EL PROBLEMA DE FROBENIUS EN EL CASO $n = 2$ Y ALGUNOS MÉTODOS PARA EL CASO $n = 3$

YERLY VANESA SOLER PORRAS

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA

2015

EL PROBLEMA DE FROBENIUS EN EL CASO $n = 2$ Y ALGUNOS MÉTODOS PARA EL CASO $n = 3$

Autora

YERLY VANESA SOLER PORRAS

Trabajo de grado como requisito parcial para optar al título de

Matemática

Director

CARLOS ARTURO RODRÍGUEZ PALMA

Magíster en Matemáticas

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA

2015

NOTA DE PROYECTO DE GRADO

NOMBRE DEL ESTUDIANTE: YERLY VANESA SOLER PORRAS.	**2110162**

TITULO DEL PROYECTO : "EL PROBLEMA DE FROBENIUS EN EL CASO n=2 Y ALGUNOS MÉTODOS PARA EL CASO n=3"

	FACULTAD : ***Ciencias***	CARRERA: ***MATEMÁTICAS***

NOTA DEFINITIVA: **CUATRO, SEIS (4.6)** CREDITOS: *10*

DIRECTOR DEL PROYECTO: **CARLOS ARTURO RODRIGUEZ PALMA**

FIRMA

Carlos A. Rodriguez

CALIFICADORES

F **CLAUDIA INÉS GRANADOS**	F **RAFAEL FERNANDO ISAACS GIRALDO**	FECHA A *15* M *11* D *6*

ENTREGA DE TRABAJOS DE GRADO, TRABAJOS DE INVESTIGACIÓN O TESIS Y AUTORIZACIÓN DE SU USO A FAVOR DE LA UIS

Yo, **YERLY VANESA SOLER PORRAS**, mayor de edad, vecino de Bucaramanga, identificado con la Cédula de Ciudadanía **No 1.098.754.184** de Bucaramanga, actuando en nombre propio, en mi calidad de autor del trabajo de grado, del trabajo de investigación, o de la tesis denominada(o): **EL PROBLEMA DE FROBENIUS EN EL CASO** $n = 2$ **Y ALGUNOS MÉTODOS PARA EL CASO** $n = 3$, hago entrega del ejemplar respectivo y de sus anexos de ser el caso, en formato digital o electrónico (CD o DVD) y autorizo a **LA UNIVERSIDAD INDUSTRIAL DE SANTANDER,** para que en los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia, utilice y use en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador de la obra objeto del presente documento.

PARÁGRAFO: La presente autorización se hace extensiva no sólo a las facultades y derechos de uso sobre la obra en formato o soporte material, sino también para formato virtual, electrónico, digital, óptico, uso en red, Internet, extranet, intranet, etc., y en general para cualquier formato conocido o por conocer.

EL AUTOR / ESTUDIANTE, manifiesta que la obra objeto de la presente autorización es original y la realizó sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de su exclusiva autoría y detenta la titularidad sobre la misma. PARÁGRAFO: En caso de presentarse cualquier reclamación o acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión, EL AUTOR / ESTUDIANTE, asumirá toda la responsabilidad, y saldrá en defensa de los derechos aquí autorizados; para todos los efectos la Universidad actúa como un tercero de buena fe. Para constancia se firma el presente documento en dos (02) ejemplares del mismo valor y tenor, en Bucaramanga, a los 19 días del mes de Noviembre de Dos Mil quince (2015).

EL AUTOR / ESTUDIANTE:

Yerly Vanesa Soler

Yerly Vanesa Soler Porras.
CC 1.098.754.184

Agradecimientos

Agradezco al ser único, omnipresente, omnisciente y supremo en el que creo, por darme la oportunidad de vivir, gozar de buena salud y regalarme el don de la inteligencia.

Me siento inmensamente agradecida con todos los profesores que a lo largo de la carrera me aportaron sus conocimientos, tiempo y dedicación, especialmente a mi director de tesis Carlos Arturo Rodríguez por su compromiso, sugerencias y correcciones. A mis familiares y amigos quienes han influido directa e indirectamente a lo largo de este camino.

Con mucho cariño, quiero agradecer y dedicar este trabajo a mis padres, Luz Marina y Omar, por el apoyo emocional, económico y espiritual brindado durante este proceso de formación, sin ellos no hubiese logrado llegar hasta aquí.

Índice general

Resumen

TÍTULO: EL PROBLEMA DE FROBENIUS EN EL CASO $n = 2$ Y ALGUNOS MÉTODOS EN EL CASO $n = 3$[1]

AUTORA: Yerly Vanesa Soler Porras[2]

PALABRAS CLAVE: El problema de Frobenius; El problema diofántico de Frobenius; Ecuaciones diofánticas.

RESUMEN

Un problema asociado a la Teoría de Números y especialmente a las ecuaciones diofánticas, es el problema de Frobenius, el cual consiste en tomar una cantidad finita de números enteros positivos que sean primos relativos, y encontrar el mayor entero positivo que no puede expresarse como combinación lineal (con coeficientes enteros no negativos) de dichos números; el número que se desea encontrar recibe el nombre de número de Frobenius.

Este trabajo se caracteriza por estudiar el problema de Frobenius en el caso $n = 2$ y algunos métodos en el caso $n = 3$. En el primer capítulo se recordarán algunos conceptos y resultados clásicos sobre divisibilidad, congruencias y fracciones continuas en los enteros, pues son necesarios para el desarrollo del siguiente capítulo.

En el segundo capítulo se prueba la existencia del número de Frobenius en el caso general, se da una fórmula explícita para hallar el número de Frobenius y otros resultado asociados al problema en el caso $n = 2$. Se demuestran algunos resultados importantes en el caso general, pues se usarán después, para calcular el número de Frobenius en el caso $n = 3$ por medio de los métodos de Hofmeister, Selmer y Beyer, y Rödseth.

[1]Tesis.

[2]Facultad de Ciencias, Escuela de Matemáticas.
DIRECTOR: Mg. Carlos Arturo Rodriguez Palma.

Abstract

TITLE: THE FROBENIUS PROBLEM IN CASE $n = 2$ AND SOME METHODS IN CASE $n = 3$ [3]

AUTHOR: Yerly Vanesa Soler Porras[4]

KEYWORDS: The problem of Frobenius; The diophantine Frobenius Problem; Diophantine equations.

ABSTRACT

A problem related with the Number Theory and particularly diophantine equations, is the problem of Frobenius, which involves taking a finite number of relatively prime positive integers, and determining the largest positive integer that cannot be expressed as a linear combination of these numbers (with non-negative integer coefficients); this number is called the Frobenius number.

In this dissertation is going to be studied the problem of Frobenius in case $n = 2$ and some methods in case $n = 3$. In the first chapter some classic concepts and results on divisibility, congruences and continued fractions of integers, since it is necessary for the development of the in the next chapter, are taken up.

In the second chapter is going to be proved the existence in general case of the Frobenius number, an explicit formula is given to find the number of Frobenius and other results to solve the problem for $n = 2$. Some important results are shown in the general case, that will be used later, to calculate the Frobenius number in the case $n = 3$ by the Hofmeister´s method, Selmer and Beyer´s method, and Rødseth´s method.

[3] Thesis.

[4]Faculty of Science, School of Mathematics.
DIRECTED BY: Mg. Carlos Arturo Rodriguez Palma.

Introducción

El problema de Frobenius es simple en su enunciado pero complejo en su solución. Consiste en tomar una cantidad finita de números enteros positivos que sean primos relativos y encontrar el mayor entero positivo que no puede expresarse como combinación lineal (con coeficientes enteros no negativos) de dichos números; el número que se desea encontrar recibe el nombre de número de Frobenius. Aunque el problema nunca se propuso explícitamente por escrito en algún manuscrito, se le atribuye a Ferdinand Georg Frobenius un matemático alemán nacido en 1849, quien cursó sus estudios superiores en la Universidad de Humboldt Berlín, su tesis sobre la solución de las ecuaciones diferenciales fue dirigida por Karl Theodor Weierstrass.

Por ejemplo, dados los enteros positivos 3 y 8, rápidamente podemos verificar que los números 1, 2, 4, 5, 7, 10 y 13 no pueden ser expresados como combinación lineal con coeficientes enteros no negativos de dichos números. Adicionalmente podemos mostrar que todo número mayor que 13 puede expresarse como combinación lineal con coeficientes enteros no negativos de 3 y 8.

El problema de la moneda está estrechamente relacionado con el problema de Frobenius, pues consiste en hallar la mayor cantidad monetaria que no se puede obtener utilizando sólo monedas de determinadas denominaciones enteras; por ejemplo no se puede obtener 13 dólares solo con billetes de 2 y 5 dólares. Otro problema asociado al problema de Frobenius es el siguiente, la cadena mundial de comida rápida McDonald vende McNuggets de pollo en

cajas de 6, 9 y 20, se podrían comprar exactamente 27 McNuggets pero no exactamente 25 McNuggets.

En general para calcular el número de Frobenius no se conoce una fórmula explícita, computacionalmente tampoco se ha desarrollado un algoritmo eficiente en tiempo polinomial que lo calcule, por ello el problema de Frobenius en el caso general aún no ha sido resuelto. Pero se ha trabajado en algunos casos particulares, como el caso $n = 2$ y $n = 3$, los cuales estudiaremos a lo largo del texto.

El caso más simple del problema de Frobenius de dos entero positivos primos relativos se encuentra totalmente resuelto, del cual daremos algunos resultados importantes. Pero el problema se complica cuando aumenta el número de enteros, en este caso estudiaremos tres métodos el de Hofmeister, Selmer y Beyer y por último el de Rödseth. Hofmeister en 1966 publicó un artículo, donde resuelve el caso para tres enteros positivos primos relativos dos a dos e independientes, que están condicionados por una desigualdad. Selmer y Beyer en 1978 extienden el resultado de Hofmeister cuando la desigualdad no se satisface, usando fracciones continuas. Rödseth asistió al décimo séptimo congreso Escandinavo de matemáticas y se interesó por el método que presentó Selmer, él modificó dicho método implementando fracciones continuas usando residuos negativos. Al final del texto podemos encontrar algoritmos implementados en el software MuPAD de los tres métodos (Hofmeister, Selmey y Beyer, Rödseth).

Es importante mencionar que las demostraciones a los resultados que presentaremos, son consecuencia un desarrollo mas detallado y del estudio minucioso de los diferentes artículos que se encuentran en la bibliografía. Cabe resaltar que para las pruebas de dichos resultados utilizaremos herramientas propias de Teoría de Números, Combinatoria, Geometría entre otras, estas no son las únicas áreas que se han interesado en estudiar el problema, existen otras como álgebra (bases de Gröbner y semigrupos numéricos) y variable compleja.

Capítulo 1

Preliminares

En este primer capítulo enunciaremos una serie de resultados a cerca de divisibilidad en los números enteros, ecuaciones diofánticas, congruencias y fracciones continuas que son típicos temas en un curso de teoría de números; que se usan a lo largo del texto, las demostraciones de dichos resultados se podrán encontrar en [5] y [3], y una demostración del teorema de Pick se puede ver en [7].

1.1. Divisibilidad

Teorema 1.1 (Algoritmo de la división)**.** *Sean a y b enteros con $b > 0$, existen enteros únicos q y r tales que*

$$a = bq + r;\ con\ \ 0 \leq r < b.$$

Los enteros q y r se llaman cociente y residuo, respectivamente, en la división de a por b.

Definición 1.1. Sean a y b enteros con $a \neq 0$, se dice que el entero b es divisible por a, si existe un entero c tal que

$$b = ac.$$

Si esto ocurre se dice que a divide a b, y se denota $a \mid b$, si esto no ocurre se dice que a no divide a b y se escribe $a \nmid b$.

Teorema 1.2. *Sean a, b, c y d enteros, entonces*

I. $a \mid 0$, $1 \mid a$ *y* $a \mid a$.

II. $a \mid 1$ *si y solo si* $a = \pm 1$.

III. *Si* $a \mid b$ *entonces* $a \mid (-b)$.

IV. *Si* $a \mid b$ *y* $c \mid d$ *entonces* $ac \mid bd$.

V. *Si* $a \mid b$ *y* $b \mid c$ *entonces* $a \mid c$.

Si existe un entero d tal que $d \mid a$ y $d \mid b$ entonces se dice que d es un divisor común de a y b.

Definición 1.2. Sean a y b enteros (con al menos uno de ellos distinto de cero). El conjunto de todos los divisores comunes de a y b es un conjunto finito de números enteros cuyo máximo se denomina máximo común divisor de a y b, y se denota $\gcd(a, b)$. Es decir si $d = \gcd(a, b)$ entonces:

I. $d \mid a$ y $d \mid b$.

II. Si existe un entero c tal que $c \mid a$ y $c \mid b$ entonces $c \mid d$.

III. si $d \mid a$ entonces $d \mid (-a)$, es fácil observar que

$$\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b).$$

Teorema 1.3. *Sean a y b enteros (con al menos uno distinto de cero) entonces* $\gcd(a, b)$ *es el menor entero positivo que es combinación lineal de a y b.*

Lema 1.4. *Sean a y b enteros, si $a = bq + r$, con q y r enteros únicos, entonces* $\gcd(a, b) = \gcd(b, r)$.

Algoritmo de Euclides

Este es un procedimiento eficiente que nos permite encontrar el máximo común divisor de dos enteros dados a y b.

Si $0 < b < a$, aplicamos el algoritmo de la división y escribimos

$$a = bq_1 + r_1, \qquad 0 \leq r_1 < b.$$

Si $r_1 = 0$ entonces $b \mid a$ y $\gcd(a, b) = b$. Si no, aplicamos de nuevo el algoritmo de la división para obtener

$$b = r_1 q_2 + r_2, \qquad 0 \leq r_2 < r_1.$$

Si $r_2 = 0$ entonces $r_1 = \gcd(r_1, b) = \gcd(a, b)$. Si no, repetimos el proceso, hasta llegar a lo sumo en b pasos a un residuo cero; obteniendo las siguientes ecuaciones:

$$\begin{aligned}
a &= bq_1 + r_1, & 0 \leq r_1 < b;\\
b &= r_1 q_2 + r_2, & 0 \leq r_2 < r_1;\\
r_1 &= r_2 q_3 + r_3, & 0 \leq r_3 < r_2;\\
&\vdots & \vdots\\
r_{k-3} &= r_{k-2} q_{k-1} + r_{k-1}, & 0 \leq r_{k-1} < r_{k-2};\\
r_{k-2} &= r_{k-1} q_k + r_k, & 0 \leq r_k < r_{k-1};\\
r_{k-1} &= r_k q_{k+1} + 0.
\end{aligned}$$

La aplicación repetida del Lema 1.4 nos permite afirmar que

$$\gcd(a, b) = \gcd(b, r_1) = \cdots = \gcd(r_{k-1}, r_k) = r_k.$$

Puesto que $\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b)$ el algoritmo anterior nos permite encontrar el máximo común divisor de cualquier par de enteros.

Teorema 1.5. *Sean a y b enteros (con al menos uno distinto de cero). Entonces,* $\gcd(a, b) = 1$ *si y solo si existen enteros* x, y *tales que*

$$1 = ax + by.$$

Corolario 1.6. *Sean a y b enteros con $d = \gcd(a, b)$ entonces*

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

Definición 1.3. Dos enteros a y b (con al menos uno distinto de cero) se llaman primos relativos si $\gcd(a, b) = 1$. Más general, si $a_1, a_2, \ldots, a_n$ son enteros tales que para todo i y para todo j con $i \neq j$, $1 \leq i, j \leq n$ se tiene $\gcd(a_i, a_j) = 1$, decimos que $a_1, a_2, \ldots, a_n$ son primos relativos dos a dos.

Teorema 1.7. *Sean a, b y c enteros tales que a y b son primos relativos, si $a \mid c$ y $b \mid c$ entonces $ab \mid c$.*

Lema 1.8 (Lema de Euclides)**.** *Sean a, b y c enteros tales que a y b son primos relativos, si $a \mid bc$ entonces $a \mid c$.*

1.2. Ecuaciones diofánticas

Definición 1.4. Una ecuación de la forma $p(x_1, x_2, ..., x_n) = 0$ donde $p(x_1, x_2, ..., x_n)$ es un polinomio con coeficientes enteros y con las variables restringidas a tomar únicamente valores enteros, se denomina una ecuación diofántica (en honor al matemático griego Diofanto de Alejandría).

El tipo más simple de dichas ecuaciones, son las ecuaciones diofánticas lineales en dos variables de la forma

$$ax + by = c. \tag{1.1}$$

donde a, b y c son enteros y x, y son variables que solo pueden tomar valores enteros. Las soluciones de (1.1) serán las parejas (x_0, y_0) que satisfacen la ecuación, es decir, al reemplazar $x = x_0, y = y_0$ en (1.1) se cumpla la igualdad.

Ejemplo 1.1.

1. La ecuación diofántica lineal $3x + 6y = 18$ tiene como solución la pareja $(0, 3)$ pues

$$\begin{aligned} 3(0) + 16(3) &= 18 \\ 0 + 18 &= 18 \\ 18 &= 18. \end{aligned}$$

2. La ecuación diofántica lineal $2x+10y = 15$ no tiene solución, pues sin importar los valores que tomen x, y el lado izquierdo de la ecuación será siempre par, mientras que el derecho es impar.

El siguiente teorema establece una condición suficiente y necesaria para que una ecuación de la forma (1.1) tenga solución.

Teorema 1.9. *La ecuación diofántica* $ax + by = c$ *tiene solución si y solo si* $\gcd(a, b) \mid c$.

Teorema 1.10. *Sea* $ax + by = c$ *una ecuación diofántica lineal si* $\gcd(a, b) = d \mid c$ *y* (x_0, y_0) *es una solución de la ecuación, entonces todas las soluciones están dadas por*

$$\begin{cases} x &= x_0 + \left(\dfrac{b}{d}\right)t \\ y &= y_0 - \left(\dfrac{a}{d}\right)t \end{cases}$$

con t en los enteros.

Corolario 1.11. *Sean a y b enteros con* $\gcd(a, b) = 1$*, si* (x_0, y_0) *es una solución a la ecuación diofántica* $ax + by = c$*, entonces todas las soluciones están dadas por*

$$\begin{cases} x &= x_0 + bt \\ y &= y_0 - at \end{cases}$$

con t en los enteros.

Ejemplo 1.2. Sea $2x + 5y = 11$ una ecuación diofántica lineal, como $\gcd(2, 5) = 1 \mid 11$ entonces la ecuación tiene solución. De hecho $(-22, 11)$ es una solución, por lo tanto todas las soluciones son de la forma:

$$\begin{cases} x &= -22 + 5t \\ y &= 11 - 2t \end{cases}$$

con t en los enteros.

1.3. Congruencias

Definición 1.5. Sean a y b enteros cualesquiera, n un entero positivo fijo. Si $n \mid (a - b)$ decimos que a y b son congruentes módulo n, lo cual se denota

$$a \equiv b \pmod{n}.$$

Si a no es congruente con b módulo n, se escribe

$$a \not\equiv b \pmod{n}.$$

Definición 1.6. Se dice que un conjunto de n enteros $\{a_1, a_2, \ldots, a_n\}$ es un sistema completo de residuos módulo n, si todo entero es congruente módulo n a exactamente uno de los a_i.

Teorema 1.12. *Sean a y b enteros cualesquiera, n un entero positivo fijo. Entonces $a \equiv b \pmod{n}$ si y solo si a y b dejan el mismo residuo al dividirse por n.*

Teorema 1.13. *Sean a, b, c y d enteros cualesquiera, n un entero fijo tal que $n \geq 1$. Entonces se tienen las siguientes propiedades*

I. $a \equiv a \pmod{n}$.

II. *Si* $a \equiv b \pmod{n}$ *entonces* $b \equiv a \pmod{n}$.

III. *Si* $a \equiv b \pmod{n}$ *y* $b \equiv c \pmod{n}$ *entonces* $a \equiv c \pmod{n}$.

IV. *Si* $a \equiv b \pmod{n}$ *y* $c \equiv d \pmod{n}$ *entonces* $a \pm c \equiv b \pm d \pmod{n}$ *y* $ac \equiv bd \pmod{n}$.

V. *Si* $a \equiv b \pmod{n}$ *entonces* $a + c \equiv b + c \pmod{n}$ *y* $ac \equiv bc \pmod{n}$ *para todo entero* c.

VI. *Si* $a \equiv b \pmod{n}$ *entonces* $a^k \equiv b^k \pmod{n}$ *para todo entero* k.

En particular las tres primeras propiedades indican que la congruencia módulo n es una relación de equivalencia.

Teorema 1.14. *Sean* a, b *y* c *enteros cualesquiera,* n *un entero fijo con* $c \neq 0$ *y* $d = \gcd(c, n)$, *si* $ca \equiv cb \pmod{n}$ *entonces* $a \equiv b \left(\mod \frac{n}{d}\right)$.

Corolario 1.15. *Sean* a, b *y* c *enteros cualesquiera,* n *un entero fijo con* $c \neq 0$ *y* $1 = \gcd(c, n)$, *si* $ca \equiv cb \pmod{n}$ *entonces* $a \equiv b \pmod{n}$.

Corolario 1.16. *Sean* a *y* b *enteros cualesquiera,* p *un número primo, si* $ca \equiv cb \pmod{p}$ *y* $p \nmid c$ *entonces* $a \equiv b \pmod{p}$.

1.3.1. Congruencias lineales

Definición 1.7. Sean a y b enteros cualesquiera, $n \geq 1$ un entero fijo. Una expresión de la forma

$$ax \equiv b \pmod{n} \tag{1.2}$$

se denomina congruencia lineal.

Una solución de (1.2) es un entero x_0 que satisface la congruencia $ax_0 \equiv b \pmod{n}$, además cuando hablamos de las soluciones de la congruencia (1.2) consideramos los enteros que la satisfacen pero que son incongruentes entre sí módulo n.

Teorema 1.17. *La congruencia lineal* $ax \equiv b \pmod{n}$ *tiene solución si y solo si* $d \mid b$ *donde* $d = \gcd(a, n)$. *Además si tiene solución, hay* d *soluciones incongruentes (entre ellas) módulo* n.

Corolario 1.18. *La congruencia lineal* $ax \equiv b \pmod{n}$ *tiene solución única si y solo si* $\gcd(a, n) = 1$.

Teorema 1.19 (Teorema chino del residuo)**.** *Sean $n_1, n_2, ..., n_r$ enteros positivos primos relativos dos a dos, y sean $a_1, a_2, ..., a_r$ enteros arbitrarios. Entonces el sistema de congruencias lineales*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}; \\ x &\equiv a_2 \pmod{n_2}; \\ &\vdots \\ x &\equiv a_r \pmod{n_r}; \end{aligned}$$

tiene solución única módulo $n = \prod_{i=1}^{r} n_i$.

1.4. Fracciones continuas finitas

Una fracción continua es una expresión de la forma

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}} \tag{1.3}$$

de donde $a_0, a_1, \ldots, a_n$ son enteros. Cuando no hay ambigüedad, simplemente la llamaremos fracción continua, usualmente son utilizadas para aproximar un número real por un racional. Existen tipos de fracciones continuas en donde los numeradores no son todos 1´s, pero no consideramos este caso. Generalmente se escribe en una de las dos formas:

$$a_0 + \frac{1}{a_1+}\frac{1}{a_2+}\cdots\frac{1}{a_n}$$

o

$$[a_0, a_1, \ldots, a_n].$$

para denotar (1.3). Los enteros $a_0, a_1, \ldots, a_n$ reciben el nombre de cocientes parciales, o simplemente cocientes, de la fracción continua.

Haciendo cálculos simples encontramos que

$$\begin{aligned} [a_0] &= \frac{a_0}{1}, \\ [a_0, a_1] &= \frac{a_1 a_0 + 1}{a_1}, \\ [a_0, a_1, a_2] &= \frac{a_2 a_1 a_0 + a_2 + a_0}{a_2 a_1 + 1}; \end{aligned}$$

y es evidente que

$$[a_0, a_1] = a_0 + \frac{1}{a_1}, \tag{1.4}$$

$$[a_0, a_1, \ldots, a_m] = \left[a_0, a_1, \ldots, a_{m-2}, a_{m-1} + \frac{1}{a_m}\right], \tag{1.5}$$

$$[a_0, a_1, \ldots, a_m] = a_0 + \frac{1}{[a_0, a_1, \ldots, a_m]} = [a_0, [a_0, a_1, \ldots, a_m]], \tag{1.6}$$

para $1 \leq m \leq n$. Podríamos definir nuestra fracción continua por (1.4), (1.5) o (1.6). Más generalmente

$$[a_0, a_1, \ldots, a_m] = [a_0, a_1, \ldots, a_{l-1}, [a_l, a_{l+1}, \ldots, a_m]], \tag{1.7}$$

para $1 \leq l < m \leq n$.

1.4.1. Convergentes de una fracción continua finita

Llamamos

$$[a_0, a_1, \ldots, a_m] \ (0 \leq m \leq n)$$

el m-ésimo convergente de $[a_0, a_1, \ldots, a_n]$. Es fácil calcular los convergentes por medio del siguiente teorema.

Teorema 1.20. *Si p_m y q_m se definen por*

$$p_0 = a_0, \quad p_1 = a_1 a_0 + 1, \quad p_m = a_m p_{m-1} + p_{m-2}, \qquad (2 \leq m \leq n),$$
$$q_0 = 1, \quad q_1 = a_1, \quad q_m = a_m q_{m-1} + q_{m-2}, \qquad (2 \leq m \leq n),$$

entonces

$$[a_0, a_1, \ldots, a_m] = \frac{p_m}{q_m}.$$

El siguiente teorema enuncia algunas propiedades que tienen p_m y q_m

Teorema 1.21. *Considere las funciones p_m y q_m definidas en el Teorema 1.20, entonces se tienen las siguientes propiedades*

I. $p_m q_{m-1} - p_{m-1} q_m = (-1)^{m-1}$.

II. $p_m q_{m-2} - p_{m-2} q_m = (-1)^m a_m$.

III. $\dfrac{p_m}{q_m} - \dfrac{p_{m-1}}{q_{m-1}} = \dfrac{(-1)^{m-1}}{q_{m-1} q_m}$.

IV. $\dfrac{p_m}{q_m} - \dfrac{p_{m-2}}{q_{m-2}} = \dfrac{(-1)^m a_m}{q_{m-2} q_m}$.

1.5. Teorema de Pick

El Teorema de Pick fue demostrado por Georg Alexander Pick quien nació en Viena, Austria. Su trabajo matemático fue extremadamente amplio, alrededor de 67 documentos de muchos temas, parte de su popularidad se debe al teorema que lleva su nombre, el cual apareció en el año de 1899, en un artículo llamado *Geometrisches zur Zahlenlehre* publicado en Praga. Este teorema no recibió mucha atención tras su publicación, hasta el año 1969 cuando Steinhaus lo incluyó en su famosos libro *Mathematical Snapshots*. Fue así como atrajo la atención y admiración por su simplicidad y elegancia.

Definición 1.8.

- Un punto p de coordenadas (x, y) se llama entero, si x, y son números enteros.
- Un polígono es simple si los vértices no coinciden unos con otros, ninguno de los vértices cae en uno de los lados del polígono y dos lados cualesquiera no se cortan.
- Una red poligonal P, es un polígono simple, cuyos vértices son puntos enteros.

Teorema 1.22 (Teorema de Pick)**.** *El área* $A(P)$ *de toda red poligonal* P *es*

$$A(P) = I(P) + \frac{B(P)}{2} - 1$$

donde $I(P)$ *representa el número de puntos enteros interiores y* $B(P)$ *representa el número de puntos enteros sobre la frontera del polígono* P*.*

Capítulo 2

El Problema de Frobenius

En aras de estudiar el número de Frobenius en el caso $n = 2$ y $n = 3$ definimos algunos conceptos relacionados con el número de Frobenius. Primero analizamos el caso $n = 2$, donde encontramos fórmulas explícitas para el número de Frobenius, el número de enteros positivos que no son representables y la suma de ellos. Después probaremos algunos resultados en el caso general, pues serán herramientas muy útiles para el desarrollo de los tres métodos en el caso $n = 3$. Al final del capítulo mostramos los tres métodos que nos proporcionan una fórmula para el número de Frobenius y una para el número de enteros positivos que no son representables. Las demostraciones de los resultados que presentaremos, fueron obtenidas de los diferentes artículos que mencionamos en la bibliografía.

Definición 2.1. Dados $a_1, a_2, \ldots, a_n$ enteros positivos primos relativos, se dice que el entero positivo m es representable por $a_1, a_2, \ldots, a_n$, si existen enteros no negativos $x_1, x_2, \ldots, x_n$ tales que:

$$\sum_{i=1}^{n} a_i x_i \quad = \quad m.$$

De la definición anterior, afirmar que m es representable por $a_1, a_2, \ldots, a_n$ equivale a decir que m es combinación lineal de $a_1, a_2, \ldots, a_n$ con coeficientes enteros no negativos.

Ejemplo 2.1. Algunos enteros positivos representables por 9 y 7 son:

$$\begin{aligned} 9 \cdot 1 + 7 \cdot 1 &= 16, \\ 9 \cdot 2 + 7 \cdot 3 &= 39, \\ 9 \cdot 3 + 7 \cdot 2 &= 41, \\ 9 \cdot 0 + 7 \cdot 7 &= 49. \end{aligned}$$

Además, se puede comprobar que los únicos enteros positivos que no son representables por 9 y 7 son: 1, 2, 3, 4, 5, 6, 8, 10, 11, 12, 13, 15, 17, 19, 20, 22, 24, 26, 29, 31, 33, 38, 40 y 47, es decir todo número mayor que 47 es representable por 9 y 7, esto es consecuencia del siguiente resultado.

Teorema 2.1. *Dados $a_1, a_2, \ldots, a_n$ enteros positivos primos relativos, existe un entero positivo K, tal que todo entero positivo m mayor que K es representable por $a_1, a_2, \ldots, a_n$.*

Demostración. Aplicamos el principio de inducción matemática sobre n.

Paso inicial $n = 2$.

Para $n = 2$ tenemos el siguiente resultado $g(a_1, a_2) = a_1a_2 - a_1 - a_2$ (ver Teorema 2.2), el cual nos garantiza que todo número mayor que $g(a_1, a_2)$ es representable por a_1 y a_2.

Paso inductivo Para $n \geq 3$, supongamos que el resultado es cierto si tenemos $n - 1$ enteros primos relativos. Dados $a_1, a_2, \ldots, a_n$ enteros positivos primos relativos, tenemos dos posibilidades:

La primera de ellas es que $a_1, a_2, \ldots, a_{n-1}$ sean primos relativos, en este caso por la hipótesis de inducción existe un entero positivo K tal que todo entero m mayor que K es representable por $a_1, a_2, \ldots, a_{n-1}$, es decir, existen enteros no negativos $x_1, x_2, \ldots, x_{n-1}$ tales que

$$m = a_1x_1 + a_2x_2 + \cdots + a_{n-1}x_{n-1},$$

de igual forma m también puede expresarse como

$$m = a_1x_1 + a_2x_2 + \cdots + a_{n-1}x_{n-1} + a_nx_n,$$

con $x_n = 0$, de ahí que todo entero suficientemente grande m puede ser representable por $a_1, a_2, \ldots, a_{n-1}, a_n$.

La segunda posibilidad es que $\gcd(a_1, a_2, \ldots, a_{n-1}) = d > 1$. Sea $a_i = a_i' d$ para cada $i = 1, \ldots, n-1$, de ahí que $\gcd(a_1', a_2', \ldots, a_{n-1}') = 1$, entonces $\gcd(d, a_n) = 1$ y sea

$$\sum_{i=1}^{n} a_i x_i = m, \tag{2.1}$$

la ecuación anterior se convierte en

$$\sum_{i=1}^{n-1} a_i' x_i = \frac{m - a_n b_n}{d}, \tag{2.2}$$

donde b_n, con $0 \leq b_n \leq d-1$ es el único entero tal que $a_n b_n \equiv m \pmod{d}$. Por hipótesis de inducción, existe un entero K_0 tal que (2.2) tiene solución con enteros no negativos $x_i = b_i$ para $1 \leq i \leq n-1$, de donde

$$\frac{m - a_n b_n}{d} \geq \frac{m - a_n(d-1)}{d} > K_0,$$

de ahí que

$$m > a_n(d-1) + dK_0.$$

Así (2.1) tiene solución con enteros no negativos $x_i = b_i$ para $1 \leq i \leq n$, es decir, m es representable por $a_1, a_2, \ldots, a_n$, de la desigualdad anterior es claro que existe un entero K tal que

$$m > a_n(d-1) + dK_0 \geq K. \qquad \square$$

Este teorema garantiza la existencia del número de Frobenius que definimos a continuación.

Definición 2.2. Dados $a_1, a_2, \ldots, a_n$ enteros positivos primos relativos, el número de Frobenius, el cual se denota como $g(a_1, a_2, \ldots, a_n)$, es el mayor entero que no es representable por $a_1, a_2, \ldots, a_n$.

Ejemplo 2.2. Dados 33 y 5, se puede garantizar que todo número mayor que 127 puede ser

representable por 33 y 91, lo cual indica que el número de Frobenius es 127.

Note que dados $a_1, a_2, \ldots, a_n$ enteros positivos primos relativos, si m es un entero positivo y alguno de los a_i es 1, digamos $a_1 = 1$, entonces

$$m = 1 \cdot m + a_2 \cdot 0 + \cdots + a_n \cdot 0,$$

lo cual significa que m es representable por $a_1, a_2, \ldots, a_n$, en tal caso $g(a_1, a_2, \ldots, a_n)$ no existe.

Si a es un entero positivo, los únicos enteros positivos representables por a son sus múltiplos, de ahí que existen infinitos números que no pueden ser representables por a, lo cual implica que el número de Frobenius en el caso $n = 1$ no existe.

Dados dos enteros positivos p y q representables por $a_1, a_2, \ldots, a_n$, es decir que se pueden escribir de la forma:

$$p = a_1x_1 + a_2x_2 + \cdots + a_nx_n \qquad \text{y} \qquad q = a_1y_1 + a_2y_2 + \cdots + a_ny_n;$$

con $x_i, y_i \geq 0$, la suma de ellos también es representable por $a_1, a_2, \ldots, a_n$ pues se puede escribir como:

$$p + q = a_1(x_1 + y_1) + a_2(x_2 + y_2) + \cdots + a_n(x_n + y_n);$$

con $x_i + y_i \geq 0$.

Definición 2.3. Dados $a_1, a_2, \ldots, a_n$ enteros positivos primos relativos, el mayor entero que no puede ser escrito como combinación lineal de $a_1, a_2, \ldots, a_n$ con coeficientes enteros positivos, lo denotamos por $f(a_1, a_2, \ldots, a_n)$.

De la definición anterior, existe una relación directa entre g y f dada por:

$$f(a_1, a_2, \ldots, a_n) \quad = \quad g(a_1, a_2, \ldots, a_n) + a_1 + a_2 + \cdots + a_n. \tag{2.3}$$

Definición 2.4. Dados $a_1, a_2, \ldots, a_n$ enteros positivos primos relativos, si ninguno de los a_i con $i = 1, 2, \ldots, n$ es representable por los demás decimos que $a_1, a_2, \ldots, a_n$ son independientes.

Ejemplo 2.3. Los números 3, 7 y 37 no son independientes, pues 37 es representable por 3 y 7, en este caso $37 = 3 \cdot 3 + 7 \cdot 4$. Los números 100, 7, 89 y 53 son independientes, ya que ninguno es representable por los demás.

Definición 2.5. Dados $a_1, a_2, \ldots, a_n$ enteros positivos primos relativos, para un entero no negativo k, $r(k)$ es el número de soluciones de la ecuación diofántica

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = k;$$

con $x_i \geq 0$.

A la luz de la definición anterior, observamos que el número de Frobenius de $a_1, a_2, \ldots, a_n$ es el mayor entero positivo m tal que $r(m) = 0$.

Ejemplo 2.4. Los enteros 12 y 27 son representables por 3 y 2 de las siguientes formas:

$$\begin{aligned} 12 &= 3 \cdot 4 + 2 \cdot 0, \\ 12 &= 3 \cdot 2 + 2 \cdot 3, \\ 12 &= 3 \cdot 0 + 2 \cdot 6, \end{aligned} \qquad \begin{aligned} 27 &= 3 \cdot 9 + 2 \cdot 0, \\ 27 &= 3 \cdot 7 + 2 \cdot 3, \\ 27 &= 3 \cdot 5 + 2 \cdot 6, \\ 27 &= 3 \cdot 3 + 2 \cdot 9, \\ 27 &= 3 \cdot 1 + 2 \cdot 12; \end{aligned}$$

de ahí que $r(12) = 3$ y $r(27) = 5$.

Definición 2.6. Sea $a_1, a_2, \ldots, a_n$ enteros positivos primos relativos, definimos $n(a_1, a_2, \ldots, a_n)$ como siendo el número de enteros positivos que no son representables por $a_1, a_2, \ldots, a_n$.

Dados $a_1, a_2, \ldots, a_n$ enteros positivos primos relativos, denotamos con $s(a_1, a_2, \ldots, a_n)$ a la suma de los enteros que no son representables por $a_1, a_2, \ldots, a_n$.

Ejemplo 2.5. El número de Frobenius de 5 y 6 es 19, además los enteros positivos que no son representables por 5 y 6 son: 1, 2, 3, 4, 7, 8, 9, 13, 14, y 19, luego

$$\begin{aligned} n(5,6) &= 10, \\ s(5,6) &= 1+2+3+4+7+8+9+13+14+19 = 80. \end{aligned}$$

2.1. El problema de Frobenius en el caso n=2

En esta sección nos dedicamos a estudiar el problema de Frobenius para el caso $n = 2$, el cual ha sido resuelto usando diferentes herramientas propias de algunas ramas de la matemática como la Teoría de números, Combinatoria, Geometría, entre otras, este hecho se verá reflejado en las tres demostraciones del Teorema 2.2 que hemos incluido en este trabajo. Además mostraremos una fórmula explícita para hallar el número de enteros positivos que no son representables y también una fórmula para calcular la suma de los enteros positivos que no son representables.

La primera prueba que presentaremos del número de Frobenius para el caso $n = 2$ se debe a el matemático Sylvester en [12], quien utiliza herramientas de Teoría de Números para establecer el resultado.

Teorema 2.2. *Sean a y b enteros positivos primos relativos, entonces:*

$$g(a,b) = ab - a - b = (a-1)(b-1) - 1.$$

Demostración 1. Sea $m = ab - a - b$. Como a y b son primos relativos, existen enteros x, y tales que $ax + by = m$, esto es $ax + by = ab - a - b$. Luego $a(x+1) = b(a-y-1)$ de donde $b \mid a(x+1)$ y $a \mid b(a-y-1)$, así del Lema 1.8, $b \mid (x+1)$ y $a \mid (a-y-1)$. Ahora, si $x \geq 0$, existe un entero positivo c tal que $x + 1 = bc$, de ahí que $a(bc) = b(a-y-1)$, esto es $ac = a - y - 1$, luego $y = a - ac - 1 = a(1-c) - 1 < 0$. Además, si $y \geq 0$, existe un entero no positivo k tal que $a - y - 1 = ak$, de ahí que $a(x+1) = b(ak)$, esto es $x + 1 = bk$, así

$x = bk - 1 < 0$. Por lo tanto, si $m = ab - a - b$ entonces $x < 0$ ó $y < 0$ y así $m = ab - a - b$ no es representable por a y b.

Por otro lado supongamos que $m > ab - a - b$ y sea (x_0, y_0) una solución entera de la ecuación $ax + by = m$, entonces del Corolario 1.11 la solución general es de la forma:

$$\begin{cases} x &= x_0 + bq \\ y &= y_0 - aq \end{cases}$$

donde q es un entero, por el algoritmo de la división podemos elegir un único q tal que $0 \leq x \leq b - 1$, luego $ax + by = m > ab - a - b$, esto es $b(y + 1) > a(b - 1 - x)$ y como $b - x - 1 \geq 0$, entonces $y + 1 > 0$ así que $y > 0$. Luego hemos encontrado una solución entera no negativa para la ecuación $ax + by = m$. Por lo tanto

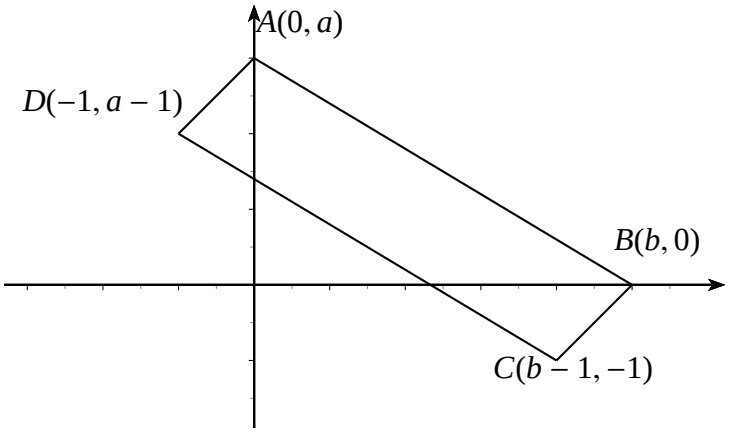
$$g(a, b) = ab - a - b. \qquad \square$$

Lema 2.3. *Dados a y b enteros positivos primos relativos entonces para todo* $i \leq ab - 1$, $r(i)$ *es* 0 *ó* 1.

Demostración. Supongamos que $r(i) \geq 2$, entonces existen enteros no negativos x, y, z, w tales que $ax + by = az + bw = i$, de la igualdad anterior tenemos $a(x - z) = b(w - y)$, así que $b|a(x - z)$ y por el Lema 1.8 $b|(x - z)$, de ahí que existe un entero k tal que $x - z = bk$. Por otro lado como $i < ab$, tenemos que $0 \leq x, z < b$, esto es $|x - z| < b$; por tanto $b|k| < b$, así $k = 0$, luego $x = z$. Análogamente se muestra que $y = w$, de esta manera observamos que en este caso $r(i) = 1$. Por lo tanto, $r(i)$ es 0 ó 1. $\square$

A continuación se dará la segunda prueba del Teorema 2.2, la herramienta principal es el Teorema de Pick.

Demostración 2. Sea P un polígono con vértices $A = (0, a)$, $B = (b, 0)$, $C = (b - 1, -1)$ y $D = (-1, a - 1)$.



Usando el Teorema 1.22 tenemos que el área de P es:

$$A(P) = I(P) + \frac{B(P)}{2} - 1, \tag{2.4}$$

recordando que $I(P)$ representa el número de puntos enteros interiores al polígono P y $B(P)$ representa el número de puntos enteros sobre la frontera del polígono P.

Veamos que los únicos puntos enteros sobre la frontera de P son los vértices A, B, C y D.

En efecto, la recta que une los puntos A y B está dada por:

$$b(a - y) = ax, \text{ con } 0 \leq x \leq b \text{ y } 0 \leq y \leq a$$

de ahí que $b \mid ax$ por el Lema 1.8 $b \mid x$ luego existe un entero t tal que $x = bt$, como x se encuentra restringido a un intervalo entonces t solo puede tomar los valores 0 y 1, los puntos respectivos son $A = (0, a)$ y $B = (b, 0)$. Lo mismo sucede con la recta $b(y + 1) = a(b - x - 1)$ que une los puntos C y D, los únicos puntos enteros sobre dicha recta son $C = (b - 1, -1)$ y $D = (-1, a - 1)$.

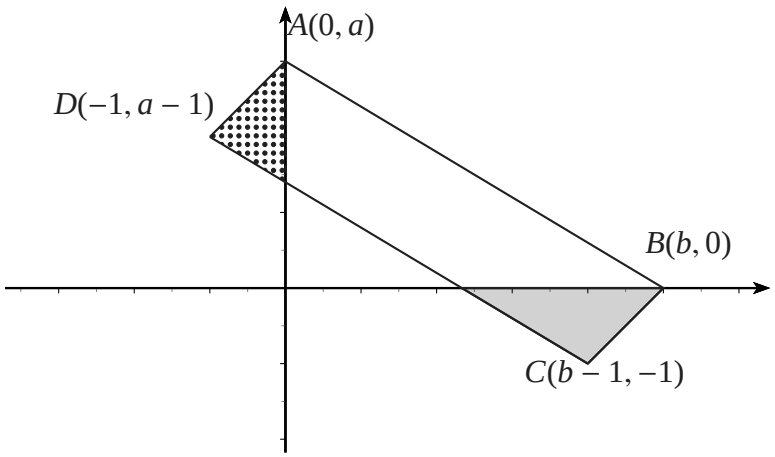
Como en la recta que une los puntos B y C, los únicos valores enteros que toma x son $b - 1$ y b entonces los únicos puntos enteros son $C = (b - 1, -1)$ y $B = (b, 0)$, lo mismo sucede con la recta que une los puntos D y A, como los únicos valores enteros que toma x son $a - 1$ y a entonces los únicos puntos enteros son $D = (b - 1, -1)$ y $A = (b, 0)$.

De esta manera mostramos que $B(P) = 4$.

El área del polígono P es

$$\begin{vmatrix} -1 & a-1 & 1 \\ b-1 & -1 & 1 \\ 0 & a & 1 \end{vmatrix} = a + b,$$

luego reemplazando $B(P) = 4$ y $A(P) = a + b$ en (2.4) encontramos que $I(P) = a + b - 1$. Ahora probaremos que todos los puntos en el interior de P están en el primer cuadrante o sobre los ejes positivos, lo que es equivalente a ver que no existen puntos enteros dentro de ninguna de las dos regiones destacadas (región punteada y la región sombreada).



La región punteada está delimitada por $-1 < x < 0$, luego x no toma ningún valor entero. La región sombreada está delimitada por $-1 < y < 0$, de ahí que y no toma valores enteros. Concluimos que no existen puntos enteros dentro de ninguna de las dos regiones.

La ecuación de la recta que pasa por los puntos A y B es $ax + by = ab$, y la recta que une los puntos C y D es $ax + by = ab - a - b$, necesitamos probar que para todo entero $ab > m > ab - a - b$, la línea $ax + by = m$ contienen al menos un punto en el primer cuadrante o en los ejes positivos.

Si $m = ab - a - b + j$ para algún entero positivo $j \leq a + b - 1$, mostraremos que la línea $ax + by = m$ contiene exactamente un punto interior a P, como $m \leq ab - 1$ entonces por Lema 2.3 tenemos que la línea $ax + by = m$ contiene a lo más un punto interior de P. Por otro

lado, como $I(P) = a+b-1$ entonces esos puntos deben estar en la línea $ax+by = ab-a-b+j$ para cualquier $j \in \{1, 2, \ldots, a+b-1\}$. Por tanto para cada uno de los $a+b-1$ valores de j, la línea $ax + by = ab - a - b + j$ contiene al menos un punto en el interior de P, pues si no fuera así por el principio de las casillas habría algún valor de j tal que dicha línea contiene dos puntos interiores contradiciendo el Lema 2.3. Luego para cada valor de j la línea $ax+by = m$ contiene exactamente un punto interior de P.

Si $m > ab$ entonces con un argumento similar (elegimos un polígono con vértices $(s, a + s)$, $(b+s, s)$, $(b+s-1, s-1)$ y $(s-1, a+s-1)$ para un entero positivo s adecuado); y vemos que la línea $ax + by = m$ siempre contiene un punto en el primer cuadrante, cuando $m = ab$ la línea contiene $(b, 0)$ y $(0, a)$ los cuales se encuentran sobre los ejes positivos. Luego el mayor valor de m tal que $ax + by = m$ no contiene puntos en el primer cuadrante ni en los ejes positivos es $ab - a - b$, finalmente $g(a, b) = ab - a - b$. □

Ahora vamos a describir un método (ver [13]) para encontrar todos los números que no son representables por a y b, de esta manera podemos presentar otra prueba del Teorema 2.2.

Método de la tabla

Dados a y b enteros positivos primos relativos, vamos a construir una tabla de ancho a y largo b, luego a partir de dicha tabla construimos una tabla reducida, la cual tendrá todos los enteros entre 0 y $ab - 1$, es decir la tabla reducida será un sistema completo de residuos módulo ab. Comenzaremos construyendo la tabla de la siguiente manera: la fila inferior es

$$0 \qquad a \qquad a \cdot 2 \qquad \cdots \qquad a \cdot (b-1)$$

la siguiente fila se obtiene sumando b a la fila inferior

$$b \qquad a+b \qquad a \cdot 2 + b \qquad \cdots \qquad a \cdot (b-1) + b$$

las demás filas se construyen de la misma manera agregando b a la fila anterior, hasta llegar

a la fila superior

$$b \cdot (a-1) \qquad a + b \cdot (a-1) \qquad a \cdot 2 + b \cdot (a-1) \qquad \cdots \qquad a \cdot (b-1) + b \cdot (a-1)$$

Trazamos una línea fronteriza entre las entradas menores que ab y las mayores o iguales que ab (de hecho ninguna entrada será ab, como veremos más adelante), llamaremos a esta tabla la tabla inicial. De ella obtenemos la tabla reducida restando ab a aquellas entradas que son mayores que ab (es decir, aquellas entradas encima o a la derecha de la línea fronteriza). Las entradas encima o a la derecha de la línea fronteriza en la tabla reducida son exactamente las que no son representables por a y b.

Probaremos que efectivamente la tabla reducida contiene todos los enteros entre 0 y $ab - 1$, también daremos una prueba formal, del hecho de que todas las entradas que están por encima o a la derecha de la línea fronteriza en la tabla reducida no son representables por a y b. Finalmente, con todos estos resultados daremos una tercera prueba del Teorema 2.2. Antes de demostrar estas afirmaciones veamos un ejemplo que ilustre la descripción del método.

Ejemplo 2.6. Para $a = 4$ y $b = 7$ la tabla inicial descrita anteriormente queda construida de la siguiente manera:

21	25	29	33	37	41	45
14	18	22	26	30	34	38
7	11	15	19	23	27	31
0	4	8	12	16	20	24

La tabla reducida se obtiene restando 28 a las entradas que están encima o a la derecha de la línea fronteriza, la tabla es:

21	25	1	5	9	13	17
14	18	22	26	2	6	10
7	11	15	19	23	27	3
0	4	8	12	16	20	24

Claramente los números 1, 2, 3, 5, 6, 9, 10, 13, 17 se encuentran encima o la derecha de la línea fronteriza y no son representables por 7 y 4.

Lema 2.4. *La tabla reducida contiene exactamente los números del 0 al* $ab - 1$.

Demostración. En la tabla inicial, cada entrada por debajo o a la izquierda de la línea fronteriza es menor que ab, para cada entrada r encima o a la derecha de la línea fronteriza tenemos

$$ab \leq r < a(b-1) + b(a-1) < ab + ab = 2ab,$$

de ahí que $0 \leq r - ab < ab$, esto es, todas las entradas de la tabla reducida son números enteros no negativos menores que ab, también es claro que hay ab números en la tabla reducida. De este modo, para completar la prueba, solo necesitamos mostrar que cualesquiera dos entradas de la tabla reducida son diferentes; la idea es similar a la prueba del Lema 2.3. Si dos entradas de la tabla reducida en el mismo lado en la línea fronteriza son iguales, entonces tenemos $ax + by = az + bw$ para enteros no negativos x, y, z, w con $0 \leq x, z < b$ y $x \neq z$, $0 \leq y, w < b$ y $w \neq y$, así $a(x - z) = b(y - w)$, pero esto es una contradicción pues $0 < |x - z| < b$ de ahí que $b \nmid (x - z)$.
Por consiguiente concluimos que cualesquiera dos entradas de la tabla reducida son diferentes, entonces la tabla reducida contiene exactamente los números entre 0 y $ab - 1$. □

Lema 2.5. *Cada entero mayor o igual que ab puede ser representable por a y b.*

Demostración. Usando el Teorema 2.2 la demostración sería trivial; sin embargo, presentamos otra prueba que será útil para dar la tercera demostración a dicho teorema.

En efecto, sea m un entero mayor o igual que ab, por el algoritmo de la división podemos escribir $m = (ab)q + r$ para q y r enteros con $q \geq 1$ y $0 \leq r \leq ab - 1$, por el Lema 2.4 r es una entrada de la tabla reducida.
Si r está por debajo o a la izquierda de la línea fronteriza, entonces r es una entrada de la tabla inicial, luego $r = ax_0 + by_0$ para x_0, y_0 enteros con $0 \leq x_0 \leq b - 1$ y $0 \leq y_0 \leq a - 1$, de

ahí que $m = (ab)q + r = a(x_0 + bq) + by_0$.

Si r está por encima o a la derecha de la línea fronteriza, tenemos que $r + ab$ es una entrada de la tabla inicial, así $r + ab = ax_1 + by_1$ para x_1, y_1 enteros con $0 \leq x_1 \leq b - 1$ y $0 \leq y_1 \leq a - 1$, de ahí que $m = (ab)q + r = a(x_1 + b(q - 1)) + by_1$, de ahí que m es representable por a y b. □

Corolario 2.6. *Los números que no son representables por a y b son exactamente aquellas entradas que están por encima o a la derecha de la línea fronteriza en la tabla reducida.*

Demostración. Sea r un entero no negativo, si $r \geq ab$ por el Lema 2.5 r es representable por a y b; si $r < ab$ entonces por el Lema 2.4 r es una entrada de la tabla reducida, si r está abajo o a la izquierda de la línea fronteriza entonces r pertenece a la tabla inicial y por lo tanto es representable por a y b, si r está encima o a la derecha de línea fronteriza entonces $r + ab \geq ab$ por tanto es representable por a y b, esto es existen enteros no negativos x, y tales que $r + ab = ax + by$ con $0 \leq x \leq b - 1$ y $0 \leq y \leq a - 1$, de ahí que $r = a(x - b) + by$ con $x - b < 0$, luego r no es representable por a y b. □

La siguiente es la tercera prueba del Teorema 2.2, para la cual usaremos el método de la tabla.

Demostración 3. Observamos que la última entrada en la fila superior de la tabla inicial es $a(b - 1) + b(a - 1) = 2ab - a - b$, después restamos ab, de ahí que la última entrada en la fila superior de la tabla reducida es $ab - a - b$, por tanto este número es el mayor de los enteros que se encuentran encima o a la derecha de la línea fronteriza, por el Corolario 2.6 este entero no es representable por a y b, luego $g(a, b) = ab - a - b$. □

Ahora, el siguiente resultado nos permite calcular el número de enteros positivos que no son representables por a y b, presentaremos una demostración ingeniosa de W. J. C. Sharp en [11].

Teorema 2.7. *Dados a y b enteros positivos primos relativos, el número de enteros que no son representables por a y b es:*

$$n(a, b) = \frac{(a - 1)(b - 1)}{2}.$$

Demostración 1. Consideremos el producto

$$(1 + x^a + x^{2a} + ... + x^{ab})(1 + x^b + x^{2b} + ... + x^{ab}),$$

el exponente de cada término entre 1 y x^{ab} corresponde a un número entero positivo representable por a y b menor que ab, también podemos observar que $2x^{ab}$ es el término del medio y los coeficientes de los demás términos son iguales a 1. Por tanto dos veces el número de términos tales que sus exponentes son enteros representables por a y b menores que ab es igual al producto anterior (cuando $x = 1$) menos cuatro, ya que los términos $1, 2x^{ab}, x^{2ab}$ no están incluidos. Luego el número de términos tales que sus exponentes son enteros representables por a y b es:

$$\frac{1}{2}(a + 1)(b + 1) - 2,$$

de ahí que el número de enteros que no son representables por a y b son:

$$ab - 1 - \left[\frac{1}{2}(a + 1)(b + 1) - 2\right] = \frac{1}{2}[ab - a - b + 1] = \frac{1}{2}(a - 1)(b - 1). \qquad \square$$

Demostración 2. Consideremos el intervalo $[0, ab - a - b]$, sea c un entero que pertenece a dicho intervalo.

Supongamos que c es representable por a y b, luego existen enteros no negativos x, y tal que $c = ax + by$, asumiremos que $ab - a - b - c$ es representable por a y b, así que existen enteros no negativos z, t tales que

$$\begin{aligned} az + bt &= ab - a - b - (ax + by) \\ az + bt &= a(b - 1 - x) + b(-1 - y) \\ a(z - b + 1 + x) &= b(-t - 1 - y). \end{aligned}$$

De ahí que $a \mid b(-t - 1 - y)$ y por el Lema 1.8 $a \mid (-t - 1 - y)$, así $z < 0$ (contradicción), como $b \mid a(z - b + 1 + x)$ nuevamente usando el Lema 1.8 $b \mid (z - b + 1 + x)$, de ahí que $t < 0$

(contradicción), luego $ab - a - b - c$ no es representable por a y b.

Supongamos que c no es representable por a y b, pero c puede escribirse como $c = xa + yb$ con $0 \leq x < b$, $y < 0$, luego

$$ab - a - b - c = a\,(b - 1 - x) + b\,(-1 - y)\,,$$

con $-1 - y \geq 0$, $b - 1 - x \geq 0$ y por tanto $ab - a - b - c$ es representable por a y b.

En consecuencia tenemos que existe una simetría en dicho intervalo respecto a los enteros que son representables por a y b, y los que no lo son, de donde cada clase en este intervalo tiene $\frac{1}{2}\,(a - 1)\,(b - 1)$ enteros. □

A continuación mostraremos una fórmula encontrada en [2], para calcular la suma $s(a, b)$ de los enteros que no son representables por a y b. Antes de ello vamos a considerar algunas cotas para $s(a, b)$.

Una cota superior trivial para $s(a, b)$, se obtiene por la suma de los $\frac{(a-1)(b-1)}{2}$ números más grandes del intervalo $[0, ab - a - b]$. Del mismo modo, una cota inferior trivial para $s(a, b)$ se obtiene tomando la suma de los $\frac{(a-1)(b-1)}{2}$ números enteros más pequeños en el intervalo $[0, ab - a - b]$.

$$\frac{1}{8}(a-1)^2(b-1)^2 - \frac{1}{4}(a-1)(b-1) \leq s(a,b) \leq \frac{3}{8}(a-1)^2(b-1)^2 - \frac{1}{4}(a-1)(b-1)$$

Teorema 2.8. *Sean a y b enteros positivos primos relativos entonces*

$$s(a,b) = \frac{1}{12}(a-1)(b-1)(2ab - a - b - 1).$$

Demostración. Definamos

$$f(x) = \sum_{n=0}^{ab-a-b} [1 - r(n)]x^n,$$

usando el Lema 2.3 $r(n) = 0$ ó $r(n) = 1$ para $0 \leq n \leq ab - 1$, así que

$$f'(x) = \sum_{n=1}^{ab-a-b} n[1 - r(n)]x^{n-1},$$

luego

$$\begin{aligned} f'(1) &= \sum_{n=1}^{ab-a-b} n[1 - r(n)] \\ &= \sum \{n : 1 \leq n \leq ab - a - b \; y \; r(n) = 0\} \\ &= s(a, b). \end{aligned}$$

Así, el problema de encontrar $s(a, b)$ se reduce a calcular $f'(1)$. Ali Ozluk descubrió una fórmula elegante para determinar $f(x)$, sea

$$f(x) = \frac{P(x) - 1}{x - 1}, \quad donde \quad P(x) = \frac{(x^{ab} - 1)(x - 1)}{(x^a - 1)(x^b - 1)},$$

como a y b son primos relativos resulta que

$$P(x) = \frac{(x^{ab} - 1)(x - 1)}{(x^a - 1)(x^b - 1)}$$

es un polinomio con coeficiente líder 1, esto se puede ver mediante la factorización tanto del denominador como del numerador en factores lineales complejos. Como a y b son primos relativos, existen enteros s, t tales que $as + bt = 1$. Sea ξ algún número complejo tal que $\xi^a = 1$ y $\xi^b = 1$, entonces

$$\xi = \xi^1 = \xi^{as+bt} = (\xi^a)^s(\xi^b)^t = 1.$$

En otras palabras, cada factor no lineal (excepto por $(x - 1)$) aparece dos veces en el deno-

minador de $P(x)$, por lo tanto cada factor lineal en el denominador se cancela con un factor lineal en el numerador.

Ya que $P(1) = 1$ por la regla de L´Hospital, tenemos que $\dfrac{P(x)-1}{x-1}$ es también un polinomio de grado $ab - a - b$, con coeficiente líder 1. Ahora haciendo

$$A(x) = \frac{1}{(1-x^a)(1-x^b)} = \left(\sum_{n=0}^{\infty} x^{an}\right)\left(\sum_{n=0}^{\infty} x^{bn}\right) = \sum_{n=0}^{\infty} r(n)x^n,$$

podemos escribir

$$\begin{aligned}
\frac{P(x)-1}{x-1} &= \frac{P(x)}{x-1} + \frac{1}{1-x} \\
&= (x^{ab}-1)A(x) + \frac{1}{1-x} \\
&= \sum_{n=0}^{\infty} r(n)x^{ab+n} - \sum_{n=0}^{\infty} r(n)x^n + \sum_{n=0}^{\infty} x^n \\
&= \sum_{n=0}^{\infty} r(n)x^{ab+n} + \sum_{n=0}^{\infty} [1-r(n)]x^n,
\end{aligned}$$

ya sabemos que esta serie de potencias es realmente un polinomio de grado $ab - a - b$ con coeficiente líder 1, podemos deducir que el coeficiente de la serie de potencias del $(ab-a-b)$ término es 1, y todos los coeficientes de la serie de potencias más tarde serán cero.
Note que $\sum_{n=0}^{\infty} r(n)x^{ab+n}$ es igual a $\sum_{n=0}^{\infty} r(n-ab)x^n$, lo cual implica que

$$\begin{aligned}
\frac{P(x)-1}{x-1} &= \sum_{n=0}^{ab-a-b} [r(n-ab)+1-r(n)]x^n + \sum_{n=ab-a-b+1}^{ab-1} [r(n-ab)+1-r(n)]x^n \\
&\quad + \sum_{n=ab}^{\infty} [r(n-ab)+1-r(n)]x^n,
\end{aligned}$$

por lo tanto, para $0 \le n \le ab-a-b$ tenemos que $r(n-ab) = 0$, para $ab-a-b < n \le ab-1$ entonces $r(n-ab) = 0$ y $r(n) = 1$, y además para $n \ge ab$ obtenemos $r(n-ab)+1 = r(n)$, de

esta manera

$$\frac{P(x)-1}{x-1} \quad = \quad \sum_{n=0}^{ab-a-b} [1-r(n)]x^n = f(x).$$

Ahora, procedemos a calcular $f'(1)$, sea $y = x^a$ entonces

$$P(x) = \frac{(x^{ab}-1)(x-1)}{(x^a-1)(x^b-1)} = \frac{\sum_{k=0}^{b-1} y^k}{\sum_{k=0}^{b-1} x^k}$$

y

$$f(x) = \frac{P(x)-1}{x-1} = \frac{\sum_{k=0}^{b-1} y^k - \sum_{k=0}^{b-1} x^k}{(x-1)\sum_{k=0}^{b-1} x^k} = \frac{\sum_{k=1}^{b-1} \frac{y^k - x^k}{x-1}}{\sum_{k=0}^{b-1} x^k} = \frac{g(x)}{h(x)},$$

donde

$$g(x) = \sum_{k=1}^{b-1} \frac{y^k - x^k}{x-1} \qquad \text{y} \qquad h(x) = \sum_{k=0}^{b-1} x^k.$$

Ahora usamos

$$\frac{y^k - x^k}{x-1} = \frac{x^{ak} - x^k}{x-1} = (x^k + x^{k+1} + \cdots + x^{ak-1})$$

para decir que

$$g(x) = \sum_{k=1}^{b-1} (x^k + x^{k+1} + \cdots + x^{ak-1})$$

Claramente el objetivo es hallar $f'(1)$, donde $f(x) = \frac{g(x)}{h(x)}$, usando la regla de derivación para

cocientes tenemos

$$f'(x) = \frac{h(x)g'(x) - g(x)h'(x)}{(h(x))^2}.$$

Calculemos la derivada de g y la de h

$$\begin{aligned} g'(x) &= \sum_{k=1}^{b-1} (kx^{k-1} + (k+1)x^k + \cdots + (ak-1)x^{ak}) \\ h'(x) &= \sum_{k=0}^{b-1} kx^{k-1} \end{aligned}$$

luego,

$$g(1) = \sum_{k=1}^{b-1} (a-1)k = \frac{1}{2}(a-1)(b-1)b, \quad h(1) = b, \quad h'(1) = \frac{1}{2}b(b-1).$$

Usando

$$k + (k+1) + \cdots + (ka-1) = \frac{1}{2}\left[ka(ka-1) - k(k-1)\right] = \frac{1}{2}\left[k^2(a^2-1) - k(a-1)\right],$$

obtenemos que

$$\begin{aligned} g'(1) &= \sum_{k=1}^{b-1} (k + (k+1) + \cdots + (ka-1)) = \sum_{k=1}^{b-1} \frac{1}{2}\left[k^2(a^2-1) - k(a-1)\right] \\ &= \frac{1}{2}(a^2-1)\sum_{k=1}^{b-1} \left(k^2\right) - \frac{1}{2}(a-1)\sum_{k=1}^{b-1} k \\ &= \frac{1}{2}(a^2-1)\frac{1}{6}(b-1)b(2b-1) - \frac{1}{2}(a-1)\frac{1}{2}(b-1)b \\ &= b(a-1)(b-1)\left(\frac{(a+1)(2b-1)}{12} - \frac{1}{4}\right) \end{aligned}$$

finalmente,

$$s(a,b) = f'(1) = \frac{h(1)g'(1) - g(1)h'(1)}{(h(1))^2} = \frac{1}{12}(a-1)(b-1)(2ab-a-b-1). \qquad \square$$

2.2. Algunos resultados generales

Enunciaremos algunos resultados encontrados en [1] y [9], que serán usados en el desarrollo de los tres métodos para encontrar el número de Frobenius. Además observaremos que la relación existente entre f y g será muy útil para calcular el número de Frobenius.

Teorema 2.9. *Sean $a_1, a_2, \ldots, a_n$ enteros positivos primos relativos entonces $f(a_1, a_2, \ldots, a_n)$ puede ser expresado en la forma:*

$$f(a_1, a_2, \ldots, a_n) = \sum_{i=2}^{n} a_i x_i; \quad con \quad x_i > 0. \tag{2.5}$$

Demostración. Podemos escribir

$$a_1 + f(a_1, a_2, \ldots, a_n) = a_1 x_1 + \sum_{i=2}^{n} a_i x_i; \quad \text{con} \quad x_i > 0,$$

de ahí que

$$f(a_1, a_2, \ldots, a_n) = a_1(x_1 - 1) + \sum_{i=2}^{n} a_i x_i; \quad \text{con} \quad x_i > 0,$$

como $x_1 - 1 > -1$, esto es $x_1 - 1 \geq 0$, lo cual contradice la definición de f, a menos que $x_1 = 1$. □

Teorema 2.10. *Sean $a_1, a_2, \ldots, a_n$ enteros positivos primos relativos, si* $\gcd(a_2, \ldots, a_n) = d$ *entonces*

$$f(a_1, a_2, \ldots, a_n) = d \cdot f\left(a_1, \frac{a_2}{d}, \ldots, \frac{a_n}{d}\right).$$

Demostración. Establecemos que $a_i = da_i'$ para $i = 2, \ldots, n$ y sea $f(a_1, a_2, \ldots, a_n) = K$. Por (2.5)

$$K = \sum_{i=2}^{n} a_i x_i = d \cdot \sum_{i=2}^{n} a_i' x_i; \quad \text{con} \quad x_i > 0,$$

así K es divisible por d, luego K se puede expresar como $K = dK'$ donde $K' = \sum_{i=2}^{n} a_i' x_i$ con $x_i > 0$. Probemos que $K' = f(a_1, a_2', \ldots, a_n')$.

Veamos que K' no puede ser expresado como combinación lineal de $a_1, a_2', \ldots, a_n'$ con coeficientes enteros positivos; supongamos lo contrario, es decir

$$K' = a_1 y_1 + \sum_{i=2}^{n} a_i' y_i; \quad \text{con} \quad y_i > 0,$$

así dado que $K = dK'$, entonces

$$K = d a_1 y_1 + \sum_{i=2}^{n} a_i y_i; \quad \text{con} \quad y_i > 0,$$

lo cual es una contradicción pues $K = \sum_{i=2}^{n} a_i x_i$ con $x_i > 0$.

Ahora si $m > K'$, veamos que m se puede expresar como combinación lineal de $a_1, a_2', \ldots, a_n'$ con coeficientes enteros positivos. Como $md > K'd = K$, entonces md se puede expresar de la forma

$$md = \sum_{i=1}^{n} a_i z_i = a_1 z_1 + d \cdot \sum_{i=2}^{n} a_i' z_i \qquad (z_i > 0)$$

por lo tanto d divide a z_1, es decir, $z_1 = dz_1'$ y $m = a_1 z_1' + \sum_{i=2}^{n} a_i' z_i$.

Hemos probado que K' es el mayor entero positivo que no puede expresarse como combinación lineal de $a_1, a_2', \ldots, a_n'$ con coeficientes enteros positivos, luego claramente

$$K' = f(a_1, a_2', \ldots, a_n') = f\left(a_1, \frac{a_2}{d}, \ldots, \frac{a_n}{d}\right). \qquad \square$$

Un resultado inmediato del teorema anterior es el siguiente:

Corolario 2.11. *Sean $a_1, a_2, \ldots, a_n$ enteros positivos primos relativos, si* $\gcd(a_2, \ldots, a_n) = d$

entonces

$$g\,(a_1, a_2, \ldots, a_n) = d \cdot g\left(a_1, \frac{a_2}{d}, \ldots, \frac{a_n}{d}\right) + a_1(d-1).$$

Demostración. Por (2.3) tenemos que

$$g(a_1, a_2, \ldots, a_n) = f(a_1, a_2, \ldots, a_n) - a_1 - a_2 - \cdots - a_n \tag{2.6}$$

y aplicando Teorema 2.10

$$g(a_1, a_2, \ldots, a_n) = d \cdot f\left(a_1, \frac{a_2}{d}, \ldots, \frac{a_n}{d}\right) - a_1 - a_2 - \cdots - a_n,$$

usando de nuevo (2.3)

$$g(a_1, a_2, \ldots, a_n) = d \cdot g\left(a_1, \frac{a_2}{d}, \ldots, \frac{a_n}{d}\right) + d\left(a_1 + \frac{a_2}{d} + \cdots + \frac{a_n}{d}\right) - a_1 - a_2 - \cdots - a_n,$$

finalmente concluimos que

$$g(a_1, a_2, \ldots, a_n) = d \cdot g\left(a_1, \frac{a_2}{d}, \ldots, \frac{a_n}{d}\right) + a_1(d-1). \qquad \square$$

Definición 2.7. Sean $a_1, a_2, \ldots, a_n$ enteros positivos primos relativos y L un sistema completo de residuos módulo a_1, para cada $l \in L$ tal que $l \not\equiv 0 \pmod{a_1}$, t_l es el menor entero que es representable por $a_1, a_2, \ldots, a_n$ y $t_l \equiv l \pmod{a_1}$.

La existencia de los t_l de la definición se garantiza por el principio del buen orden.

Lema 2.12. *Sean $a_1, a_2, \ldots, a_n$ enteros positivos primos relativos, si t_l es representable por $a_1, a_2, \ldots, a_n$ entonces t_l se puede escribir de la siguiente manera*

$$t_l = \sum_{i=2}^{n} a_i x_i \qquad\qquad (x_i \geq 0).$$

Demostración. Como t_l es representable por $a_1, a_2, \ldots, a_n$ entonces existen enteros no nega-

tivos $x_1, x_2, \ldots, x_n$ tales que

$$t_l = \sum_{i=1}^{n} a_i x_i = a_1 x_1 + \sum_{i=2}^{n} a_i x_i,$$

como por definición $t_l \equiv l \pmod{a_1}$, entonces

$$a_1 x_1 + \sum_{i=2}^{n} a_i x_i \equiv l \pmod{a_1},$$

de donde

$$\sum_{i=2}^{n} a_i x_i \equiv l \pmod{a_1}.$$

Hemos encontrado un entero $\sum_{i=2}^{n} a_i x_i$ más pequeño que t_l, representable por $a_1, a_2, \ldots, a_n$ y que es congruente con l módulo a_1, para evitar una contradicción con la escogencia del t_l entonces si consideramos $x_1 = 0$, tenemos

$$t_l = \sum_{i=2}^{n} a_i x_i; \quad \text{con} \quad x_i \geq 0. \qquad \square$$

Teorema 2.13. *Sean $a_1, a_2, \ldots, a_n$ enteros positivos primos relativos entonces*

$$g(a_1, a_2, ..., a_n) = \max_{l \in L} \; t_l - a_1. \tag{2.7}$$

Demostración. Supongamos que $\max_{l \in L} \; t_l - a_1$ es representable por $a_1, a_2, \ldots, a_n$ es decir

$$\begin{aligned} \max_{l \in L} \; t_l - a_1 &= a_1 x_1 + a_2 x_2 + \cdots + a_n x_n; \quad \text{con } x_i \geq 0, \\ \max_{l \in L} \; t_l - (x_1 + 1) a_1 &= a_2 x_2 + \cdots + a_n x_n, \end{aligned}$$

que contradice el hecho de que $\max_{l \in L} \; t_l$ es el más pequeño de su clase de residuos. Cualquier número mayor que $\max_{l \in L} \; t_l - a_1$ es mayor o igual al número más pequeño en su clase de residuos que es representable por $a_1, a_2, \ldots, a_n$. De ahí que $\max_{l \in L} \; t_l - a_1$ es el mayor entero que no es representable por $a_1, a_2, \ldots, a_n$. $\square$

Teorema 2.14. *Sean $a_1, a_2, \ldots, a_n$ enteros positivos primos relativos entonces*

$$n(a_1, a_2, ..., a_n) = \frac{1}{a_1} \cdot \sum_{l \in L} t_l - \frac{a_1 - 1}{2}. \tag{2.8}$$

Demostración. De la definición de t_l, si $k \equiv l \not\equiv 0 \pmod{a_1}$ con $0 < k < t_l$ entonces k no es representable por $a_1, a_2, \ldots, a_n$. Entonces el número de enteros positivos menores que t_l y congruentes con l módulo a_1 esta dado por $\left[\frac{t_l}{a_1}\right]$; asumiendo $0 < l < a_1$, entonces tenemos $\left[\frac{t_l}{a_1}\right] = \frac{t_l - l}{a_1}$, luego sumando sobre $l \in L$

$$\begin{aligned}
\sum_{l \in L} \frac{t_l - l}{a_1} &= \frac{1}{a_1} \cdot \sum_{l \in L} t_l - \sum_{l \in L} \frac{l}{a_1} \\
&= \frac{1}{a_1} \cdot \sum_{l \in L} t_l - \frac{1}{a_1} \cdot \frac{(a_1 - 1)a_1}{2} \\
&= \frac{1}{a_1} \cdot \sum_{l \in L} t_l - \frac{a_1 - 1}{2}.
\end{aligned}$$

□

Corolario 2.15. *Sean $a_1, a_2, \ldots, a_n$ enteros positivos primos relativos, si* $\gcd(a_2, \ldots, a_n) = d$ *entonces*

$$n(a_1, a_2, \ldots, a_n) = d \cdot n\left(a_1, \frac{a_2}{d}, \ldots, \frac{a_n}{d}\right) + \frac{(a_1 - 1)(d - 1)}{2}.$$

Demostración. Supongamos que $a_i = da_i'$ para $i = 2, \ldots, n$, sea t_l' el menor entero positivo congruente con l módulo a_1 y que es representable por $a_1, a_2', \ldots, a_n'$, observemos que

$$dt_l' = d \sum_{i=2}^{n} a_i' x_i = \sum_{i=2}^{n} a_i x_i \qquad (x_i \geq 0)$$

es claro que dt_l' es el menor entero positivo que es representable por $a_1, a_2, \ldots, a_n$ y congruen-

te con dl módulo a_1. Por definición tenemos que $dt'_l = t_{dl}$. Ahora usando (2.8)

$$\begin{aligned} n(a_1, a_2, \ldots, a_n) &= \frac{1}{a_1} \cdot \sum_{l=1}^{a_1-1} dt'_l - \frac{a_1 - 1}{2} \\ &= d\left(\frac{1}{a_1} \cdot \sum_{l=1}^{a_1-1} t'_l\right) - \frac{(a_1-1)}{2} + \frac{d(a_1-1)}{2} - \frac{d(a_1-1)}{2} \\ &= d\left(\frac{1}{a_1} \cdot \sum_{l=1}^{a_1-1} t'_l - \frac{(a_1-1)}{2}\right) + \frac{(a_1-1)(d-1)}{2} \\ &= d \cdot n(a_1, a'_2, \ldots, a'_n) + \frac{(a_1-1)(d-1)}{2} \\ &= d \cdot n\left(a_1, \frac{a_2}{d}, \ldots, \frac{a_n}{d}\right) + \frac{(a_1-1)(d-1)}{2}. \end{aligned}$$

□

2.3. Métodos para calcular el número de Frobenius en el caso n=3

Por último dedicamos esta sección a estudiar tres métodos, los cuales dan una solución para encontrar el número de Frobenius a tres enteros positivos primos relativos dos a dos e independientes, destacamos el uso de fracciones continuas finitas en los dos últimos métodos. Incluimos algoritmos de dichos métodos en el software MuPAD en el apéndice A.

2.3.1. Método de Hofmeister

Aunque no existe una fórmula general para $g(a, b, c)$ donde a, b y c son primos relativos, Hofmeister en [4] da un método para encontrar el número de Frobenius para el caso $n = 3$, asumiendo que se tienen tres enteros positivos primos relativos dos a dos e independientes.

Sean a, b y c enteros positivos primos relativos dos a dos e independientes. La congruencia $bx \equiv c \pmod{a}$ tiene solución única ya que a y b son primos relativos, es decir, existe un

entero $0 \leq s < a$ tal que

$$bs \equiv c \pmod{a}, \tag{2.9}$$

si $s = 0$ entonces $c \equiv 0 \pmod{a}$ y si $s = 1$ entonces c es representable por a y b, ambos casos contradicen las condiciones iniciales, luego $1 < s < a$. De la congruencia (2.9) existe un entero t tal que $bs = c + ta$, esto es

$$c = bs - ta, \tag{2.10}$$

de donde deducimos que $t > 0$, pues a, b y c son independientes. Por otro lado, aplicando el algoritmo de la división existen enteros positivos únicos q y r, con $0 \leq r < s$, tales que

$$a = qs + r, \tag{2.11}$$

si $r = 0$ se contradice el hecho de que a y c son primos relativos, de ahí que $0 < r < s$.
Con el fin de encontrar un sistema minimal de residuos módulo a, construiremos el siguiente diagrama

$$\begin{array}{ccccccc} & b & 2b & \dots & (s-1)b \\ c & b+c & 2b+c & \dots & (s-1)b+c \\ 2c & b+2c & 2b+2c & \dots & (s-1)b+2c \\ \dots & \dots & \dots & \dots & \dots \\ (q-1)c & b+(q-1)c & 2b+(q-1)c & \dots & (s-1)b+(q-1)c \\ qc & b+qc & 2b+qc & \dots & (r-1)b+qc \end{array} \tag{2.12}$$

Las q líneas completas (asumiendo que hay un cero en la esquina superior izquierda) tienen cada una s elementos y la línea incompleta tiene r elementos, de ahí que el diagrama tiene $qs + r = a$ elementos. Ahora veamos que el diagrama (2.12) constituye un sistema completo de residuos módulo a.

Todos los elementos de las q líneas completas son de la forma $ib + jc$ con $0 \leq i \leq s-1$ y $0 \leq j \leq q-1$, luego

$$ib + jc \equiv ib + jbs \equiv (i + js)b \pmod{a}$$

con $0 \leq i + js \leq qs - 1$, y los elementos de la línea incompleta son de la forma $ib + qc$ con $0 \leq i \leq r - 1$, de donde

$$ib + qc \equiv ib + sqb \equiv (i + qs)b \pmod{a}$$

con $qs \leq i + qs \leq a - 1$, podemos concluir que todos los elementos del diagrama (2.12) son congruentes con uno y solo un entero de la forma kb con $0 \leq k \leq a - 1$, formando así un sistema completo de residuos.

El siguiente teorema nos indica bajo que condición el diagrama (2.12) representa el sistema minimal t_l, el cual usaremos para hallar el número de Frobenius, aplicando el Teorema 2.13.

Teorema 2.16. *Sean a, b y c enteros positivos primos relativos dos a dos e independientes, y sean s, q y r enteros que satisfacen las ecuaciones* (2.9), (2.10) *y* (2.11). *Si* $(q+1)c \geq (s-r)b$ *entonces*

$$g(a, b, c) = \max\{(s-1)b + (q-1)c, (r-1)b + qc\} - a.$$

Demostración. De la igualdad en (2.10) tenemos que $c < bs$, entonces no se gana nada extendiendo el diagrama (2.12) a la derecha, pues si llenamos la línea incompleta, tenemos $s - r$ nuevos elementos congruentes módulo a con los $s - r$ elementos iniciales de la primera línea (incluyendo un cero inicial en la esquina superior izquierda). Ya que las líneas aumentan monótonamente hacia la derecha, los nuevos elementos son claramente mayores que los correspondientes de la primera línea. Si extendemos el diagrama (2.12) debajo de la línea incompleta, aumentando la línea incompleta por c, obtenemos una nueva línea cuyos elementos son congruentes módulo a con los r últimos elementos de la primera línea. Pero

los nuevos elementos no son más pequeños que los de la primera línea, debido a la condición $(q+1)c \geq (s-r)b$, por lo tanto el diagrama (2.12) representa el sistema minimal t_l.
El máximo de los t_l se encuentra en una de las esquinas inferiores derechas del diagrama (2.12), es decir, $(s-1)b + (q-1)c$ ó $(r-1)b + qc$, y así usando (2.7) tenemos que

$$g(a,b,c) = \max_{l \in L} t_l - a = \max\{(s-1)b + (q-1)c, (r-1)b + qc\} - a. \qquad \square$$

Teorema 2.17. *Sean a, b y c enteros positivos primos relativos dos a dos e independientes, y sean s, q y r enteros que satisfacen las ecuaciones* (2.9), (2.10) *y* (2.11). *Si* $(q+1)c \geq (s-r)b$ *entonces*

$$n(a,b,c) = n(a,b) - \frac{1}{2}qt(a-s+r).$$

Demostración. Sumamos los elementos del diagrama (2.12)

$$\begin{aligned}
\sum_{l \in L} t_l &= q\sum_{i=0}^{s-1} ib + \sum_{i=0}^{q-1} isc + \sum_{i=0}^{r-1} ib + qrc \\
&= \frac{q(s-1)s}{2}b + \frac{s(q-1)q}{2}c + \frac{(r-1)r}{2}b + qrc \\
&= \frac{(s-1)a - (s-r)r}{2}b + \frac{q(a-s+r)}{2}c,
\end{aligned}$$

insertando lo anterior en la fórmula (2.8) tenemos

$$\begin{aligned}
n(a,b,c) &= \frac{1}{a}\sum_{l \in L} t_l - \frac{a-1}{2} \\
&= \frac{1}{a}\left(\frac{(s-1)a - (s-r)r}{2}b + \frac{q(a-s+r)}{2}c\right) - \frac{a-1}{2} \\
&= \frac{(qs+r-1)b - (a-1)}{2} - \frac{qt(a-s+r)}{2} \\
&= n(a,b) - \frac{qt(a-s+r)}{2}
\end{aligned}$$

$\square$

A continuación ilustraremos como hallar el número de Frobenius (usando el método de Hofmeister) y el número de enteros positivos que no son representables.

Ejemplo 2.7. Veamos que los números $a = 31$, $b = 71$, $c = 209$ cumplen la condición bajo la cual el diagrama (2.12) representa el sistema minimal t_l. Dado que

$$\begin{aligned} 209 &\equiv 6 \cdot 71 \pmod{31} \\ 209 &= 6 \cdot 71 - 31 \cdot 7 \\ 31 &= 6 \cdot 5 + 1, \end{aligned}$$

tenemos $s = 6$, $t = 7$, $q = 5$ y $r = 1$, luego la condición $(q + 1)c \geq (s - r)b$ se satisface pues $6 \cdot 209 > 5 \cdot 71$, así el diagrama (2.12) queda de la siguiente forma:

	71	142	213	284	355
209	280	351	422	493	564
418	489	560	631	702	773
627	698	769	840	911	982
836	907	978	1049	1120	1191
1045					

luego

$$g(31, 71, 209) = \max\{1191, 1045\} - 31 = 1191 - 31 = 1160$$

y

$$n(31, 71, 209) = n(31, 71) - \frac{35 \cdot 26}{2} = 1050 - 455 = 595.$$

2.3.2. Método de Selmer y Beyer

El método para calcular el número de Frobenius para tres enteros positivos primos relativos dos a dos e independientes, presentado por Selmer y Beyer en [10] podríamos decir que es una extensión del método de Hofmeister, ya que nos indica como debemos proceder cuando

la desigualdad en el Teorema 2.16 no se satisface.

Sean a, b y c primos relativos dos a dos e independientes, además considere los enteros positivos s, t, q y r (los mismos del método de Hofmeister) tales que satisfacen las siguientes ecuaciones:

$$bs \equiv c \ (\text{mód } a), \tag{2.13}$$

$$c = bs - ta, \tag{2.14}$$

$$a = qs + r, \tag{2.15}$$

con $1 < s < a$, $0 < t$ y $0 < r < s$. El diagrama (2.12) en el método de Hofmeister, lo podemos escribir en un nuevo diagrama como un sistema de coordenadas (x, y) de la siguiente forma

$$\begin{array}{ccccccc} (0,0) & (1,0) & (2,0) & \dots & (s-1,0) \\ (0,1) & (1,1) & (2,1) & \dots & (s-1,1) \\ (0,2) & (1,2) & (2,2) & \dots & (s-1,2) \\ \dots & \dots & \dots & \dots & \dots \\ (0,q-1) & (1,q-1) & (2,q-1) & \dots & (s-1,q-1) \\ (0,q) & (1,q) & (2,q) & \dots & (r-1,q) \end{array} \tag{2.16}$$

el método de Hofmeister garantiza que todos los elementos del diagrama (2.12) representan los residuos módulo a una y solo una vez, de esta manera cuando $(q+1)c \geq (s-r)b$ podemos obtener el número de Frobenius como lo indica el Teorema 2.16.

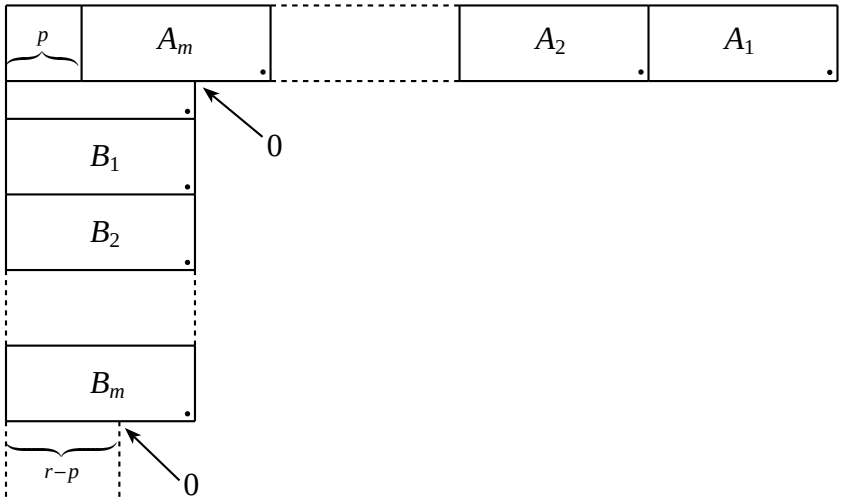
Ahora, cuando $(q+1)c \geq (s-r)b$ no se satisface, Selmer y Beyer demuestran que el diagrama (2.16) debe ampliarse para encontrar representantes más pequeños $bx+cy$ para algunas clases de residuos módulo a. Como en el método de Hofmeister, nada se gana extendiendo el diagrama (2.16) a la derecha, ya que bs puede reemplazarse por un entero positivo congruente más pequeño, c. Y además tenemos que en la posición (r, q),

$$br + cq \equiv br + bsq = b(qs + r) = ba \equiv 0 \ (\text{mód } a),$$

en consecuencia, ninguna representación minimal $bx + cy$ se encontrará en una extensión a la derecha. La única extensión posible del diagrama (2.16) será por lo tanto debajo de la línea incompleta. Para llevar a cabo dicha extensión, aplicamos el algoritmo de la división a los enteros positivos s y r, luego existen enteros positivos únicos m y p con $0 \leq p < r$ tales que

$$s = mr + p. \tag{2.17}$$

Por el momento vamos a suponer que $p > 0$. El primer paso de este método es considerar el diagrama de la siguiente figura, al cual nos referiremos en adelante como el **diagrama de bloques**



la franja horizontal y la franja estrecha debajo de ella representan los puntos del diagrama (2.16), y el resto de la franja vertical es la extensión. Ambas franjas están divididas en m bloques de ancho q y largo r. Estos bloques son congruentes por pares, es decir, los puntos del bloque A_i son congruentes módulo a con los puntos del bloque B_i para todo $i = 1, \ldots, m$. Esto se puede comprobar fácilmente representando todos los puntos tanto de los bloques A_i como de los bloques B_i.

En efecto, dado que los puntos de los bloques A_i y B_i son de la forma $(s - 1 - (i - 1)r - k, j)$ y $(r - 1 - k, iq + 1 + j)$ respectivamente, con $1 \leq i \leq m$, $0 \leq j \leq q - 1$ y $0 \leq k \leq r - 1$, entonces

$$
\begin{aligned}
(r-1-k)b+(iq+1+j)c &\equiv rb-b-kb+iqc+c+jc \pmod{a}\\
&\equiv rb-b-kb+iqbs+bs+jc \pmod{a}\\
&\equiv bs-b-kb+jc+rb+(i-1)rb-(i-1)rb+iqbs \pmod{a}\\
&\equiv bs-b-kb+jc-(i-1)rb+(qs+r)ib \pmod{a}\\
&\equiv bs-b-(i-1)rb-kb+jc \pmod{a}\\
&\equiv (s-1-(i-1)r-k)b+jc \pmod{a}.
\end{aligned}
$$

Como las esquinas inferiores derechas de los bloques A_i y B_i son los puntos mas grandes de cada bloque, vamos a considerar y designar las combinaciones correspondientes por

$$
\begin{aligned}
\alpha_i &= (s-1-(i-1)r)b+(q-1)c.\\
\beta_i &= (r-1)b+(i+1)qc.
\end{aligned}
\tag{2.18}
$$

Por otro lado, en particular la clase residual cero no se encuentra en ninguno de los bloques B_i. Sin embargo, esta clase se encuentra representada directamente debajo del bloque B_m, por el punto $(r-p,(m+1)q+1)$, ya que

$$
\begin{aligned}
(r-p)b+((m+1)q+1)c &\equiv (r-p)b+((m+1)q+1)bs \pmod{a}\\
&\equiv rb-pb+mqbs+qbs+bs \pmod{a}\\
&\equiv mb(sq+r) \pmod{a}\\
&\equiv (b+mb)a \pmod{a}\\
&\equiv 0 \pmod{a}.
\end{aligned}
$$

Los primeros $r-p$ puntos de la línea inmediatamente debajo de B_m serán por lo tanto congruentes módulo a con los últimos $r-p$ puntos en la franja estrecha arriba de B_1. Si los antiguos puntos representan combinaciones $bx+cy$ más grandes que estos últimos, no es necesario extender el diagrama abajo de B_m. La condición para ello, se da comparando los

dos puntos representantes de la clase residual cero, esto es

$$(r-p)b + ((m+1)q+1)c > rb + qc,$$

lo cual se puede reescribir como

$$\frac{c}{b} > \frac{p}{qm+1}. \tag{2.19}$$

Lema 2.18. *Con la notación anterior, si*

$$\frac{c}{b} > \frac{p}{qm+1},$$

entonces

$$g(a,b,c) = \max\{\beta_0, \alpha_m, \min\{\alpha_1,\beta_1\}, \ldots, \min\{\alpha_{m-1},\beta_{m-1}\}\} - a. \tag{2.20}$$

Demostración. Cuando la condición (2.19) se satisface, los candidatos para los t_l son todos los que se encontraron en el diagrama de bloques. Para determinar el máximo de los t_l, es claro que solo necesitamos tomar en cuenta las esquinas inferiores derechas de cada bloque A_i y B_i, que son los enteros α_i y β_i en (2.18). Adicionalmente, debemos considerar el elemento $\beta_0 = (r-1)b + qc$, el cual se encuentra más a la derecha por encima del bloque B_1. Por otra parte, podemos eliminar β_m de la lista, ya que $\beta_m \equiv \alpha_m \pmod{a}$ y además $\beta_m > \alpha_m$. Esta última afirmación es consecuencia de (2.17) y (2.19); en efecto, como $\frac{c}{b} > \frac{p}{qm+1}$ entonces

$$\begin{aligned}
(qm+1)c &> pb \\
qmc + c &> b(s-mr) \\
qmc &> b(s-mr) - c \\
qmc + cq + (r-1)b &> b(s-mr) - c + cq + (r-1)b \\
(r-1)b + (m+1)qc &> (s-1-(m-1)r)b + (q-1)c \\
\beta_m &> \alpha_m.
\end{aligned}$$

Para $i = 1, \ldots, m-1$, debemos elegir el correspondiente $t_l \equiv \alpha_i \equiv \beta_i \pmod{a}$, como t_l es el

más pequeño entre α_i y β_i, reemplazando en (2.7) tenemos

$$g(a,b,c) = \max\{\beta_0, \alpha_m, \min\{\alpha_1,\beta_1\},\ldots,\min\{\alpha_{m-1},\beta_{m-1}\}\} - a. \qquad \square$$

Indudablemente, esta es una fórmula explícita para el número de Frobenius, aunque bastante tosca. Con el objetivo de hacer un poco más elegante la fórmula, Selmer y Beyer introducen una cierta función $M\{x_1, x_2, \ldots, x_{2m}\}$ de un número par de argumentos, dada por

$$M\{x_1, x_2, \ldots, x_{2m}\} = x_{i_{m+1}} \quad \text{si} \quad x_{i_1} \leq x_{i_2} \leq \ldots, x_{i_{2m}}$$

en otras palabras, organizamos los argumentos en orden creciente y seleccionamos el número más pequeño de la mitad superior. Cuando $m = 1$, entonces $M\{x_1, x_2\} = \max\{x_1, x_2\}$.

Lema 2.19. *Con la notación anterior, si*

$$\frac{c}{b} > \frac{p}{qm+1},$$

entonces

$$g(a,b,c) = M\{\alpha_1,\alpha_2,\ldots,\alpha_m,\beta_0,\beta_1,\ldots,\beta_{m-1}\} - a.$$

Demostración. Observamos que

$$\alpha_1 > \alpha_2 > \cdots > \alpha_m, \quad \text{y} \quad \beta_0 < \beta_1 < \cdots < \beta_{m-1}.$$

Estas desigualdades, implican que la función máximo en la ecuación (2.20) puede ser reemplazada por la M-función de $2m$ argumentos α_i y β_i.
Ahora, probemos que si $k = \max\{\beta_0, \alpha_m, \min\{\alpha_1,\beta_1\},\ldots,\min\{\alpha_{m-1},\beta_{m-1}\}\}$, entonces

$$k = M\{\alpha_1,\alpha_2,\ldots,\alpha_m,\beta_0,\beta_1,\ldots,\beta_{m-1}\},$$

esto ocurre si k se encuentra en la posición $m+1$ con los argumentos ordenados ascendentemente, pues la M-función en este caso tiene $2m$ argumentos. De la definición de k, esta debe

ser algún α_i o β_i.

Si $k = \alpha_i = \min\{\alpha_i, \beta_i\}$ para algún i entonces $k = \alpha_i < \beta_i < \cdots < \beta_{m-1}$ y $k = \alpha_i < \alpha_{i-1} < \cdots < \alpha_1$, por lo tanto hay $(m - i) + (i - 1) = m - 1$ elementos delante de k. Veamos que no existe otro elemento delante de k. Supongamos que existe $j < i$ tal que $k = \alpha_i < \beta_j$, para ello consideramos dos casos:

- Si $\min\{\alpha_j, \beta_j\} = \alpha_j$, como $j < i$ entonces $\alpha_i < \alpha_j$, lo cual contradice el hecho de que $k = \alpha_i$ es el máximo.
- Si $\min\{\alpha_j, \beta_j\} = \beta_j$, β_j no puede estar delante de $k = \alpha_i$, pues contradice el hecho de que k es máximo.

Si $k = \beta_i = \min\{\alpha_i, \beta_i\}$ para algún i entonces $k = \beta_i < \alpha_i < \cdots < \alpha_1$ y $k = \beta_i < \beta_{i+1} < \cdots < \beta_{m-1}$, por lo tanto hay $i + (m - 1 - i) = m - 1$ elementos delante de k. Nuevamente veamos que no existe otro elemento delante de k. Supongamos que existe $j > i$ tal que $k = \beta_i < \alpha_j$, para ello consideramos dos casos:

- Si $\min\{\alpha_j, \beta_j\} = \beta_j$, como $j > i$ entonces $\beta_i < \beta_j$, lo cual contradice el hecho de que $k = \beta_i$ es el máximo.
- Si $\min\{\alpha_j, \beta_j\} = \alpha_j$, α_j no puede estar delante de $k = \beta_i$, pues contradice el hecho de que k es máximo.

Los elementos que se encuentran delante de k son exactamente $m - 1$ y los que se encuentran por debajo de k son m, en otras palabras k se encuentra en la posición $m + 1$ con los elementos ordenados ascendentemente. De este modo, hemos probamos que

$$M\{\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_0, \beta_1, \ldots, \beta_{m-1}\} = \max\{\beta_0, \alpha_m, \min\{\alpha_1, \beta_1\}, \ldots, \min\{\alpha_{m-1}, \beta_{m-1}\}\},$$

y reemplazando en (2.20) tenemos

$$g(a, b, c) = M\{\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_0, \beta_1, \ldots, \beta_{m-1}\} - a. \qquad \square$$

Teorema 2.20. *Con la notación anterior, si*

$$\frac{c}{b} > \frac{p}{qm+1},$$

entonces

$$g(a,b,c) = (r-1)b + (q-1)c + M\{(s-(i+1)r)b, (1+jq)c\} - a, \tag{2.21}$$

con $i, j = 0, 1, \ldots, m-1$.

Demostración. Por el Lema 2.19 obtenemos

$$g(a,b,c) = M\{\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_0, \beta_1, \ldots, \beta_{m-1}\} - a.$$

Sustituyendo α_i y β_i en (2.18)

$$g(a,b,c) = M\{(s-1)b + (q-1)c, ((s-1)-r)b + (q-1)c, \ldots,$$
$$((s-1)-(m-1)r)b + (q-1)c, (r-1)b + qc, (r-1)b + 2qc, \ldots, (r-1)b + mqc\} - a,$$

sacando los sumandos comunes de la M-función tenemos

$$g(a,b,c) = (r-1)b + (q-1)c + M\{(s-r)b, (s-2r)b, \ldots, (s-mr)b,$$
$$c, (q+1)c, \ldots, ((m-1)q+1)c\} - a$$

y así obtenemos

$$g(a,b,c) = (r-1)b + (q-1)c + M\{(s-(i+1)r)b, (1+jq)c\} - a,$$

con $i, j = 0, 1, \ldots, m-1$. □

A continuación presentamos una fórmula para hallar el número de enteros positivos no representables, dada por Selmer y Beyer.

Teorema 2.21. *Con la notación anterior, si*

$$\frac{c}{b} > \frac{p}{qm+1}$$

entonces

$$n(a,b,c) = -\frac{a-1}{2} + \frac{(r-1)b + (q-1)c}{2} + \frac{(s-(\lambda+1)r)(s-\lambda r)qb + (1+(\lambda+1)q)(1+\lambda q)rc}{2a}, \tag{2.22}$$

donde λ es un entero tal que $0 \leq \lambda \leq m-1$.

Demostración. Primero debemos determinar el sistema completo de residuos minimal t_l en el diagrama de bloques. Estos t_l se encuentran en el bloque de tamaño $r \times 1$ encima de B_1, en el bloque de tamaño $p \times q$ que está en la parte superior izquierda, y en los m bloques (A_i o B_i) de tamaño $r \times q$. La elección de los m bloques de tamaño $r \times q$ depende del valor de la M-función en (2.21). Esta función determina un entero $0 \leq \lambda \leq m-1$, tal que

$$M = (s-(\lambda+1)r)b \text{ selecciona } \alpha_{\lambda+1} \text{ de } A_{\lambda+1},$$
$$M = (1+\lambda q)c \text{ selecciona } \beta_\lambda \text{ de } B_\lambda.$$

En ambos casos, es claro que los residuos minimales restantes t_l deberán ser escogidos de los bloques

$$B_1, B_2, \ldots, B_\lambda, A_{\lambda+1}, A_{\lambda+2}, \ldots, A_m$$

(el conjunto de los B_i es vació si $\lambda = 0$). Teniendo así determinado el sistema de los t_l en el diagrama de bloques.

Ahora, si realizamos la suma de los t_l tenemos

$$\begin{aligned}\sum_{l\in L} t_l &= \sum_{i=0}^{r-1}(ib+qc)+\sum_{i=1}^{p}((s-mr-i)b+(q-1)c)\\ &\quad+\sum_{k=1}^{\lambda}\sum_{j=0}^{q-1}\sum_{i=0}^{r-1}((r-1-i)b+(kq+1+j)c)\\ &\quad+\sum_{k=\lambda+1}^{m}\sum_{j=0}^{q-1}\sum_{i=0}^{r-1}((s-1-(k-1)r-i)b+jc),\end{aligned}$$

como

$$\begin{aligned}\sum_{i=0}^{r-1} ib+qc &= \frac{(r-1)rb+2rqc}{2},\\ \sum_{i=1}^{p}(s-mr-i)b+(q-1)c &= \frac{(2s-2mr-p-1)pb+2(q-1)pc}{2},\\ \sum_{k=1}^{\lambda}\sum_{j=0}^{q-1}\sum_{i=0}^{r-1}(r-1-i)b+(kq+1+j)c &= \frac{((r-1)b+(\lambda q+2q+1)c)qr\lambda}{2},\\ \sum_{k=\lambda+1}^{m}\sum_{j=0}^{q-1}\sum_{i=0}^{r-1}(s-1-(k-1)r-i)b+jc &= \frac{((2s-mr-1)b+(q-1)c)mqr}{2}\\ &\quad-\frac{((2s-1-\lambda r)b+(q-1)c)\lambda qr}{2},\end{aligned}$$

entonces

$$\sum_{l\in L} t_l = \frac{((r-1)b+(q-1)c)a}{2}+\frac{(s-(\lambda+1)r)(s-\lambda r)qb+(1+(\lambda+1)q)(1+\lambda q)rc}{2}.$$

Finalmente reemplazando la suma de los t_l en la ecuación (2.8) obtenemos

$$n(a,b,c) = -\frac{a-1}{2}+\frac{(r-1)b+(q-1)c}{2}+\frac{(s-(\lambda+1)r)(s-\lambda r)qb+(1+(\lambda+1)q)(1+\lambda q)rc}{2a}.$$

□

Hasta aquí, asumiremos que $p > 0$ en (2.17). Como a y c son primos relativos, se tiene que $p = 0$ si y solo si $r = 1$. En este caso, todos los bloques del diagrama de bloques tienen ancho

1, y el residuo 0 en la parte superior de A_m aparecerá de nuevo en la parte superior de B_m, por lo que el diagrama termina en B_{m-1}.

Selmer y Beyer dan una extensión del diagrama de bloques, cuando (2.19) no se satisface. El diagrama se debe extender debajo de B_m, los nuevos bloques serán más angostos y dependen del algoritmo de la fracción continua para la razón $a : s$.
Los dos primeros pasos de este algoritmo ya están realizados por (2.15) y (2.17), los cuales reescribimos como

$$a = qs + r = q_0 s + r_0, \quad 0 < r_0 < s;$$
$$s = mr + p = q_1 r_0 + r_1, \quad 0 < r_1 < r_0.$$

El paso general esta dado por

$$r_n = q_{n+2} r_{n+1} + r_{n+2}, \quad 0 < r_{n+2} < r_{n+1}.$$

Como a y c son primos relativos entonces a y s son primos relativos, el último residuo distinto de 0 es 1, por lo tanto la siguiente división termina el algoritmo. A partir de los cocientes $q_0, q_1, q_2, \ldots$, formamos los convergentes de manera usual por

$$\frac{P_0}{Q_0} = \frac{q_0}{1}, \quad \frac{P_1}{Q_1} = \frac{q_0 q_1 + 1}{q_1}, \quad \frac{P_2}{Q_2} = \frac{(q_0 q_1 + 1) q_2 + q_0}{q_1 q_2 + 1}, \ldots$$

Como $p = r_1$ y $qm + r = q_0 q_1 + r_0 = P_1$, entonces con la nueva notación la condición (2.19) se puede escribir como

$$\frac{c}{b} > \frac{r_1}{P_1}. \tag{2.23}$$

Esta es la condición que nos indicará si se debe o no extender el diagrama de bloques.
Las esquinas son completamente descritas por las coordenadas de los ceros, los dos primeros

están incluidos en el diagrama de bloques y se reescriben como:

$$(r, q) = (r_0, P_0),$$

y

$$(r - p, (m + 1)q + 1) = (r_0 - r_1, q_0 + (q_1 q_0 + 1)) = (r_0 - r_1, P_0 + P_1).$$

Si $\frac{c}{b} < \frac{r_1}{P_1}$, el diagrama permite una extensión y el próximo cero se encuentra en la posición $(r_0 - 2r_1, P_0 + 2P_1)$, comparando los ceros $(r_0 - r_1, P_0 + P_1)$ y $(r_0 - 2r_1, P_0 + 2P_1)$ tenemos que

$$\begin{aligned} (r_0 - 2r_1)b + (P_0 + 2P_1)c &> (r_0 - r_1)b + (P_0 + P_1)c, \\ P_1 c &> r_1 b, \\ \frac{c}{b} &> \frac{r_1}{P_1}; \end{aligned}$$

lo cual es una contradicción, luego se debe seguir extendiendo el diagrama. Los próximos ceros se encuentran en

$$(r_0 - kr_1, P_0 + kP_1), \qquad k = 1, 2, \ldots, q_2 - 1.$$

Cuando $k = q_2$,

$$(r_0 - q_2 r_1, P_0 + q_2 P_1) = (r_2, P_2),$$

y el próximo cero está en $(r_2 - r_3, P_2 + P_3)$, ahora comparando (r_2, P_2) y $(r_2 - r_3, P_2 + P_3)$

$$\begin{aligned} (r_2 - r_3)b + (P_2 + P_3)c &> r_2 b + P_2 c, \\ P_3 c &> r_3 b, \\ \frac{c}{b} &> \frac{r_3}{P_3}; \end{aligned}$$

así que la nueva condición para detener la extensión del diagrama es

$$\frac{r_3}{P_3} < \frac{c}{b} < \frac{r_1}{P_1}.$$

Si $\frac{r_3}{P_3} > \frac{c}{b}$, el diagrama debe seguirse extendiendo y los próximos ceros se encuentran en

$$(r_2 - kr_3, P_2 + kP_3), \qquad k = 1, 2, \ldots, q_4 - 1.$$

Cuando $k = q_4$,

$$(r_2 - q_4 r_3, P_2 + q_4 P_3) = (r_4, P_4).$$

El proceso termina cuando encontramos un $n \geq 1$ tal que se cumple la siguiente condición

$$\frac{r_{2n+1}}{P_{2n+1}} < \frac{c}{b} < \frac{r_{2n-1}}{P_{2n-1}}.$$

De esta manera, el siguiente teorema es una extensión del Teorema 2.20.

Teorema 2.22. *Con la notación anterior, sea* $n \geq 1$ *el entero determinado por*

$$\frac{r_{2n+1}}{P_{2n+1}} < \frac{c}{b} < \frac{r_{2n-1}}{P_{2n-1}},$$

entonces

$$g(a, b, c) = (r_{2n} - 1)b + (P_{2n} - 1)c + M\{(r_{2n-1} - (i + 1)r_{2n})b, (P_{2n-1} + jP_{2n})c\} - a, \quad (2.24)$$

con $i, j = 0, 1, \ldots, q_{2n+1} - 1$.

También se puede extender la fórmula (2.22). La M-función de (2.24) determina un entero $0 \leq \lambda \leq q_{2n+1} - 1$ tal que

$$M = (r_{2n-1} - (\lambda + 1)r_{2n})b \;\text{ ó }\; M = (P_{2n-1} + \lambda P_{2n})c;$$

en cualquiera de los dos casos la aplicación de (2.8) da la siguiente fórmula para calcular $n(a, b, c)$, que es una extensión de (2.22).

Teorema 2.23. *Con la notación anterior, sea $n \geq 1$ el entero determinado por*

$$\frac{r_{2n+1}}{P_{2n+1}} < \frac{c}{b} < \frac{r_{2n-1}}{P_{2n-1}},$$

entonces

$$\begin{aligned} n(a,b,c) &= -\frac{a-1}{2} + \frac{(r_{2n}-1)b + (P_{2n}-1)c}{2} + \frac{(r_{2n-1} - (\lambda+1)r_{2n})(r_{2n-1} - \lambda r_{2n})P_{2n}b}{2a} \\ &\quad + \frac{(P_{2n-1} + (\lambda+1)P_{2n})(P_{2n-1} + \lambda P_{2n})r_{2n}c}{2a}, \end{aligned}$$

donde λ es un entero tal que $0 \leq \lambda \leq q_{2n+1} - 1$.

Ejemplo 2.8. Para $a = 31$, $b = 71$ y $c = 250$ tenemos

a	b	c	s	q	r	m	p
31	71	250	14	2	3	4	2

Ahora veamos que pasa con la condición $(q + 1)c \geq (s - 1)b$, reemplazando los valores correspondientes obtenemos

$$\begin{aligned} 3 \cdot 250 &\not\geqslant 13 \cdot 71 \\ 750 &\not\geqslant 923. \end{aligned}$$

Como la condición anterior no se cumple, entonces construimos el diagrama de bloques y revisamos la segunda condición, $(qm + 1)c > pb$. Como esta se satisface, pues

$$\begin{aligned} 250 \cdot 9 &> 2 \cdot 71 \\ 2250 &> 142, \end{aligned}$$

el diagrama de bloques no debe extenderse, y queda construido de la siguiente manera

0 71	142 213 284	355 426 497	568 639 710	781 852 923
250 321	392 463 534	605 676 747	818 889 960	1031 1102 1173

500 571 642
750 821 892
1000 1071 1142
1250 1321 1392
1500 1571 1642
1750 1821 1892
2000 2071 2142
2250 2321 2392
2500 2571 2642
2750

Para verificar que los elementos del bloque A_i son congruentes módulo 31 con los elementos del bloque B_i para todo $i = 1, 2, 3, 4$, construimos el mismo diagrama anterior pero con los elementos módulo 31.

0 9	18 27 5	14 23 1	10 19 28	6 15 24
2 11	20 29 7	16 25 3	12 21 30	8 17 26

4 13 22
6 15 24
8 17 26
10 19 28
12 21 30
14 23 1
16 25 3
18 27 5
20 29 7
22

Reemplazando en (2.21) tenemos

$$g(31, 71, 250) = 2 \cdot 71 + 1 \cdot 250 + M\{(14 - (i + 1) \cdot 3) \cdot 71, (1 + 2 \cdot j) \cdot 250\} - 31,$$

con $i, j = 0, 1, 2, 3$, luego

$$g(31, 71, 250) = 142 + 250 + M\{781, 250, 568, 750, 355, 1250, 142, 1750\} - 31,$$

ordenando los elementos de la M-función de forma ascendente

$$g(31, 71, 250) = 142 + 250 + M\{142, 250, 355, 568, 750, 781, 1250, 1750\} - 31,$$

ya que la M-función en este caso tiene $2 \cdot 4$ argumentos, obtenemos

$$g(31, 71, 250) = 142 + 250 + 750 - 31 = 1111.$$

2.3.3. Método de Rödseth

Sean a, b y c enteros positivos primos relativos dos a dos e independientes, para los cuales existe un único $0 \leq s_0 < a$ tal que

$$bs_0 \equiv c \ (\text{mód}\ a), \quad \text{con} \ \ 0 < s_0 < a. \tag{2.25}$$

Si $s_0 = 0$ entonces c es un múltiplo a, lo cual contradice el hecho de que a y c son primos relativos. Rödseth en [8] usa otra expansión de fracciones continuas de $a : s_0$ lo que resulta en fórmulas para $g(a, b, c)$ y $n(a, b, c)$, incluso más simple que la de Selmer y Beyer [10].

Ahora usaremos el algoritmo de Euclides de la siguiente forma:

$$\begin{array}{rcrcll} a & = & s_{-1} & = & q_1 s_0 - s_1, & 0 \leq s_1 < s_0; \\ & & s_0 & = & q_2 s_1 - s_2, & 0 \leq s_2 < s_1; \\ & & s_1 & = & q_3 s_2 - s_3, & 0 \leq s_3 < s_2; \\ & & & \vdots & & \\ & & s_{m-2} & = & q_m s_{m-1} - s_m, & 0 \leq s_m < s_{m-1}; \\ & & s_{m-1} & = & q_{m+1} s_m - s_{m+1}, & 0 = s_{m+1} < s_m. \end{array} \tag{2.26}$$

También definimos los enteros P_i que son los numeradores de los convergentes, con las condiciones iniciales $P_{-1} = 0$ y $P_0 = 1$, para así poder definir la siguiente fórmula de recurrencia

$$P_{i+1} = q_{i+1} P_i - P_{i-1}, \quad \text{para } \ i = 0, 1, \ldots, m. \tag{2.27}$$

Ya que $q_i \geq 2$ (porque se está trabajando con residuos negativos) se tiene que la sucesión de los P_i es creciente ($P_i < P_{i+1}$), para ello usamos el principio de inducción matemática sobre i; en efecto:

Paso inicial Verifiquemos que es cierto para $i = 0$

$$P_0 = 1 < 2 \leq q_1 = P_1.$$

Paso inductivo Supongamos cierto para $i = k$

$$P_k < P_{k+1},$$

probaremos que es cierto para $i = k + 1$,

$$P_{k+2} - P_{k+1} = q_{k+2} P_{k+1} - P_k - P_{k+1} = q_{k+2} P_{k+1} - (P_k + P_{k+1})$$
$$P_{k+2} - P_{k+1} > q_{k+2} P_{k+1} - 2P_{k+1} = P_{k+1}(q_{k+2} - 2) \geq 0.$$

Luego hemos probado que $P_i < P_{i+1}$ para todo $i = 0, 1, \ldots, m$.

Escribimos convencionalmente $\dfrac{s_{-1}}{P_{-1}} = \infty$, de esta forma obtenemos una sucesión decreciente

de los cocientes $\frac{s_i}{P_i}$

$$0 = \frac{s_{m+1}}{P_{m+1}} < \frac{s_m}{P_m} < \cdots < \frac{s_0}{P_0} < \frac{s_{-1}}{P_{-1}} = \infty,$$

como $P_{i+1} > P_i$ y $0 \leq s_{i+1} < s_i$ fácilmente comprobamos que esta sucesión $\frac{s_{i+1}}{P_{i+1}} < \frac{s_i}{P_i}$ es decreciente.

Luego existe un único entero v con $-1 \leq v \leq m$, que satisface

$$\frac{s_{v+1}}{P_{v+1}} \leq \frac{c}{b} < \frac{s_v}{P_v}. \tag{2.28}$$

Esto nos va a permitir obtener las fórmulas para $g(a,b,c)$ y $n(a,b,c)$ que se presentan en los dos resultados siguientes

Teorema 2.24. *Sean a, b y c enteros positivos, donde a y b son primos relativos, entonces*

$$g(a,b,c) = b(s_v - 1) + c(P_{v+1} - 1) - \text{mín}\{bs_{v+1}, cP_v\} - a, \tag{2.29}$$

donde v es el único entero determinado por (2.28)*.*

Demostración. Consideremos $R_i = \frac{1}{a}(bs_i - cP_i)$, para $i = -1, 0, \ldots, m+1$. Entonces por (2.26) y (2.27)

$$\begin{aligned} R_{i+1} &= \frac{1}{a}(bs_{i+1} - cP_{i+1}) = \frac{1}{a}\left[b\left(q_{i+1}s_i - s_{i-1}\right) - c\left(q_{i+1}P_i - P_{i-1}\right)\right] \\ &= q_{i+1}\frac{1}{a}(bs_i - cP_i) - \frac{1}{a}(bs_{i-1} - cP_{i-1}) = q_{i+1}R_i - R_{i-1}, \end{aligned}$$

así encontramos que R_i satisface la recurrencia lineal

$$R_{i+1} = q_{i+1}R_i - R_{i-1}, \quad \text{para } i = 0, 1, \ldots, m \tag{2.30}$$

con las condiciones iniciales

$$R_{-1} = b \qquad\qquad R_0 = \frac{1}{a}(bs_0 - c) \tag{2.31}$$

luego por (2.25) R_{-1} y R_0 son enteros, de igual forma la ecuación (2.30) muestra que todos los R_i son enteros. Por otra parte, ya que $P_i - P_{i+1} < 0 < s_i - s_{i+1}$, $R_{i+1} < R_i$ y usando (2.28) encontramos que $R_{v+1} \leq 0 < R_v$, de esta forma tenemos

$$R_{m+1} < R_m < \cdots < R_{v+1} \leq 0 < R_v < \cdots < R_{-1}. \tag{2.32}$$

Ahora consideramos $t_l = t_l(a, b, c)$. Dado l, existe una pareja de enteros no negativos (y, z) tal que $t_l = by + cz$. Sea (y_l, z_l) una pareja tal que z_l es mínimo. Por (2.30)

$$t_l - aR_v = (by_l + cz_l) - (bs_v - cP_v) = b(y_l - s_v) + c(z_l + P_v).$$

Como R_v es un entero positivo, de la definición de t_l tenemos que $t_l - aR_v$ no es representable por a, b y c, es decir $y_l - s_v < 0$, $y_l < s_v$.
Del mismo modo,

$$t_l + aR_{v+1} = b(y_l + s_{v+1}) + c(z_l - P_{v+1}),$$

si $R_{v+1} < 0$, entonces $z_l < P_{v+1}$. En el otro caso, $R_{v+1} = 0$, tenemos $z_l < P_{v+1}$, por la minimalidad de z_l. Sumando las anteriores igualdades

$$t_l - a(R_v - R_{v+1}) = b(y_l - s_v + s_{v+1}) + c(z_l + P_v - P_{v+1}),$$

nuevamente por definición de t_l, $t_l - a(R_v - R_{v+1})$ no es representable por a, b y c, así $y_l - s_v + s_{v+1} < 0$ o $z_l + P_v - P_{v+1} < 0$, de ahí que $y_l < s_v - s_{v+1}$ o $z_l < P_{v+1} - P_v$.

Así $(y_l, z_l) \in A \cup B$, donde A y B son conjuntos disjuntos de parejas de enteros dado por

$$\begin{aligned} A &= \{(y,z) \mid 0 \leq y < s_v - s_{v+1}, 0 \leq z < P_{v+1}\}, \\ B &= \{(y,z) \mid s_v - s_{v+1} \leq y < s_v, 0 \leq z < P_{v+1} - P_v\}. \end{aligned}$$

El número de elementos en $A \cup B$ está dado por

$$\mid A \cup B \mid = \mid A \mid + \mid B \mid = (s_v - s_{v+1})P_{v+1} + s_{v+1}(P_{v+1} - P_v) = s_v P_{v+1} - P_v s_{v+1},$$

ya que

$$s_i P_{i+1} - s_{i+1} P_i = a, \quad \text{para } i = -1, \ldots, m. \tag{2.33}$$

En efecto, para verificar (2.33) usaremos el principio de inducción matemática sobre i,

Paso inicial Verifiquemos que es cierto para $i = -1$

$$s_{-1} P_0 - s_0 P_{-1} = a.$$

Paso inductivo Supongamos cierto para $i = k$

$$s_k P_{k+1} - s_{k+1} P_k = a,$$

probaremos que es cierto para $i = k + 1$, por (2.26) y (2.27), $s_{i+2} = q_{i+2} s_{i+1} - s_i$ y $P_{i+2} = q_{i+2} P_{i+1} - P_i$ de ahí que

$$\begin{aligned} s_{k+1} P_{k+2} - s_{k+2} P_{k+1} &= s_{k+1}(q_{k+2} P_{k+1} - P_k) - P_{k+1}(q_{k+2} s_{k+1} - s_k) \\ s_{k+1} P_{k+2} - s_{k+2} P_{k+1} &= s_k P_{k+1} - s_{k+1} P_k = a. \end{aligned}$$

Lo cual demuestra (2.33).

De esta forma usando (2.33) $\mid A \cup B \mid = a$, de modo que para un sistema L completo de residuos módulo a.

$$\{t_l \mid l \in L\} = \{by + cz \mid (y,z) \in A \cup B\},$$

de donde

$$\max_{l\in L} t_l = \max_{(y,z)\in A\cup B} \{by + cz\},$$

y como

$$\max_{(y,z)\in A} \{by + cz\} = b(s_v - s_{v+1} - 1) + c(P_{v+1} - 1)$$

y

$$\max_{(y,z)\in B} \{by + cz\} = b(s_v - 1) + c(P_{v+1} - P_v - 1)$$

Entonces usando (2.7), tenemos

$$\begin{aligned} g(a,b,c) &= \max_{l\in L} t_l - a \\ &= \max_{(y,z)\in A\cup B} \{by + cz\} - a \\ &= \max\{b(s_v - 1) + c(P_{v+1} - 1) - bs_{v+1}, b(s_v - 1) + c(P_{v+1} - 1) - cP_v\} - a \\ &= b(s_v - 1) + c(P_{v+1} - 1) + \max\{-bs_{v+1}, -cP_v\} - a \\ &= b(s_v - 1) + c(P_{v+1} - 1) - \min\{bs_{v+1}, cP_v\} - a. \end{aligned}$$

□

Teorema 2.25. *Con la notación del Teorema 2.24, tenemos*

$$n(a,b,c) = \frac{1}{2}\left\{1 - a + b(s_v - s_{v+1} - 1) + c(P_{v+1} - 1) + \frac{1}{a}(P_{v+1} - P_v)(bs_v - cP_v)s_{v+1}\right\} \quad (2.34)$$

Demostración. Observamos que

$$\begin{aligned} \sum_{l\in L} t_l &= \sum_{(y,z)\in A} (by + cz) + \sum_{(y,z)\in B} (by + cz) \\ &= \sum_{y=0}^{s_v - s_{v+1} - 1} \sum_{z=0}^{P_{v+1}-1} (by + cz) + \sum_{y=s_v - s_{v+1}}^{s_v - 1} \sum_{z=0}^{P_{v+1} - P_v - 1} (by + cz), \end{aligned}$$

donde

$$\begin{aligned}\sum_{y=0}^{s_v-s_{v+1}-1}\sum_{z=0}^{P_{v+1}-1}(by+cz) &= \sum_{y=0}^{s_v-s_{v+1}-1}\left(\sum_{z=0}^{P_{v+1}-1}by+\sum_{z=0}^{P_{v+1}-1}cz\right)\\ &= \sum_{y=0}^{s_v-s_{v+1}-1}\left(P_{v+1}(by)+\frac{c(P_{v+1}-1)P_{v+1}}{2}\right)\\ &= \frac{bP_{v+1}(s_v-s_{v+1}-1)(s_v-s_{v+1})}{2}+\frac{c(s_v-s_{v+1})(P_{v+1}-1)P_{v+1}}{2}\end{aligned}$$

y

$$\begin{aligned}\sum_{y=s_v-s_{v+1}}^{s_v-1}\sum_{z=0}^{P_{v+1}-P_v-1}(by+cz) &= \sum_{y=s_v-s_{v+1}}^{s_v-1}\left((P_{v+1}-P_v)by+\frac{c(P_{v+1}-P_v-1)(P_{v+1}-P_v)}{2}\right)\\ &= b(P_{v+1}-P_v)\left(\frac{(s_v-1)s_v-(s_v-s_{v+1}-1)(s_v-s_{v+1})}{2}\right)\\ &\quad+\frac{c(P_{v+1}-P_v-1)(P_{v+1}-P_v)s_{v+1}}{2},\end{aligned}$$

luego

$$\sum_{l\in L}t_l = \frac{1}{2}\{(s_vP_{v+1}-s_{v+1}P_v)(b(s_v-s_{v+1}-1)+c(P_{v+1}-1))+s_{v+1}(P_{v+1}-P_v)(bs_v-cP_v)\};$$

usando (2.33) tenemos

$$\sum_{l\in L}t_l = \frac{1}{2}\{a(b(s_v-s_{v+1}-1)+c(P_{v+1}-1))+s_{v+1}(P_{v+1}-P_v)(bs_v-cP_v)\}$$

y reemplazando en (2.8)

$$\begin{aligned}n(a,b,c) &= \frac{1}{a}\cdot\frac{1}{2}\{a(b(s_v-s_{v+1}-1)+c(P_{v+1}-1))+s_{v+1}(P_{v+1}-P_v)(bs_v-cP_v)\}-\frac{a-1}{2}\\ &= \frac{1}{2}\{1-a+b(s_v-s_{v+1}-1)+c(P_{v+1}-1)+\frac{1}{a}(P_{v+1}-P_v)(bs_v-cP_v)s_{v+1}\}\end{aligned}$$

□

Ejemplo 2.9. Sean $a = 137$, $b = 251$ y $c = 256$. Por la congruencia (2.25) tenemos que

$s_0 = 108$, y por el algoritmo (2.26)

$$\begin{aligned}
137 &= 2 \cdot 108 - 79, \quad P_1 = 2;\\
108 &= 2 \cdot 79 - 50, \quad P_2 = 3;\\
79 &= 2 \cdot 50 - 21, \quad P_3 = 4;\\
50 &= 3 \cdot 21 - 13, \quad P_4 = 9;\\
21 &= 2 \cdot 13 - 5, \quad P_5 = 14;\\
13 &= 3 \cdot 5 - 2, \quad P_6 = 33;\\
5 &= 3 \cdot 2 - 1, \quad P_7 = 85;\\
2 &= 2 \cdot 1, \quad P_8 = 137;
\end{aligned}$$

encontramos que

$$\frac{s_5}{P_5} = \frac{5}{14} < \frac{256}{251} < \frac{13}{9} = \frac{s_4}{P_4},$$

por el Teorema 2.24

$$g(137, 251, 256) = -137 + 251 \cdot 12 + 256 \cdot 13 - \text{mín}\{251 \cdot 5, 256 \cdot 9\} = 4948,$$

y por el Teorema 2.25

$$n(137, 251, 256) = \frac{1}{2}\left(1 - 137 + 251 \cdot 7 + 256 \cdot 13 + 5 \cdot 5 \cdot \frac{1}{137}(251 \cdot 13 - 256 \cdot 9)\right) = 2562.$$

Capítulo 3

Conclusiones

Todos los objetivos propuestos en el trabajo de grado, los llevamos a cabo en el Capítulo 2 de la siguiente manera:

- En la sección 2.1, presentamos demostraciones minuciosas de los resultados del problema de Frobenius en el caso $n = 2$.
- En la sección 2.3, estudiamos el problema de Frobenius para el caso $n = 3$, analizando los métodos de Hofmeister, Selmer y Beyer y por último el de Rödseth.
- En las subsecciones 2.3.2 y 2.3.3, observamos el papel que desempeñaron las fracciones continuas en el desarrollo de los métodos de Selmer y Beyer y el de Rödseth.
- En la sección 2.2, Resaltamos la importancia del Teorema 2.13 y el Teorema 2.14 para calcular $g(a, b, c)$ y $n(a, b, c)$.
- Implementamos algoritmos en el software MuPAD para calcular el número de Frobenius en el caso $n = 3$, por medio de los métodos presentados por Hofmeister, Selmer y Beyer, Rödseth.

Apéndice A

Algoritmos

Después de haber estudiado los métodos de Hofmeister, Selmer y Beyer y el de Rödseth para hallar el número de Frobenius en el caso $n = 3$, es natural pensar en programar dichos métodos, ya que ello nos ahorra tiempo a la hora de dar ejemplos o de verificar lo que afirmamos en teoría. Los algoritmos son fáciles de entender con un lenguaje de programación muy básico e implementados en el software MuPAD, pues tiene herramientas de teoría de números que nos facilitaron los cálculos.

Algoritmo rep

Determinar si *num* es representable por a, b y c.

Entrada: *num*, a, b y c enteros positivos.

Salida: Cierto si *num* es representable por a, b y c, Falso en el caso contrario.

```
rep:=proc(num,a,b,c)
local i,j,k,cont,x,y,z;
begin
if a>1 and b>1 and c>1 and gcd(a,b,c)=1 then
x:=num div a;
y:=num div b;
z:=num div c;
cont:=0;
for i from 0 to x do
for j from 0 to y do
for k from 0 to z do
m:=i*a+j*b+k*c;
if m=num then
print([i,j,k]);
```

```
cont:=cont+1;
end_if;
end_for;
end_for;
end_for;
if cont=0 then
print("Falso")
else
print("Cierto")
end_if;
else
print("Cambie los números")
end_if;
end_proc;
```

Algoritmo ind

Determinar si *num* es representable por *a* y *b*.

Entrada: *num*, *a* y *b* enteros positivos.

Salida: Devuelve 1 si *num* es representable por *a* y *b*, 0 en el caso contrario.

```
ind:=proc(num,a,b)
local i,j,cont,r,x,y;
begin
x:=num div a;
y:=num div b;
r:=0;
cont:=0;
for i from 0 to x do
for j from 0 to y do
m:=i*a+j*b;
```

```
if m=num then
r:=r+1;
end_if;
end_for;
end_for;
if r>0 then
cont:=1;
end_if;
end_proc;
```

Algoritmo Hofmeister

Determinar el número de Frobenius (g) para tres enteros positivos a, b y c primos relativos dos a dos e independientes, usando el método de Hofmeister.

Entrada: a, b y c enteros positivos.

Salida: Devuelve g.

```
Hofmeister:=proc(a,b,c)
local x,y,z,w,s,t,q,r,g,n;
begin
y:=ind(a,b,c);
z:=ind(b,a,c);
w:=ind(c,a,b);
if y=1 or z=1 or w=1 then
print("no son independientes")
else
if gcd(a,b)>1 or gcd(b,c)>1 or gcd(a,c)>1 then
print("no son primos relativos")
else
x:=numlib::lincongruence(b,c,a);
s:=x[1];
```

```
t:=(s*b-c)/a;
q:=a div s;
r:=a mod s;
if (q+1)*c<(s-r)*b then
print("los números no cumplen la condición")
else
g:=max((s-1)*b+(q-1)*c,(r-1)*b+q*c)-a;
end_if;
end_if;
end_if;
end_proc;
```

Algoritmo Selmer

Determinar el número de Frobenius (g) para tres enteros positivos a, b y c primos relativos dos a dos e independientes, usando el método de Selmer y Beyer.

Entrada: a, b y c enteros positivos.

Salida: Devuelve g.

```
Selmer:=proc(a,b,c)
local x,y,z,w,q0,r0,q1,r1,q2,r2,q3,r3,num,P0,P1,P2,P3,g,n;
begin
y:=ind(a,b,c);
z:=ind(b,a,c);
w:=ind(c,a,b);
if y=1 or z=1 or w=1 then
print("no son independientes")
else
if gcd(a,b)>1 or gcd(b,c)>1 or gcd(a,c)>1 then
print("no son primos relativos")
else
```

```
x:=numlib::lincongruence(b,c,a);
s:=x[1];
q0:=a div s;
r0:=a mod s;
if (q0+1)*c>=(s-r0)*b then
Hofmeister(a,b,c);
end_if;
P0:=q0;
q1:=s div r0;
r1:=s mod r0;
P1:=q0*q1+1;
num:=float(c/a);
q3:=q1;
P:=1;
r:=s;
r2:=r0;
P2:=P0;
while float(r1/P1)>num do
q2:=r0 div r1;
r2:=r0 mod r1;
q3:=r1 div r2;
r3:=r1 mod r2;
P2:=P1*q2+P0;
P3:=P2*q3+P1;
P:=P1;
r:=r1;
q0:=q2;
r0:=r2;
q1:=q3;
```

```
r1:=r3;
P0:=P2;
P1:=P3;
end_while;
A:=[];
for i from 0 to q3-1 do
A:=[op(A),(r-(i+1)*r2)*b,(P+i*P2)*c];
g:=-a+(r2-1)*b+(P0-1)*c+op(sort(A),nops(A)/2+1);
end_for;
end_if;
end_if;
end_proc;
```

Algoritmo ADiv

Algoritmo de la división con residuos negativos.

Entrada: a, b enteros positivos.

Salida: Devuelve M.

```
ADiv:=proc(a,b)
local M;
begin
if (a mod b)=0
then M:=[(a div b),(a mod b)];
else M:=[(a div b)+1,-((a mod b)-b)];
end_if
end_proc;
```

Algoritmo Rodseth

Determinar el número de Frobenius (g) para tres enteros positivos a, b y c primos relativos dos a dos e independientes, usando el método de Rödseth.

Entrada: a, b y c enteros positivos.

Salida: Devuelve g.

```
Rodseth:=proc(a,b,c)
local x,y,z,w,S,P,Q,D,R,g,n;
begin
y:=ind(a,b,c);
z:=ind(b,a,c);
w:=ind(c,a,b);
if y=1 or z=1 or w=1 then
print("no son independientes")
else
if gcd(a,b)>1 or gcd(b,c)>1 or gcd(a,c)>1 then
print("no son primos relativos")
else
x:=numlib::lincongruence(b,c,a); /*calcula x=s_0*/
D:=ADiv(a,x[1]);
S[1]:=a;
S[2]:=x[1];
Q[1]:=0;
Q[2]:=0;
Q[3]:=D[1];
P[1]:=0;
P[2]:=1;
R[1]:=b;
R[2]:=(b*x[1]-c)/a;
i:=1;
while D[2]<>0 do
D:=ADiv(S[i],S[i+1]);
```

```
S[i+2]:=D[2];
Q[i+2]:=D[1];
P[i+2]:=Q[i+2]*P[i+1]-P[i];
R[i+2]:=Q[i+2]*R[i+1]-R[i];
i:=i+1;
end_while;
k:=1;
while (R[k]>0) do
 k:=k+1;
end_while;
v:=k-1;
g:=-a+b*(S[v]-1)+c*(P[v+1]-1)-min(b*S[v+1],c*P[v]);
end_if;
end_if;
end_proc;
```

Referencias

[1] Brauer A. and Shockley J. *On a problem of Frobenius*. J. reine angew. Math. 211 (1962), 215-220.

[2] Brown T. and Shiue P. *A remark related to the Frobenius problem*. The Fibonacci Quarterly 31(1) (1993), 32-36.

[3] Hardy G. and Wright E. *An introduction to the theory of numbers*. Sixth Edition. Oxford University Press.

[4] Hofmeister G. *Zu einem Problem von Frobenius*. Norske Videnskabers Selskabs Skrifter 5 (1966), 1-37.

[5] Jiménez L., Gordillo J. y Rubiano G. *Teoría de números [para principiantes]*. Segunda Edición. Universidad Nacional de Colombia.

[6] Palacios C. y Gómez S. *El problema de Frobenius en tres variables*.Tesis de pregrado. Universidad de Nariño (2008).

[7] Ramírez J. *El teorema de Pick y redes de puntos*. Materials Matemàtics. (2010), 1-41.

[8] Rödseth Ö. *On a linear diophantine problem of Frobenius*. J. reine angew. Math. 301 (1978), 171-178.

[9] Selmer E. *On the linear diophantine problem of Frobenius*. J. reine angew. Math. 293/294 (1977), 1-17.

[10] Selmer E. and Beyer Ö. *On the linear diophantine problem of Frobenius in three variables*. J. reine angew. Math. 301 (1978), 161-170.

[11] Sharp W. *Solution to Problem 7382*. Educational Times 37 (1884), 26; *reprinted in Mathematical questions with their solutions*. Educational Times (with additional papers and solution) 41 (1884), 21.

[12] Sylvester J. *Mathematical questions, with their solutions*. Educational Times 41 (1884), 21.

[13] Wei Y. *The Diophantine Frobenius Problem*. The Digital Enterprise Research Institute at Stanford.

Bibliografía

Brauer A. and Shockley J. *On a problem of Frobenius*. J. reine angew. Math. 211 (1962), 215-220.

Brown T. and Shiue P. *A remark related to the Frobenius problem*. The Fibonacci Quarterly 31(1) (1993), 32-36.

Hardy G. and Wright E. *An introduction to the theory of numbers*. Sixth Edition. Oxford University Press.

Hofmeister G. *Zu einem Problem von Frobenius*. Norske Videnskabers Selskabs Skrifter 5 (1966), 1-37.

Jiménez L., Gordillo J. y Rubiano G. *Teoría de números [para principiantes]*. Segunda Edición. Universidad Nacional de Colombia.

Palacios C. y Gómez S. *El problema de Frobenius en tres variables*.Tesis de pregrado. Universidad de Nariño (2008).

Ramírez J. *El teorema de Pick y redes de puntos*. Materials Matemàtics. (2010), 1-41.

Rödseth Ö. *On a linear diophantine problem of Frobenius*. J. reine angew. Math. 301 (1978), 171-178.

Selmer E. *On the linear diophantine problem of Frobenius*. J. reine angew. Math. 293/294 (1977), 1-17.

Selmer E. and Beyer Ö. *On the linear diophantine problem of Frobenius in three variables*. J. reine angew. Math. 301 (1978), 161-170.

Sharp W. *Solution to Problem 7382*. Educational Times 37 (1884), 26; *reprinted in Mathematical questions with their solutions*. Educational Times (with additional papers

and solution) 41 (1884), 21.

Sylvester J. *Mathematical questions, with their solutions*. Educational Times 41 (1884), 21.

Wei Y. *The Diophantine Frobenius Problem*. The Digital Enterprise Research Institute at Stanford.