + a_k)\beta$.

Sea $k \in \mathbb{N} \setminus \{0\}$ tal que $k\alpha \leq x \leq k\beta$. Esto implica que $\alpha \leq x/k \leq \beta$, es decir, $x/k \in [\alpha, \beta] \subseteq T$. Ya que T es un monoide, obtenemos que $k(x/k) = x \in T$. □

COMENTARIO 2.2. Observamos que si $\alpha = 0$, entonces $T = \mathbb{R}_0^+$. Por ello, para el resto de esta sección suprondremos además que $0 < \alpha < \beta$. □

LEMA 2.3. *El conjunto $[\alpha, \beta]$ es un sistema minimal de generadores para T si y sólo si $2\alpha > \beta$.*

DEMOSTRACIÓN. Si $[\alpha, \beta]$ es un sistema minimal de generadores para T, entonces $2\alpha \in T \setminus [\alpha, \beta]$ y en consecuencia $2\alpha > \beta$.

Supongamos ahora que $2\alpha > \beta$ y sea $x \in [\alpha, \beta]$. Si x no es un generador minimal para T, entonces $x = u + v$ con $u, v \in T \setminus \{0\}$. Por tanto $2\alpha \leq u + v = x$ y usando la hipótesis $2\alpha > \beta$ resulta $x > \beta$, lo cual es imposible. □

COMENTARIO 2.4. En vista del Lema 2.4, podemos suponer que $0 < \alpha < \beta < 2\alpha$, pues si $2\alpha \leq \beta$, entonces $T = [\alpha, \infty) \cup \{0\}$. Un subsemigrupo T de $\mathbb{R}_0^+$ de la forma $T = [\alpha, \infty) \cup \{0\}$ diremos que es una semirecta. □

PROPOSICIÓN 2.5. *Si T es el submonoide de $\mathbb{R}_0^+$ generado por $[\alpha, \beta]$, con $0 \leq \alpha < \beta$, entonces T contiene una semirecta. Además*

$$\left\lceil \frac{\alpha}{\beta - \alpha} \right\rceil \alpha = \min\{r \in \mathbb{R}_0^+ \mid [r, \infty) \subseteq T\}.$$

DEMOSTRACIÓN. Por el Lema 2.1 sabemos que

$$T = \{0\} \cup [\alpha, \beta] \cup [2\alpha, 2\beta] \cup \cdots \cup [k\alpha, k\beta] \cup \cdots.$$

Si $k\beta \geq (k+1)\alpha$, entonces $(k+h)\beta \geq (k+h+1)\alpha$ para todo $h \in \mathbb{N}$ y por tanto $[k\alpha, \infty) \subseteq T$. Por consiguiente, es suficiente probar que existe $k \in \mathbb{N}$ tal que $k\beta \geq (k+1)\alpha$. Sea $k = \lceil \frac{\alpha}{\beta-\alpha} \rceil$. De la desigualdad $\lceil \frac{\alpha}{\beta-\alpha} \rceil \geq \frac{\alpha}{\beta-\alpha}$ resulta $k(\beta - \alpha) \geq \alpha$ y ésto implica que $k\beta \geq (k+1)\alpha$. Como consecuencia obtenemos que $[\lceil \frac{\alpha}{\beta-\alpha} \rceil \alpha, \infty) \subseteq T$. Obsérvese también que $\lceil \frac{\alpha}{\beta-\alpha} \rceil - 1 < \frac{\alpha}{\beta-\alpha}$ y por tanto $(\lceil \frac{\alpha}{\beta-\alpha} \rceil - 1)\beta < \alpha + \alpha(\lceil \frac{\alpha}{\beta-\alpha} \rceil - 1) = \lceil \frac{\alpha}{\beta-\alpha} \rceil \alpha$. Teniendo en cuenta de nuevo el Lema 2.1 concluimos la prueba. □

Diremos que el número real $\min\{r \in \mathbb{R}_0^+ \mid [r, \infty) \subseteq T\}$ es el conductor de T y lo representaremos como $\mathrm{c}(T)$. Por tanto la Proposición previa afirma que $\mathrm{c}(T) = \lceil \frac{\alpha}{\beta-\alpha} \rceil \alpha$.

Dados $a \in \mathbb{R}$ y $b \in \mathbb{R}^+$, existen dos únicos números $q \in \mathbb{Z}$ y $r \in \mathbb{R}_0^+$ verificando $a = qb + r$ y $0 \leq r < b$. Representamos dichos valores como $q = a \div b$ y $r = a \bmod b$. Obsérvese que $a \div b = \lfloor \frac{a}{b} \rfloor$ y $a - (a \bmod b) = (a \div b)b$. Cuando a y b son además enteros resulta que q y r son el cociente y el resto de la división, respectivamente. El siguiente lema se demuesta fácilmente.

LEMA 2.6. *Dados $a \in \mathbb{R}$ y $b, c \in \mathbb{R}^+$, se verifica que $c(a \bmod b) = ca \bmod cb$.*

COMENTARIO 2.7. Observar que $ax \bmod b = (a \bmod b)x \bmod b$, por lo cual al escribir $ax \bmod b$ podemos siempre suponer que $0 \leq a < b$. □

TEOREMA 2.8. *Sea T un submonoide propio de $\mathbb{R}_0^+$. Entonces T está generado por un intervalo cerrado si y sólo si existen números reales a y b tales que $1 < a < b$ y $T = \{x \in \mathbb{R}_0^+ \mid ax \bmod b \leq x\}$.*

DEMOSTRACIÓN.

Condición necesaria. Supongamos que T es el submonoide de $\mathbb{R}_0^+$ generado por el intervalo $[\alpha, \beta]$ siendo α y β números reales tales que $0 < \alpha < \beta$. Demostramos que $x \in T$ si y sólo si $\frac{\beta}{\beta-\alpha} x \bmod \frac{\beta\alpha}{\beta-\alpha} \leq x$. Por el Lema 2.1, si $x \in T$, entonces exite $k \in \mathbb{N}$ tal que $k\alpha \leq x \leq k\beta$. Ya que $k \leq (x \div \alpha)$, tenemos que $x \leq (x \div \alpha)\beta$. De ésto deducimos que $x \leq \frac{x - (x \bmod \alpha)}{\alpha} \beta$ y por tanto $\frac{\beta}{\beta-\alpha}(x \bmod \alpha) \leq x$. Usando el Lema 2.6 obtenemos que $\frac{\beta}{\beta-\alpha} x \bmod \frac{\beta\alpha}{\beta-\alpha} \leq x$. Recíprocamente, si $\frac{\beta}{\beta-\alpha} x \bmod \frac{\beta\alpha}{\beta-\alpha} \leq x$, entonces por el Lema

2.6, tenemos que $\frac{\beta}{\beta-\alpha}(x \bmod \alpha) \leq x$, lo cual implica que $\beta(x \bmod \alpha) \leq (\beta-\alpha)x$. Por consiguiente $\alpha x \leq \beta(x-(x \bmod \alpha)) = \beta(x \div \alpha)\alpha$. Ésto lleva a que $x \leq \beta(x \div \alpha)$, y ya que $\alpha(x \div \alpha) \leq x$, concluimos que $\alpha(x \div \alpha) \leq x \leq \beta(x \div \alpha)$, lo cual por el Lema 2.1 significa que $x \in T$.

Condición suficiente. Probamos que para cualquier $x \in \mathbb{R}_0^+$, se verifica que $ax \bmod b \leq x$ si y sólo si x pertenece al submonoide de $\mathbb{R}_0^+$ generado por el intervalo $[\frac{b}{a}, \frac{b}{a-1}]$. Si $ax \bmod b \leq x$, entonces $0 \leq ax-(ax \div b)b \leq x$ por lo que $(ax \div b)b \leq ax \leq (ax \div b)b + x$. Por tanto $(ax \div b)\frac{b}{a} \leq x \leq (ax \div b)\frac{b}{a-1}$. Aplicando de nuevo el Lema 2.1, ésto significa que x pertenece al submonoide de $\mathbb{R}_0^+$ generado por $[\frac{b}{a}, \frac{b}{a-1}]$. Recíprocamente, si x pertenece al submonoide de $\mathbb{R}_0^+$ generado por $[\frac{b}{a}, \frac{b}{a-1}]$, entonces por el Lema 2.1 obtenemos que $k\frac{b}{a} \leq x \leq k\frac{b}{a-1}$ para algún $k \in \mathbb{N}$. Ésto implica que $kb \leq ax \leq kb + x$ y por tanto $ax \bmod b \leq x$. □

Como consecuencia de la demostración de este teorema, obtenemos el siguiente resultado.

COROLARIO 2.9.

1. *Sean α y β dos números reales verificando que $0 < \alpha < \beta$. Entonces el submonoide de $\mathbb{R}_0^+$ generado por el intervalo $[\alpha, \beta]$ es igual a*

$$\{x \in \mathbb{R}_0^+ \mid \frac{\beta}{\beta-\alpha}x \bmod \frac{\beta\alpha}{\beta-\alpha} \leq x\}.$$

2. *Sean a y b dos números reales tales que $1 < a < b$. Entonces*

$$\{x \in \mathbb{R}_0^+ \mid ax \bmod b \leq x\}$$

es el submonoide de $\mathbb{R}_0^+$ generado por el intervalo $[\frac{b}{a}, \frac{b}{a-1}]$.

COMENTARIO 2.10. Sean a y b dos números reales tales que $1 < a < b$ y sea $T = \{x \in \mathbb{R}_0^+ \mid ax \bmod b \leq x\}$. Entonces por el Corolario 2.9 sabemos que T es el submonoide de $\mathbb{R}_0^+$ generado por el intervalo $[\frac{b}{a}, \frac{b}{a-1}]$. Además, por el Comentario 2.4 tenemos que T es una semirecta si y sólo si $2\frac{b}{a} \leq \frac{b}{a-1}$, por lo que T es una semirecta si y sólo si $a \leq 2$. En este caso se cumple que $T = [\frac{b}{a}, \infty) \cup \{0\}$. □

COROLARIO 2.11. *Sean a y b dos números reales tales que $1 < a < b$ y sea $T = \{x \in \mathbb{R}_0^+ \mid ax \bmod b \leq x\}$. Entonces*

$$c(T) = \lceil a-1 \rceil \frac{b}{a}.$$

DEMOSTRACIÓN. Es consecuencia del Corolario 2.9 y de la Proposición 2.5. □

2. Semigrupos numéricos proporcionalmente modulares

Sea T un submonoide de $\mathbb{R}_0^+$ generado por un intervalo cerrado I y sea $S = T \cap \mathbb{N}$. Por la Proposición 2.5 es inmediato que S es un semigrupo numérico el cual representaremos como $\mathrm{S}(I)$. Un semigrupo numérico obtenido de esta forma lo llamaremos **semigrupo proporcionalmente modular**. También diremos que el intervalo cerrado I define al semigrupo S.

Si S es un semigrupo proporcionalmente modular, desde un punto de vista intuitivo parece razonable que existan varias posibilidades a la hora de elegir el submonoide T de $\mathbb{R}_0^+$ generado por un intervalo cerrado $[\alpha,\beta]$ de manera que $T \cap \mathbb{N} = S$. De forma más exacta, lo que nos estamos planteando es la posibilidad de cambiar el intervalo de generadores $[\alpha,\beta]$ de modo que el correspondiente conjunto de enteros no negativos (aquellos que pertenecen a T) no varíe. Por lo pronto, comenzamos demostrando en el siguiente resultado que α y β pueden siempre ser elegidos de modo que sean números racionales.

LEMA 2.12. *Sea S un semigrupo proporcionalmente modular. Entonces existen $p,q \in \mathbb{Q}$ tales que $0 \leq p < q$ y $S = T \cap \mathbb{N}$, siendo T el submonoide de $\mathbb{R}_0^+$ generado por $[p,q]$.*

DEMOSTRACIÓN. Al ser S proporcionalmente modular, existen $\alpha,\beta \in \mathbb{R}^+$ tales que $S = M \cap \mathbb{N}$, siendo M el submonoide de $\mathbb{R}_0^+$ generado por el intervalo $[\alpha,\beta]$. Por el Lema 2.1 y por la Proposición 2.5, deducimos que exite $t \in \mathbb{N}$ tal que

$$S = \mathbb{N} \cap \big(\{0\} \cup [\alpha,\beta] \cup [2\alpha,2\beta] \cup \cdots \cup [t\alpha,t\beta] \cup [(t+1)\alpha,\infty)\big),$$

siendo $\mathrm{c}(M) = (t+1)\alpha$. Definimos los números

$$\alpha_0 = \text{máx}\left\{\lfloor\alpha\rfloor, \frac{\lfloor 2\alpha\rfloor}{2}, \ldots, \frac{\lfloor (t+1)\alpha\rfloor}{t+1}\right\}$$

y

$$\beta_0 = \text{mín}\left\{\lfloor\beta\rfloor + 1, \frac{\lfloor 2\beta\rfloor + 1}{2}, \ldots, \frac{\lfloor t\beta\rfloor + 1}{t}\right\}.$$

Tanto α_0 como β_0 son números racionales verificando que $0 \leq \alpha_0 \leq \alpha \leq \beta \leq \beta_0$. Si α es racional, hacemos $p = \alpha$; en caso contrario, elegimos un número racional p tal que $\alpha_0 < p \leq \alpha$. De forma similar, si β es racional, entonces hacemos $q = \beta$; si no, elegimos un número racional q verificando que $\beta \leq q < \beta_0$ (la densidad de $\mathbb{Q}$ en $\mathbb{R}$ nos garantiza la existencia de p y q). Sea T el submonoide de $\mathbb{R}_0^+$ generado por el intervalo cerrado $[p,q]$. Es inmediato constatar que $S = M \cap \mathbb{N} = T \cap \mathbb{N}$. □

TEOREMA 2.13. *Sea $S \neq \mathbb{N}$ un semigrupo numérico. Entonces S es proporcionalmente modular si y sólo si existen enteros positivos $c < a < b$ tales que*

$$S = \{x \in \mathbb{N} \mid ax \bmod b \leq cx\}.$$

DEMOSTRACIÓN. Por el Teorema 2.8 y el Lema 2.12 deducimos que S es proporcionalmente modular si y sólo si $S = \{x \in \mathbb{N} \mid \frac{a}{c}x \bmod \frac{b}{c} \leq x\}$ siendo a,b y c enteros

positivos tales que $c < a < b$. Para completar la demostración, basta aplicar el Lema 2.6. □

COMENTARIO 2.14. En vista del Lema 2.6, podemos suponer que $\text{mcd}\{a,b,c\} = 1$, ya que $ax \bmod b \leq cx$ si y sólo si $adx \bmod bd \leq cdx$ para cualquier entero $d \neq 0$. □

En el Capítulo 1 estudiamos los semigrupos modulares, es decir, aquellos de la forma $S = \{x \in \mathbb{N} \mid ax \bmod b \leq x\}$. En vista del Teorema 2.13 todo semigrupo modular es proporcionalmente modular. Además, aplicando el Corolario 2.9, tenemos que $S = T \cap \mathbb{N}$, siendo T el submonoide de $\mathbb{R}_0^+$ generado por el intervalo cerrado $[\frac{b}{a}, \frac{b}{a-1}]$.

Dados tres números enteros positivos a, b y c, una **inecuación diofántica proporcionalmente modular** es una expresión del tipo "$ax \bmod b \leq cx$" donde x es una variable en $\mathbb{Z}$. Definimos $\text{S}(a,b,c) = \{x \in \mathbb{N} \mid ax \bmod b \leq cx\}$.

Por tanto, un semigrupo numérico S es proporcionalmente modular si y sólo si existen tres números enteros positivos a, b y c tales que $S = \text{S}(a,b,c)$. En tal caso decimos que $\text{S}(a,b,c)$ es una **representación proporcionalmente modular** para el semigrupo numérico S. Además denominamos a a, b y c el **factor**, el **módulo**, y la **constante de proporcionalidad** para S, respectivamente.

Por el Comentario 2.14, si $\text{S}(a,b,c)$ es una representación proporcionalmente modular para un semigrupo numérico S, entonces para cualquier entero $d > 0$, tenemos que $\text{S}(da,db,dc)$ también es una representación proporcionalmente modular para S. Decimos que una **representación proporcionalmente modular** $S = \text{S}(a,b,c)$ es **primitiva** si $\text{mcd}\{a,b,c\} = 1$. Si S es modular y $S = \text{S}(a,b)$ es una representación modular para S, entonces claramente ésta se trata de una representación proporcionalmente modular primitiva pues $S = \text{S}(a,b,1)$. En el Capítulo 7 estudiaremos con más detalle las representaciones modulares.

Basándonos en el Corolario 2.9 y en el Lema 2.12, deducimos el siguiente resultado que será muy utilizado en las secciones y en los capítulos siguientes.

LEMA 2.15.

1. *Si a, b y c son tres enteros positivos tales que $c < a < b$, entonces se verifica que* $\text{S}(a,b,c) = \text{S}([\frac{b}{a}, \frac{b}{a-c}])$.
2. *Si $\frac{a_1}{b_1}$ y $\frac{a_2}{b_2}$ son dos números racionales positivos tales que $\frac{a_1}{b_1} < \frac{a_2}{b_2}$, entonces se verifica que* $\text{S}([\frac{a_1}{b_1}, \frac{a_2}{b_2}]) = \text{S}(a_2b_1, a_1a_2, a_2b_1 - a_1b_2)$.

El Lema 2.1 también puede ser reformulado como sigue.

LEMA 2.16. *Sea $S = \text{S}([\frac{a_1}{b_1}, \frac{a_2}{b_2}])$ con a_1, a_2, b_1 y b_2 enteros positivos. Entonces un entero positivo x pertenece a S si y sólo si existe un entero positivo y tal que $\frac{a_1}{b_1} \leq \frac{x}{y} \leq \frac{a_2}{b_2}$.*

Escribimos el siguiente lema que es consecuencia del anterior y que además generaliza al Lema 1.3.

LEMA 2.17. *Sean a, b y c tres números enteros no negativos de forma que $b > a$ y $b > c$. Entonces* $\text{S}(a,b,c) = \text{S}(b + c - a, b, c)$

DEMOSTRACIÓN. Si $c \geq a$, entonces $\mathrm{S}(a,b,c) = \mathbb{N} = \mathrm{S}(b+c-a,b,c)$. Supongamos por tanto que $c < a < b$. Si $c = 0$, entonces ni $\mathrm{S}(a,b,c)$ ni $\mathrm{S}(b+c-a,b,c)$ son semigrupos numéricos, aunque incluso en este caso $\mathrm{S}(a,b,c) = \mathrm{S}(b+c-a,b,c) = \{\frac{b}{(a,b)}t \mid t \in \mathbb{N}\}$. Si $c > 0$, por el Lema 2.16, es suficiente observar que $\frac{b}{a} \leq \frac{x}{k} \leq \frac{b}{a-c}$ si y sólo si $\frac{b}{b+c-a} \leq \frac{x}{x-k} \leq \frac{b}{b-a}$. □

Ahora damos una nueva caracterización para los semigrupos proporcionalmente modulares.

Para un semigrupo numérico S y un número entero positivo p, definimos el conjunto

$$\frac{S}{p} = \{x \in \mathbb{N} \mid px \in S\}.$$

Claramente S/p es de nuevo un semigrupo numérico que contiene a S. Además, si $p \in S$, entonces $S/p = \mathbb{N}$. Diremos que S/p es el **cociente** del semigrupo S **por el entero** p.

Recordemos que un semigrupo aritmético es un semigrupo numérico generado por un conjunto de números naturales de la forma $\{n, n+1, \ldots, n+d\}$.

TEOREMA 2.18. *Para un semigrupo numérico S, las siguientes afirmaciones son equivalentes:*

1. *S es proporcionalmente modular,*
2. *existen un semigrupo aritmético A y un entero positivo p tal que* $S = A/p$.

DEMOSTRACIÓN.

(1) implica (2). Por el Lema 2.12 existen enteros positivos a, b y c de modo que $S = T \cap \mathbb{N}$, siendo T el submonoide de $\mathbb{R}_0^+$ generado por el intervalo cerrado $[a/c, b/c]$ Sea T' el submonoide de R_0^+ generado por el intervalo cerrado $[a,b]$ y sea $A = T' \cap \mathbb{N}$. Es evidente que $A = \langle a, a+1, \ldots, b\rangle$. Demostremos que $S = A/c$. Si $x \in S$, entonces $x \in T$ y por consiguiente existe $k \in \mathbb{N}$ tal que $ka/c \leq x \leq kb/c$, es decir, $ka \leq cx \leq kb$. Ésto implica que $cx \in T' \cap \mathbb{N} = A$, y así $x \in A/c$. Recíprocamente, si $x \in A/c$, entonces $cx \in A = T' \cap \mathbb{N}$ y en particular $cx \in T'$. Por tanto existe $k \in \mathbb{N}$ tal que $ka \leq cx \leq kb$, lo cual equivale a $ka/c \leq x \leq kb/c$. Ésto último significa que $x \in T \cap \mathbb{N} = S$.

(2) implica (1). Supongamos que a y b son dos enteros no negativos y sea $A = \langle a, a+1, \ldots, a+b\rangle$. En tal caso, por el Corolario 2 que aparece en [**13**] sabemos que $x \in A$ si y sólo si $x \bmod a \leq \lfloor \frac{x}{a} \rfloor b$. De forma equivalente, $x \in A$ si y sólo si $x \bmod a \leq \frac{x - (x \bmod a)}{a} b$. Por tanto $x \in A$ si y sólo si $(a+b)x \bmod a(a+b) \leq bx$. Como consecuencia

$$S = A/p = \{x \in \mathbb{N} \mid (a+b)px \bmod a(a+b) \leq bpx\},$$

lo cual significa que S es proporcionalmente modular. □

COROLARIO 2.19. *Si S es un semigrupo aritmético, entonces existen enteros positivos* $c < a < b$ *tales que* $a^2 = b + ac$ *y* $S = \{x \in \mathbb{N} \mid ax \bmod b \leq cx\}$. *Recíprocamente,*

si $c < a < b$ son enteros positivos tales que $a^2 = b + ac$ y $S = \{x \in \mathbb{N} \mid ax \bmod b \leq cx\}$, entonces S es un semigrupo aritmético.

DEMOSTRACIÓN. Supongamos que $S = \langle m, m+1, \ldots, m+p \rangle$ para ciertos enteros no negativos m y p. Por la demostración del Teorema 2.18 sabemos que $S = \{x \in \mathbb{N} \mid (m+p)x \bmod m(m+p) \leq px\}$. Además se verifica que $(m+p)^2 = m(m+p) + (m+p)p$.

Recíprocamente, si $a^2 = b + ac$, entonces $S = \{x \in \mathbb{N} \mid ax \bmod b \leq cx\} = \{x \in \mathbb{N} \mid ax \bmod (a-c)a \leq cx\}$. De nuevo, basándonos en la demostración del Teorema 2.18, obtenemos que $S = \langle a-c, a-c+1, \ldots, (a-c)+c \rangle$. □

Recordemos que un elemento $h \in \mathbb{N}$ es un hueco fundamental para un semigrupo numérico S, si $h \notin S$ y $kh \in S$ para todo $k \in \mathbb{N} \setminus \{1\}$. Además denotamos por $\mathrm{FH}(S)$ el conjunto de todos los huecos fundamentales de S. Dado $X \subseteq \mathbb{N}$, sea $\mathrm{D}(X)$ el conjunto formado por todos los enteros positivos que dividen a algún elemento de X. Claramente se verifica que $S = \mathbb{N} \setminus \mathrm{D}(\mathrm{FH}(S))$, y por tanto vemos que el conjunto $\mathrm{FH}(S)$ determina completamente a S (véase [**38**]).

El siguiente resultado describe los huecos fundamentales de un semigrupo cociente S/p en términos de los huecos fundamentales de S.

LEMA 2.20. *Sea S un semigrupo numérico y sea p un entero positivo. Entonces*

$$\mathrm{FH}\left(\frac{S}{p}\right) = \left\{ \frac{h}{p} \mid h \in \mathrm{FH}(S) \text{ y } h \text{ es múltiplo de } p \right\}.$$

DEMOSTRACIÓN. Se sigue de las definiciones que $h \in \mathrm{FH}(S/p)$ si y sólo si $ph \notin S$ y $k \cdot ph \in S$ para todo $k \geq 1$. □

COROLARIO 2.21. *Sea S un semigrupo numérico. Entonces S es proporcionalmente modular si y sólo si existe un semigrupo aritmético A y un entero positivo p de modo que los huecos fundamentales de A que son múltiplos de p son exactamente los huecos fundamentales de S multiplicados por p.*

DEMOSTRACIÓN. Simplemente hay que aplicar el Teorema 2.18 y el Lema 2.20, así como el hecho de que dos semigrupos numéricos S' y S'' son iguales si y sólo si $\mathrm{FH}(S') = \mathrm{FH}(S'')$. □

EJEMPLO 2.22. Sea el semigrupo numérico $A = \langle 5,6,7 \rangle = \{0,5,6,7,10,\rightarrow\}$. Vamos a calcular la familia de todos los semigrupos numéricos proporcionalmente modulares de la forma A/p con $p \in \mathbb{N} \setminus \{0\}$. Observemos en primer lugar que $\mathrm{H}(A) = \mathbb{N} \setminus A = \{1,2,3,4,8,9\}$ y $\mathrm{FH}(A) = \{8,9\}$. A partir de estos datos y aplicando los resultados anteriores obtenemos las siguientes posibilidades:

- Si $p \notin \{1,2,3,4,8,9\}$, entonces $p \in A$ y por tanto $A/p = \mathbb{N}$.
- Si $p = 1$, entonces $A/1 = A$.
- Si $p = 2$, entonces $\mathrm{FH}(A/2) = \{4\}$ y $A/2 = \mathbb{N} \setminus \mathrm{D}(4) = \mathbb{N} \setminus \{1,2,4\} = \langle 3,5,7 \rangle$.
- Para $p = 3$ resulta $\mathrm{FH}(A/3) = \{3\}$ y $A/3 = \mathbb{N} \setminus \mathrm{D}(3) = \langle 2,5 \rangle$.

- Para $p = 4$ se obtiene $\mathrm{FH}(A/4) = \{2\}$ y $A/4 = \mathbb{N} \setminus \mathrm{D}(2) = \langle 3,4,5\rangle$.
- Si $p \in \{8,9\}$, entonces $\mathrm{FH}(A/p) = \{1\}$, lo cual implica que $A/p = \mathbb{N} \setminus \mathrm{D}(1) = \langle 2,3\rangle$.

□

3. Un algoritmo para dedicir si un semigrupo numérico es proporcionalmente modular

Sea S un semigrupo numérico distinto de $\mathbb{N}$. Por el Teorema 2.8 sabemos que S es proporcionalmente modular si y sólo si existen números reales positivos $1 < a < b$ para los que $S = T \cap \mathbb{N}$ siendo $T = \{x \in \mathbb{R}_0^+ \mid ax \bmod b \leq x\}$. Por el Corolario 2.9 además sabemos que T coincide con el submonoide de $\mathbb{R}_0^+$ generado por $[\frac{b}{a}, \frac{b}{a-1}]$. Obsérvese que $1 < \frac{b}{a} < \frac{b}{a-1}$. Como consecuencia podemos enunciar el siguiente resultado.

LEMA 2.23. *Un semigrupo numérico $S \neq \mathbb{N}$ es proporcionalmente modular si y sólo si $S = T \cap \mathbb{N}$ donde T es el submonoide de $\mathbb{R}_0^+$ generado por un intervalo cerrado $[\alpha,\beta]$ para ciertos números reales $1 < \alpha < \beta$.*

PROPOSICIÓN 2.24. *Sea $S \neq \mathbb{N}$ un semigrupo numérico generado por el conjunto $\{n_1,\ldots,n_p\}$. Sean α y β números reales verificando que $1 < \alpha < \beta$, y sea T el submonoide de $\mathbb{R}_0^+$ generado por el intervalo cerrado $[\alpha,\beta]$. Entonces $S = T \cap \mathbb{N}$ si y sólo si se verifican las siguientes condiciones:*

1. *para todo $i \in \{1,\ldots,p\}$, existe $k_i \in \{1,\ldots,n_i - 1\}$ tal que $n_i/k_i \in [\alpha,\beta]$,*
2. *para todo $x \in \mathrm{H}(S)$ y para todo $k_x \in \{1,\ldots,x-1\}$, se verifica que $x/k_x \notin [\alpha,\beta]$.*

DEMOSTRACIÓN. Por el Lema 2.1, para $x \in \mathbb{N} \setminus \{0\}$ se verifica que $x \in T$ si y sólo si $k\alpha \leq x \leq k\beta$ para algún $k \in \mathbb{N} \setminus \{0\}$. Por tanto $x \in T$ si y sólo si existe $k \in \mathbb{N} \setminus \{0\}$ tal que $\alpha \leq \frac{x}{k} \leq \beta$. Ya que $\alpha > 1$, podemos afirmar que $x \in T$ si y sólo si $x/k \in [\alpha,\beta]$ para algún $k \in \{1,\ldots,x-1\}$. □

Este resultado puede ser mejorado teniendo en cuenta lo siguiente. Sea $S \neq \mathbb{N}$ un semigrupo numérico y sea $x \in \mathrm{H}(S) = \mathbb{N} \setminus S$. Entonces $S \cup \{x\}$ es de nuevo un semigrupo numérico si y sólo si $2x \in S$ y $x + s \in S$ para todo $s \in S \setminus \{0\}$. Sea $\mathrm{EH}(S)$ el conjunto de los huecos de S que verifican esta condición. Claramente $\mathrm{EH}(S)$ está formado por aquellos elementos en $\mathrm{FH}(S)$ que son además pseudo-números de Frobenius para S. Dicho de otra forma, $\mathrm{EH}(S)$ consta de aquellos elementos de $\mathrm{H}(S)$ que son maximales al mismo tiempo respecto de la relación de divisibilidad y de la relación de orden $\leq_S$ sobre $\mathrm{H}(S)$ inducida por S (para un estudio detallado de los conjuntos $\mathrm{EH}(S)$, véase [**39**]). Aparte, nótese también que si S' es un semigrupo numérico que contiene propiamente a S, entonces $\max(S' \setminus S) \in \mathrm{EH}(S)$. El conjunto $\mathrm{EH}(S)$ puede ser bastante más pequeño que $\mathrm{H}(S)$, y tal y como vemos a continuación puede reemplazar a $\mathrm{H}(S)$ en la condición (2) de la Proposición 2.24.

PROPOSICIÓN 2.25. *Sea $S \neq \mathbb{N}$ un semigrupo numérico generado por el conjunto $\{n_1,\ldots,n_p\}$. Sean α y β dos números reales tales que $1 < \alpha < \beta$, y sea T el submonoide*

de $\mathbb{R}_0^+$ *generado por el intervalo cerrado* $[\alpha,\beta]$. *Entonces* $S = T \cap \mathbb{N}$ *si y sólo si se verifican las siguientes condiciones:*

1. *para todo* $i \in \{1,\dots,p\}$, *existe* $k_i \in \{1,\dots,n_i-1\}$ *tal que* $n_i/k_i \in [\alpha,\beta]$,
2. *para todo* $x \in \mathrm{EH}(S)$ *y para todo* $k_x \in \{1,\dots,x-1\}$, *se verifica que* $x/k_x \notin [\alpha,\beta]$.

DEMOSTRACIÓN.

Condición necesaria. Es consecuencia directa de la Proposición 2.24, pues $\mathrm{EH}(S) \subseteq \mathrm{H}(S)$.

Condición suficiente. Por la condición (1) obtenemos que $\{n_1,\dots,n_p\} \subset T \cap \mathbb{N}$ y por tanto $S \subseteq T \cap \mathbb{N}$. Si $S \neq T \cap \mathbb{N}$, entonces tal y como hemos observado más arriba se verifica que $x = \max((T \cap \mathbb{N}) \setminus S) \in \mathrm{EH}(S)$. Pero ésto en particular implica que $x \in T$ y por tanto existe $k \in \mathbb{N}$ tal que $\alpha \leq x/k \leq \beta$. Ya que $\alpha > 1$, obtenemos que $k \in \{1,\dots,x-1\}$, lo cual contradice la condición (2). □

Este último resultado nos permite dar un algoritmo (algo más eficiente) para decidir si un semigrupo numérico dado es o no proporcionalmente modular.

ALGORITMO 2.26.

ENTRADA: Un sistema de generadores $\{n_1,\dots,n_p\}$ para un semigrupo numérico $S \neq \mathbb{N}$.

SALIDA: "*S es proporcionalmente modular*" ó "*S no es proporcionalmente modular*".

1. Calcular $\mathrm{EH}(S)$.
2. Sea $A = (\mathrm{EH}(S) \setminus \{1\}) \cup \{n_1,\dots,n_p\}$.
3. Sea $B = \{(a,k_a) \mid a \in A, k_a \in \{1,\dots,a-1\}\}$.
4. Ordenar los elementos de B de forma que $(a,k_a) \leq (a',k_{a'})$ si y sólo si $a/k_a < a'/k_{a'}$, ó $a/k_a = a'/k_{a'}$ y $a < a'$. Sea $B' = ((x_1,y_1),\dots,(x_l,y_l))$ la lista ordenada resultante.
5. Si existe un segmento $((x_q,y_q),\dots,(x_{q+r},y_{q+r}))$ de elementos consecutivos de B' tal que $\frac{x_{q-1}}{y_{q-1}} \neq \frac{x_q}{y_q}$, $\frac{x_{q+r}}{y_{q+r}} \neq \frac{x_{q+r+1}}{y_{q+r+1}}$ y $\{x_q,\dots,x_{q+r}\} = \{n_1,\dots,n_p\}$, entonces devolver como respuesta "*S* es proporcionalmente modular" y finalizar.
6. En caso contrario, devolver como respuesta "*S* no es proporcionalmente modular" y finalizar.

A continuación justificamos la corrección del Algoritmo 2.26. Supongamos que

$$((x_q,y_q),\dots,(x_{q+r},y_{q+r}))$$

es un segmento de la lista ordenada B' verificando las condiciones en el paso (5) del algoritmo. En tal caso tenemos que $\{x_q,\dots,x_{q+r}\} = \{n_1,\dots,n_p\}$, lo cual significa que se satisfacen las condiciones (1) y (2) de la Proposición 2.25 con $\alpha = \frac{x_q}{y_q}$ y $\beta = \frac{x_{q+r}}{y_{q+r}}$. En consecuencia, $S = T \cap \mathbb{N}$ siendo T el submonoide de $\mathbb{R}_0^+$ generado por el intervalo cerrado $[\frac{x_q}{y_q},\frac{x_{q+r}}{y_{q+r}}]$. Supongamos ahora por el contrario que no se verifican las condiciones en el paso (5) del algoritmo. En tal caso vemos que no existen dos números reales

α y β cumpliendo las condiciones (1) y (2) en la Proposición 2.25. Por el Lema 2.23 concluimos que S no es proporcionalmente modular.

EJEMPLO 2.27. Le aplicamos el Algoritmo 2.26 al semigrupo numérico $S = \langle 4,9,10,11\rangle$. En primer lugar calculamos $\mathrm{EH}(S) = \{5,6,7\}$ y a continuación obtenemos la lista ordenada B'

$$\begin{aligned}((11,10),(10,9),(9,8),(7,6),(6,5),(11,9),(5,4),(10,8),(9,7),(4,3),\\ (11,8),(7,5),(10,7),(6,4),(9,6),(11,7),(5,3),(10,6),(7,4),\\ (9,5),(11,6),(4,2),(6,3),(10,5),(11,5),(9,4),(7,3),(5,2),\\ (10,4),(11,4),(6,2),(9,3),(10,3),(7,2),(11,3),(4,1),(9,2),\\ (5,1),(10,2),(11,2),(6,1),(7,1),(9,1),(10,1),(11,1)).\end{aligned}$$

Se puede comprobar por simple inspección que no existe ningún segmento en B' verificando las condiciones en el paso (5) del algoritmo. Por consiguiente deducimos que S no es proporcionalmente modular. □

Obsérvese que el Algoritmo 2.26 puede ser usado también para determinar todos los semigrupos proporcionalmente modulares que son minimales entre aquellos que contienen a S.

Para el Ejemplo anterior, al analizar la lista ordenada B' encontramos el segmento $((10,3),(7,2),(11,3),(4,1),(9,2))$, lo cual significa que $S\cup\{7\}$ es un semigrupo minimal entre todos los semigrupos proporcionalmente modulares que contienen a S. □

EJEMPLO 2.28. Sea $S = \langle 3,8,10\rangle$. Al igual que antes comenzamos calculando $\mathrm{EH}(S) = \{5,7\}$ y la correspondiente lista ordenada B' en el Algoritmo 2.26:

$$\begin{aligned}((10,9),(8,7),(7,6),(5,4),(10,8),(8,6),(7,5),(10,7),(3,2),(8,5),\\ (5,3),(10,6),(7,4),(8,4),(10,5),(7,3),(5,2),(10,4),(8,3),\\ (3,1),(10,3),(7,2),(8,2),(5,1),(10,2),(7,1),(8,1),(10,1)).\end{aligned}$$

En este caso existen dos segmentos en B' verificando los requisitos del paso (5). Concretamente son $((10,7),(3,2),(8,5))$ y $((8,3),(3,1),(10,3))$. Por consiguiente S es proporcionalmente modular y $S = T_1\cap\mathbb{N} = T_2\cap\mathbb{N}$ siendo T_1 y T_2 los submonoides de $\mathbb{R}_0^+$ generados por los intervalos cerrados $[10/7,8/5]$ y $[8/3,10/3]$, respectivamente. Observar que de acuerdo con el Teorema 2.18 tenemos $S = \langle 3,8,10\rangle = \langle 8,9,10\rangle/3$.

Además el Algoritmo 2.26 puede ser utilizado para obtener todos los posibles intervalos cerrados $[\alpha,\beta]$ para los cuales se cumple que $S = \mathbb{N}\cap T$, siendo T el submonoide de $\mathbb{R}_0^+$ generado por el intervalo cerrado $[\alpha,\beta]$. De manera más precisa para el ejemplo que estamos considerando, ha de cumplirse que el par ordenado (α,β) pertenezca al conjunto $((7/5,10/7]\times[8/5,5/3))\cup((5/2,8/3]\times[10/3,7/2))$.

Podemos utilizar esta información para decidir si S es o no un semigrupo modular. Tal y como indicamos tras el Comentario 2.14, S es modular si y sólo si es posible elegir α y β de modo que $\alpha = b/a$ y $\beta = b/(a-1)$, siendo a y b dos enteros positivos con $b > a > 1$. Pueden ocurrir dos casos:

(a) $7/5 < b/a \leq 10/7$ y $8/5 \leq b/(a-1) < 5/3$, o equivalentemente, $5/7 < a/b \leq 7/10$ y $8/5 \leq b/(a-1) < 5/3$. Multiplicando ambas desigualdades término a término, deducimos que $28/25 \leq a/(a-1) < 25/21$, lo cual implica que $7 \leq a < 9$. Se puede comprobar que para cualquier valor de a verificando dicha inecuación, es decir para $a \in \{7,8\}$, el sistema original de desigualdades es incompatible.

(b) $5/2 < b/a \leq 8/3$ y $10/3 \leq b/(a-1) < 7/2$. Para este caso, procediendo de forma análoga al caso anterior obtenemos que $a \in \{4,5\}$, y al igual que antes el sistema de desigualdades es incompatible.

En vista de estos resultados, conluimos que S no es modular (comparar este método con el dado en el Capítulo 1; véase el Ejemplo 1.27). □

Decimos que un semigrupo numérico S es un **sistema proporcionalmente modular**, si existen enteros positivos $a_1, b_1, c_1, \ldots, a_r, b_r, c_r$ de forma que

$$S = \left\{ x \in \mathbb{N} \;\middle|\; \begin{array}{c} a_1 x \bmod b_1 \leq c_1 x \\ \vdots \\ a_r x \bmod b_r \leq c_r x \end{array} \right\},$$

es decir, cuando S es la intersección de un número finito de semigrupos proporcionalmente modulares. Dentro de poco veremos que existen semigrupos numéricos que son un sistema proporcionalmente modular pero no son proporcionalmente modulares.

Además existen semigrupos numéricos que no son un sistema proporcionalmente modular. Esta conclusión se deduce del siguiente argumento similar al que usamos en su momento con los semigrupos sistema modulares. Recordemos que un semigrupo numérico se dice irreducible si no puede ser expresado como la intersección de dos semigrupos numéricos que lo contienen propiamente. En [**35**] se probó que S es irreducible si y sólo si S es simétrico ó pseudo-simétrico. Se puede comprobar fácilmente que el semigrupo $S = \langle 4,6,7 \rangle$ es simétrico y por tanto es irreducible. Por consiguiente S no puede ser expresado como la intersección de semigrupos numéricos que lo contienen propiamente. Ésto en particular implica que si S es un sistema proporcionalmente modular, entonces S ha de ser proporcionalmente modular. Pero usando el Algoritmo 2.26 veremos que S no es proporcionalmente modular, y por tanto tampoco puede ser un sistema proporcionalmente modular (véase el Ejemplo 2.31).

A continuación damos un algoritmo para decidir cuándo un semigrupo numérico dado es o no un sistema proporcionalmente modular.

ALGORITMO 2.29.

ENTRADA: un sistema de generadores $\{n_1, \ldots, n_p\}$ para un semigrupo numérico $S \neq \mathbb{N}$.

SALIDA: "*S es un sistema proporcionalmente modular*" ó "*S no es un sistema proporcionalmente modular*".

1. Calcular $\mathrm{EH}(S)$.
2. Hacer $A = (\mathrm{EH}(S) \setminus \{1\}) \cup \{n_1, \ldots, n_p\}$.
3. Hacer $B = \{(a, k_a) \mid a \in A, k_a \in \{1, \ldots, a-1\}\}$.

4. Ordenar los elementos de B de modo que $(a,k_a) \leq (a',k_{a'})$ si y sólo si $a/k_a < a'/k_{a'}$, ó $a/k_a = a'/k_{a'}$ y $a < a'$. Sea $B' = ((x_1,y_1),\ldots,(x_m,y_m))$ la lista ordenada resultante.
5. Para cada segmento $l = ((x_q,y_q),\ldots,(x_{q+r},y_{q+r}))$ de elementos consecutivos en B' tal que $\frac{x_{q-1}}{y_{q-1}} \neq \frac{x_q}{y_q}$, $\frac{x_{q+r}}{y_{q+r}} \neq \frac{x_{q+r+1}}{y_{q+r+1}}$ y $\{n_1,\ldots,n_p\} \subseteq \{x_q,\ldots,x_{q+r}\}$, sea $C_l = \{x_q,\ldots,x_{q+r}\}$.
6. Si $\cap C_l = \{n_1,\ldots,n_p\}$, entonces devolver "$S$ es un sistema proporcionalmente modular" y finalizar.
7. En caso contrario, devolver "S no es un sistema proporcionalmente modular" y finalizar.

LEMA 2.30. *El Algoritmo 2.29 es correcto.*

DEMOSTRACIÓN. Sea $S = \langle n_1,\ldots,n_p\rangle$ un semigrupo numérico no trivial. Si $l = ((x_q,y_q),\ldots,(x_{q+r},y_{q+r}))$ es un segmento de la lista ordenada B' verificando las condiciones impuestas en el paso (5) del Algoritmo 2.29 y T_l es el submonoide de $\mathbb{R}_0^+$ generado por el intervalo cerrado $[\frac{x_q}{y_q},\frac{x_{q+r}}{y_{q+r}}]$, entonces $S_l = T_l \cap \mathbb{N}$ es un semigrupo proporcionalmente modular tal que $S \subseteq S \cup C_l \subseteq S_l$.

Observamos que si $S' \neq \mathbb{N}$ es un semigrupo proporcionalmente modular que contiene a S, entonces por el Lema 2.23 sabemos que $S' = T \cap \mathbb{N}$ siendo T un submonoide de $\mathbb{R}_0^+$ generado por un intervalo cerrado $[\alpha,\beta]$ con $1 < \alpha < \beta$. Además, la inclusión $S \subseteq S'$ conlleva que la condición (1) en las Proposiciones 2.24 y 2.25 se satisfaga para el intervalo cerrado $[\alpha,\beta]$. Ésto implica que ha de existir un segmento $l = ((x_q,y_q),\ldots,(x_{q+r},y_{q+r}))$ en la lista B' tal que $[\frac{x_q}{y_q},\frac{x_{q+r}}{y_{q+r}}] \subseteq [\alpha,\beta]$, y por tanto $S_l \subseteq S'$.

Sean $l_1,\ldots,l_r$ los segmentos de B' encontrados tras la ejecución del paso (5) en el algoritmo. Entonces se verifica que $S \subseteq \bigcap_{i=1}^r (S \cup C_{l_i}) = S \cup (\bigcap_{i=1}^r C_{l_i}) \subseteq \bigcap_{i=1}^r S_{l_i}$. Como consecuencia del párrafo anterior tenemos que S es un sistema proporcionalmente modular si y sólo si $S = \bigcap_{i=1}^r S_{l_i}$. Ahora probamos que este hecho es a su vez equivalente a $\bigcap_{i=1}^r C_{l_i} = \{n_1,\ldots,n_r\}$. Supongamos que $S \neq \bigcap_{i=1}^r S_{l_i}$. Entonces $x = \max((\bigcap_{i=1}^r S_{l_i}) \setminus S) \in \mathrm{EH}(S)$ y en particular $x \in S_{l_i}$ para todo $i \in \{1,\ldots,r\}$. Por tanto para cualquier i, si $l_i = ((x_q,y_q),\ldots,(x_{q+r},y_{q+r}))$, entonces existe $k_i \in \mathbb{N}$ tal que $x/k_i \in [\frac{x_q}{y_q},\frac{x_{q+r}}{y_{q+r}}]$, lo cual implica que $x \in C_{l_i}$. Deducimos pues que $x \in \bigcap_{i=1}^r C_{l_i}$ y por consiguiente que $\bigcap_{i=1}^r C_{l_i} \neq \{n_1,\ldots,n_r\}$. Para concluir, si suponemos ahora que $S = \bigcap_{i=1}^r S_{l_i}$, entonces $S = S \cup \bigcap_{i=1}^r C_{l_i}$ lo cual conlleva que $\bigcap_{i=1}^r C_{l_i} \subseteq S$. Por la definición de los conjuntos C_{l_i}, ésto implica que $\bigcap_{i=1}^r C_{l_i} = \{n_1,\ldots,n_r\}$. Por tanto hemos probado la corrección del Algoritmo 2.29. □

EJEMPLO 2.31. Sea el semigrupo numérico $S = \langle 4,6,7\rangle$. Veamos en primer lugar que S no es proporcionalmente modular. Comenzamos calculando $\mathrm{EH}(S) = \{9\}$ y a continuación la lista ordenada B':

$$((9,8),(7,6),(6,5),(9,7),(4,3),(7,5),(6,4),(9,6),(7,4),(9,5),(4,2),(6,3),$$
$$(9,4),(7,3),(6,2),(9,3),(7,2),(4,1),(9,2),(6,1),(7,1),(9,1)).$$

Vemos que no hay ningún segmento de B' cumpliendo las condiciones del paso (5) del Algoritmo 2.26. Hacemos notar que el segmento $(4,3),(7,5),(6,4)$ queda invalidado pues justo a continuación aparece el elemento $(9,6)$ y $\frac{6}{4}=\frac{9}{6}$.

Tal y como comentamos más arriba, al ser S irreducible y no ser proporcionalmente modular, ésto implica que S no puede ser un sistema proporcionalmente modular. Obtengamos ahora esta misma conclusión aplicando el Algoritmo 2.29. Observemos que todos los conjuntos C_l en el paso (5) siempre contienen al entero 9 y por consiguiente $9 \in \cap C_l \setminus \{4,6,7\}$. Por tanto en este caso el Algoritmo 2.29 devuelve "S no es un sistema proporcionalmente modular". □

EJEMPLO 2.32. Para $S=\langle 4,9,10,11\rangle$ ya hemos calculado en el Ejemplo 2.27 la correspondiente lista ordenada B'. Consideremos los siguientes segmentos de B':

$$l_1=((11,9),(5,4),(10,8),(9,7),(4,3)) \text{ y}$$
$$l_2=((4,3),(11,8),(7,5),(10,7),(6,4),(9,6)).$$

Resulta que $C_{l_1}\cap C_{l_2}=\{4,9,10,11\}$, lo cual implica que el conjunto $\cap C_l$ en el paso (6) del Algoritmo 2.29 es precisamente $\{4,9,10,11\}$, por lo que S es un sistema proporcionalmente modular. Es inmediato comprobar que $\mathrm{S}_{l_1}=\mathrm{S}([\frac{11}{9},\frac{4}{3}])=\{0,4,5,8,\rightarrow\}=\langle 4,5,11\rangle$ y $\mathrm{S}_{l_2}=\mathrm{S}([\frac{4}{3},\frac{9}{6}])=\{0,3,4,6,\rightarrow\}=\langle 3,4\rangle$, y así $S=\mathrm{S}_{l_1}\cap \mathrm{S}_{l_2}$. □

4. Una familia de semigrupos proporcionalmente modulares

En esta sección definimos una familia de semigrupos numéricos y probamos que son proporcionalmente modulares. Dicha familia contiene a los semigrupos numéricos de dos generadores y más generalmente a los semigrupos numéricos generados por progresiones aritméticas.

LEMA 2.33. *Sean a,b,c y d enteros positivos tales que* $\mathrm{mcd}\{a,b\}=1$, *y sea* $S=\{\lambda a+\mu b \mid \lambda,\mu\in\mathbb{N}$ *and* $\mu\leq\frac{c}{d}\lambda\}$. *Entonces S es un semigrupo numérico.*

DEMOSTRACIÓN. Claramente $0\in S$. Si $x,y\in S$, sabemos que existen $\lambda_1,\lambda_2,\mu_1,\mu_2\in\mathbb{N}$ verificando que $\mu_i\leq\frac{c}{d}\lambda_i$ para cada $i\in\{1,2\}$ de forma que $x=\lambda_1 a+\mu_1 b$ e $y=\lambda_2 a+\mu_2 b$. Entonces $x+y=(\lambda_1+\lambda_2)a+(\mu_1+\mu_2)b$ y $\mu_1+\mu_2\leq\frac{c}{d}(\lambda_1+\lambda_2)$, lo cual significa que $x+y\in S$. Ésto demuestra que S es un semigrupo. Para ver que S es un semigrupo numérico, es suficiente probar que existen dos elementos $x,y\in S$ los cuales son primos relativos. Sea $\lambda\in\mathbb{N}$ verificando que $1\leq\frac{c}{d}\lambda$. En tal caso $\lambda a+b\in S$. Puesto que $a=1\cdot a+0\cdot b\in S$ y por hipótesis $\mathrm{mcd}\{a,b\}=1$, deducimos que $\mathrm{mcd}\{a,\lambda a+b\}=1$, con lo que se concluye la demostración. □

TEOREMA 2.34. *Sean a,b,c y d enteros positivos tales que* $\mathrm{mcd}\{a,b\}=1$, *y sea* $S=\{\lambda a+\mu b \mid \lambda,\mu\in\mathbb{N}$ *and* $\mu\leq\frac{c}{d}\lambda\}$. *Entonces S es un semigrupo proporcionalmente modular.*

DEMOSTRACIÓN. Ya sabemos por el Lema 2.33 que S es un semigrupo numérico. El que $\mathrm{mcd}\{a,b\}=1$, nos asegura que existe $k\in\mathbb{N}$ tal que $kb\equiv 1 \bmod a$. Demostramos que $S=\{x\in\mathbb{N}\mid k(ad+cb)x \bmod (ad+cb)a\leq cx\}$, lo cual por el Teorema 2.13

significa que S es proporcionalmente modular. Sea $x \in S$. Entonces existen $\lambda, \mu \in \mathbb{N}$ tal que $\mu \leq \frac{c}{d}\lambda$ y $x = \lambda a + \mu b$. Ésto implica que $\mu b \equiv x \bmod a$, lo cual equivale a $\mu \equiv kx \bmod a$. De aquí deducimos que $\mu = (kx \bmod a) + ta$ con $t \in \mathbb{N}$, y por tanto que $x = \lambda a + ((kx \bmod a) + ta)b$. Despejando, resulta

$$\lambda = \frac{x - ((kx \bmod a) + ta)b}{a} \leq \frac{x - (kx \bmod a)b}{a},$$

siendo la desigualdad de la derecha obvia. Ya que por hipótesis estamos suponiendo que $\mu \leq \frac{c}{d}\lambda$, utilizando la expresión que hemos deducido más arriba para μ y la desigualdad anterior para λ, se llega a

$$kx \bmod a \leq \frac{c}{d} \cdot \frac{x - (kx \bmod a)b}{a}.$$

Ésto último implica que $ad(kx \bmod a) \leq cx - cb(kx \bmod a)$ y consecuentemente que $(ad + cb)(kx \bmod a) \leq cx$. Por el Lema 2.6 ésto equivale a $(ad + cb)kx \bmod (ad + cb)a \leq cx$. Veamos ahora el recíproco. Sea $x \in \mathbb{N}$ verificando que $k(ad + cb)x \bmod (ad + cb)a \leq cx$. Ésta condición, por el Lema 2.6 equivale a $(ad + cb)(kx \bmod a) \leq cx$. Por otra parte, observamos que

$$x = \frac{x - (kx \bmod a)b}{a}a + (kx \bmod a)b$$

(de hecho, esta identidad se verifica para cualquier número entero x). Puesto que $(kx \bmod a)b \equiv x(\bmod a)$, deducimos que $\frac{x-(kx \bmod a)b}{a} \in \mathbb{Z}$. Sean $\lambda = \frac{x-(kx \bmod a)b}{a}$ y $\mu = kx \bmod a$. Resulta pues que $x = \lambda a + \mu b$. Para concluir la demostración, tenemos que comprobar que $\mu \leq \frac{c}{d}\lambda$, es decir,

$$kx \bmod a = \mu \leq \frac{c}{d}\lambda = \frac{c}{d} \cdot \frac{x - (kx \bmod a)b}{a},$$

lo cual es inmediato en vista de la hipótesis $(ad + cb)(kx \bmod a) \leq cx$. □

COROLARIO 2.35. *Sean a, b y c enteros positivos tales que* $\mathrm{mcd}\{a, b\} = 1$. *Entonces $S = \langle a, a + b, a + 2b, \ldots, a + cb\rangle$ es un semigrupo numérico proporcionalmente modular.*

DEMOSTRACIÓN. Es inmediato comprobar que $S = \{\lambda a + \mu b \mid \lambda, \mu \in \mathbb{N} \text{ y } \mu \leq c\lambda\}$. Aplicando el Teorema 2.34, deducimos que S es proporcionalmente modular. □

Como consecuencia del Teorema 2.34 obtenemos la siguiente propiedad.

COROLARIO 2.36. *Todo semigrupo numérico generado por dos elementos es un semigrupo modular.*

DEMOSTRACIÓN. Sean a y b dos números enteros positivos y primos relativos y sea $S = \langle a, a + b\rangle$. Entonces $S = \{\lambda a + \mu b \mid \lambda, \mu \in \mathbb{N} \text{ and } \mu \leq \lambda\}$. Si k es un número natural verificando que $kb \equiv 1(\bmod a)$, entonces a partir de la demostración del Teorema 2.34, haciendo $c = d = 1$, deducimos que $S = \{x \in \mathbb{N} \mid (a + b)kx \bmod a(a + b) \leq x\}$ y por tanto S es un semigrupo modular. □

COROLARIO 2.37. *Sea S un semigrupo numérico. Entonces S es proporcionalmente modular si y sólo si existen enteros positivos a, c y p tal que*

$$S = \left\{ x \in \mathbb{N} \mid x = \lambda\frac{a}{p} + \mu\frac{1}{p},\ \textit{con } \lambda, \mu \in \mathbb{N} \textit{ y } \mu \leq c\lambda \right\}.$$

DEMOSTRACIÓN.

Condición necesaria. Por el Teorema 2.18, sabemos que existe un semigrupo aritmético $A = \langle a, a+1, \ldots, a+c \rangle$ y un entero positivo p tal que $S = A/p$. Por la demostración del Corolario 2.35 deducimos que $A = \{\lambda a + \mu \cdot 1 \mid \lambda, \mu \in \mathbb{N} \text{ y } \mu \leq c\lambda\}$. Puesto que $S = A/p$, tenemos que $x \in S$ si y sólo si $px \in A$. Por consiguiente $S = \{x \in \mathbb{N} \mid x = \lambda\frac{a}{p} + \mu\frac{1}{p} \text{ con } \lambda, \mu \in \mathbb{N} \text{ y } \mu \leq c\lambda\}$.

Condición suficiente. A partir de la igualdad

$$S = \left\{ x \in \mathbb{N} \mid x = \lambda\frac{a}{p} + \mu\frac{1}{p},\ \text{con } \lambda, \mu \in \mathbb{N} \text{ y } \mu \leq c\lambda \right\},$$

resulta claro que $S = A/p$, siendo $A = \langle a, a+1, \ldots, a+c \rangle$. Por el Teorema 2.18, deducimos que S es proporcionalmente modular. □

CAPÍTULO 3

Semigrupos modulares cuyo factor divide al módulo

En este capítulo estudiamos los semigrupos modulares de la forma $S = \mathrm{S}(a, ab)$. Ya que $\mathbb{N} = \mathrm{S}(1, b) = \mathrm{S}(a, a)$, siempre consideraremos que $a, b > 1$. Dado $S = \mathrm{S}(a, ab)$, en la primera sección proporcionamos una descripción de $\mathrm{Ap}(S, \mathrm{m}(S))$ en función de a y b, y como consecuencia obtenemos una fórmula explícita para el número de Frobenius de S. En la sección segunda obtenemos los generadores minimales para S en términos de a y b. A continuación, en la sección tercera estudiamos los pseudo-números de Frobenius para S y caracterizamos cuándo S es simétrico y cuándo S es pseudo-simétrico mediante condiciones aritméticas simples. Finalmente en la sección cuarta presentamos varias familias de semigrupos del tipo considerado y para cada una de ellas calculamos de forma explícita su sistema minimal de generadores así como sus pseudo-números de Frobenius. Los resultados de este capítulo están incluidos en [**41**].

1. El conjunto de Apéry

Veamos en primer lugar que la multiplicidad es fácilmente calculable para los semigrupos considerados.

LEMA 3.1.

$$\mathrm{m}(\mathrm{S}(a, ab)) = b.$$

DEMOSTRACIÓN. Sea $S = \mathrm{S}(a, ab)$. Si $x \in \{1, \ldots, b-1\}$, entonces $ax < ab$ y por tanto $ax \bmod ab = ax > x$, lo que significa que $x \notin S$. Ya que $b \in S$, deducimos que $\mathrm{m}(S) = b$. □

Dado un semigrupo numérico S y un elemento $n \in S \setminus \{0\}$, recordemos que el conjunto de Apéry de n en S es

$$\mathrm{Ap}(S, n) = \{s \in S \mid s - n \notin S\}.$$

Emplearemos la notación $\mathrm{Ap}(S, n) = \{w(0) = 0, w(1), \ldots, w(n-1)\}$, siendo $w(i)$ el menor elemento $s \in S$ que es congruente con i módulo n.

El siguiente resultado es una consecuencia de [**30**, Lema 3.3] y nos da una caracterización de los conjuntos de Apéry a partir de la cual describiremos de forma precisa $\mathrm{Ap}(\mathrm{S}(a, ab))$.

LEMA 3.2. *Sea m un entero positivo y $X = \{0 = w(0), w(1), \ldots, w(m-1)\}$ un subconjunto de $\mathbb{N}$ tal que $i < w(i) \equiv i \bmod m$ para todo $i \in \{1, \ldots, m-1\}$. Sea S el submonoide de $\mathbb{N}$ generado por $X \cup \{m\}$. Entonces S es un semigrupo numérico con*

multiplicidad m. Además, $\mathrm{Ap}(S,m) = X$ *si y sólo si para todo* $i, j \in \{1,\dots,m-1\}$ *existen* $k \in \{0,\dots,m-1\}$ *y* $t \in \mathbb{N}$ *tales que* $w(i)+w(j) = w(k)+tm$.

TEOREMA 3.3. *Sea* $S = \mathrm{S}(a,ab)$. *Entonces*

$$\mathrm{Ap}(S,b) = \{0, k_1 b+1, k_2 b+2, \dots, k_{b-1} b+b-1\},$$

donde $k_i = \lceil (a-1)i/b \rceil$ *para todo* $i \in \{1,\dots,b-1\}$.

DEMOSTRACIÓN. Sea S' el semigrupo numérico generado por el conjunto $\{b, k_1 b+1, \dots, k_{b-1} b+b-1\}$. Al ser $k_i \geq 1$ para todo $i \in \{1,\dots,b-1\}$, vemos que $\mathrm{m}(S') = b$. Además, por la definición de los valores k_i, claramente se verifica que $k_1 \leq \cdots \leq k_{b-1}$ y $k_i + k_j \geq k_{i+j}$ para cualesquiera $i, j \in \{1,\dots,b-1\}$ con $2 \leq i+j \leq b-1$. Aplicando el Lema 3.2 deducimos que $\mathrm{Ap}(S',b) = \{0, k_1 b+1, \dots, k_{b-1} b+b-1\}$. Recordemos que un número entero x pertenece a S' si y sólo si x es mayor o igual que el único elemento en $\mathrm{Ap}(S',b)$ que es congruente con x módulo b, es decir, si y sólo si $x \geq k_{x \bmod b} b + x \bmod b$. Demostremos que $S' = S$. Un entero x pertenece a S' si y sólo si $\lfloor x/b \rfloor \geq k_{x \bmod b}$, lo que equivale a que $\lfloor x/b \rfloor \geq \lceil (a-1)(x \bmod b)/b \rceil$. Esta última condición claramente equivale a $\lfloor x/b \rfloor \geq (a-1)(x \bmod b)/b$, es decir, $\lfloor x/b \rfloor b \geq (a-1)(x \bmod b)$, lo cual se puede escribir como $x - (x \bmod b) \geq (a-1)(x \bmod b)$. Simplificando, resulta $a(x \bmod b) \leq x$, que es lo mismo que $ax \bmod ab \leq x$, siendo ésta la condición que define cuándo un elemento x pertenece a S. □

Como consecuencia de este teorema y teniendo en cuenta el Lema 0.1, deducimos una fórmula para $\mathrm{g}(\mathrm{S}(a,ab))$.

COROLARIO 3.4.

$$\mathrm{g}(\mathrm{S}(a,ab)) = \left\lceil \frac{(b-1)(a-1)}{b} \right\rceil b - 1.$$

Particularizando la fórmula para el número de huecos dada en el Teorema 1.13 para $S = \mathrm{S}(a,ab)$, obtenemos la fórmula:

$$\#\mathrm{H}(\mathrm{S}(a,ab)) = \frac{a(b-1) - (a-1,b) + 1}{2}.$$

COMENTARIO 3.5. Puesto que por el Teorema 3.3 sabemos que $\mathrm{Ap}(\mathrm{S}(a,ab),b) = \{0, k_1 b+1, k_2 b+2, \dots, k_{b-1} b+b-1\}$, siendo $k_i = \lceil (a-1)i/b \rceil$ para todo $i \in \{1,\dots,b-1\}$, aplicando una vez más el Lema 0.1 resulta $\#\mathrm{H}(\mathrm{S}(a,ab)) = \sum_{i=1}^{b-1} \left\lceil \frac{(a-1)i}{b} \right\rceil$, y por tanto

$$\frac{a(b-1) - (a-1,b) + 1}{2} = \sum_{i=1}^{b-1} \left\lceil \frac{(a-1)i}{b} \right\rceil.$$

Notamos además que la expresión $\sum_{i=1}^{b-1} \left\lceil \frac{(a-1)i}{b} \right\rceil$, y por tanto $\#\mathrm{H}(\mathrm{S}(a,ab))$, representa el número de puntos reticulares (es decir, puntos del plano real con ambas coordenadas enteras) que se encuentran en el interior del triángulo rectángulo de vértices $(0,0)$, $(b,0)$ y $(0,a-1)$, contando también aquellos puntos que están sobre la hipotenusa. □

2. Generadores minimales

Si $\{n_0 < n_1 < \cdots < n_p\}$ es el sistema minimal de generadores de S, por el Lema 3.1, tenemos que $n_0 = b$. En esta sección vamos a describir el resto de los generadores minimales para S.

Observar que en general, si S es un semigrupo numérico y $m \in S \setminus \{0\}$, entonces S está generado por $X = (\mathrm{Ap}(S,m) \setminus \{0\}) \cup \{m\} = \{m, w(1), \ldots, w(m-1)\}$. Además, los generadores minimales de S son precisamente los elementos del conjunto $X \setminus (X+X)$.

LEMA 3.6. *Sean x e y dos enteros positivos. Entonces $\lceil x/b \rceil + \lceil y/b \rceil = \lceil (x+y)/b \rceil$ si y sólo si $x \equiv 0 \bmod b$ ó $y \equiv 0 \bmod b$ ó $(x \bmod b) + (y \bmod b) > b$.*

DEMOSTRACIÓN.

Condición necesaria. Supongamos que $\lceil x/b \rceil + \lceil y/b \rceil = \lceil (x+y)/b \rceil$ y además que $x \not\equiv 0 \bmod b$ e $y \not\equiv 0 \bmod b$. Entonces $\lceil x/b \rceil > x/b$ y $\lceil y/b \rceil > y/b$, por lo que $\lceil (x+y)/b \rceil = \lceil x/b \rceil + \lceil y/b \rceil \neq (x+y)/b$ y en consecuencia $x+y \not\equiv 0 \bmod b$. Así pues, $\lceil z/b \rceil = \lfloor z/b \rfloor + 1$ para todo $z \in \{x, y, x+y\}$. Ésto implica que $\lfloor x/b \rfloor + 1 + \lfloor y/b \rfloor + 1 = \lfloor (x+y)/b \rfloor + 1$ y por tanto que $\lfloor x/b \rfloor b + b + \lfloor y/b \rfloor b + b = \lfloor (x+y)/b \rfloor b + b$. Ésto último se escribe de modo equivalente como $x - (x \bmod b) + y - (y \bmod b) + b = x + y - ((x+y) \bmod b)$, de lo cual finalmente deducimos que $(x \bmod b) + (y \bmod b) > b$ pues $(x+y) \bmod b \neq 0$.

Condición suficiente. Es inmediato comprobar el resultado cuando $x \equiv 0 \bmod b$ ó $y \equiv 0 \bmod b$, por lo que suponemos que $x \not\equiv 0 \bmod b$, $y \not\equiv 0 \bmod b$ y $(x \bmod b) + (y \bmod b) > b$. Procediendo como en el párrafo anterior, vemos que es suficiente probar que $\lfloor x/b \rfloor + 1 + \lfloor y/b \rfloor + 1 = \lfloor (x+y)/b \rfloor + 1$. Vemos que esta igualdad se verifica si y sólo si $x - (x \bmod b) + y - (y \bmod b) + b = x + y - ((x+y) \bmod b)$, siendo esto último equivalente a $(x \bmod b) + (y \bmod b) > b$. □

COMENTARIO 3.7. Por el Teorema 3.3 sabemos que $\mathrm{Ap}(S,b) = \{0, k_1 b + 1, \ldots, k_{b-1} b + b - 1\}$ siendo $k_i = \lceil (a-1)i/b \rceil$ para todo $i \in \{1, \ldots, b-1\}$. Teniendo en cuenta la observación hecha en el párrafo que precede al Lema 3.6, vemos que $k_t b + t$ es un generador minimal para S si y sólo si para todo $i \in \{1, \ldots, t-1\}$ se verifica que $k_t \neq k_i + k_{t-i}$. □

Para dos enteros positivos x e y denotamos por $[a,b]$ el mínimo común multiplo de x e y.

LEMA 3.8. *Sean a y b enteros mayores que 1, $S = \mathrm{S}(a, ab)$, $t \in \{1, \ldots, b-1\}$ y $k_i = \lceil (a-1)i/b \rceil$ para todo $i \in \{1, \ldots, b-1\}$.*

1. *Si $t < b/(a-1,b)$, entonces $k_t b + t$ es un generador minimal de S si y sólo si $(a-1)i \bmod b < (a-1)t \bmod b$ para todo $i \in \{1, \ldots, t-1\}$.*
2. *Si $t > b/(a-1,b)$, entonces $k_t b + t$ no es un generador minimal de S.*
3. *Si $t = b/(a-1,b)$, entonces $k_t b + t$ es un generador minimal de S.*

DEMOSTRACIÓN. Basándonos en el Comentario 3.7 y utilizando el Lema 3.6, deducimos que $k_t b + t$ es un generador minimal de S si y sólo si para todo $i \in \{1, \ldots, t -$

1}, se verifica que $(a-1)i \not\equiv 0 \bmod b$ y $(a-1)i \bmod b + (a-1)(t-i) \bmod b \leq b$. Obsérvese además que

$$\frac{b}{(a-1,b)} = \frac{[a-1,b]}{a-1} = \min\{i \mid (a-1)i \bmod b = 0\}. \qquad (*)$$

1. A partir del párrafo anterior deducimos que si $t < b/(a-1,b)$, entonces $k_t b + t$ es un generador minimal de S si y sólo si $(a-1)i \bmod b + (a-1)(t-i) \bmod b \leq b$ para todo $i \in \{1,\ldots,t-1\}$. Si $(a-1)i \bmod b + (a-1)(t-i) \bmod b = b$, entonces $(a-1)t \bmod b = 0$, y ya que estamos suponiendo que $t < b/(a-1,b)$, ésto contradice $(*)$. Por tanto $k_t b + t$ es un generador minimal de S si y sólo si para todo $i \in \{1,\ldots,t-1\}$ se verifica que $(a-1)i \bmod b + (a-1)(t-i) \bmod b < b$, siendo esta condición a su vez equivalente a $(a-1)i \bmod b + (a-1)(t-i) \bmod b = (a-1)t \bmod b$. Al ser $(a-1)(t-i) \bmod b \neq 0$, concluimos que $k_t b + t$ es un generador minimal de S si y sólo si $(a-1)i \bmod b < (a-1)t \bmod b$ para todo $i \in \{1,\ldots,t-1\}$.
2. Sea $i = b/(a-1,b)$. Entonces $(a-1)i \equiv 0 \bmod b$ y en vista del Lema 3.6 obtenemos que $k_i + k_{t-i} = k_t$, lo cual implica que $k_t b + b$ no es un generador minimal de S.
3. Si $t = b/(a-1,b)$, entonces $(a-1)t \bmod b = 0$ y para todo $i \in \{1,\ldots,t-1\}$ se verifica que $(a-1)i \bmod b \neq 0$. De ésto resulta que $(a-1)i \bmod b + (a-1)(t-i) \bmod b = b$ para todo $i \in \{1,\ldots,t-1\}$, y por el Lema 3.6 deducimos que $k_t \neq k_i + k_{t-i}$ para todo $i \in \{1,\ldots,t-1\}$. Por consiguiente $k_t b + t$ es un generador minimal de S.

□

Como consecuencia del Lema 3.8 obtenemos el siguiente resultado que describe explícitamente el sistema minimal de generadores de S.

TEOREMA 3.9. *Sean a y b dos números enteros mayores que* 1, $S = \mathrm{S}(a,ab)$ *y* $k_i = \lceil (a-1)i/b \rceil$ *para todo* $i \in \{1,\ldots,b-1\}$.

1. *Si $(b,a-1) = 1$, entonces el sistema minimal de generadores de S es $\{b, k_{t_1} b + t_1, \ldots, k_{t_r} b + t_r\}$, donde $\{t_1,\ldots,t_r\}$ es igual a*

$$\{t \in \{1,\ldots,b-1\} \mid (a-1)i \bmod b < (a-1)t \bmod b \text{ para todo } i \in \{1,\ldots,t-1\}\}.$$

2. *Si $(b,a-1) \neq 1$, sea $t_{r+1} = b/(b,a-1)$. Entonces el sistema minimal de generadores de S es $\{b, k_{t_1} b + t_1, \ldots, k_{t_r} b + t_r, k_{t_{r+1}} b + t_{r+1}\}$, donde $\{t_1,\ldots,t_r\}$ es igual a*

$$\{t \in \{1,\ldots,t_{r+1}-1\} \mid (a-1)i \bmod b < (a-1)t \bmod b \text{ para todo } i \in \{1,\ldots,t-1\}\}.$$

EJEMPLO 3.10. Sea $S = \mathrm{S}(5,30)$. Aplicando el apartado (1) del Teorema 3.9 con $a = 5$ y $b = 7$, resulta que

- $\{t_1,\ldots,t_r\} = \{1,3,5\}$ (1 siempre pertenece a $\{t_1,\ldots,t_r\}$),
- S está minimalmente generado por $\{7,8,17,26\}$.

□

EJEMPLO 3.11. Sea $S = \mathrm{S}(5,30)$. Aplicando el apartado (2) del Teorema 3.9 con $a = 5$ y $b = 6$, obtenemos que

- $t_{r+1} = 3$,
- $\{t_1, \ldots, t_r\} = \{1\}$,
- S está minimalmente generado por $\{6, 7, 15\}$.

□

COROLARIO 3.12. *Sean a y b números enteros mayores que 1, sea $S = \mathrm{S}(a, ab)$ y $k_i = \lceil (a-1)i/b \rceil$ para todo $i \in \{1, \ldots, b-1\}$.*

1. *Si $(b, a-1) = 1$, sea $t = \min\{x \in \mathbb{N} \mid (a-1)x \equiv b-1 (\bmod b)\}$.*
2. *Si $(b, a-1) \neq 1$, sea $t = b/(b, a-1)$.*

Entonces $k_t b + t$ es el mayor generador minimal de S.

COROLARIO 3.13. *Sean a y b enteros positivos, con $a \geq 3$. Entonces*

$$\mathrm{e}(\mathrm{S}(a, ab)) \geq \lfloor b/(a-1) \rfloor + 1.$$

DEMOSTRACIÓN. Como ya sabemos, el entero b es siempre un generador minimal de $\mathrm{S}(a, ab)$. Observar también que si $(a-1)t \leq b$, entonces por el Lema 3.8, $k_t b + t$ es un generador minimal de S. □

3. Pseudo-números de Frobenius

Dado un semigrupo numérico S, podemos definir la relación de orden $\leq_S$ sobre S como sigue: $a \leq_S b$ si y sólo si $b - a \in S$. Para un subconjunto A de S, el conjunto $\mathrm{Max}_{\leq_S} A$ denota el conjunto de los elementos maximales de A con respecto al orden $\leq_S$. El siguiente resultado aparece en [**34**].

LEMA 3.14. *Sea S un semigrupo numérico con multiplicidad m. Si*

$$\mathrm{Max}_{\leq_S}(\mathrm{Ap}(S, m)) = \{w_{i_1}, \ldots, w_{i_t}\},$$

entonces

$$\mathrm{Pg}(S) = \{w_{i_1} - m, \ldots, w_{i_t} - m\}.$$

Obsérvese que si $w, w' \in \mathrm{Ap}(S, m)$ y $w - w' \in S$, entonces $w - w'$ ha de ser también un elemento de $\mathrm{Ap}(S, m)$. Por tanto

$$\mathrm{Max}_{\leq_S}(\mathrm{Ap}(S, m)) = \{w \in \mathrm{Ap}(S, m) \mid w + w' \notin \mathrm{Ap}(S, m) \text{ para todo } 0 \neq w' \in \mathrm{Ap}(S, m)\}.$$

Sea $S = \mathrm{S}(a, ab)$ para ciertos enteros a y b mayores que 1. Nuestro primer objetivo en esta sección es determinar de forma más exacta el conjunto $\mathrm{Max}_{\leq_S}(\mathrm{Ap}(S, b))$ y así, en vista del Lema 3.14, el conjunto $\mathrm{Pg}(S)$.

COMENTARIO 3.15. Nótese que por el Teorema 3.3, tenemos que $k_i b + i \notin \mathrm{Max}_{\leq_S}(\mathrm{Ap}(S, b))$ si y sólo si existe $j \in \{1, \ldots, b-1\}$ tal que $i + j \leq b - 1$ y $k_i + k_j = k_{i+j}$. □

TEOREMA 3.16. *Sean a y b dos enteros mayores o iguales que* 1, *y sea* $S = \mathrm{S}(a,ab)$. *Sea* $k_i = \lceil (a-1)i/b \rceil$ *para todo* $i \in \{1,\ldots,b-1\}$. *Entonces* $k_i b + i \in \mathrm{Max}_{\leq_S}(\mathrm{Ap}(S,b))$ *si y sólo si se verifica alguna de las siguientes condiciones:*

1. $(a-1)i \equiv 0 \bmod b$ *e* $i = b-1$,
2. $(a-1)i \not\equiv 0 \bmod b$ *y para todo* $t \in \{i+1,\ldots,b-1\}$, $(a-1)i \bmod b < (a-1)t \bmod b$ *ó* $(a-1)t \bmod b = 0$.

DEMOSTRACIÓN.

Condición necesaria. Supongamos en primer lugar que $(a-1)i \equiv 0 \bmod b$ e $i < b-1$. Entonces por el Lema 3.6 deducimos que $k_i + k_1 = k_{i+1}$, y por el Comentario 3.15 concluimos que $k_i b + i \notin \mathrm{Max}_{\leq_S}(\mathrm{Ap}(S,b))$.

Si $(a-1)i \not\equiv 0 \bmod b$, entonces por el Lema 3.6 tenemos que $k_i b_i + i \in \mathrm{Max}_{\leq_S}(\mathrm{Ap}(S,b))$ si y sólo si para todo $t \in \{i+1,\ldots,b-1\}$ se verifica que $(a-1)(t-i) \not\equiv 0 \bmod b$ y $(a-1)i \bmod b + (a-1)(t-i) \bmod b \leq b$. Si $(a-1)i \bmod b + (a-1)(t-i) \bmod b < b$, entonces $(a-1)i \bmod b + (a-1)(t-i) \bmod b = (a-1)t \bmod b$ con lo cual $(a-1)i \bmod b < (a-1)t \bmod b$. Si $(a-1)i \bmod b + (a-1)(t-i) \bmod b = b$, entonces $(a-1)t \bmod b = 0$.

Condición suficiente. Supongamos que $k_i b + i \notin \mathrm{Max}_{\leq_S}(\mathrm{Ap}(S,b))$. Entonces existe $t \in \{1+i,\ldots,b-1\}$ tal que $k_i + k_{t-i} = k_t$. Por el Lema 3.6 deducimos que $(a-1)i \equiv 0 \bmod b$ ó $(a-1)(t-i) \equiv 0 \bmod b$ ó $(a-1)i \bmod b + (a-1)(t-i) \bmod b > b$. Si $(a-1)i \equiv 0 \bmod b$, entonces i debería de ser igual a $b-1$, lo cual es imposible pues $t \in \{i+1,\ldots,b-1\}$. Si $(a-1)(t-i) \equiv 0 \bmod b$, entonces $(a-1)i \bmod b = (a-1)t \bmod b$, lo cual es imposible al contradecir una de las hipótesis. Finalmente, si $(a-1)i \bmod b + (a-1)(t-i) \bmod b > b$, entonces $(a-1)t \bmod b = (a-1)i \bmod b + (a-1)(t-i) \bmod b - b < (a-1)i \bmod b$, lo cual conduce de nuevo a una contradicción. □

EJEMPLO 3.17. Sea $S = \mathrm{S}(5,30)$. Aplicando el Teorema 3.16 deducimos que $\mathrm{Max}_{\leq_S}(\mathrm{Ap}(S,6)) = \{29\}$, lo que por el Lema 3.14 significa que $\mathrm{Pg}(S) = \{23\}$. □

Recordemos que un semigrupo numérico M es simétrico (respectivamente pseudo-simétrico) si y sólo si $\mathrm{Pg}(M) = \{\mathrm{g}(M)\}$ (respectivamente $\mathrm{Pg}(M) = \{\mathrm{g}(M), \mathrm{g}(M)/2\}$); véase por ejemplo [**2, 11**]. Por tanto, en relación con el Ejemplo 3.17, podemos concluir que el semigrupo numérico $\mathrm{S}(5,30)$ es simétrico. De hecho para los semigrupos modulares $S = \mathrm{S}(a,ab)$ que estamos considerando en esta sección es posible decidir mediante un simple test si S es simétrico o pseudo-simétrico. Este es el objeto de la siguiente proposición.

PROPOSICIÓN 3.18. *Sean a y b dos números enteros mayores que* 1 *y sea* $S = \mathrm{S}(a,ab)$.

1. *S es simétrico si y sólo si* $(a-1,b) + (a-1) \bmod b = b$.
2. *S es pseudo-simétrico si y sólo si* $(a-1,b) + (a-1) \bmod b = b-1$.

DEMOSTRACIÓN.

1. Por el apartado (1) del Corolario 1.19 sabemos que S es simétrico si y sólo si $g(S) = ab-a-(a-1,b)$. Aplicando el Corolario 3.4, deducimos que S es simétrico si y sólo si $\lceil (b-1)(a-1)/b \rceil b - 1 = ab-a-(a-1,b)$. Teniendo en cuenta la identidad $\lceil (b-1)(a-1)/b \rceil = a-1-\lfloor (a-1)/b \rfloor$, esto último equivale a $(a-1)b - \lfloor (a-1)/b \rfloor b - 1 = ab-a-(a-1,b)$, ó equivalentemente, $ab-b-(a-1-(a-1) \bmod b)-1 = ab-a-(a-1,b)$. Por tanto S es simétrico si y sólo si $(a-1) \bmod b + (a-1,b) = b$.
2. Mediante un argumento similar al anterior, pero esta vez utilizando el apartado (2) del Corolario 1.19, se demuestra que S es pseudo-simétrico si y sólo si $(a-1) \bmod b + (a-1,b) = b-1$.

□

El siguiente corolario muestra una familia infinita de semigrupos modulares del tipo que estamos considerado los cuales son simétricos.

COROLARIO 3.19. *Sea k un entero positivo y sea b un múltiplo positivo de k. Entonces el semigrupo $S(b-k+1+bn,(b-k+1+bn)b)$ es simétrico para todo $n \in \mathbb{N}$.*

4. Algunas familias

En esta sección presentamos algunas familias de semigrupos numéricos de la forma $S(a,ab)$ con a y b enteros mayores que 1 y verificando además que $(a-1,b) = 1$. En cada caso calculamos explícitamente el sistema minimal de generadores y los pseudo-números de Frobenius.

Particularizando al caso que nos ocupa y como consecuencia de los Teoremas 3.9 y 3.16, tenemos el siguiente resultado.

PROPOSICIÓN 3.20. *Sean a y b dos enteros mayores que 1 verificando que $(a-1,b) = 1$. Sean $S = S(a,ab)$ y $k_i = \lceil (a-1)i/b \rceil$ para todo $i \in \{1,\dots,b-1\}$. Sea además $t \in \{1,\dots,b-1\}$. Entonces*

1. *$k_t b + t$ es un generador minimal de S si y sólo si $(a-1)i \bmod b < (a-1)t \bmod b$ para todo $i \in \{1,\dots,t-1\}$,*
2. *$k_t b + t \in \mathrm{Max}_{\leq_S}(\mathrm{Ap}(S,b))$ si y sólo si $(a-1)t \bmod b < (a-1)i \bmod b$ para todo $i \in \{t+1,\dots,b-1\}$.*

Si x e y son enteros positivos primos relativos, llamamos $\sigma_{x,y}$ a la permutación perteneciente a S_{y-1} tal que $\sigma_{x,y}(i) = (xi) \bmod y$, para todo $i \in \{1,\dots,y-1\}$.

Dada una permutación $\sigma \in S_n$, definimos además

$$E(\sigma) = \{t \in \{1,\dots,n\} \mid \sigma(i) < \sigma(t) \text{ para todo } i \in \{1,\dots,t-1\}\}$$

y

$$T(\sigma) = \{t \in \{1,\dots,n\} \mid \sigma(t) < \sigma(i) \text{ paa todo } i \in \{t+1,\dots,n\}\}.$$

Usando esta nueva notación, la Proposición 3.20 se puede reescribir como sigue.

COROLARIO 3.21. *Sean* $a,b \in \mathbb{N}\setminus\{0,1\}$ *tales que* $(a-1,b)=1$ *y sea* $S=\mathrm{S}(a,ab)$. *Entonces*

1. $\mathrm{e}(\mathrm{S}(a,ab)) = \#\mathrm{E}(\sigma_{a-1,b})+1$,
2. $\mathrm{t}(\mathrm{S}(a,ab)) = \#\mathrm{T}(\sigma_{a-1,b})$.

Además

$$\{b\}\cup\{\lceil (a-1)i/b\rceil b+i \mid i\in \mathrm{E}(\sigma_{a-1,b})\}$$

es el sistema minimal de generadores de $\mathrm{S}(a,ab)$ *y*

$$\mathrm{Max}_{\leq_S}(\mathrm{Ap}(S,b)) = \{\lceil (a-1)i/b\rceil b+i \mid i\in \mathrm{T}(\sigma_{a-1,b})\}.$$

EJEMPLO 3.22. Sea $S=\mathrm{S}(6,42)$. Tenemos que $a=6$, $b=7$ y $(a-1,b)=(5,42)=1$, por lo que aplicamos el Corolario 3.21. Consideramos la permutación modular

$$\sigma_{5,7} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 4 & 2 \end{pmatrix}$$

a partir de la cual obtenemos que $\mathrm{E}(\sigma_{5,7})=\{1,4\}$ y $\mathrm{T}(\sigma_{5,7})=\{3,6\}$. Por tanto $\mathrm{e}(S)=3$ y $\mathrm{t}(S)=2$. Además, el conjunto

$$\{7, \lceil (5\times 1)/7\rceil 7+1, \lceil (5\times 4)/7\rceil 7+4\} = \{7,8,25\}$$

es el sistema minimal de generadores de S y

$$\mathrm{Max}_{\leq_S}(\mathrm{Ap}(S,7)) = \{\lceil (5\times 3)/7\rceil 7+3, \lceil (5\times 6)/7\rceil 7+6\} = \{24,41\}.$$

□

COROLARIO 3.23. *Sea* $n\in\mathbb{N}$ *y sea* b *un entero impar mayor o igual que* 5. *Sea* $S=\mathrm{S}((b-1)+bn,((b-1)+bn)b)$. *Entonces* S *está generado minimalmente por el conjunto*

$$\left\{b,(n+1)b+1,\left(\frac{b-1}{2}+n\frac{b+1}{2}\right)b+\frac{b+1}{2}\right\}$$

y

$$\mathrm{Max}_{\leq_S}(\mathrm{Ap}(S,b)) = \left\{\left(\frac{b-1}{2}+n\frac{b-1}{2}\right)b+\frac{b-1}{2}, ((b-2)+n(b-1))b+b-1\right\}.$$

DEMOSTRACIÓN. Puesto que $(b-2+bn,b)=(b-2,b)=1$, podemos aplicar el Corolario 3.21. Claramente

$$\sigma_{b-2+bn,b}=\sigma_{b-2,b}=\begin{pmatrix} 1 & 2 & \cdots & \frac{b-1}{2} & \frac{b+1}{2} & \frac{b+3}{2} & \cdots & b-1 \\ b-2 & b-4 & \cdots & 1 & b-1 & b-3 & \cdots & 2 \end{pmatrix},$$

$\mathrm{E}(\sigma_{b-2,b})=\{1,(b+1)/2\}$ y $\mathrm{T}(\sigma_{b-2,b})=\{(b-1)/2,b-1\}$. Por el Corolario 3.21 y teniendo en cuenta que

$$\left\lceil\frac{((b-2)+bn)1}{b}\right\rceil = n+1,\ \left\lceil\frac{((b-2)+bn)\frac{b\pm1}{2}}{b}\right\rceil = \frac{b-1}{2}+n\frac{b\pm1}{2},$$

$$\text{y}\ \left\lceil\frac{((b-2)+bn)(b-1)}{b}\right\rceil = (b-2)+n(b-1),$$

concluimos la demostración. □

COROLARIO 3.24. *Sea b un número entero mayor o igual que 2 y sea $n \in \mathbb{N}$. Entonces el semigrupo $S = \mathrm{S}((n+1)b, (n+1)b^2)$ está minimalmente generado por $\{b, (n+1)b+1\}$ y $\mathrm{Max}_{\leq_S}(\mathrm{Ap}(S,b)) = \{(n+1)(b-1)b+b-1\}$.*

DEMOSTRACIÓN. Bastar aplicar simplemente el Corolario 3.21 teniendo en cuenta que

$$\sigma_{(n+1)b-1,b} = \sigma_{b-1,b} = \begin{pmatrix} 1 & 2 & \cdots & b-1 \\ b-1 & b-2 & \cdots & 1 \end{pmatrix}.$$

□

COROLARIO 3.25. *Sea b un entero mayor o igual que 2 y sea $n \in \mathbb{N}$. Entonces el semigrupo $S = \mathrm{S}(2+nb, (2+nb)b)$ está minimalmente generado por*

$$X = \{b, (n+1)b+1, (2n+1)b+2, \ldots, ((b-1)n+1)b+b-1\}$$

y $\mathrm{Max}_{\leq_S}(\mathrm{Ap}(S,b)) = X \setminus \{b\}$.

DEMOSTRACIÓN. A partir de las hipótesis resulta que $\sigma_{1+nb,b} = \sigma_{1,b}$ es la aplicación identidad, por lo que $\mathrm{E}(\sigma_{1,b}) = \mathrm{T}(\sigma_{1,b}) = \{1, \ldots, b-1\}$. A continuación, basta aplicar el Corolario 3.21. □

COROLARIO 3.26. *Sea b un entero impar mayor o igual que 3 y sea $n \in \mathbb{N}$. Entonces $S = \mathrm{S}(3+nb, (3+nb)b)$ está minimalmente generado por*

$$\left\{b, (n+1)b+1, (2n+1)b+2, \ldots, \left(\frac{b-1}{2}n+1\right) + \frac{b-1}{2}\right\}$$

y

$$\mathrm{Max}_{\leq_S}(\mathrm{Ap}(S,b)) = \left\{\left(\frac{b+1}{2}n+2\right)b + \frac{b+1}{2}, \ldots, ((b-1)n+2)b+b-1\right\}.$$

DEMOSTRACIÓN. De las hipótesis resulta

$$\sigma_{2+bn,b} = \sigma_{2,b} = \begin{pmatrix} 1 & 2 & \cdots & \frac{b-1}{2} & \frac{b+1}{2} & \frac{b+3}{2} & \cdots & b-1 \\ 2 & 4 & \cdots & b-1 & 1 & 3 & \cdots & b-2 \end{pmatrix},$$

$\mathrm{E}(\sigma_{2,b}) = \{1, \ldots, (b-1)/2\}$ y $\mathrm{T}(\sigma_{2,b}) = \{(b+1)/2, \ldots, b-1\}$. La prueba concluye teniendo en cuenta que

$$\left\lceil \frac{(2+bn)i}{b} \right\rceil b = \begin{cases} (ni+1)b+i & \text{si } i \leq \frac{b-1}{2}, \\ (ni+2)b+i & \text{si } i \geq \frac{b+1}{2}, \end{cases}$$

y usando el Corolario 3.21. □

CAPÍTULO 4

Semigrupos proporcionalmente modulares y secuencias de Bézout

En la primera sección introducimos el concepto de secuencia de Bézout, el cual será de gran ayuda para el estudio de los semigrupos proporcionalmente modulares. El resultado principal en esta sección es el Teorema 4.4 según el cual dos fracciones racionales positivas se pueden conectar siempre mediante una secuencia de Bézout. En la segunda sección asociamos a cada secuencia de Bézout un semigrupo proporcionalmente modular y probamos que los numeradores que aparecen en dicha secuencia son un sistema de generadores para dicho semigrupo. Como consecuencia obtenemos un método para resolver inecuaciones diofánticas proporcionalmente modulares. En la tercera sección definimos condiciones sobre las secuencias de Bézout para que sus numeradores constituyan un sistema minimal de generadores para el semigrupo numérico asociado. Concretamente, definimos el concepto de secuencia de Bézout propia y secuencia de Bézout de extremos adyacentes. Vemos cómo tales condiciones determinan ciertas propiedades de tipo aritmético para las secuencias de Bézout. El resultado principal en esta sección es el Teorema 4.21 según el cual el hecho de que una secuencia de Bézout propia tenga extremos adyacentes equivale a que sus numeradores sean precisamente el sistema minimal de generadores para el semigrupo proporcionalmente modular asociado. En la sección cuarta damos resultados que caracterizan cuándo un semigrupo numérico es proporcionalmente modular en términos de sus generadores minimales (véase el Teorema 4.32 y el Corolario 4.35). Cerramos este capítulo estudiando los semigrupos proporcionalmente modulares cuya dimensión de inmersión es igual a tres. Como resultado obtenemos fórmulas para el número de Frobenius y para el número de huecos de tales semigrupos. Incluso particularizamos dichas expresiones en el caso en el que tales semigrupos además sean simétricos.

Los resultados en este capítulo están incluidos en [**42**].

1. Secuencias de Bézout

Una **secuencia de Bézout** es una secuencia creciente formada por dos o más números racionales $\frac{a_1}{b_1} < \frac{a_2}{b_2} < \cdots < \frac{a_p}{b_p}$ tal que $a_1,\ldots,a_p,b_1,\ldots,b_p$ son números enteros positivos y $b_i a_{i+1} - b_{i+1}a_i = 1$ para todo $i \in \{1,\ldots,p-1\}$.

Decimos que p es la **longitud**, $\frac{a_1}{b_1}$ y $\frac{a_p}{b_p}$ son los **extremos** y $b_1a_p - b_pa_1$ es el **producto cruzado** de dicha secuencia.

El siguiente resultado se puede considerar como una versión más detallada del Lema 2.16.

LEMA 4.1. *Sean a_1, a_2, b_1, b_2, x e y enteros positivos tales que $\frac{a_1}{b_1} < \frac{a_2}{b_2}$. Entonces $\frac{a_1}{b_1} < \frac{x}{y} < \frac{a_2}{b_2}$ si y sólo si $\frac{x}{y} = \frac{\lambda a_1 + \mu a_2}{\lambda b_1 + \mu b_2}$ para ciertos $\lambda, \mu \in \mathbb{N} \setminus \{0\}$.*

DEMOSTRACIÓN.

Condición necesaria. Si se verifica $\frac{a_1}{b_1} < \frac{x}{y} < \frac{a_2}{b_2}$, entonces no es difícil ver que el par ordenado (x,y) pertenece al cono positivo generado por los pares ordenados (a_1,b_1) y (a_2,b_2). Por tanto existen números racionales positivos $\frac{p_1}{q_1}$ y $\frac{p_2}{q_2}$ tales que $(x,y) = \frac{p_1}{q_1}(a_1,b_1) + \frac{p_2}{q_2}(a_2,b_2)$. Ésto implica $q_1q_2x = p_1q_2a_1 + p_2q_1a_2$ y $q_1q_2y = p_1q_2b_1 + p_2q_1b_2$ y en consecuencia $\frac{x}{y} = \frac{q_1q_2x}{q_1q_2y} = \frac{p_1q_2a_1 + p_2q_1a_2}{p_1q_2b_1 + p_2q_1b_2}$.

Condición suficiente. Se sigue del hecho de que para cualesquiera enteros positivos a, b, c y d, si $\frac{a}{b} < \frac{c}{d}$, entonces $\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}$. □

Para $a, b \in \mathbb{N} \setminus \{0\}$, denotamos por (a,b) el máximo común divisor de a y b.

El objetivo de esta sección es demostrar el Teorema 4.4, el cual afirma que para dos números racionales positivos cualesquiera $r < s$, siempre se puede construir una secuencia de Bézout de extremos r y s. En este sentido, el siguiente resultado establece el paso básico para llevar a cabo tales contrucciones.

LEMA 4.2. *San a_1, a_2, b_1 y b_2 enteros positivos tales que $\frac{a_1}{b_1} < \frac{a_2}{b_2}$ y $(a_1,b_1) = 1$. Entonces existen $x, y \in \mathbb{N} \setminus \{0\}$ verificando que $\frac{a_1}{b_1} < \frac{x}{y} < \frac{a_2}{b_2}$ y $b_1x - a_1y = 1$.*

DEMOSTRACIÓN. Puesto que $(a_1,b_1) = 1$, la ecuación en congruencia $a_1y \equiv -1 \bmod b_1$ tiene infinitas soluciones positivas para y. Observar que $b_1x - a_1y = 1$ si y sólo si $x = \frac{1+a_1y}{b_1}$, por lo que $\frac{x}{y} = \frac{1+a_1y}{b_1y} = \frac{a_1}{b_1} + \frac{1}{b_1y}$. Por tanto existe un número entero positivo y suficientemente grande que verifica la congruencia $a_1y \equiv -1 \bmod b_1$ y además se cumple $\frac{a_1}{b_1} + \frac{1}{b_1y} < \frac{a_2}{b_2}$. Llamando $x = 1 + a_1y$, resulta que $\frac{a_1}{b_1} < \frac{x}{y} < \frac{a_2}{b_2}$. □

Siguiendo con la notación del lema anterior, entre todas las elecciones posibles para x e y, nos quedaremos con una que nos permita aplicar el método de inducción para demostrar el Teorema 4.4.

LEMA 4.3. *Sean a_1, a_2, b_1 y b_2 enteros positivos tales que $\frac{a_1}{b_1} < \frac{a_2}{b_2}$, $(a_1,b_1) = (a_2,b_2) = 1$ y $a_2b_1 - a_1b_2 = d > 1$. Entonces existe $t \in \mathbb{N}$, verificando que $1 \le t < d$ y $(ta_1 + a_2, tb_1 + b_2) = d$.*

DEMOSTRACIÓN. Por el Lema 4.2, existen $x, y \in \mathbb{N}$ cumpliendo que $\frac{a_1}{b_1} < \frac{x}{y} < \frac{a_2}{b_2}$ y $b_1x - a_1y = 1$. Además por el Lema 4.1, tenemos que $\frac{x}{y} = \frac{\lambda a_1 + \mu a_2}{\lambda b_1 + \mu b_2}$ para ciertos números $\lambda, \mu \in \mathbb{N} \setminus \{0\}$. Como $b_1x - a_1y = 1$, deducimos que $(x,y) = 1$ y por tanto que $x = \frac{\lambda a_1 + \mu a_2}{(\lambda a_1 + \mu a_2, \lambda b_1 + \mu b_2)}$ e $y = \frac{\lambda b_1 + \mu b_2}{(\lambda a_1 + \mu a_2, \lambda b_1 + \mu b_2)}$. Substituyendo estos valores en la igualdad $b_1x - a_1y = 1$, deducimos que $(\lambda a_1 + \mu a_2, \lambda b_1 + \mu b_2) = \mu(a_2b_1 - a_1b_2) = \mu d$. En particular obtenemos que $\mu \mid \lambda a_1 + \mu a_2$ y $\mu \mid \lambda b_1 + \mu b_2$, y de aquí $\mu \mid \lambda a_1$ y $\mu \mid \lambda b_1$. Usando la hipótesis $(a_1,b_1) = 1$, llegamos a que $\mu \mid \lambda$. Sea $\alpha = \frac{\lambda}{\mu} \in \mathbb{N} \setminus \{0\}$. Por tanto resulta $d = (\alpha a_1 + a_2, \alpha b_1 + b_2)$.

Obsérvese que si $d=(a,b)$, entonces $d \mid (a-kd, b-\bar{k}d)$ para cualesquiera $k,\bar{k}\in\mathbb{N}$. Aplicando este hecho, deducimos que si $t=\alpha \bmod d$, entonces $d \mid (ta_1+a_2, tb_1+b_2)$. Además se verifica $b_1\frac{ta_1+a_2}{d}-a_1\frac{tb_1+b_2}{d}=\frac{b_1a_2-a_1b_2}{d}=\frac{d}{d}=1$, lo que significa que $(\frac{ta_1+a_2}{d},\frac{tb_1+b_2}{d})=1$ y por tanto $(ta_1+a_2,tb_1+b_2)=d$.

Finalmente, ya que por definición $t=\alpha \bmod d$, tenemos $t<d$; además $t\neq 0$, pues $(a_2,b_2)=1\neq d$. □

Ya estamos en condiciones de demostrar el principal resultado de esta sección.

TEOREMA 4.4. *Sean $a_1,\ a_2,\ b_1$ y b_2 enteros positivos verificando que $\frac{a_1}{b_1}<\frac{a_2}{b_2}$, $(a_1,b_1)=(a_2,b_2)=1$ y $a_2b_1-a_1b_2=d$. Entonces existe una secuencia de Bézout de extremos $\frac{a_1}{b_1}$ y $\frac{a_2}{b_2}$ y de longitud menor o igual que $d+1$.*

DEMOSTRACIÓN. Lo demostraremos por inducción sobre d. Cuando $d=1$ el resultado es trivial. Supongamos como hipótesis de inducción que el enunciado del teorema se verifica para todo número entero k tal que $1\leq k<d$. En primer lugar, por el Lema 4.3, sabemos que existe un entero positivo t verificando que $1\leq t<d$ y $(ta_1+a_2,tb_1+b_2)=d$. Sean $x_1=\frac{ta_1+a_2}{d}$ e $y_1=\frac{tb_1+b_2}{d}$. Entonces $\frac{x_1}{y_1}=\frac{ta_1+a_2}{tb_1+b_2}$. Por el Lema 4.1 tenemos $\frac{a_1}{b_1}<\frac{x_1}{y_1}<\frac{a_2}{b_2}$. Además se cumple que $b_1x_1-a_1y_1=b_1\frac{ta_1+a_2}{d}-a_1\frac{tb_1+b_2}{d}=\frac{b_1a_2-a_1b_2}{d}=\frac{d}{d}=1$ y $a_2y_1-b_2x_1=a_2\frac{tb_1+b_2}{d}-b_2\frac{ta_1+a_2}{d}=\frac{t(a_2b_1-a_1b_2)}{d}=\frac{td}{d}=t<d$. Aplicando la hipótesis de inducción a las fracciones $\frac{x_1}{y_1}<\frac{a_2}{b_2}$, deducimos que existe una secuencia de Bézout $\frac{x_1}{y_1}<\frac{x_2}{y_2}<\cdots<\frac{x_s}{y_s}<\frac{a_2}{b_2}$ con $s\leq t$. Por tanto, $\frac{a_1}{b_1}<\frac{x_1}{y_1}<\frac{x_2}{y_2}<\cdots<\frac{x_s}{y_s}<\frac{a_2}{b_2}$ es una secuencia de Bézout de longitud menor o igual que $t+2\leq d+1$. □

Ilustremos el proceso de construcción dado en este teorema mediante un ejemplo.

EJEMPLO 4.5. Vamos a construir una secuencia Bézout cuyos extremos sean las fracciones $13/3$ y $6/1$. Como $13/3<6/1$, el producto cruzado de dicha secuencia es $d=5$ y por tanto existe $t\in\{1,\ldots,4\}$ tal que $(13t+6,3t+1)=5$. El valor $t=3$ satisface dicha condición, por lo que podemos "intercalar" la fracción $\frac{3\times 13+6}{3\times 3+1}=9/2$ entre $13/3$ y $6/1$. Ahora repetimos el mismo proceso con $9/2<6/1$. Obtenemos $d=3$ y $(1\times 9+6,1\times 2+1)=3$. Por consiguiente insertamos la fracción $\frac{9+6}{2+1}=\frac{5}{1}$ entre $9/6$ y $6/1$. Finalmente para $5/1<6/1$, tenemos que $d=1$ con lo que el proceso acaba. Así pues, una secuencia de Bézout con los extremos dados es

$$\frac{13}{3}<\frac{9}{2}<\frac{5}{1}<\frac{6}{1}.$$

Observamos que es posible encontrar infinitas secuencias Bézout para dos extremos dados. Para ello, basta observar que si $\frac{a}{b}<\frac{c}{d}$ es una secuencia de Bézout, entonces también lo es $\frac{a}{b}<\frac{a+c}{b+d}<\frac{c}{d}$. □

2. El semigrupo proporcionalmente modular asociado a una secuencia de Bézout

Comenzamos observando que si n_i y n_j son los numeradores de dos fracciones consecutivas en una secuencia de Bézout dada, entonces n_i y n_j son primos relativos. Por tanto a toda secuencia de Bézout le podemos asociar un semigrupo numérico, que es el semigrupo generado por los numeradores que aparecen en sus fracciones. En esta sección demostramos el Teorema 4.8 que esencialmente afirma que los numeradores de las fracciones que forman una secuencia de Bézout generan un semigrupo proporcionalmente modular.

En primer lugar comenzamos considerando las secuencias de Bézout más simples que son aquellas que tienen longitud dos.

De la demostración del Corolario 2.36 obtenemos el siguiente resultado.

LEMA 4.6. *Sean $a<b$ enteros positivos tales que $(a,b)=1$ y sea u un entero tal que $ub\equiv 1 \bmod a$. Entonces*

$$\langle a,b\rangle = \mathrm{S}(ub,ab).$$

A partir de este resultado demostramos este otro.

LEMA 4.7. *Sean a, b, u y v enteros positivos verificando que $bu-av=1$. Entonces* $\langle a,b\rangle = \mathrm{S}([\frac{a}{u},\frac{b}{v}])$.

DEMOSTRACIÓN. Observemos en primer lugar que si $a=b$, entonces ya que $bu-av=1$, ha de ocurrir que $a=1$ y $u=v+1$. En este caso, usando el Lema 2.16, obtenemos fácilmente que $\mathrm{S}([1/(v+1),1/v])=\mathbb{N}$.

Si $a<b$, entonces por el Lema 4.6 sabemos que $\langle a,b\rangle = \mathrm{S}(ub,ab)$. Aplicando el Lema 2.15 resulta que $\langle a,b\rangle$ es el semigrupo proporcionalmente modular definido por el intevalo cerrado $[\frac{ab}{bu},\frac{ab}{bu-1}]$. De las hipótesis deducimos que $[\frac{ab}{bu},\frac{ab}{bu-1}]=[\frac{ab}{bu},\frac{ab}{av}]=[\frac{a}{u},\frac{b}{v}]$, por lo que $\langle a,b\rangle=\mathrm{S}([\frac{a}{u},\frac{b}{v}])$.

Finalmente, si $b<a$, entonces aplicando una vez más el Lema 4.6 obtenemos que

$$\langle b,a\rangle = \{x\in\mathbb{N} \mid kax \bmod ab \leq x\},$$

siendo k un entero positivo tal que $ka\equiv 1 \bmod b$ y $k<b$, y por tanto que $ka<ab$. Sea $t\in\mathbb{N}\setminus\{0\}$ tal que $ka=1+tb$. Por el Lema 1.3,

$$\langle b,a\rangle = \{x\in\mathbb{N} \mid (ab+1-ka)x \bmod ab \leq x\} = \{x\in\mathbb{N} \mid b(a-t)x \bmod ab \leq x\}.$$

Observar que $b(a-t)\equiv bu \bmod ab$, pues $bu+bt=1+av-1+ka$. Este último valor es un múltiplo de a y b, y como además $(a,b)=1$, deducimos que también es múltiplo de ab. Por tanto

$$\langle b,a\rangle = \{x\in\mathbb{N} \mid bux \bmod ab \leq x\}.$$

Argumentando como en el párrafo anterior, concluimos la demostración. □

En vista de la demostración del Lema 4.7, nos damos cuenta a posteriori de que la hipótesis "$a<b$" que aparece en el Lema 4.6 es superflua.

Ahora ya podemos demostrar el resultado general para secuencias de Bézout de longitud arbitraria.

TEOREMA 4.8. *Sea* $\frac{a_1}{b_1} < \frac{a_2}{b_2} < \cdots < \frac{a_p}{b_p}$ *una secuencia de Bézout. Entonces*

$$\langle a_1, \ldots, a_p \rangle = \mathrm{S}\Big(\Big[\frac{a_1}{b_1}, \frac{a_p}{b_p}\Big]\Big).$$

DEMOSTRACIÓN. Sea $S = \mathrm{S}([\frac{a_1}{b_1}, \frac{a_p}{b_p}])$. Por el Lema 2.16 deducimos que $\{a_1, \ldots, a_p\} \subseteq S$, y por tanto $\langle a_1, \ldots, a_p \rangle \subseteq S$. Demostremos que la otra inclusión también se verifica. Si $x \in S \setminus \{0\}$, entonces de nuevo por el Lema 2.16 sabemos que existe un entero positivo y tal que $\frac{a_1}{b_1} \leq \frac{x}{y} \leq \frac{a_p}{b_p}$. Así pues existe $i \in \{1, \ldots, p-1\}$ de forma que $\frac{a_i}{b_i} \leq \frac{x}{y} \leq \frac{a_{i+1}}{b_{i+1}}$, con lo cual x pertenece a $S([\frac{a_i}{b_i}, \frac{a_{i+1}}{b_{i+1}}])$ (Lema 2.16 otra vez). Por tanto hemos reducido la situación al caso de longitud dos que ya hemos estudiado en el Lema 4.7. Ésto implica que $x \in \langle a_i, a_{i+1} \rangle \subseteq \langle a_1, \ldots, a_p \rangle$. □

Ahora ilustraremos mediante algunos ejemplos cómo el Teorema 4.8 puede emplearse para calcular todas las soluciones de una inecuación diofántica proporcionalmente modular.

EJEMPLO 4.9. Sea S el conjunto de todas las soluciones enteras de la inecuación diofántica

$$12x \bmod 32 \leq 3x.$$

En primer lugar, por el Lema 2.15 sabemos que $S = \mathrm{S}([\frac{32}{12}, \frac{32}{12-3}])$. De acuerdo con el Teorema 4.4, es posible construir una secuencia de Bézout con extremos $\frac{8}{3}$ y $\frac{32}{9}$. Obtenemos la secuencia de Bézout $\frac{8}{3} < \frac{3}{1} < \frac{7}{2} < \frac{32}{9}$. Por último, aplicando el Teorema 4.8, concluimos que

$$\mathrm{S}(12, 32, 3) = \{x \in \mathbb{N} \mid 12x \bmod 32 \leq 3x\} = \langle 8, 3, 7, 21 \rangle = \langle 3, 7, 8 \rangle.$$

□

EJEMPLO 4.10. Obtengamos el conjunto completo de soluciones en $\mathbb{N}$ de $10x \bmod 85 \leq 2x$.

Llamamos $a = 10$, $b = 85$, $c = 2$ y $S = \mathrm{S}\Big(\Big[\frac{b}{a}, \frac{b}{a-c}\Big]\Big) = \mathrm{S}\Big(\Big[\frac{17}{2}, \frac{85}{8}\Big]\Big)$.

Por tanto, hemos de encontrar una secuencia de Bézout de extremos $\frac{17}{2}$ y $\frac{85}{8}$.

Por el Teorema 4.4 obtenemos la secuencia de Bézout

$$\frac{17}{2} < \frac{9}{1} < \frac{10}{1} < \frac{21}{2} < \frac{53}{5} < \frac{85}{8},$$

y por el Teorema 4.8 resulta que $S = \langle 17, 9, 10, 21, 53, 85 \rangle$.

El sistema minimal de generadores de S es $\{9, 10, 17, 21\}$, por lo cual

$$\mathrm{S}(10, 85, 2) = \{x \in \mathbb{N} \mid 10x \bmod 85 \leq 2x\} =$$

$$\{9\lambda_1 + 10\lambda_2 + 17\lambda_3 + 21\lambda_4 \mid \lambda_1, \lambda_2, \lambda_3, \lambda_4 \in \mathbb{N}\}.$$

□

El siguiente resultado establece una cota superior para la dimensión de inmersión de un semigrupo proporcionalmente modular en términos de los extremos del intervalo que lo define.

COROLARIO 4.11. *Sean a_1, a_2, b_1 y b_2 enteros positivos tales que $(a_1, b_1) = (a_2, b_2) = 1$ y sea $S = \mathrm{S}([\frac{a_1}{b_1}, \frac{a_2}{b_2}])$. Entonces* $\mathrm{e}(S) \leq a_2 b_1 - a_1 b_2 + 1$.

DEMOSTRACIÓN. De acuerdo con el Teorema 4.4, existe una secuencia de Bézout $\frac{a_1}{b_1} < \frac{x_1}{y_1} < \cdots < \frac{x_s}{y_s} < \frac{a_2}{b_2}$ con $s + 2 \leq a_2 b_1 - a_1 b_2 + 1$. Por el Teorema 4.8, también sabemos que $S = \langle a_1, x_1, \ldots, x_s, a_2 \rangle$, por lo que $\mathrm{e}(S) \leq a_2 b_1 - a_1 b_2 + 1$. □

EJEMPLO 4.12. La secuencia $\frac{5}{3} < \frac{12}{7} < \frac{7}{4} < \frac{9}{5}$ es de Bézout. El Teorema 4.8 nos asegura que $S = \mathrm{S}([\frac{5}{3}, \frac{9}{5}])$ está generado por $\{5, 7, 9, 12\}$. Es inmediato comprobar que $\mathrm{e}(S) = 3$, por lo que la cota dada en el Corolario 4.11 para $\mathrm{e}(S)$ es alcanzable. □

3. Secuencias de Bézout propias

Como hemos visto en el Teorema 4.8, los numeradores que aparecen en las fracciones de una secuencia de Bézout generan un semigrupo proporcionalmente modular. Ahora estamos interesados en obtener los sistemas minimales de generadores para dichos semigrupos. Concretamente, definimos condiciones sobre secuencias de Bézout las cuales nos garantizan que el conjunto de los numeradores que aparecen en dichas fracciones constituye un conjunto independiente.

LEMA 4.13. *Sea $\frac{a}{u} < \frac{b}{v} < \frac{c}{w}$ una secuencia de Bézout y sea $d = cu - aw$. Entonces $b = \frac{a+c}{d}$.*

DEMOSTRACIÓN. Por ser una secuencia de Bezout, sabemos que $ub - va = 1$ y $vc - wb = 1$. Despejando v en ambas expresiones e igualando, obtenemos $\frac{ub-1}{a} = \frac{wb+1}{c}$, lo cual equivale a $b(uc - wa) = a + c$, es decir, $bd = a + c$. □

Como consecuencia de este lema, tenemos que si $\frac{a_1}{b_1} < \frac{a_2}{b_2} < \frac{a_3}{b_3}$ y $\frac{a_1}{b_1} < \frac{a_3}{b_3}$ son ambas secuencias de Bézout, entonces $a_2 \in \langle a_1, a_3 \rangle$. Esta observación motiva la siguiente definición.

Una **secuencia de Bézout** $\frac{a_1}{b_1} < \frac{a_2}{b_2} < \cdots < \frac{a_p}{b_p}$ es **propia** si $a_{i+h} b_i - a_i b_{i+h} \geq 2$ para todo $h \geq 2$ tal que $i, i + h \in \{1, \ldots, p\}$.

En una secuencia de Bézout $\mathcal{S}_1$, si tras suprimir algunas fracciones la secuencia resultante $\mathcal{S}_2$ sigue siendo de Bézout, entonces decimos que $\mathcal{S}_1$ se ha refinado a $\mathcal{S}_2$, o que $\mathcal{S}_2$ es un **refinamiento** de $\mathcal{S}_1$.

COMENTARIO 4.14. Observar que toda secuencia de Bézout puede ser refinada a una secuencia de Bézout propia de modo que ambas tengan los mismos extremos. □

EJEMPLO 4.15. Sea la secuencia de Bézout

$$\frac{14}{11} < \frac{23}{18} < \frac{32}{25} < \frac{9}{7} < \frac{4}{3} < \frac{15}{11} < \frac{11}{8}.$$

Como las secuencias $\frac{14}{11} < \frac{9}{7}$ y $\frac{4}{3} < \frac{11}{8}$ son de Bézout, resulta que

$$\frac{14}{11} < \frac{9}{7} < \frac{4}{3} < \frac{11}{8},$$

es una secuencia de Bézout propia. □

El hecho de que una secuencia de Bézout sea propia no es suficiente para garantizar que el conjunto de los numeradores que aparecen en sus fracciones sea un conjunto independiente. Basta considerar la secuencia de Bézout propia $\frac{2}{1} < \frac{3}{1} < \frac{4}{1}$ cuyo conjunto de numeradores $\{2,3,4\}$ no es independiente.

Nuestro próximo objetivo será el Teorema 4.21. Antes damos algunos resultados previos necesarios para la demostración de este teorema, y que exhiben algunas propiedades aritméticas relacionadas con las secuencias de Bézout propias. Comenzamos demostrando que el máximo de los numeradores siempre se alcanza en uno de los extremos.

LEMA 4.16. *Sea $\frac{a_1}{b_1} < \frac{a_2}{b_2} < \cdots < \frac{a_p}{b_p}$ una secuencia de Bézout propia. Entonces*

$$\text{máx}\{a_1, a_2, \ldots, a_p\} = \text{máx}\{a_1, a_p\}.$$

DEMOSTRACIÓN. Razonamos por inducción sobre p. Cuando $p = 2$, la afirmación es trivialmente cierta. Supongamos como hipótesis de inducción que la propiedad se verifica para toda secuencia de Bézout propia de longitud $p-1$. Al ser $\frac{a_2}{b_2} < \cdots < \frac{a_p}{b_p}$ de nuevo una secuencia de Bézout propia, por la hipótesis de inducción deducimos que $\text{máx}\{a_2, \ldots, a_p\} = \text{máx}\{a_2, a_p\}$. A continuación vamos a probar que $\text{máx}\{a_1, \ldots, a_p\} = \text{máx}\{a_1, a_p\}$. Si $\text{máx}\{a_2, a_p\} = a_p$, entonces la propiedad se verifica trivialmente. Supongamos que $\text{máx}\{a_2, a_p\} = a_2$. Si aplicamos el Lema 4.13 a la secuencia de Bézout $\frac{a_1}{b_1} < \frac{a_2}{b_2} < \frac{a_3}{b_3}$, obtenemos que $a_2 = \frac{a_1 + a_3}{a_3 b_1 - a_1 b_3}$, y al ser ésta una secuencia de Bézout propia, ha de verificarse que $a_3 b_1 - a_1 b_3 \geq 2$. Por consiguiente $a_2 \leq \frac{a_1 + a_3}{2} \leq \frac{2\,\text{máx}\{a_1, a_3\}}{2}$. Distinguimos dos casos dependiendo del valor de $\text{máx}\{a_1, a_3\}$.

- Si $\text{máx}\{a_1, a_3\} = a_3$, entonces deducimos que $a_2 \leq a_3$. Puesto que $\text{máx}\{a_2, \ldots, a_p\} = a_2$, ésto implica que $a_2 = a_3$. Al ser $\frac{a_2}{b_2} < \frac{a_3}{b_3}$ una secuencia de Bézout y $a_2 = a_3$, obtenemos que $a_2(b_2 - b_3) = 1$, y en particular $a_2 = 1$. Como $a_1 \geq 1$, finalmente concluimos que $\text{máx}\{a_1, \ldots, a_p\} = a_1$.
- Si $\text{máx}\{a_1, a_3\} = a_1$, entonces $a_2 \leq a_1$, y la conclusión se obtiene fácilmente.

□

A su vez, como consecuencia de este resultado, tenemos que los numeradores de las fracciones de una secuencia de Bézout están ordenados de una forma especial.

COROLARIO 4.17. *Sea $\frac{a_1}{b_1} < \frac{a_2}{b_2} < \cdots < \frac{a_p}{b_p}$ una secuencia de Bézout propia. Entonces $a_1, \ldots, a_p$ es una secuencia convexa, es decir, existe $h \in \{1, \ldots, p\}$ tal que*

$$a_1 \geq a_2 \geq \cdots \geq a_h \leq a_{h+1} \leq \cdots \leq a_p.$$

En [**26**] se analiza totalmente la estructura de las secuencias de Bézout cuya secuencia de numeradores es decreciente así como aquellas cuya secuencia de denominadores es creciente.

Se comienza viendo que dados dos enteros positivos a_1 y b_1 verificando que $a_1 \geq b_1 \geq 1$ y $\mathrm{mcd}\{a_1,b_1\} = 1$, si $\frac{a_1}{b_1} < \frac{a_2}{b_2} < \cdots < \frac{a_p}{b_p}$ es una secuencia de Bézout tal que $a_1 \geq a_2 \geq \cdots \geq a_p$, entonces los numeradores así como los denominadores están determinados de forma única mediante las expresiones $a_{i+1} = (-a_{i-1}) \bmod a_i$ y $b_{i+1} = (-b_{i-1}) \bmod b_i$ para todo $i \in \{2,\ldots,p-1\}$.

Teniendo en cuenta que $\frac{a_1}{b_1} < \frac{a_2}{b_2} < \cdots < \frac{a_p}{b_p}$ es una secuencia de Bézout si y sólo si $\frac{a_p}{a_p-b_p} < \cdots < \frac{a_1}{a_1-b_1}$ también lo es, ésto permite obtener un resultado análogo al anterior:

Sea $\frac{a_p}{b_p} < \cdots < \frac{a_2}{b_2} < \frac{a_1}{b_1}$ una secuencia de Bézout tal que $a_1 \geq a_2 \geq \cdots \geq a_p$ y $\frac{a_p}{b_p} \geq 1$. Entonces para todo $i \in \{2,\ldots,p\}$ y supuesto que $b_i \neq 1$, se verifica que $a_{i+1} = (-a_{i-1}) \bmod a_i$ y $b_{i+1} = (-b_{i-1}) \bmod b_i$.

Como consecuencia en [**26**] se obtiene una versión más fuerte del Teorema 4.4 la cual incluimos a continuación.

TEOREMA 4.18. *Sean a,b,c y d enteros positivos tales que* $\mathrm{mcd}\{a,b\} = \mathrm{mcd}\{c,d\} = 1$ *y* $\frac{a}{b} < \frac{c}{d}$. *Entonces existe una única secuencia de Bézout propia con extremos* $\frac{a}{b}$ *y* $\frac{c}{d}$.

Resulta pues que toda secuencia de Bézout propia se puede obtener concatenando una secuencia de Bézout de numeradores decrecientes con una secuencia de Bézout de numeradores crecientes. Se obtiene así un método efectivo para encontrar la única secuencia de Bézout propia con dos extremos dados y por tanto un método para resolver cualquier inecuación diofántica proporcionalmente modular (veáse [**26**]).

Decimos que dos **fracciones** $\frac{a_1}{b_1} < \frac{a_2}{b_2}$ son **adyacentes** si

$$\frac{a_2}{b_2+1} < \frac{a_1}{b_1}, \text{ y si } b_1 \neq 1, \text{ entonces } \frac{a_2}{b_2} < \frac{a_1}{b_1-1}.$$

EJEMPLO 4.19. La secuencia de Bézout $\frac{13}{3} < \frac{9}{2} < \frac{5}{1} < \frac{6}{1}$ es propia y tiene extremos adyacentes. Sin embargo la secuencia de Bézout $\frac{13}{3} < \frac{9}{2} < \frac{5}{1} < \frac{6}{1} < \frac{7}{1}$, aunque es propia, no tiene extremos adyacentes. Ésto es debido (tal y como veremos en el Teorema 4.21) a que la fracción con numerador $13 = 6+7$ es supérflua. Si eliminamos dicha fracción, obtenemos una secuencia de Bézout propia con extremos adyacentes. □

Hemos llegado pues al concepto clave en esta sección, es decir, el concepto de **secuencia de Bézout propia de extremos adyacentes**. Como veremos dentro de poco, la adyacencia de los extremos será esencial en la demostración del Teorema 4.21 para asegurar la independencia de los numeradores. Antes, damos un lema técnico.

LEMA 4.20. *Si* $\frac{a_1}{b_1} < \frac{a_2}{b_2}$ *es una secuencia de Bézout de extremos adyacentes, entonces* $1 \notin \{a_1,a_2\}$.

DEMOSTRACIÓN. Supongamos que $a_1 = 1$. Entonces $1 = a_2b_1 - a_1b_2 = a_2b_1 - b_2$. Al ser las dos fracciones adyacentes, $\frac{a_2}{b_2+1} < \frac{1}{b_1}$, de donde $a_2b_1 < b_2 + 1$, lo cual es contradictorio con $a_2b_1 = b_2 + 1$.

Supongamos ahora que $a_2 = 1$. Obsérvese que en este contexto ha de ser $b_1 \neq 1$, pues de lo contrario $\frac{a_1}{1} < \frac{1}{b_2}$ y por tanto $a_1b_2 < 1$. De nuevo, por la adyacencia tenemos $\frac{1}{b_2} < \frac{a_1}{b_1-1}$ y de aquí $b_1 - 1 < a_1b_2$. Pero ésto es imposible pues $1 = a_2b_1 - a_1b_2 = b_1 - a_1b_2$. □

TEOREMA 4.21. *Sea $\frac{a_1}{b_1} < \frac{a_2}{b_2} < \cdots < \frac{a_p}{b_p}$ una secuencia de Bézout propia. Entonces los extremos $\frac{a_1}{b_1}$ y $\frac{a_p}{b_p}$ son adyacentes si y sólo si $\{a_1, \ldots, a_p\}$ es un conjunto independiente.*

DEMOSTRACIÓN. Supongamos que los extremos $\frac{a_1}{b_1}$ y $\frac{a_p}{b_p}$ son adyacentes. Demostramos por inducción sobre p que el conjunto $\{a_1, \ldots, a_p\}$ es independiente. Si $p = 2$, al ser $\frac{a_1}{b_1} < \frac{a_2}{b_2}$ secuencia de Bézout, deducimos que $(a_1, a_2) = 1$ y por el Lema 4.20 tenemos que a_1 y a_2 son ambos números enteros mayores o iguales que 2. Por tanto $\{a_1, a_2\}$ es independiente y la propiedad se verifica para $p = 2$.

Supongamos como hipótesis de inducción que para toda secuencia de Bézout propia, de longitud $p-1$ y con extremos adayentes, el conjunto de sus numeradores es independiente. Por el Lema 4.16, sabemos que $\max\{a_1, \ldots, a_p\} = \max\{a_1, a_p\}$. Distinguimos dos casos según el valor de $\max\{a_1, a_p\}$.

- Supongamos que $\max\{a_1, \ldots, a_p\} = a_1$. Obviamente $\frac{a_2}{b_2} < \cdots < \frac{a_p}{b_p}$ es una secuencia de Bézout propia. Veamos que los extremos de dicha secuencia son adyacentes. Resulta claro que $\frac{a_p}{b_p+1} < \frac{a_2}{b_2}$. Nótese también que $b_1 \neq 1$, pues de lo contrario la desigualdad $\frac{a_1}{1} < \frac{a_2}{b_2}$ implicaría que $a_2 > a_1$, contradiciendo que $a_1 = \max\{a_1, \ldots, a_p\}$. De las desigualdades $a_1b_2 < a_2b_1$ y $a_2 \leq a_1$, obtenemos que $a_1b_2 - a_1 < a_2b_1 - a_2$. Por tanto, si $b_2 \neq 1$, tenemos que $\frac{a_p}{b_p} < \frac{a_1}{b_1-1} < \frac{a_2}{b_2-1}$. Ésto demuestra que $\frac{a_2}{b_2} < \cdots \frac{a_p}{b_p}$ es una secuencia de Bézout propia y con extremos adyacentes. Aplicando la hipótesis de inducción deducimos que el conjunto $\{a_2, \ldots, a_p\}$ es independiente. Como estamos suponiendo que $a_1 = \max\{a_1, \ldots, a_p\}$, para demostrar que el conjunto $\{a_1, \ldots, a_p\}$ es independiente, es suficiente probar que $a_1 \notin \langle a_2, \ldots, a_p \rangle$. Por el Teorema 4.8 sabemos que $\langle a_2, \ldots, a_p \rangle = \mathrm{S}([\frac{a_2}{b_2}, \frac{a_p}{b_p}])$. Por tanto, si $a_1 \in \langle a_2, \ldots, a_p \rangle$, entonces por el Lema 2.16 existe un entero positivo y tal que $\frac{a_2}{b_2} \leq \frac{a_1}{y} \leq \frac{a_p}{b_p}$. Ésto implica que $\frac{a_1}{b_1-1} \leq \frac{a_1}{y} \leq \frac{a_p}{b_p}$, lo cual contradice que $\frac{a_1}{b_1}$ y $\frac{a_p}{b_p}$ son fracciones adyacentes.
- Si $\max\{a_1, \ldots, a_p\} = a_p$, entonces la demostración es similar a la del caso anterior pero ahora usando que $\frac{a_1}{b_1} < \cdots < \frac{a_{p-1}}{b_{p-1}}$ es una secuencia de Bézout propia de extremos adyacentes.

Recíprocamente, supongamos ahora que el conjunto de los numeradores $\{a_1,\dots,a_p\}$ es independiente. Si los extremos $\frac{a_1}{b_1}$ y $\frac{a_p}{b_p}$ de la secuencia de Bézout $\frac{a_1}{b_1} < \frac{a_2}{b_2} < \cdots < \frac{a_p}{b_p}$ no son adyacentes, es porque $\frac{a_1}{b_1} \leq \frac{a_p}{b_p+1}$ ó bien $\frac{a_1}{b_1-1} \leq \frac{a_p}{b_p}$ si $b_1 > 1$. Supongamos que $b_1 > 1$ y $\frac{a_1}{b_1-1} \leq \frac{a_p}{b_p}$. Entonces existe $i \in \{1,\dots,p-1\}$ tal que $\frac{a_i}{b_i} < \frac{a_1}{b_1-1} < \frac{a_{i+1}}{b_{i+1}}$. Si $i = 1$, tenemos $\frac{a_1}{b_1} < \frac{a_1}{b_1-1} < \frac{a_2}{b_2}$, y ya que $\frac{a_1}{b_1} < \frac{a_2}{b_2}$ es secuencia de Bézout, ésto implica que $(b_1-1)a_2 - b_2a_1 = 1 - a_2 < 0$, lo que es absurdo. Si $i > 1$, por el Lema 4.7 deducimos que $a_1 \in \mathrm{S}([\frac{a_i}{b_i}, \frac{a_{i+1}}{b_{i+1}}]) = \langle a_i, a_{i+1}\rangle$ lo que contradice la hipótesis de que $\{a_1,\dots,a_p\}$ sea un conjunto independiente. El otro caso es análogo. □

COMENTARIO 4.22. Observamos que en el teorema anterior, la condición $p \leq \text{mín}\{a_1,a_2,\dots,a_p\}$ no puede reemplazar a la condición de que los extremos de la secuencia dada sean adyacentes. Basta considerar la secuencia de Bézout $\frac{17}{5} < \frac{7}{2} < \frac{4}{1} < \frac{9}{2}$, la cual aunque es propia, tiene un conjunto de numeradores que no es independiente. □

4. Teorema de estructura para los semigrupos proporcionalmente modulares

Nuestro objetivo en esta sección es probar el Teorema 4.32 el cual da una caracterización para los semigrupos proporcionalmente modulares en términos de sus generadores minimales. Antes damos algunos resultados previos, entre los que destacamos el Teorema 4.24.

LEMA 4.23. *Sea S un semigrupo proporcionalmente modular. Entonces existen dos generadores minimales n_1 y n_p de S así como enteros positivos b_1 y b_p de modo que $S = \mathrm{S}([\frac{n_1}{b_1}, \frac{n_p}{b_p}])$, siendo además las fracciones $\frac{n_1}{b_1}$ y $\frac{n_p}{b_p}$ adyacentes.*

DEMOSTRACIÓN. Sean α y β dos números racionales positivos tales que $\alpha < \beta$ y $S = \mathrm{S}([\alpha,\beta])$. Por el Lema 2.16, si n es un generador minimal de S, existe un entero positivo x tal que $\alpha \leq \frac{n}{x} \leq \beta$. Observar que $(n,x) = 1$, puesto que si $(n,x) = d \neq 1$, entonces $\alpha \leq \frac{n/d}{x/d} \leq \beta$, lo que significaría que $\frac{n}{d}$ pertenece a S, contradiciendo que n es un generador minimal de S. Sea $a(n) = \text{máx}\{x \in \mathbb{N}\setminus\{0\} \mid \alpha \leq \frac{n}{x}\}$. Si n_i y n_j son dos generadores minimales de S distintos, entonces $\frac{n_i}{a(n_i)} \neq \frac{n_j}{a(n_j)}$, ya que $(n_i, a(n_i)) = (n_j, a(n_j)) = 1$. Por tanto existe una ordenación $n_1,\dots,n_p$ de los generadores minimales de S tal que $\alpha \leq \frac{n_1}{a(n_1)} < \frac{n_2}{a(n_2)} < \cdots < \frac{n_p}{a(n_p)} \leq \beta$. Para cualquier $i \in \{1,\dots,p-1\}$, sea $b(n_i) = \text{mín}\{x \in \mathbb{N}\setminus\{0\} \mid \frac{n_i}{x} \leq \frac{n_p}{a(n_p)}\}$. Entonces existe una permutación σ del conjunto $\{1,\dots,p-1\}$ tal que

$$\alpha \leq \frac{n_{\sigma(1)}}{b(n_{\sigma(1)})} < \frac{n_{\sigma(2)}}{b(n_{\sigma(2)})} < \cdots < \frac{n_{\sigma(p-1)}}{b(n_{\sigma(p-1)})} < \frac{n_p}{a(n_p)} \leq \beta.$$

Nótese que $\alpha \leq \frac{n_{\sigma(1)}}{a(n_{\sigma(1)})} \leq \frac{n_{\sigma(1)}}{b(n_{\sigma(1)})}$ puesto que $b(n_{\sigma(1)}) \leq a(n_{\sigma(1)})$. Además se verifica que $\frac{n_p}{a(n_p)+1} < \alpha$ debido a la maximalidad de $a(n_p)$. Así pues $\frac{n_p}{a(n_p)+1} < \frac{n_{\sigma(1)}}{b(n_{\sigma(1)})}$. Por otra

parte, de la definición de $b(n_{\sigma(1)})$ observamos que si $b(n_{\sigma(1)}) \neq 1$, entonces $\frac{n_p}{a(n_p)} < \frac{n_{\sigma(1)}}{b(n_{\sigma(1)})-1}$.

Para concluir la demostración, es suficiente probar que S es igual al semigrupo numérico $\overline{S} = \mathrm{S}([\frac{n_{\sigma(1)}}{b(n_{\sigma(1)})}, \frac{n_p}{a(n_p)}])$. Como $[\frac{n_{\sigma(1)}}{b(n_{\sigma(1)})}, \frac{n_p}{a(n_p)}] \subseteq [\alpha, \beta]$, tenemos que $\overline{S} \subseteq S$. En vista de la secuencia $\frac{n_{\sigma(1)}}{b(n_{\sigma(1)})} < \frac{n_{\sigma(2)}}{b(n_{\sigma(2)})} < \cdots < \frac{n_{\sigma(p-1)}}{b(n_{\sigma(p-1)})} < \frac{n_p}{a(n_p)}$, por el Lema 2.16 deducimos que $\{n_1, \ldots, n_p\} \subseteq \overline{S}$ y por tanto que $S = \overline{S}$. □

TEOREMA 4.24. *Sea S un semigrupo proporcionalmente modular con* $\mathrm{e}(S) = p \geq 2$. *Entonces existe una ordenación $n_1, \ldots, n_p$ de los generadores minimales de S y existen enteros positivos $b_1, \ldots, b_p$ de modo que $\frac{n_1}{b_1} < \frac{n_2}{b_2} < \cdots < \frac{n_p}{b_p}$ es una secuencia de Bézout propia con extremos adyacentes.*

DEMOSTRACIÓN. Por el Lema 4.23 existen dos generadores minimales n_1 y n_p de S así como dos enteros positivos b_1 y b_p de modo que $S = \mathrm{S}([\frac{n_1}{b_1}, \frac{n_p}{b_p}])$ y además los extremos $\frac{n_1}{b_1}$ y $\frac{n_p}{b_p}$ son adyacentes.

Al igual que señalamos en la demostración del Lema 4.23, al ser n_1 y n_p generadores minimales de S, ha de ocurrir que $(n_1, b_1) = (n_p, b_p) = 1$.

Si ahora aplicamos el Teorema 4.4 a las fracciones $\frac{n_1}{b_1} < \frac{n_p}{b_p}$ y refinamos la secuencia de Bézout resultante, entonces obtenemos una secuencia de Bézout propia $\frac{n_1}{b_1} < \frac{x_1}{y_1} < \cdots < \frac{x_l}{y_l} < \frac{n_p}{b_p}$ con extremos adyacentes. En vista de los Teoremas 4.8 y 4.21, concluimos que $\{n_1, x_1, \ldots, x_l, n_p\}$ es el sistema minimal de generadores de S. □

Como consecuencia del Teorema 4.24 y del Corolario 4.17 deducimos el siguiente resultado.

COROLARIO 4.25. *Sea S un semigrupo proporcionalmente modular el cual está minimalmente generado por $n_1 < n_2 < \ldots < n_p$, con $p \geq 2$. Entonces n_1 y n_2 son primos relativos.*

COROLARIO 4.26. *Sea S un semigrupo proporcionalmente modular con sistema minimal de generadores $\{n_1, \ldots, n_p\}$ y $p \geq 3$. Si $n = \max\{n_1, \ldots, n_p\}$, entonces $\overline{S} = \langle \{n_1, \ldots, n_p\} \setminus \{n\} \rangle$ es de nuevo un semigrupo proporcionalmente modular.*

DEMOSTRACIÓN. Aplicando el Teorema 4.24, sabemos que existe una ordenación de los generadores minimales (digamos $n_1, \ldots, n_p$) así como enteros positivos $b_1, \ldots, b_p$ tal que $\frac{n_1}{b_1} < \cdots < \frac{n_p}{b_p}$ es una secuencia de Bézout propia. Además por el Lema 4.16 sabemos que $\max\{n_1, n_2, \ldots, n_p\} = \max\{n_1, n_p\}$. Supongamos que $n_p = \max\{n_1, n_p\}$. Como $\frac{n_1}{b_1} < \cdots < \frac{n_{p-1}}{b_{p-1}}$ es también una secuencia de Bézout, por el Teorema 4.8, deducimos que $\overline{S} = \langle n_1, \ldots, n_{p-1} \rangle$ es un semigrupo proporcionalmente modular. Si $\max\{n_1, n_p\} = n_1$, entonces mediante un argumento análogo obtenemos la misma conclusión. □

COMENTARIO 4.27. Observamos que si S es un semigrupo proporcionalmente modular el cual está minimalmente generado por $n_1 < \ldots < n_p$, entonces el semigrupo numérico $\langle \{n_1, \ldots, n_p\} \cup \{g(S)\} \rangle$ no tiene por qué ser proporcionalmente modular. Para ilustrar ésto, simplemente considerar el semigrupo definido por la inecuación diofántica $15x \bmod 19 \leq 2x$. Se puede comprobar fácilmente que $S = \langle 4,7,9,10 \rangle$ y $g(S) = 6$. Por el Corolario 4.25 vemos que $\langle 4,6,7,9,10 \rangle$ no puede ser proporcionalmente modular. □

COROLARIO 4.28. *Sea S un semigrupo proporcionalmente modular. Entonces existe una ordenación $n_1, \ldots, n_p$ para los generadores minimales de S de forma que*

$$S = \langle n_1, n_2 \rangle \cup \langle n_2, n_3 \rangle \cup \cdots \cup \langle n_{p-1}, n_p \rangle.$$

DEMOSTRACIÓN. Por el Teorema 4.24 existe una ordenación $n_1, \ldots, n_p$ de los generadores minimales de S así como enteros positivos $b_1, \ldots, b_p$ tales que $\frac{n_1}{b_1} < \frac{n_2}{b_2} < \cdots < \frac{n_p}{b_p}$ es una secuencia de Bézout. Ahora aplicando el Teorema 4.8 resulta $S = S([\frac{n_1}{b_1}, \frac{n_p}{b_p}])$. Recordemos una vez más el Lema 2.16 según el cual si $x \in S \setminus \{0\}$, entonces existe $y \in \{1, \ldots, p-1\}$ verificando que $\frac{n_i}{b_i} \leq \frac{x}{y} \leq \frac{n_{i+1}}{b_{i+1}}$. En vista del Lema 4.7 ésto implica que $x \in \langle n_i, n_{i+1} \rangle$. Por consiguiente $S \subseteq \bigcup_{i=1}^{p-1} \langle n_i, n_{i+1} \rangle$. La otra inclusión es trivial. □

EJEMPLO 4.29. Sea $S = S(3,13)$. Se puede comprobar fácilmente que $S = \langle 5,6,9,13 \rangle$. Veamos cómo la noción de convexidad vista en la sección anterior (Corolario 4.17) es suficiente para construir una secuencia de Bézout para dichos elementos. Como $1 \times 6 - 1 \times 5 = 1$, tenemos que $5/1 < 6/1$ es una secuencia de Bézout. Intentemos ahora añadir una fracción del tipo $9/x$, con x un entero positivo. Ahora tenemos dos posibilidades, según se añada por la izquierda o por la derecha. Observamos que no es posible añadir la fracción por la derecha puesto que $6/1 < 9/x$ no forma secuencia de Bézout para ningún $x > 0$. Sin embargo, $9/x < 5/1$ es una secuencia de Bézout para $x = 2$ (y sólo para dicho valor). Por consiguiente obtenemos la secuencia de Bézout $9/2 < 5/1 < 6/1$. Procediendo de manera análoga con el generador 13, resulta que tanto

$$\frac{13}{3} < \frac{9}{2} < \frac{5}{1} < \frac{6}{1} \text{ como } \frac{9}{2} < \frac{5}{1} < \frac{6}{1} < \frac{13}{2}$$

son secuencias de Bézout. En vista del Corolario 4.28 (y de su demostración), deducimos que

$$S = \langle 13,9 \rangle \cup \langle 9,5 \rangle \cup \langle 5,6 \rangle = \langle 9,5 \rangle \cup \langle 5,6 \rangle \cup \langle 6,13 \rangle.$$

Ya este ejemplo tan simple nos plantea la cuestión de cuántas secuencias de Bézout propias se pueden construir a partir de los generadores minimales de un semigrupo proporcionalmente modular. Este problema lo estudiaremos y lo resolveremos en el Capítulo 7. □

EJEMPLO 4.30. Para $S = \langle 10,11,21 \rangle$, se tiene que $S = \langle 10,21 \rangle \cup \langle 21,11 \rangle$. Sin embargo ésto no significa que el conjunto $\{10,11,21\}$ sea el sistema minimal de generadores del semigrupo S, pues $\langle 10,11,21 \rangle = \langle 10,11 \rangle$. □

Recordemos que dados dos enteros a y b primos relativos, denotamos por $a^{-1} \bmod b$ el inverso de a módulo b, es decir, el menor entero positivo u tal que $au \equiv 1 \bmod b$.

LEMA 4.31. *Sean n_1 y n_2 números enteros primos relativos, ambos mayores o iguales que 2. Entonces $n_2(n_2^{-1} \bmod n_1) - n_1((-n_1)^{-1} \bmod n_2) = 1$.*

DEMOSTRACIÓN. De $n_2(n_2^{-1} \bmod n_1) \equiv 1 \bmod n_1$ y $n_2^{-1} \bmod n_1 < n_1$, deducimos que $\frac{n_2(n_2^{-1} \bmod n_1)-1}{n_1}$ es un número entero menor o igual que n_2. Además, $n_2(n_2^{-1} \bmod n_1) - n_1\frac{n_2(n_2^{-1} \bmod n_1)-1}{n_1} = 1$, lo cual implica que $n_1\frac{n_2(n_2^{-1} \bmod n_1)-1}{n_1} \equiv -1 \bmod n_2$. Deducimos de aquí que $\frac{n_2(n_2^{-1} \bmod n_1)-1}{n_1}$ ha de ser igual a $(-n_1)^{-1} \bmod n_2$ y por tanto $n_2(n_2^{-1} \bmod n_1) - n_1((-n_1)^{-1} \bmod n_2) = 1$. □

Ya estamos en condiciones de dar la caracterización anunciada al comienzo de esta sección para los semigrupos proporcionalmente modulares en términos de sus generadores minimales.

TEOREMA 4.32. *Un semigrupo numérico S es proporcionalmente modular si y sólo si existe una ordenación $n_1, \ldots, n_p$ de sus generadores minimales de modo que se verifiquen las siguientes condiciones:*

1. $(n_i, n_{i+1}) = 1$ *para todo* $i \in \{1, \ldots, p-1\}$,
2. $n_{i-1} + n_{i+1} \equiv 0 \bmod n_i$ *para todo* $i \in \{2, \ldots, p-1\}$.

DEMOSTRACIÓN.

Condición necesaria. Por el Teorema 4.24 existe una ordenación $n_1, \ldots, n_p$ de los generadores minimales de S así como enteros positivos $b_1, \ldots, b_p$ tales que $\frac{n_1}{b_1} < \frac{n_2}{b_2} < \cdots < \frac{n_p}{b_p}$ es una secuencia de Bézout. Ésto implica que $(n_i, n_{i+1}) = 1$ para todo $i \in \{1, \ldots, p-1\}$. En vista del Lema 4.13, tenemos que $n_i = \frac{n_{i-1}+n_{i+1}}{n_{i+1}b_{i-1}-n_{i-1}b_{i+1}}$ para todo $i \in \{2, \ldots, p-1\}$ y en consecuencia $n_{i-1} + n_{i-1} \equiv 0 \bmod n_i$ para todo $i \in \{2, \ldots, p-1\}$.

Condición suficiente. Usando el Lema 4.31 y la condición (2), es fácil probar que la secuencia

$$\frac{n_1}{n_2^{-1} \bmod n_1} < \frac{n_2}{n_3^{-1} \bmod n_2} < \cdots < \frac{n_{p-1}}{n_p^{-1} \bmod n_{p-1}} < \frac{n_p}{(-n_{p-1})^{-1} \bmod n_p}$$

es de Bézout. Por el Teorema 4.8 concluimos que S es un semigrupo proporcionalmente modular. □

EJEMPLO 4.33. Sea el semigrupo numérico $S = \langle 5, 7, 11 \rangle$. Vamos a utilizar el Teorema 4.32 para ver que S no es proporcionalmente modular. Por el Lema 4.17 sólo hemos de considerar ordenaciones convexas de los generadores minimales. Las posibles ordenaciones convexas de los generadores minimales son $5, 7, 11$ y $7, 5, 11$ así como las correspondientes ordenaciones simétricas, aunque estas últimas no es necesario comprobarlas (ver las condiciones del Teorema 4.32). Como $5 + 11 = 16 \not\equiv 0 \bmod 7$ y

$7+11=18\not\equiv 0 \bmod 5$, por el Teorema 4.32 deducimos que S no es proporcionalmente modular. □

De nuevo se deja entrever en este ejemplo la importancia del número de secuencias de Bézout para los generadores minimales del semigrupo.

EJEMPLO 4.34. Sea $S=\langle 3,8,10\rangle$. Procediendo como en el ejemplo anterior, las únicas secuencias que hemos de considerar son $3,8,10$ y $8,3,10$. La primera no nos sirve para deducir que S es proporcionalmente modular pues $3+10=13\not\equiv 0 \bmod 3$. Si embargo para la segunda tenemos $8+10=18\equiv 0 \bmod 3$, por lo que $n_1=8$, $n_2=3$ y $n_3=10$ satisfacen las condiciones del Teorema 4.32. En consecuencia S es proporcionalmente modular. Como $3=3^{-1} \bmod 8$, $1=10^{-1} \bmod 3$ y $3=(-3)^{-1} \bmod 10$, resulta que

$$\frac{8}{3}<\frac{3}{1}<\frac{10}{3}$$

es una secuencia de Bézout propia asociada a S. Por tanto $S=\mathrm{S}([\frac{8}{3},\frac{10}{3}])$ y en vista del Lema 2.15, obtenemos

$$S=\{x\in\mathbb{N}\mid 30x \bmod 80\leq 6x\}=\{x\in\mathbb{N}\mid 15x \bmod 40\leq 3x\}.$$

□

Vemos que el Teorema 4.32 puede ser utilizado para obtener un algoritmo, de naturaleza distinta al que vimos en el Capítulo 2, para decidir si un semigrupo numérico es o no proporcionalmente modular. Compárese el ejemplo anterior con los Ejemplos 2.27 y 2.28 en el Capítulo 2.

Si analizamos el Corolario 4.28 y el Teorema 4.32, vemos que en ambos casos hemos utilizado una ordenación de los generadores minimales. Es lógico preguntarse si ambas ordenaciones son o no la misma. Además si escribimos la conclusión del Corolario 4.28 para tres generadores minimales consecutivos n_{i-1},n_i,n_{i+1} bajo la ordenación considerada, obtenemos $\langle n_{i-1},n_i,n_{i+1}\rangle=\langle n_{i-1},n_i\rangle\cup\langle n_i,n_{i+1}\rangle$. Cabe preguntarse si esta condición tiene alguna relación con la condición (2) en el Teorema 4.32. Pues bien, bajo el supuesto de que $n_1,\ldots,n_p$ es el sistema minimal de generadores del semigrupo y de que $(n_i,n_{i+1})=1$ para todo i, resulta que ambas condiciones son equivalentes. Veamos ésto. Si $n_{i-1}+n_{i+1}\equiv 0 \bmod n_i$, entonces $n_{i-1}+n_{i+1}=kn_i$ para cierto $k\in\mathbb{N}$. Ésto implica que toda combinación lineal $an_{i-1}+bn_i+cn_{i+1}$, con $a,b,c\in\mathbb{N}$, puede ser expresada bien como $a'n_{i-1}+b'n_i$ ó $b''n_i+c''n_{i+1}$ siendo a',b',b'',c'' enteros no negativos. Pero ésto a su vez significa que $\langle n_{i-1},n_i,n_{i+1}\rangle\subseteq\langle n_{i-1},n_i\rangle\cup\langle n_i,n_{i+1}\rangle$, y puesto que la otra inclusión siempre se verifica, resulta por tanto que la condición (2) del Teorema 4.32 implica que $\langle n_{i-1},n_i,n_{i+1}\rangle=\langle n_{i-1},n_i\rangle\cup\langle n_i,n_{i+1}\rangle$. Recíprocamente, si $\langle n_{i-1},n_i,n_{i+1}\rangle=\langle n_{i-1},n_i\rangle\cup\langle n_i,n_{i+1}\rangle$, entonces en particular tenemos que $n_{i-1}+n_{i+1}\in\langle n_{i-1},n_i\rangle\cup\langle n_i,n_{i+1}\rangle$. Ésto lleva a que $n_{i-1}+n_{i+1}=an_{i-1}+bn_i$ o bien $n_{i-1}+n_{i+1}=cn_i+dn_{i+1}$. Aplicando la independencia del conjunto $\{n_1,\ldots,n_p\}$, deducimos que $a=d=0$. Por tanto en ambos casos se cumple que $n_{i-1}+n_{i+1}\equiv 0 \bmod n_i$.

Como consecuencia resulta el siguiente corolario.

COROLARIO 4.35. *Sea S un semigrupo numérico minimalmente generado por $\{n_1,\dots,n_p\}$. Las siguientes condiciones son equivalentes:*

1. *S es proporcionalmente modular,*
2. *existe una ordenación $n_1,\dots,n_p$ de los generadores minimales de S tal que*
   a) $(n_i,n_{i+1})=1$ *para todo* $i\in\{1,\dots,p-1\}$, *y*
   b) $\langle n_{i-1},n_i,n_{i+1}\rangle=\langle n_{i-1},n_i\rangle\cup\langle n_i,n_{i+1}\rangle$, *para todo* $i\in\{2,\dots,p-1\}$.

Además en tal caso se verifica que

$$S=\langle n_1,n_2\rangle\cup\langle n_2,n_3\rangle\cup\cdots\cup\langle n_{p-1},n_p\rangle$$

COMENTARIO 4.36. El hecho de que S sea un semigrupo numérico minimalmente generado por $\{n_1,\dots,n_p\}$ y de que se verifique que $S=\langle n_1,n_2\rangle\cup\langle n_2,n_3\rangle\cdots\cup\langle n_{p-1},n_p\rangle$ con $(n_i,n_{i+1})=1$ para cada $i\in\{1,\dots,p-1\}$, no implica en general que S tenga que ser proporcionalmente modular.

Por ejemplo el semigrupo $S=\langle 7,8,9,10,12\rangle$ se puede descomponer como $S=\langle 12,7\rangle\cup\langle 7,8\rangle\cup\langle 8,9\rangle\cup\langle 9,10\rangle$, y sin embargo no es proporcionalmente modular ya que no se puede formar ninguna secuencia de Bézout con $7,8,9,10,12$. □

Recordemos que una representación proporcionalmente modular $S=\mathrm{S}(a,b,c)$ es primitiva, si $\mathrm{mcd}\{a,b,c\}=1$. Cerramos esta sección dando un resultado que también es consecuencia del Lema 4.23.

LEMA 4.37. *Todo semigrupo proporcionalmente modular distinto de $\langle 2,3\rangle$ tiene infinitas representaciones proporcionalmente modulares y primitivas de la forma $\mathrm{S}(a,b,c)$, con $c<a<b$.*

DEMOSTRACIÓN. La afirmación es trivialmente cierta para $S=\mathbb{N}$. Sea S un semigrupo proporcionalmente modular distinto de $\mathbb{N}$ y de $\langle 2,3\rangle$, y sea $g=\mathrm{g}(S)$. Según el Lema 4.23 existen dos generadores minimales n_1 y n_p de S así como dos enteros positivos $b_1\in\{1,\dots,n_1-1\}$ y $b_p\in\{1,\dots,n_p-1\}$ tales que $S=\mathrm{S}([\frac{n_1}{b_1},\frac{n_p}{b_p}])$. Si $1<\frac{n_1}{b_1}<\frac{n_p}{b_p}<\frac{g}{g-1}$, entonces todos los generadores minimales de S son menores que g, por lo que S es una semirecta. Definimos en este caso $u=1$ y $v=\frac{g}{g-1}$. En caso contrario, sean $u=\max\{\frac{h}{x_h}\mid h\in\mathrm{H}(S),x_h\in\{1,\dots,h-1\},\frac{h}{x_h}<\frac{n_1}{b_1}\}$ y $v=\min\{\frac{h}{x_h}\mid h\in\mathrm{H}(S),x_h\in\{1,\dots,h-1\},\frac{h}{x_h}>\frac{n_p}{b_p}\}$.

Elijamos dos fracciones irreducibles $\alpha=\frac{m_1}{r_1}\in(u,\frac{n_1}{b_1}]$ y $\beta=\frac{m_2}{r_2}\in[v,\frac{n_p}{b_p})$, con la condición adicional de que $\mathrm{mcd}\{m_1,m_2\}=1$. Entonces por el Lema 2.15 tenemos que $S=\mathrm{S}(r_1m_2,m_1m_2,r_1m_2-r_2m_1)$. Es inmediato dedudir que dicha representación proporcionalmente modular es primitiva.

Al haber infinitas posibilidades a la hora de elegir (α,β) en las condiciones anteriores, obtenemos la conclusión del lema. □

5. Semigrupos proporcionalmente modulares con dimensión de inmersión tres

En esta sección S será un semigrupo proporcionalmente modular minimalmente generado por $\{n_1,n_2,n_3\}$. Por el Teorema 4.32, podemos suponer que $(n_1,n_2) = (n_2,n_3) = 1$ y que $dn_2 = n_1+n_3$ para cierto $d \in \mathbb{N}\setminus\{0,1\}$.

Recordemos que el conjunto $\mathrm{Ap}(S,n_2)$ contiene para cada $i \in \{0,\dots,n_2-1\}$ el menor elemento de S congruente con i módulo n_2. En nuestro contexto los elementos de dicho conjunto serán de la forma an_1 o bien bn_3 para ciertos $a,b \in \mathbb{N}$. Por tanto requerimos saber cuándo an_1 y bn_3 son congruentes módulo n_2. Esta cuestión viene resuelta por el siguiente lema el cual aparece en [**37**].

LEMA 4.38. *Sean a,b,m,k,s y t dos números naturales tales que $(a,m) = 1$ y $a+b = km$. Entonces $ta \equiv sb \bmod m$ si y sólo si $t+s \equiv 0 \bmod m$.*

El siguiente lema, el cual también aparece en [**37**], describe el conjunto $\mathrm{Ap}(S,m)$ cuando S está generado por tres elementos.

LEMA 4.39. *Sea T un semigrupo numérico generado por $\{m,a,tm-a\}$ siendo m,a y t enteros positivos tales que $(m,a) = 1$ y $tm-a > m$. Entonces existen dos naturales λ y μ tales que $\lambda+\mu = m-1$ y*

$$\mathrm{Ap}(T,m) = \{0,a,2a,\dots,\lambda a, tm-a, 2(tm-a),\dots,\mu(tm-a)\}.$$

Por tanto ya podemos dar de forma explícita el conjunto $\mathrm{Ap}(S,n_2)$ para el caso que estamos considerando en esta sección.

PROPOSICIÓN 4.40. *Bajo las hipótesis de esta sección,*

$$\mathrm{Ap}(S,n_2) = \left\{0,n_1,\dots,\left\lfloor\frac{n_3}{d}\right\rfloor n_1, n_3,\dots,(n_2-\left\lfloor\frac{n_3}{d}\right\rfloor-1)n_3\right\}.$$

DEMOSTRACIÓN. Usando el Lema 4.39, tenemos que $an_1 \notin \mathrm{Ap}(S,n_2)$ si y sólo si existe un entero positivo b tal que $a+b \le n_2$, $an_1 \equiv bn_3 \bmod n_2$ y $bn_3 < an_1$. Por el Lema 4.38 ésto es equivalente a que exista un entero positivo b tal que $a+b \le n_2$, $a+b \equiv 0 \bmod n_2$ y $bn_3 < an_1$. Ésto equivale a que $bn_3 < an_1$ siendo $b = n_2-a$. Por tanto hemos probado que $an_1 \in \mathrm{Ap}(S,n_2)$ si y sólo si $an_1 \le (n_2-a)n_3$. Teniendo en cuenta además que $n_2 = \frac{n_1+n_3}{d}$, finalmente resulta que se verifica dicha desigualdad si y sólo si $a \le \frac{n_3}{d}$. □

Como consecuencia de la proposición precedente y del hecho de que $\mathrm{g}(S) = \mathrm{máx}(\mathrm{Ap}(S,n_2)) - n_2$, obtenemos el siguiente corolario.

COROLARIO 4.41. *Bajo las hipótesis de esta sección,*

$$\mathrm{g}(S) = \mathrm{máx}\left\{\left\lfloor\frac{n_3}{d}\right\rfloor n_1 - n_2, \left\lfloor\frac{n_1}{d}\right\rfloor n_3 - n_2\right\}.$$

Aplicando el Lema 0.1 a los resultados de la Proposición 4.40, obtenemos el siguiente resultado.

PROPOSICIÓN 4.42. *Bajo las hipótesis de esta sección,*

$$\#\mathrm{H}(S) = \frac{n_1(1+\lfloor \frac{n_3}{d} \rfloor)\lfloor \frac{n_3}{d} \rfloor + n_3(n_2 - \lfloor \frac{n_3}{d} \rfloor)(n_2 - \lfloor \frac{n_3}{d} \rfloor - 1) - n_2(n_2-1)}{2n_2}.$$

Herzog demuestra en [**16**] que para el caso de dimensión de inmersión igual a 3, un semigrupo numérico es simétrico si y sólo si es intersección completa (véase también [**8**]). A partir de los resultados de [**8**] y para dicho caso se puede demostrar además que S es una intersección completa si y sólo si $(n_1,n_3)\cdot n_2 \in \langle n_1,n_3\rangle$. Por tanto S es simétrico si y sólo si $(n_1,n_3)\cdot n_2 \in \langle n_1,n_3\rangle$.

Para el caso especial de los semigrupos proporcionalmente modulares que estamos considerando en esta sección, podemos enunciar el siguiente resultado.

PROPOSICIÓN 4.43. *Bajo las hipótesis de esta sección, S es simétrico si y sólo si $d = (n_1,n_3)$.*

DEMOSTRACIÓN.

Condición necesaria. Por el comentario del párrafo precedente, si S es simétrico podemos suponer que $(n_1,n_3)n_2 = an_1 + bn_3$ con $a,b \in \mathbb{N}$ y $a+b>0$. Sea $a \neq 0$. Puesto que estamos suponiendo que $dn_2 = n_1+n_3$ y además se verifica que $(n_1,n_2,n_3) = (n_2,(n_1,n_3)) = 1$, deducimos que $(n_1,n_3) \mid d$. Si ocurriese que $(n_1,n_3) < d$, entonces $n_3 = (d-(n_1,n_3))n_2 + (a-1)n_1 + bn_3$, lo cual implicaría que $b=0$ y por tanto que $n_3 \in \langle n_1,n_2\rangle$, contradiciendo la hipótesis de que $\{n_1,n_2,n_3\}$ es el sistema minimal de generadores de S.

Condición suficiente. Es consecuencia inmediata de los comentarios en el párrafo anterior. □

Cuando $d|n_1$ y $d|n_3$, por el Corolario 4.41 resulta $\mathrm{g}(S) = \frac{n_1n_3}{d} - n_2$. Teniendo en cuenta además que un semigrupo numérico S es simétrico si y sólo si $\#\mathrm{H}(S) = \frac{\mathrm{g}(S)+1}{2}$ (véase por ejemplo [**11**]), así como la Proposición 4.43, obtenemos el siguiente resultado.

COROLARIO 4.44. *Bajo las hipótesis de esta sección, si además S es simétrico, entonces*

1. $\mathrm{g}(S) = \dfrac{n_1n_2n_3 - n_1n_2 - n_2n_3}{n_1+n_3}$,
2. $\#\mathrm{H}(S) = \dfrac{n_1n_2n_3 - n_1n_2 - n_2n_3 + n_1 + n_3}{2(n_1+n_3)}$.

CAPÍTULO 5

Semigrupos afines completos y semigrupos proporcionalmente modulares

Dado un semigrupo numérico S y un número entero positivo p, tal y como hemos visto en el Capítulo 2, el conjunto $\frac{S}{p} = \{x \in \mathbb{N} \mid px \in S\}$ es un semigrupo numérico (denominado el cociente de S por p) el cual contiene a S. Además sabemos que todo semigrupo proporcionalmente modular es el cociente de un semigrupo aritmético. En la primera sección probamos en el Teorema 5.2 que la clase de los semigrupos proporcionalmente modulares es igual a la clase de los semigrupos que se obtienen como cociente por un entero positivo de un semigrupo numérico de dos generadores. A continuación definimos una familia de semigrupos afines completos los cuales denotamos como $\mathrm{A}(a_1, a_2, a_3)$. La relación entre tales semigrupos y los semigrupos proporcionalmente modulares viene dada por la Proposición 5.3. Por tanto el calcular un sistema de generadores para un semigrupo proporcionalemente modular se reduce a calcular un sistema de generadores para un semigrupo de la forma $\mathrm{A}(a_1, a_2, a_3)$. En la sección segunda describimos de forma explícita los sistemas minimales de generadores de los semigrupos $\mathrm{A}(a_1, a_2, a_3)$ (véase el Teorema 5.10). Como consecuencia, en la sección tercera describimos los sistemas de generadores para los semigrupos proporcionalmente modulares cuando éstos vienen dados como cocientes de semigrupos numéricos de dos generadores (Proposición 5.15). A continuación ilustramos esta idea calculando de forma explítica sistemas de generadores para los semigrupos $\frac{\langle n_1, n_2 \rangle}{d}$ cuando d vale 2, 3 y 12. Finalmente, en la sección cuarta retomamos el concepto de hueco fundamental para dar algunos resultados los cuales establecen cuándo un semigrupo proporcionalmente modular representado como un cociente por un número, es simétrico. El estudio de los semigrupos proporcionalmente modulares que son simétricos y más generalmente irreducibles será llevado a cabo en el capítulo siguiente.

Los resultados en este capítulo pueden encontrarse principalmente en [**45**].

1. Una nueva caracterización para los semigrupos proporcionalmente modulares

Comenzamos dando un lema técnico el cual nos va a permitir demostrar el Teorema 5.2.

LEMA 5.1. *Sean $c < a < b$ enteros positivos. Entonces existen enteros positivos k y d tales que* $\mathrm{S}([\frac{b}{a}, \frac{b}{a-c}]) = \mathrm{S}([\frac{b}{a}, \frac{kb+1}{d}])$.

DEMOSTRACIÓN. Llamemos $S = \mathrm{S}([\frac{b}{a}, \frac{b}{a-c}])$. De acuerdo con el Lema 2.16, si $x \in \mathbb{N} \setminus S$, entonces existe un único número $n_x \in \mathbb{N}$ tal que $\frac{x}{n_x+1} < \frac{b}{a} < \frac{b}{a-c} < \frac{x}{n_x}$. Como S es un semigrupo numérico, sabemos que el conjunto $\mathbb{N} \setminus S$ es finito y por tanto existe el mínimo, llamémoslo q, del conjunto $\{\frac{x}{n_x} \mid x \in \mathbb{N} \setminus S\}$. Obsérvese que $\frac{b}{a-c} < q$. De aquí deducimos que existen dos enteros positivos d y k tales que $d\frac{b}{a-c} \leq kb+1 < dq$. De la inclusión de intervalos $[\frac{b}{a}, \frac{b}{a-c}] \subseteq [\frac{b}{a}, \frac{kb+1}{d}]$ obtenemos que $S \subseteq \mathrm{S}([\frac{b}{a}, \frac{kb+1}{d}])$. Para probar que $\mathrm{S}([\frac{b}{a}, \frac{kb+1}{d}]) \subseteq S$, supongamos que $x \in \mathrm{S}([\frac{b}{a}, \frac{kb+1}{d}])$. Por el Lema 2.16, existe un entero positivo y tal que $\frac{b}{a} \leq \frac{x}{y} \leq \frac{kb+1}{d}$. Puesto que $\frac{x}{y} < q$, ésto implica que $x \in S$. □

Este lema nos garantiza pues que todo semigrupo proporcionalmente modular puede definirse mediante un intervalo cerrado cuyos numeradores son primos relativos.

TEOREMA 5.2. *Sean n_1, n_2 y d enteros positivos tales que n_1 y n_2 son primos relativos. Entonces $\frac{\langle n_1, n_2 \rangle}{d}$ es un semigrupo proporcionalmente modular. Recíprocamente, todo semigrupo proporcionalmente modular puede ser representado de esta forma.*

DEMOSTRACIÓN. Si $\mathrm{mcd}\{n_1, n_2\} = 1$, entonces existen dos enteros positivos u y v tal que $un_2 - vn_1 = 1$. Por el Lema 4.6 sabemos que

$$\langle n_1, n_2 \rangle = \{x \in \mathbb{N} \mid un_2 x \bmod n_1 n_2 \leq x\},$$

y en consecuencia

$$\frac{\langle n_1, n_2 \rangle}{d} = \{x \in \mathbb{N} \mid un_2 dx \bmod n_1 n_2 \leq dx\},$$

lo cual prueba que $\frac{\langle n_1, n_2 \rangle}{d}$ es un semigrupo proporcionalmente modular.

Recíprocamente, supongamos ahora que S es un semigrupo proporcionalmente modular definido por la inecuación diofántica $ax \bmod b \leq cx$. Por el Lema 2.15 sabemos que $S = \mathrm{S}([\frac{b}{a}, \frac{b}{a-c}])$ y por el Lema 5.1, que existen enteros positivos a_1, b_1, a_2 y b_2 tales que $\frac{a_1}{b_1} < \frac{a_2}{b_2}$, $\mathrm{mcd}\{a_1, a_2\} = 1$ y $S = \mathrm{S}([\frac{a_1}{b_1}, \frac{a_2}{b_2}])$. Basándonos de nuevo en el Lema 2.15, tenemos que $S = \{x \in \mathbb{N} \mid a_2 b_1 x \bmod a_1 a_2 \leq dx\}$, con $d = a_2 b_1 - a_1 b_2$.

Ahora demostramos que $S = \frac{\langle a_1, a_2 \rangle}{d}$. Como estamos suponiendo que $\mathrm{mcd}\{a_1, a_2\} = 1$, ésto implica que existen dos enteros positivos u y v tal que $a_2 u - a_1 v = 1$. Por el comentario dado al comienzo, tenemos que

$$\frac{\langle a_1, a_2 \rangle}{d} = \{x \in \mathbb{N} \mid ua_2 dx \bmod a_1 a_2 \leq dx\}.$$

Para finalizar la demostración, basta ver que las inecuaciones diofánticas $a_2 b_1 x \bmod a_1 a_2 \leq dx$ y $ua_2 dx \bmod a_1 a_2 \leq dx$ son equivalentes, es decir, tienen el mismo conjunto de soluciones. Para ello, es suficiente probar que $ua_2 d \equiv a_2 b_1 \bmod a_1 a_2$. Puesto que $a_2 u \equiv 1 \bmod a_1$, resulta que $a_2 u b_1 \equiv b_1 \bmod a_1$, y por tanto $(a_2 b_1 - a_1 b_2)u \equiv b_1 \bmod a_1$, es decir, $du \equiv b_1 \bmod a_1$. Finalmente, multiplicando por a_2 obtenemos $dua_2 \equiv a_2 b_1 \bmod a_1 a_2$. □

Un **semigrupo afín** es un subsemigrupo finitamente generado de $\mathbb{N}^r$. Si H es un subgrupo de $\mathbb{Z}^r$, entonces $H\cap\mathbb{N}^r$ es un subsemigrupo de $\mathbb{N}^r$. Estos semigrupos son afines ya que están generados por el conjunto X de los elementos minimales de $H\cap\mathbb{N}^r\setminus\{(0,\dots,0)\}$ con respecto al orden producto cartesiano, el cual es siempre finito (véase [**36**]). Denominaremos a estos semigrupos **afines completos**.

Dados tres enteros positivos a_1,a_2 y a_3, defininos el semigrupo

$$\mathrm{A}(a_1,a_2,a_3)=\{(x_1,x_2)\in\mathbb{N}^2 \mid a_1x_1+a_2x_2\equiv 0 \bmod a_3\}.$$

Observemos que $\mathrm{A}(a_1,a_2,a_3)=\{(x_1,x_2)\in\mathbb{Z}^2|a_1x_1+a_2x_2\equiv 0 \bmod a_3\}\cap\mathbb{N}^2$, por lo cual $\mathrm{A}(a_1,a_2,a_3)$ es un semigrupo afín completo.

El siguiente resultado relaciona los semigrupos $\mathrm{A}(a_1,a_2,a_3)$ recién definidos con los semigrupos proporcionalmente modulares.

PROPOSICIÓN 5.3. *Sean n_1,n_2 y d enteros positivos tales que n_1 y n_2 son primos relativos. Entonces*

$$\frac{\langle n_1,n_2\rangle}{d}=\left\{\frac{n_1x_1+n_2x_2}{d} \mid (x_1,x_2)\in\mathrm{A}(n_1,n_2,d)\right\}.$$

Además, si $\{(x_1,y_1),\dots,(x_r,y_r)\}$ es un sistema de generadores para el semigrupo $\mathrm{A}(n_1,n_2,d)$, entonces $\{\frac{n_1x_1+n_2y_1}{d},\dots,\frac{n_1x_r+n_2y_r}{d}\}$ es un sistema de generadores para el semigrupo $\frac{\langle n_1,n_2\rangle}{d}$.

DEMOSTRACIÓN. Si $s\in\frac{\langle n_1,n_2\rangle}{d}$, entonces $ds\in\langle n_1,n_2\rangle$, lo que significa que existe $(x,y)\in\mathbb{N}^2$ tal que $ds=n_1x+n_2y$. Por tanto $s=\frac{n_1x+n_2y}{d}$ con $(x,y)\in\mathrm{A}(n_1,n_2,d)$. Se ve claramente que la inclusión contraria también se verifica.

Si $s\in\frac{\langle n_1,n_2\rangle}{d}$, entonces existe $(x,y)\in\mathrm{A}(n_1,n_2,d)$ tal que $s=\frac{n_1x+n_2y}{d}$. Por hipótesis existen $\lambda_1,\dots,\lambda_r\in\mathbb{N}$ verificándose que $(x,y)=\lambda_1(x_1,y_1)+\cdots+\lambda_r(x_r,y_r)$. Por tanto $s=\lambda_1\frac{n_1x_1+n_2y_1}{d}+\ldots+\lambda_r\frac{n_1x_r+n_2y_r}{d}$. □

En [**28**] se demuestra el siguiente resultado el cual está relacionado con la proposición anterior.

TEOREMA 5.4. *Sean $a<b$ enteros positivos. Entonces*

$$\mathrm{S}(a,b)=\{x+y \mid (x,y)\in\mathrm{A}(a-1,a,b)\}.$$

En la siguiente sección describiremos totalmente el sistema minimal de generadores para cada semigrupo de la forma $\mathrm{A}(a_1,a_2,a_3)$. Por consiguiente, en vista de la Proposición 5.3 tendremos un método alternativo a las secuencias de Bézout para obtener un sistema de generadores para cualquier semigrupo proporcionalmente modular.

2. El sistema minimal de generadores de $\mathrm{A}(a_1,a_2,a_3)$

Sean a_1,a_2 y a_3 enteros positivos. Observemos en primer lugar que si $b=\mathrm{mcd}\{a_1,a_2,a_3\}$, entonces $\mathrm{A}(a_1,a_2,a_3)=\mathrm{A}(\frac{a_1}{b},\frac{a_2}{b},\frac{a_3}{b})$, por lo que podemos suponer, sin pérdida de generalidad, que $\mathrm{mcd}\{a_1,a_2,a_3\}=1$. Además, si $b=$

$\mathrm{mcd}\{a_1,a_2\}$, entonces $\mathrm{A}(a_1,a_2,a_3) = \mathrm{A}(\frac{a_1}{b},\frac{a_2}{b},a_3)$, de modo que también supondremos que $gcd\{a_1,a_2\} = 1$. Finalmente, observamos que $\mathrm{A}(a_1,a_2,a_3) = \mathrm{A}(a_1 \bmod a_3, a_2 \bmod a_3, a_3)$, con lo cual podemos tomar los números a_1,a_2 y a_3 de modo que $0 \leq a_1,a_2 < a_3$.

En esta sección n_1,n_2 y d representarán enteros positivos tales que $\mathrm{mcd}\{n_1,n_2\} = 1$, $\mathrm{mcd}\{n_1,d\} = d_1$ y $\mathrm{mcd}\{n_2,d\} = d_2$.

El siguiente lema es consecuencia inmediata de las definiciones.

LEMA 5.5. *Con la notación anterior,*

1. $\{(d/d_1,0),(0,d/d_2)\} \subseteq \mathrm{A}(n_1,n_2,d)$,
2. $(x_1,0) \in \mathrm{A}(n_1,n_2,d)$ *si y sólo si* x_1 *es un múltiplo de* d/d_1,
3. $(0,x_2) \in \mathrm{A}(n_1,n_2,d)$ *si y sólo si* x_2 *es un múltiplo de* d/d_2,
4. *Si* $(x_1,x_2) \in \mathrm{A}(n_1,n_2,d)$, *entonces* $d_2|x_1$ *y* $d_1|x_2$.

Definimos

$$\mathrm{H}(n_1,n_2,d) = \{(x_1,x_2) \in \mathbb{Z}_{d/d_1} \times \mathbb{Z}_{d/d_2} \mid (x_1,x_2) \in \mathrm{A}(n_1,n_2,d)\}.$$

Resulta claro que $\mathrm{H}(n_1,n_2,d)$ es un subgrupo de $\mathbb{Z}_{d/d_1} \times \mathbb{Z}_{d/d_2}$. Ya que para cada entero positivo n estamos tomando $\mathbb{Z}_n = \{0,1,\ldots,n-1\}$, ello nos permitirá considerar a $\mathrm{H}(n_1,n_2,d)$ como un subconjunto finito de $\mathbb{N}^2$.

LEMA 5.6. *El conjunto* $\mathrm{H}(n_1,n_2,d) \cup \{(d/d_1,0),(0,d/d_2)\}$ *es un sistema de generadores para el semigrupo* $\mathrm{A}(n_1,n_2,d)$.

DEMOSTRACIÓN. Sean $\alpha_1 = d/d_1$ y $\alpha_2 = d/d_2$. Para cualquier elemento $(x_1,x_2) \in \mathrm{A}(n_1,n_2,d)$ es inmediato que $(x_1,x_2) = \lfloor x_1/\alpha_1 \rfloor(\alpha_1,0) + \lfloor x_2/\alpha_2 \rfloor(0,\alpha_2) + (x_1 \bmod \alpha_1, x_2 \bmod \alpha_2)$ y que $(x_1 \bmod \alpha_1, x_2 \bmod \alpha_2) \in \mathrm{H}(n_1,n_2,d)$. □

Vamos a estudiar a continuación la estructura de los grupos $\mathrm{H}(n_1,n_2,d)$. Para ello definimos un nuevo tipo de grupos:

$$\mathrm{H}'(n_1,n_2,d) = \left\{ (x_1,x_2) \in (\mathbb{Z}_{\frac{d}{d_1d_2}})^2 \mid \frac{n_1}{d_1}x_1 + \frac{n_2}{d_2}x_2 \equiv 0 \bmod \frac{d}{d_1d_2} \right\}.$$

La relación existente entre los grupos $\mathrm{H}(n_1,n_2,d)$ y $\mathrm{H}'(n_1,n_2,d)$ viene dada por el siguiente lema.

LEMA 5.7. *Bajo las hipótesis de esta sección, se verifica que*

$$\mathrm{H}(n_1,n_2,d) = \{(d_2x_1,d_1x_2) \mid (x_1,x_2) \in \mathrm{H}'(n_1,n_2,d)\}.$$

DEMOSTRACIÓN. Si $(x_1,x_2) \in \mathrm{H}'(n_1,n_2,d)$, entonces tenemos que $x_1 < \frac{d}{d_1d_2}$, $x_2 < \frac{d}{d_1d_2}$ y $\frac{n_1}{d_1}x_1 + \frac{n_2}{d_2}x_2 \equiv 0 \bmod \frac{d}{d_1d_2}$, de lo cual deducimos que $d_2x_1 < \frac{d}{d_1}$, $d_1x_2 < \frac{d}{d_2}$ y $n_1d_2x_1 + n_2d_1x_2 \equiv 0 \bmod d$. Ésto significa que $(d_2x_1,d_1x_2) \in \mathrm{H}(n_1,n_2,d)$.

Recíprocamente, supongamos que $(x_1,x_2) \in \mathrm{H}(n_1,n_2,d)$. Entonces $n_1x_1 + n_2x_2 \equiv 0 \bmod d$. Por el Lema 5.5 también sabemos que $d_2|x_1$ y $d_1|x_2$, de lo cual resulta

$$\frac{n_1}{d_1}\frac{x_1}{d_2} + \frac{n_2}{d_2}\frac{x_2}{d_1} \equiv 0 \bmod \frac{d}{d_1d_2}.$$

Por tanto $(\frac{x_1}{d_2},\frac{x_2}{d_1}) \in \mathrm{H}'(n_1,n_2,d)$. □

COMENTARIO 5.8. Observemos que si $d = d_1d_2$, entonces $\mathrm{H}'(n_1,n_2,d) = \{(0,0)\}$, y en consecuencia $\mathrm{H}(n_1,n_2,d) = \{(0,0)\}$. Por el Lema 5.6, en este caso tenemos que el semigrupo $\mathrm{A}(n_1,n_2,d)$ está generado minimalmente por el conjunto $\{(d/d_1,0),(0,d/d_2)\}$. □

El siguiente lema describe totalmente la estructura de los grupos $\mathrm{H}'(n_1,n_2,d)$.

LEMA 5.9. *Bajo las hipótesis de esta sección, supongamos además que* $d \neq d_1d_2$. *Se verifican las siguientes propiedades.*

1. *Si* $(x_1,x_2) \in \mathrm{H}'(n_1,n_2,d) \setminus \{(0,0)\}$, *entonces* $x_1 \neq 0$ *y* $x_2 \neq 0$.
2. *Existe un elemento* $p \in \{1,\ldots,\frac{d}{d_1d_2}-1\}$ *tal que* $(1,p) \in \mathrm{H}'(n_1,n_2,d)$.
3. $\mathrm{H}'(n_1,n_2,d)$ *es el subgrupo cíclico de* $(\mathbb{Z}_{\frac{d}{d_1d_2}})^2$ *generado por el elemento* $(1,p)$.

DEMOSTRACIÓN.

1. Si $(0,x_2) \in \mathrm{H}'(n_1,n_2,d)$, entonces $\frac{n_2}{d_2}x_2 \equiv 0 \bmod \frac{d}{d_1d_2}$ y $x_2 < \frac{d}{d_1d_2}$. Como estamos suponiendo que $\mathrm{mcd}\{n_2,d\} = d_2$, ésto implica que $x_2 = 0$. Análogamente, si $(x_1,0) \in \mathrm{H}'(n_1,n_2,d)$, deducimos que $x_1 = 0$.
2. La hipótesis $\mathrm{mcd}\{n_2,d\} = d_2$ implica que la congruencia $\frac{n_1}{d_1} + \frac{n_2}{d_2}p \equiv 0 \bmod \frac{d}{d_1d_2}$ tiene sólo una solución módulo $\frac{d}{d_1d_2}$. Ésta es $p = ((\frac{n_2}{d_2})^{-1}(-\frac{n_1}{d_1})) \bmod \frac{d}{d_1d_2}$.
3. Si (x_1,x_2) es un elemento del grupo $\mathrm{H}'(n_1,n_2,d)$, entonces $(x_1,x_2) - x_1(1,p)$ es de nuevo un elemento de $\mathrm{H}'(n_1,n_2,d)$. Por el apartado (1), ésto implica que $(x_1,x_2) - x_1(1,p)$ debe de ser igual a $(0,0)$, y por tanto $(x_1,x_2) = x_1(1,p)$.

□

Representamos por S_n el grupo simétrico de grado n, es decir, el conjunto de todas las aplicaciones biyectivas del conjunto $\{1,\ldots,n\}$ en sí mismo. Decimos que una **permutación** $\sigma \in \mathrm{S}_n$ es **modular** si existe un entero positivo k tal que $\sigma(i) = (ki) \bmod (n+1)$ para todo $i \in \{1,\ldots,n\}$. Además, si x e y son enteros positivos primos relativos, denotamos por $\sigma_{x,y}$ la permutación modular de S_{y-1} definida como $\sigma_{x,y}(i) = (xi) \bmod y$, para todo $i \in \{1,\ldots,y-1\}$. Dada $\sigma \in \mathrm{S}_n$, definimos

$$\mathrm{I}(\sigma) = \{i \in \{1,\ldots,n\} \mid \sigma(i) \leq \sigma(j) \text{ para todo } j \in \{1,\ldots,i\}\}.$$

TEOREMA 5.10. *Sean* n_1,n_2 *y* d *enteros positivos verificando que* $\mathrm{mcd}\{n_1,n_2\} = 1$, $\mathrm{mcd}\{n_1,d\} = d_1$ *y* $\mathrm{mcd}\{n_2,d\} = d_2$. *Si* $d = d_1d_2$, *entonces el semigrupo* $\mathrm{A}(n_1,n_2,d)$ *está minimalmente generado por* $\{(d/d_1,0),(0,d/d_2)\}$. *Si* $d \neq d_1d_2$ *y* p *es la única solución módulo* $\frac{d}{d_1d_2}$ *de la congruencia* $\frac{n_1}{d_1} + \frac{n_2}{d_2}p \equiv 0 \bmod \frac{d}{d_1d_2}$, *entonces:*

1. $\mathrm{H}(n_1,n_2,d) = \{(d_2k, d_1\sigma_{p,\frac{d}{d_1d_2}}(k)) \mid k \in \{1,\ldots,\frac{d}{d_1d_2}-1\}\} \cup \{(0,0)\}$,

2. *el conjunto de los elementos minimales en* $\mathrm{H}(n_1,n_2,d)\setminus\{(0,0)\}$ *con respecto al orden usual producto cartesiano sobre* $\mathbb{N}^2$ *es igual a* $\{(d_2k, d_1\sigma_{p,\frac{d}{d_1d_2}}(k)) \mid k\in \mathrm{I}(\sigma_{p,\frac{d}{d_1d_2}})\}$,
3. $\mathrm{A}(n_1,n_2,d)$ *está minimalmente generado por* $\{(d/d_1,0),(0,d/d_2)\}\cup\{(d_2k, d_1\sigma_{p,\frac{d}{d_1d_2}}(k)) \mid k\in \mathrm{I}(\sigma_{p,\frac{d}{d_1d_2}})\}$.

DEMOSTRACIÓN. El caso $d=d_1d_2$ ha sido tratado en el Comentario 5.8. Supongamos pues que $d\neq d_1d_2$. Entonces tenemos que el enunciado (1) es consecuencia de los Lemas 5.7 y 5.9. El enunciado (2) es inmediato a partir de la definición de $\mathrm{I}(\sigma_{p,\frac{d}{d_1d_2}})$. Finalmente, el enunciado (3) es consecuencia del apartado (2) y del Lema 5.6. □

EJEMPLO 5.11. Obtengamos el sistema minimal de generadores del semigrupo afín completo $\mathrm{A}(10,21,48)$. Asignamos $n_1=10, n_2=21, d=48, d_1=2$ y $d_2=3$. La única solución módulo 8 para la congruencia $5+7p\equiv 0 \bmod 8$ es $p=5$. Resulta pues la permutación modular

$$\sigma_{5,8}=\begin{pmatrix}1&2&3&4&5&6&7\\5&2&7&4&1&6&3\end{pmatrix}$$

y el correspondiente conjunto $\mathrm{I}(\sigma_{5,8})=\{1,2,5\}$. Por el Teorema 5.10 deducimos que $\mathrm{A}(10,21,48)$ está minimalmente generado por el conjunto

$$\{(24,0),(0,16)\}\cup\{(3\cdot 1,2\cdot 5),(3\cdot 2,2\cdot 2),(3\cdot 5,2\cdot 1)\}=$$
$$\{(24,0),(0,16),(3,10),(6,4),(15,2)\}.$$

Finalmente, aplicando la Proposición 5.3 obtenemos que el semigrupo numérico proporcionalmente modular $\frac{\langle 10,21\rangle}{48}$ está generado por

$$\left\{\frac{24\cdot 10}{48},\frac{16\cdot 21}{48},\frac{3\cdot 10+10\cdot 21}{48},\frac{6\cdot 10+4\cdot 21}{48},\frac{15\cdot 10+2\cdot 21}{48}\right\}=\{5,7,5,3,4\}.$$

De aquí deducimos que $\frac{\langle 10,21\rangle}{48}=\langle 3,4,5\rangle$. □

3. Sistemas de generadores de semigrupos proporcionalmente modulares

Vemos en primer lugar que la representación para un semigrupo proporcionalmente modular como un cociente por un entero positivo dada en el Teorema 5.2, puede ser reducida a una en la cual los tres números n_1,n_2,d que aparecen sean primos relativos dos a dos.

LEMA 5.12. *Sean* n_1,n_2 *y* t *enteros positivos tales que* $\mathrm{mcd}\{n_1,tn_2\}=1$. *Entonces*

$$\frac{\langle n_1,tn_2\rangle}{td}=\frac{\langle n_1,n_2\rangle}{d}.$$

DEMOSTRACIÓN. Supongamos que $x \in \frac{\langle n_1, tn_2\rangle}{td}$. Entonces existen $\lambda_1, \lambda_2 \in \mathbb{N}$ de forma que $tdx = \lambda_1 n_1 + \lambda_2 tn_2$. Teniendo en cuenta además que $\mathrm{mcd}\{n_1, tn_2\} = 1$, deducimos que $t|\lambda_1$, y por tanto $dx = \frac{\lambda_1}{t} n_1 + \lambda_2 n_2$. Ésto significa que $x \in \frac{\langle n_1, n_2\rangle}{d}$.

Recíprocamente, si $x \in \frac{\langle n_1, n_2\rangle}{d}$, entonces existen $\lambda_1, \lambda_2 \in \mathbb{N}$ tal que $dx = \lambda_1 n_1 + \lambda_2 n_2$. Ésto implica que $tdx = (t\lambda_1) n_1 + \lambda_2 (tn_2)$, lo que significa que $x \in \frac{\langle n_1, tn_2\rangle}{td}$. □

Como consecuencia de este lema y del Teorema 5.2, obtenemos el siguiente resultado.

PROPOSICIÓN 5.13. *Cualquier semigrupo proporcionalmente modular puede ser representado como un cociente* $\frac{\langle n_1, n_2\rangle}{d}$*, siendo* n_1, n_2 *y* d *enteros positivos primos relativos dos a dos.*

EJEMPLO 5.14.

$$\frac{\langle 10, 21\rangle}{48} = \frac{\langle 10, 3\times 7\rangle}{3\times 16} = \frac{\langle 10, 7\rangle}{16} = \frac{\langle 2\times 5, 7\rangle}{2\times 8} = \frac{\langle 5, 7\rangle}{8}.$$

□

Combinando el Teorema 5.10 con la Proposición 5.3, llegamos a la siguiente proposición.

PROPOSICIÓN 5.15. *Sean* n_1, n_2 *y* d *enteros positivos primos relativos dos a dos, sea* $S = \frac{\langle n_1, n_2\rangle}{d}$ *y* p *la única solución módulo* d *para la congruencia* $n_1 + pn_2 \equiv 0 \bmod d$*. Entonces el conjunto*

$$\{n_1, n_2\} \cup \left\{ \frac{n_1 k + n_2 \sigma_{p,d}(k)}{d} \mid k \in \mathrm{I}(\sigma_{p,d}) \right\}$$

es un sistema de generadores para S*. En particular,* $\mathrm{e}(S) \leq \#\mathrm{I}(\sigma_{p,d}) + 2 \leq d + 1$.

Este resultado generaliza algunos resultados que aparecen en [**28**] para el caso de semigrupos modulares.

La Proposición 5.15 puede emplearse para obtener varias familias de semigrupos proporcionalmente modulares al ir variando los parámetros n_1, n_2 y d. Ilustramos esta idea para $d = 2$, $d = 3$ y $d = 12$.

COROLARIO 5.16. *Sean* n_1 *y* n_2 *números enteros positivos impares los cuales son primos relativos. Entonces*

$$\frac{\langle n_1, n_2\rangle}{2} = \left\langle n_1, n_2, \frac{n_1 + n_2}{2} \right\rangle.$$

DEMOSTRACIÓN. En vista de la congruencia $n_1 + n_2 \equiv 0 \bmod 2$, basta aplicar la Proposición 5.15 con $p = 1$ y $\sigma_{1,2} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. □

COROLARIO 5.17. *Sean* n_1 *y* n_2 *enteros positivos tales que* n_1, n_2 *y* 3 *son primos relativos dos a dos, y sea* $S = \frac{\langle n_1, n_2\rangle}{3}$*. Se verifica:*

1. *si* $n_1+n_2 \equiv 0 \bmod 3$, *entonces* $S = \langle n_1, n_2, \frac{n_1+n_2}{3} \rangle$,
2. *si* $n_1+2n_2 \equiv 0 \bmod 3$, *entonces* $S = \langle n_1, n_2, \frac{n_1+2n_2}{3}, \frac{2n_1+n_2}{3} \rangle$.

COROLARIO 5.18. *Sean* n_1 *y* n_2 *enteros positivos tales que* n_1, n_2 *y* 12 *son primos relativos dos a dos, y sea* $S = \frac{\langle n_1, n_2 \rangle}{12}$. *Se verifica:*

1. *si* $n_1+n_2 \equiv 0 \bmod 12$, *entonces* $S = \langle n_1, n_2, \frac{n_1+n_2}{12} \rangle$,
2. *si* $n_1+5n_2 \equiv 0 \bmod 12$, *entonces* $S = \langle n_1, n_2, \frac{n_1+5n_2}{12}, \frac{3n_1+3n_2}{12}, \frac{5n_1+n_2}{12} \rangle$,
3. *si* $n_1+7n_2 \equiv 0 \bmod 12$, *entonces* $S = \langle n_1, n_2, \frac{n_1+7n_2}{12}, \frac{2n_1+2n_2}{12}, \frac{7n_1+n_2}{12} \rangle$,
4. *si* $n_1+11n_2 \equiv 0 \bmod 12$, *entonces* S *está generado por el conjunto* $\{\frac{\lambda n_1+(12-\lambda)n_2}{12} | \lambda \in \{0,1,\ldots,12\}\}$.

Si un semigrupo numérico S viene definido por una inecuación diofántica proporcionalmente modular, la siguiente propiedad hace posible que la Proposición 5.15 pueda ser aplicada directamente también en este caso.

PROPOSICIÓN 5.19. *Sean* $c < a < b$ *enteros positivos y sea* $S = \mathrm{S}(a,b,c)$. *Entonces*

$$S = \frac{\langle b, b+1 \rangle}{a} \cup \frac{\langle b, b+1 \rangle}{c(b+1)-a}.$$

DEMOSTRACIÓN. Por el Lema 2.15 sabemos que $S = \mathrm{S}([\frac{b}{a}, \frac{b}{a-c}])$. Observemos que $[\frac{b}{a}, \frac{b}{a-c}] = [\frac{b}{a}, \frac{b+1}{a}] \cup [\frac{b+1}{a}, \frac{b}{a-c}]$. El Lema 2.16 implica entonces que $\mathrm{S}([\frac{b}{a}, \frac{b}{a-c}]) = \mathrm{S}([\frac{b}{a}, \frac{b+1}{a}]) \cup \mathrm{S}([\frac{b+1}{a}, \frac{b}{a-c}])$. Finalmente, por la demostración del Teorema 5.2 tenemos que $\mathrm{S}([\frac{b}{a}, \frac{b+1}{a}]) = \frac{\langle b, b+1 \rangle}{a}$ y $\mathrm{S}([\frac{b+1}{a}, \frac{b}{a-c}]) = \frac{\langle b, b+1 \rangle}{c(b+1)-a}$. □

EJEMPLO 5.20. Obtengamos un sistema de generadores para el semigrupo $S = \mathrm{S}(3, 17, 2)$ utilizando la idea de la Proposición 5.19.

Aplicando dicha proposición resulta $S = \frac{\langle 17, 18 \rangle}{3} \cup \frac{\langle 17, 18 \rangle}{33}$. Ahora por el Lema 5.12 tenemos que $\frac{\langle 17, 18 \rangle}{3} = \frac{\langle 17, 6 \rangle}{1} = \langle 6, 17 \rangle$. De hecho este cálculo no es necesario en este caso pues $3 | 33$ y por tanto $\frac{\langle 17, 18 \rangle}{3} \subseteq \frac{\langle 17, 18 \rangle}{33}$. Para el semigrupo $\frac{\langle 17, 18 \rangle}{33}$ tenemos $\frac{\langle 17, 18 \rangle}{33} = \frac{\langle 6, 17 \rangle}{11}$. Nótese que $\mathrm{A}(6, 17, 11) = \mathrm{A}(6, 6, 11) = \mathrm{A}(1, 1, 11)$. Ahora aplicando la Proposición 5.15 con $p = 10$, $n_1 = n_2 = 1$ y $d = 11$ resulta $\frac{\langle 6, 17 \rangle}{11} = \langle 6, 7, 8, 9, 10, 11 \rangle$, por lo que $S = \langle 6, 7, 8, 9, 10, 11 \rangle$. □

4. Huecos fundamentales de semigrupos proporcionalmente modulares

Para un semigrupo numérico S, recordemos que un hueco $x \in \mathrm{H}(S)$ es un hueco fundamental de S si $\{2x, 3x\} \subseteq S$, es decir, $kx \in S$ para todo $k \geq 2$. Además representamos el conjunto de todos los huecos fundamentales de S como $\mathrm{FH}(S)$.

Recordemos que el Lema 2.20 relacionaba los huecos fundamentales de un semigrupo numérico S con los del semigrupo $\frac{S}{d}$. Como consecuencia directa de dicho lema obtenemos el siguiente resultado.

COROLARIO 5.21. *Sea S un semigrupo numérico y sea d un entero positivo. Entonces $d \in \mathrm{FH}(S)$ si y sólo si $\frac{S}{d} = \mathbb{N} \setminus \{1\}$.*

El siguiente resultado aparece en [**27**] y describe totalmente los huecos fundamentales de cualquier semigrupo numérico generado por dos elementos.

TEOREMA 5.22. *Sean n_1 y n_2 dos enteros mayores o iguales que 3 tales que $(n_1, n_2) = 1$.*

1. *Si n_2 es par, entonces* $\mathrm{FH}(\langle n_1, n_2 \rangle) =$

$$\left\{ \frac{n_2}{2} + an_1 + bn_2 \;\middle|\; \begin{array}{c} (\frac{n_2}{6} \leq a \leq \frac{n_2}{2} - 1 \;\; y \;\; 0 \leq b \leq \frac{n_1-1}{2} - 1) \\ \text{ó} \\ (0 \leq a \leq \frac{n_2}{2} - 1 \;\; y \;\; \frac{n_1-3}{6} \leq b \leq \frac{n_1-1}{2} - 1) \end{array} \right\}.$$

2. *Si n_1 y n_2 son impares, entonces* $\mathrm{FH}(\langle n_1, n_2 \rangle) =$

$$\left\{ \frac{n_1+n_2}{2} + an_1 + bn_2 \;\middle|\; \begin{array}{c} (\frac{n_2-3}{6} \leq a \leq \frac{n_2-1}{2} - 1 \;\; y \;\; 0 \leq b \leq \frac{n_1-1}{2} - 1) \\ \text{ó} \\ (0 \leq a \leq \frac{n_2-1}{2} - 1 \;\; y \;\; \frac{n_1-3}{6} \leq b \leq \frac{n_1-1}{2} - 1) \end{array} \right\}.$$

Por tanto combinando el Lema 2.20 con los Teoremas 5.2 y 5.22 obtenemos una forma alternativa de definir semigrupos proporcionalmente modulares. En la primera aproximación que hemos dado en los capítulos anteriores siempre hemos especificado tales semigrupos mediante tres números enteros positivos a, b y c que son los que aparecen en la representación proporcionalmente modular del semigrupo. Además siempre hemos trabajado con los generadores minimales del semigrupo. Ahora, con este nuevo enfoque, para dar un semigrupo proporcionalmente modular volvemos a emplear tres números enteros positivos n_1, n_2 y d con los que se define el cociente. Sin embargo ahora se presta atención a los huecos fundamentales del semigrupo.

EJEMPLO 5.23. Consideremos el semigrupo $S = \frac{\langle 7,11 \rangle}{5}$.
Usando el Teorema 5.22 resulta $\mathrm{FH}(\langle 7, 11 \rangle) =$

$$\begin{array}{l} \{\frac{7+11}{2} + 7x + 11y \mid \frac{11-3}{6} \leq x \leq \frac{11-1}{2} - 1,\ 0 \leq y \frac{7-1}{2} - 1\} \cup \\ \{\frac{7+11}{2} + 7x + 11y \mid 0 \leq x \frac{11-1}{2} - 1,\ \frac{7-3}{6} \leq y \leq \frac{7-1}{2} - 1\} = \\ \{23, 34, 45, 30, 41, 52, 37, 48, 59\} \cup \{20, 31, 27, 38, 34, 45, 41, 52, 48, 59\}. \end{array}$$

Por tanto obtenemos $\mathrm{FH}(S) = \{20, 23, 27, 30, 31, 34, 37, 38, 41, 45, 48, 52, 59\}$ sin necesidad de calcular previamente $\mathrm{H}(S)$.

Ahora aplicando el Lema 2.20 resulta $\mathrm{FH}(\frac{\langle 7,11 \rangle}{5}) = \{\frac{20}{5}, \frac{30}{5}, \frac{45}{5}\} = \{4, 6, 9\}$, con lo cual $S = \mathbb{N} \setminus \{1, 2, 3, 4, 6, 9\}$, es decir, $S = \{0, 5, 7, 8, 10, \rightarrow\}$. De aquí deducimos que $S = \langle 5, 7, 8, 11 \rangle$.

Observamos que al margen de estos cálculos, teniendo en cuenta la demostración del Teorema 5.2 se comprueba que $S = \mathrm{S}(33, 77, 5)$, de donde es posible obtener también el sistema minimal de generadores para S. □

Mostramos ahora algunos resultados que relacionan a los semigrupos proporcionalmente modulares dados en forma de cociente con los semigrupos simétricos y con el concepto de hueco fundamental. Claramente $\mathrm{g}(S) = \max \mathrm{FH}(S)$. Recordemos que un semigrupo numérico S es simétrico, si $x \in \mathbb{Z} \setminus S$ implica que $\mathrm{g}(S) - x \in S$. Además todo semigrupo numérico generado por dos elementos es simétrico.

PROPOSICIÓN 5.24. *Sean n_1, n_2 y d enteros positivos tales que* $\mathrm{mcd}\{n_1, n_2\} = 1$. *Si d divide a $n_1 n_2 - n_1 - n_2$, entonces $\frac{\langle n_1, n_2\rangle}{d}$ es un semigrupo numérico simétrico cuyo número de Frobenius es igual a $\frac{n_1 n_2 - n_1 - n_2}{d}$.*

DEMOSTRACIÓN. Llamemos $g = n_1 n_2 - n_1 - n_2$ y $S = \frac{\langle n_1, n_2\rangle}{d}$. De las definiciones es inmediato que $\mathrm{g}(S) = \frac{g}{d}$. Probemos que el semigrupo S es también simétrico. Si $x \in \mathbb{Z} \setminus S$, entonces $dx \notin \langle n_1, n_2\rangle$, y ésto implica que $g - dx \in \langle n_1, n_2\rangle$ puesto que $\langle n_1, n_2\rangle$ es simétrico. Así $d(\frac{g}{d} - x) \in \langle n_1, n_2\rangle$ y por tanto $\frac{g}{d} - x \in \frac{\langle n_1, n_2\rangle}{d}$. □

EJEMPLO 5.25. Sea $S = \langle 5, 17\rangle$. Se puede comprobar fácilmente que $\mathrm{g}(S) = 63$ y $\mathrm{D}(63) = \{1, 3, 7, 9, 21, 63\}$. Aplicando la Proposición 5.24 resulta que cada uno de los semigrupos siguientes es simétrico: $\frac{\langle 5,17\rangle}{3} = \langle 5, 9, 13, 17\rangle$, $\frac{\langle 5,17\rangle}{7} = \langle 5, 6, 7, 8\rangle$, $\frac{\langle 5,17\rangle}{9} = \langle 3, 5\rangle$, $\frac{\langle 5,17\rangle}{21} = \langle 2, 5\rangle$ y $\frac{\langle 5,17\rangle}{63} = \langle 2, 3\rangle$. □

PROPOSICIÓN 5.26. *Sean n_1, n_2 y d enteros positivos tales que* $\mathrm{mcd}\{n_1, n_2\} = 1$, *sea $S = \langle n_1, n_2\rangle$ y supongamos que $g_1 < g_2 < \ldots < g_r$ son todos los huecos fundamentales de S que son múltiplos de d. Entonces el semigrupo $\frac{S}{d}$ es simétrico si y sólo si $\frac{g_r}{d}$ es impar y* $\#\mathrm{D}(\frac{g_1}{d}, \ldots, \frac{g_r}{d}) = \frac{1}{2}(\frac{g_r}{d} + 1)$.

DEMOSTRACIÓN. Claramente $\mathrm{g}(\frac{S}{d}) = \frac{g_r}{d}$, y por el Lema 2.20 sabemos que $\mathrm{H}(\frac{S}{d}) = \mathrm{D}(\frac{g_1}{d}, \ldots, \frac{g_r}{d})$. Para concluir la demostración basta aplicar el Lema 0.5. □

EJEMPLO 5.27. Sea $S = \langle 5, 7\rangle$ y $d = 2$. Entonces se puede comprobar fácilmente que $\mathrm{FH}(S) = \{11, 13, 16, 18, 23\}$. Los únicos elementos en $\mathrm{FH}(S)$ que son múltiplos de 2 son 16 y 18. Puesto que $\#\mathrm{D}(\frac{16}{2}, \frac{18}{2}) = \#\mathrm{D}(8, 9) = 6 \neq 5 = \frac{9+1}{2}$, concluimos que $\frac{S}{2}$ no es simétrico. □

EJEMPLO 5.28. Sea $S = \langle 5, 11\rangle$. Se puede comprobar que $\mathrm{FH}(S) = \{18, 19, 23, 24, 28, 29, 34, 39\}$. Si $d = 2$, entonces vemos que los elementos de $\mathrm{FH}(S)$ que son múltiplos de 2 son $18, 24, 28$ y 34. En vista de $\#\mathrm{D}(\frac{18}{2}, \frac{24}{2}, \frac{28}{2}, \frac{34}{2}) = \#\mathrm{D}(9, 12, 14, 17) = 10 \neq 9 = \frac{17+1}{2}$, concluimos que el semigrupo $\frac{S}{2} = \langle 5, 8, 11\rangle$ no es simétrico.

Supongamos ahora que $d = 3$. Los elementos de $\mathrm{FH}(S)$ que son múltiplos de 3 son $18, 24$ y 39. Como $\#\mathrm{D}(\frac{18}{3}, \frac{24}{3}, \frac{39}{3}) = \#\mathrm{D}(6, 8, 13) = 7 = \frac{13+1}{2}$ y además $\frac{g_r}{d} = \frac{39}{3} = 13$ es impar, resulta que el semigrupo $\frac{S}{3} = \langle 5, 7, 9, 11\rangle$ es simétrico. □

CAPÍTULO 6

Semigrupos irreducibles y semigrupos proporcionalmente modulares

Recordemos que un semigrupo numérico se dice irreducible si no puede ser expresado como la intersección de dos semigrupos numéricos que lo contengan propiamente (véase [**35**]). Los semigrupos numéricos irreducibles con número de Frobenius impar (respectivamente par) se denominan simétricos (respectivamente pseudo-simétricos); véase [**2**]. En la primera sección veremos que los semigrupos numéricos generados por intervalos acotados de $\mathbb{R}_0^+$, no necesariamente cerrados, son también proporcionalmente modulares. Partiendo de esta idea, en la sección segunda caracterizamos los semigrupos irreducibles proporcionalmente modulares en términos de las representaciones de la forma $\mathrm{S}(]\frac{b}{a},\frac{b}{a-1}[)$. En la sección siguiente determinamos el sistema minimal de generadores para el semigrupo $\mathrm{S}(]\frac{b}{a},\frac{b}{a-1}[)$ cuando éste es simétrico y una secuencia de Bézout propia de la forma $\frac{b}{a}<\frac{n_1}{b_1}<\cdots<\frac{n_p}{b_p}<\frac{b}{a-1}$ es conocida. De manera similar, en la sección cuarta determinamos el sistema minimal de generadores para el semigrupo $\mathrm{S}(]\frac{b}{a},\frac{b}{a-1}[)$ cuando éste es pseudo-simétrico y se dispone de una secuencia de Bézout propia del tipo $\frac{b/2}{a/2}<\frac{n_1}{b_1}<\cdots<\frac{n_p}{b_p}<\frac{b}{a-1}$. En la sección quinta, fijado b estudiamos las representaciones de la forma $\mathrm{S}(]\frac{b}{a},\frac{b}{a-1}[)$ para los semigrupos numéricos. En particular, determinamos de forma aritmética tanto el número de semigrupos proporcionalmente modulares simétricos como el número de semigrupos proporcionalmente modulares pseudo-simétricos con un número de Frobenius dado. Finalmente, en la sección sexta incluimos algunos resultados sobre semigrupos modulares simétricos y sobre semigrupos modulares pseudo-simétricos que aparecen en otros trabajos de investigación.

Los resultados de este capítulo pueden ser encontrados en [**28**], [**31**], [**32**] y [**43**].

1. El semigrupo numérico asociado a un intervalo acotado

En esta sección I representará un intervalo acotado de $\mathbb{R}_0^+$ (ya sea cerrado, abierto o semiabierto) con más de un elemento, $\langle I\rangle$ el correspondiente submonoide de $\mathbb{R}_0^+$ generado por I y $\mathrm{S}(I)=\langle I\rangle\cap\mathbb{N}$. Nuestro objetivo es probar que $\mathrm{S}(I)$ es un semigrupo proporcionalmente modular.

LEMA 6.1. *Si $x_1,\ldots,x_k\in I$, entonces $\frac{1}{k}(x_1+\cdots+x_k)\in I$.*

DEMOSTRACIÓN. Es inmediato que $k\cdot\min\{x_1,\ldots,x_k\}\leq x_1+\cdots+x_k\leq k\cdot\max\{x_1,\ldots,x_k\}$ y por tanto $\min\{x_1,\ldots,x_k\}\leq\frac{1}{k}(x_1+\cdots+x_k)\leq\max\{x_1,\ldots,x_k\}$, de donde deducimos que $\frac{1}{k}(x_1+\cdots+x_k)\in I$. □

LEMA 6.2. *Sea $x \in \mathbb{R}^+$. Entonces $x \in \langle I \rangle$ si y sólo si existe un entero positivo k tal que $\frac{x}{k} \in I$.*

DEMOSTRACIÓN. Si $x \in \langle I \rangle$, entonces existen $\lambda_1, \ldots, \lambda_k \in \mathbb{N}$ así como $a_1, \ldots, a_k \in I$ tales que $x = \lambda_1 a_1 + \cdots + \lambda_k a_k$. Por el Lema 6.1 deducimos que $\frac{x}{\lambda_1 + \cdots + \lambda_k} \in I$. Recíprocamente, si $\frac{x}{k} \in I$, entonces $x = k \cdot \frac{x}{k} \in \langle I \rangle$. □

Ya estamos en condiciones de probar el siguiente resultado.

PROPOSICIÓN 6.3. *$\mathrm{S}(I)$ es un semigrupo proporcionalmente modular.*

DEMOSTRACIÓN. En primer lugar tenemos que $\mathrm{S}(I) = \langle I \rangle \cap \mathbb{N}$ is a submonoide de $\mathbb{R}_0^+$ incluido en $\mathbb{N}$ por lo que $\mathrm{S}(I)$ es un semigrupo. Sean $\alpha, \beta \in I$ tales que $\alpha < \beta$. Entonces $[\alpha, \beta] \subseteq I$, lo que implica que $\mathrm{S}([\alpha, \beta]) \subseteq \mathrm{S}(I)$. Al ser $\mathrm{S}([\alpha, \beta])$ un semigrupo numérico, sabemos que $\mathbb{N} \setminus \mathrm{S}([\alpha, \beta])$ es finito y por tanto también lo es $\mathbb{N} \setminus \mathrm{S}(I)$. Por consiguiente $\mathrm{S}(I)$ es un semigrupo numérico. Sea $\{n_1, \ldots, n_p\}$ el sistema minimal de generadores de $\mathrm{S}(I)$. Por el Lema 6.2, existen enteros positivos $\lambda_1, \ldots, \lambda_p$ tales que $\{\frac{n_1}{\lambda_1}, \ldots, \frac{n_p}{\lambda_p}\} \subseteq I$. Supongamos que $\frac{n_1}{\lambda_1} < \cdots < \frac{n_p}{\lambda_p}$. Entonces $\mathrm{S}([\frac{n_1}{\lambda_1}, \frac{n_p}{\lambda_p}]) \subseteq \mathrm{S}(I)$, y aplicando el Lema 6.2 de nuevo obtenemos que $\{n_1, \ldots, n_p\} \subseteq \mathrm{S}([\frac{n_1}{\lambda_1}, \frac{n_p}{\lambda_p}])$. Ésto implica que $\mathrm{S}(I) = \langle n_1, \ldots, n_p \rangle \subseteq \mathrm{S}([\frac{n_1}{\lambda_1}, \frac{n_p}{\lambda_p}])$ y por tanto $S(I) = \mathrm{S}([\frac{n_1}{\lambda_1}, \frac{n_p}{\lambda_p}])$, lo que significa que $\mathrm{S}(I)$ es proporcionalmente modular. □

EJEMPLO 6.4. Sea el intervalo $I =]\frac{43}{35}, \frac{23}{18}[$. Calculemos el semigrupo $S = \mathrm{S}(I)$. Sea t el número entero más pequeño verificando que $\frac{23}{18}t > \frac{43}{35}(t+1)$. Entonces $t = 25$, $[\frac{43}{35}t, \frac{23}{18}t] \cap \mathbb{N} = \{30\}$ y por tanto $\{30, \to\} \subseteq \mathrm{S}(I)$. Se puede comprobar fácilmente que

$$\left(\bigcup_{k=1}^{t-1} \left] \frac{43}{35}k, \frac{23}{18}k \right[\right) \cap \mathbb{N} = \{5, 10, 14, 15, 16, 19, 20, 21, 24, 25, 26, 28, 29, 30\},$$

de lo cual resulta que $S = \langle 5, 14, 16 \rangle$. Como $\frac{16}{13}, \frac{5}{4}, \frac{14}{11} \in I$ y $\frac{16}{13} < \frac{5}{4} < \frac{14}{11}$, por la demostración de la Proposición 6.3, obtenemos que $S = \mathrm{S}([\frac{16}{13}, \frac{14}{11}])$. □

COMENTARIO 6.5. En el Ejemplo 2.28 ya se dejaba entrever la posibilidad de permitir intervalos acotados no necesariamente cerrados para definir semigrupos proporcionalmente modulares.

Concretamente, dijimos que el semigrupo S allí considerado podía ser definido por cualquier intervalo cerrado $[\alpha, \beta]$ cuando el par ordenado (α, β) perteneciera al conjunto $((7/5, 10/7] \times [8/5, 5/3)) \cup ((5/2, 8/3] \times [10/3, 7/2))$.

Por la Proposición 2.25, también es correcto decir que dicho semigrupo S puede ser definido por cualquier intervalo de la forma $]\alpha, \beta]$ cuando (α, β) pertenezca al conjunto $([7/5, 10/7) \times [8/5, 5/3)) \cup ([5/2, 8/3) \times [10/3, 7/2))$. □

2. Una caracterización para los semigrupos proporcionalmente modulares irreducibles

En esta sección a y b representarán dos números enteros tales que $2 \leq a < b$. Llamamos $d = \text{mcd}\{a,b\}$ y $d' = \text{mcd}\{a-1,b\}$.

LEMA 6.6. *Si $x \in \mathbb{R}^+$, entonces $b+x \in \langle]\frac{b}{a}, \frac{b}{a-1}[\rangle$. En particular, $\{b+1,\rightarrow\} \subseteq \text{S}(]\frac{b}{a}, \frac{b}{a-1}[)$.*

DEMOSTRACIÓN. A partir de la desigualdad $b < b+x$, vemos que existe un entero positivo k tal que $(a-1)(b+x) < bk < a(b+x)$, es decir, $\frac{b}{a} < \frac{b+x}{k} < \frac{b}{a-1}$. Por el Lema 6.2 deducimos que $b+x \in \langle]\frac{b}{a}, \frac{b}{a-1}[\rangle$. □

PROPOSICIÓN 6.7. *Sea $x \in \mathbb{N}$. Entonces $x \in \text{S}([\frac{b}{a}, \frac{b}{a-1}])$ y $x \notin \text{S}(]\frac{b}{a}, \frac{b}{a-1}[)$ si y sólo si $x \in \{\lambda\frac{b}{d} \mid \lambda \in \{1,\ldots,d\}\} \cup \{\lambda\frac{b}{d'} \mid \lambda \in \{1,\ldots,d'\}\}$.*

DEMOSTRACIÓN. Sean $\overline{S} = \text{S}([\frac{b}{a}, \frac{b}{a-1}])$ y $S = \text{S}(]\frac{b}{a}, \frac{b}{a-1}[)$. Por el Lema 6.2, si $x \in \overline{S} \setminus S$, entonces existe un entero positivo k tal que $\frac{x}{k} = \frac{b}{a}$ ó $\frac{x}{k} = \frac{b}{a-1}$. Ésto significa que x es un múltiplo de $\frac{b}{d}$ o bien x es un múltiplo de $\frac{b}{d'}$. Usando el Lema 6.6, concluimos que $x \in \{\lambda\frac{b}{d} \mid \lambda \in \{1,\ldots,d\}\}$ o bien $x \in \{\lambda\frac{b}{d'} \mid \lambda \in \{1,\ldots,d'\}\}$.

Recíprocamente, supongamos que $x = t\frac{b}{d}$ con $t \in \mathbb{N}\setminus\{0\}$. Claramente $x \in \overline{S}$. Si $x \in S$, entonces existe un entero positivo k verificándose que $\frac{b}{a} < \frac{t\frac{b}{d}}{k} < \frac{b}{a-1}$. Ésto implica que $(a-1)t < dk < at$, y puesto que a es un múltiplo de d, deducimos que $(a-1)t < at-d$, es decir, $d < t$. Por tanto hemos probado que si $x \in \{\lambda\frac{b}{d} \mid \lambda \in \{1,\ldots,d\}\}$, entonces $x \in \overline{S}$ y $x \notin S$. De manera similar se demuesta que si $x \in \{\lambda\frac{b}{d'} \mid \lambda \in \{1,\ldots,d'\}\}$, entonces $x \in \overline{S}$ y $x \notin S$. □

Tal y como se ha mencionado ya en esta memoria, la forma como se representa un semigrupo numérico es muy importante a la hora de dar respuesta a determinadas cuestiones sobre dicho semigrupo. Los siguientes resultados ponen de manifiesto este hecho para los semigrupos numéricos que estamos considerando en este capítulo.

COROLARIO 6.8.

$$\#\text{H}\left(\text{S}\left(\left]\frac{b}{a}, \frac{b}{a-1}\right[\right)\right) \;=\; \frac{1}{2}\left(b-1+d+d'\right).$$

DEMOSTRACIÓN. Como $\text{mcd}\{d,d'\} = 1$, ésto implica que $\lambda\frac{b}{d} \neq \mu\frac{b}{d'}$ para todo $\lambda \in \{1,\ldots,d-1\}$ y $\mu \in \{1,\ldots,d'-1\}$. Aplicando la Proposición 6.7 deducimos que $\#\text{H}(\text{S}(]\frac{b}{a}, \frac{b}{a-1}[)) = \#\text{H}(\text{S}([\frac{b}{a}, \frac{b}{a-1}])) + d + d' - 1$. Sea $S = \text{S}(a,b,1)$. Ya que por el Teorema 1.13 sabemos que $\#\text{H}(S) = \frac{1}{2}(b+1-d-d')$ y además por el Lema 2.15 se verifica que $S = \text{S}([\frac{b}{a}, \frac{b}{a-1}])$, vemos que el resultado se deduce fácilmente. □

TEOREMA 6.9. *Sean a y b números enteros tales que $2 \leq a < b$, y sean $d = \mathrm{mcd}\{a, b\}$ y $d' = \mathrm{mcd}\{a-1, b\}$. Entonces $\mathrm{S}(]\frac{b}{a}, \frac{b}{a-1}[)$ es un semigrupo proporcionalmente modular con número de Frobenius igual a b y grado de singularidad igual a $\frac{1}{2}(b-1+d+d')$.*

DEMOSTRACIÓN. Llamemos $S = \mathrm{S}(]\frac{b}{a}, \frac{b}{a-1}[)$. Ya sabemos por la Proposición 6.3 que S es proporcionalmente modular. Del Lema 6.6 y la Proposición 6.7 deducimos que $\mathrm{g}(S) = b$. Finalmente, por el Corolario 6.8 tenemos que $\#\mathrm{H}(S) = \frac{1}{2}(b-1+d+d')$. □

Teniendo el cuenta el Teorema 6.9 y los Lemas 0.5 y 0.6, deducimos el siguiente corolario.

COROLARIO 6.10. *El semigrupo $\mathrm{S}(]\frac{b}{a}, \frac{b}{a-1}[)$ es simétrico (respectivamente, pseudo-simétrico) si y sólo si $d = d' = 1$ (respectivamente, $\{d, d'\} = \{1, 2\}$).*

El siguiente resultado es consecuencia inmediata de la Proposición 6 de [**35**].

LEMA 6.11. *Si S es un semigrupo numérico irreducible y $\mathrm{m}(S) \geq 4$, entonces $\mathrm{e}(S) \leq \mathrm{m}(S) - 1$.*

A partir de este resultado deducimos el siguiente.

LEMA 6.12. *Un semigrupo numérico S es una semirecta irreducible si y sólo si*

$$S \in \{\mathbb{N}, \langle 2, 3\rangle, \langle 3, 4, 5\rangle\}.$$

DEMOSTRACIÓN. Si $S = \{0, \mathrm{m}(S), \rightarrow\}$, entonces S está generado minimalmente por $\{\mathrm{m}(S), \mathrm{m}(S)+1, \ldots, 2\mathrm{m}(S)-1\}$ con lo cual $\mathrm{e}(S) = \mathrm{m}(S)$. Por el Lema 6.11, si S es irreducible, entonces $\mathrm{m}(S) \in \{1, 2, 3\}$. Ésto implica que $S \in \{\mathbb{N}, \langle 2, 3\rangle, \langle 3, 4, 5\rangle\}$. El recíproco se puede probar fácilmente usando los Lemas 0.5 y 0.6. □

COMENTARIO 6.13. Nótese que $\mathbb{N} = \mathrm{S}(1, 2, 1)$, $\langle 2, 3\rangle = \mathrm{S}(2, 3, 1)$ y $\langle 3, 4, 5\rangle = \mathrm{S}(2, 6, 1)$, con lo cual dichos semigrupos son proporcionalmente modulares. □

El siguiente resultado es el Teorema 1 en [**35**].

LEMA 6.14. *Para cualquier semigrupo numérico S, las siguientes condiciones son equivalentes:*

1. *S es irreducible,*
2. *S es maximal en el conjunto de todos los semigrupos numéricos con número de Frobenius $\mathrm{g}(S)$,*
3. *S es maximal en el conjunto de todos los semigrupos numéricos que no contienen a $\mathrm{g}(S)$.*

LEMA 6.15. *Sean α y β dos números reales verificando que $1 < \alpha < \beta$ y sea el semigrupo $S = \mathrm{S}([\alpha, \beta])$. Si S no es una semirecta, entonces*

$$\frac{\mathrm{g}(S)}{\mathrm{g}(S)-1} < \alpha < \beta < \mathrm{g}(S).$$

DEMOSTRACIÓN. Ya que S no es una semirecta, tenemos $\mathrm{m}(S) < \mathrm{g}(S)$. Al verificarse que $\mathrm{m}(S) \in S$, por el Lema 6.2 existe un entero positivo $k \in \{1, \ldots, \mathrm{m}(S)-1\}$ tal que $\alpha \leq \frac{\mathrm{m}(S)}{k} \leq \beta$. Ésto en particular implica que $\alpha \leq \frac{\mathrm{m}(S)}{k} < \frac{\mathrm{g}(S)}{k} \leq \frac{\mathrm{g}(S)}{1}$. De nuevo teniendo en cuenta el Lema 6.2 y que $\mathrm{g}(S) \notin S$, deducimos que $\beta < \frac{\mathrm{g}(S)}{1}$. Claramente se verifica $\beta \geq \frac{\mathrm{m}(S)}{k} \geq \frac{\mathrm{m}(S)}{\mathrm{m}(S)-1} > \frac{\mathrm{g}(S)}{\mathrm{g}(S)-1}$. Puesto que $\mathrm{g}(S) \notin S$, por el Lema 6.2 obtenemos que $\frac{\mathrm{g}(S)}{\mathrm{g}(S)-1} < \alpha$. □

PROPOSICIÓN 6.16. *Sea S un semigrupo numérico proporcionalmente modular e irreducible que no es una semirecta. Entonces existe un entero positivo k tal que $2 \leq k < \mathrm{g}(S)$ y $S = \mathrm{S}(]\frac{\mathrm{g}(S)}{k}, \frac{\mathrm{g}(S)}{k-1}[)$.*

DEMOSTRACIÓN. Llamemos $\overline{S} = \mathrm{S}(]\frac{\mathrm{g}(S)}{k}, \frac{\mathrm{g}(S)}{k-1}[)$ y probemos que $S = \overline{S}$. Por el Lema 2.23 deducimos que $S = \mathrm{S}([\alpha, \beta])$ siendo α y β dos números reales tales que $1 < \alpha < \beta$. Como $\mathrm{g}(S) \notin S$, los Lemas 6.2 y 6.15 implican que existe un entero k tal que $2 \leq k < \mathrm{g}(S)$ y $\frac{\mathrm{g}(S)}{k} < \alpha < \beta < \frac{\mathrm{g}(S)}{k-1}$. Por tanto $[\alpha, \beta] \subseteq]\frac{\mathrm{g}(S)}{k}, \frac{\mathrm{g}(S)}{k-1}[$, lo cual a su vez implica que $S \subseteq \overline{S}$. Por el Teorema 6.9 sabemos además que $\overline{S}$ es un semigrupo numérico con número de Frobenius $\mathrm{g}(S)$. Aplicando el Lema 6.14 deducimos la otra inclusión y por tanto la igualdad $S = \overline{S}$. □

Combinando la Proposición 6.16, el Corolario 6.10, el Lema 6.12 y el Comentario 6.13 obtenemos el siguiente resultado.

TEOREMA 6.17. *Sea S un semigrupo proporcionalmente modular.*

1. *S es simétrico si y sólo si $S = \mathbb{N}$, $S = \langle 2, 3 \rangle$ ó $S = \mathrm{S}(]\frac{b}{a}, \frac{b}{a-1}[)$ para ciertos números enteros a y b verificando que $2 \leq a < b$ y $\mathrm{mcd}\{a-1, b\} = \mathrm{mcd}\{a, b\} = 1$.*
2. *S es pseudo-simétrico si y sólo si $S = \langle 3, 4, 5 \rangle$ ó $S = \mathrm{S}(]\frac{b}{a}, \frac{b}{a-1}[)$ para ciertos números enteros a y b verificando que $2 \leq a < b$ y $\{\mathrm{mcd}\{a-1, b\}, \mathrm{mcd}\{a, b\}\} = \{1, 2\}$.*

3. Los generadores minimales en el caso simétrico

En esta sección a y b representarán dos números enteros tales que $2 \leq a < b$ y $\mathrm{mcd}\{a, b\} = \mathrm{mcd}\{a-1, b\} = 1$.

Recordemos que un semigrupo numérico S es simétrico si y sólo si para cualquier número entero x, si $x \in \mathbb{Z} \setminus S$, entonces $\mathrm{g}(S) - x \in S$.

Vamos a aplicar los resultados del Capítulo 4 sobre secuencias de Bézout para determinar el sistema minimal de generadores del semigrupo $S = \mathrm{S}(]\frac{b}{a}, \frac{b}{a-1}[)$ cuando éste es simétrico.

LEMA 6.18. *Sea $\frac{b}{a} < \frac{n_1}{b_1} < \cdots < \frac{n_p}{b_p} < \frac{b}{a-1}$ una secuencia de Bézout propia. Entonces:*

1. $\frac{b}{a} < \frac{n_1}{b_1} < \cdots < \frac{n_p}{b_p}$ *es una secuencia de Bézout propia con extremos adyacentes,*
2. *el semigrupo* $\mathrm{S}([\frac{b}{a}, \frac{b}{a-1}])$ *está minimalmente generado por el conjunto* $\{b, n_1, \ldots, n_p\}$,
3. *si* $p = 1$, *entonces* $n_1 = 2$,
4. *si* $p \geq 2$, *entonces* $\{2b, b+n_1, \ldots, b+n_p\} \subseteq \langle n_1, \ldots, n_p \rangle$.

DEMOSTRACIÓN. Llamemos $S = \mathrm{S}(]\frac{b}{a}, \frac{b}{a-1}[)$ y $\overline{S} = \mathrm{S}([\frac{b}{a}, \frac{b}{a-1}])$.

1. Claramente $\frac{b}{a} < \frac{n_1}{b_1} < \cdots < \frac{n_p}{b_p}$ es una secuencia de Bézout propia. Ya que por hipótesis se verifica que $\frac{n_p}{b_p} < \frac{b}{a-1}$, sólo tenemos que comprobar la desigualdad $\frac{n_p}{b_p+1} < \frac{b}{a}$. Aplicando el Corolario 4.17 a la secuencia $\frac{b}{a} < \frac{n_1}{b_1} < \cdots < \frac{n_p}{b_p} < \frac{b}{a-1}$ obtenemos que $n_p \leq b$. De la desigualdad $\frac{n_p}{b_p} < \frac{b}{a-1}$ deducimos que $an_p < bb_p + n_p$. Por tanto resulta que $an_p < bb_p + b$, es decir, $\frac{n_p}{b_p+1} < \frac{b}{a}$.
2. Al ser $\frac{b}{a} < \frac{n_1}{b_1} < \cdots < \frac{n_p}{b_p} < \frac{b}{a-1}$ una secuencia de Bézout, el Teorema 4.8 establece que $\overline{S} = \langle b, n_1, \ldots, n_p \rangle$. Aplicando el Teorema 4.21 a la secuencia de Bézout que aparece en el apartado (1), obtenemos que $\overline{S}$ está minimalmente generado por el conjunto $\{b, n_1, \ldots, n_p\}$.
3. Si $\frac{b}{a} < \frac{n_1}{b_1} < \frac{b}{a-1}$ es una secuencia de Bézout, entonces $an_1 - bb_1 = 1$ y $bb_1 - (a-1)n_1 = 1$, de lo cual deducimos que $n_1 = 2$.
4. Puesto que en esta sección estamos suponiendo que $\mathrm{mcd}\{a, b\} = \mathrm{mcd}\{a-1, b\} = 1$, aplicando la Proposición 6.7 deducimos que $S = \overline{S} \setminus \{b\}$. Por el Teorema 6.9 y el Corolario 6.10 también sabemos que S es un semigrupo numérico simétrico con número de Frobenius b. Obsérvese además que el Lema 6.2 implica que $\langle n_1, \ldots, n_p \rangle \subseteq S$.

   Por el apartado (2) anterior sabemos que n_1 y b son dos generadores minimales de $\overline{S}$ distintos. De aquí llegamos a que $n_1 - b \notin \overline{S}$ y por tanto $n_1 - b \notin S$. Por la definición de semigrupo simétrico deducimos que $2b - n_1 \in S \subseteq \overline{S}$. Usando de nuevo el apartado (2), podemos escribir $2b - n_1 = \lambda b + a_1 n_1 + \cdots + a_p n_p$ para ciertos $\lambda, a_1, \ldots, a_p \in \mathbb{N}$. Pero $b \notin S$ y $\langle n_1, \ldots, n_p \rangle \subseteq S$, de lo cual deducimos que $\lambda = 0$ y por tanto $2b \in \langle n_1, \ldots, n_p \rangle$.

   Sea $i \in \{1, \ldots, p\}$. Como estamos suponiendo que $p \geq 2$, existe $j \in \{1, \ldots, p\} \setminus \{i\}$. Entonces n_i y n_j son dos generadores minimales de $\overline{S}$ distintos. Ésto implica que $n_j - n_i \notin \overline{S}$ y por tanto $n_j - n_i \notin S$. Al ser S un semigrupo simétrico, deducimos que $b + n_i - n_j \in S \subseteq \overline{S}$, es decir, $b + n_i - n_j = \lambda b + a_1 n_1 + \cdots + a_p n_p$ para ciertos $\lambda, a_1, \ldots, a_p \in \mathbb{N}$. Como $\{b, n_1, \ldots, n_p\}$ es el sistema minimal de generadores de $\overline{S}$, obtenemos que $\lambda = 0$ y por tanto $b + n_i \in \langle n_1, \ldots, n_p \rangle$.

□

TEOREMA 6.19. *Sea* $\frac{b}{a} < \frac{n_1}{b_1} < \cdots < \frac{n_p}{b_p} < \frac{b}{a-1}$ *una secuencia de Bézout propia. En tal caso:*

1. *si* $p = 1$, *entonces* $\{2, b+2\}$ *es el sistema minimal de generadores del semigrupo* $\mathrm{S}(]\frac{b}{a}, \frac{b}{a-1}[)$,
2. *si* $p \geq 2$, *entonces* $\{n_1, \ldots, n_p\}$ *es el sistema minimal de generadores del semigrupo* $\mathrm{S}(]\frac{b}{a}, \frac{b}{a-1}[)$.

DEMOSTRACIÓN. Llamemos $S = \mathrm{S}(]\frac{b}{a}, \frac{b}{a-1}[)$ y $\overline{S} = \mathrm{S}([\frac{b}{a}, \frac{b}{a-1}])$.

1. Por los apartados (2) y (3) en el Lema 6.18 sabemos que $\overline{S}$ está minimalmente generado por $\{2, b\}$. Puesto que por la Proposición 6.7 tenemos además que $S = \overline{S} \setminus \{b\}$, deducimos que $S = \langle 2, b+2 \rangle$.
2. Por el apartado (2) en el Lema 6.18, $\overline{S}$ está minimalmente generado por $\{b, n_1, \ldots, n_p\}$, y por la Proposición 6.7, $S = \overline{S} \setminus \{b\}$. Teniendo en cuenta además el apartado (4) en el Lema 6.18, se deduce fácilmente de aquí que S está minimalmente generado por el conjunto $\{n_1, \ldots, n_p\}$.

□

COMENTARIO 6.20. Observemos que si $p \geq 2$ y $\frac{b}{a} < \frac{n_1}{b_1} < \ldots < \frac{n_p}{b_p} < \frac{b}{a-1}$ es una secuencia de Bézout propia, entonces por el Teorema 6.19 y el Lema 4.8 tenemos que $\mathrm{S}(]\frac{b}{a}, \frac{b}{a-1}[) = \mathrm{S}([\frac{n_1}{b_1}, \frac{n_p}{b_p}])$. Aplicando el Lema 2.15 resulta que

$$\mathrm{S}\left(\left]\frac{b}{a}, \frac{b}{a-1}\right[\right) = \{x \in \mathbb{N} \mid b_1 n_p x \bmod n_1 n_p \leq (b_1 n_p - n_1 b_p)x\}.$$

□

Cerramos esta sección dando un ejemplo.

EJEMPLO 6.21. Sean $b = 5$ y $a = 2$, y sea el semigrupo $S = \mathrm{S}(]\frac{b}{a}, \frac{b}{a-1}[)$. De los Teoremas 6.9 y 6.17 resulta que S es un semigrupo numérico simétrico y proporcionalmente modular con número de Frobenius 5.

Nótese que $\frac{5}{2} < \frac{3}{1} < \frac{4}{1} < \frac{5}{1}$ es una secuencia de Bézout propia. Aplicando el Teorema 6.19 deducimos que $S = \langle 3, 4 \rangle$. Finalmente, por el Comentario 6.20 resulta que $S = \mathrm{S}([\frac{3}{1}, \frac{4}{1}]) = \mathrm{S}(4, 12, 1)$. □

4. Los generadores minimales en el caso pseudo-simétrico

Si a y b son dos números enteros verificando que $2 \leq a < b$, entonces observamos que $2 \leq b+1-a < b$, $\mathrm{mcd}\{a, b\} = \mathrm{mcd}\{b-a, a\}$ y $\mathrm{mcd}\{a-1, b\} = \mathrm{mcd}\{b+1-a, b\}$.

LEMA 6.22. *Si* a *y* b *son números enteros tales que* $2 \leq a < b$, *entonces* $\mathrm{S}(]\frac{b}{a}, \frac{b}{a-1}[) = \mathrm{S}(]\frac{b}{b+1-a}, \frac{b}{b-a}[)$.

DEMOSTRACIÓN. Por el Lema 6.2, es suficiente observar que $\frac{b}{a} < \frac{x}{k} < \frac{b}{a-1}$ si y sólo si $\frac{b}{b+1-a} < \frac{x}{x-k} < \frac{b}{b-a}$. □

Como consecuencia directa del Lema 6.22 y del Teorema 6.17 se obtiene el siguiente resultado que nos permite evitar el caso $\mathrm{mcd}\{a,b\}=1$ y $\mathrm{mcd}\{a-1,b\}=2$.

PROPOSICIÓN 6.23. *Sea S un semigrupo numérico. Entonces S es proporcionalmente modular y pseudo-simétrico si y sólo si $S=\langle 3,4,5\rangle$ ó $S=\mathrm{S}(]\frac{b}{a},\frac{b}{a-1}[)$, siendo a y b números enteros verificando que $2\leq a<b$, $\mathrm{mcd}\{a,b\}=2$ y $\mathrm{mcd}\{a-1,b\}=1$.*

A partir de ahora y hasta el final de la sección, a y b serán dos números enteros tales que $2\leq a<b$, $\mathrm{mcd}\{a,b\}=2$ y $\mathrm{mcd}\{a-1,b\}=1$.

Recordemos que un semigrupo numérico S se dice pseudo-simétrico si y sólo si $\mathrm{g}(S)$ es par y para cualquier entero x, si $x\in\mathbb{Z}\setminus S$, entonces $\mathrm{g}(S)-x\in S$ ó $x=\frac{\mathrm{g}(S)}{2}$.

LEMA 6.24. *Si $\frac{b/2}{a/2}<\frac{n_1}{b_1}<\cdots<\frac{n_p}{b_p}<\frac{b}{a-1}$ es una secuencia de Bézout propia, entonces:*

1. *$\frac{b/2}{a/2}<\frac{n_1}{b_1}<\cdots<\frac{n_p}{b_p}$ es una secuencia de Bézout propia con extremos adyacentes,*
2. *$\mathrm{S}([\frac{b}{a},\frac{b}{a-1}])$ está minimalmente generado por el conjunto $\{\frac{b}{2},n_1,\ldots,n_p\}$,*
3. *$\frac{b/2}{a/2}<\frac{\frac{b}{2}+n_1}{\frac{a}{2}+b_1}<\frac{n_1}{b_1}<\cdots<\frac{n_p}{b_p}<\frac{b}{a-1}$ es una secuencia de Bézout,*
4. *$\langle n_1,\ldots,n_p,\frac{b}{2}+n_1\rangle\subseteq\mathrm{S}(]\frac{b}{a},\frac{b}{a-1}[)$,*
5. *$3\frac{b}{2}=(a_1+1)n_1+a_2n_2+\cdots+a_pn_p$ para ciertos $a_1,a_2,\ldots,a_p\in\mathbb{N}$,*
6. *$2b\in\langle n_1,\ldots,n_p,\frac{b}{2}+n_1\rangle$,*
7. *si $p=1$, entonces $n_1=3$,*
8. *si $p\geq 2$, entonces $b+n_p\in\langle n_1,\ldots,n_p,\frac{b}{2}+n_1\rangle$,*
9. *si $p\geq 2$, entonces $\mathrm{S}(]\frac{b}{a},\frac{b}{a-1}[)=\langle n_1,\ldots,n_p,\frac{b}{2}+n_1\rangle$.*

DEMOSTRACIÓN. Llamemos $S=\mathrm{S}(]\frac{b}{a},\frac{b}{a-1}[)$ y $\overline{S}=\mathrm{S}([\frac{b}{a},\frac{b}{a-1}])$. De acuerdo con la Proposición 6.7 se verifica que $S=\overline{S}\setminus\{b,\frac{b}{2}\}$. Por el Teorema 6.9 y el Corolario 6.10 además sabemos que S es un semigrupo pseudo-simétrico con número de Frobenius igual a b.

1. Es evidente a partir de la hipótesis de que $\frac{b/2}{a/2}<\frac{n_1}{b_1}<\cdots<\frac{n_p}{b_p}$ es una secuencia de Bézout propia. De la desigualdad $\frac{b}{a-1}<\frac{\frac{b}{2}}{\frac{a}{2}-1}$ obtenemos que $\frac{n_p}{b_p}<\frac{\frac{b}{2}}{\frac{a}{2}-1}$. Siguiendo un razonamiento análogo al aplicado en la demostración del apartado (1) del Lema 6.18, deducimos que $\frac{n_p}{b_p+1}<\frac{b}{a}=\frac{b/2}{a/2}$.
2. La demostración es similar a la que dimos para el apartado (2) en el Lema 6.18.
3. Se puede comprobar fácilmente.
4. Teniendo en cuenta el Lema 4.8 y el apartado (3) obtenemos que $\langle n_1,\ldots,n_p,\frac{b}{2}+n_1\rangle=\mathrm{S}([\frac{\frac{b}{2}+n_1}{\frac{a}{2}+b_1},\frac{n_p}{b_p}])\subseteq S$.
5. Al ser n_1 y $\frac{b}{2}$ dos generadores minimales de $\overline{S}$ distintos, deducimos que $n_1-\frac{b}{2}\notin\overline{S}$, y por tanto $n_1-\frac{b}{2}\notin S$. De la definición de semigrupo pseudo-simétrico

obtenemos dos posibilidades: $b-(n_1-\frac{b}{2})\in S$ ó $n_1-\frac{b}{2}=\frac{b}{2}$. Si $n_1-\frac{b}{2}=\frac{b}{2}$, entonces $n_1=b$, lo que contradice que $b\notin S$. Deducimos por tanto que $3\frac{b}{2}-n_1\in\overline{S}$. Por el apartado (2) existen $\lambda,a_1,\ldots,a_p\in\mathbb{N}$ tales que $3\frac{b}{2}-n_1=\lambda\frac{b}{2}+a_1n_1+\cdots+a_pn_p$, es decir, $(3-\lambda)\frac{b}{2}=(a_1+1)n_1+a_2n_2+\cdots+a_pn_p$. Teniendo en cuenta que $\{\frac{b}{2},b\}\cap S=\emptyset$, deducimos que $\lambda=0$, de donde $3\frac{b}{2}=(a_1+1)n_1+a_2n_2+\cdots+a_pn_p$.

6. Sabemos que n_1 es un generador minimal de $\overline{S}$, $b\in\overline{S}$ y $n_1\neq b$. Ésto implica que $n_1-b\notin\overline{S}$. De nuevo por la definición de semigrupo pseudo-simétrico tenemos dos posibilidades: $b-(n_1-b)\in S$ ó $n_1-b=\frac{b}{2}$. Observamos que la igualdad $n_1-b=\frac{b}{2}$ no puede darse, pues de ser cierta contradiría que n_1 es un generador minimal de $\overline{S}$. Por consiguiente $2b-n_1\in\overline{S}$, lo que lleva a $2b-n_1=\lambda\frac{b}{2}+a_1n_1+\cdots+a_pn_p$ para ciertos $\lambda,a_1,\ldots,a_p\in\mathbb{N}$. Recordando que $\{\frac{b}{2},b\}\cap S=\emptyset$, deducimos que $\lambda\in\{0,1\}$ y así $2b\in\langle n_1,\ldots,n_p,\frac{b}{2}+n_1\rangle$.
7. Si $\frac{b/2}{a/2}<\frac{n_1}{b_1}<\frac{b}{a-1}$ es una secuencia de Bézout, entonces se verifican las igualdades $\frac{a}{2}n_1-\frac{b}{2}b_1=1$ y $bb_1-n_1(a-1)=1$, a partir de las cuales es inmediato deducir que $n_1=3$.
8. Al ser n_1 y n_p dos generadores minimales de $\overline{S}$ diferentes, tenemos que $n_1-n_p\notin\overline{S}$ y por tanto $n_1-n_p\notin S$. Por la definición de semigrupo pseudo-simétrico resultan dos posibilidades: $b-(n_1-n_p)\in S$ o $n_1-n_p=\frac{b}{2}$. La igualdad $n_1-n_p=\frac{b}{2}$ no puede darse ya que n_1 es un generador minimal de $\overline{S}$. Por consiguiente $b+n_p-n_1\in\overline{S}$, lo que significa que existen $\lambda,a_1,\ldots,a_p\in\mathbb{N}$ tales que $b+n_p-n_1=\lambda\frac{b}{2}+a_1n_1+\cdots+a_pn_p$. De aquí deducimos que $\lambda\in\{0,1\}$, y en consecuencia $b+n_p\in\langle n_1,\ldots,n_p,\frac{b}{2}+n_1\rangle$.
9. Por el apartado (4) ya sabemos que $\langle n_1,\ldots,n_p,\frac{b}{2}+n_1\rangle\subseteq S$. Ahora demostraremos que la otra inclusión también se verifica. Sea $x\in S$. Por el Lema 6.2 existe un entero positivo k tal que $\frac{b/2}{a/2}<\frac{x}{k}<\frac{b}{a-1}$. Distinguimos tres casos:
   a) Si $\frac{n_1}{b_1}\leq\frac{x}{k}\leq\frac{n_p}{b_p}$, entonces tenemos que $x\in \mathrm{S}([\frac{n_1}{b_1},\frac{n_p}{b_p}])$, lo cual por el Teorema 4.8 significa que $x\in\langle n_1,\ldots,n_p\rangle$.
   b) Si $\frac{n_p}{b_p}<\frac{x}{k}<\frac{b}{a-1}$, entonces $x\in \mathrm{S}([\frac{n_p}{b_p},\frac{b}{a-1}])$. Por el Teorema 4.8 ésto implica que $x\in\langle n_p,b\rangle$. Obsérvese que $x\neq b$ pues $x\in S$. Como consecuencia, $x=\lambda b+\mu n_p$ siendo $\lambda,\mu\in\mathbb{N}$ y $(\lambda,\mu)\neq(1,0)$. Ahora, teniendo en cuenta los apartados (5), (6) y (8), deducimos que $x\in\langle n_1,\ldots,n_p,\frac{b}{2}+n_1\rangle$.
   c) Si $\frac{b/2}{a/2}<\frac{x}{k}<\frac{n_1}{b_1}$, entonces $x\in \mathrm{S}([\frac{b/2}{a/2},\frac{n_1}{b_1}])$. Usando el Teorema 4.8 obtenemos que $x\in\langle\frac{b}{2},n_1\rangle$. La hipótesis $x\in S$ implica que $x\notin\{\frac{b}{2},b\}$, de donde $x=\lambda\frac{b}{2}+\mu n_1$ siendo $\lambda,\mu\in\mathbb{N}$ tales que $(\lambda,\mu)\notin\{(1,0),(2,0)\}$. Usando el apartado (5), deducimos que $x\in\langle n_1,\ldots,n_p,\frac{b}{2}+n_1,b+n_1\rangle$.

Hasta aquí hemos probado que $S \subseteq \langle n_1, \ldots, n_p, \frac{b}{2}+n_1, b+n_1\rangle$. Nótese que $b+n_1 \in S$ de donde $S = \langle n_1, \ldots, n_p, \frac{b}{2}+n_1, b+n_1\rangle$. Para concluir la demostración, probamos que $b+n_1$ no es un generador minimal de S. Análogamente a la demostración del apartado (8), deducimos que $n_p - n_1 \notin S$. Por la definición de semigrupo pseudo-simétrico tenemos dos posibilidades: $b-(n_p-n_1) \in S$ ó $n_p - n_1 = \frac{b}{2}$. Vemos que la igualdad $n_p - n_1 = \frac{b}{2}$ contradice el hecho de que n_p sea un generador minimal de $\overline{S}$. Por tanto $b+n_1-n_p \in S$ lo que significa que $b+n_1$ no puede ser un generador minimal de S.

□

El siguiente resultado es el Teorema 7 de [**35**].

LEMA 6.25. *Las siguientes condiciones son equivalentes para un semigrupo numérico S:*

1. *S es irreducible y verifica que* $\mathrm{m}(S) = \mathrm{e}(S) = 3$,
2. *S está generado por el conjunto* $\{3, x+3, 2x+3\}$ *siendo x un entero positivo que no es múltiplo de* 3.

COMENTARIO 6.26. Señalamos que en el lema anterior está implícito el hecho de que $x = \frac{\mathrm{g}(S)}{2}$. □

TEOREMA 6.27. *Sea* $\frac{b/2}{a/2} < \frac{n_1}{b_1} < \cdots < \frac{n_p}{b_p} < \frac{b}{a-1}$ *una secuencia de Bézout propia.*

1. *Si* $p = 1$, *entonces* $\{3, \frac{b}{2}+3, b+3\}$ *es el sistema minimal de generadores de* $\mathrm{S}(]\frac{b}{a}, \frac{b}{a-1}[)$.
2. *Si* $p \geq 2$, *entonces* $\{n_1, \ldots, n_p, \frac{b}{2}+n_1\}$ *es el sistema minimal de generadores de* $\mathrm{S}(]\frac{b}{a}, \frac{b}{a-1}[)$.

DEMOSTRACIÓN. Sea $S = \mathrm{S}(]\frac{b}{a}, \frac{b}{a-1}[)$.

1. Si $p = 1$, por los apartados (7) y (4) en el Lema 6.24 sabemos que $n_1 = 3$ y $\{3, \frac{b}{2}+3\} \subseteq S$. Ya que $\mathrm{g}(S) = b$, deducimos que $b+3 \in S$, con lo cual $\langle 3, \frac{b}{2}+3, b+3\rangle \subseteq S$. Al ser $\frac{b/2}{a/2} < \frac{n_1}{b_1}$ una secuencia de Bézout, resulta que $\mathrm{mcd}\{\frac{b}{2}, 3\} = 1$. Teniendo en cuenta esta observación y el hecho de que $2(\frac{b}{2}+3) > b+3$, es inmediato comprobar que el conjunto $\{3, \frac{b}{2}+3, b+3\}$ es independiente. En particular deducimos que $\mathrm{e}(S) = 3$. Para concluir la demostración basta tener en cuenta el Lema 6.25 y el Comentario 6.26.
2. Para hacer la demostración distinguimos dos casos:
   a) Si $n_1 > \frac{b}{2}$, entonces aplicando el Lema 4.17 deducimos que $\frac{b}{2} < n_1 < \cdots < n_p < b$. Obsérvese que como consecuencia del apartado (2) en el Lema 6.24 sabemos que el conjunto $\{n_1, \ldots, n_p\}$ es independiente. Por consiguiente sólo tenemos que demostrar que $\frac{b}{2}+n_1 \notin \langle n_1, \ldots, n_p\rangle$. Pero si $\frac{b}{2}+n_1 \in \langle n_1, \ldots, n_p\rangle$, entonces $\frac{b}{2}+n_1 = n_j$ para algún $j \in \{2, \ldots, p\}$, lo cual es imposible en vista de las desigualdades $\frac{b}{2} < n_1 < \cdots < n_p < b$.

b) Supongamos ahora que $\frac{b}{2} > n_1$ y probemos que $\frac{\frac{b}{2}+n_1}{\frac{a}{2}+b_1} < \frac{n_1}{b_1} < \cdots < \frac{n_p}{b_p} < \frac{b}{a-1}$ es una secuencia de Bézout propia de extremos adyacentes. Para demostrar que la secuencia es propia, es suficiente comprobar que $(\frac{a}{2}+b_1)n_i-(\frac{b}{2}+n_1)b_i \geq 2$ para todo $i \geq 2$, y $(\frac{a}{2}+b_1)b-(\frac{b}{2}+n_1)(a-1) \geq 2$. Por hipótesis se verifica que $\frac{a}{2}n_i-\frac{b}{2}b_i \geq 2$ y $b_1n_i-n_1b_i \geq 1$ para todo $i \geq 2$. Ésto implica que $(\frac{a}{2}+b_1)n_i-(\frac{b}{2}+n_1)b_i = \frac{a}{2}n_i-\frac{b}{2}b_i+b_1n_i-n_1b_i \geq 2$ para todo $i \geq 2$. La desigualdad $(\frac{a}{2}+b_1)b-(\frac{b}{2}+n_1)(a-1) \geq 2$ se deduce fácilmente teniendo en cuenta que $\frac{n_1}{b_1} < \frac{b}{a-1}$, es decir, $bb_1+n_1-an_1 \geq 1$. Probemos ahora la propiedad sobre los extremos adyacentes. A partir de la hipótesis $\frac{b/2}{a/2} < \frac{n_1}{b_1}$ deducimos $\frac{b/2}{a/2} < \frac{\frac{b}{2}+n_1}{\frac{a}{2}+b_1} < \frac{n_1}{b_1}$. Por consiguiente $\frac{b}{a} < \frac{\frac{b}{2}+n_1}{\frac{a}{2}+b_1}$. Esta desigualdad equivale a $b(\frac{a}{2}+b_1) < a(\frac{b}{2}+n_1)$.

Ahora comprobamos que $\frac{b}{a-1} < \frac{\frac{b}{2}+n_1}{\frac{a}{2}+b_1-1}$, es decir, $b(\frac{a}{2}+b_1)-b < a(\frac{b}{2}+n_1)-(\frac{b}{2}+n_1)$. Esta desigualdad es consecuencia inmediata de la hipótesis $\frac{b}{2} > n_1$ y de la desigualdad anteriomente deducida $b(\frac{a}{2}+b_1) < a(\frac{b}{2}+n_1)$.

Por tanto $\frac{\frac{b}{2}+n_1}{\frac{a}{2}+b_1} < \frac{n_1}{b_1} < \cdots < \frac{n_p}{b_p} < \frac{b}{a-1}$ es una secuencia de Bézout propia con extremos adyacentes. Ahora aplicando el Lema 4.21 deducimos que el conjunto $\{\frac{b}{2}+n_1, n_1, \ldots, n_p, b\}$ es independiente, por lo que también lo es el conjunto $\{\frac{b}{2}+n_1, n_1, \ldots, n_p\}$. En vista del apartado (9) del Lema 6.24 deducimos que S está minimalmente generado por el conjunto $\{n_1, \ldots, n_p, \frac{b}{2}+n_1\}$.

□

COMENTARIO 6.28. Como consecuencia del Teorema 6.27, el Lema 4.8 y el apartado (3) del Lema 6.24, si $\frac{b/2}{a/2} < \frac{n_1}{b_1} < \cdots < \frac{n_p}{b_p} < \frac{b}{a-1}$ es una secuencia de Bézout propia, entonces $\mathrm{S}(]\frac{b}{a}, \frac{b}{a-1}[) = \langle n_1, \ldots, n_p, \frac{b}{2}+n_1\rangle = \mathrm{S}([\frac{\frac{b}{2}+n_1}{\frac{a}{2}+b_1}, \frac{n_p}{b_p}])$. Aplicando el Lema 2.15 obtenemos que

$$\mathrm{S}\left(\left]\frac{b}{a}, \frac{b}{a-1}\right[\right) = \left\{x \in \mathbb{N} \mid n_p(\frac{a}{2}+b_1)x \bmod n_p(\frac{b}{2}+n_1) \leq (n_p(\frac{a}{2}+b_1)-b_p(\frac{b}{2}+n_1))x\right\}.$$

□

COMENTARIO 6.29. Observamos que bajo las hipótesis del Teorema 6.27, y usando el Corolario 1.6, se puede demostrar también que $\frac{\frac{b}{2}+n_1}{\frac{a}{2}+b_1} < \frac{n_1}{b_1} < \frac{n_2}{b_2} < \cdots < \frac{n_p}{b_p} < \frac{b}{a-1}$ es una secuencia de Bézout propia con extremos adyacentes, independientemente de la relación existente entre $\frac{b}{2}$ y n_1. □

EJEMPLO 6.30. Sea el semigrupo $S = \mathrm{S}(]\frac{14}{4}, \frac{14}{3}[)$. Por los Teoremas 6.9 y 6.17 sabemos que S es proporcionalmente modular y pseudo-simétrico con número de Frobenius igual a 14. Observar que $\frac{7}{2} < \frac{4}{1} < \frac{9}{2} < \frac{14}{3}$ es una secuencia de Bézout propia. Aplicando el Teorema 6.27 obtenemos que $S = \langle 4, 9, 11\rangle$ y por el Comentario 6.28 que $S = \mathrm{S}([\frac{11}{3}, \frac{9}{2}]) = \mathrm{S}(27, 99, 5)$. □

5. Semigrupos numéricos irreducibles con un número de Frobenius dado

Fijado b comenzamos estudiando las representaciones de la forma $S(]\frac{b}{a}, \frac{b}{a-1}[)$ para los semigrupos numéricos.

LEMA 6.31. *Sean $n_1 < n_2 < \cdots < n_p$ enteros positivos, σ una permutación del conjunto $\{1, \ldots, p\}$ y $\frac{n_{\sigma(1)}}{b_1} < \cdots < \frac{n_{\sigma(p)}}{b_p}$ una secuencia de Bézout propia tal que $1 < \frac{n_{\sigma(1)}}{b_1}$. Entonces $\mathrm{mcd}\{n_1, n_2\} = 1$ y $\{\frac{n_1}{n_2^{-1} \bmod n_1}, \frac{n_1}{n_1 - (n_2^{-1} \bmod n_1)}\} \cap \{\frac{n_{\sigma(1)}}{b_1}, \ldots, \frac{n_{\sigma(p)}}{b_p}\} \neq \emptyset$.*

DEMOSTRACIÓN. El Lema 4.17 implica que n_1 y n_2 han de ser los numeradores de dos fracciones consecutivas en la secuencia $\frac{n_{\sigma(1)}}{b_1} < \cdots < \frac{n_{\sigma(p)}}{b_p}$, ya sea de la forma $\cdots < \frac{n_1}{x_1} < \frac{n_2}{x_2} < \cdots$, o bien $\cdots < \frac{n_2}{x_2} < \frac{n_1}{x_1} < \cdots$. Al tratarse de una secuencia de Bézout con todas las fracciones mayores que 1, los denominadores x_1 y x_2 están determinados de forma única en cada caso. Más exactamente $x_1 = n_2^{-1} \bmod n_1$ ó $x_1 = n_1 - (n_2^{-1} \bmod n_1)$. □

Si S es un semigrupo numérico minimalmente generado por $n_1 < n_2 < \cdots < n_p$, recordemos que $\mathrm{m}(S)$ representa a n_1. Si además $p \geq 2$, llamamos $\mathrm{r}(S)$ a n_2.

TEOREMA 6.32. *Sea b un número entero mayor o igual que 3 y sean $a, a' \in \{2, \ldots, b-1\}$. Llamemos $S = \mathrm{S}(]\frac{b}{a}, \frac{b}{a-1}[)$ y $S' = \mathrm{S}(]\frac{b}{a'}, \frac{b}{a'-1}[)$. Si $\mathrm{m}(S) = \mathrm{m}(S')$ y $\mathrm{r}(S) = \mathrm{r}(S')$, entonces $a = a'$ ó $a + a' = b + 1$.*

DEMOSTRACIÓN. Supongamos que $\{n_1, \ldots, n_p\}$ es el sistema minimal de generadores de S. De acuerdo con el Lema 4.23 y el Teorema 4.24 sabemos que existe una ordenación de los generadores minimales de S, digamos $n_1, \ldots, n_p$, así como enteros positivos $b_1, \ldots, b_p$ de modo que $\frac{b}{a} < \frac{n_1}{b_1} < \cdots < \frac{n_p}{b_p} < \frac{b}{a-1}$, siendo $\frac{n_1}{b_1} < \cdots < \frac{n_p}{b_p}$ una secuencia de Bézout propia con extremos adyacentes. Aplicando el Lema 6.31 obtenemos dos casos posibles:

1. Supongamos que $\frac{b}{a} < \frac{\mathrm{m}(S)}{\mathrm{r}(S)^{-1} \bmod \mathrm{m}(S)} < \frac{b}{a-1}$. Ésto implica que

$$\frac{b(\mathrm{r}(S)^{-1} \bmod \mathrm{m}(S))}{\mathrm{m}(S)} < a < \frac{b(\mathrm{r}(S)^{-1} \bmod \mathrm{m}(S))}{\mathrm{m}(S)} + 1,$$

de donde deducimos que existe a lo sumo un entero positivo a verificando estas desigualdades.

2. Si $\frac{b}{a} < \frac{\mathrm{m}(S)}{\mathrm{m}(S)-(\mathrm{r}(S)^{-1} \bmod \mathrm{m}(S))} < \frac{b}{a-1}$, entonces

$$\frac{b(\mathrm{m}(S)-(\mathrm{r}(S)^{-1} \bmod \mathrm{m}(S)))}{\mathrm{m}(S)} < a < \frac{b(\mathrm{m}(S)-(\mathrm{r}(S)^{-1} \bmod \mathrm{m}(S)))}{\mathrm{m}(S)} + 1.$$

Vemos de nuevo que existe a lo sumo un entero positivo a verificando estas desigualdades.

Por tanto, si $\mathrm{m}(S) = \mathrm{m}(S')$, $\mathrm{r}(S) = \mathrm{r}(S')$ y $a \neq a'$, podemos suponer sin pérdida de generalidad que a verifica la condición del caso (1) y a' verifica la condición del caso (2). Tenemos pues que

$$\frac{b(\mathrm{r}(S)^{-1} \bmod \mathrm{m}(S))}{\mathrm{m}(S)} < a < \frac{b(\mathrm{r}(S)^{-1} \bmod \mathrm{m}(S))}{\mathrm{m}(S)} + 1, \quad \text{y}$$

$$\frac{b(\mathrm{m}(S)-(\mathrm{r}(S)^{-1} \bmod \mathrm{m}(S)))}{\mathrm{m}(S)} < a' < \frac{b(\mathrm{m}(S)-(\mathrm{r}(S)^{-1} \bmod \mathrm{m}(S)))}{\mathrm{m}(S)} + 1.$$

Ésto implica que $b < a + a' < b + 2$, de donde $a + a' = b + 1$. □

A continuación, a partir de este teorema deducimos varios corolarios.

COROLARIO 6.33. *Sea b un número entero mayor o igual que 3 y sean $a, a' \in \{2, \ldots, b-1\}$. Entonces $\mathrm{S}(]\frac{b}{a}, \frac{b}{a-1}[) = \mathrm{S}(]\frac{b}{a'}, \frac{b}{a'-1}[)$ si y sólo si $a = a'$ ó $a + a' = b + 1$.*

DEMOSTRACIÓN. El hecho de que "$a = a'$ ó $a + a' = b + 1$" sea condición necesaria, es consecuencia del Teorema 6.32, y que sea condición suficiente es consecuencia del Lema 6.22. □

COROLARIO 6.34.

1. *Si b es un número entero impar mayor o igual que 3, entonces el número de semigrupos simétricos proporcionalmente modulares con número de Frobenius b es igual a*

$$\#\{a \in \{2, \ldots, \frac{b+1}{2}\} \mid \mathrm{mcd}\{a, b\} = \mathrm{mcd}\{a-1, b\} = 1\}.$$

2. *Si b es un número entero par mayor o igual que 4, entonces el número de semigrupos pseudo-simétricos proporcionalmente modulares con número de Frobenius b es igual a*

$$\#\{a \in \{2, \ldots, b-1\} \mid \mathrm{mcd}\{a, b\} = 2, \mathrm{mcd}\{a-1, b\} = 1\}.$$

COROLARIO 6.35. *Sea b un número entero impar mayor o igual que 3. Entonces b es primo si y sólo si hay exactamente $\frac{b+1}{2} - 1$ semigrupos simétricos proporcionalmente modulares y con número de Frobenius b.*

EJEMPLO 6.36. Obtengamos todos los semigrupos simétricos proporcionalmente modulares con número de Frobenius 9.

Es inmediato comprobar que el conjunto

$$\{a \in \{2, 3, 4, 5\} \mid \mathrm{mcd}\{a, 9\} = \mathrm{mcd}\{a-1, 9\} = 1\}$$

es igual a $\{2,5\}$, de donde resultan los semigrupos $S(]\frac{9}{2},\frac{9}{1}[)$ y $S(]\frac{9}{5},\frac{9}{4}[)$. Como $\frac{9}{2}<\frac{5}{1}<\frac{6}{1}<\frac{7}{1}<\frac{8}{1}<\frac{9}{1}$ y $\frac{9}{5}<\frac{2}{1}<\frac{9}{4}$ son secuencias de Bézout propias, aplicando el Teorema 6.19 obtenemos que $S(]\frac{9}{2},\frac{9}{1}[)=\langle 5,6,7,8\rangle$ y $S(]\frac{9}{5},\frac{9}{4}[)=\langle 2,11\rangle$ son los únicos semigrupos simétricos proporcionalmente modulares cuyo número de Frobenius es igual a 9. □

EJEMPLO 6.37. Obtengamos todos los semigrupos pseudo-simétricos proporcionalmente modulares con número de Frobenius 10.

Calculamos en primer lugar el conjunto

$$\{a\in\{2,\dots,9\}\mid \operatorname{mcd}\{a,10\}=2,\ \operatorname{mcd}\{a-1,10\}=1\}$$

el cual es igual a $\{2,4,8\}$. Por tanto dichos semigrupos son $S(]\frac{10}{2},\frac{10}{1}[)$, $S(]\frac{10}{4},\frac{10}{3}[)$ y $S(]\frac{10}{8},\frac{10}{7}[)$. Ya que $\frac{5}{1}<\frac{6}{1}<\frac{7}{1}<\frac{8}{1}<\frac{9}{1}<\frac{10}{1}$, $\frac{5}{2}<\frac{3}{1}<\frac{10}{3}$ y $\frac{5}{4}<\frac{4}{3}<\frac{7}{5}<\frac{10}{7}$ son secuencias de Bézout propias, aplicando el Teorema 6.27 resulta $S(]\frac{10}{2},\frac{10}{1}[)=\langle 6,7,8,9,11\rangle$, $S(]\frac{10}{4},\frac{10}{3}[)=\langle 3,8,13\rangle$ y $S(]\frac{10}{8},\frac{10}{7}[)=\langle 4,7,9\rangle$.

Para cualquier entero positivo b definimos

$$\mathrm{X}(b)=\begin{cases}\{a\in\{1,\dots,b\}\mid \operatorname{mcd}\{a,b\}=\operatorname{mcd}\{a-1,b\}=1\} & \text{si } b \text{ es impar,}\\ \{a\in\{1,\dots,b\}\mid \operatorname{mcd}\{a,b\}=2,\ \operatorname{mcd}\{a-1,b\}=1\} & \text{si } b \text{ es par,}\end{cases}$$

y $\chi(b)=\#\mathrm{X}(b)$.

Con esta nueva notación el Corolario 6.34 se puede enunciar como sigue.

COROLARIO 6.38.

1. *Si b es un número entero impar mayor o igual que 3, entonces el número de semigrupos simétricos proporcionalmente modulares con número de Frobenius b es igual a $\chi(\frac{b+1}{2})$.*
2. *Si b es un número entero par mayor o igual que 4, entonces el número de semigrupos pseudo-simétricos proporcionalmente modulares con número de Frobenius b es igual a $\chi(b)$.*

A continuación vamos a estudiar algunas propiedades aritméticas que verifica la función χ.

LEMA 6.39.

1. $\chi(1)=\chi(2)=\chi(4)=1$.
2. *$\chi(2^k)=2^{k-2}$ para cualquier entero $k\geq 3$.*
3. *Si p es un número primo impar, entonces $\chi(p^k)=p^{k-1}(p-2)$ para cualquier entero positivo k.*
4. *Si b es un entero positivo impar, entonces $\chi(b)=\chi(2b)=\chi(4b)$.*
5. *Si b es un entero positivo impar, entonces $\chi(2^kb)=2\cdot\chi(2^{k-1}b)$ para cualquier entero $k\geq 3$.*

DEMOSTRACIÓN.

1. Son consecuencia inmediata de la definición.
2. Hemos de contar el número de enteros a tales que $1 \leq a \leq 2^k$ y $a = 2t$ con t impar. Ésto equivale a contar el número de enteros impares t tales que $1 \leq t \leq 2^{k-1}$. Dicho número es igual a 2^{k-2}.
3. Sea $p \geq 3$ un número primo y sea k un entero positivo. Tenemos que excluir del conjunto $\{1, \ldots, p^k\}$ todos los números que son de la forma $t \cdot p$ así como todos los de la forma $t \cdot p + 1$ con $1 \leq t \leq p^{k-1}$. Es inmediato ver que hay p^{k-1} números del primer tipo y p^{k-1} del segundo. Por tanto $\chi(p^k) = p^k - 2p^{k-1} = p^{k-1}(p-2)$.
4. Veamos en primer lugar que $\chi(b) = \chi(2b)$. Para ello definimos una aplicación f de $\mathrm{X}(b)$ en $\mathrm{X}(2b)$ como sigue:

$$f(a) = \begin{cases} a & \text{si } a \text{ es par,} \\ a+b & \text{si } a \text{ es impar.} \end{cases}$$

   Se puede verificar fácilmente que f está bien definida, y además que la aplicación g de $\mathrm{X}(2b)$ en $\mathrm{X}(b)$ dada por

$$g(a') = \begin{cases} a' & \text{si } a' < b, \\ a'-b & \text{en otro caso,} \end{cases}$$

   está bien definida y es la inversa de f. Por consiguiente f es biyectiva de lo cual deducimos que $\chi(b) = \chi(2b)$.

   Para probar ahora que $\chi(2b) = \chi(4b)$, de manera similar definimos la aplicación f de $\mathrm{X}(2b)$ en $\mathrm{X}(4b)$ como

$$f(a) = \begin{cases} a & \text{si } a \text{ no es múltiplo de 4,} \\ a+2b & \text{en otro caso.} \end{cases}$$

   Al igual que para el caso anterior, se puede comprobar fácilmente que f está bien definida y que la aplicación g de $\mathrm{X}(4b)$ en $\mathrm{X}(2b)$ dada por

$$g(a) = \begin{cases} a & \text{si } a < 2b, \\ a-2b & \text{en otro caso,} \end{cases}$$

   está bien definida y es la inversa de f. Por tanto f es una aplicación biyectiva y $\chi(2b) = \chi(4b)$.
5. Veamos primero la inclusión $\mathrm{X}(2^{k-1}b) \subseteq \mathrm{X}(2^k b)$. Si $a \in \mathrm{X}(2^{k-1}b)$, entonces $1 \leq a \leq 2^{k-1}b$, $\mathrm{mcd}\{a, 2^{k-1}b\} = 2$ y $\mathrm{mcd}\{a-1, 2^{k-1}b\} = 1$. Como estamos suponiendo que b es impar y $k \geq 3$, resulta que $1 \leq a \leq 2^k b$, $\mathrm{mcd}\{a, 2^k b\} = 2$ y $\mathrm{mcd}\{a-1, 2^k b\} = 1$, lo que significa que $a \in \mathrm{X}(2^k b)$.

   Probemos ahora que si $a \in \mathrm{X}(2^{k-1}b)$, entonces $a + 2^{k-1}b \in \mathrm{X}(2^k b)$. Para ello consideremos un elemento a verificando que $1 \leq a \leq 2^{k-1}b$, $\mathrm{mcd}\{a, 2^{k-1}b\} = 2$ y $\mathrm{mcd}\{a-1, 2^{k-1}b\} = 1$. Se verifica que $\mathrm{mcd}\{a + 2^{k-1}b, 2^k b\} = \mathrm{mcd}\{a + 2^{k-1}b, 2^{k-1}b\}$ pues $a + 2^{k-1}b$ es de la forma $2t$ con t impar. Además $\mathrm{mcd}\{a + 2^{k-1}b, 2^{k-1}b\} = \mathrm{mcd}\{a, 2^{k-1}b\} = 2$. Por tanto $\mathrm{mcd}\{a + 2^{k-1}b, 2^k b\} = 2$. De forma análoga, $\mathrm{mcd}\{a + 2^{k-1}b - 1, 2^k b\} =$

$\mathrm{mcd}\{a+2^{k-1}b-1, 2^{k-1}b\}$ (pues $a+2^{k-1}b-1$ es un número impar) y ésto es igual a $\mathrm{mcd}\{a-1, 2^{k-1}b\} = 1$. Por consiguiente $\mathrm{mcd}\{a+2^{k-1}b-1, 2^k b\} = 1$.

Por tanto hemos demostrado que

$$\mathrm{X}(2^{k-1}b) \cup \{a+2^{k-1}b \mid a \in \mathrm{X}(2^{k-1}b)\} \subseteq \mathrm{X}(2^k b).$$

Para concluir la demostración, consideremos $a' \in \mathrm{X}(2^k b)$. Si $a' < 2^{k-1}b$, entonces se deduce fácilmente que $a' \in \mathrm{X}(2^{k-1}b)$. Si $a' > 2^{k-1}b$, llamemos $a = a' - 2^{k-1}b$. Análogamente es fácil probar que $a \in \mathrm{X}(2^{k-1}b)$. Por tanto tenemos la igualdad

$$\mathrm{X}(2^{k-1}b) \cup \{a+2^{k-1}b \mid a \in \mathrm{X}(2^{k-1}b)\} = \mathrm{X}(2^k b).$$

Al verificarse además que $\mathrm{X}(2^{k-1}b) \cap \{a+2^{k-1}b \mid a \in \mathrm{X}(2^{k-1}b)\} = \emptyset$, deducimos que $\#\mathrm{X}(2^k b) = 2 \cdot \#\mathrm{X}(2^{k-1}b)$.

□

Sea f una **función de la teoría de los números**, es decir, f es una aplicación cuyo dominio es el conjunto de los enteros positivos. Se dice que f es **multiplicativa** si verifica la propiedad $f(m \cdot n) = f(m) \cdot f(n)$ para cualesquiera dos enteros positivos m y n primos relativos.

TEOREMA 6.40. *χ es una función multiplicativa de la teoría de los números.*

DEMOSTRACIÓN. Sea b y b' dos enteros positivos impares los cuales son primos relativos. En este caso, la multiplicatividad de χ se puede demostrar de manera similar a como se hace para "la función phi de Euler", es decir, considerando el isomorfismo $x \mapsto (x \bmod b, x \bmod b')$ del grupo de las unidades de $\mathbb{Z}_{bb'}$ en el grupo de las unidades de $\mathbb{Z}_b \times \mathbb{Z}_{b'}$. Para los casos restantes, la multiplicatividad de χ se deduce aplicando el Lema 6.39. □

EJEMPLO 6.41. El número de semigrupos numéricos pseudo-simétricos que son proporcionalmente modulares y cuyo número de Frobenius es igual a 1000 es $\chi(1000) = \chi(2^3 5^3) = \chi(2^3)\chi(5^3) = 2^1 5^2 (5-2) = 150$.

El número de semigrupos numéricos simétricos que son proporcionalmente modulares y cuyo número de Frobenius es igual a 1001 es $\chi(\frac{1001+1}{2}) = \chi(501) = \chi(3 \cdot 167) = \chi(3)\chi(167) = \chi(167) = 165$. □

6. Semigrupos modulares irreducibles

Incluimos en esta sección algunos resultados adicionales sobre semigrupos modulares irreducibles los cuales aparecen en trabajos recientes. Concretamente en [**32**], [**28**] y [**31**].

En esta sección a y b serán dos enteros no negativos tales que $0 \leq a < b$, $\mathrm{mcd}\{a,b\} = d$ y $\mathrm{mcd}\{a-1,b\} = d'$. Como $\mathrm{S}(0,b) = \mathrm{S}(1,b) = \mathbb{N}$, el cual es trivialmente simétrico, podemos suponer además que $a \geq 2$.

El punto de comienzo es el siguiente resultado que recoge varias propiedades básicas y que es consecuencia de los Corolarios 1.6, 1.18 y 1.19, y del Lema 1.12.

LEMA 6.42.

1. *Si* $x \in \mathbb{Z} \setminus \mathrm{S}(a,b)$, *entonces* $b-x \in \mathrm{S}(a,b)$.
2. *Sea* x *un entero positivo. Entonces* $x \in \mathrm{S}(a,b)$ *y* $b-x \in \mathrm{S}(a,b)$ *si y sólo si*

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

3. $b-d-d' \geq \mathrm{g}(\mathrm{S}(a,b))$.
4. $\mathrm{S}(a,b)$ *es simétrico si y sólo si* $\mathrm{g}(\mathrm{S}(a,b)) = b-d-d'$.
5. $\mathrm{S}(a,b)$ *es pseudo-simétrico si y sólo si* $\mathrm{g}(\mathrm{S}(a,b)) = b-d-d'-1$.

En [**32**] se hace un estudio de los semigrupos modulares simétricos en el que se analiza la relación existente entre los generadores y la representación modular del semigrupo.

Basándose en el lema anterior se demuestra el siguiente otro.

LEMA 6.43. $\mathrm{S}(a,b)$ *es simétrico si y sólo si* $b-d-d' \notin \mathrm{S}(a,b)$.

Además se incluye el siguiente resultado que se puede deducir de [**16**] (y que nosotros también utilizamos ya en la Sección 5 del Capítulo 4).

LEMA 6.44. *Si* $S = \langle n_1, n_2, n_3 \rangle$ *es un semigrupo numérico y* $(\mathrm{mcd}\{n_1,n_2\})n_3 \in \langle n_1, n_2 \rangle$, *entonces* S *es simétrico.*

Basándose en los dos últimos lemas se demuestra la siguiente proposición.

PROPOSICIÓN 6.45. $\mathrm{S}(a,b)$ *es simétrico si y sólo si* $\mathrm{S}(a,b) = \langle \frac{b}{d}, \frac{b}{d'}, d+d' \rangle$.

Como consecuencia de este último resultado, se deduce que si $\mathrm{S}(a,b)$ es simétrico, entonces $\mathrm{e}(S) \leq 3$.

A continuación se caracterizan aritméticamente las parejas (a,b) que dan lugar a semigrupos numéricos modulares y simétricos.

TEOREMA 6.46. $\mathrm{S}(a,b)$ *es simétrico si y sólo si* $(a,b) = (ut, ktt')$ *para ciertos enteros positivos* t, t', u, v *y* k *verificando que* $ut - vt' = 1$ *y* $k | u+v$.

Combinando la Proposición 6.45 y el Teorema 6.46 se obtiene el siguiente corolario.

COROLARIO 6.47. *Sea* S *un semigrupo numérico. Entonces* S *es simétrico y modular si y sólo si* $S = \langle kt, kt', t+t' \rangle$, *siendo* t, t' *y* k *enteros positivos tales que* $\mathrm{mcd}\{t,t'\} = \mathrm{mcd}\{k, t+t'\} = 1$. *Además en tal caso se cumple que* $\mathrm{g}(S) = ktt' - t - t'$.

El siguiente resultado determina cuándo un semigrupo numérico modular y simétrico tiene dimensión de inmersión igual a 3.

PROPOSICIÓN 6.48. *Sean* k, t *y* t' *enteros positivos tales que* $\mathrm{mcd}\{t,t'\} = \mathrm{mcd}\{k, t+t'\} = 1$. *Entonces* $\mathrm{e}(\langle kt, kt', t+t' \rangle) = 3$ *si y sólo si* $1 \notin \{k, t, t'\}$.

A continuación se observa que si g es un entero positivo impar, entonces $\langle 2, g+2\rangle$ es un semigrupo numérico modular cuyo número de Frobenius es igual a g. Se plantea el correspondiente problema inverso para el número de Frobenius cuando la dimensión de inmersión es igual a 3. Concretamente, ¿para qué números enteros positivos g existe un semigrupo modular S con dimensión de inmersión 3 y número de Frobenius g? Se incluye el siguiente resultado que da una respuesta parcial de tipo aritmético a este problema cuando S es además modular y simétrico.

COROLARIO 6.49. *Sea g un entero positivo. Existe un semigrupo numérico modular y simétrico con dimensión de inmersión 3 y número de Frobenius g si y sólo si $g = ktt' - t - t'$ para ciertos enteros k, t y t' mayores o iguales que 2 verificando que* $\mathrm{mcd}\{t, t'\} = \mathrm{mcd}\{k, t + t'\} = 1$.

Además se ofrece un ejemplo en el que se aplica el corolario anterior para demostrar que no existe ningún semigrupo numérico modular, simétrico, con dimensión de inmersión 3 y número de Frobenius 9.

Concluye dicho trabajo mostrando algunas familias de semigrupos numéricos modulares, simétricos y con dimensión de inmersión 3.

Incluimos también los siguientes resultados sobre semigrupos numéricos simétricos los cuales aparecen en [**28**].

LEMA 6.50. *Sea S un semigrupo numérico minimalmente generado por el conjunto $\{n_1 < n_2 < \cdots < n_e\}$ y supongamos que $e \geq 3$. Si $n_e = \mathrm{g}(S) + n_1$ y $S \setminus \{n_e\}$ es un semigrupo numérico simétrico, entonces $S \setminus \{n_e\}$ está minimalmente generado por $\{n_1, n_2, \ldots, n_{e-1}\}$.*

A partir de este lema se demuestra el siguiente teorema el cual nos permite construir semigrupos modulares simétricos con un número de Frobenius dado.

Recordemos que si x e y son enteros positivos primos relativos, denotamos por $\sigma_{x,y}$ la permutación perteneciente a S_{y-1} tal que $\sigma_{x,y}(i) = (xi) \bmod y$, para todo $i \in \{1, \ldots, y-1\}$. Además dada $\sigma \in \mathrm{S}_n$, definimos

$$\mathrm{I}(\sigma) = \{i \in \{1, \ldots, n\} \mid \sigma(i) \leq \sigma(j) \text{ para todo } j \in \{1, \ldots, i\}\}.$$

TEOREMA 6.51. *Sean $2 \leq t < b$ enteros positivos tales que* $\mathrm{mcd}\{t, d\} = \mathrm{mcd}\{t+1, b\} = 1$. *Entonces el semigrupo generado por $\{k + \sigma_{t,b}(k) \mid k \in \{1, \ldots, b-1\}\}$ es un semigrupo numérico simétrico con número de Frobenius b. Además* $\mathrm{e}(S) \leq \#\mathrm{I}(\sigma_{t,b})$.

De manera similar, en [**31**] se hace el correspondiente estudio para los semigrupos modulares pseudo-simétricos, cuyos resultados más destacados incluimos a continuación.

Teniendo en cuenta el Lema 6.42, se demuestran los siguientes.

LEMA 6.52. $\mathrm{S}(a, b)$ *es pseudo-simétrico si y sólo si* $b - d - d' - 1 \notin \mathrm{S}(a, b)$.

LEMA 6.53. *Si* $\mathrm{S}(a, b)$ *es pseudo-simétrico, entonces*

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

Basándose en los dos lemas anteriores se obtiene la siguiente caracterización para semigrupos modulares pseudo-simétricos.

LEMA 6.54. $\mathrm{S}(a,b)$ *es pseudo-simétrico si y sólo si* $0 < a(d+d'+1) \bmod b < d+d'+1$.

Combinando este último resultado con el Lema 1.3, se deduce el siguiente.

LEMA 6.55. *Si* $\mathrm{S}(a,b)$ *es pseudo-simétrico, entonces* $1 \in \{d,d'\}$.

Todos estos resultados dan lugar al siguiente teorema.

TEOREMA 6.56. *Sean a y b enteros positivos tales que* $2 \leq a < b$ *y* $\mathrm{mcd}\{a-1,b\} = 1$. *Sea* $d = \mathrm{mcd}\{a,b\}$. *Entonces* $\mathrm{S}(a,b)$ *es pseudo-simétrico si y sólo si* $0 < a(d+2) \bmod b < d+2$. *Además en dicho caso se verifica que* $\mathrm{S}(a,b) = \langle \frac{b}{d}, d+2, \frac{b+d+2}{2} \rangle$ *y* $\mathrm{g}(\mathrm{S}(a,b)) = b-d-2$.

Puesto que todo semigrupo numérico S verificando que $\mathrm{e}(S) \leq 2$ es simétrico, a partir del teorema anterior se obtiene la siguiente consecuencia.

COROLARIO 6.57. *Si* $\mathrm{S}(a,b)$ *es pseudo-simétrico, entonces* $\mathrm{e}(\mathrm{S}(a,b)) = 3$.

El siguiente resultado da otra caracterización para semigrupos modulares pseudo-simétricos.

TEOREMA 6.58. *Sean* $t < n$ *enteros positivos tales que t divide a n. Entonces* $\langle \frac{n}{t}, t+2, \frac{n+t+2}{2} \rangle$ *es un semigrupo modular pseudo-simétrico con número de Frobenius* $n-t-2$ *si y sólo si* $\frac{n}{t}$ *es impar y* $\mathrm{mcd}\{t+2, \frac{n}{t}\} = 1$.

Como consecuencia se deduce el siguiente corolario que da una respuesta parcial al problema inverso para el número de Frobenius cuando el semigrupo requerido es además modular y pseudo-simétrico.

COROLARIO 6.59. *Sea g un entero positivo. Existe un semigrupo modular pseudo-simétrico con número de Frobenius g si y sólo si existen enteros positivos* k,k' *tales que k es impar,* $k \geq 3$, $\mathrm{mcd}\{k'+2,k\} = 1$ *y* $g = kk'-k'-2$.

Por último indicar que en la Sección 4 del capítulo siguiente estudiaremos los semigrupos modulares $\mathrm{S}(a,b)$ irreducibles en los cuales a divide a b.

CAPÍTULO 7

Representaciones modulares

Sabemos que todo semigrupo proporcionalmente modular S distinto de $\mathbb{N}$ y de $\langle 2,3\rangle$, admite infinitas representaciones proporcionalmente modulares $S = \mathrm{S}(a,b,c)$ verificando que $c < a < b$ y $\mathrm{mcd}\{a,b,c\} = 1$ (véase el Teorema 2.13, el Comentario 2.14 y el Lema 4.37). En el caso particular en el que $c = 1$, simplemente escribimos $\mathrm{S}(a,b)$ en vez de $\mathrm{S}(a,b,1)$ y decimos que $\mathrm{S}(a,b)$ es una representación modular para S. En este capítulo estudiamos las representaciones modulares para un semigrupo numérico.

En la primera sección damos algunos resultados previos entre los que destacamos el Teorema 7.4 según el cual toda representación modular $\mathrm{S}(a,b)$ con $a < b$ para un semigrupo numérico S, está relacionada con una secuencia de Bézout cuyos numeradores son los generadores minimales de S, siendo alguno de sus extremos igual a $\frac{b}{a}$ ó $\frac{b}{a-1}$. Además obtenemos el Teorema 7.9 que da la unicidad de la representación modular para un semigrupo numérico bajo ciertas condiciones. Por el Corolario 2.36, todo semigrupo numérico generado por dos elementos es modular. En la sección segunda damos de forma explícita todas las representaciones modulares para un semigrupo numérico con dimensión de inmersión dos. En la sección tercera probamos en el Teorema 7.23 que para todo semigrupo modular S existen a lo sumo cuatro secuencias de Bézout propias cuyos numeradores son los generadores minimales de S y donde todas las fracciones que aparecen son mayores que 1. Destacamos también la Proposición 7.30 según la cual fijado el módulo b de una representación modular, existen exactamente dos valores para el factor a. Por consiguiente es crucial determinar cuántos módulos distintos pueden aparecer en una representación modular para un semigrupo numérico dado S, o al menos conocer una cota superior para el número de tales módulos. En la sección cuarta probamos que para un semigrupo numérico S, con $\mathrm{e}(S) \geq 3$, existen a lo sumo dos módulos posibles. Éste es el contenido del Teorema 7.36 en el cual damos de forma explícita las expresiones para dichos módulos en función de los generadores minimales de S y de $\mathrm{g}(S)$. Finalmente, en la sección quinta obtenemos el Teorema 7.42 en el que caracterizamos de forma aritmética aquellas representaciones modulares que pueden obtenerse para un semigrupo numérico S a partir de una secuencia de Bézout propia y con extremos adyacentes. Como consecuencia, damos un algoritmo para calcular todas las representaciones modulares para S y lo aplicamos a varios ejemplos.

Los resultados de este capítulo aparecen en [**44**].

1. Resultados básicos

Del Teorema 4.8 y del hecho ya conocido de que toda secuencia de Bézout puede refinarse a una secuencia propia, obtenemos el siguiente resultado.

LEMA 7.1. *Si* $\{n_1,\dots,n_p\}$ *es un conjunto independiente y* $\frac{n_1}{b_1} < \cdots < \frac{n_p}{b_p}$ *es una secuencia de Bézout, entonces dicha secuencia es propia.*

El siguiente resultado es una reformulación del Teorema 4.4 teniendo en cuenta el Comentario 4.14.

LEMA 7.2. *Sean* a_1, a_2, b_1 *y* b_2 *enteros positivos tales que* $\frac{a_1}{b_1} < \frac{a_2}{b_2}$ *y* $\mathrm{mcd}\{a_1,b_1\} = \mathrm{mcd}\{a_2,b_2\} = 1$. *Entonces existe una secuencia de Bézout propia de longitud menor o igual que* $a_2b_1 - a_1b_2 + 1$ *y con extremos* $\frac{a_1}{b_1}$ *y* $\frac{a_2}{b_2}$.

Como consecuencia de la demostración del Lema 4.23 y del Teorema 4.24 obtenemos la siguiente propiedad.

TEOREMA 7.3. *Sean* α *y* β *dos números racionales positivos tales que* $\alpha < \beta$ *y sea* $X = \{n_1,\dots,n_p\}$ *el sistema minimal de generadores del semigrupo* $\mathrm{S}([\alpha,\beta])$. *Entonces existe una ordenación de los elementos de* X, *digamos* $n_1,\dots,n_p$, *y enteros positivos* $b_1,\dots,b_p$ *tales que* $\frac{n_1}{b_1} < \frac{n_2}{b_2} < \cdots < \frac{n_p}{b_p}$ *es una secuencia de Bézout propia con extremos adyacentes y* $\alpha \le \frac{n_1}{b_1} < \frac{n_2}{b_2} < \cdots < \frac{n_p}{b_p} \le \beta$.

TEOREMA 7.4. *Sea* $S = \mathrm{S}(a,b)$ *con* $2 \le a < b$. *Entonces existe una secuencia de Bézout propia* $\frac{n_1}{b_1} < \frac{n_2}{b_2} < \cdots < \frac{n_p}{b_p}$ *con extremos adyacentes, tal que:*

1. $\{n_1,\dots,n_p\}$ *es el sistema minimal de generadores de* S,
2. $\frac{b}{a} \le \frac{n_1}{b_1} \le \dots \le \frac{n_p}{b_p} \le \frac{b}{a-1}$,
3. $\frac{b}{a} = \frac{n_1}{b_1}$ *ó* $\frac{b}{a-1} = \frac{n_p}{b_p}$.

DEMOSTRACIÓN. Aplicando el Lema 2.15 obtenemos que $S = \mathrm{S}([\frac{b}{a}, \frac{b}{a-1}])$. Por el Teorema 7.3, si $\{n_1,\dots,n_p\}$ es el sistema minimal de generadores de S, entonces existe una secuencia de Bézout propia $\frac{n_1}{b_1} < \frac{n_2}{b_2} < \cdots < \frac{n_p}{b_p}$ con extremos adyacentes tal que $\frac{b}{a} \le \frac{n_1}{b_1} < \frac{n_2}{b_2} < \cdots < \frac{n_p}{b_p} \le \frac{b}{a-1}$. Además el Teorema 4.8 nos garantiza que $S = \mathrm{S}\left(\left[\frac{n_1}{b_1}, \frac{n_p}{b_p}\right]\right)$. Al ser b un elemento de S, del Lema 2.16 deducimos que existe un entero positivo y verificando que $\frac{n_1}{b_1} \le \frac{b}{y} \le \frac{n_p}{b_p}$. Por tanto obtenemos que $\frac{b}{a} \le \frac{n_1}{b_1} \le \frac{b}{y} \le \frac{n_p}{b_p} \le \frac{b}{a-1}$, de forma que $y = a$ ó $y = a-1$, y por consiguiente $\frac{b}{a} = \frac{n_1}{b_1}$ ó $\frac{b}{a-1} = \frac{n_p}{b_p}$. □

COMENTARIO 7.5. En relación con el teorema anterior, nótese que si $\frac{n_1}{b_1} < \frac{n_2}{b_2} < \cdots < \frac{n_p}{b_p}$ es una secuencia de Bézout propia de extremos adyacentes para la cual se verifican los enunciados de los apartados (1) y (2), entonces también se verifica el enunciado del apartado (3). □

Con la notación del Teorema 7.4, por ser $\frac{n_1}{b_1} < \frac{n_2}{b_2} < \cdots < \frac{n_p}{b_p}$ una secuencia de Bézout, ha de verificarse que $\mathrm{mcd}\{n_i, b_i\} = 1$ para todo i. Observamos además que si $\frac{b}{a} = \frac{n_1}{b_1}$, entonces $b = kn_1$ y $a = kb_1$, con $k = \mathrm{mcd}\{a,b\}$, resultando por tanto $S = \mathrm{S}(kb_1, kn_1)$.

A continuación estudiamos la relación existente entre los semigrupos de la forma $\mathrm{S}(ka,kb)$ cuando k varía en $\mathbb{N}$.

LEMA 7.6. *Sean a,b,k k' enteros positivos tales que $a < b$ y $k \leq k'$. Entonces* $\mathrm{S}(k'a,k'b) \subseteq \mathrm{S}(ka,kb)$.

DEMOSTRACIÓN. Tenemos $\frac{kb}{ka} = \frac{k'b}{k'a} < \frac{k'b}{k'a-1} \leq \frac{kb}{ka-1}$, lo que implica que $[\frac{k'b}{k'a}, \frac{k'b}{k'a-1}] \subseteq [\frac{kb}{ka}, \frac{kb}{ka-1}]$, y de aquí deducimos que $\mathrm{S}(k'a,k'b) = \mathrm{S}([\frac{k'b}{k'a}, \frac{k'b}{k'a-1}]) \subseteq \mathrm{S}([\frac{kb}{ka}, \frac{kb}{ka-1}]) = \mathrm{S}(ka,kb)$. □

Recordemos que para un semigrupo numérico S, el conjunto de los huecos de S es el conjunto $\mathrm{H}(S) = \mathbb{N} \setminus S$.

PROPOSICIÓN 7.7. *Sean a,b,k y k' enteros positivos verificando que* $\mathrm{mcd}\{a,b\} = 1$ *y $k \leq k'$. Si* $\mathrm{S}(ka,kb) = \mathrm{S}(k'a,k'b)$, *entonces $k' = k$ ó $k' = k+1$.*

DEMOSTRACIÓN. De acuerdo con el Lema 7.6 siempre se verifica que $\mathrm{S}(k'a,k'b) \subseteq \mathrm{S}(ka,kb)$. Se dará la igualdad si y sólo si ambos semigrupos tienen el mismo número de huecos. Por el Teorema 1.13, vemos que ésto equivale a que se verifique la igualdad

$$k'b - \mathrm{mcd}\{k'a,k'b\} - \mathrm{mcd}\{k'a-1,k'b\} = kb - \mathrm{mcd}\{ka,kb\} - \mathrm{mcd}\{ka-1,kb\}.$$

Como estamos suponiendo que $\mathrm{mcd}\{a,b\} = 1$, dicha igualdad se puede escribir como

$$k'b - k' - \mathrm{mcd}\{k'a-1,b\} = kb - k - \mathrm{mcd}\{ka-1,b\},$$

y por tanto

$$k'(b-1) = k(b-1) + \mathrm{mcd}\{k'a-1,b\} - \mathrm{mcd}\{ka-1,b\}.$$

Observar que en nuestro contexto se verifica que $\mathrm{mcd}\{k'a-1,b\} - \mathrm{mcd}\{ka-1,b\} \leq b-1$, dándose la igualdad si y sólo si $\mathrm{mcd}\{k'a-1,b\} = b$ y $\mathrm{mcd}\{ka-1,b\} = 1$. Deducimos que $k'(b-1) \leq (k+1)(b-1)$, y en consecuencia $k' \leq k+1$. Puesto que estamos suponiendo además que $k \leq k'$, obtenemos que $k' = k$ ó $k' = k+1$. □

El siguiente corolario caracteriza cuándo se da la igualdad en la Proposición 7.7.

COROLARIO 7.8. *Sean a,b y k enteros positivos tales que* $\mathrm{mcd}\{a,b\} = 1$. *Entonces* $\mathrm{S}(ka,kb) = \mathrm{S}((k+1)a,(k+1)b)$ *si y sólo si* $\mathrm{mcd}\{(k+1)a-1,b\} = b$ *y* $\mathrm{mcd}\{ka-1,b\} = 1$. *Además en tal caso* $\mathrm{S}(ka,kb) = \mathrm{S}((k+1)a,(k+1)b) = \langle b,k+1\rangle$.

DEMOSTRACIÓN. La demostración de la primera parte del enunciado está contenida en la demostración de la Proposición 7.7, por lo que sólo probaremos la segunda parte. De las hipótesis deducimos que $b|(k+1)a-1$, lo que significa que

existe un entero positivo u tal que $(k+1)a - bu = 1$. Ésto implica que las fracciones $\frac{b}{a} < \frac{k+1}{u}$ constituyen una secuencia de Bézout. De las igualdades $\frac{b}{a} = \frac{(k+1)b}{(k+1)a}$ y $\frac{k+1}{u} = \frac{(k+1)b}{ub} = \frac{(k+1)b}{(k+1)a-1}$ obtenemos que $[\frac{(k+1)b}{(k+1)a}, \frac{(k+1)b}{(k+1)a-1}] = [\frac{b}{a}, \frac{k+1}{u}]$ y por tanto $\mathrm{S}((k+1)a,(k+1)b) = \mathrm{S}([\frac{b}{a}, \frac{k+1}{u}])$. Tal y como hemos observado anteriormente, $\frac{b}{a} < \frac{k+1}{u}$ es una secuencia de Bézout, por lo que aplicando el Teorema 4.8, finalmente resulta que $\mathrm{S}([\frac{b}{a}, \frac{k+1}{u}]) = \langle b, k+1\rangle$. □

Recordemos que por el Lema 1.3, si a y b son enteros positivos tales que $a < b$, entonces $\mathrm{S}(a,b) = \mathrm{S}(b+1-a,b)$. Diremos que $\mathrm{S}(a,b)$ y $\mathrm{S}(b+1-a,b)$ son **representaciones modulares simétricas**. También diremos que a y $b+1-a$ son dos valores simétricos respecto de b.

El siguiente teorema será utilizado en secciones siguientes para estudiar la unicidad de las representaciones modulares.

TEOREMA 7.9. *Supongamos que* $S = \mathrm{S}(a,b) = \mathrm{S}(a',b')$ *con* $\mathrm{e}(S) \geq 3$. *Si* $\frac{b}{a} = \frac{b'}{a'}$ *ó* $\frac{b}{a-1} = \frac{b'}{a'-1}$, *entonces* $a = a'$ *y* $b = b'$.

DEMOSTRACIÓN.

1. Si $\frac{b}{a} = \frac{b'}{a'}$, entonces existen enteros positivos c,d,k y k' tales que $\mathrm{mcd}\{c,d\} = 1, a = kc, b = kd, a' = k'c$ y $b' = k'd$. Por tanto $\mathrm{S}(kc,kd) = \mathrm{S}(k'c,k'd)$. La hipótesis $\mathrm{e}(S) \geq 3$ evita el caso $|k-k'| = 1$ que fué tratado en el Corolario 7.8, con lo cual, aplicando la Proposición 7.7 obtenemos que $k = k'$ y por consiguiente $a = a'$ y $b = b'$.
2. Si $\frac{b}{a-1} = \frac{b'}{a'-1}$, entonces $\frac{b}{b-(a-1)} = \frac{b'}{b'-(a'-1)}$. Aplicando el Lema 1.3 a la hipótesis $S = \mathrm{S}(a,b) = \mathrm{S}(a',b')$, deducimos que $S = \mathrm{S}(b-(a-1),b) = \mathrm{S}(b'-(a'-1),b')$. Vemos por tanto que hemos reducido la demostración al caso anterior ya demostrado.

□

Sea $\mathrm{S}(a,b)$ una representación modular para un semigrupo modular S minimalmente generado por un conjunto $\{n_1,\ldots,n_p\}$. A la vista del Teorema 7.4, sabemos que existe una secuencia de Bézout $\frac{n_1}{b_1} < \cdots < \frac{n_p}{b_p}$ verificando que $\frac{b}{a} = \frac{n_1}{b_1}$ ó $\frac{b}{a-1} = \frac{n_p}{b_p}$ (pudiendo darse ambas posibilidades simultáneamente). Además, si imponemos que $\mathrm{e}(S) \geq 3$, entonces por el Teorema 7.9 deducimos que existe únicamente un par ordenado (a,b) verificando que $\frac{b}{a} = \frac{n_1}{b_1}$. Estas observaciones nos indican que existe una relación muy estrecha entre las representaciones modulares para S y las secuencias de Bézout con numeradores $n_1,\ldots,n_p$. Dicha relación será ampliamente estudiada en la Sección 4. Previamente describimos las representaciones modulares para el caso $\mathrm{e}(S) = 2$.

2. Las representaciones modulares para un semigrupo numérico S con dimensión de inmersión dos

Ya conocemos por el Corolario 2.36 que todo semigrupo numérico S con $\mathrm{e}(S)=2$ es modular. Nuestro propósito en esta sección es demostrar el Teorema 7.11 el cual afirma que todo semigrupo numérico con dimensión de inmersión dos tiene a lo sumo seis representaciones modulares.

Dado el semigrupo numérico $S=\langle n_1,n_2\rangle$, el siguiente lema muestra tres representaciones modulares diferentes para S. Por simetría (es decir, aplicando el Lema 1.3) resultarán pues a lo sumo seis representaciones modulares para S.

LEMA 7.10. *Sean $n_1,n_2\in\mathbb{N}\setminus\{0,1\}$, $u\in\{1,\dots,n_1-1\}$ y $v\in\{1,\dots,n_2-1\}$ tales que $un_2-vn_1=1$. Entonces se verifica*

$$\langle n_1,n_2\rangle=\mathrm{S}(un_2,n_1n_2)=\mathrm{S}(u(n_2-1),n_1(n_2-1))=\mathrm{S}(un_2-v,n_2(n_1-1)).$$

DEMOSTRACIÓN. Comprobemos la validez de cada representación modular separadamente.

1. Puesto que $[\frac{n_1n_2}{un_2},\frac{n_1n_2}{un_2-1}]=[\frac{n_1}{u},\frac{n_2}{v}]$, usando el Lema 2.15 y el Teorema 4.8, resulta $\mathrm{S}(un_2,n_1n_2)=\mathrm{S}([\frac{n_1}{u},\frac{n_2}{v}])=\langle n_1,n_2\rangle$.
2. Llamemos $S=\mathrm{S}(u(n_2-1),n_1(n_2-1))$. Para probar que S es igual a $\langle n_1,n_2\rangle$, es suficiente ver que $\{n_1,n_2\}\subseteq S$ y $\#\mathrm{H}(S)=\#\mathrm{H}(\langle n_1,n_2\rangle)$. Trivialmente se verifica que $u(n_2-1)n_1 \bmod n_1(n_2-1)=0\leq n_1$, lo cual implica que $n_1\in S$. Ahora multiplicando los tres miembros de la congruencia $1+vn_1\equiv 1 \bmod n_1$ por n_2-1, resulta $(n_2-1)(1+vn_1)\equiv n_2-1 \bmod (n_2-1)n_1$, de donde $u(n_2-1)n_2 \bmod n_1(n_2-1)=(n_2-1)(1+vn_1) \bmod (n_2-1)n_1=n_2-1\leq n_2$, lo cual significa que $n_2\in S$.

   Ahora comprobamos la coincidencia de los números de huecos de ambos semigrupos. Aplicando el Teorema 1.13, obtenemos que $\#\mathrm{H}(S)$ es igual a

   $$\tfrac{1}{2}\big(n_1(n_2-1)+1-\mathrm{mcd}\{u(n_2-1),n_1(n_2-1)\}-\mathrm{mcd}\{u(n_2-1)-1,n_1(n_2-1)\}\big).$$

   Observemos que $\mathrm{mcd}\{u(n_2-1),n_1(n_2-1)\}=n_2-1$ y $\mathrm{mcd}\{u(n_2-1)-1,n_1(n_2-1)\}=1$, pues $v(n_1(n_2-1))-n_2(u(n_2-1)-1)=1$. Por tanto resulta que $\#\mathrm{H}(S)=\frac{1}{2}(n_1-1)(n_2-1)$, y en vista del Lema 0.2 concluimos la prueba.
3. Sea ahora $S=\mathrm{S}(un_2-v,n_2(n_1-1))$. Aplicamos un argumento similar al usado en la demostración del apartado (2) para probar que $S=\langle n_1,n_2\rangle$. El hecho de que $n_1\in S$ se deduce de que $(un_2-v)n_1 \bmod n_2(n_1-1)=(un_1n_2-vn_1) \bmod n_2(n_1-1)=(un_1n_2+1-un_2) \bmod n_2(n_1-1)=(un_2(n_1-1)+1) \bmod n_2(n_1-1)=1\leq n_1$. De forma análoga $(un_2-v) \bmod (n_1-1)=(1+vn_1-v) \bmod (n_1-1)=1$ implica que $(un_2-v)n_2 \bmod n_2(n_1-1)=n_2$, lo que lleva a que $n_2\in S$. Nótese que $\mathrm{mcd}\{un_2-v,n_2(n_1-1)\}=1$, pues se tiene la igualdad $n_1(un_2-v)-un_2(n_1-1)=1$. Además se puede comprobar fácilmente que $\mathrm{mcd}\{un_2-v-1,n_2(n_1-1)\}=\mathrm{mcd}\{1+vn_1-$

$v-1, n_2(n_1-1)\} = n_1-1$. Aplicando ahora el Teorema 1.13, resulta que $\#\mathrm{H}(S) = \frac{1}{2}(n_1-1)(n_2-1)$ y por el Lema 0.2 concluimos la demostración.

□

Ya estamos en condiciones de probar que las representaciones modulares para $\langle n_1, n_2\rangle$ dadas en el Lema 7.10 son las únicas posibles, salvo simetría.

TEOREMA 7.11. *Sean $n_1, n_2 \in \mathbb{N}\setminus\{0,1\}$, $u \in \{1,\dots,n_1-1\}$ y $v \in \{1,\dots,n_2-1\}$ tales que $un_2 - vn_1 = 1$. Los siguientes enunciados son equivalentes:*

1. $\langle n_1, n_2\rangle = \mathrm{S}(a,b)$, *para ciertos enteros positivos $a < b$,*
2. $$(a,b) \in \left\{ \begin{array}{l} (u(n_2-1), n_1(n_2-1)), \\ ((n_1-u)(n_2-1)+1, n_1(n_2-1)), \\ (un_2 - v, n_2(n_1-1)), \\ ((n_2-v)(n_1-1), n_2(n_1-1)), \\ (un_2, n_1n_2), \\ (n_2(n_1-u)+1, n_1n_2) \end{array} \right\}.$$

DEMOSTRACIÓN.

(2) $\Rightarrow$ (1) Es consecuencia de los Lemas 7.10 y 1.3.

(1) $\Rightarrow$ (2) Observemos en primer lugar que $\frac{n_1}{u} < \frac{n_2}{v}$ y $\frac{n_2}{n_2-v} < \frac{n_1}{n_1-u}$ son las únicas secuencias de Bézout con numeradores n_1, n_2 y cuyas fracciones son todas mayores que 1. Si $\langle n_1, n_2\rangle = \mathrm{S}(a,b)$ para ciertos enteros positivos $a < b$, entonces por el Teorema 7.4 resulta $\frac{b}{a} = \frac{n_1}{u}$ ó $\frac{b}{a-1} = \frac{n_2}{v}$ ó $\frac{b}{a} = \frac{n_2}{n_2-v}$ ó $\frac{b}{a-1} = \frac{n_1}{n_1-u}$. Distinguimos dos casos:

1. Supongamos que $b \neq n_1n_2$. Si $\frac{b}{a} = \frac{n_1}{u}$, entonces por la Proposición 7.7 y el Corolario 7.8 deducimos que b y a están determinados de manera única; para ver ésto, observemos que si se verifica que $\frac{b}{a} = \frac{b'}{a'}$ y $\mathrm{S}(a,b) = \mathrm{S}(a',b') = \langle n_1, n_2\rangle$, siendo $b' = \max\{b,b'\}$, entonces el Corolario 7.8 implica $b' = n_1n_2$, lo que contradice la hipótesis. Como por el Lema 7.10 ya conocemos que $\mathrm{S}(u(n_2-1), n_1(n_2-1)) = \langle n_1, n_2\rangle$ y además se verifica que $\frac{n_1(n_2-1)}{u(n_2-1)} = \frac{n_1}{u}$, deducimos que $(a,b) = (u(n_2-1), n_1(n_2-1))$. Procediendo análogamente para los restantes subcasos se obtienen las siguientes conclusiones: si $\frac{b}{a-1} = \frac{n_2}{v}$, entonces $(a,b) = (un_2 - v, n_2(n_1-1))$; si $\frac{b}{a} = \frac{n_2}{n_2-v}$, entonces $(a,b) = ((n_2-v)(n_1-1), n_2(n_1-1))$; si $\frac{b}{a-1} = \frac{n_1}{n_1-u}$, entonces $(a,b) = ((n_1-u)(n_2-1)+1, n_1(n_2-1))$.
2. Supongamos ahora $b = n_1n_2$. Si $\frac{n_1n_2}{a} = \frac{n_1}{u}$ o bien $\frac{n_1n_2}{a-1} = \frac{n_2}{v}$, entonces $a = un_2$. Si $\frac{n_1n_2}{a} = \frac{n_2}{n_2-v}$ ó $\frac{n_1n_2}{a-1} = \frac{n_1}{n_1-u}$, entonces $a = n_2(n_1-u)+1$.

□

EJEMPLO 7.12. Obtengamos todas las representaciones modulares para el semigrupo $S = \langle 5, 7\rangle$.

De acuerdo con el Teorema 7.11, tenemos $n_1 = 7, n_2 = 5, u = 3$ y $v = 2$, de donde $S = \mathrm{S}(12,28) = \mathrm{S}(17,28) = \mathrm{S}(13,30) = \mathrm{S}(18,30) = \mathrm{S}(15,35) = \mathrm{S}(21,35)$. □

EJEMPLO 7.13. Obtengamos todas las representaciones modulares para el semigrupo numérico $S = \langle n, n+1\rangle$, con $n \geq 2$.

De acuerdo con el Teorema 7.11, identificamos $n_1 = n, n_2 = n+1, u = 1$ y $v = 1$, obteniendo las representaciones modulares $S = \mathrm{S}(n+1, n(n+1)) = \mathrm{S}(n, n^2) = \mathrm{S}(n, (n-1)(n+1))$, a las cuales hemos de añadir las correspondientes representaciones simétricas $S = \mathrm{S}(n^2, n(n+1)) = \mathrm{S}(n^2-n+1, n^2) = \mathrm{S}((n-1)n, (n-1)(n+1))$.

Obsérvese que para $n = 2$ (y sólo para este valor) las representaciones $\mathrm{S}(n, (n-1)(n+1))$ y $\mathrm{S}((n-1)n, (n-1)(n+1))$ son la misma, por lo que en este caso se obtienen exactamente cinco representaciones modulares diferentes: $\mathrm{S}(2,3), \mathrm{S}(2,4), \mathrm{S}(3,4), \mathrm{S}(3,6)$ y $\mathrm{S}(4,6)$. □

Recordemos del Lema 1.8 que para b impar se verifica $\langle 2, b\rangle = \mathrm{S}(\frac{1}{2}(b+1), b)$. Esta situación se resuelve totalmente en el ejemplo siguiente.

EJEMPLO 7.14. Sea $b \geq 3$ un número entero impar y sea $S = \langle 2, b\rangle$. Llamando $n_1 = 2$, $n_2 = b$, $u = 1$ y $v = \lfloor \frac{b}{2} \rfloor$, si aplicamos el Teorema 7.11 obtenemos que las únicas representaciones modulares para S son $\mathrm{S}(b, 2b), \mathrm{S}(b-1, 2(b-1))$ y $\mathrm{S}(b - \lfloor \frac{b}{2} \rfloor, b)$, a las cuales hemos de añadir las correspondientes representaciones simétricas $\mathrm{S}(b+1, 2b), \mathrm{S}(b, 2(b-1))$ y $\mathrm{S}(\lfloor \frac{b}{2} \rfloor + 1, b)$.

Como b es impar tenemos $b - \lfloor \frac{b}{2} \rfloor = \lfloor \frac{b}{2} \rfloor + 1$, por lo cual S tiene exactamente cinco representaciones modulares diferentes: $\mathrm{S}(b, 2b), \mathrm{S}(b+1, 2b), \mathrm{S}(b-1, 2(b-1)), \mathrm{S}(b, 2(b-1))$ y $\mathrm{S}(\lfloor \frac{b}{2} \rfloor + 1, b)$. □

COMENTARIO 7.15. Los semigrupos del Ejemplo 7.14 constituyen el único caso en el cual un semigrupo numérico $S = \langle n_1, n_2\rangle$ tiene exactamente cinco representaciones modulares.

1. Existe una única representación modular para S con el módulo $n_1 n_2$ si y sólo si $n_1 n_2 + 1 - u n_2 = u n_2$, es decir, $n_2(2u - n_1) = 1$, lo cual es imposible.
2. Existe una única representación modular para S con el módulo $n_1(n_2 - 1)$ si y sólo si $n_1(n_2-1) + 1 - u(n_2-1) = u(n_2-1)$, es decir, $(2u - n_1)(n_2 - 1) = 1$. Ésto implica que $n_1 = 2u - 1$ y $n_2 = 2$.
3. Por último, existe una única representación modular para S con el módulo $n_2(n_1 - 1)$ si y sólo si $n_2(n_1-1) + 1 - u(n_2 - v) = u(n_2 - v)$. Usando que $u n_2 - v n_1 = 1$, ello equivale a $n_1 = 2$ y $n_2 = 2v + 1$.

Como vemos, los casos (2) y (3) son incompatibles entre sí por lo que siempre todo semigrupo numérico $S = \langle n_1, n_2\rangle$ tendrá cinco o seis representaciones modulares. □

Usando las identidades del Ejemplo 7.14 se puede obtener fácilmente el siguiente resultado.

COROLARIO 7.16. *Sea $b \geq 2$ un entero y sea $S = \mathrm{S}(\lfloor \frac{1}{2}(b+1) \rfloor, b)$. Entonces*

$$S = \begin{cases} \langle 2, b\rangle & \text{si } b \text{ es impar, en cuyo caso } \mathrm{g}(S) = b - 2, \\ \langle 2, \frac{b}{2} + 1\rangle & \text{si } b \equiv 0 \bmod 4, \text{ en cuyo caso } \mathrm{g}(S) = \frac{b}{2} - 1, \\ \langle 2, \frac{b}{2}\rangle & \text{si } b \equiv 2 \bmod 4, \text{ en cuyo caso } \mathrm{g}(S) = \frac{b}{2} - 2. \end{cases}$$

COROLARIO 7.17. *Sea b un entero mayor o igual que 3. Entonces b es primo si y sólo si $a = \lfloor \frac{b+1}{2} \rfloor$ es el único valor perteneciente a $\{2, \ldots, \frac{b+1}{2}\}$ para el cual* $\mathrm{e}(\mathrm{S}(a,b)) = 2$.

DEMOSTRACIÓN. Supongamos que $b \geq 3$ es primo y que existe $a \in \{2, \ldots, \frac{b+1}{2}\}$ tal que $\mathrm{S}(a,b) = \langle n_1, n_2 \rangle$ y $\mathrm{e}(\mathrm{S}(a,b)) = 2$. Por el Teorema 7.11 sólo caben dos posibilidades: $b = n_1(n_2 - 1)$ en cuyo caso $n_1 = b$ y $n_2 = 2$, o bien $b = (n_1 - 1)n_2$ en cuyo caso $n_1 = 2$ y $n_2 = b$. En ambos casos resulta $\mathrm{S}(a,b) = \langle 2, b \rangle$. Teniendo en cuenta el Ejemplo 7.13, deducimos que $a = b - \lfloor \frac{b}{2} \rfloor = \lfloor \frac{b}{2} \rfloor + 1$, coincidiendo estos valores con $\lfloor \frac{b+1}{2} \rfloor$.

Supongamos que b no es primo y probemos que existen otros valores para a, aparte de $\lfloor \frac{b+1}{2} \rfloor$, para los cuales $\mathrm{e}(\mathrm{S}(a,b)) = 2$.

- Si $b = n_1 n_2$ con n_1 y n_2 enteros positivos mayores que 1 y primos relativos, en vista del Teorema 7.11, definimos el semigrupo numérico $S = \langle n_1, n_2 \rangle$ el cual admite la representación modular $S = \mathrm{S}((n_2^{-1} \bmod n_1)n_2, b)$. Es inmediato probar que ni el valor $a = (n_2^{-1} \bmod n_1)n_2$ ni su simétrico $b + 1 - a$ pueden ser iguales a $\lfloor \frac{b+1}{2} \rfloor = \frac{n_1 n_2 + 1}{2}$.
- Si $b = p^k$, con p un primo mayor o igual que 3 y $k \geq 2$, tomando $n_1 = p^{k-1}$ y $n_2 = p + 1$ obtenemos un semigrupo numérico $S = \langle n_1, n_2 \rangle$ el cual admite la representación modular $S = \mathrm{S}((n_2^{-1} \bmod n_1)(n_2 - 1), b)$. De nuevo se puede comprobar que ni el valor $a = (n_2^{-1} \bmod n_1)(n_2 - 1)$ ni su simétrico $b + 1 - a$ son iguales a $\lfloor \frac{b+1}{2} \rfloor = \frac{n_1 n_2 + 1}{2}$.

□

Tal y como veremos en las próximas secciones, los semigrupos modulares con $\mathrm{e}(S) = 2$ pueden ser caracterizados como aquellos semigrupos modulares que admiten el máximo número de representaciones modulares.

3. Las secuencias de Bézout propias para un semigrupo proporcionalmente modular

El objetivo principal de esta sección es probar el Teorema 7.23 según el cual todo semigrupo proporcionalmente modular admite a lo sumo cuatro secuencias de Bézout propias para sus generadores minimales como numeradores y con todas sus fracciones mayores que 1. Comenzamos viendo un lema el cual se puede probar fácilmente a partir de las definiciones.

LEMA 7.18. *Si $\frac{a_1}{b_1} < \cdots < \frac{a_p}{b_p}$ es una secuencia de Bézout propia con todas las fracciones mayores que* 1*, entonces se puede afirmar lo mismo de $\frac{a_p}{a_p - b_p} < \cdots < \frac{a_1}{a_1 - b_1}$.*

Diremos que las **secuencias de Bézout** $\frac{a_1}{b_1} < \cdots < \frac{a_p}{b_p}$ y $\frac{a_p}{a_p - b_p} < \cdots < \frac{a_1}{a_1 - b_1}$ son **simétricas**.

Tal y como vimos en el Capítulo 4, las secuencias de Bézout son una herramienta muy útil para estudiar los semigrupos proporcionalmente modulares. Ahora las utilizaremos para estudiar representaciones modulares $S = \mathrm{S}(a,b)$ para semigrupos numéricos modulares. Si $n_1,\dots,n_p$ son los generadores minimales de S y $\frac{n_1}{b_1} < \frac{n_2}{b_2} < \cdots < \frac{n_p}{b_p}$ es una secuencia de Bézout, siempre nos encontraremos en el caso $\frac{b}{a} \leq \frac{n_1}{b_1} < \frac{n_2}{b_2} < \cdots < \frac{n_p}{b_p} \leq \frac{b}{a-1}$. Al estar suponiendo siempre que $a < b$, ésto implica que todas las fracciones que aparecen en la secuencia han de ser mayores que 1. Por tanto, a partir de ahora y salvo que se afirme lo contrario, al considerar una secuencia de Bézout supondremos siempre que todas sus fracciones son mayores que 1.

El siguiente resultado es una consecuencia inmediata del Corolario 4.17 y extiende al Corolario 4.25.

LEMA 7.19. *Sea $n_1 < n_2 < \cdots < n_p$ el sistema minimal de generadores de un semigrupo numérico S proporcionalmente modular. Entonces* $\mathrm{mcd}\{n_1,n_2\} = 1$. *Además, si $u \in \{1,\dots,n_1-1\}$, $v \in \{1,\dots,n_2-1\}$ y verifican $un_2 - vn_1 = 1$, entonces cualquier secuencia de Bézout propia con numeradores $n_1,\dots,n_p$ debe contener como fracciones consecutivas bien a $\frac{n_1}{u} < \frac{n_2}{v}$ o a $\frac{n_2}{n_2-v} < \frac{n_1}{n_1-u}$.*

LEMA 7.20. *Sea $\{n_1,\dots,n_p\}$ un conjunto independiente de números enteros positivos y sea $\frac{n_1}{b_1} < \cdots < \frac{n_p}{b_p}$ una secuencia de Bézout. Si existe un entero positivo b'_p tal que $\frac{n_p}{b'_p} < \frac{n_1}{b_1}$ es una secuencia de Bézout, entonces $b'_p = b_p + 1$.*

DEMOSTRACIÓN. Veamos primero el caso $p = 2$. Si $\frac{n_1}{b_1} < \frac{n_2}{b_2}$ y $\frac{n_2}{b_2+\lambda} < \frac{n_1}{b_1}$ son secuencias de Bézout, entonces $b_1n_2 - b_2n_1 = 1$ y $b_2n_1 + \lambda n_1 - b_1n_2 = 1$. Ésto implica que $\lambda n_1 = 2$, y por tanto $n_1 = 2$ y $\lambda = 1$.

Supongamos ahora que $p \geq 3$, y además que $\frac{n_1}{b_1} < \cdots < \frac{n_{p-1}}{b_{p-1}} < \frac{n_p}{b_p}$ y $\frac{n_p}{b_p+\lambda} < \frac{n_1}{b_1} < \cdots < \frac{n_{p-1}}{b_{p-1}}$ son secuencias de Bézout. Si $\lambda > 1$, entonces $\frac{n_1}{b_1} < \frac{n_p}{b_p+1} < \frac{n_{p-1}}{b_{p-1}}$, y por tanto existe $i \in \{1,\dots,p-2\}$ tal que $\frac{n_i}{b_i} < \frac{n_p}{b_p+1} < \frac{n_{i+1}}{b_{i+1}}$. Por los Lemas 4.7 y 2.16 ésto significa que $n_p \in \langle n_i, n_{i+1}\rangle$, lo que contradice la independencia del conjunto $\{n_1,\dots,n_p\}$. □

Antes de enunciar y demostrar el Teorema 7.23, damos dos ejemplos para ilustrar los dos casos que aparecen en dicho teorema.

EJEMPLO 7.21. Construyamos todas las secuencias de Bézout propias con numeradores $7,9,11,13$.

Por el Lema 7.19 sabemos que cualquiera de dichas secuencias ha de contener bien a la subsecuencia $\frac{7}{4} < \frac{9}{5}$ o a la subsecuencia $\frac{9}{4} < \frac{7}{3}$. Supongamos que contiene a $\frac{7}{4} < \frac{9}{5}$; por el Corolario 4.17 esta última puede extenderse a una secuencia de Bézout a lo sumo de dos formas posibles que son $\frac{7}{4} < \frac{9}{5} < \frac{11}{x}$ y $\frac{11}{y} < \frac{7}{4} < \frac{9}{5}$ para ciertos enteros positivos x,y. Se puede comprobar fácilmente que la ampliación sólo es posible de la primera forma con $x = 6$. Por tanto resulta la secuencia de Bézout $\frac{7}{4} < \frac{9}{5} < \frac{11}{6}$. Repitiendo el mismo proceso con esta nueva secuencia vemos que $\frac{13}{y} < \frac{7}{4}$ no es secuencia de Bézout

para cualquier entero positivo y. Sin embargo $\frac{11}{6} < \frac{13}{x}$ sí es secuencia de Bézout para $x = 7$, por lo cual $\frac{7}{4} < \frac{9}{5} < \frac{11}{6} < \frac{13}{7}$ es una secuencia de Bézout completa para los numeradores dados y conteniendo a la subsecuencia inicial $\frac{7}{4} < \frac{9}{5}$.

Ahora, comenzando con la subsecuencia $\frac{9}{4} < \frac{7}{3}$ y procediendo de forma análoga, de nuevo resulta una única secuencia de Bézout que es la simétrica de la obtenida en el caso anterior. □

EJEMPLO 7.22. Obtengamos todas las secuencias de Bézout propias con numeradores $5, 6, 9, 13$.

Al igual que en el ejemplo anterior, aplicando el Lema 7.19 obtenemos dos posibilidades iniciales que son $\frac{5}{1} < \frac{6}{1}$ y $\frac{6}{5} < \frac{5}{4}$.

Comenzando con $\frac{5}{1} < \frac{6}{1}$ y procediendo como en el ejemplo anterior obtenemos $\frac{9}{2} < \frac{5}{1} < \frac{6}{1}$; pero ahora esta secuencia puede ser ampliada de dos formas a una secuencia de Bézout. Éstas son $\frac{9}{2} < \frac{5}{1} < \frac{6}{1} < \frac{13}{2}$ y $\frac{13}{3} < \frac{9}{2} < \frac{5}{1} < \frac{6}{1}$.

Si se comienza con $\frac{6}{5} < \frac{5}{4}$, de nuevo resultan dos secuencias de Bézout que son $\frac{13}{11} < \frac{6}{5} < \frac{5}{4} < \frac{9}{7}$ y $\frac{6}{5} < \frac{5}{4} < \frac{9}{7} < \frac{13}{10}$, siendo éstas las simétricas de las obtenidas previamente. □

Observemos que en el Ejemplo 7.21, si llamamos $S = \langle 7, 9, 11, 13\rangle$, se verifica que $g(S) = 19$, siendo dicha cantidad mayor que cualquiera de los generadores minimales del semigrupo numérico S. Sin embargo en el Ejemplo 7.22, si $S = \langle 5, 6, 9, 13\rangle$, entonces $g(S) = 8$, cantidad que es menor que algunos de los generadores minimales de S. En el siguiente teorema se recoge esta distinción de casos.

TEOREMA 7.23. *Sea S un semigrupo proporcionalmente modular minimalmente generado por el conjunto $\{n_1, \ldots, n_p\}$, y sea $\frac{n_1}{b_1} < \cdots < \frac{n_p}{b_p}$ una secuencia de Bézout propia.*

1. *Si $g(S) > \max\{n_1, \ldots, n_p\}$, entonces $\frac{n_1}{b_1} < \cdots < \frac{n_p}{b_p}$ y $\frac{n_p}{n_p - b_p} < \cdots < \frac{n_1}{n_1 - b_1}$ son las únicas secuencias de Bézout propias para los numeradores $n_1, \ldots, n_p$.*
2. *Si $g(S) < n_p = \max\{n_1, \ldots, n_p\}$ y $\frac{n_p}{b_p + 1} < \frac{n_1}{b_1}$ es una secuencia de Bézout, entonces hay exactamente cuatro secuencias de Bézout propias para los numeradores $n_1, \ldots, n_p$, siendo éstas:*

$$\frac{n_1}{b_1} < \cdots < \frac{n_p}{b_p},$$

$$\frac{n_p}{n_p - b_p} < \cdots < \frac{n_1}{n_1 - b_1},$$

$$\frac{n_p}{b_p + 1} < \frac{n_1}{b_1} < \cdots < \frac{n_{p-1}}{b_{p-1}}$$

y

$$\frac{n_{p-1}}{n_{p-1} - b_{p-1}} < \cdots < \frac{n_1}{n_1 - b_1} < \frac{n_p}{n_p - b_p - 1}.$$

3. *Si* $\mathrm{g}(S) < n_p = \max\{n_1,\dots,n_p\}$ *y* $\frac{n_p}{b_p+1} < \frac{n_1}{b_1}$ *no es una secuencia de Bézout, entonces*

$$\frac{n_1}{b_1} < \cdots < \frac{n_p}{b_p}$$

y

$$\frac{n_p}{n_p - b_p} < \cdots < \frac{n_1}{n_1 - b_1}$$

son las únicas secuencias de Bézout propias para los numeradores $n_1,\dots,n_p$.

DEMOSTRACIÓN. Supongamos que los generadores minimales de S están ordenados de la siguiente forma: $n_1 < n_2 < \cdots < n_p$. Entonces, de acuerdo con el Lema 7.19, toda secuencia de Bézout para dichos numeradores debe de ser una extensión de la secuencia $\frac{n_1}{b_1} < \frac{n_2}{b_2}$ o bien de $\frac{n_2}{n_2-b_2} < \frac{n_1}{n_1-b_1}$, siendo b_1 y b_2 los únicos enteros positivos que verifican la condiciones $b_1 < n_1, b_2 < n_2$ y $b_1n_2 - b_2n_1 = 1$. Consideremos la primera de las dos subsecuencias.

Si existen dos enteros positivos x e y tales que $\frac{n_3}{y} < \frac{n_1}{b_1} < \frac{n_2}{b_2} < \frac{n_3}{x}$ es una secuencia de Bézout, entonces aplicando el Teorema 4.8 y el Lema 2.15 resulta $\langle n_1,n_2,n_3\rangle = \mathrm{S}([\frac{n_3}{y},\frac{n_3}{x}]) = \{n \in \mathbb{N} \mid yn \bmod n_3 \leq (y-x)n\}$ (de hecho por el Lema 7.20 tenemos $y-x=1$). Ésto en particular implica que $\{n_3, n_3+1, \to\} \subseteq \langle n_1,n_2,n_3\rangle$, de lo cual deducimos que n_3 es el mayor generador minimal de S y $\mathrm{g}(S) < n_3$.

En caso contrario tenemos que la extensión de la secuencia inicial sólo es posible por uno de sus extremos. A continuación repetimos el mismo proceso para la secuencia recién obtenida y el siguiente generador minimal, y así hasta agotar todos los generadores minimales. Vemos que las dos posibilidades de ampliación sólo pueden darse para el último generador minimal y además en el caso en que éste sea mayor que $\mathrm{g}(S)$. Por el Lema 7.20 si existe un $i \in \{3,\dots,p\}$ tal que $\frac{n_i}{b_i+1} < \frac{n_1}{b_1} < \cdots < \frac{n_i}{b_i}$ es una secuencia de Bézout, entonces $\langle n_1,\dots,n_i\rangle = \mathrm{S}([\frac{n_i}{b_i+1},\frac{n_i}{b_i}]) = \mathrm{S}(b_i+1,n_i)$. De aquí deducimos que $\{n_i,\to\} \subseteq \langle n_1,\dots,n_i\rangle$ y $\mathrm{g}(S) < n_i$, y por tanto que n_i es el mayor generador minimal de S. Ésto fuerza $i = p$. □

COMENTARIO 7.24. En vista del teorema anterior deducimos que para un semigrupo numérico S proporcionalmente modular el cual está minimalmente generado por $\{n_1,\dots,n_p\}$, si $p = \mathrm{e}(S) \geq 3$ y $\frac{n_1}{b_1} < \frac{n_2}{b_2} < \cdots < \frac{n_p}{b_p}$ es una secuencia de Bézout, entonces para todo $i \in \{2,\dots,p-1\}$ se verifica que el denominador de n_i en cualquier secuencia de Bézout con numeradores $n_1,\dots,n_p$ ha de ser b_i ó $n_i - b_i$. □

En el siguiente ejemplo se pone de manifiesto que aún cuando alguno de los generadores minimales de S es mayor que $\mathrm{g}(S)$, esta condición no es suficiente para garantizar la existencia de cuatro secuencias de Bézout para dichos generadores minimales.

EJEMPLO 7.25. Obtengamos todas la secuencias de Bézout propias con numeradores $4, 5$ y 7.

Observamos en primer lugar que $\mathrm{g}(\langle 4,5,7\rangle) = 6$. Por el Lema 7.19, cualquier secuencia válida debe contener a una de las dos secuencias iniciales: $\frac{4}{1} < \frac{5}{1}$ ó $\frac{5}{4} < \frac{4}{3}$. Se

puede comprobar que la única extensión de $\frac{4}{1} < \frac{5}{1}$ es $\frac{7}{2} < \frac{4}{1} < \frac{5}{1}$. Similarmente, la única extensión de $\frac{5}{4} < \frac{4}{3}$ es $\frac{5}{4} < \frac{4}{3} < \frac{7}{5}$ (siendo ésta la simétrica de la anterior). Por tanto, aún cuando $\mathrm{g}(S) < \max\{4,5,7\}$, sólo hay dos secuencias de Bézout. □

COROLARIO 7.26. *Sea S un semigrupo modular con $\mathrm{e}(S) \geq 3$ y tal que todos sus generadores minimales son menores que $\mathrm{g}(S)$. Entonces*

$$\#\{b \mid S = \mathrm{S}(a,b) \text{ para algún } a < b\} \leq 2.$$

DEMOSTRACIÓN. Supongamos que S está generado minimalmente por $n_1, \ldots, n_p$. Por el Teorema 7.23 sabemos que hay exactamente dos secuencias de Bézout propias con numeradores $n_1, \ldots, n_p$. Sean éstas $\frac{n_1}{b_1} < \cdots < \frac{n_p}{b_p}$ y $\frac{n_p}{n_p - b_p} < \cdots < \frac{n_1}{n_1 - b_1}$. Teniendo en cuenta el Teorema 7.4 y el Comentario 7.5, para cualquier representación modular $\mathrm{S}(a,b)$ con $a < b$, vemos que ha de verificarse alguna de las siguientes igualdades:

$$(1)\ \frac{b}{a} = \frac{n_1}{b_1}, \qquad (2)\ \frac{b}{a} = \frac{n_p}{n_p - b_p}, \qquad (3)\ \frac{b}{a-1} = \frac{n_p}{b_p}, \qquad (4)\ \frac{b}{a-1} = \frac{n_1}{n_1 - b_1}.$$

Observamos además que para cada uno de los casos anteriores, por el Teorema 7.9 los valores de a y b están determinados de manera única. Finalmente, teniendo en cuenta que $\frac{b}{a} = \frac{n_1}{b_1}$ si y sólo si $\frac{b}{(b+1-a)-1} = \frac{n_1}{n_1 - b_1}$, vemos que los casos (1) y (4) dan lugar a representaciones modulares simétricas, y lo mismo ocurre para los casos (2) y (3). □

EJEMPLO 7.27. Obtengamos todas las representaciones modulares para el semigrupo numérico $S = \langle 5,7,9 \rangle$.

En primer lugar calculamos $\mathrm{g}(S) = 13$ de lo cual observamos que todos los generadores minimales son menores que $\mathrm{g}(S)$. A continuación, procediendo como en los ejemplos anteriores, obtenemos dos secuencias de Bézout propias con numeradores 5, 7 y 9: $\frac{9}{4} < \frac{7}{3} < \frac{5}{2}$ y $\frac{5}{3} < \frac{7}{4} < \frac{9}{5}$. Teniendo en cuenta el Corolario 7.26 (y su demostración), resulta que S admite, salvo simetría, a lo sumo dos representaciones modulares $\mathrm{S}(4k,9k)$ y $\mathrm{S}(3k',5k')$ para ciertos enteros positivos k y k'. Para $k = 2$ y $k' = 4$ se puede comprobar fácilmente que $\mathrm{S}(8,18) = \langle 5,7,9 \rangle = \mathrm{S}(12,20)$. Por consiguiente todas las representaciones modulares para S son $\mathrm{S}(8,18), \mathrm{S}(11,18), \mathrm{S}(12,20)$ y $\mathrm{S}(9,20)$. □

En el siguiente ejemplo mostramos un semigrupo modular el cual, salvo simetría, tiene sólo una representación modular.

EJEMPLO 7.28. Para el semigrupo $S = \langle 4,7,10 \rangle$ se verifica que $\mathrm{g}(S) = 13$ y por tanto de nuevo todo generador minimal es menor que el número de Frobenius. Las únicas secuencias de Bézout con 4, 7 y 10 como numeradores son $\frac{10}{3} < \frac{7}{2} < \frac{4}{1}$ y $\frac{4}{3} < \frac{7}{5} < \frac{10}{7}$. Por tanto, las únicas representaciones modulares para S, salvo simetría, han de ser del tipo $\mathrm{S}(3k,10k)$ y $\mathrm{S}(3k',4k')$. Para $k = 2$ obtenemos $S = \mathrm{S}(6,20)$ y para $k' = 5$ resulta $S = \mathrm{S}(15,20)$. Nótese que ambas representaciones modulares son simétricas. □

COMENTARIO 7.29. Se puede enunciar un resultado similar al Corolario 7.26, pero ahora bajo la hipótesis de que el máximo generador minimal de S sea mayor que $\mathrm{g}(S)$.

En este caso obtendríamos como conclusión que

$$\#\{b \mid S = \mathrm{S}(a,b) \text{ para algún } a < b\} \leq 4.$$

La demostración se haría de manera similar a la del Corolario 7.26 aunque ahora teniendo en cuenta que pueden existir a lo sumo cuatro secuencias de Bézout propias. No hemos incluido dicho resultado porque tal y como veremos en la próxima sección, éste es mejorable. □

PROPOSICIÓN 7.30. *Si S es un semigrupo modular tal que $S = \mathrm{S}(a,b) = \mathrm{S}(a',b)$ con $a < b$ y $a' < b$, entonces $a = a'$ ó $a + a' = b + 1$.*

DEMOSTRACIÓN. Si $\mathrm{e}(S) = 2$, entonces el resultado es consecuencia del Teorema 7.11, pues en tal caso existen tres módulos b diferentes que son $n_1(n_1-1), n_2(n_1-1)$ y n_1n_2, y para cada uno de ellos existen dos factores a simétricos entre sí.

Supongamos que S está minimalmente generado por $n_1, \ldots, n_p$ y $\mathrm{e}(S) \geq 3$. Si $S = \mathrm{S}(a,b)$, entonces sabemos que existe una secuencia de Bézout propia $\frac{n_1}{b_1} < \frac{n_2}{b_2} < \cdots < \frac{n_p}{b_p}$ verificando que $\frac{b}{a} \leq \frac{n_1}{b_1} < \frac{n_2}{b_2} < \cdots < \frac{n_p}{b_p} \leq \frac{b}{a-1}$. La hipótesis $p = \mathrm{e}(S) \geq 3$ implica que $\frac{b}{a} < \frac{n_2}{b_2} \leq \frac{b}{a-1}$, es decir, $\frac{bb_2}{n_2} < a \leq \frac{bb_2}{n_2} + 1$. De acuerdo con el Comentario 7.24, deducimos que el valor para a está determinado de manera única, salvo simetría, ya que el denominador b_2 puede tomar uno de entre dos valores posibles ("simétricos"). □

4. Los posibles módulos para un semigrupo modular

El propósito de esta sección es demostrar el Teorema 7.36 según el cual todo semigrupo modular S, con $\mathrm{e}(S) \geq 3$, admite salvo simetría a lo sumo dos representaciones modulares.

Recordemos que una semirecta es un semigrupo numérico de la forma $\{0, m, \rightarrow\}$. En el Ejemplo 1.9 vimos que para cualquier entero positivo b, se verifica que $\mathrm{S}(2,b) = \{0, \lfloor \frac{b+1}{2} \rfloor, \rightarrow\}$. Ésto nos dice que toda semirecta es un semigrupo modular. La siguiente proposición describe todas las representaciones modulares para una semirecta.

PROPOSICIÓN 7.31. *Sea $m \geq 3$ un entero positivo y sea la semirecta $S = \{0, m, \rightarrow\}$. Los siguientes enunciados son equivalentes:*

1. *$S = \mathrm{S}(a,b)$ para ciertos enteros positivos $a < b$,*
2. *$(a,b) \in \{(2,2m), (2m-1,2m), (2,2m-1), (2m-2,2m-1)\}$.*

DEMOSTRACIÓN.

(2) $\Rightarrow$ (1) Por el Ejemplo 1.9 tenemos $S = \mathrm{S}(2,2m) = \mathrm{S}(2,2m-1)$. Aplicando ahora el Lema 1.3 a dichas representaciones, resulta $S = \mathrm{S}(2m-1,2m) = \mathrm{S}(2m-2,2m-1)$.

(1) $\Rightarrow$ (2) Observamos en primer lugar que $\mathrm{g}(S) = m-1$ y que S está minimalmente generado por el conjunto $m, m+1, \ldots, 2m-1$. Aplicando el Teorema 7.23 deducimos que, salvo simetría, las únicas secuencias de Bézout propias para los numeradores

$m, m+1, \ldots, 2m-1$ son:

$$\frac{m}{1} < \frac{m+1}{1} < \cdots < \frac{2m-1}{1} \qquad \text{y} \qquad \frac{2m-1}{2} < \frac{m}{1} < \frac{m+1}{1} < \cdots < \frac{2m-2}{1}.$$

Si $\mathrm{S}(a,b)$ es una representación modular para S, entonces por el Teorema 7.4 ha de verificarse alguna de las siguientes igualdades:

$$(1)\ \frac{b}{a} = \frac{m}{1}, \qquad (2)\ \frac{b}{a} = \frac{2m-1}{2}, \qquad (3)\ \frac{b}{a-1} = \frac{2m-1}{1}, \qquad (4)\ \frac{b}{a-1} = \frac{2m-2}{1}.$$

Observamos que si considerásemos las dos secuencias de Bézout restantes, es decir, las simétricas de las anteriores, resultarían otros cuatro casos los cuales no es necesario analizar, pues dan lugar a representaciones modulares simétricas de las que vamos a obtener nosotros.

1. Si $\frac{b}{a} = \frac{m}{1}$, entonces $(a,b) = (2, 2m)$.
2. Si $\frac{b}{a} = \frac{2m-1}{2}$, entonces $(a,b) = (2, 2m-1)$.
3. Si $\frac{b}{a-1} = \frac{2m-1}{1}$, entonces $(a,b) = (2, 2m-1)$.

   Las conclusiones para estos tres primeros casos se han obtenido aplicando el Teorema 7.9 y teniendo en cuenta la implicación $(2) \Rightarrow (1)$ ya demostrada.
4. Para finalizar la demostración, probamos que el caso $\frac{b}{a-1} = \frac{2m-2}{1}$ nunca se da. En primer lugar, si suponemos que $a = 2$, resulta $b = 2m-2$ y por tanto $S = \mathrm{S}(2, 2m-2)$, lo cual es imposible pues $m-1 \in \mathrm{S}(2, 2m-2)$ y $m-1 \notin S$. Supongamos por tanto que $a \geq 3$. La hipótesis $\frac{b}{a-1} = \frac{2m-2}{1}$ implica que $b = (a-1)(2m-2)$. Como $m \in \mathrm{S}(a,b)$, se verifica que $am \bmod b \leq m$ y en particular $am \geq b = (a-1)(2m-2)$. De aquí obtenemos que $3 \leq a \leq \frac{2m-2}{m-2}$, de donde $m \leq 4$.
   a) Si $m = 3$, entonces $\frac{b}{a-1} = 4$, es decir, $b = 4a-4$. Además, como $3 = m \in \mathrm{S}(a,b)$, deducimos que $3a \geq 4a-4$, es decir, $a \leq 4$. Para $a = 3$ resulta $b = 8$ y por consiguiente el semigrupo $\mathrm{S}(3,8)$, el cual es distinto de S pues $5 \notin \mathrm{S}(3,8)$. Análogamente, para $a = 4$ obtenemos $b = 12$ y el semigrupo $\mathrm{S}(4,12)$, que también es distinto de S ya que $5 \notin \mathrm{S}(4,12)$.
   b) Si $m = 4$, entonces $\frac{b}{a-1} = 6$, es decir, $b = 6a-6$. En este caso $4 = m \in \mathrm{S}(a,b)$, lo que implica que $4a \geq 6a-6$, y por tanto $a = 3$. Sustituyendo dicho valor en la igualdad anterior, obtenemos que $b = 12$ y por tanto el semigrupo modular $\mathrm{S}(3,12)$, que también difiere de S pues $7 \in S$ pero $7 \notin \mathrm{S}(3,12)$.

□

Antes de probar el Teorema 7.36, necesitamos algunos lemas técnicos.

LEMA 7.32. *Sea S un semigrupo modular tal que $\mathrm{e}(S) \geq 3$ y $S \neq \{0, \mathrm{m}(S), \rightarrow\}$, es decir, S no es una semirecta. Entonces existe a lo sumo un par ordenado (a,b) de enteros positivos, con $a < b$, verificando que $S = \mathrm{S}(a,b)$ y $\mathrm{m}(S) = \frac{b}{\mathrm{mcd}\{a,b\}}$.*

DEMOSTRACIÓN. Sea $\{n_1,\dots,n_p\}$ el sistema minimal de generadores de S. De acuerdo con el Teorema 7.4 existe una secuencia de Bézout propia $\frac{n_1}{b_1}<\cdots<\frac{n_p}{b_p}$ tal que $\frac{b}{a}\leq\frac{n_1}{b_1}<\ldots<\frac{n_p}{b_p}\leq\frac{b}{a-1}$. Sea $\mathrm{m}(S)=n_i$ para algún $i\geq 1$, y demostremos que $i=1$. Supongamos por reducción al absurdo que $i\geq 2$. Llamamos $d=\mathrm{mcd}\{a,b\}$. Por hipótesis tenemos $n_i=\frac{b}{d}$, con lo cual $\frac{b}{a}=\frac{b/d}{a/d}\leq\frac{n_1}{b_1}<\ldots<\frac{n_i}{b_i}=\frac{b/d}{b_i}$. Deducimos de aquí $\mathrm{S}([\frac{b/d}{a/d},\frac{b/d}{b_i}])\subseteq\mathrm{S}([\frac{b}{a},\frac{b}{a-1}])=S$ y por tanto que todo entero mayor o igual que $\frac{b}{d}=\mathrm{m}(S)$ pertenece a S. Pero esto último contradice la hipótesis $S\neq\{0,\mathrm{m}(S),\rightarrow\}$. Por consiguiente $\frac{b}{a}=\frac{n_1}{b_1}$, con $n_1=\mathrm{m}(S)$. Así pues, por el Corolario 4.17 y en concordancia con el Teorema 7.23, hemos probado que, salvo simetría, $\frac{n_1}{b_1}<\cdots<\frac{n_p}{b_p}$ es la única secuencia de Bézout con numeradores $n_1,\dots,n_p$. Finalmente, el Teorema 7.9 nos garantiza que el par ordenado (a,b) es único. □

COMENTARIO 7.33. La única representación modular, salvo simetría, a la que se refiere el Lema 7.32 se puede calcular fácilmente a partir de las hipótesis. Siguiendo la notación en dicho lema, la igualdad $\frac{b}{a}=\frac{n_1}{b_1}$ implica que existe un único entero positivo k tal que $b=kn_1$ y $a=kb_1$, con lo cual

$$\frac{kn_1}{kb_1}=\frac{n_1}{b_1}<\cdots<\frac{n_p}{b_p}\leq\frac{kn_1}{kb_1-1}.$$

Observamos que la última de las desigualdades es equivalente a $k\leq\frac{n_p}{b_1n_p-b_pn_1}$. Puesto que siempre se verifica que $\frac{t_1x}{t_1y_1-1}\leq\frac{t_2x}{t_2y_1-1}$ si y sólo si $t_2\leq t_1$, la unicidad de k implica $k=\lfloor\frac{n_p}{b_1n_p-b_pn_1}\rfloor$. □

El siguiente lema es una consecuencia inmediata de los Lemas 7.32 y 1.3.

LEMA 7.34. *Sea S un semigrupo modular tal que $\mathrm{e}(S)\geq 3$ y $S\neq\{0,\mathrm{m}(S),\rightarrow\}$, es decir, no es una semirecta. Entonces existe a lo sumo un par ordenado (a,b) de enteros positivos, con $a<b$, verificando que $S=\mathrm{S}(a,b)$ y $\mathrm{m}(S)=\frac{b}{\mathrm{mcd}\{a-1,b\}}$.*

DEMOSTRACIÓN. Por hipótesis tenemos $\mathrm{m}(S)=\frac{b}{\mathrm{mcd}\{a-1,b\}}$, valor que coincide con $\frac{b}{\mathrm{mcd}\{b+1-a,b\}}$. Ya que según el Lema 1.3 se verifica que $\mathrm{S}(a,b)=\mathrm{S}(b+1-a,b)$, aplicando el Lema 7.32, deducimos que el par ordenado $(b+1-a,b)$ está determinado de manera única y por tanto lo mismo ocurre con el par ordenado (a,b). □

Recordemos que las secuencias de Bézout que estamos considerando tienen todas sus fracciones mayores que 1. Como consecuencia del Lema 4.31 recogemos el siguiente resultado.

LEMA 7.35. *Sea $\frac{n_1}{b_1}<\frac{n_2}{b_2}<\ldots<\frac{n_p}{b_p}$ una secuencia de Bézout. Entonces $b_1=n_2^{-1}\bmod n_1$, $b_2=n_3^{-1}\bmod n_2,\dots,b_{p-1}=n_p^{-1}\bmod n_{p-1}$ y $b_p=(-n_{p-1})^{-1}\bmod n_p$.*

Ya estamos en condiciones de probar el resultado principal de esta sección.

TEOREMA 7.36. *Sea S un semigrupo modular minimalmente generado por $n_1 < n_2 < \cdots < n_p$, con $p \geq 3$. Si $\mathrm{S}(a,b)$ es una representación modular para S, entonces se verifica que $b = \mathrm{m}(S) + \mathrm{g}(S)$ ó*

$$b = \left\lfloor \frac{n_p}{(n_2^{-1} \bmod n_1)n_p - ((-n_{p-1})^{-1} \bmod n_p)n_1} \right\rfloor n_1.$$

DEMOSTRACIÓN. Si $S = \{0, m, \rightarrow\}$, entonces $n_1 = \mathrm{m}(S) = m$, $n_2 = m+1$, $n_{p-1} = 2m-2$, $n_p = 2m-1$ y $\mathrm{g}(S) = m-1$. En este caso es inmediato comprobar que las dos fórmulas dadas para b se reducen a $b = 2m-1$ y $b = 2m$, respectivamente, siendo el resultado consecuencia de la Proposición 7.31. Supongamos ahora $S \neq \{0, m, \rightarrow\}$. Si $b \neq \mathrm{m}(S) + \mathrm{g}(S)$, entonces por el Lema 1.24 obtemos sólo dos valores posibles para $\mathrm{m}(S)$. Estos nuevos casos se resuelven utilizando los Lemas 7.32 y 7.34, así como el Comentario 7.33 y el Lema 7.35. □

En vista del Teorema 7.36 así como del Teorema 7.11, podemos enunciar la siguiente propiedad.

COROLARIO 7.37. *Para un semigrupo modular S, se verifica que:*

- *si $\mathrm{e}(S) = 1$, entonces S tiene infinitas representaciones modulares;*
- *si $\mathrm{e}(S) = 2$, entonces S tiene exactamente seis representaciones modulares, excepto para el caso $S = \langle 2, b\rangle$ con b impar, el cual tiene cinco representaciones modulares;*
- *si $\mathrm{e}(S) \geq 3$, entonces S tiene a lo sumo cuatro representaciones modulares.*

Si tenemos una representación modular $S = \mathrm{S}(a,b)$, siendo $b = \mathrm{m}(S) + \mathrm{g}(S)$, diremos que el **módulo** b es **de tipo 1**. Por contra, si b toma el otro valor posible (el cual es siempre mayor que $\mathrm{m}(S) + \mathrm{g}(S)$, por el Lema 1.23), diremos que el **módulo** b es **de tipo 2**.

Recordemos que el Algoritmo 1.25 nos permitía decidir si un semigrupo numérico dado era o no modular. Basándonos en el Teorema 7.36, podríamos dar una versión ampliada para dicho algoritmo la cual devolviese todas las representaciones modulares posibles para S, teniendo en cuenta que para $\mathrm{e}(S) \geq 3$, al obtener dos representaciones modulares para S con módulos diferentes se acabaría la ejecución del mismo. Como veremos en la sección siguiente, este método es mejorable.

Concluimos esta sección dando algunos ejemplos los cuales ponen de manifiesto que los dos casos que se presentan en el Teorema 7.36 son independentes.

EJEMPLO 7.38. Sea $S = \langle 5, 7, 9\rangle$. Del Ejemplo 7.27 ya sabemos que $\mathrm{m}(S) = 5$, $\mathrm{g}(S) = 13$ y que S es modular, siendo $\mathrm{S}(8,18), \mathrm{S}(11,18), \mathrm{S}(12,20)$ y $\mathrm{S}(9,20)$ todas las representaciones modulares para S. Observemos que $18 = \mathrm{m}(S) + \mathrm{g}(S)$ y que $\frac{5}{3} < \frac{7}{4} < \frac{9}{5}$ es una secuencia de Bézout a partir de la cual se obtiene $20 = \lfloor \frac{9}{2} \rfloor 5$. Vemos pues que en este ejemplo se obtienen los dos tipos de módulos. □

EJEMPLO 7.39. Sea $S = \langle 4, 7, 10\rangle$. De acuerdo con el Ejemplo 7.28, tenemos ahora $\mathrm{m}(S) = 4$, $\mathrm{g}(S) = 13$ y $\mathrm{S}(6,20)$, $\mathrm{S}(15,20)$ como las únicas representaciones modulares

para S. Vemos que en este caso el módulo $17 = \mathrm{m}(S)+\mathrm{g}(S)$ no ocurre. El único módulo válido $b = 20$ es de tipo 2 y procede de la secuencia de Bézout $\frac{4}{3} < \frac{7}{5} < \frac{10}{7}$. □

EJEMPLO 7.40. Sea $S = \langle 10, 13, 27\rangle$. Se puede comprobar fácilmente que $\mathrm{m}(S) = 10$ y $\mathrm{g}(S) = 71$. Además las únicas representaciones modulares para S son $\mathrm{S}(25, 81)$ y $\mathrm{S}(57, 81)$ que corresponden a las secuencias de Bézout $\frac{13}{4} < \frac{10}{3} < \frac{27}{8}$ y $\frac{27}{19} < \frac{10}{7} < \frac{13}{9}$. Obsérvese que $81 = \mathrm{m}(S)+\mathrm{g}(S)$. El segundo tipo de módulo no ocurre pues no existe ningún entero positivo x para el cual $\frac{10}{7} < \frac{13}{9} < \frac{27}{x}$ sea una secuencia de Bézout. □

5. Las representaciones modulares para un semigrupo modular

El objetivo de esta sección es enunciar y demostrar el Teorema 7.42, el cual a groso modo caracteriza aritméticamente las representaciones modulares que pueden obtenerse a partir de un secuencia de Bézout dada.

LEMA 7.41. *Sea* $\frac{n_1}{b_1} < \frac{n_2}{b_2} < \cdots < \frac{n_p}{b_p}$ *una secuencia de Bézout propia con extremos adyacentes y sea* $\mathrm{S}(a,b)$ *una representación modular para el semigrupo numérico* $S = \langle n_1, \ldots, n_p\rangle$ *verificando que* $\frac{b}{a} = \frac{n_1}{b_1}$ *y* $\frac{n_p}{b_p} < \frac{b}{a-1}$. *Si* $d = \mathrm{mcd}\{a-1, b\}$, *entonces* $\frac{n_p}{b_p} < \frac{b/d}{(a-1)/d}$ *es una secuencia de Bézout y* $\frac{b}{d} \in S$.

DEMOSTRACIÓN. En vista de la igualdad $\frac{b/d}{(a-1)/d} = \frac{b}{a-1}$, por el Lema 2.16 deducimos que $\frac{b}{d} \in \mathrm{S}([\frac{b}{a}, \frac{b}{a-1}]) = \mathrm{S}(a,b) = S$. Supongamos por reducción al absurdo que $\frac{n_p}{b_p} < \frac{b/d}{(a-1)/d}$ no es una secuencia de Bézout. Entonces aplicando el Lema 7.2 a dichas fracciones se puede obtener una secuencia de Bézout propia $\frac{n_p}{b_p} < \frac{x}{y} < \cdots < \frac{b/d}{(a-1)/d}$. Por el Corolario 4.17 deducimos que $x \leq \max\{n_p, \frac{b}{d}\}$. Además, según el Lema 1.23 se verifica que $b \geq \mathrm{m}(S)+\mathrm{g}(S)$. Ya que por hipótesis $\frac{n_1}{b_1} < \frac{n_2}{b_2} < \cdots < \frac{n_p}{b_p}$ es una secuencia de Bézout propia con extremos adyacentes, por los Teoremas 4.8 y 4.21 tenemos que el conjunto $\{n_1, \ldots, n_p\}$ es el sistema minimal de generadores de S y por tanto $n_p \leq \mathrm{m}(S)+\mathrm{g}(S)$. Deducimos pues que $x \leq b$. Obsérvese también que $x \in \mathrm{S}(a,b)$, puesto que $\frac{b}{a} < \frac{x}{y} < \frac{b}{a-1}$.

Probemos que $\frac{n_1}{b_1} < \cdots < \frac{n_p}{b_p} < \frac{x}{y}$ es una secuencia de Bézout propia. En caso contrario, existiría un subíndice $i \in \{1, \ldots, p-1\}$ tal que $\frac{n_i}{b_i} < \frac{x}{y}$ es una secuencia de Bézout. Por el Lema 2.16 y el Teorema 4.8 ésto implicaría que $n_p \in \langle n_i, x\rangle$. Al ser n_p un generador minimal para S, resultaría $n_p = x$. Pero ésto es contradictorio con el hecho de que $\frac{n_p}{b_p} < \frac{x}{y}$ es una secuencia de Bézout, pues $xb_p - n_p y = n_p b_p - n_p y = n_p(b_p - y) \neq 1$.

Ahora veamos que las fracciones $\frac{n_1}{b_1} < \frac{x}{y}$ son adyacentes. De la secuencia de Bézout construida anteriormente deducimos que $\frac{x}{y} < \frac{b}{a-1}$, es decir, $xa < yb + x$. Combinando esta desigualdad con $x \leq b$, resulta que $xa < yb + b$, y por tanto $\frac{x}{y+1} < \frac{b}{a} = \frac{n_1}{b_1}$. Supongamos que $b_1 \neq 1$. La hipótesis $\frac{b}{a} = \frac{n_1}{b_1}$ implica que existe un entero positivo k tal

que $b = kn_1$ y $a = kb_1$. En consecuencia $\frac{x}{y} < \frac{b}{a-1} = \frac{kn_1}{kb_1-1} \leq \frac{n_1}{b_1-1}$, lo que prueba la condición de adyacencia.

Para finalizar la demostración observamos que si $\frac{n_1}{b_1} < \ldots < \frac{n_p}{b_p} < \frac{x}{y}$ es una secuencia de Bézout propia con extremos adyacentes, entonces aplicando los Teoremas 4.21 y 4.21, deducimos que el conjunto $\{n_1, \ldots, n_p, x\}$ es el sistema minimal de generadores de S, lo que contradice las hipótesis. □

TEOREMA 7.42. *Sea $\frac{n_1}{b_1} < \frac{n_2}{b_2} < \cdots < \frac{n_p}{b_p}$ una secuencia de Bézout propia con extremos adyacentes y $p \geq 3$. Sea S el semigrupo numérico generado por $\{n_1, \ldots, n_p\}$ y sean a y b enteros positivos verificando que $\frac{b}{a} = \frac{n_1}{b_1}$. Llamemos $d = \mathrm{mcd}\{a-1, b\}$. Entonces $\mathrm{S}(a,b)$ es una representación modular para S si y sólo si se verifican las siguientes condiciones:*

1. *$\frac{b}{d} \in S$,*
2. *se da la igualdad $\frac{n_p}{b_p} = \frac{b/d}{(a-1)/d}$, o bien $\frac{n_p}{b_p} < \frac{b/d}{(a-1)/d}$ es una secuencia de Bézout.*

En tal caso, además se verifica que $\mathrm{mcd}\{a,b\} = \lfloor \frac{n_p}{b_1 n_p - b_p n_1} \rfloor$.

DEMOSTRACIÓN. Veamos primero que las condiciones dadas en el enunciado son necesarias. Por los Teoremas 4.8 y 4.21 sabemos que $\{n_1, \ldots, n_p\}$ es el sistema minimal de generadores de S con lo cual $\mathrm{e}(S) \geq 3$. Aplicando el Teorema 7.9 deducimos que el par ordenado (a,b) está determinado de manera única. A partir de la hipótesis $\frac{b}{a} = \frac{n_1}{b_1}$ y del hecho de que $\mathrm{mcd}\{n_1, b_1\} = 1$, podemos escribir $b = kn_1$ y $a = kb_1$, siendo $k = \mathrm{mcd}\{a,b\}$. Por el Comentario 7.33 también sabemos que $k = \lfloor \frac{n_p}{b_1 n_p - b_p n_1} \rfloor$. Para concluir esta parte de la demostración, basta tener en cuenta el Lema 7.41.

Probemos ahora que las condiciones del enunciado son suficientes. Por las hipótesis y el Teorema 4.8 tenemos $S = \mathrm{S}([\frac{n_1}{b_1}, \frac{n_p}{b_p}])$. Si $\frac{n_p}{b_p} = \frac{b}{a-1}$, entonces obtenemos la secuencia $\frac{b}{a} = \frac{n_1}{b_1} < \frac{n_2}{b_2} < \cdots < \frac{n_p}{b_p} = \frac{b/d}{(a-1)/d} = \frac{b}{a-1}$. Aplicando el Lema 2.15 deducimos que $\mathrm{S}(a,b) = \mathrm{S}([\frac{b}{a}, \frac{b}{a-1}]) = \mathrm{S}([\frac{n_1}{b_1}, \frac{n_p}{b_p}]) = S$. Supongamos ahora que se verifica la desigualdad $\frac{n_p}{b_p} < \frac{b}{a-1}$ de manera que $\frac{n_p}{b_p} < \frac{b/d}{(a-1)/d}$ es una secuencia de Bézout. Entonces $\frac{n_1}{b_1} < \frac{n_2}{b_2} < \cdots < \frac{n_p}{b_p} < \frac{b/d}{(a-1)/d}$ es también una secuencia de Bézout. De nuevo por el Lema 2.15 y el Teorema 4.8, obtenemos $\mathrm{S}(a,b) = \mathrm{S}([\frac{b}{a}, \frac{b}{a-1}]) = \mathrm{S}([\frac{n_1}{b_1}, \frac{b/d}{(a-1)/d}]) = \langle n_1, \ldots, n_p, b/d \rangle$. Como estamos suponiendo que $b/d \in S$, entonces resulta $\mathrm{S}(a,b) = S$ con lo que termina la demostración. □

Observamos que bajo las hipótesis del teorema previo, cuando $d = 1$ la condición $\frac{b}{d} \in S$ se verifica trivialmente.

El Teorema 7.42 proporciona un método efectivo para decidir cuándo un semigrupo numérico es o no modular. En la descripción que hemos dado más abajo se devuelven todas las representaciones modulares existentes para el semigrupo dado.

ALGORITMO 7.43.

ENTRADA: un semigrupo numérico $S \neq \mathbb{N}$, minimalmente generado por $n_1, \ldots, n_p$.

SALIDA: el conjunto R de todas las parejas ordenadas (a,b), con $a < b$ enteros positivos tales que $S = \mathrm{S}(a,b)$.

1. Asignar $R = \emptyset$.
2. Para cada secuencia de Bézout propia $\frac{n_1}{b_1} < \cdots < \frac{n_p}{b_p}$ para los generadores $n_1, \ldots, n_p$, hacer:
   a) Asignar $k = \lfloor \frac{n_p}{b_1 n_p - b_p n_1} \rfloor$, $a = kb_1$, $b = kn_1$ y $S' = \mathrm{S}(a,b)$.
   b) Asignar $d = \mathrm{mcd}\{a-1, b\}$.
   c) Si $b/d \in S$ y además $\frac{n_p}{b_p} = \frac{b}{a-1}$ ó $b_p b - (a-1)n_p = d$, entonces añadir los pares ordenados (a,b) y $(b+1-a,b)$ al conjunto R.
3. Devolver el conjunto R.

Vemos que este algoritmo es más simple y eficiente que el Algoritmo 1.25 estudiado en el Capítulo 1, el cual estaba basado en una búsqueda acotada de valores.

Observamos además que todas las secuencias de Bézout propias (a lo sumo cuatro) para los generadores minimales del semigrupo pueden ser obtenidas fácilmente tal y como vimos en la demostración del Teorema 7.23. Además el Algoritmo 7.43 cubre el caso $p = 2$.

A continuación ilustramos el funcionamiento del Algoritmo 7.43 con algunos ejemplos.

EJEMPLO 7.44. Calcular todas las representaciones modulares para el semigrupo numérico $S = \langle 5, 7, 9 \rangle$.

Asignamos $R = \emptyset$. Sabemos del Ejemplo 7.27 que las únicas secuencias de Bézout propias para $5, 7, 9$ son

$$\frac{9}{4} < \frac{7}{3} < \frac{5}{2} \quad \text{y} \quad \frac{5}{3} < \frac{7}{4} < \frac{9}{5}.$$

Por consiguiente las representaciones modulares no simétricas candidatas para S son $\mathrm{S}(4k, 9k)$ y $\mathrm{S}(3k', 5k')$. Para la primera de ellas, de acuerdo con el Teorema 7.42, resulta $k = 2$, $b/\mathrm{mcd}\{a-1, b\} = 18 \in S$ y $\frac{5}{2} < \frac{18}{7}$ es una secuencia de Bézout. Por tanto $\mathrm{S}(8, 18)$ es una representación modular válida para S. Añadimos los pares ordenados $(8, 18)$ y $(11, 18)$ a R. Procedemos de manera similar para la segunda secuencia de Bézout. Ahora se obtiene $k' = 4$, $b/\mathrm{mcd}\{a-1, b\} = 20 \in S$ y la secuencia $\frac{9}{5} < \frac{20}{11}$ es de Bézout, por lo que aplicando de nuevo el Teorema 7.42 concluimos que $\mathrm{S}(12, 20)$ es una representación modular para S. Añadimos los pares ordenados $(12, 20)$ y $(9, 20)$ a R.

Así pues el algoritmo devuelve $R = \{(8, 18), (11, 18), (12, 20), (9, 20)\}$. □

EJEMPLO 7.45. Obtener todas las representaciones modulares para el semigrupo numérico $S = \langle 7, 15, 20, 53 \rangle$.

Comenzamos asignando $R = \emptyset$. Ahora hay cuatro secuencias de Bézout propias para los generadores minimales $7, 15, 20, 53$:

$$\frac{15}{13} < \frac{7}{6} < \frac{20}{17} < \frac{53}{45}, \qquad \frac{53}{46} < \frac{15}{13} < \frac{7}{6} < \frac{20}{17},$$
$$\frac{20}{3} < \frac{7}{1} < \frac{15}{2} < \frac{53}{7} \qquad \text{y} \qquad \frac{53}{8} < \frac{20}{3} < \frac{7}{1} < \frac{15}{2}.$$

Estudiamos cada una de ellas de forma separada.

Para la primera obtenemos una representación modular $\mathrm{S}(a,b)$ tal que $\frac{b}{a} = \frac{15}{13}$. Aplicando el Teorema 7.42, resulta $k = 3$, $a = 39$ y $b = 45$. Además $d = \mathrm{mcd}\{a-1, b\} = 1$, por lo que la condición (1) en dicho teorema se verifica trivialmente. Sin embargo $\frac{n_p}{b_p} = \frac{53}{45} < \frac{45}{38} = \frac{b/d}{(a-1)/d}$ no es una secuencia de Bézout, por lo que descartamos esta representación modular.

Para la segunda secuencia de Bézout obtenemos $k = 1$, $a = 46$ y $b = 53$. Las condiciones (1) y (2) del Teorema 7.42 se verifican pues $d = \mathrm{mcd}\{a-1, b\} = 1$ y $\frac{n_p}{b_p} = \frac{20}{17} < \frac{53}{45} = \frac{b/d}{(a-1)/d}$ es una secuencia de Bézout. Por consiguiente $\mathrm{S}(46, 53)$ es una representación modular para S. Añadimos los pares ordenados $(46, 53)$ y $(8, 53)$ al conjunto R.

Para la tercera secuencia de Bézout resulta $k = 2$, $a = 6$ y $b = 40$. Ahora $d = \mathrm{mcd}\{a-1, b\} = 5$ y $b/d = 8 \notin S$, por lo cual $\mathrm{S}(6, 40)$ no es una representación modular para S.

Finalmente, para la cuarta secuencia de Bézout calculamos $k = 1$, $a = 8$ y $b = 53$. En este caso $d = \mathrm{mcd}\{a-1, b\} = 1$ y $\frac{n_p}{b_p} = \frac{15}{2} < \frac{53}{7} = \frac{b/d}{(a-1)/d}$ es una secuencia de Bézout, de donde $\mathrm{S}(8, 53)$ es una representación modular para S. Observamos que los pares ordenados $(8, 53), (46, 53)$ ya pertenecen a R, por lo que el algoritmo devuelve $R = \{(8, 53), (46, 53)\}$. □

EJEMPLO 7.46. Sea el semigrupo numérico $S = \langle 10, 13, 27 \rangle$. Asignamos $R = \emptyset$. Se puede comprobar fácilmente que las únicas secuencias de Bézout propias para $10, 13, 27$ son

$$\frac{27}{19} < \frac{10}{7} < \frac{13}{9} \quad \text{y} \quad \frac{13}{4} < \frac{10}{3} < \frac{27}{8}.$$

Por el Teorema 7.42, las representaciones modulares no simétricas candidatas para S son $\mathrm{S}(57, 81)$ y $\mathrm{S}(24, 78)$. La primera es una representación modular para S pues $81 \in S$ y $\frac{13}{9} < \frac{81}{56}$ es una secuencia de Bézout. Consecuentemente añadimos los pares ordenados $(57, 81)$ y $(25, 81)$ al conjunto R. Sin embargo para la segunda secuencia de Bézout deducimos que $\mathrm{S}(24, 78)$ no es una representación modular para S, pues la secuencia $\frac{27}{8} < \frac{78}{23}$ no es de Bézout. El algoritmo devuelve $R = \{(57, 81), (25, 81)\}$. □

Para finalizar esta sección consideramos el siguiente ejemplo más teórico.

EJEMPLO 7.47. Veamos que todos los semigupos numéricos de la forma $S = \langle m, 2m-1, 2m+1 \rangle$, con m un entero positivo, son modulares y obtengamos todas sus representaciones modulares.

Claramente si $m = 1$, entonces $S = \mathbb{N}$ el cual es modular. Para $m = 2$ resulta $S = \langle 2,3\rangle$ que de acuerdo con el Corolario 2.36 también es modular. Además por el Teorema 7.11 todas las representaciones modulares para S son $\mathrm{S}(2,3), \mathrm{S}(2,4), \mathrm{S}(3,4), \mathrm{S}(3,6)$ y $\mathrm{S}(4,6)$.

Por tanto suponemos que $m \geq 3$. Teniendo en cuenta que m divide a $(2m-1)+(2m+1)$, es fácil ver que el conjunto de Apéry para el elemento m en S es

$$\begin{array}{ll} \{0\} \cup \{(2m-1)\cdot k, (2m+1)\cdot k \mid \ k = 1,2,\ldots,\frac{m-1}{2}\} & \text{si } m \text{ es impar,} \\ \{0\} \cup \{(2m-1)\cdot k, (2m+1)\cdot k \mid \ k = 1,2,\ldots,\frac{m-2}{2}\} \cup \{(2m-1)\cdot \frac{m}{2}\} & \text{si } m \text{ es par.} \end{array}$$

De aquí deducimos que

$$\mathrm{g}(S) = \begin{cases} (2m+1)\cdot \frac{m-1}{2} - m & \text{si } m \text{ es impar,} \\ (2m-1)\cdot \frac{m}{2} - m & \text{si } m \text{ es par,} \end{cases}$$

expresiones que se pueden unificar en una sola fórmula

$$\mathrm{g}(S) = (2m + (-1)^{m+1}) \cdot \lfloor \frac{m}{2} \rfloor - m.$$

Además aplicando el Lema 0.1 obtenemos la expresión siguiente para el número de huecos de S:

$$\#\mathrm{H}(S) = \frac{m(m-1)}{2}.$$

Ahora obtenemos todas las secuencias de Bézout que se pueden formar con los numeradores $m, 2m-1, 2m+1$.

Por la condición de convexidad para los numeradores (Corolario 4.17), tenemos salvo simetría dos ordenaciones posibles: $2m-1, m, 2m+1$ y $2m+1, 2m-1, m$.

1. Para la ordenación $2m-1, m, 2m+1$ resultan dos secuencias de Bézout (simétricas):

$$\frac{2m-1}{2} < \frac{m}{1} < \frac{2m+1}{2} \quad \text{y} \quad \frac{2m+1}{2m-1} < \frac{m}{m-1} < \frac{2m-1}{2m-3}.$$

   - Supongamos que $\mathrm{S}(a,b)$ es una representación modular para S tal que $\frac{b}{a} = \frac{2m-1}{2}$. Entonces $b = (2m-1)\lfloor \frac{2m+1}{4} \rfloor = (2m-1)\lfloor \frac{m}{2} \rfloor$ y $a = 2\lfloor \frac{2m+1}{4} \rfloor = 2\lfloor \frac{m}{2} \rfloor$. Teniendo en cuenta la hipótesis $m \geq 3$ es inmediato comprobar que cada generador de S pertenece a $\mathrm{S}(a,b)$ y por tanto $S \subseteq \mathrm{S}(a,b)$.
     Si m es par, es decir $m = 2k$, entonces $d = \mathrm{mcd}\{a-1, b\} = \mathrm{mcd}\{2k-1, 4k-1\} = 1$, por lo que $\frac{b}{d} = b = (2m-1)\lfloor \frac{m}{2} \rfloor \in S$. Siguiendo la notación del Teorema 7.42 se comprueba fácilmente que la secuencia $\frac{n_p}{b_p} < \frac{b/d}{(a-1)/d}$ es de Bézout, es decir la secuencia $\frac{4k+1}{2} < \frac{(4k-1)k}{2k-1}$ tiene producto cruzado igual a 1. Por tanto según el Teorema 7.42, cuando m es par se verifica que S es modular y $S = \mathrm{S}(a,b)$, es decir, $S = \mathrm{S}(2\lfloor \frac{m}{2} \rfloor, (2m-1)\lfloor \frac{m}{2} \rfloor)$.

Cuando m es impar, digamos $m = 2k+1$ tenemos $d = \mathrm{mcd}\{a-1, b\} = \mathrm{mcd}\{2k-1, 3\}$. Se verifica que

$$d = \begin{cases} 3 & \text{si } k \equiv 2 \bmod 3, \\ 1 & \text{en otro caso.} \end{cases}$$

Cuando $d = 1$ se puede verificar fácilmente que no se cumple ninguna de las dos condiciones del apartado (2) del Teorema 7.42, por lo cual en este caso $\mathrm{S}(a,b)$ no es una representación modular para S.

Cuando $d = 3$, resulta que $\frac{n_p}{b_p} < \frac{b/d}{(a-1)/d}$ es una secuencia de Bézout, por lo cual hemos de estudiar si el elemento b/d pertenece o no a S. Este problema, que es resoluble ya que disponemos del conjunto de Apèry para m, resulta a primera vista engorroso.

Estos dos últimos casos se resuelven de manera más fácil aplicando el siguiente argumento. Ya sabemos que $S \subseteq \mathrm{S}(a,b)$. De darse la igualdad ello implicaría la coincidencia de los respectivos números de huecos. Sabemos que $\mathrm{mcd}\{a-1, b\} \in \{1, 3\}$ y además es obvio que $\mathrm{mcd}\{a, b\} = k$. Aplicando la fórmula 7.47 así como el Teorema 1.13 se puede comprobar de manera inmediata que para m impar, ya sea $d = 1$ ó $d = 3$, los semigrupos tienen distinto número de huecos. Por consiguiente, cuando m es impar, $\mathrm{S}(a,b)$ no es una representación modular para S.

- Supongamos ahora que $\mathrm{S}(a,b)$ es una representación modular para S tal que $\frac{b}{a} = \frac{2m+1}{2m-1}$. Entonces $b = (2m+1)\lfloor \frac{2m-1}{4} \rfloor$ y $a = (2m-1)\lfloor \frac{2m-1}{4} \rfloor$. Obsérvese que

$$\lfloor \frac{2m-1}{4} \rfloor = \begin{cases} \lfloor \frac{m}{2} \rfloor & \text{si } m \text{ es impar,} \\ \lfloor \frac{m}{2} \rfloor - 1 & \text{si } m \text{ es par.} \end{cases}$$

De nuevo se puede verificar que cada generador de S pertenece a $\mathrm{S}(a,b)$ y por tanto $S \subseteq \mathrm{S}(a,b)$.

Supongamos que m es impar, digamos $m = 2k+1$. Aplicando el algoritmo de Euclides resulta $\mathrm{mcd}\{a-1, b\} = 1$. Siguiendo la notación del Teorema 7.42 se comprueba de nuevo que la secuencia $\frac{n_p}{b_p} < \frac{b/d}{(a-1)/d}$ es de Bézout, es decir la secuencia $\frac{4k+1}{4k-1} < \frac{(4k^2+3k)k}{4k^2+k-1}$ tiene producto cruzado igual a 1. Aplicando el Teorema 7.42 deducimos que cuando m es impar se verifica que S es modular y $S = \mathrm{S}(a,b)$, es decir $S = \mathrm{S}((2m-1)\lfloor \frac{2m-1}{4} \rfloor, (2m+1)\lfloor \frac{2m-1}{4} \rfloor)$.

Si m es par, digamos $m = 2k$ se puede verificar que $\mathrm{mcd}\{a, b\} = k-1$ y $\mathrm{mcd}\{a-1, b\} \in \{1, 3\}$. Usando de nuevo la fórmula 7.47 y el Teorema 1.13 vemos que en cualquiera de los dos casos no hay coincidencia de los números de huecos. Como $S \subseteq \mathrm{S}(a,b)$, deducimos que S está estrictamente incluido en $\mathrm{S}(a,b)$.

2. Cualquier secuencia de Bézout para la ordenación $2m+1, 2m-1, m$ ha de contener a la subsecuencia $\frac{2m-1}{2} < \frac{m}{1}$. Hemos de encontrar un entero positivo

u tal que $\frac{2m+1}{u} < \frac{2m-1}{2} < \frac{m}{1}$ sea una secuencia de Bézout, es decir, $u(2m-1)-2(2m+1)=1$. Ésto equivale a $(u-2)(2m-1)=5$, de donde resulta que $m=1$ y $u=7$, ó $m=3$ y $u=3$. Cuando $m=3$ tenemos el semigrupo $S=\langle 3,5,7\rangle$ cuyas representaciones modulares son $\mathrm{S}(3,7),\mathrm{S}(5,7),\mathrm{S}(4,9)$ y $\mathrm{S}(6,9)$.

Resumiendo, S es modular para cualquier entero positivo m.

- Si $m=1$, entonces $S=\mathbb{N}$.
- Si $m=2$, entonces $\mathrm{S}(2,3),\mathrm{S}(2,4),\mathrm{S}(3,4),\mathrm{S}(3,6)$ y $\mathrm{S}(4,6)$ son todas las representaciones modulares para S.
- Si $m=3$, entonces $\mathrm{S}(3,7),\mathrm{S}(5,7),\mathrm{S}(4,9)$ y $\mathrm{S}(6,9)$ son todas las representaciones modulares para S.
- Si $m\geq 4$ es par, entonces salvo simetría,
$$S=\mathrm{S}(2\lfloor\frac{m}{2}\rfloor,(2m-1)\lfloor\frac{m}{2}\rfloor)$$
es la única representación modular para S.
- Si $m\geq 4$ es impar, entonces salvo simetría,
$$S=\mathrm{S}((2m-1)\lfloor\frac{2m-1}{4}\rfloor,(2m+1)\lfloor\frac{2m-1}{4}\rfloor)$$
es la única representación modular para S.

Finalmente comentamos que en todos los casos $S=\mathrm{S}(\mathrm{m}(S),\mathrm{m}(S)+\mathrm{g}(S))$ es siempre una representación modular correcta para S. Esto puede verse fácilmente bien comprobando la inclusión $S\subseteq\mathrm{S}(\mathrm{m}(S),\mathrm{m}(S)+\mathrm{g}(S))$ y a continuación la coincidencia de los números de huecos, o bien teniendo en cuenta el Lema 1.24. □

CAPÍTULO 8

Semigrupos modulares generados por una progresión aritmética

Vimos en el Corolario 2.35 que todo semigrupo numérico generado por los primeros términos de una progresión aritmética es proporcionalmente modular. Sin embargo no todo semigrupo numérico generado por los primeros términos de una progresión aritmética es modular. En este capítulo estudiamos aquellos semigrupos numéricos generados por los primeros términos de una progresión aritmética y que son modulares. Por tanto vamos a considerar semigrupos S de la forma

$$S = \langle m, m+c, m+2c, \ldots, m+kc \rangle$$

tales que $\mathrm{mcd}\{m,c\} = 1$ y $1 \leq k \leq m-1$. Ya que cuando $m = 1$ resulta $S = \mathbb{N}$, el cual ya sabemos que es modular, supondremos siempre que $m \geq 2$.

Recordemos que según el Teorema 7.36, todo semigrupo modular con dimensión de inmersión mayor que dos admite a lo sumo dos módulos distintos para sus representaciones modulares. Por los Lemas 1.23 y 1.24 del Capítulo 1 sabemos además que $b \geq \mathrm{m}(S) + \mathrm{g}(S)$, y en el caso de que $b > \mathrm{m}(S) + \mathrm{g}(S)$, entonces $\mathrm{m}(S) | b$. Además, dada una representación modular $\mathrm{S}(a,b)$ para un semigrupo modular, decimos que el módulo b es de tipo 1, si $b = \mathrm{m}(S) + \mathrm{g}(S)$, y decimos que b es de tipo 2, si $b > \mathrm{m}(S) + \mathrm{g}(S)$.

El siguiente lema recoge resultados bien conocidos sobre semigrupos generados por progresiones aritméticas y que pueden ser encontrados en [**24**] y en [**46**].

LEMA 8.1. *Sea* $S = \langle m, m+c, m+2c, \ldots, m+kc \rangle$ *tal que* $\mathrm{mcd}\{m,c\} = 1$ *y* $1 \leq k \leq m-1$. *Entonces*

$$\mathrm{g}(S) = \left\lfloor \frac{m-2}{k} \right\rfloor m + (m-1)c \quad y \quad \#\mathrm{H}(S) = \frac{1}{2}((m-1)(q+c) + r(q+1)),$$

siendo q *y* r *el cociente y el resto, respectivamente, de la división de* $m-1$ *entre* k.

A continuación describimos cómo son las secuencias de Bézout para estos semigrupos.

LEMA 8.2. *Sea* $S = \langle m, m+c, m+2c, \ldots, m+kc \rangle$ *tal que* $\mathrm{mcd}\{m,c\} = 1$ *y* $1 \leq k \leq m-1$, *y sean* $u = c^{-1} \bmod m$ *y* $e = \frac{uc-1}{m}$.

1. *Si* $k < m-1$, *entonces hay exactamente dos secuencias de Bézout con sus fracciones mayores que* 1 *para los generadores minimales de S:*

$$\frac{m}{u} < \frac{m+c}{u+e} < \cdots < \frac{m+kc}{u+ke} \quad y \quad \frac{m+kc}{m-u+k(c-e)} < \cdots < \frac{m}{m-u}.$$

2. *Para $k = m-1$ hay exactamente cuatro secuencias de Bézout con sus fracciones mayores que* 1 *para los generadores minimales de S:*

$$\frac{m}{u} < \frac{m+c}{u+e} < \cdots < \frac{m+(m-1)c}{u+(m-1)e},$$

$$\frac{m+(m-1)c}{m-u+(m-1)(c-e)} < \cdots < \frac{m+c}{m-u+(c-e)} < \frac{m}{m-u},$$

$$\frac{m+(m-1)c}{u+(m-1)e+1} < \frac{m}{u} < \frac{m+c}{u+e} < \cdots < \frac{m+(m-2)c}{u+(m-2)e}$$

y

$$\frac{m+(m-2)c}{m-u+(m-2)(c-e)} < \cdots < \frac{m+c}{m-u+(c-e)} < \frac{m}{m-u} < \frac{m+(m-1)c}{m-u+(m-1)(c-e)-1}.$$

Además todas estas secuencias son propias con extremos adyacentes.

DEMOSTRACIÓN. Es inmediato comprobar que la secuencia $\frac{m}{u} < \frac{m+c}{u+e} < \cdots < \frac{m+kc}{u+ke}$ y su simétrica $\frac{m+kc}{m-u+k(c-e)} < \cdots < \frac{m}{m-u}$ son secuencias de Bézout para cualquier k tal que $1 \leq k \leq m-1$. Si $k < m-1$, entonces $m+kc < \mathrm{g}(S)$, con lo cual todos los generadores minimales son menores que el número de Frobenius. En este caso el Teorema 7.23 nos garantiza que dichas secuencias de Bézout son las únicas existentes.

Si $k = m-1$, entonces $m+kc > \mathrm{g}(S)$. En este caso, según el Teorema 7.23 aparte de las dos secuencias ya mencionadas, pueden existir dos más. Es inmediato comprobar que las secuencias

$$\frac{m+(m-1)c}{u+(m-1)e+1} < \frac{m}{u} < \frac{m+c}{u+e} < \cdots < \frac{m+(m-2)c}{u+(m-2)e}$$

y

$$\frac{m+(m-2)c}{m-u+(m-2)(c-e)} < \cdots < \frac{m+c}{m-u+(c-e)} < \frac{m}{m-u} < \frac{m+(m-1)c}{m-u+(m-1)(c-e)-1},$$

también son de Bézout, por lo que ya las tenemos todas.

Además todas las secuencias mencionadas son propias por el Lema 7.1 y con extremos adyacentes por el Teorema 4.21. □

COMENTARIO 8.3. Dada una secuencia de Bézout $\frac{n_1}{b_1} < \frac{n_2}{b_2} < \cdots < \frac{n_p}{b_p}$, recordemos que el producto cruzado para dicha secuencia es el valor $b_1 n_p - b_p n_1$. Es inmediato comprobar que una secuencia de Bézout y su simétrica tienen el mismo producto cruzado. □

Los siguientes lemas técnicos son utilizados en la demostración del Lema 8.7. El primero de ellos tiene una demostración inmediata.

LEMA 8.4. *Para cualesquiera dos números m y k tales que $2 \leq k \leq m-1$, se verifica*

$$\left\lfloor \frac{m-2}{k} \right\rfloor = \begin{cases} \lfloor \frac{m}{k} \rfloor - 1 & \text{si } m \equiv 0 \bmod k \text{ ó } m \equiv 1 \bmod k, \\ \lfloor \frac{m}{k} \rfloor & \text{en otro caso.} \end{cases}$$

LEMA 8.5. *Sea $S = \langle m, m+c, m+2c, \ldots, m+kc \rangle$ tal que $\mathrm{mcd}\{m,c\} = 1$ y $1 \leq k \leq m-1$, y sean además $u = c^{-1} \bmod m$ y $e = \frac{uc-1}{m}$. Definimos $a_1 = u(\lfloor \frac{m}{k} \rfloor + c), b_1 = m(\lfloor \frac{m}{k} \rfloor + c)$, $a_2 = (m-u+k(c-e))\lfloor \frac{m}{k} \rfloor$ y $b_2 = (m+kc)\lfloor \frac{m}{k} \rfloor$. Entonces $S \subseteq \mathrm{S}(a_1, b_1)$ y $S \subseteq \mathrm{S}(a_2, b_2)$.*

DEMOSTRACIÓN. Comprobamos que $m+ic \in \mathrm{S}(a_1, b_1)$ para todo i tal que $0 \leq i \leq k$, es decir, $a_1(m+ic) \bmod b_1 \leq m+ic$. Substituyendo a_1 y b_1 por sus definiciones y simplificando, resulta

$$\begin{aligned} u(\lfloor \frac{m}{k} \rfloor + c)(m+ic) \bmod m(\lfloor \frac{m}{k} \rfloor + c) &= uic(\lfloor \frac{m}{k} \rfloor + c) \bmod m(\lfloor \frac{m}{k} \rfloor + c) \\ = i(\lfloor \frac{m}{k} \rfloor + c) \bmod m(\lfloor \frac{m}{k} \rfloor + c) &= i(\lfloor \frac{m}{k} \rfloor + c) \leq m+ic \end{aligned}$$

para todo i tal que $0 \leq i \leq k$.

A continuación comprobamos que $m+ic \in \mathrm{S}(a_2, b_2)$ para todo i tal que $0 \leq i \leq k$, es decir, $a_2(m+ic) \bmod b_2 \leq m+ic$. Se verifica

$$\begin{aligned} a_2(m+ic) \bmod b_2 &= (m-u+k(c-e))\lfloor \frac{m}{k} \rfloor (m+ic) \bmod (m+kc)\lfloor \frac{m}{k} \rfloor \\ &= (-(u+ke)\lfloor \frac{m}{k} \rfloor (m+ic)) \bmod (m+kc)\lfloor \frac{m}{k} \rfloor. \end{aligned}$$

Calculamos

$$\begin{aligned} &(-(u+ke)(m+ic)) \bmod (m+kc) = ((-1)(um+uic+kem+keic)) \bmod (m+kc) \\ &= ((-1)(um+i+emi+kem+keic)) \bmod (m+kc) = ((-1)(um+i+kem)) \bmod (m+kc) \\ &= ((-1)(um+i+kcu-k)) \bmod (m+kc) = k-i, \end{aligned}$$

por lo que $a_2(m+ic) \bmod b_2 = (k-i)\lfloor \frac{m}{k} \rfloor$ y claramente esta cantidad es siempre menor o igual que $m+ic$. □

LEMA 8.6. *Sean m, c, k números enteros positivos tales que $\mathrm{mcd}\{m,c\} = 1$ y $1 \leq k \leq m-1$, y sean además $u = c^{-1} \bmod m$ y $e = \frac{uc-1}{m}$. Definimos $a_1 = u(\lfloor \frac{m}{k} \rfloor + c), b_1 = m(\lfloor \frac{m}{k} \rfloor + c)$, $a_2 = (m-u+k(c-e))\lfloor \frac{m}{k} \rfloor$ y $b_2 = (m+kc)\lfloor \frac{m}{k} \rfloor$. Entonces:*

1. $\mathrm{mcd}\{a_1, b_1\} = \lfloor \frac{m}{k} \rfloor + c$,
2. $\mathrm{mcd}\{a_2, b_2\} = \lfloor \frac{m}{k} \rfloor$,
3. *si $m \equiv 0 \bmod k$, entonces* $\mathrm{mcd}\{a_1 - 1, b_1\} = \lfloor \frac{m}{k} \rfloor$ y $\mathrm{mcd}\{a_2 - 1, b_2\} = \lfloor \frac{m}{k} \rfloor + c$,
4. *si $m \equiv 1 \bmod k$, entonces* $\mathrm{mcd}\{a_1 - 1, b_1\} = 1$ y $\mathrm{mcd}\{a_2 - 1, b_2\} = 1$.

DEMOSTRACIÓN. Observamos en primer lugar que $\mathrm{mcd}\{u+ek, m+ck\} = 1$, ya que $c(u+ek) - e(m+ck) = cu - em = 1$.

1. Como $\mathrm{mcd}\{u,m\}=1$, ésto implica que $\mathrm{mcd}\{a_1,b_1\}=\lfloor\frac{m}{k}\rfloor+c$.
2. Usando la igualdad $\mathrm{mcd}\{u+ek,m+ck\}=1$, resulta que $\mathrm{mcd}\{a_2,b_2\}=\lfloor\frac{m}{k}\rfloor$.
3. Supongamos que $m\equiv 0 \bmod k$.
   - Usando la hipótesis $cu-em=1$, se obtiene $\mathrm{mcd}\{a_1-1,b_1\}=\mathrm{mcd}\{u(\lfloor\frac{m}{k}\rfloor+c)-1,m(\lfloor\frac{m}{k}\rfloor+c)\}=\mathrm{mcd}\{u(\lfloor\frac{m}{k}\rfloor+em,m(\lfloor\frac{m}{k}\rfloor+c)\}$. Obsérvese que por la hipótesis $k|m$, ambos elementos son múltiplos de $\lfloor\frac{m}{k}\rfloor$. Por tanto, se reduce a comprobar que $\mathrm{mcd}\{u+ek,m+ck\}=1$. Pero ésto es inmediato, ya que $c(u+ek)-e(m+ck)=cu-em=1$.
   - Se verifica que $\mathrm{mcd}\{a_2-1,b_2\}=\mathrm{mcd}\{(u+ke)\lfloor\frac{m}{k}\rfloor+1,(m+kc)\lfloor\frac{m}{k}\rfloor\}$. Si $k|m$, entonces $\mathrm{mcd}\{a_2-1,b_2\}=\mathrm{mcd}\{u\lfloor\frac{m}{k}\rfloor+em+1,m\lfloor\frac{m}{k}\rfloor+mc\}=\mathrm{mcd}\{u\lfloor\frac{m}{k}\rfloor+cu,m\lfloor\frac{m}{k}\rfloor+mc\}=\lfloor\frac{m}{k}\rfloor+c$.
4. Supongamos ahora que $m\equiv 1 \bmod k$.
   - $\mathrm{mcd}\{a_1-1,b_1\}=\mathrm{mcd}\{u(\lfloor\frac{m}{k}\rfloor+c)-1,m(\lfloor\frac{m}{k}\rfloor+c)\}$. Veamos que este último término es igual a 1. Ya que $\mathrm{mcd}\{u(\lfloor\frac{m}{k}\rfloor+c)-1,\lfloor\frac{m}{k}\rfloor+c\}=1$, entonces queda $\mathrm{mcd}\{a_1-1,b_1\}=\mathrm{mcd}\{u(\lfloor\frac{m}{k}\rfloor+c)-1,m\}$. Pero $u(\lfloor\frac{m}{k}\rfloor+c)-1=u\lfloor\frac{m}{k}\rfloor+em$, por lo que $\mathrm{mcd}\{a_1-1,b_1\}=\mathrm{mcd}\{u\lfloor\frac{m}{k}\rfloor+em,m\}$. Recordando que $\mathrm{mcd}\{u,m\}=1$, resulta que $\mathrm{mcd}\{a_1-1,b_1\}=\mathrm{mcd}\{\lfloor\frac{m}{k}\rfloor,m\}$, lo cual vale 1 por la hipótesis $m\equiv 1 \bmod k$, ya que ésta implica $m-\lfloor\frac{m}{k}\rfloor k=1$.
   - $\mathrm{mcd}\{a_2-1,b_2\}=\mathrm{mcd}\{(m-u+k(c-e))\lfloor\frac{m}{k}\rfloor-1,(m+kc)\lfloor\frac{m}{k}\rfloor\}=\mathrm{mcd}\{(u+ke)\lfloor\frac{m}{k}\rfloor+1,(m+kc)\lfloor\frac{m}{k}\rfloor\}$; usando que $m-1=\lfloor\frac{m}{k}\rfloor k$ y $cu-em=1$, resulta $\mathrm{mcd}\{u\lfloor\frac{m}{k}\rfloor+e(m-1)+1,m\lfloor\frac{m}{k}\rfloor+c(m-1)\}=\mathrm{mcd}\{u\lfloor\frac{m}{k}\rfloor+cu-e,m\lfloor\frac{m}{k}\rfloor+cm-c\}=1$, pues si llamamos $\alpha=u\lfloor\frac{m}{k}\rfloor+cu-e$ y $\beta=m\lfloor\frac{m}{k}\rfloor+cm-c$, entonces $m\alpha-u\beta=1$.

□

LEMA 8.7. *Sea* $S=\langle m,m+c,m+2c,\ldots,m+kc\rangle$ *tal que* $\mathrm{mcd}\{m,c\}=1$ *y* $1\leq k\leq m-1$, *y sean además* $u=c^{-1} \bmod m$ *y* $e=\frac{uc-1}{m}$. *Definimos* $a_1=u(\lfloor\frac{m}{k}\rfloor+c)$, $b_1=m(\lfloor\frac{m}{k}\rfloor+c)$, $a_2=(m-u+k(c-e))\lfloor\frac{m}{k}\rfloor$ *y* $b_2=(m+kc)\lfloor\frac{m}{k}\rfloor$. *Se verifican las siguientes propiedades:*

1. *si* $m\equiv 0 \bmod k$, *entonces* $S=\mathrm{S}(a_1,b_1)=\mathrm{S}(a_2,b_2)$,
2. *si* $m\equiv 1 \bmod k$, *entonces* $S=\mathrm{S}(a_1,b_1)=\mathrm{S}(a_2,b_2)$.

DEMOSTRACIÓN. En cada caso y para cada una de las representaciones propuestas $\mathrm{S}(a_i,b_i)$, demostramos que $S\subseteq\mathrm{S}(a_i,b_i)$ y $\#\mathrm{H}(S)=\#\mathrm{H}(\mathrm{S}(a_i,b_i))$. Por el Lema 8.5 sabemos que $S\subseteq\mathrm{S}(a_1,b_1)$ y $S\subseteq\mathrm{S}(a_2,b_2)$, por lo que únicamente hay que comprobar las coincidencias de los números de huecos.

1. Supongamos que $m\equiv 0 \bmod k$. Por el Lema 8.6 sabemos que $\mathrm{mcd}\{a_1,b_1\}=\lfloor\frac{m}{k}\rfloor+c$ y $\mathrm{mcd}\{a_1-1,b_1\}=\lfloor\frac{m}{k}\rfloor$. Aplicando el Teorema 1.13, resulta

$$\begin{aligned}\#\mathrm{H}(\mathrm{S}(a_1,b_1))&=\frac{1}{2}(m(\lfloor\frac{m}{k}\rfloor+c)+1-(\lfloor\frac{m}{k}\rfloor+c)-\lfloor\frac{m}{k}\rfloor)\\&=\frac{1}{2}((m-1)(\lfloor\frac{m}{k}\rfloor+c)+1-\lfloor\frac{m}{k}\rfloor).\end{aligned}$$

Por otra parte, particularizando la fórmula para el número de huecos que aparece en el Lema 8.1, resulta

$$\#\mathrm{H}(S)=\frac{1}{2}((m-1)(\lfloor\frac{m-1}{k}\rfloor+c)+(\lfloor\frac{m-1}{k}\rfloor+1)(m-1-\lfloor\frac{m-1}{k}\rfloor k)).$$

La hipótesis $m\equiv 0 \bmod k$ implica que $\lfloor\frac{m-1}{k}\rfloor=\lfloor\frac{m}{k}\rfloor-1$, y por tanto

$$\#\mathrm{H}(S)=\frac{1}{2}((m-1)(\lfloor\frac{m}{k}\rfloor-1+c)+\lfloor\frac{m}{k}\rfloor(m-1-(\lfloor\frac{m}{k}\rfloor-1)k))$$

$$=\frac{1}{2}((m-1)(\lfloor\frac{m}{k}\rfloor+c)+1-\lfloor\frac{m}{k}\rfloor),$$

fórmula que coincide con la anteriormente calculada para $\#\mathrm{H}(\mathrm{S}(a_1,b_1))$.

Notamos que la hipótesis $m\equiv 0 \bmod k$ implica que $b_1=b_2=b$ y $a_1+a_2=b+1$, por lo que por el Lema 1.3 deducimos que $\mathrm{S}(a_1,b_1)=\mathrm{S}(a_2,b_2)$.

2. Supongamos ahora $m\equiv 1 \bmod k$. Calculamos previamente $\#\mathrm{H}(S)$ aplicando la fórmula del Lema 8.1:

$$\#\mathrm{H}(S)=\frac{1}{2}((m-1)(\lfloor\frac{m-1}{k}\rfloor+c)+(\lfloor\frac{m-1}{k}\rfloor+1)(m-1-\lfloor\frac{m-1}{k}\rfloor k)).$$

Ahora la hipótesis $m\equiv 1 \bmod k$ implica que $\lfloor\frac{m-1}{k}\rfloor=\lfloor\frac{m}{k}\rfloor$ y $m-1=\lfloor\frac{m-1}{k}\rfloor k$, por lo cual

$$\#\mathrm{H}(S)=\frac{1}{2}((m-1)(\lfloor\frac{m-1}{k}\rfloor+c)).$$

a) Consideramos en primer lugar $\mathrm{S}(a_1,b_1)$.
Usando los resultados del Lema 8.6, así como el Teorema 1.13, resulta

$$\#\mathrm{H}(\mathrm{S}(a_1,b_1))=\frac{1}{2}(m(\lfloor\frac{m}{k}\rfloor+c)+1-(\lfloor\frac{m}{k}\rfloor+c)-1)=\frac{1}{2}((m-1)(\lfloor\frac{m}{k}\rfloor+c)),$$

valor que coincide con el que hemos calculado para $\#\mathrm{H}(S)$.

b) Ahora tratamos $\mathrm{S}(a_2,b_2)$.
De nuevo por el Lema 8.6 y el Teorema 1.13, obtenemos

$$\#\mathrm{H}(\mathrm{S}(a_2,b_2))=\frac{1}{2}((m+kc)\lfloor\frac{m}{k}\rfloor+1-\lfloor\frac{m}{k}\rfloor-1)$$

$$=\frac{1}{2}\lfloor\frac{m}{k}\rfloor(m+kc-1)=\frac{1}{2}(\lfloor\frac{m}{k}\rfloor+c(m-1))=\frac{1}{2}((m-1)(\lfloor\frac{m-1}{k}\rfloor+c)),$$

que coincide con el valor de $\#\mathrm{H}(S)$.

□

TEOREMA 8.8. *Sea* $S=\langle m,m+c,m+2c,\ldots,m+kc\rangle$ *tal que* $\mathrm{mcd}\{m,c\}=1$. *Entonces S es un semigrupo modular si y sólo si* $(m \bmod k)\in\{0,1\}$.

Para $3\le m$ *y* $2\le k\le m-1$, *sean* $u=c^{-1} \bmod m$, $e=\frac{uc-1}{m}$, $a_1=u(\lfloor\frac{m}{k}\rfloor+c)$, $b_1=m(\lfloor\frac{m}{k}\rfloor+c)$, $a_2=(m-u+k(c-e))\lfloor\frac{m}{k}\rfloor$ *y* $b_2=(m+kc)\lfloor\frac{m}{k}\rfloor$. *En dicho caso las dos*

únicas representaciones modulares para S, salvo simetría, son $\mathrm{S}(a_1,b_1)$ *y* $\mathrm{S}(a_2,b_2)$*, es decir,* $S=\mathrm{S}(a,b)$ *para ciertos enteros positivos* $a<b$*, si y sólo si*

$$(a,b)\in\left\{\begin{array}{l}(u(\lfloor\frac{m}{k}\rfloor+c),m(\lfloor\frac{m}{k}\rfloor+c)),\\((m-u)(\lfloor\frac{m}{k}\rfloor+c)+1,m(\lfloor\frac{m}{k}\rfloor+c)),\\((m-u+k(c-e))\lfloor\frac{m}{k}\rfloor,(m+kc)\lfloor\frac{m}{k}\rfloor),\\((u+ke)\lfloor\frac{m}{k}\rfloor+1,(m+kc)\lfloor\frac{m}{k}\rfloor)\end{array}\right\}.$$

DEMOSTRACIÓN. Ya que según el Corolario 2.36 todo semigrupo numérico generado por dos elementos es modular y la condición $(m \bmod k)\in\{0,1\}$ se verifica trivialmente en este caso, podemos suponer que $m\geq 3$.

Veamos que la condición es necesaria. Supongamos que S es modular y que $\mathrm{S}(a,b)$ es una representación modular para S. Hemos de considerar todas las secuencias de Bézout propias y con extremos adyacentes para S. Según el Lema 8.2 hay dos secuencias de ese tipo cuando $k<m-1$ y cuatro cuando $k=m-1$. Tal y como veremos a posteriori, es suficiente considerar en cada caso las dos primeras secuencias que aparecen en dicho lema.

1. Consideremos la secuencia $\frac{m}{u}<\frac{m+c}{u+e}<\cdots<\frac{m+kc}{u+ke}$. Por el Teorema 7.42 tenemos $\frac{b}{a}=\frac{m}{u}$ siendo $b=tm$, $a=tu$ y $t=\lfloor\frac{m+kc}{kcu-kem}\rfloor=\lfloor\frac{m+kc}{k}\rfloor=\lfloor\frac{m}{k}\rfloor+c$. Por tanto $a=u(\lfloor\frac{m}{k}\rfloor+c)$ y $b=m(\lfloor\frac{m}{k}\rfloor+c)$. El módulo b obtenido es múltiplo de m, que es la multiplicidad de S, luego es un módulo de tipo 2. Además, por el Lema 8.1 sabemos que $\mathrm{g}(S)\equiv -c \bmod \mathrm{m}(S)$, de donde por los Lemas 1.23 y 1.24, b ha de ser de la forma $b=\mathrm{m}(S)+\mathrm{g}(S)+c+r\mathrm{m}(S)$, para cierto $r\geq 0$. Esta igualdad implica (usando la fórmula para $\mathrm{g}(S)$ dada en el Lema 8.1) que $m(\lfloor\frac{m}{k}\rfloor+c)=m+\lfloor\frac{m-2}{k}\rfloor m+(m-1)c+c+rm$. Simplificando resulta $\lfloor\frac{m}{k}\rfloor=1+\lfloor\frac{m-2}{k}\rfloor+r$. Aplicando el Lema 8.4, deducimos que $m\equiv 0 \bmod k$ ó $m\equiv 1 \bmod k$, y además que $r=0$, por lo que $b=\mathrm{m}(S)+\mathrm{g}(S)+c$.
2. Ahora hacemos un razonamiento similar para la secuencia simétrica de la considerada en el apartado anterior: $\frac{m+kc}{m-u+k(c-e)}<\cdots<\frac{m}{m-u}$. De nuevo por el Teorema 7.42 tenemos $\frac{b}{a}=\frac{m+kc}{m-u+k(c-e)}$, siendo que $b=tm$, $a=tu$ y $t=\lfloor\frac{m}{k}\rfloor$ (recuérdese que una secuencia de Bézout y su simétrica tienen el mismo producto cruzado). Por tanto, $a=(m-u+k(c-e))\lfloor\frac{m}{k}\rfloor$ y $b=(m+kc)\lfloor\frac{m}{k}\rfloor$. Si $k|m$, el módulo b coincide con el del caso anterior para el cual ya hemos comprobado que la conclusión del teorema es cierta. Así pues, podemos suponer que $k\nmid m$, lo cual nos lleva a que $m\nmid b$. Por los Lemas 1.23 y 1.24, b ha de ser un módulo de tipo 1, es decir $b=\mathrm{m}(S)+\mathrm{g}(S)$. Esta igualdad implica (usando la fórmula para $\mathrm{g}(S)$ en el Lema 8.1) que $(m+kc)\lfloor\frac{m}{k}\rfloor=\lfloor\frac{m-2}{k}\rfloor m+(m-1)c$. Si m no fuese congruente con 0 ni con 1 módulo k, aplicando el Lema 8.4 obtendríamos que $(m+kc)\lfloor\frac{m}{k}\rfloor=\lfloor\frac{m}{k}\rfloor m+(m-1)c$, es decir, $kc\lfloor\frac{m}{k}\rfloor=m+(m-1)c$. De aquí resultaría $(m-(m \bmod k))c=m+mc-c$, y por tanto $c(1-(m \bmod k))=m$, lo cual es absurdo. Por tanto llegamos

en este caso a que $m \equiv 0 \bmod k$ ó $m \equiv 1 \bmod k$, y además $k \nmid m$, es decir, $m \equiv 1 \bmod k$.

La condición suficiente es consecuencia del Lema 8.7.

Para el caso particular $k = m-1$, en principio tendríamos que considerar otras dos secuencias de Bézout más (Lema 8.2). Sin embargo, ello no es necesario, puesto que en este caso los dos valores ya obtenidos para b son distintos, es decir,

$$b_1 = m(\lfloor \frac{m}{k} \rfloor + c) = m(c+1) \neq m + (m-1)c = (m+kc)\lfloor \frac{m}{k} \rfloor = b_2.$$

Como por el Teorema 7.36 todo semigrupo modular con dimensión de inmersión mayor que dos admite a lo sumo dos módulos distintos, deducimos que las dos secuencias de Bézout restantes no dan información nueva. Por consiguiente, S tiene exactamente cuatro representaciones modulares. □

COROLARIO 8.9. *Para cualesquiera dos enteros positivos m y c primos relativos, el semigrupo* $\langle m, m+c, m+2c \rangle$ *es modular.*

COROLARIO 8.10. *Sean m y c enteros positivos primos relativos, con* $m \geq 4$. *Entonces para cualquier k tal que* $\lfloor \frac{m}{2} \rfloor + 1 \leq k \leq m-2$, *el semigrupo numérico* $\langle m, m+c, m+2c, \ldots, m+kc \rangle$ *no es modular.*

El Lema 8.8 también generaliza a la Proposición 7.31. El siguiente resultado está implícito en la demostración del Lema 8.8.

COROLARIO 8.11. *Sea S un semigrupo numérico generado por los primeros términos de una progresión aritmética de diferencia c. Si S es modular y* $\mathrm{S}(a,b)$ *es una representación modular para S, entonces* $b = \mathrm{m}(S) + \mathrm{g}(S)$ *ó* $b = \mathrm{m}(S) + \mathrm{g}(S) + c$.

COMENTARIO 8.12. Si un semigrupo modular S posee una representación modular con un módulo b de tipo 2, entonces el valor para dicho módulo ha de ser de la forma $b = \mathrm{m}(S) + \mathrm{g}(S) + (\mathrm{m}(S) - (\mathrm{g}(S) \bmod \mathrm{m}(S))) + r \cdot \mathrm{m}(S)$, con $r \geq 0$ (Lema 1.24). En los semigrupos generados por progresiones aritméticas, cuando se da este caso, hemos visto que $r = 0$. Sin embargo hay ejemplos de semigrupos modulares en los cuales $r > 0$, como por ejemplo $S = \langle 5, 11, 17 \rangle$. Este semigrupo es modular, pues $S = \mathrm{S}(7,34) = \mathrm{S}(8,40)$, y además $\mathrm{m}(S) = 5, \mathrm{g}(S) = 29$. El módulo $b = 40$ es de tipo 2 y ahora $r = 1$. □

Observar que la condición "$m \bmod k \in \{0,1\}$"dada en el Teorema 8.8 se puede escribir también como "$m \bmod k \leq 1$". De esta observación tan simple obtenemos el siguiente resultado bastante curioso.

TEOREMA 8.13. *Sea S un semigrupo numérico generado por los primeros términos de una progresión aritmética. Las siguientes afirmaciones son equivalentes:*

1. *S es un semigrupo modular,*
2. $\mathrm{m}(S) \bmod (\mathrm{e}(S) - 1) \leq 1$,
3. $\mathrm{S}(\mathrm{m}(S), \mathrm{e}(S) - 1) = \mathbb{N}$.

CAPÍTULO 9

Problemas abiertos

En este último capítulo de la memoria recogemos una lista de problemas en relación con los semigrupos modulares y los semigrupos proporcionalmente modulares para los cuales a día de hoy no conocemos una solución general.

PROBLEMA 1: Dados a y b enteros positivos tales que $a < b$, encontrar una fórmula en términos de a y de b para el número de Frobenius y para la multiplicidad de $\mathrm{S}(a,b)$.

Tal y como hemos ido viendo en la memoria, existen varios resultados parciales para este problema. En primer lugar, de acuerdo con los Lemas 1.3 y 1.4, dado un módulo b es suficiente considerar los valores para a tales que $a \leq \frac{b+1}{2}$.

Cuando el factor divide al módulo, vimos en el Corolario 3.4 que

$$\mathrm{g}(\mathrm{S}(a,ab)) = \left\lceil \frac{(b-1)(a-1)}{b} \right\rceil b - 1,$$

y en el Lema 3.1 que

$$\mathrm{m}(\mathrm{S}(a,ab)) = b.$$

Mencionamos también los siguientes resultados que aparecen en [**28**]. Si σ es una permutación perteneciente a S_n, se define $\sigma(0) = 0$.

TEOREMA 9.1. *Para dos enteros positivos $a < b$, definimos $d = \mathrm{mcd}\{a,b\}$ y $d' = \mathrm{mcd}\{a-1,b\}$. Si $dd' \neq b$, sea $p = ((\frac{a}{d})^{-1}(-\frac{a-1}{d'})) \bmod \frac{b}{dd'}$. Entonces*

$$\mathrm{Ap}\left(\mathrm{S}(a,b), \frac{b}{d'}\right) = \left\{ dk + d'\sigma_{p,\frac{b}{dd'}}(k) \mid k \in \{0,\ldots,\frac{b}{dd'}-1\} \right\} + \{0, \frac{b}{d}, 2\frac{b}{d}, \ldots, (d-1)\frac{b}{d}\}.$$

Teniendo en cuenta las fórmulas que aparecen en la Proposición 0.1, se obtiene el siguiente resultado.

COROLARIO 9.2. *Bajo las mismas hipótesis del Teorema 9.1,*

$$\mathrm{g}(\mathrm{S}(a,b)) = \mathrm{máx}\left\{ dk + d'\sigma_{p,\frac{b}{dd'}}(k) \mid k \in \{0,\ldots,\frac{b}{dd'}-1\} \right\} + (d-1)\frac{b}{d} - \frac{b}{d'}.$$

También son interesantes los siguientes resultados que aparecen en [**41**] y que en algunos casos particulares aportan fórmulas concretas.

LEMA 9.3. *Sean a y b dos enteros positivos tales que $a < b$ y $(b \bmod a) \neq 0$. Entonces*

$$g(S(a,b)) \leq b - \left\lceil \frac{b}{a} \right\rceil .$$

PROPOSICIÓN 9.4. *Sean a y b enteros positivos tales que $a < b$ y $(b \bmod a) \neq 0$. Entonces $g(S(a,b)) = b - \lceil b/a \rceil$ si y sólo si $(a-1)\cdot(a-(b \bmod a)) < b$.*

COROLARIO 9.5. *Sean a y b enteros positivos tales que $a < b$, $(b \bmod a) \neq 0$ y $(a-1)\cdot(a-(b \bmod a)) < b$. Entonces $m(S(a,b)) = \lceil b/a \rceil$.*

El siguiente argumento intuitivo llega a un resultado similar al de la Proposición 9.4. Dado $S = S(a,b)$, por el Lema 2.15 sabemos que $S = S([\frac{b}{a}, \frac{b}{a-1}])$, es decir,

$$S = (\bigcup_{0 \leq k} [\frac{kb}{a}, \frac{kb}{a-1}] \cap \mathbb{N}).$$

Geométricamente, entre 0 y b, los elementos que pertenecen a $S(a,b)$ son aquellos x que se encuentran en la base de algún triángulo rectángulo de vértices $(\frac{kb}{a}, 0)$, $(\frac{kb}{a-1}, 0)$ y $(\frac{kb}{a-1}, \frac{kb}{a-1})$, para algún k tal que $0 \leq k \leq a-1$.

Véase la figura siguiente donde se dibuja la situación para $S(5,8) = \{0, 2, 4, \rightarrow\}$.

Observamos que en el triángulo rectángulo más a la derecha no hay huecos, con lo cual $\{\lfloor \frac{(a-1)b}{a} \rfloor, \rightarrow\} \subseteq S$. Por consiguiente

$$S = (\bigcup_{0 \leq k \leq a-2} [\frac{kb}{a}, \frac{kb}{a-1}] \cap \mathbb{N}) \cup \{\lfloor \frac{(a-1)b}{a} \rfloor, \rightarrow\}$$

y

$$H(S) = (\bigcup_{0 \leq k \leq a-2} (\frac{kb}{a-1}, \frac{(k+1)b}{a})) \cap \mathbb{N}.$$

Consideremos el intervalo que aparece más a la derecha, es decir, $(\frac{(a-2)b}{a-1}, \frac{(a-1)b}{a})$. Su amplitud es $\frac{b}{a(a-1)}$. Si $\frac{b}{a(a-1)} > 1$, entonces $g(S)$ es el mayor entero que pertenece al intervalo $(\frac{(a-2)b}{a-1}, \frac{(a-1)b}{a})$. Obtenemos el siguiente resultado.

PROPOSICIÓN 9.6. *Sean a y b enteros positivos tales que $a < b$. Si $b > a(a-1)$, entonces*

$$g(S(a,b)) = \begin{cases} \frac{(a-1)b}{a} - 1 & \text{si } a|b, \\ \lfloor \frac{(a-1)b}{a} \rfloor & \text{en caso contrario.} \end{cases}$$

COMENTARIO 9.7. La desigualdad en la condición "$b > a(a-1)$"de la proposición anterior ha de ser estricta. Si se da la igualdad, la conlusión no tiene por qué darse como se puede comprobar fácilmente con el ejemplo $S = S(3,6)$.

Observamos además que si $a < \sqrt{b}$, entonces se verifica $a(a-1) < b$, obteniendo la conclusión de la proposición anterior. □

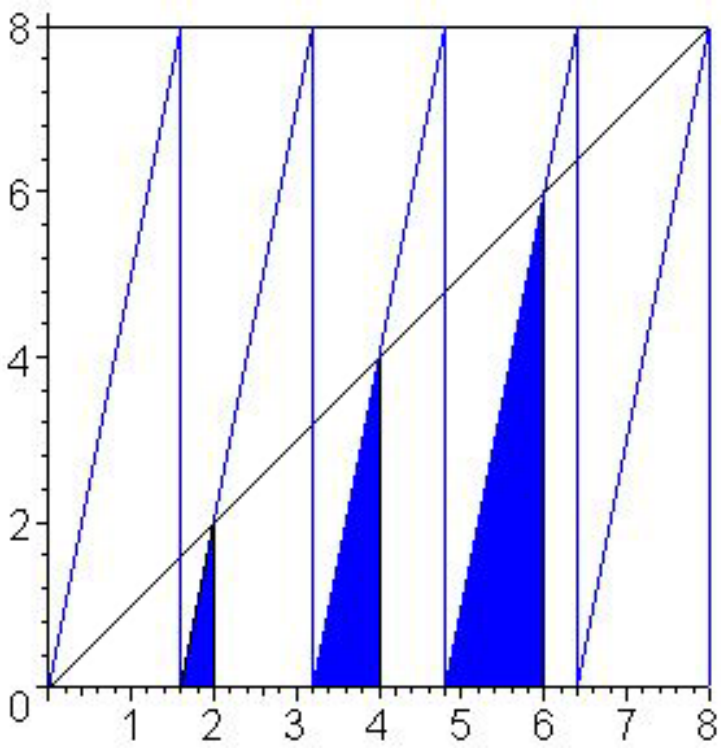

FIGURA 1. $S(5,8)$

El Teorema 1.13 da una fórmula general para el número de huecos de $S(a,b)$ en términos de a y b. Ésto nos lleva a plantear el siguiente problema.

> PROBLEMA 2: Dados a,b y c enteros positivos tales que $c < a < b$, encontrar un fórmula en términos de a,b y c para el número de huecos de $S(a,b,c)$.

Aparte de los semigrupos modulares, existen familias de semigrupos proporcionalmente modulares para los cuales se dispone de una respuesta para el problema anterior. Este es el caso de los semigrupos numéricos generados por una progresión aritmética los cuales fueron estudiados en el capítulo anterior.

> PROBLEMA 3: Dado un semigrupo proporcionalmente modular S descrito de la forma $S = \frac{\langle n_1,n_2\rangle}{d}$, estudiar si existen fórmulas en términos de n_1,n_2 y d para $g(S)$, $m(S)$ y $\#H(S)$.

Desde este punto de vista, $g(S)$ es el mayor múltiplo del entero d que no pertenece a $\langle n_1,n_2\rangle$.

Recordemos que según la Proposición 5.13, podemos asumir que los enteros n_1, n_2, d son primos relativos dos a dos.

El siguiente resultado fué obtenido por P.A. García-Sánchez.

LEMA 9.8. *Sean n_1, n_2 y d enteros positivos tales que $(n_1, n_2) = (n_1, d) = (n_2, d) = 1$ y $n_1 < n_2$. Entonces existe un entero positivo k tal que $0 < k < d$ y $\frac{kn_1+n_2}{d} \in \mathrm{Ap}(\frac{\langle n_1,n_2\rangle}{d}, n_1)$. Además*

$$\mathrm{Ap}\left(\frac{\langle n_1,n_2\rangle}{d}, n_1\right) = \left\{\frac{((ik) \bmod d)n_1 + in_2}{d} \mid i \in \{0,\ldots,n_1-1\}\right\}.$$

Aplicando las fórmulas que aparecen en la Proposición 0.1 al resultado dado en el lema anterior, resulta

$$\mathrm{g}\left(\frac{\langle n_1,n_2\rangle}{d}\right) = \max\left\{\frac{((ik) \bmod d)n_1 + in_2}{d} \mid i \in \{0,\ldots,n_1-1\}\right\} - n_1$$

y

$$\#\mathrm{H}\left(\frac{\langle n_1,n_2\rangle}{d}\right) = \frac{1}{n_1}\left(\frac{n_1}{d}\sum_{i=1}^{n_1-1}((ik) \bmod d) + \frac{(n_1-1)n_1n_2}{2d}\right) - \frac{n_1-1}{2},$$

siendo $k = ((-n_2)n_1^{-1}) \bmod d$.

Sin embargo no hemos encontrado criterios que caractericen cuándo la expresión "$((ik) \bmod d)n_1 + in_2$.ªlcanza el máximo al variar i en el conjunto $\{0,\ldots,n_1-1\}$. Tampoco hemos podido encontrar una fórmula compacta para $\sum_{i=1}^{n_1-1}((ik) \bmod d)$. De hecho, usando la identidad $(ik) \bmod d = ik - \lfloor \frac{ik}{d} \rfloor \cdot d$, el cálculo de la sumatoria anterior se reduce al cálculo de $\sum_{i=1}^{n_1-1} \lfloor \frac{ik}{d} \rfloor$. Estamos contando el número de puntos reticulares que hay en el interior del triángulo rectángulo de vértices $(0,0), (n_1,0)$ y $(0, \frac{n_1k}{d})$ incluyendo aquellos que se encuentran sobre la diagonal principal (nótese que uno de los catetos del triángulo tiene longitud no entera).

PROBLEMA 4: Sean a, b y c enteros positivos tales que $c < a < b$. Si $S = \mathrm{S}(a,b,c)$, encontrar un fórmula en términos de a, b y c para $\mathrm{m}(S)$, $\mathrm{e}(S)$ y $\mathrm{t}(S)$.

Para un semigrupo numérico S se define $\mathrm{n}(S) = \#(S \cap \{0,1,\ldots,\mathrm{g}(S)\})$, es decir, $\mathrm{n}(S) = \mathrm{g}(S) + 1 - \#\mathrm{H}(S)$. La conjetura de Wilf afirma que $\#\mathrm{H}(S) \leq (\mathrm{e}(S)-1) \cdot \mathrm{n}(S)$ (véase [**53**]). Existen varios tipos de semigrupos numéricos para los cuales se ha demostrado que la conjetura de Wilf es cierta, entre los que mencionamos los semigrupos irreducibles, los semigrupos con máxima dimensión de inmersión y los semigrupos S con $\mathrm{e}(S) \leq 3$ (véase [**10**]).

PROBLEMA 5: Estudiar si la clase de los semigrupos modulares así como la clase de los semigrupos proporcionalmente modulares verifica la conjetura de Wilf.

PROBLEMA 6: Dados a,b y c enteros positivos tales que $c < a < b$, si $S = \mathrm{S}(a,b,c)$, determinar en términos de a,b y c cuándo S es de alguno de los siguientes tipos especiales: simétrico, pseudo-simétrico, MED-semigrupo.

PROBLEMA 7: Dado un semigrupo numérico S, encontrar un algoritmo que nos permita decidir si existen enteros positivos n_1,n_2,n_3 y d tales que $S = \frac{\langle n_1,n_2,n_3\rangle}{d}$.

En el resto de este capítulo a,b y c serán números enteros mayores que 1 y primos relativos dos a dos. Además n representará un entero mayor o igual que 3. Es inmediato demostrar por inducción sobre n que $c^n-(c-1)^n > 3c$. Teniendo en cuenta este hecho se obtiene el siguiente lema.

LEMA 9.9. *Si $a^n+b^n=c^n$, entonces $a^n > 3c$.*

LEMA 9.10. *Si $a^n+b^n=c^n$, entonces $S=\langle a^n,c^{n-1},b^n\rangle$ es un semigrupo numérico proporcionalmente modular con dimensión de inmersión igual a* 3.

DEMOSTRACIÓN. Veamos en primer lugar que los generadores de S son independientes. Si $\lambda a^n+\mu c^{n-1}=b^n$ con λ y μ distintos de cero, entonces $\lambda c a^n+\mu c^n = cb^n$, lo cual implica que $(\lambda c+\mu)a^n=(c-\mu)b^n$. En particular vemos que a^n divide a $(c-\mu)b^n$. Teniendo en cuenta que $\mathrm{mcd}\{a,b\}=1$, deducimos que $c-\mu \geq a^n$, y por tanto $c > a^n$, lo cual es absurdo por el Lema 9.9. Si $\lambda a^n = c^{n-1}$, ésto implicaría que $\mathrm{mcd}\{a,b\} \neq 1$.

Finalmente, ya que $a^n+b^n \equiv 0 \bmod c^{n-1}$, aplicando el Teorema 4.32 deducimos que S es proporcionalmente modular. □

PROPOSICIÓN 9.11.

$$a^n+b^n=c^n \iff \frac{\langle a^n,b^n\rangle}{c} = \langle a^n,c^{n-1},b^n\rangle$$

DEMOSTRACIÓN.

Sean u y v enteros positivos verificando que $b^n u - a^n v = 1$.

Condición necesaria. Es inmediato constatar que la secuencia $\frac{a^n}{uc} < \frac{c^{n-1}}{u+v} < \frac{b^n}{vc}$ es de Bézout. Entonces por el Teorema 4.8 se tiene $\langle a^n,c^{n-1},b^n\rangle = \mathrm{S}([\frac{a^n}{uc},\frac{b^n}{vc}])$, y por la demostración del Teorema 5.2 resulta $\mathrm{S}([\frac{a^n}{uc},\frac{b^n}{vc}]) = \frac{\langle a^n,b^n\rangle}{c}$, con lo cual se obtiene la conclusión del enunciado.

Condición suficiente. De nuevo, por la demostración del Teorema 5.2 tenemos $\mathrm{S}([\frac{a^n}{uc},\frac{b^n}{vc}]) = \frac{\langle a^n,b^n\rangle}{c}$. Denotemos este semigrupo por S. Supongamos además que $\frac{\langle a^n,b^n\rangle}{c} = \langle a^n,c^{n-1},b^n\rangle$. Por el Teorema 4.4 existe una secuencia de Bézout con extremos $\frac{a^n}{uc}$ y $\frac{b^n}{vc}$. Ya que por el Teorema 4.8 los numeradores de dicha secuencia generan a S, y toda secuencia de Bézout se puede refinar a otra secuencia de Bézout propia con los mismos extremos, concluimos que existe una secuencia de Bézout de la forma

$\frac{a^n}{uc} < \frac{c^{n-1}}{\alpha} < \frac{b^n}{vc}$. Obsérvese que además $\frac{a^n}{uc}$ y $\frac{b^n}{vc}$ son extremos adyacentes. Aplicando el Lema 4.13 concluimos que $c^{n-1} = \frac{a^n+b^n}{c}$ y por tanto $c^n = a^n + b^n$. □

El denominado **Último Teorema de Fermat** afirma que para cualquier número natural $n \geq 3$, la ecuación diofántica $x^n + y^n = z^n$ no admite ninguna solución verificando $x \cdot y \cdot z \neq 0$. Como es bien conocido, este teorema tras más de trescientos años de intentos infructuosos, finalmente fué demostrado por Andrew Wiles con la ayuda de Richard Taylor en 1995 (véase [**51**], [**52**]).

Obsérvese que para $n \geq 3$, la ecuación diofántica $x^n + y^n = z^n$ no tiene ninguna solución verificando $x \cdot y \cdot z \neq 0$ en la que alguna de las incógnitas sea igual a 1. Por tanto, de cara a resolver dicha ecuación, se puede además suponer que x, y, z son enteros mayores o iguales que 2 y primos relativos dos a dos. Con todo ésto podemos enunciar el siguiente resultado.

TEOREMA 9.12. *Son equivalentes:*

1. *el Último Teorema de Fermat,*
2. *el semigrupo numérico* $\frac{\langle a^n, b^n \rangle}{c}$ *no está generado minimalmente por* $\{a^n, c^{n-1}, b^n\}$.

PROBLEMA 8: Sean a, b y c números enteros mayores que 1 y primos relativos dos a dos y sea n un entero mayor o igual que 3. Probar que el semigrupo numérico $\frac{\langle a^n, b^n \rangle}{c}$ no está generado minimalmente por $\{a^n, c^{n-1}, b^n\}$.

APÉNDICE

TABLAS

En este apéndice incluimos algunas tablas que hemos generado utilizando unas rutinas que hemos escrito en el lenguaje funcional Haskell (véase [**15**]).

En las primeras tablas mostramos los invariantes que hemos estudiado en esta memoria para los primeros semigrupos modulares. Si $S = \mathrm{S}(a,b)$, denotamos por m la multiplicidad, e la dimensión de inmersión, g el número de Frobenius y h el número de huecos de S.

La última tabla muestra para los primeros valores de g, todos los semigrupos modulares cuyo número de Frobenius es g.

a	b	m	e	g	h
1	2	1	1	-1	0
1	3	1	1	-1	0
2	3	2	2	1	1
1	4	1	1	-1	0
2	4	2	2	1	1
1	5	1	1	-1	0
2	5	3	3	2	2
3	5	2	2	3	2
1	6	1	1	-1	0
2	6	3	3	2	2
3	6	2	2	1	1
1	7	1	1	-1	0
2	7	4	4	3	3
3	7	3	3	4	3
4	7	2	2	5	3
1	8	1	1	-1	0
2	8	4	4	3	3
3	8	3	2	5	3
4	8	2	2	3	2
1	9	1	1	-1	0
2	9	5	5	4	4
3	9	3	2	5	3
4	9	3	3	4	3
5	9	2	2	7	4
1	10	1	1	-1	0
2	10	5	5	4	4
3	10	4	3	6	4
4	10	3	2	7	4
5	10	2	2	3	2
1	11	1	1	-1	0
2	11	6	6	5	5
3	11	4	3	7	5
4	11	3	3	8	5
5	11	5	5	6	5
6	11	2	2	9	5
1	12	1	1	-1	0
2	12	6	6	5	5
3	12	4	3	7	4
4	12	3	2	5	3
5	12	3	2	7	4
6	12	2	2	5	3

a	b	m	e	g	h
1	13	1	1	-1	0
2	13	7	7	6	6
3	13	5	4	8	6
4	13	4	4	9	6
5	13	3	3	10	6
6	13	5	5	8	6
7	13	2	2	11	6
1	14	1	1	-1	0
2	14	7	7	6	6
3	14	5	3	9	6
4	14	4	3	10	6
5	14	3	2	11	6
6	14	5	4	9	6
7	14	2	2	5	3
1	15	1	1	-1	0
2	15	8	8	7	7
3	15	5	3	9	6
4	15	4	2	11	6
5	15	3	3	8	5
6	15	3	2	7	4
7	15	5	5	8	6
8	15	2	2	13	7
1	16	1	1	-1	0
2	16	8	8	7	7
3	16	6	4	10	7
4	16	4	2	11	6
5	16	4	4	9	6
6	16	3	2	13	7
7	16	5	3	11	7
8	16	2	2	7	4
1	17	1	1	-1	0
2	17	9	9	8	8
3	17	6	4	11	8
4	17	5	5	12	8
5	17	4	3	13	8
6	17	3	3	14	8
7	17	5	5	12	8
8	17	7	7	10	8
9	17	2	2	15	8
1	18	1	1	-1	0
2	18	9	9	8	8

a	b	m	e	g	h
3	18	6	4	11	7
4	18	5	3	13	7
5	18	4	3	14	8
6	18	3	2	11	6
7	18	3	3	10	6
8	18	5	3	13	8
9	18	2	2	7	4
1	19	1	1	-1	0
2	19	10	10	9	9
3	19	7	5	12	9
4	19	5	3	14	9
5	19	4	4	15	9
6	19	7	7	12	9
7	19	3	3	16	9
8	19	5	4	14	9
9	19	7	7	12	9
10	19	2	2	17	9
1	20	1	1	-1	0
2	20	10	10	9	9
3	20	7	4	13	9
4	20	5	3	14	8
5	20	4	2	11	6
6	20	4	3	13	7
7	20	3	2	17	9
8	20	5	5	12	8
9	20	5	3	13	8
10	20	2	2	9	5
1	21	1	1	-1	0
2	21	11	11	10	10
3	21	7	4	13	9
4	21	6	4	15	9
5	21	5	5	16	10
6	21	4	2	17	9
7	21	3	2	11	6
8	21	3	2	13	7
9	21	5	3	16	9
10	21	7	7	12	9
11	21	2	2	19	10
1	22	1	1	-1	0
2	22	11	11	10	10
3	22	8	5	14	10

a	b	m	e	g	h
4	22	6	3	16	10
5	22	5	3	17	10
6	22	4	3	18	10
7	22	7	6	15	10
8	22	3	2	19	10
9	22	5	3	17	10
10	22	7	5	15	10
11	22	2	2	9	5
1	23	1	1	-1	0
2	23	12	12	11	11
3	23	8	5	15	11
4	23	6	4	17	11
5	23	5	5	18	11
6	23	4	3	19	11
7	23	7	6	16	11
8	23	3	3	20	11
9	23	8	8	15	11
10	23	5	3	18	11
11	23	9	9	14	11
12	23	2	2	21	11
1	24	1	1	-1	0
2	24	12	12	11	11
3	24	8	5	15	10
4	24	6	3	17	9
5	24	5	2	19	10
6	24	4	4	15	9
7	24	4	2	17	9
8	24	3	3	14	8
9	24	3	2	13	7
10	24	5	3	19	10
11	24	7	4	17	11
12	24	2	2	11	6
1	25	1	1	-1	0
2	25	13	13	12	12
3	25	9	6	16	12
4	25	7	5	18	12
5	25	5	2	19	10
6	25	5	5	16	10
7	25	4	4	21	12
8	25	7	7	18	12
9	25	3	3	22	12
10	25	5	3	17	10
11	25	5	3	18	10
12	25	9	9	16	12
13	25	2	2	23	12

a	b	m	e	g	h
1	26	1	1	-1	0
2	26	13	13	12	12
3	26	9	5	17	12
4	26	7	4	19	12
5	26	6	5	20	12
6	26	5	3	21	12
7	26	4	3	22	12
8	26	7	4	19	12
9	26	3	2	23	12
10	26	8	7	18	12
11	26	5	4	21	12
12	26	7	4	19	12
13	26	2	2	11	6
1	27	1	1	-1	0
2	27	14	14	13	13
3	27	9	5	17	12
4	27	7	3	20	12
5	27	6	5	21	13
6	27	5	3	22	12
7	27	4	2	23	12
8	27	7	7	20	13
9	27	3	2	17	9
10	27	3	3	16	9
11	27	5	3	22	13
12	27	7	5	20	12
13	27	9	9	16	12
14	27	2	2	25	13
1	28	1	1	-1	0
2	28	14	14	13	13
3	28	10	6	18	13
4	28	7	3	20	12
5	28	6	3	22	12
6	28	5	3	23	13
7	28	4	3	19	10
8	28	4	2	17	9
9	28	7	7	18	12
10	28	3	2	25	13
11	28	8	6	20	13
12	28	5	2	23	12
13	28	7	4	19	12
14	28	2	2	13	7
1	29	1	1	-1	0
2	29	15	15	14	14
3	29	10	6	19	14
4	29	8	6	21	14

a	b	m	e	g	h
5	29	6	3	23	14
6	29	5	5	24	14
7	29	9	9	20	14
8	29	4	3	25	14
9	29	7	5	22	14
10	29	3	3	26	14
11	29	8	8	21	14
12	29	5	5	24	14
13	29	7	4	22	14
14	29	11	11	18	14
15	29	2	2	27	14
1	30	1	1	-1	0
2	30	15	15	14	14
3	30	10	6	19	13
4	30	8	4	22	13
5	30	6	3	23	12
6	30	5	2	19	10
7	30	5	3	21	12
8	30	4	3	26	14
9	30	7	4	23	13
10	30	3	2	17	9
11	30	3	2	19	10
12	30	5	3	22	12
13	30	5	2	23	12
14	30	9	6	21	14
15	30	2	2	13	7
1	31	1	1	-1	0
2	31	16	16	15	15
3	31	11	7	20	15
4	31	8	4	23	15
5	31	7	7	24	15
6	31	6	6	25	15
7	31	5	3	26	15
8	31	4	4	27	15
9	31	7	7	24	15
10	31	10	10	21	15
11	31	3	3	28	15
12	31	8	5	23	15
13	31	5	4	26	15
14	31	7	5	24	15
15	31	11	11	20	15
16	31	2	2	29	15
1	32	1	1	-1	0
2	32	16	16	15	15
3	32	11	6	21	15

g	$S(a_1, b_1), \ldots$
2	S(2,6),S(2,5)
3	S(5,10),S(4,8),S(2,8),S(2,7),S(3,5)
4	S(2,10),S(4,9),S(2,9),S(3,7)
5	S(7,14),S(6,12),S(4,12),S(2,12),S(2,11),S(3,9),S(3,8),S(4,7)
6	S(2,14),S(2,13),S(5,11),S(3,10)
7	S(9,18),S(8,16),S(2,16),S(6,15),S(2,15), S(5,12),S(3,12),S(3,11),S(4,10),S(5,9)
8	S(2,18),S(2,17),S(7,15),S(5,15),S(6,13),S(3,13),S(4,11)
9	S(11,22),S(10,20),S(2,20),S(2,19),S(5,16), S(3,15),S(6,14),S(3,14),S(4,13),S(6,11)
10	S(2,22),S(2,21),S(7,18),S(8,17),S(3,16),S(4,14),S(5,13)
11	S(13,26),S(12,24),S(2,24),S(2,23),S(7,21),S(5,20),S(6,18), S(3,18),S(3,17),S(7,16),S(4,16),S(4,15),S(5,14),S(7,13)
12	S(2,26),S(2,25),S(10,21),S(8,20),S(9,19),S(6,19),S(3,19),S(7,17),S(4,17)
13	S(15,30),S(14,28),S(2,28),S(2,27),S(9,24),S(8,21),S(3,21),S(9,20), S(6,20),S(3,20),S(8,18),S(4,18),S(5,17),S(6,16),S(8,15)
14	S(2,30),S(2,29),S(8,24),S(11,23),S(3,22), S(4,20),S(8,19),S(4,19),S(5,18),S(6,17)
15	S(17,34),S(16,32),S(2,32),S(2,31),S(6,24),S(3,24),S(9,23), S(3,23),S(10,22),S(7,22),S(4,21),S(5,19),S(9,17)
16	S(2,34),S(2,33),S(13,27),S(10,27),S(12,25),S(6,25), S(3,25),S(7,23),S(4,22),S(9,21),S(5,21),S(7,19)
17	S(19,38),S(18,36),S(2,36),S(2,35),S(10,30),S(8,28),S(9,27),S(3,27), S(3,26),S(10,25),S(11,24),S(7,24),S(4,24),S(4,23),S(9,22),S(5,22), S(6,21),S(7,20),S(10,19)
18	S(2,38),S(2,37),S(14,29),S(9,28),S(3,28),S(10,26), S(11,25),S(8,25),S(4,25),S(10,23),S(5,23),S(6,22)
19	S(21,42),S(20,40),S(2,40),S(2,39),S(12,33),S(11,30),S(6,30),S(3,30), S(3,29),S(13,28),S(7,28),S(12,26),S(8,26),S(4,26),S(5,25),S(10,24), S(5,24),S(6,23),S(8,22),S(11,21)
20	S(2,42),S(2,41),S(16,33),S(11,33),S(15,31),S(3,31),S(7,29), S(11,28),S(4,28),S(12,27),S(8,27),S(4,27),S(5,26),S(8,23)
21	S(23,46),S(22,44),S(2,44),S(2,43),S(3,33),S(12,32),S(9,32),S(3,32), S(10,31),S(14,30),S(7,30),S(11,29),S(4,29),S(5,27),S(11,26),S(6,26), S(7,25),S(12,23)
22	S(2,46),S(2,45),S(13,36),S(17,35),S(3,34),S(12,30),S(4,30), S(13,29),S(9,29),S(5,28),S(11,27),S(6,27),S(7,26),S(9,25)
23	S(25,50),S(24,48),S(2,48),S(2,47),S(13,39),S(12,36),S(9,36),S(3,36), S(15,35),S(3,35),S(15,32),S(8,32),S(4,32),S(12,31),S(4,31),S(13,30), S(9,30),S(5,30),S(5,29),S(12,28),S(6,28),S(7,27),S(9,26),S(13,25)
24	S(2,50),S(2,49),S(19,39),S(18,37),S(3,37),S(13,35),S(10,35),S(7,35), S(11,34),S(8,33),S(4,33),S(14,31),S(9,31),S(5,31),S(12,29),S(6,29)
25	S(27,54),S(26,52),S(2,52),S(2,51),S(15,42),S(14,39),S(3,39),S(3,38), S(17,36),S(10,36),S(7,36),S(11,35),S(16,34),S(8,34),S(4,34),S(13,33), S(14,32),S(10,32),S(5,32),S(6,31),S(8,29),S(10,28),S(14,27)

Bibliografía

[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] J. Bertin and P. Carbonne, Semi-groupes d'entiers et application aux branches, J. Algebra **49** (1977), 81-95.

[4] A. Brauer, On a problem of partitions, Amer. J. Math. **64** (1942), 299-312.

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

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

[7] J. L. Davison, On the linear Diophantine problem of Frobenius, J. Number Theory **48**(1994), 353-363.

[8] C. Delorme, Sous-monoïdes d'intersection complète de $\mathbb{N}$, Ann. Scient. École Norm. Sup. (4), **9** (1976), 145-154.

[9] M. Djawadi and G. Hofmeister, Linear Diophantine problems, Arch. Math. (Basel) **66** (1996), 19-29.

[10] D. E. Dobbs, G. L. Matthews, On a question of Wilf concerning numerical semigroups, International Journal of Commutative Rings, **3** (2003).

[11] R. Fröberg, G. Gottlieb and R. Häggkvist, On numerical semigroups, Semigroup Forum **35** (1987), 63-83.

[12] R. Fröberg, G. Gottlieb and R. Häggkvist, "Semigroups, semigroups rings and analytically irreducible rings", Reports of the Department of Mathematics, University of Stockholm, Sweden, **1** (1986), ISSN 0348-7652.

[13] P. A. García-Sánchez and J. C. Rosales, Numerical semigroups generated by intervals, Pacific J. Math. **191** (1999), no. 1, 75–83.

[14] R. Gilmer, "Commutative semigroup rings", The University of Chicago Press, 1984.

[15] www.haskell.org

[16] J. Herzog, Generators and relations of abelian semigroups and semigroup rings, Manuscripta Math., **3** (1970), 175-193.

[17] M. Hochster, Rings of invariants of tori, Cohen-Macaulay rings generated by monomials and polytopes, Ann. Math. **96** (1972), 318-337.

[18] S. M. Johnson, A linear Diophantine problem, Can. J. Math. **12** (1960),390-398.

[19] J. Komeda, Non-Weierstrass numerical semigroups, Semigroup Forum, **57** (1998), 157-185.

[20] E. Kunz, The value-semigroup of a one-dimensional Gorenstein ring, Proc. Amer. Math. Soc., **25** (1973), 748-751.

[21] C.D. Olds, A. Lax y G. Davidoff, The geometry of numbers, The Mathematical Association of America, ISBN 0-88385-643-3

[22] H. Pinkham, Deformations of algebraic varieties with G_m action, Asterisque, **20**, (1974).

[23] J. L. Ramírez Alfonsín, The Diophantine Frobenius problem, Forschungsintitut für Diskrete Mathematik, Bonn, Report No.00893 (2000).
[24] J. L. Ramírez Alfonsín, The Diophantine Frobenius problem, manuscrito.
[25] J.C. Rosales, Adding or removing an element from a pseudo-symmetric numerical semigroup, trabajo enviado para su revisión.
[26] J.C. Rosales, An algorithm to solve proportionally modular diophantine inequations, trabajo en preparación.
[27] J.C. Rosales, Fundamental gaps of numerical semigroups generated by two elements, aparecerá en Linear Algebra Appl.
[28] J.C. Rosales, Modular Diophantine inequalities and some of their invariants, aparecerá en Indian J. Pure Appl. Math.
[29] J.C. Rosales, Numerical semigroups that differ from a symmetric numerical semigroup in one element, aparecerá en Algebra Colloquium.
[30] J.C. Rosales, On numerical semigroups, Semigroup Forum, **52** (1996), 307-318.
[31] J.C. Rosales, Pseudo-symmetric modular Diophantine inequalities, trabajo en preparación.
[32] J.C. Rosales, Symmetric modular Diophantine inequalities, trabajo enviado para su revisión.
[33] J. C. Rosales and M. B. Branco, Decomposition of a numerical semigroup as an intersection of irreducible numerical semigroups, B. Belg. Math. Soc-Sim. **9** (2002), 372-381.
[34] J. C. Rosales and M. B. Branco, Numerical semigroups that can be expressed as an intersection of symmetric numerical semigroups, J. Pure Appl. Algebra, **171** (2002), 303-314..
[35] J. C. Rosales and M. B. Branco, Irreducible numerical semigroups, Pacific J. Math. **209** (2003), 131-143.
[36] J. C. Rosales and P. A. García-Sánchez, "Finitely generated commutative monoids," Nova Science Publishers, New York, 1999.
[37] J. C. Rosales, P. A. García-Sánchez and J. I. García-García, Every positive integer is the Frobenius number of a numerical semigroup with three generators, Math. Scandinavica, **94** (2004), 5-12.
[38] J.C. Rosales, P.A. García-Sánchez, J.I. García-García and J.A. Jiménez-Madrid, Fundamental gaps in numerical semigroups, J. Pure Appl. Alg., **189** (2004), 301-313
[39] J.C. Rosales, P.A. García-Sánchez, J.I. García-García and J.A. Jiménez-Madrid, The oversemigroups of a numerical semigroup, Semigroup Forum **67** (2003) 145-158.
[40] 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.
[41] J. C. Rosales, P. A. García-Sánchez and J. M. Urbano-Blanco, Modular Diophantine inequalities and numerical semigroups, aparecerá en Pacific J. Math. **218** (2005).
[42] J. C. Rosales, P. A. García-Sánchez and J. M. Urbano-Blanco, The set of solutions of a proportionally modular Diophantine inequality, trabajo enviado para su revisión.
[43] J.C. Rosales and J. M. Urbano-Blanco, Irreducible proportionally modular Diophantine inequations, trabajo en preparación.
[44] J. C. Rosales, and J. M. Urbano-Blanco, Equivalent modular Diophantine inequalities, trabajo en preparación.
[45] J. C. Rosales, and J. M. Urbano-Blanco, Proportionally modular Diophantine inequalities and full semigroups, trabajo enviado para su revisión.
[46] E. S. Selmer, On a linear Diophantine problem of Frobenius, J. Reine Angew. Math. **293/294** (1977), 1-17.
[47] J. J. Sylvester, Excursus on rational fractions and partitions, Amer. J. Math. **5** (1882), 119-136.
[48] J. J. Sylvester, Mathematical questions with their solutions, Educational Times **41** (1884), 21.
[49] B. Teissier, Appendice à "Le probléme des modules pour le branches planes", cours donné par O. Zariski au Centre de Math. de L'École Polytechnique, Paris (1973).

[50] K. Watanabe, Some examples of one dimensional Gorenstein domains, Nagoya Math. J. **49** (1973), 101-109.
[51] A. Wiles, Modular elliptic curves and Fermat's Last Theorem, Ann. Math. **141** (1995), 443-551.
[52] A. Wiles, R. Taylor, Ring-theoretic properties of certain Hecke algebras, Ann. Math. **141** (1995), 553-572.
[53] H. S. Wilf, A circle-of-lights algorithm for the "money-changing problem", Amer. Math Monthly **85** (1978), 562-565.

Índice de definiciones