# El problema de Frobenius en tres variables

**Claudia Mercedes Palacios de la Cruz**

**Sergio Alexander Gómez Noguera**

**Universidad de Nariño**
**Facultad de Ciencias Exactas y Naturales**
**Departamento de Matemáticas**
**Programa de Licenciatura en Matemáticas**
**San Juan de Pasto**

2008

# El problema de Frobenius en tres variables

**Claudia Mercedes Palacios de la Cruz**

**Sergio Alexander Gómez Noguera**

**Trabajo de grado presentado como requisito parcial para optar al título de Licenciado en Matemáticas**

John Hermes Castillo Gómez

Director

**Universidad de Nariño**

**Facultad de Ciencias Exactas y Naturales**

**Departamento de Matemáticas y Estadística**

**Programa de Licenciatura en Matemáticas**

**San Juan de Pasto**

2008

Nota de Aceptación:

_____

_____

_____

_____

Director.

_____

Jurado.

_____

Jurado.

San Juan de Pasto, Julio de 2008

## AGRADECIMIENTOS

En primer lugar agradecer a Dios porque soy partidario que sin el nada podemos realizar, también agradecer a mi asesor, Mg. John Castillo por la atención, el tiempo, el apoyo y la ayuda brindada para la realización de este trabajo.

Además agradecer a mi compañera de Tesis Claudia Palacios por su entera dedicación y colaboración para la realización de este trabajo, a mi familia, particularmente a mi padre Hernando Gómez, a mi madre Marina Noguera y a mis hermanos Hernán y Diego Gómez, que aunque desde lejos siempre estuvieron apoyándome a lo largo de toda mi carrera. Agradecer también a mi novia Ximena López por su paciencia y comprensión en los momentos difíciles que viví al realizar este trabajo de grado.

**SERGIO GÓMEZ**

Al culminar los estudios de Licenciatura en Matemáticas quiero agradecer de manera muy especial a mi asesor Mg. Jhon Castillo, quien con su experiencia y grandes conocimientos nos ayudó para lograr alcanzar, a carta cabal, los objetivos de este trabajo, además él con su gran calidad humana y sus consejos posibilitó de una u otra forma el cambió de mis espectativas de vida.

A mi gran amigo y compañero de trabajo Sergio mis más sentidos sentimientos de gratitud por su apoyo en la realización de este trabajo. De igual forma, a mi familia, en especial a mi padre y a mi madre, a quienes me debo como persona y quienes con su comprensión y apoyo me han permitido hacer muchos sueños realidad.

Mis agradecimientos a Felipe, quien con su amor ha sabido comprenderme, apoyarme y muchas veces me ha dado la fuerza y el valor para seguir adelante.

**CLAUDIA PALACIOS**

## DEDICATORIA

A nuestro asesor el profesor John Castillo, quien dispuso su tiempo para colaborarnos con la realización del presente trabajo, a los profesores Saulo Mosquera, Claudia Gómez y Fernando Soto por los conocimientos brindados a lo largo de la carrera y finalmente, a nuestras familias por el apoyo incondicional que nos brindaron.

CLAUDIA PALACIOS
SERGIO GÓMEZ

*UNIVERSIDAD DE NARIÑO*
Julio de 2008

**CONTENIDO**

## ÍNDICE DE FIGURAS

## RESUMEN

En el presente documento se realiza un estudio sobre un problema que recae en el interés de la teoría aditiva de números denominado el problema de Frobenius en tres variables. En este sentido se presenta un estudio detallado de los resultados conocidos acerca de este problema que permiten encontrar su solución. Además, se aborda el problema de Frobenius en conjuntos de números con propiedades particulares. Finalmente, se plantean algunas cuestiones abiertas para la investigación las cuales están relacionadas al problema de Frobenius y que pueden recaer en el intrés del lector.

## ABSTRACT

In the present document it realizes a study on a problem that is of the interest of the Number Additive Theory called The Frobenius Problem in three. In this sense, it presents a detailed study of the Knew results about this problem that permit to find its solution. Also, it takes up The Frobenius Problem in sets of numbers with special properties. Finally, it plans some open questions for the investigation which are related with The Frobenius Problem and that can be of the interest of the reader.

# INTRODUCCIÓN

El presente trabajo es un requisito parcial para optar al título de Licenciados en Matemáticas de la Universidad de Nariño, fue realizado con la asesoría del profesor John Hermes Castillo Gómez y tiene como propósito realizar un recorrido a través de algunos resultados que sa han obtenido para el cálculo del número de Frobenius en tres variables.

Este trabajo se ha organizado en cuatro capítulos que se han denominado de la siguiente manera: Preliminares, métodos para calcular $g(a, b, c)$ (número de Frobenius en tres variables), casos especiales y finalmente un capítulo denominado problemas abiertos y conclusiones.

En el primero de ellos se muestra algunas definiciones y teoremas que justifican el problema y además que serán de utilidad para el desarrollo y comprensión de los temas que se abordan en los capítulos posteriores, en el segundo se recopilan algunos de los métodos para el cálculo del número de Frobenius como son los métodos de Hofmeister, Selmer y Beyer, Rödseth, Brauer y Davison, métodos que fueron implementados en forma de algoritmos con la ayuda del sistema de álgebra computacional MuPAD y que son presentados como apéndices. En el tercer capítulo se estudia el cálculo del número de Frobenius para conjuntos de números particulares como sucesiones aritméticas, casi - sucesiones y una terna de números de Fibonacci, finalmente se considera algunos problemas estrechamente relacionados con este y que están abiertos para la investigación según sea el interés del lector.

Cabe resaltar que la mayoría de demostraciones que aquí se abordan son producción del estudio detallado que los autores realizaron de artículos los cuales se referencian al final de este documento. En algunos otros casos las demostraciones son el resultado de una transposición a un lenguaje más claro de dichos artículos.

# 1. PRELIMINARES

## 1.1. EL PROBLEMA DE FROBENIUS

El problema de Frobenius asociado al matemático Alemán Ferdinand Georg Frobenius, se utiliza como base matemática para el estudio del problema del cambio de moneda, en el cual se busca hacer cambios exactos con monedas de denominaciones específicas dado un billete o una moneda de denominación superior.

Los restaurantes McDonald de Estados Unidos venden McNuggets de pollo en cantidades de 6, 9 y 20. Sí se quiere comprar exactamente 26 o 27 McNugget, se podría hacerlo, pero no se puede comprar 25 o 28. Se puede comprar exactamente 41, pero no se puede comprar exactamente 43 McNuggets. Si se quiere comprar un número mayor que 43 se puede escoger cualquiera que sea, así 43 es el mayor número de McNuggets de pollo que no se puede comprar en cajas de 6, 9 y 20 Nuggets. Este es un caso especial del problema de Frobenius.

**1.1.1. Justificación del problema de Frobenius** En lo que sigue se denotará al máximo común divisor de dos números $a$ y $b$ como $\gcd(a, b)$. Además se debe tener en cuenta que dados $a_1, a_2, \ldots, a_k$ enteros positivos, se dice que $a_1, a_2, \ldots, a_k$ son primos relativos entre sí, si $\gcd(a_1, a_2, \ldots, a_k) = 1$. Por otro lado $a_1, a_2, \ldots, a_k$ son primos dos a dos si $\gcd(a_i, a_j) = 1$ $quad 1 \leq i, j \leq k$ con $i \neq j$.

Es esencial diferenciar entre un conjunto de enteros primos relativos y un conjunto de enteros primos dos a dos, basta con observar

**Ejemplo 1.** Dado $a_1 = 4$, $a_2 = 6$ y $a_3 = 9$ se tiene que $\gcd(4, 6, 9) = 1$ y por lo tanto $a_1, a_2$ y $a_3$ son primos relativos. Sin embargo, $\gcd(4, 6) = 2$ y por consiguiente $a_1, a_2$ y $a_k$ no son primos dos a dos.

Un resultado clásico de la teoría de números es el siguiente

**Teorema 1.1.** *Sean $a$ y $b$ enteros no ambos nulos. Entonces $a$ y $b$ son primos relativos si y sólo si existen $x$, y enteros tales que $ax + by = 1$.*

Una consecuencia de este resultado es que todo entero $n$ se puede representar como combinación lineal de $a$ y $b$ con coeficientes enteros. En efecto, para $n \in \mathbb{Z}$

$$n = n \cdot 1 = n(ax + by) = a(nx) + b(ny)$$

Un problema interesante surge cuando se restringe el dominio de $x$ y $y$ a los enteros no negativos.

**Teorema 1.2.** *Si $a$ y $b$ son enteros positivos primos relativos entre sí, entonces todo entero suficientemente grande se puede representar como combinación lineal de $a$ y $b$ con coeficientes enteros no negativos. Es decir, si $n$ es suficientemente grande, existen enteros no negativos $x$ e $y$ tales que*

$$n = ax + by \tag{1.1}$$

*Demostración.* Primero se prueba que todo entero $m > ab$ se puede representar como en la ecuación (1.1). Por el teorema 1.1 existen enteros $x'$, $y'$, tales que

$$ax' + by' = m.$$

Por lo que todas las formas de representar a $m$ como combinación lineal de $a$ y $b$ están dadas por

$$a(x' + bt) + b(y' - at) = m, \quad t \in \mathbb{Z}$$

Así pues, se necesita probar que existe un entero $t$ tal que

$$x' + bt \geq 0 \quad y \quad y' - at \geq 0$$

Lo que es equivalente a encontrar un entero $t$ tal que

$$\frac{y'}{a} \geq t \geq -\frac{x'}{b} \tag{1.2}$$

para probar la existencia de tal entero $t$ basta ver que la diferencia entre $\frac{y'}{a}$ y $-\frac{x'}{b}$ es mayor que 1. En efecto,

$$\frac{y'}{a} + \frac{x'}{b} = \frac{by' + ax'}{ab} = \frac{m}{ab} > 1$$

Por lo tanto debe existir por lo menos un entero $t$ que verifica la desigualdad (1.2). De esta forma, para todo entero suficientemente grande (en realidad todo entero mayor ó igual que $ab$), existen enteros no negativos que satisfacen la ecuación (1.1).

□

El teorema 1.2 muestra que, a partir de cierto punto todo entero se puede representar como combinación lineal de $a$ y $b$ con coeficientes enteros no negativos. Esto motiva la siguiente pregunta: ¿cuál es el mayor entero que no se puede representar como combinación lineal de $a$ y $b$ con coeficientes enteros no negativos? En otras palabras, ¿cuál es el mayor entero tal que la ecuación (1.1) no tiene solución en enteros no negativos? La respuesta a esta pregunta se presenta en el siguiente resultado.

**Teorema 1.3.** *Sean $a$ y $b$ enteros positivos primos relativos entre sí, el mayor entero $n$ que no se puede representar como combinación lineal de $a$ y $b$ con coeficientes enteros no negativos es $n = ab - a - b$.*

*Demostración.* Se comienza por probar que $N = ab - a - b$, no se puede representar como combinación lineal de $a$ y $b$ con coeficientes enteros no negativos. Supóngase que existen enteros $x$,$y \geq 0$ tales que

$$ax + by = ab - a - b$$

De donde, $a(x+1) + b(y+1) = ab$. Por lo tanto $a|y+1$ y $b|x+1$. Entonces $a \leq y+1$ y $b \leq x+1$, y de ahí que

$$ab \leq a(x+1) \qquad ab \leq b(y+1)$$

Sumando estas desigualdades

$$2ab \leq a(x+1) + b(y+1) = ab$$

lo que es una contradicción. Para completar la prueba basta con demostrar que para todo entero $m \geq ab - a - b + 1$, la ecuación (1.1) tiene solución en enteros no negativos $x$, $y$. Esto es equivalente a demostrar que para todo $r \geq 1$, existen enteros $x_0, y_0 \geq 0$, tales que

$$ax_0 + by_0 = ab - a - b + r$$

Si esto se cumple entonces $a(x_0+1)+b(y_0+1) = ab+r$. Así que es suficiente demostrar que para todo $r$ la ecuación

$$ax + by = ab + r \tag{1.3}$$

tiene solución en enteros positivos $x, y$. En la demostración del teorema 1.2 se probó que para todo entero $r \geq 1$, existen enteros $x_0, y_0 \geq 0$ tales que $ax_0 + by_0 = ab + r$. Si tanto $x_0$ como $y_0$ son mayores que cero, la demostración está completa. Si uno de los dos es cero, supóngase por ejemplo que $x_0 = 0$, entonces $by_0 = ab + r$, y esto implica que $r$ es divisible por $b$; es decir, existe un entero $t > 0$ tal que $by_0 = ab + bt$. Por lo tanto

$$by_0 = b(a+t) = ab + r$$

En consecuencia, para todo entero $r \geq 1$, $n = ab + r$ es una combinación lineal con coeficientes enteros positivos de $a$ y $b$. Esto completa la demostración. □

### 1.1.2. El problema general

**Lema 1.1.** *Sea $A = \{a_1, a_2, \ldots, a_k\}$ un conjunto de enteros positivos primos relativos entre sí, tales que $a_1 \leq a_2 \leq \cdots \leq a_k$ y sea*

$$S_k = S(a_1, a_2, \ldots, a_k) = a_2 + a_3 + \cdots + a_{k-1} + a_1 a_k.$$

*Entonces, para $n > S_k$ existen enteros positivos $x_1, x_2, \ldots, x_k$, tales que*

$$n = a_1 x_1 + a_2 x_2 + \cdots + a_k x_k. \tag{1.4}$$

*Demostración.* Se utiliza inducción sobre $k$, el número de elementos del conjunto $A$. En el caso $k = 2$, sea $n = a_1a_2 + r$ con $r > 0$. Como $\gcd(a_1, a_2) = 1$, existe un entero $1 \leq x_1 \leq a_2$, tal que $a_1x_1 \equiv r \,\text{mód}\, a_2$. Como $r = n - a_1a_2$ se tiene $a_1x_1 \equiv n - a_1a_2 \,\text{mód}\, a_2$, luego $a_1x_1 \equiv n \,\text{mód}\, a_2$ así existe $x_2$ tal que $x_2|n - a_1x_1$ de allí

$$x_2 = \frac{n - a_1x_1}{a_2}$$

es un entero positivo. Luego $n = a_1x_1 + a_2x_2$, y en consecuencia todo entero $n > S(a_1, a_2) = a_1a_2$, se puede representar como combinación lineal de $a_1$ y $a_2$ con coeficientes positivos.

Ahora supóngase que $k \geq 3$ y que el resultado del lema se cumple para conjuntos de $k - 1$ enteros positivos primos relativos entre sí. Considérese un conjunto de $k$ enteros positivos primos relativos entre sí, $A = \{a_1 \leq a_2 \leq \cdots \leq a_k\}$. Si $d = \gcd(a_1, a_3, \ldots, a_k)$, entonces $\gcd(a_2, d) = 1$. De esta forma, para cada entero $n$ la congruencia

$$n \equiv a_2x \,\text{mód}\, d$$

tiene solución. Es decir, para cada entero $n$, existe un entero $1 \leq x_2 \leq d$, tal que $d|(n - a_2x_2)$.
Sea $A' = \left\{\frac{a_1}{d}, \frac{a_3}{d}, \cdots, \frac{a_k}{d}\right\}$. Nótese que $\gcd\left(\frac{a_1}{d}, \frac{a_3}{d}, \cdots, \frac{a_k}{d}\right) = 1$. Por la hipótesis de inducción, si

$$\frac{n - a_2x_2}{d} > \frac{a_3}{d} + \frac{a_4}{d} + \cdots + \frac{a_{k-1}}{d} + \frac{a_1a_k}{d^2}$$

existen enteros positivos $x_1, x_3, \ldots, x_k$ tales que

$$\frac{n - a_2x_2}{d} = \frac{a_1}{d}x_1 + \frac{a_3}{d}x_3 + \cdots + \frac{a_k}{d}x_k$$

Es decir, si

$$n > a_2x_2 + a_3 + a_4 + \cdots + a_{k-1} + \frac{a_1a_k}{d}$$

existen enteros positivos $x_1, x_3, \ldots, x_k$, tales que

$$n = a_1x_1 + a_2x_2 + \cdots + a_kx_k.$$

Ahora como $1 \leq x_2 \leq d$, y $a_1 \geq 0$ entonces, todo entero $n > a_2d + a_3 + \cdots + a_{k-1} + \frac{a_1a_k}{d}$ se puede representar como combinación lineal de $a_1, a_2, \ldots, a_k$ con coeficientes positivos. Sea $S_d = a_2d + a_3 + \cdots + a_{k-1} + \frac{a_1a_k}{d}$. Para completar la inducción basta con demostrar que $S_d \leq S$. Esto se verifica, pues se tiene que

$$\begin{aligned} S - S_d &= a_2(1 - d) + a_1a_k\frac{d - 1}{d} \\ &= (d - 1)(\frac{a_1a_k}{d} - a_2) \\ &\geq (d - 1)(a_k - a_2) \geq 0 \end{aligned}$$

□

**Teorema 1.4.** *Dado un conjunto de enteros positivos primos relativos entre sí,* $A = \{a_1, a_2, \ldots, a_k\}$ *entonces, todo entero suficientemente grande se puede representar como combinación lineal de* $a_1, a_2, \ldots, a_k$ *con coeficientes enteros no negativos.*

*Demostración.* Sin pérdida de generalidad se puede suponer que $a_1 \leq a_2 \leq \cdots \leq a_k$. Del lema 1.1, se tiene que todo $n > a_2 + a_3 + \cdots + a_{k-1} + a_1 a_k$ se puede representar como una combinación lineal de $a_1, a_2, \ldots, a_k$ con $x_i > 0, \quad i = 1, \ldots, k$, es decir $n = a_1 x_1 + a_2 x_2 + \cdots + a_k x_k$. De esta manera para todo $r > 0$ se tiene que

$$n = a_2 + a_3 + \cdots + a_1 a_k + r = a_1 x_1 + a_2 x_2 + \cdots + a_k x_k, \qquad x_i > 0, i = 1, \ldots, k$$

luego

$$n = a_2 + a_3 + \cdots + a_1 a_k + r - a_1 - a_2 - \cdots - a_k = a_1(x_1 - 1) + a_2(x_2 - 1) + \cdots + a_k(x_k - 1)$$

Sea ahora $y_i = x_i - 1 \geq 0, \quad , i = 1, \ldots, k$ así

$$n = a_1 a_k - a_1 - a_k + r = a_1 y_1 + a_2 y_2 + \cdots + a_k y_k, \qquad y_i \geq 0, i = 1, \ldots, k$$

de donde para todo $n \geq a_1 a_k - a_1 - a_k + 1 = (a_1 - 1)(a_k - 1)$ se tiene que $n$ se puede expresar como combinación lineal de $a_1, a_2, \ldots, a_k$ con coeficientes enteros no negativos, lo que termina la demostración. □

El teorema anterior justifica que se plantee el siguiente problema, dados $a_1, a_2, \ldots, a_k$ enteros positivos primos relativos entre sí, ¿Cuál es el mayor entero que no se puede representar como una combinación lineal con coeficientes enteros no negativos de $a_1, a_2, \ldots, a_k$? Este problema se conoce con el Problema de Frobenius, en honor del matemático alemán *Ferdinand Georg Frobenius (1849-1917)* quien parece ser mencionó repetidamente el problema en sus conferencias.

**Definición 1.1.** *Dado un conjunto de enteros positivos primos relativos entre sí* $A = \{a_1, a_2, \ldots a_k\}$*, se dice que el entero* $n$ *es representable por* $a_1, a_2, \ldots, a_k$ *(o simplemente representable por A) si existen enteros no negativos* $m_1, m_2, \ldots, m_k$ *tales que*

$$n = m_1 a_1 + m_2 a_2 + \cdots + m_k a_k \tag{1.5}$$

El *problema de Frobenius* consiste en encontrar el mayor entero que no es representable por $A$. Este número se denomina el **número de Frobenius de** $A$**,** y se le denota por $g(a_1, a_2, \ldots, a_k)$ ó $g(A)$.

**1.1.3. Resultados Generales** El caso particular de un par de enteros primos relativos $a_1, a_2$ fue resuelto, según Selmer [1] por *J.J Silvester* en 1884. Sin embargo, cuando el número de enteros primos relativos crece el problema se hace más difícil. El caso de tres

[1] SELMER, Ernst. (1977) *On the linear Diophantine problem of Frobenius.*

enteros primos relativos entre sí fue resuelto por Selmer y Beyer en 1978[2], utilizando un algoritmo de fracciones continuas.
Del teorema 1.3 se tiene que para $k = 2$

$$g(a_1, a_2) = a_1a_2 - a_1 - a_2 = (a_1 - 1)(a_2 - 1) - 1 \tag{1.6}$$

Y de la demostración de teorema 1.4 se tiene que sí $a_1 \leq a_2 \leq \cdots \leq a_k$ entonces

$$g(a_1, a_2, \ldots, a_k) \leq (a_1 - 1)(a_k - 1) - 1 \tag{1.7}$$

**Lema 1.2.** *Sean $a_1, a_2, \ldots, a_k$ enteros positivos primos relativos entre sí. Si existe $1 \leq j \leq k$ tal que $a_j$ es representable como combinación lineal de los otros $a_i$ con coeficientes enteros no negativos entonces*

$$g(a_1, a_2, \ldots, a_k) = g(a_1, \ldots, a_{j-1}, a_{j+1}, \ldots, a_k)$$

*Demostración.* Sea $t = g(a_1, a_2, \ldots, a_k)$, se requiere probar que $t = g(a_1, \ldots, a_{j-1}, a_{j+1}, \ldots, a_k)$. Para este fin es necesario demostrar

1. Que para todo $r \in \mathbb{Z}^+$, $t + r$ es representable por $a_1, \ldots, a_{j-1}, a_{j+1}, \ldots, a_k$.

   En este sentido, si existe $j$ tal que $a_j$ es representable por los $a_i$ con $i \neq j$, entonces toda combinación lineal de los $a_i$ con coeficientes enteros no negativos se puede expresar como una combinación lineal solamente de $a_1, \ldots, a_{j-1}, a_{j+1}, \ldots, a_k$ con coeficientes no negativos.

2. Que $t$ no es representable por $a_1, \ldots, a_{j-1}, a_{j+1}, \ldots, a_k$.

   Supóngase que $t$ es representable por $a_1, \ldots, a_{j-1}, a_{j+1}, \ldots, a_k$, luego

   $$t = a_1x_1 + \cdots + a_{j-1}x_{j-1} + a_{j+1}x_{j+1} + \cdots + a_kx_k$$

   con $x_i$ enteros no negativos e $1 \leq i \leq k, \quad i \neq j$. De esta manera

   $$t = a_1x_1 + \cdots + a_{j-1}x_{j-1} + a_jx_j + a_{j+1}x_{j+1} + \cdots + a_kx_k$$

   con $x_j = 0$, así $t$ es representable por $a_1, a_2, \ldots, a_k$ lo que es una contradicción puesto que $t = g(a_1, a_2, \ldots, a_k)$.

De (1) y (2)

$$g(a_1, \ldots, a_{j-1}, a_{j+1}, \ldots, a_k) = g(a_1, \ldots, a_k)$$

Que era lo que se quería demostrar. □

[2]BEYER, Öyvind. SELMER, Ernst. (1978) *On the linear Diophantine problem of Frobenius in three variables.*

Del lema 1.2 se sigue que el problema de calcular $g(a_1, a_2, \ldots, a_k)$ se puede reducir a calcular el número de Frobenius de $k-1$ elementos siempre que exista $1 \leq j \leq k$ talque $a_j$ sea representable por los $a_i$ con $i \neq j$.

Sea $f(a_1, a_2, \ldots, a_k)$ el mayor entero que no es una combinación lineal de $a_1, a_2, \ldots, a_k$ con coeficientes enteros positivos. De las definiciones de $f$ y $g$ se tiene que

$$g(a_1, a_2, \ldots, a_k) = f(a_1, a_2, \ldots, a_k) - a_1 - a_2 - \cdots - a_k$$

De la igualdad (1.6) y la desigualdad (1.7) se tiene que

$$f(a_1, a_2) = a_1 a_2 \tag{1.8}$$

$$f(a_1, a_2, \ldots, a_k) \leq a_2 + a_3 + \cdots + a_{k-1} + a_1 a_k \tag{1.9}$$

La importancia de definir $f$ se verá reflejada en los siguientes resultados pues a partir de $f$ se puede caracterizar el número de Frobenius y obtener propiedades que serán fundamentales en lo que sigue.

**Teorema 1.5.** *Sean $a_1, a_2, \ldots, a_k$ enteros positivos primos relativos entre sí, entonces*

$$f(a_1, a_2, \ldots, a_k) = \sum_{i=2}^{k} x_i a_i$$

*para ciertos enteros positivos $x_2, x_3, \ldots, x_k$.*

*Demostración.* De la definición de $f(a_1, a_2, \ldots, a_k)$ se tiene que

$$f(a_1, a_2, \ldots, a_k) < a_1 + f(a_1, a_2, \ldots, a_k) = a_1 x_1 + \sum_{i=2}^{k} a_i x_i$$

con $x_i > 0$ luego $f(a_1, a_2, \ldots, a_k) = a_1(x_1 - 1) + \sum_{i=2}^{k} a_i x_i$ y de la definición de $f(a_1, a_2, \ldots, a_k)$ se tiene que $x_1 = 1$ y por tanto $f(a_1, a_2, \ldots, a_k) = \sum_{i=2}^{k} x_i a_i$. □

**Lema 1.3.** *Sean $a_1, a_2, \ldots, a_k$ enteros positivos primos relativos entre sí. Si $d$ es un divisor común de $a_2, \ldots, a_k$, entonces*

$$f(a_1, a_2, \ldots, a_k) = df\left(a_1, \frac{a_2}{d}, \frac{a_3}{d}, \ldots, \frac{a_k}{d}\right)$$

*Demostración.* Sean $a_i = da_i'$, $i = 2, \ldots, k$ y $f(a_1, a_2, \ldots, a_k) = N$. Por el teorema 1.5

$$N = \sum_{i=2}^{k} x_i a_i = d \sum_{i=2}^{k} x_i a_i' \qquad (x_i > 0)$$

Así $N$ es divisible por $d$; es decir, $N = dN'$, con $N' = \sum_{i=2}^{k} a_i' x_i$. Para terminar la demostración basta probar que $N' = f(a_1, a_2', \ldots, a_k')$. Se prueba primero que $N'$ no se puede expresar como una combinación lineal de $a_1, a_2', \ldots, a_k'$ con coeficientes enteros positivos. Supóngase lo contrario; es decir, que existen enteros positivos $y_i$ tales que

$$N' = y_1 a_1 + \sum_{i=2}^{k} y_i a_i' \qquad (y_i > 0)$$

entonces

$$f(a_1, a_2, \ldots, a_k) = N = dN' = (y_1 d)a_1 + \sum_{i=2}^{k} y_i a_i \qquad (y_i > 0)$$

lo que lleva a una contradicción.

Ahora se prueba que si $n > N'$, entonces $n$ se puede expresar como combinación lineal de $a_1, a_2', \ldots, a_k'$ con coeficientes enteros positivos. En efecto, pues

$$nd > N'd = N$$

entonces $nd$ se puede expresar como

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

luego

$$nd = z_1 a_1 + d \sum_{i=2}^{k} z_i a_i' \qquad (z_i > 0)$$

Ahora multiplicando por $\dfrac{1}{d}$ a ambos lados se tiene

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

Dado que $n \in \mathbb{Z}$ se tiene que $t = \dfrac{z_1 a_1}{d} \in \mathbb{Z}$, y por hipótesis $d \nmid a_1$ luego $d$ divide a $z_1$. Sea $z_1 = dz_1'$, entonces

$$n = z_1' a_1 + \sum_{i=2}^{K} z_i a_i'$$

Por lo tanto, $N' = f(a_1, a_2', \ldots, a_k')$ □

**Lema 1.4.** *Sean $a_1, a_2, \ldots, a_k$ enteros positivos primos relativos entre sí. Si existe $1 \leq j \leq k$ tal que $a_j$ es representable como combinación lineal de los otros $a_i$ con coeficientes no negativos entonces*

$$f(a_1, a_2, \ldots, a_k) = f(a_1, \ldots, a_{j-1}, a_{j+1}, \ldots, a_k) + a_j$$

*Demostración.* Del lema 1.2 se tiene

$$g(a_1, \ldots, a_{j-1}, a_{j+1}, \ldots, a_k) = g(a_1, \ldots, a_k)$$

y por lo tanto,

$$\begin{aligned} f(a_1, a_2, \ldots, a_k) &= g(a_1, \ldots, a_k) + a_1 + a_2 + \cdots + a_k \\ &= g(a_1, \ldots, a_{j-1}, a_{j+1}, \ldots, a_k) + a_1 + a_2 + \cdots + a_k \\ &= f(a_1, \ldots, a_{j-1}, a_{j+1}, \ldots, a_k) + a_j \end{aligned}$$

□

De los lemas 1.3 y 1.4 se sigue que el problema de calcular $f(a_1, \ldots, a_k)$ se puede reducir al caso en el que cada subconjunto de $k-1$ números de $a_1, a_2, \ldots, a_k$ son primos relativos entre sí y ninguno de los $a_j$ es una combinación lineal de los $a_i$ restantes con coeficientes no negativos.

**Definición 1.2.** *Se dice que un conjunto de $n$ enteros $a_1, a_2, \ldots, a_n$, forma un sistema completo de residuos módulo $n$ si cada uno de ellos es congruente módulo $n$ a algún $t \in \{0, 1, 2, \ldots, n-1\}$ y que cada pareja de ellos sea incongruente módulo $n$.*

**Definición 1.3.** *Un sistema completo de residuos módulo $n$ se dice minimal si esta conformado por los residuos positivos más pequeños módulo $n$.*

A continuación se obtiene un resultado que proporciona los fundamentos necesarios para construir un algoritmo que permite calcular el número de Frobenius de un conjunto de enteros positivos primos relativos entre sí. Dado, $A = \{a_1, a_2, \ldots, a_k\}$. Cada clase residual módulo $a_1$ contiene números representables por $a_2, a_3, \ldots, a_k$. En cada una de estas clases residuales se escoge el menor entero positivo representable por $a_2, a_3, \ldots, a_k$. Se denota este entero por $t_l$, donde $t_l \equiv l \pmod{a_1}$, y por $w$ se denota el máximo de estos números. Es decir

$$t_l = \text{mín}\,\{n = x_2a_2 + x_3a_3 + \cdots + x_ka_k : x_i \geq 0, n \equiv l \pmod{a_1}\}.$$

$$w = \max_{1 \leq l \leq a_1 - 1} t_l$$

De esta manera los $t_l, \quad 0 \leq l \leq a_1 - 1$ forman un sitema completo minimal de residuos módulo $a_1$.

Se puede ver que si $N \equiv 0 \pmod{a_1}$, entonces $N$ es representable por $a_1, a_2, \ldots, a_k$. El siguiente lema presenta una manera de caracterizar a los enteros que son representables por $a_1, a_2, \ldots, a_k$ a partir de los $t_l$.

**Lema 1.5.** *Sean $a_1, a_2, \ldots, a_k$ enteros positivos primos relativos entre sí. Sea $N \equiv l \not\equiv 0 \pmod{a_1}$. Entonces $N$ es representable por $a_1, a_2, \ldots, a_k$ si y solo sí $N \geq t_l$.*

*Demostración.* Supóngase que $N$ tiene una representación por $a_1, a_2, \ldots, a_k$; es decir que existen enteros no negativos $x_i$ tales que

$$N = x_1a_1 + x_2a_2 + \cdots + x_ka_k$$

entonces $N - x_1a_1$ tiene una representación por $a_2, \ldots, a_k$, y por definición de $t_l$

$$N \geq N - x_1a_1 \geq t_l.$$

Por otra parte si $N \geq t_l$ y como $t_l \equiv l$ mód $a_1$, entonces existe un entero positivo $m$ tal que $N = t_l + a_1m$, de donde $N$ tiene una representación por $a_1, a_2, \ldots, a_k$. □

**Teorema 1.6.** *Sean $a_1, a_2, \ldots, a_k$ enteros positivos primos relativos entre sí. Para cada entero $l = 0, \ldots, a_1 - 1$, por $t_l$ se denota el menor entero positivo congruente con $l$ módulo $a_1$ que es representable por $a_2, \ldots, a_k$, entonces*

$$g(a_1, a_2, \ldots, a_k) = w - a_1.$$

*Demostración.* Sea $w = \max t_l$, de donde $w = t_s$ para algún $0 \leq s \leq a_1 - 1$. Supóngase que $w - a_1$ es representable por $a_1, \ldots, a_k$; es decir, existen enteros $x_i \geq 0, \quad 1 \leq i \leq k$, para los cuales

$$w - a_1 = x_1a_1 + x_2a_2 + \cdots + x_ka_k$$

lo que implica que $w - (x_1 + 1)a_1 = x_2a_2 + \cdots + x_ka_k \leq w - a_1 < w$, así $w - (x_1 + 1)a_1$ es un entero menor que $w = t_s$, representable por $a_2, \ldots, a_k$ y además congruente con $w = t_s$ módulo $a_1$, lo que contradice la escogencia de $t_s$, pues $t_s$ es el menor entero representable por $a_2, \ldots, a_k$ en su clase residual. Por lo tanto tal representación no puede existir, y esto implica que $g(a_1, \ldots, a_k) \geq w - a_1$.

Para probar que $g(a_1, a_2, \ldots, a_k) = w - a_1$, basta con demostrar que si $N > w - a_1$, $N$ tiene una representación por $a_1, a_2, \ldots, a_k$. Sea $N \equiv l$ mód $a_1$, si $N > w - a_1$, entonces $N \geq t_l - a_1$. Supóngase que $N$ no es representable por $a_1, a_2, \ldots, a_k$. Del lema anterior $N < t_l$. Entonces existe un entero $m > 0$ tal que

$$t_l = N + ma_1.$$

Ahora como $N + a_1 \geq t_l$ entonces $m = 1$. Esto implica que $w \geq t_l = N + a_1$. De donde $w - a_1 \geq N$, lo que es claramente una contradicción. En conclusión todo entero mayor que $w - a_1$ es representable por $a_1, a_2, \ldots, a_k$. □

**Definición 1.4.** *Sea $A = \{a_1, a_2, \ldots, a_k\}$ un conjunto de enteros positivos primos relativos entre sí. Se dice que $A$ es un conjunto independiente si ningún $a_i, \quad 1 \leq i \leq k$ es representable por los demás elementos de $A$.*

**Teorema 1.7.** *Si $A = \{a_1, a_2, \ldots, a_k\}$ es un conjunto independiente entonces $k \leq \min a_i$.*

*Demostración.* Sin pérdida de generalidad sea $a_1 = \min\limits_{1\leq i\leq k} a_i$. Supóngase que $k \geq a_1 + 1$, así el número de elementos de $a_2, a_3, \ldots, a_k$ es al menos $a_1$. De esta manera en este listado podrían haber $a_1$ elementos incongruentes módulo $a_1$ o en caso contrario debe haber por lo menos un par de ellos congruentes módulo $a_1$. En el primer caso se debe cumplir que existe $i \geq 2$ tal que $a_i \equiv 0$ mód $a_1$ y por lo tanto $a_i = ka_1$, contradiciendo el supuesto de independencia del conjunto. En el segundo caso debe ocurrir que existen $i, j \geq 2$ tales que $a_i \equiv a_j$ mód $a_1$ con $a_i \geq a_j$ y entonces $a_i = a_j + ta_1$ con $t \geq 0$ que contradice nuevamente el supuesto de independencia del conjunto. Por lo tanto $k \leq a_1 = \min a_i$. □

## 1.2. FRACCIONES CONTINUAS

Una *Fracción Continua* es una expresión de la forma,

$$a_1 + \cfrac{b_1}{a_2 + \cfrac{b_2}{a_3 + \cfrac{b_3}{a_4 + \cdots}}}$$

donde los $a_i$ y $b_i$ son números reales o complejos. Si todos los $b_i$ son 1, $a_1$ es un entero arbitrario y todos los $a_i$ con $i \geq 2$ son enteros positivos, se dice que la fracción es una *Fracción Continua Simple*; es decir, una fracción continua simple tiene la forma,

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cdots}}}$$

donde $a_1$ es entero y $a_i > 0$ para $i \geq 2$.

Los números $a_i$ en una fracción continua simple se llaman los términos de la fracción. Si el número de términos de una fracción continua simple es finito, se dice que la fracción es una *Fracción Continua Simple Finita* y esta representa un número racional. Si el número de términos es infinito, se dice que la fracción es una *Fracción Continua Simple Infinita*.

En adelante, cuando se hable de *Fracciones Continuas* se asumirá que son *Fracciones Continuas Simples*.

**1.2.1. Fracciones continuas finitas** La fracción continua simple finita,

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}}$$

se representa con la notación $[a_1, a_2, \ldots, a_n]$ y es un número racional que se obtiene efectuando las operaciones indicadas. El recíproco de esta afirmación también es cierto y se verá en el siguiente resultado.

**Teorema 1.8.** *Todo número racional se puede expresar como una fracción continua simple finita.*

*Demostración.* Sea $r = \frac{p}{q}$ un número racional con $q > 0$. Aplicando repetidamente el algoritmo de la división se tiene

$$\begin{aligned}
p &= qa_1 + r_1, && 0 < r_1 < q \\
q &= r_1a_2 + r_2, && 0 < r_2 < r_1 \\
r_1 &= r_2a_3 + r_3, && 0 < r_3 < r_2 \\
&\vdots && \vdots \\
r_{n-3} &= r_{n-2}a_{n-1} + r_{n-1}, && 0 < r_{n-1} < r_{n-2} \\
r_{n-2} &= r_{n-1}a_n + r_n && \text{con} \quad r_n = 0
\end{aligned}$$

Como los residuos $r_1, r_2, \ldots$ forman una sucesión decreciente de enteros positivos menores que $q$, el proceso debe terminarse en un número finito de pasos con un residuo $r_n = 0$ como se ha indicado.

Las ecuaciones anteriores pueden escribirse en la forma

$$\begin{aligned}
\frac{p}{q} &= a_1 + \frac{r_1}{q} = a_1 + \frac{1}{\frac{q}{r_1}} \\
\frac{q}{r_1} &= a_2 + \frac{r_2}{r_1} = a_2 + \frac{1}{\frac{r_1}{r_2}} \\
\frac{r_1}{r_2} &= a_3 + \frac{r_3}{r_2} = a_3 + \frac{1}{\frac{r_2}{r_3}} \\
&\vdots \\
\frac{r_{n-3}}{r_{n-2}} &= a_{n-1} + \frac{r_{n-1}}{r_{n-2}} = a_{n-1} + \frac{1}{\frac{r_{n-2}}{r_{n-1}}} \\
\frac{r_{n-2}}{r_{n-1}} &= a_n
\end{aligned}$$

y por sustituciones sucesivas se obtiene

$$\begin{aligned}\frac{p}{q} &= a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}} \\ &= [a_1, a_2. \ldots, a_n]\end{aligned}$$

□

En general todo número racional puede expresarse como una fracción continua simple finita de dos formas diferentes. En efecto, si $\frac{p}{q} = [a_1, a_2, \ldots, a_n]$ con $a_n > 1$, escribiendo el último término $a_n$ en la forma $a_n = (a_n - 1) + 1$ se tiene

$$\frac{p}{q} = [a_1, a_2, \ldots, a_n] = [a_1, a_2, \ldots, a_{n-1}, a_n - 1, 1],$$

y si $a_n = 1$, se puede escribir

$$a_{n-1} + \frac{1}{a_n} = a_{n-1} + \frac{1}{1} = a_{n-1} + 1$$

y por lo tanto

$$\frac{p}{q} = [a_1, a_2, \ldots, a_n] = [a_1, a_2, \ldots, a_{n-2}, a_{n-1} + 1].$$

El razonamiento anterior también muestra que si una representación de un número racional como fracción continua finita tiene un número par de términos, su otra representación tiene un número impar de términos.

**1.2.2. Convergentes** Dada una fracción continua simple $[a_1, a_2, \ldots]$, que puede ser finita o infinita, se define sus *convergentes* o *reducidas* como los números racionales $C_i = [a_1, a_2, \ldots, a_{i-1}, a_i]$ donde $i = 1, 2, 3, \ldots$

**Ejemplo 2.** Considérese la fracción continua finita $[2, 4, 1, 6]$. Sus convergentes son

$$C_1 = [2] = 2$$
$$C_2 = [2, 4] = 2 + \frac{1}{4} = \frac{9}{4}$$
$$C_3 = [2, 4, 1] = 2 + \frac{1}{4 + \frac{1}{1}} = \frac{11}{5}$$
$$C_4 = [2, 4, 1, 6] = 2 + \frac{1}{4 + \frac{1}{1 + \frac{1}{6}}} = \frac{75}{6}$$

**Teorema 1.9.** *Sea* $C_n = \dfrac{P_n}{q_n}$ *la convergente n-ésima de una fracción continua simple* $[a_1, a_2, \ldots]$. *Se define además* $P_0 = 1$, $q_0 = 0$, $P_{-1} = 0$ *y* $q_{-1} = 1$. *Entonces se tienen las fórmulas de recurrencia*

$$\begin{aligned} P_n &= a_n P_{n-1} + P_{n-2} \\ q_n &= a_n q_{n-1} + q_{n-2} \end{aligned} \tag{1.10}$$

*válidas para todo* $n \geq 1$.

*Demostración.* La demostración es por inducción sobre $n$. Si $n = 1$ las fórmulas (1.10) se transforman en

$$P_1 = a_1 \cdot 1 + 0 = a_1$$
$$q_1 = a_1 \cdot 0 + 1 = 1,$$

luego $C_1 = \dfrac{P_1}{q_1} = a_1 = [a_1]$ como se requiere.

Supóngase ahora que el resultado es cierto para $n = k$ y cualquier fracción continua. Se tiene

$$C_{k+1} = [a_1, a_2, \ldots, a_k, a_{k+1}] = \left[a_1, a_2, \ldots, a_{k-1}, a_k + \frac{1}{a_{k+1}}\right]$$

y por la hipótesis de inducción

$$\begin{aligned} C_{k+1} &= \frac{\left(a_k + \dfrac{1}{a_{k+1}}\right) P_{k-1} + P_{k-2}}{\left(a_k + \dfrac{1}{a_{k+1}}\right) q_{k-1} + q_{k-2}} \\ &= \frac{a_{k+1}(a_k P_{k-1} + P_{k-2}) + P_{k-1}}{a_{k+1}(a_k q_{k-1} + q_{k-2}) + q_{k-1}} \\ &= \frac{a_{k+1} P_k + P_{k-1}}{a_{k+1} q_k + q_{k-1}} \end{aligned}$$

En consecuencia

$$P_{k+1} = a_{k+1}P_k + P_{k-1}$$
$$q_{k+1} = a_{k+1}q_k + q_{k-1}$$

Por lo tanto, las fórmulas (1.10) son válidas para todo entero $n \geq 1$. □

**Teorema 1.10.** *Sea* $C_n = \dfrac{P_n}{q_n}$ *la convergente n-ésima de la fracción continua simple* $[a_1, a_2, \ldots]$, *entonces*

$$P_n q_{n-1} - P_{n-1}q_n = (-1)^n \tag{1.11}$$

*para todo* $n \geq 1$.

*Demostración.* La demostración es por inducción sobre $n$. Si $n = 1$ se tiene

$$P_1q_0 - P_0q_1 = a_1 \cdot 0 - 1 \cdot 1 = (-1) = (-1)^1$$

puesto que $P_1 = a_1$, $q_1 = 1$ y por definición $P_0 = 1$ y $q_0 = 0$.

Supóngase que el resultado es cierto para $n = k$. Por las fórmulas (1.10) se tiene

$$\begin{aligned} P_{k+1}q_k - P_kq_{k+1} =& (a_{k+1}P_k + P_{k-1})q_k - P_k(a_{k+1}q_k + q_{k-1}) \\ =& -(P_kq_{k-1} - P_{k-1}q_k) \\ =& -(-1)^k = (-1)^{k+1} \end{aligned}$$

y por el principio de inducción matemática, la ecuación (1.11) es cierta para todo $n \geq 1$. □

**Corolario 1.1.** *Para todo* $n \geq 2$

$$C_n - C_{n-1} = \frac{(-1)^n}{q_nq_{n-1}} \tag{1.12}$$

*Demostración.* Dividiendo (1.11) por $q_nq_{n-1}$ se tiene el resultado deseado. □

**Corolario 1.2.** *Para todo* $n \geq 1$, $(P_n, q_n) = 1$.

*Demostración.* De (1.11) se sigue que

$$P_n\frac{q_{n-1}}{(-1)^n} + q_n\frac{P_{n-1}}{(-1)^{n+1}} = 1$$

y por el teorema 1.1 $(P_n, q_n) = 1$. □

**Teorema 1.11.** *Sea* $C_n = \dfrac{P_n}{q_n}$ *la convergente n-ésima de la fracción continua simple* $[a_1, a_2, \ldots]$, *entonces*

$$P_nq_{n-2} - P_{n-2}q_n = (-1)^{n-1}a_n$$

*para todo* $n \geq 1$.

*Demostración.* Para $n \geq 1$, por las fórmulas de recurrencia y el teorema 1.10 se tiene

$$\begin{aligned} P_n q_{n-2} - P_{n-2} q_n =& (a_n P_{n-1} + P_{n-2}) q_{n-2} - P_{n-2}(a_n q_{n-1} + q_{n-2}) \\ =& a_n (P_{n-1} q_{n-2} - P_{n-2} q_{n-1}) \\ =& a_n (-1)^{n-1}. \end{aligned}$$

□

Dividiendo por $q_n q_{n-2}$ se tiene el siguiente corolario.

**Corolario 1.3.** *Para todo $n \geq 3$,*

$$C_n - C_{n-2} = \frac{(-1)^{n-1} a_n}{q_n q_{n-2}} \tag{1.13}$$

**Teorema 1.12.** *Si $C_n = \dfrac{P_n}{q_n}$ es la convergente n-ésima de la fracción continua simple $[a_1, a_2, \ldots]$, entonces para todo $n \geq 1$*

$$q_n \geq q_{n-1}$$

*y la desigualdad es estricta para $n > 1$.*

*Demostración.* Si $n = 1$ la desigualdad se reduce a $q_1 \geq q_0 = 1$ que es verdadera puesto que $q_1 = 1$. Usando el Teorema 1.9 y observando que $a_k \geq 1$, se tiene

$$q_k = a_k q_{k-1} + q_{k-2} \geq q_{k-1} + q_{k-2} > q_{k-1}.$$

Por lo tanto el resultado es cierto para todo entero positivo $n \geq 1$. □

**Corolario 1.4.** *Para todo $n \geq 1, q_n \geq n$.*

*Demostración.* Como $q_0 = 1$, el resultado es consecuencia de la desigualdad estricta. □

**Teorema 1.13.** *Las convergentes $C_n$ de una fracción continua simple satisfacen las desigualdades*

$$C_1 < C_3 < C_5 < \cdots,$$
$$C_2 > C_4 > C_6 > \cdots.$$

*Además toda convergente de subíndice impar es menor que toda convergente de subíndice par.*

*Demostración.* Si $n \geq 3$ y $n$ es un entero impar, el lado derecho de la ecuación (1.13) es positivo y por lo tanto las convergentes impares forman una sucesión creciente. En forma similar se ve que las convergentes pares forman una sucesión decreciente.

Por el corolario 1.1 se tiene que

$$C_n - C_{n-1} = \frac{(-1)^n}{q_n q_{n-1}}, \text{para} \quad n \geq 2$$

tomando $n = 2k$ se tiene

$$C_{2k} - C_{2k-1} = \frac{1}{q_{2k} q_{2k-1}} > 0,$$

luego

$$C_{2k} > C_{2k-1} \quad \text{para todo} \quad k \geq 1. \tag{1.14}$$

Sean ahora $r$ y $s$ enteros positivos tales que $r$ sea par y $s$ impar. Se pueden presentar dos casos

1. Si $r > s$. Como $r$ es par, se tiene $r = 2k$ para algún $k \in \mathbb{Z}^+$ luego $s \in \{1, 3, 5, \ldots, 2k-1\}$ entonces

$$C_r = C_{2k} > C_{2k-1} \geq C_s.$$

2. Si $r < s$ con $s \geq 3$. Como $s$ es impar, se tiene $s = 2t + 1$ para algún $t \in \mathbb{Z}^+$ luego $r \in \{2, 4, 6, \ldots, 2t\}$ así

$$C_r \geq C_{2t} > c_{2t+2} > C_{2t+1} = C_s$$

De 1 y 2 se concluye que toda convergente impar es menor que toda convergente par. □

## 2. MÉTODOS PARA CALCULAR EL NÚMERO DE FROBENIUS

En lo que sigue se presentarán de forma detallada algunos métodos para encontrar el número de Frobenius en tres variables. Estos métodos fueron presentados por algunos matemáticos como: *Hofmeister*, *Selmer*, *Beyer*, *Rödseth*, *Brauer* y *Davison*. Sin embargo, en ninguno de ellos se obtiene una fórmula simple para el cálculo de dicho número. En efecto, todos se reducen a la aplicación del teorema 1.6.

Dado un conjunto $A = \{a_1, a_2, \ldots, a_k\}$ de enteros positivos primos relativos entre sí, el método de Hofmeister[1] consiste en la construcción de un sistema completo de residuos módulo $a_1$, para calcular 1.6.

Selmer y Beyer[2] hicieron una extensión del sistema propuesto por Hofmeister y presentaron una reducción a la fórmula de Hofmeister para el cálculo de 1.6 utilizando fracciones continuas[3]. Por su parte Rödseth[4] también implementa fracciones continuas utilizando residuos negativos. En contraste a los anteriores Brauer[5] propone un método geométrico para el cálculo del número de Frobenius, método que fue implementado en un algoritmo por Davison[6].

De lo anterior se debe tener claro que los métodos de *Selmer* y *Rödseth* son extensiones del método de Hofmeister los algoritmos que se presentan como apéndice se comportan de la misma manera.

El interés del presente trabajo es ver que cada uno de los métodos es capaz de calcular el número de Frobenius para ternas de números cada vez más grandes y sin tantas condiciones, lo que se hace evidente en la última sección del presente escrito. Sin embargo, determinar cual de lo métodos llevado a un algoritmo es el más eficiente no recae entre los objetivos de este documento ya que nunca se calculó el tiempo de ejecución de cada algoritmo ni fueron comparados bajo ningún criterio.

Por otro lado deacuerdo al lema 1.2, $g(a_1, a_2, a_3)$ puede reducirse al cálculo del número de Frobenius en dos variables cuando uno de los elementos de $a_1$, $a_2$ y $a_3$ es representable por los dos restantes.

---

[1] SELMER, Ernst. (1977) *On the linear Diophantine problem of Frobenius.*

[2] BEYER, Öyvind. SELMER, Ernst. (1978) *On the linear Diophantine problem of Frobenius in three variables.*

[3] GORDILLO, Enrique. JIMENEZ, Rafael. RUBIANO, Gustavo. (2004) *Teoria de Números.*

[4] RÖDSETH, Öystein. (1978) *On a linear Diophantine problem of Frobenius.*

[5] BRAUER, Alfred. SHOCKLEY, James. (1962) *On a problem of Frobenius.*

[6] DAVISON, J.L. (1994) *On the linear Diophantine problem of Frobenius.*

## 2.1. MÉTODO DE HOFMEISTER

Hofmeister mostró que todas las fórmulas para $k = 3$ previas a su artículo[7] de 1966 pueden ser deducidas del resultado que se muestra a continuación.

Sea $A = \{a_1, a_2, a_3\}$ un conjunto de tres enteros positivos independientes primos dos a dos. Como $\gcd(a_1, a_2) = 1$ y $A$ es independiente, la congruencia $a_2 x \equiv a_3$ mód $a_1$ tiene solución única módulo $a_1$, es decir existe $s \in \{0, 1, \ldots, a_1 - 1\}$ tal que

$$a_2 s \equiv a_3 \text{ mód } a_1 \tag{2.1}$$

Sin embargo, si $s = 0$, se tendría $a_3 \equiv 0$ mód $a_1$ y si $s = 1$ se tiene $a_2 = a_3 + a_1 p$ para algún $p \in \mathbb{Z}^+$. En ambos casos se contradice la independencia de $A$. Así $1 < s \leq a_1 - 1$.

Además de (2.1) existe, $t \in \mathbb{Z}$, único, tal que $a_2 s - a_3 = a_1 t$ de donde

$$a_3 = a_2 s - a_1 t. \tag{2.2}$$

Dado que $A$ es independiente se debe tener $t > 0$.

Por otro lado, por el algoritmo de la división, existen enteros $q$ y $r$ tales que

$$a_1 = qs + r \qquad 0 < r \leq s - 1 \tag{2.3}$$

Puesto que si $r = 0$, $a_1 = qs$, de esta manera de (2.1) se tiene

$$\begin{aligned}
&a_2 s \equiv a_3 \text{ mód } a_1 && \text{multiplicando por } q \\
&q a_2 s \equiv q a_3 \text{ mód } a_1 && \text{dado que } a_1 = qs \\
&a_1 a_2 \equiv q a_3 \text{ mód } a_1 && \\
&0 \equiv q a_3 \text{ mód } a_1 && \text{luego existe } m \in \mathbb{Z}^+ \text{ talque} \\
&q a_3 = a_1 m && \text{así} \\
&a_3 = sm &&
\end{aligned}$$

De manera que $a_3 = sm$ y como $a_1 = qs$ resulta que $\gcd(a_1, a_3) \neq 1$, contradiciendo que $a_1, a_2$ y $a_3$ son primos dos a dos.

En el diagrama (2.4) se presenta un conjunto de enteros representables por $a_2$ y $a_3$.

$$\left.\begin{array}{rllll}
 & a_2 & 2a_2 & \cdots\cdots\cdots & (s-1)a_2 \\
a_3 & a_2 + a_3 & 2a_2 + a_3 & \cdots\cdots\cdots & (s-1)a_2 + a_3 \\
\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots \\
(q-1)a_3 & a_2 + (q-1)a_3 & 2a_2 + (q-1)a_3 & \cdots\cdots\cdots & (s-1)a_2 + (q-1)a_3 \\
qa_3 & a_2 + qa_3 & 2a_2 + qa_3 \cdots & (r-1)a_2 + qa_3 &
\end{array}\right\} \tag{2.4}$$

[7] HOFMEISTER, G. R. (1966) *Zu einem Problem von Frobenius.*

Los elementos que están en el diagrama son de la forma $a_2x+a_3y$ donde $(x,y) \in T_1 \cup T_2$ y

$$T_1 = \{(x,y) : 0 \leq x \leq s-1, 0 \leq y \leq q-1,\ x,y \in \mathbb{Z}^+ \cup 0\}$$
$$T_2 = \{(x,y) : 0 \leq x \leq r-1, y = q,\ x,y \in \mathbb{Z}^+ \cup 0\}$$

De la ecuación (2.1)

$$a_2x + a_3y \equiv a_2x + sa_2y \equiv a_2(x+sy)(\text{mód}\, a_1)$$

Como $\gcd(a_2,a_3) = 1$ y se puede probar que $0 \leq x+sy < a_1$, los elementos en el diagrama constituyen un sistema completo de residuos módulo $a_1$.

Luego para utilizar el teorema 1.6 se debe tener que el diagrama representa un sistema minimal módulo $a_1$. Esto se muestra en el siguiente resultado de Hofmeister.

**Teorema 2.1.** *Sea $A = \{a_1,a_2,a_3\}$ un conjunto de enteros positivos independiente primos dos a dos. Sean $q,s$ y $r$ como en la ecuaciones (2.1),(2.2) y (2.3). Si $(q+1)a_3 \geq (s-r)a_2$ entonces*

$$g(a_1,a_2,a_3) = \text{máx}\{(s-1)a_2 + (q-1)a_3, (r-1)a_2 + qa_3\} - a_1 \tag{2.5}$$

*Demostración.* Sea $t_l$ el menor entero representable por $a_2$ y $a_3$ congruente con $l$ módulo $a_1$. Ahora los elementos del diagrama (2.4) son los $t_l$. En efecto, primero se demostró que cada elemento que está en el diagrama (2.4) es congruente con algún $t_l$ módulo $a_1$. De la ecuación (2.1) y como $a_3 < sa_2$, no tiene sentido extender el diagrama más allá de la última columna. Los $s-r$ elementos restantes de la última fila, son congruentes módulo $a_1$ con los primeros $s-r$ elementos de la primera fila en el diagrama. Además, como $(q+1)a_3 \geq (s-r)a_2$, esto implica que no se obtienen enteros menores que los que ya se tienen en el diagrama al agregarle más filas. De esta forma en el diagrama (2.4) se encuentran los enteros $t_l$.

Finalmente del teorema 1.6, y como los elementos del diagrama están en $T_1 \cup T_2$, el máximo de los $t_l$ es $(s-1)a_2 + (q-1)a_3$ ó $(r-1)a_2 + qa_3$ se tiene que

$$g(a_1,a_2,a_3) = \text{máx}\, t_l - a_1 = \text{máx}\{(s-1)a_2 + (q-1)a_3, (r-1)a_2 + qa_3\} - a_1$$

□

## 2.2. MÉTODO DE SELMER Y BEYER

**2.2.1. Descripción del método** A continuación se presenta un método para calcular el número de Frobenius encontrado por Beyer cuando realizó su tesis bajo la asesoría

de Selmer[8]. Su resultado fue presentado en el décimo séptimo congreso Escandinavo de Matemáticas en Aabo(Turku) en Finlandia en agosto de 1976.

Beyer introduce la M-función, la cual escoge en una lista de números ordenados el entero más pequeño de la segunda mitad de dicho listado. Esta función fue introducida para calcular el número de Frobenius en tres variables. Este método se basa en los resultados obtenidos por *Hofmeister* cuando la condición $(q+1)a_3 \geq (s-r)a_2$ no se cumple.

Como se mencionó anteriormente se puede asumir $a_1, a_2$ y $a_3$ primos dos a dos e independientes. Sean $s$, $t$ y $r$ enteros como en las ecuaciones (2.1),(2.2) y (2.3).

El diagrama (2.4) presentado en el método de Hofmeister se puede reescribir como un sistema de coordenadas cartesianas $(x, y)$ como sigue

$$\begin{array}{cccc} (0,0) & (1,0) & \cdots & (s-1,0) \\ (0,1) & (1,1) & \cdots & (s-1,1) \\ \vdots & \vdots & \vdots & \vdots \\ (0,q-1) & (1,q-1) & \cdots & (s-1,q-1) \\ (0,q) & (1,q) & \cdots\ (r-1,q) & \end{array} \tag{2.6}$$

Como en el método de Hofmeister dentro de este diagrama las combinaciones (2.4) representan todos los residuos (mód$a_1$) sólo una vez, así bajo las condiciones del teorema 2.1, se obtiene el número de Frobenius en una de las dos esquinas inferiores derechas del diagrama anterior.

Si la condición $(q+1)a_3 \geqq (s-r)a_2$ no se cumple, entonces Selmer y Beyer demuestran que al diagrama (2.6) se le pueden agregar otras líneas. En este caso el diagrama debe ser extendido para encontrar representaciones más pequeñas $xa_2 + ya_3$ para algunos residuos módulo $a_1$. Sin embargo no es útil extender el diagrama hacia la derecha dado que $sa_2$ puede siempre ser reemplazado por un entero más pequeño congruente con él, $a_3$ . Del mismo modo en la posición $(r, q)$ se tiene

$$ra_2 + qa_3 \equiv ra_2 + q.sa_2 = (qs+r)a_2 = a_1a_2 \equiv 0 \text{ mód } a_1$$

Por esto ninguna representación minimal $xa_2 + ya_3$ será encontrada en una extensión hacia la derecha. De allí la única extensión posible del diagrama será por lo tanto abajo de la última línea incompleta.

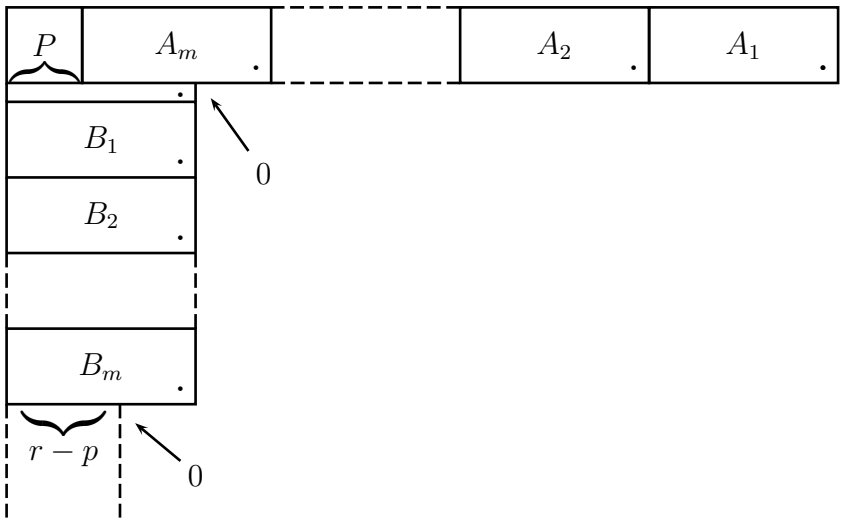
Para llevar a cabo esta extensión considérese

$$s = mr + p, \qquad 0 \leqq p < r \tag{2.7}$$

[8]BEYER, Öyvind. SELMER, Ernst. (1978) *On the linear Diophantine problem of Frobenius in three variables.*

y se asume $p > 0$. El primer paso de este proceso está en la construcción del siguiente diagrama.

Figura 2.1: Encasillamiento de 2.6 cuando $(q+1)a_3 \geq (s-r)a_2$ no se cumple.




La franja horizontal y la linea estrecha debajo de esta, corresponden a los puntos del diagrama (2.6) y el resto de la franja vertical es la extensión.

Ambas franjas son divididas en $m$ bloques de ancho $r$ y alto $q$. Estos bloques son congruentes por pares, en el sentido que puntos correspondientes de los bloques $A_i$ y $B_i$ representan combinaciones congruentes módulo $a_1$. Esta propiedad se puede verificar comparando las esquinas inferiores derechas de los pares de bloques correspondientes que tienen la siguiente forma

$$\begin{aligned} de \quad A_i: \quad & (s-1-(i-1)r, q-1), \\ de \quad B_i: \quad & (r-1, (i+1)q). \end{aligned} \tag{2.8}$$

y sus respectivas combinaciones lineales son:

$$\alpha_i = (s-1-(i-1)r)a_2 + (q-1)a_3, \;\; \beta_i = (r-1)a_2 + (i+1)qa_3. \tag{2.9}$$

Entonces se tiene que $\alpha_i \equiv \beta_i$ mód $a_1$.

En efecto, se sabe que

$$ra_2 + qa_3 \equiv 0 \text{ mód } a_1$$

multiplicando por $-i$ a ambos lados se tiene

$$-i(ra_2 + qa_3) \equiv 0 \text{ mód } a_1$$

de allí

$$-ira_2 \equiv iqa_3 \text{ mód } a_1$$

ahora como $sa_2 \equiv a_3$ mód $a_1$ podemos sumar $sa_2$ y restar $a_3$

$$sa_2 - ira_2 - a_3 \equiv iqa_3 \text{ mód } a_1$$

restando $a_2$ y sumando $ra_2$ y $qa_3$ a ambos lados de la congruencia se tiene

$$sa_2 - a_2 - ira_2 - a_3 + ra_2 + qa_3 \equiv (iqa_3 - a_2 + ra_2 + qa_3) \text{ mód } a_1$$

$$(s-1)a_2 - (i-1)ra_2 + (q-1)a_3 \equiv (i+1)qa_3 + (r-1)a_2 \text{ mód } a_1$$

$$(s-1-(i-1)r)a_2 + (q-1)a_3 \equiv (i+1)qa_3 + (r-1)a_2 \text{ mód } a_1$$

luego

$$\alpha_i \equiv \beta_i \text{ mód } a_1$$

Lo que demuestra la congruencia de los bloques.

En particular la clase residual 0 no se encuentra en ninguno de los bloques $B_i$. Esta clase está representada debajo de $B_m$ por el punto $(r-p, (m+1)q+1)$.
Basta con demostrar que

$$(r-p)a_2 + ((m+1)q+1)a_3 \equiv 0 \text{ mód } a_1$$

Sea entonces

$$a_1 \equiv 0 \text{ mód } a_1$$

como $a_1 = qs + r$ se tiene

$$(qs+r) \equiv 0 \text{ mód } a_1$$

multiplicando a ambos lados por $ma_2$

$$mra_2 + mqsa_2 \equiv 0 \text{ mód } a_1$$

sumando y restando $sa_2$

$$-sa_2 + mra_2 + mqsa_2 + sa_2 \equiv 0 \text{ mód } a_1$$

$$-a_2(s - mr) + mqsa_2 + sa_2 \equiv 0 \text{ mód } a_1$$

Como $s = mr + p$ se deduce que

$$-pa_2 + mqsa_2 + sa_2 \equiv 0 \text{ mód } a_1$$

Como $a_1a_2 \equiv 0$ mód $a_1$ podemos sumar $a_1a_2$ sin que se afecte la congruencia

$$a_1a_2 - pa_2 + mqsa_2 + sa_2 \equiv 0 \text{ mód } a_1$$

Dado que $a_1 = qs + r$ se tiene

$$(qs + r)a_2 - pa_2 + mqsa_2 + sa_2 \equiv 0 \text{ mód } a_1$$

$$qsa_2 + ra_2 - pa_2 + mqsa_2 + sa_2 \equiv 0 \text{ mód } a_1$$
$$(r - p)a_2 + (m + 1)qsa_2 + sa_2 \equiv 0 \text{ mód } a_1$$
$$(r - p)a_2 + ((m + 1)q + 1)sa_2 \equiv 0 \text{ mód } a_1$$

que era lo que se quería demostrar.

De este modo los primeros $r - p$ puntos de la línea inmediatamente abajo de $B_m$ serán por lo tanto congruentes a los últimos $r - p$ puntos en la franja estrecha arriba de $B_1$. Si los primeros puntos representan combinaciones más grandes $xa_2 + ya_3$ que los últimos no es necesario extender el diagrama abajo de $B_m$. La condición para esto puede ser encontrada al comparar los dos puntos representantes del residuo 0 $(r - p)a_2 + ((m + 1)q + 1)a_3$ y $ra_2 + qa_3$, es decir el diagrama no debe extenderse abajo de $B_m$ si

$$(r - p)a_2 + ((m + 1)q + 1)a_3 > ra_2 + qa_3$$

o lo que es lo mismo

$$ra_2 - pa_2 + mqa_3 + qa_3 + a_3 > ra_2 + qa_3$$
$$(mq + 1)a_3 > pa_2$$

Luego

$$\frac{a_3}{a_2} > \frac{p}{mq + 1} \tag{2.10}$$

**Lema 2.1.** *Con la notación anterior. Si*

$$\frac{a_3}{a_2} > \frac{p}{mq + 1}$$

*entonces*

$$g(a_1, a_2, a_3) = -a_1 + \text{máx}\{\beta_0, \alpha_m, \text{mín}\,\{\alpha_1, \beta_1\}, \ldots, \text{mín}\,\{\alpha_{m-1}, \beta_{m-1}\}\}$$

*Demostración.* Cuando la condición (2.10) se satisface los candidatos para los $t_l$ son encontrados en el diagrama de la figura 2.1 Para determinar el máx $t_l$ es suficiente comparar las esquinas inferiores derechas de cada bloque $A_i$ y $B_i$, que son los valores $\alpha_i$ y $\beta_i$ (ver (2.9)). Además, se debe considerar el elemento $\beta_0$ encima de $B_1$, (ver teorema 2.1). Sin embargo se puede eliminar $\beta_m$ de la lista ya que como se demostró $\beta_m \equiv \alpha_m$ y además $\beta_m > \alpha_m$ que se puede demostrar como sigue

$$\frac{a_3}{a_2} > \frac{p}{mq + 1}$$

$$(qm+1)a_3 > a_2 p$$
$$(qm+1)a_3 > a_2(s-mr)$$
$$mqa_3 > sa_2 - mra_2 - a_3$$

si se suma $ra_2$ y $qa_3$ a ambos lados de la desigualdad se tiene

$$ra_2 + mqa_3 + qa_3 > sa_2 - mra_2 - a_3 + ra_2 + qa_3$$
$$ra_2 + (m+1)qa_3 > (s-(m-1)r)a_2 + (q-1)a_3$$

Y restando $a_2$ a ambos lados de la desigualdad

$$(r-1)a_2 + (m+1)qa_3 > (s-1-(m-1)r)a_2 + (q-1)a_3$$

de allí

$$\beta_m > \alpha_m$$

Para $i = 0, 1, \ldots, m-1$, se debe escoger el correspondiente $t_l \equiv \alpha_i \equiv \beta_i$ como el más pequeño de $\alpha_i$ y $\beta_i$ (esto por la definición de los $t_l$). Bajo la condición (2.10), el teorema 1.6 implica que

$$g(a_1, a_2, a_3) = -a_1 + \text{máx}\{\beta_0, \alpha_m, \text{mín}\{\alpha_1, \beta_1\}, \ldots, \text{mín}\{\alpha_{m-1}, \beta_{m-1}\}\} \tag{2.11}$$

□

Indudablemente, esto es una forma explícita para calcular $g(a_1, a_2, a_3)$, aunque muy difícil de manejar. Sin embargo es posible simplificar esta fórmula con la introducción de la función $M\{x_1, x_2, \ldots, x_{2m}\}$ de un número par de argumentos, dada por

$$M\{x_1, x_2, \ldots, x_{2m}\} = x_{i_{m+1}} \qquad x_{i_1} \leq x_{i_2} \leq x_{i_3} \leq \cdots \leq x_{i_{2m}} \tag{2.12}$$

Es decir se organizan los argumentos en orden creciente y se selecciona el número más pequeño de la segunda mitad.
Con $m = 1$ se tiene que $M\{x_1, x_2\} = \text{máx}\{x_1, x_2\}$

**Lema 2.2.** *Con la notación anterior. Si*

$$\frac{a_3}{a_2} > \frac{p}{mq+1}$$

*entonces*

$$g(a_1, a_2, a_3) = -a_1 + M\{\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_0, \beta_1, \ldots, \beta_{m-1}\}$$

*Demostración.* Volviendo a (2.9) se nota que

$$\alpha_1 > \alpha_2 > \cdots > \alpha_m, \qquad \beta_0 < \beta_1 < \cdots < \beta_{m-1}$$

Estas desigualdades hacen que la función máximo de (2.11) pueda ser reemplazada por la función $M$ de $2m$ argumentos $\alpha_i$ y $\beta_i$ (ver ecuación (2.12)).
Se debe probar que

$$M\{\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_0, \beta_1, \ldots, \beta_{m-1}\} = \text{máx}\{\beta_0, \alpha_m, \text{mín}\{\alpha_1, \beta_1\}, \ldots, \text{mín}\{\alpha_{m-1}, \beta_{m-1}\}\}$$

Para este fin sea $t = \text{máx}\{\beta_0, \alpha_m, \text{mín}\{\alpha_1, \beta_1\}, \ldots, \text{mín}\{\alpha_{m-1}, \beta_{m-1}\}\}$. Para que se cumpla la igualdad, $t$ debe estar en la posición $m+1$, ya que la función es de $2m$ argumentos, es decir antes de $t$ debe haber $m$ elementos y después de $t$ deben haber $m-1$ elementos, cuando se encuentran organizados en forma creciente los $\alpha_i$ y $\beta_i$.

Se va a demostrar que después de $t$ hay $m-1$ elementos y que además no se puede introducir otro elemento en esta lista.

Por hipótesis se tiene que

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

Ahora, existen dos opciones para el máximo

1. Si $t = \beta_i$

   - $t = \beta_i < \beta_{i+1} < \cdots < \beta_{m-1} = \beta_{i+(m-1)-i}$
     Así a la derecha de $t$ hay $(m-1)-i$ elementos.

   - Por otro lado $t = \beta_i = \text{mín}\{\alpha_i, \beta_i\}$
     así $t = \beta_i < \alpha_i < \alpha_{i-1} < \cdots < \alpha_1$ a la derecha de $t$ hay $i$ elementos.

   De los dos items anteriores se tiene que a la derecha de $t$ hay $(m-1)-i+i$ elementos es decir hay $m-1$ elementos.

   Ahora se demostrará que sólo son estos los elementos que están a la derecha de $t$, para esto se intentará introducir un elemento más.

   Supóngase entonces que existe $j > i$ tal que $t < \alpha_j$ para lo cual se tiene dos opciones

   *a)* $\text{mín}\{\alpha_j, \beta_j\} = \alpha_j$
   $\alpha_j$ no puede estar a la derecha de $t$ por que contradice la escogencia de $t$ como máximo.

*b*) $\min\{\alpha_j, \beta_j\} = \beta_j$ Como $j > i$ se tiene $t = \beta_i < \beta_j$ lo que es absurdo porque $t$ es el máximo.

Como ninguna de las dos opciones es posible, queda demostrado que no se puede introducir ningún elemento más a la derecha de $t$

2. Si $t = \alpha_i$

   - $t = \alpha_i < \alpha_{i-1} < \alpha_{i-2} < \cdots < \alpha_1$ a la derecha de $t$ hay $(i-1)$ elementos.
   - Por otro lado $t = \alpha_i = \min\{\alpha_i, \beta_i\} < \beta_i < \beta_{i+1} < \cdots < \beta_{m-1}$
     por esto a la derecha de $t$ hay $m - 1 - i + 1$ elementos, es decir hay $m - i$ elementos .

   Por tanto a la derecha de $t$ hay $m - i + i - 1 = m - 1$ elementos.

   Nuevamente se debe demostrar que sólo son estos los elementos. Para esto se intentará introducir un nuevo elemento en la lista.

   Supóngase entonces que existe $j < i$ tal que $t < \beta_j$. Para lo cual se tienen dos opciones

   *a*) $\min\{\alpha_j, \beta_j\} = \alpha_j$ como $j < i$ se tiene $t = \alpha_i < \alpha_j$ lo que contradice la escogencia de $t$ como máximo.

   *b*) $\min\{\alpha_j, \beta_j\} = \beta_j$. $\beta_j$ no puede estar a la derecha de $t$ ya que contradice la escogencia de $t$ como máximo.

   Como ninguna de las dos opciones es posible, queda demostrado que no se puede introducir ningún elemento a la derecha de $t$.

De (1) y (2) se deduce que a la derecha de $t$ sólo hay $m-1$ elementos y como la función M es de $2m$ argumentos incluyendo $t$ es claro que a la izquierda de $t$ se encuentran $m$ elementos, llegando así a lo que se quería probar y por lo tanto

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

Así la ecuación (2.11) es reescrita

$$g(a_1, a_2, a_3) = -a_1 + M\{\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_0, \beta_1, \ldots, \beta_{m-1}\}$$

□

**Teorema 2.2.** *Con la notación anterior. Si*

$$\frac{a_3}{a_2} > \frac{p}{mq+1}$$

*entonces*

$$g(a_1, a_2, a_3) = -a_1 + (r-1)a_2 + (q-1)a_3 + M\{(s-(i+1)r)a_2, (1+jq)a_3\}$$
$$i, j = 0, 1, \ldots, m-1.$$

*Demostración.* Dado que

$$\alpha_i = (s-1-(i-1)r)a_2 + (q-1)a_3,$$
$$\beta_i = (r-1)a_2 + (i+1)qa_3.$$

$$g(a_1,a_2,a_3) = -a_1 + M\{(s-1)a_2 + (q-1)a_3, ((s-1)-r)a_2 + (q-1)a_3, \ldots,$$
$$(s-1)-(m-1)ra_2 + (q-1)a_3, (r-1)a_2 + qa_3, (r-1)a_2 + 2qa_3, \ldots, (r-1)a_2 + mqa_3\}$$

Sacando de la función M el término $(q-1)a_3$ que aparece en todos las componentes donde se calcula la función M se tiene

$$g(a_1,a_2,a_3) = -a_1 + (q-1)a_3 + M\{(s-1)a_2, ((s-1)-r)a_2, \ldots, ((s-1)-(m-1)r)a_2,$$
$$(r-1)a_2 + a_3, (r-1)a_2 + (1+q)a_3, \ldots, (r-1)a_2 + (1+(m-1)q)a_3\}$$

ya que

$$(r-1)a_2 + mqa_3 - (q-1)a_3 = (r-1)a_2 + (m-1)qa_3 + a_3 = (r-1)a_2 + (1+(m-1)q)a_3$$

Si además se extrae de la función M $(r-1)a_2$ se obtiene

$$= -a_1 + (q-1)a_3 + (r-1)a_2 + M\{(s-r)a_2, (s-2r)a_2, \ldots, (s-mr)a_2, a_3, (1+q)a_3, \ldots, (1+(m-1)q)a_3\}$$

esto por que

$$((s-1)-(m-1)r)a_2 - (r-1)a_2$$
$$= sa_2 - a_2 - mra_2 + a_2 =$$
$$sa_2 - mra_2 = (s-mr)a_2$$

$$g(a_1,a_2,a_3) = -a_1 + (r-1)a_2 + (q-1)a_3 + M\{(s-(i+1)r)a_2, (1+jq)a_3\} \quad (2.13)$$
$$i,j = 0,1,\ldots,m-1.$$

□

La fórmula es válida para la condición (2.10). Si (2.10) no se satisface se debe extender la figura 2.1 justo debajo de $B_m$. Los nuevos bloques serán más angostos. La forma de la figura 2.1 depende de el algoritmo de la fracción continua para el radio $a_1 : s$.

**2.2.2. Cálculo del número de Frobenius para tres variables utilizando fracciones continuas** A continuanción se presenta un procedimiento encontrado por Selmer. Este es una extensión del teorema 2.2 el cual se aplica cuando es necesario hacer una ampliación en la figura 2.1.

Los primeros dos pasos de este algoritmo son de hecho ya mostrados por las ecuaciones (2.3) y (2.7), donde $a_1, a_2$ y $a_3$ son primos relativos e independientes, los cuales se

escribirán como

$$a_1 = qs + r = q_0 s + r_0 \qquad 0 < r_0 < s \tag{2.14}$$
$$s = mr + p = q_1 r_0 + r_1 \qquad 0 < r_1 < r_0 \tag{2.15}$$

el paso general es dado por

$$r_n = q_{n+2} r_{n+1} + r_{n+2} \qquad 0 < r_{n+2} < r_{n+1}$$

Como $\gcd(a_1, a_3) = 1$ entonces $\gcd(a_1, s) = 1$, el último residuo diferente de cero es 1, luego la próxima división termina el procedimiento.
Con los cocientes $q_0$, $q_1$, $q_2$,..., se construye la fracción continua simple $[q_0, q_1, q_2, \ldots,]$ y se consideran los convergentes de la forma usual (ver 1).

$$\begin{aligned} C_0 &= \frac{P_0}{Q_0} = \frac{q_0}{1} \\ C_1 &= \frac{P_1}{Q_1} = [q_0, q_1] = \frac{q_0 q_1 + 1}{q_1} \\ C_2 &= \frac{P_2}{Q_2} = [q_0, q_1, q_2] = \frac{(q_0 q_1 + 1) q_2 + q_0}{q_1 q_2 + 1} \\ &\vdots \end{aligned}$$

Por otro lado de la ecuación (2.10) se tiene que $\dfrac{a_3}{a_2} > \dfrac{p}{qm+1}$ es la condición para saber si es necesario o no extender el diagrama de la figura 1 abajo de $B_m$ y de la ecuación (2.9) se tiene $p = s - mr$, además $q = q_0$ y $m = q_1$ entonces

$$\frac{a_3}{a_2} > \frac{s - mr}{q_0 q_1 + 1} = \frac{s - mr}{P_1}$$

Más aún de las ecuaciones (2.14) resulta $r_1 = s - q_1 r_0, \quad q_1 = m$ y $r = r_0$ de este modo $r_1 = s - mr$, luego la ecuación (2.10) puede ser reescrita como

$$\frac{a_3}{a_2} > \frac{r_1}{P_1} \tag{2.16}$$

que será ahora asumida como la condición para la extensión del diagrama.

En esta notación las esquinas o los ceros del diagrama de la figura 2.1 pueden ser reescritas como

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

Además el siguiente cero que se muestra en el diagrama dado por $(r-p,(m+1)q+1)$ puede ser reescrito por

$$\begin{aligned}(r-p,(m+1)q+1) &= (r_0-s+mr_0,(m+1)q_0+1)\\ &= (r_0-s+q_1r_0,q_0+mq_0+1)\\ &= (r_0-(s-q_1r_0),q_0+q_1q_0+1)\\ &= (r_0-r_1,P_0+P_1)\end{aligned}$$

Si

$$\frac{a_3}{a_2} < \frac{r_1}{P_1} \qquad (a)$$

el diagrama permite extensión y el próximo cero que se encuentra está en $(r_0-2r_1,P_0+2P_1)$.

Comparando $(r_0-r_1,P_0+P_1)$ con $(r_0-2r_1,P_0+2P_1)$ para detener la extensión del diagrama se tiene

$$\begin{aligned}(r_0-2r_1)a_2+(P_0+2P_1)a_3 &> (r_0-r_1)a_2+(P_0+P_1)a_3\\ r_0a_2-2r_1a_2+P_0a_3+2P_1a_3 &> r_0a_2-r_1a_2+P_0a_3+P_1a_3\\ P_1a_3 &> r_1a_2\\ \frac{a_3}{a_2} &> \frac{r_1}{P_1}\end{aligned}$$

Que es una contradicción de (a); así se debe seguir extendiendo.

Los próximos ceros se sitúan en

$$\begin{aligned}&(r_0-3r_1,P_0+3P_1)\\ &(r_0-4r_1,P_0+4P_1)\\ &\vdots\\ &(r_0-kr_1,P_0+kP_1), \qquad\qquad k=1,2,\ldots,q_2-1\end{aligned}$$

$k$ va hasta $q_2-1$ porque cuando es $q_2$ se tiene

$$(r_0-q_2r_1,P_0+q_2P_1)=(r_2,P_2)$$

ya que

- $r_0-q_2r_1=r_2$ porque $r_0=q_2r_1+r_2$ en las divisiones sucesivas.

- $P_0 + q_2P_1 = P_2$ por propiedad de los numeradores de los convergentes $P_n = q_nP_{n-1} + P_{n-2}$.

el próximo cero es

$$(r_2 - r_3, P_2 + P_3)$$

Comparando $(r_2, P_2)$ con $(r_2 - r_3, P_2 + P_3)$

$$\begin{aligned}(r_2 - r_3)a_2 + (P_2 + P_3)a_3 &> r_2a_2 + P_2a_3\\ r_2a_2 - r_3a_3 + P_2a_3 + P_3a_3 &> r_2a_2 + P_2a_3\\ P_3a_3 &> r_3a_2\\ \frac{a_3}{a_2} &> \frac{r_3}{P_3} \qquad (b)\end{aligned}$$

de (a) y (b)

$$\frac{r_3}{P_3} < \frac{a_3}{a_2} < \frac{r_1}{P_1}$$

Si $\frac{a_3}{a_2} < \frac{r_3}{P_3}$, se debe proceder extendiendo. El próximo cero estará en

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

$k$ va hasta $q_4 - 1$, porque cuando $k = q_4$, quedaría $(r_2 - q_4r_3, P_2 + q_4P_3) = (r_4, P_4)$
De esta forma utilizando las ideas presentadas en la demostración del teorema 2.2, se tiene el siguiente resultado.

**Teorema 2.3.** *Con la notación anterior, dado un entero n determinado por:*

$$\frac{r_{2n+1}}{P_{2n+1}} < \frac{a_3}{a_2} < \frac{r_{2n-1}}{P_{2n-1}} \tag{2.17}$$

*Luego*

$$\begin{aligned}g(a_1, a_2, a_3) = -a_1 + (r_{2n} - 1)a_2 + (P_{2n} - 1)a_3\\ + M\{(r_{2n-1} - (i+1)r_{2n})a_2, (p_{2n-1} + jP_{2n})a_3\},\\ i, j = 0, 1, \ldots, q_{2n+1} - 1 \qquad (2.18)\end{aligned}$$

## 2.3. MÉTODO DE RÖDSETH

Rödseth se encontraba entre la audiencia del décimo séptimo congreso Escandinavo de matemáticas en Aabo(Turku) y se interesó en el método de solución por fracciones

continuas para simplificar el resultado que en dicho congreso Selmer presentó, ver (2).

El método de Rödseth[9] para el cálculo del número de Frobenius en tres variables consiste en la implementación de fracciones continuas utilizando residuos negativos obtenidos de la aplicación del algoritmo de la división a $a_1 : s_0$. Se definen los convergentes de la fracción continua[10], para formar una sucesión decreciente de los cocientes entre los residuos y los numeradores de los convergentes respectivos, esto con el fin de encontrar dos términos de la sucesión entre los cuales se encuentra el cociente $\frac{a_3}{a_2}$, para posteriormente llegar a una expresión que permita el cálculo del número de Frobenius en tres variables.

Sea $A = \{a_1, a_2, a_3\}$ un conjunto de enteros positivos independiente y primos dos a dos; $s_0$ determinado por

$$a_2 s_0 \equiv a_3 \text{ mód } a_1, \quad 0 < s_0 < a_1. \tag{2.19}$$

Por las características de $A$, $s_0$ existe y es único.

Se aplica el algoritmo de Euclides a $a_1 : s_0$ utilizando residuos negativos.

$$\left.\begin{array}{rlll} a_1 = s_{-1} & = q_1 s_0 - s_1, & 0 \leq s_1 < s_0; \\ s_0 & = q_2 s_1 - s_2, & 0 \leq s_2 < s_1; \\ s_1 & = q_3 s_2 - s_3, & 0 \leq s_3 < s_2; \\ \cdots & & \\ s_{m-2} & = q_m s_{m-1} - s_m, & 0 \leq s_m < s_{m-1}; \\ s_{m-1} & = q_{m+1} s_m & 0 = s_{m+1} < s_m. \end{array}\right\} \tag{2.20}$$

Se definen los numeradores de los convergentes $P_i$ de enteros con condiciones iniciales $P_{-1} = 0$, $P_0 = 1$, y con la recurrencia lineal

$$P_{i+1} = q_{i+1} P_i - P_{i-1}, \quad i = 0, 1, \ldots, m. \tag{2.21}$$

Dado que $\frac{s_{-1}}{P_{-1}} = \infty$ y $\frac{s_{m+1}}{P_{m+1}} = 0$. Se forma una sucesión decreciente de cocientes $\frac{s_i}{P_i}$

$$0 = \frac{s_{m+1}}{P_{m+1}} < \frac{s_m}{P_m} < \cdots < \frac{s_0}{P_0} < \frac{s_{-1}}{P_{-1}} = \infty, \tag{2.22}$$

Se demuestra por inducción sobre $i$ que $\frac{s_{i+1}}{P_{i+1}} < \frac{s_i}{P_i}$, utilizando como hipótesis $s_{i+1} < s_i$ y $P_{i+1} > P_i$.

[9] RÖDSETH, Öystein. (1978) *On a linear Diophantine problem of Frobenius.*
[10] GORDILLO, Enrique. JIMENEZ, Rafael. RUBIANO, Gustavo. (2004) *Teoria de Números.*

- Sea $i = 0$
  $\dfrac{s_0}{P_0} - \dfrac{s_1}{P_1} = \dfrac{s_0P_1 - s_1P_0}{P_0P_1} > 0$ ya que $s_0 > s_1$, $P_1 > P_0$ y $P_i$ son enteros positivos o cero.

- Se supone cierto para $i = k$
  $\dfrac{s_k}{P_k} - \dfrac{s_{k+1}}{P_{k+1}} = \dfrac{s_kP_{k+1} - s_{k+1}P_k}{P_kP_{k+1}} > 0$ es decir $s_kP_{k+1} - s_{k+1}P_k > 0$

- Se demuestra para $i = k + 1$

$$\begin{aligned}
\frac{s_{k+1}}{P_{k+1}} - \frac{s_{k+2}}{P_{k+2}} &= \frac{s_{k+1}P_{k+2} - s_{k+2}P_{k+1}}{P_{k+1}P_{k+2}} \\
&= \frac{s_{k+1}(q_{k+2}P_{k+1} - P_k) - s_{k+2}P_{k+1}}{P_{k+1}P_{k+2}} \\
&= \frac{s_{k+1}q_{k+2}P_{k+1} - s_{k+1}P_k - s_{k+2}P_{k+1}}{P_{k+1}P_{k+2}} \\
&= \frac{(s_k + s_{k+2})P_{k+1} - s_{k+1}P_k - s_{k+2}P_{k+1}}{P_{k+1}P_{k+2}} \quad \text{ver (2.20)} \\
&= \frac{s_kP_{k+1} + s_{k+2}P_{k+1} - s_{k+1}P_k - s_{k+2}P_{k+1}}{P_{k+1}P_{k+2}} \\
&= \frac{s_kP_{k+1} - s_{k+1}P_k}{P_{k+1}P_{k+2}} > 0
\end{aligned}$$

Por hipótesis de inducción, queda demostrado.

En la sucesión (2.22) existe un único entero $v$, $-1 \leq v \leq m$, que satisface

$$\frac{s_{v+1}}{P_{v+1}} \leq \frac{a_3}{a_2} < \frac{s_v}{P_v}. \tag{2.23}$$

**Teorema 2.4.** *Dados $a_1, a_2, a_3$ enteros positivos, donde $a_1$ y $a_2$ son primos relativos, entonces*

$$g(a_1, a_2, a_3) = -a_1 + a_2(s_v - 1) + a_3(P_{v+1} - 1) - \text{mín}\{a_2s_{v+1}, a_3P_v\}, \tag{2.24}$$

*donde $v$ es el único entero determinado por (2.23).*

*Demostración.* Sea $R_i = \dfrac{1}{a_1}(a_2s_i - a_3P_i)$, $\quad i = -1, 0, \ldots, m+1$. Se definen los enteros $R_i$ con las condiciones iniciales $R_0 = \dfrac{1}{a_1}(a_2s_0 - a_3)$, $R_{-1} = a_2$ y con la recurrencia lineal

$$R_{i+1} = q_{i+1}R_i - R_{i-1}, \quad i = 0, 1, \ldots, m.$$

Para los cuales se tiene

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

Sean
$R_i = \dfrac{1}{a_1}(a_2 s_i - a_3 P_i), \quad R_{i+1} = \dfrac{1}{a_1}(a_2 s_{i+1} - a_3 P_{i+1}).$

$$\begin{aligned} R_i - R_{i+1} &= \frac{1}{a_1}(a_2 s_i - a_3 P_i - a_2 s_{i+1} + a_3 P_{i+1}) \\ &= \frac{1}{a_1}\left[a_2(s_i - s_{i+1}) + a_3(P_{i+1} - P_i)\right] > 0. \end{aligned}$$

Dado que $P_i - P_{i+1} < 0 < s_i - s_{i+1}$. Entonces $R_i > R_{i+1}$.

$R_{v+1} = \dfrac{1}{a_1}(a_2 s_{v+1} - a_3 P_{v+1}) = 0$ si $s_{v+1} = a_3$ y $P_{v+1} = a_2$.

Considerando $t_l = t_l(a_1, a_2, a_3)$. Dado $l$, existen parejas $(y, z)$ de enteros no negativos tales que $t_l = a_2 y + a_3 z$ y sea $(y_l, z_l)$ una pareja para la cual $z_l$ es minimal.

Sea

$$\begin{aligned} t_l - a_1 R_v &= a_2 y_l + a_3 z_l - a_1 \left[\frac{1}{a_1}(a_2 s_v - a_3 P_v)\right] \\ &= a_2 y_l + a_3 z_l - a_2 s_v + a_3 P_v \\ &= a_2(y_l - s_v) + a_3(z_l + P_v) \end{aligned}$$

como $R_v$ es un entero positivo y por definición de $t_l$, $y_l < s_v$.

De forma análoga

$$t_l + a_1 R_{v+1} = a_2(y_l + s_{v+1}) + a_3(z_l - P_{v+1})$$

como $R_{v+1} < 0$, por definición de $t_l$, $z_l < P_{v+1}$. Si $R_{v+1} = 0$, por la minimalidad de $z_l$, $z_l < P_{v+1}$.
y

$$t_l - a_1(R_v - R_{v+1}) = a_2(y_l - s_v + s_{v+1}) + a_3(z_l + P_v - P_{v+1})$$

como $R_v > R_{v+1}$, por definición de $t_l$, $y_l < s_v - s_{v+1}$ 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 puntos látices (es decir con coordenadas enteras), tales que

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

El número $|A \cup B|$ de elementos en $A \cup B$ esta dada por

$$\begin{aligned} |A \cup B| = |A| + |B| &= (s_v - s_{v+1})(P_{v+1}) + (s_{v+1})(P_{v+1} - P_v) \\ &= s_v P_{v+1} - s_{v+1} P_{v+1} + s_{v+1} P_{v+1} - s_{v+1} P_v \\ &= s_v P_{v+1} - s_{v+1} P_v = a_1 \end{aligned}$$

Puesto que para cada $i$, $s_i P_{i+1} - s_{i+1} P_i = a_1, \quad i = -1, \ldots, m.$

- Sea $i = -1$
  $s_{-1}P_0 - s_0P_{-1} = a_1(1) - s_0(0) = a_1$
- Se supone cierto para $i = k$
  $s_kP_{k+1} - s_{k+1}P_k = a_1$
- Se demuestra para $i = k + 1$

$$\begin{aligned} s_{k+1}P_{k+2} - s_{k+2}P_{k+1} &= s_{k+1}(q_{k+2}P_{k+1} - P_k) - s_{k+2}P_{k+1} \\ &= (s_{k+1}q_{k+2})P_{k+1} - s_{k+1}P_k - s_{k+2}P_{k+1} \\ &= (s_k + s_{k+2})P_{k+1} - s_{k+1}P_k - s_{k+2}P_{k+1} \\ &= s_kP_{k+1} + s_{k+2}P_{k+1} - s_{k+1}P_k - s_{k+2}P_{k+1} \\ &= s_kP_{k+1} - s_{k+1}P_k = a_1 \end{aligned}$$

por hipótesis de inducción, queda demostrado.

Sea $\{t_l \backslash l \in L\} = \{a_2y + a_3z/(y,z) \in A \cup B\}$, un sistema completo de residuos módulo $a_1$.
Ahora

$$\begin{aligned} \max_{(y,z)\in A}\{a_2y + a_3z\} &= a_2(s_v - s_{v+1} - 1) + a_3(P_{v+1} - 1). \\ \max_{(y,z)\in B}\{a_2y + a_3z\} &= a_2(s_v - 1) + a_3(P_{v+1} - P_v - 1). \end{aligned}$$

Y por consiguiente

$$\begin{aligned} g(a_1,a_2,a_3) &= -a_1 + \max_{l\in L} t_l \\ &= -a_1 + \max_{(y,z)\in A\cup B}\{a_2y + a_3z\} \\ &= -a_1 + \max\{a_2(s_v - s_{v+1} - 1) + a_3(P_{v+1} - 1), (s_v - 1)a_2 + a_3(P_{v+1} - P_v - 1)\} \\ &= -a_1 + a_2(s_v - 1) + a_3(P_{v+1} - 1) + \max\{a_2(-s_{v+1}), a_3(-P_v)\} \\ &= -a_1 + a_2(s_v - 1) + a_3(P_{v+1} - 1) - \min\{a_2s_{v+1}, a_3P_v\} \end{aligned}$$

□

## 2.4. MÉTODO DE BRAUER

**2.4.1. Descripción del método** En 1962, Brauer y Shockley[11] dieron un resultado importante para el cálculo explícito de $f(a,b,c)$. En este apartado se presenta una breve descripción de este método.

[11] BRAUER, Alfred. SHOCKLEY, James. (1962) *On a problem of Frobenius.*

Sean $a, b, c$ tres enteros positivos primos relativos entre sí. Sin pérdida de generalidad se puede suponer que $a, b, c$ son primos relativos dos a dos, $a < b < c$ y $c$ no es representable por $a, b$.

Sea $S = \{(x, y) : bx \equiv cy(\text{mód}a), 0 < x \leq a, 0 < y \leq a. \quad x, y \in \mathbb{Z}^+\}$ y sean

$$T_1 = \{(x, y) : bx > cy, 0 < x \leq a, 0 < y \leq a. \quad x, y \in \mathbb{Z}^+\}$$
$$T_2 = \{(x, y) : bx < cy, 0 < x \leq a, 0 < y \leq a. \quad x, y \in \mathbb{Z}^+\}$$

Sea $(x, y) \in S$, luego $(x, y)$ es una solución de la congruencia lineal $bx - cy \equiv 0(\,\text{mód}\,a)$. Si $y = 1$, se tiene que existe una solución que satisface $bx - cy > 0$, pues de lo contrario $c$ sería representable por $a, b$. De forma análoga si $x = 1$ y como $b < c$ se tiene que existe una solución tal que $bx - cy < 0$. Así se tiene que $S \cap T_1$ y $S \cap T_2$ son no vacíos, entonces se pueden encontrar los siguientes enteros

$$x_1 = \text{mín}\{x : (x, y) \in S \cap T_1\}$$
$$y_2 = \text{mín}\{y : (x, y) \in S \cap T_2\}$$

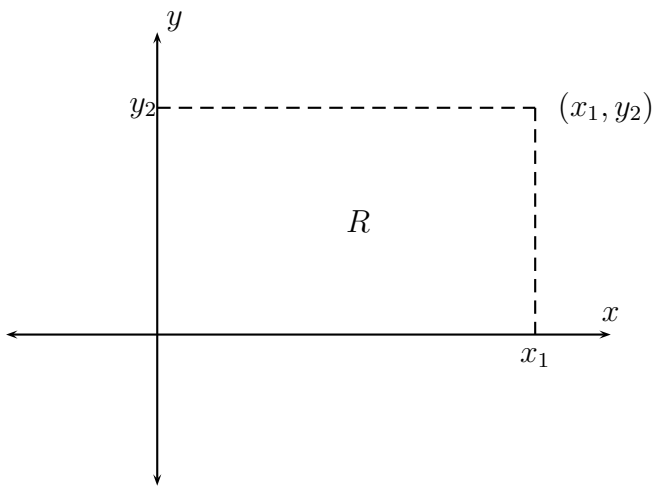
y sean $y_1, x_2$, tales que $(x_1, y_1), (x_2, y_2) \in S$.

Sea $H(x, y) = bx + cy$, considerando un sistema de coordenadas cartesianas. Se dice que dos puntos latices (es decir con coordenadas enteras) $(x', y'), (x'', y'')$ con coordenadas no negativas son congruentes si

$$H(x', y') \equiv H(x'', y'')(\text{mód}a) \tag{2.25}$$

Sea $R$ el rectángulo que consiste de todos los puntos látices $(x, y)$ tales que $0 \leq x < x_1, \quad 0 \leq y < y_2$.

Figura 2.2: Gráfica de la región $R$.



Primero se prueba que para cada punto látice $(x, y)$ con coordenadas no negativas en el exterior de $R$ existe un punto látice congruente $(u, v)$ tal que $H(x, y) > H(u, v)$. Sea $(x, y)$ un punto látice con coordenadas no negativas en el exterior de $R$. Si $x \geq x_1$, sea $u = x - x_1, v = y + y_1$. Entonces

$$\begin{aligned} H(u, v) = bu + cv = b(x - x_1) + c(y + y_1) &= bx + cy - (bx_1 - cy_1) \\ &= H(x, y) - (bx_1 - cy_1) \end{aligned}$$

De esta forma, $H(x, y) > H(u, v)$ y $H(x, y) \equiv H(u, v)(\,\mathrm{mód}\, a)$, puesto que $bx_1 - cy_1 > 0$ y $bx_1 - cy_1 \equiv 0(\mathrm{mód} a)$.

Por otra parte si $y \geq y_2$, sea $u = x + x_2, \quad v = y - y_2$ y como antes se tiene que $H(x, y) > H(u, v)$ y $H(x, y) \equiv H(u, v)(\mathrm{mód} a)$. Así, empezando con un punto látice arbitrario $(x_0, y_0)$ con coordenadas no negativas en el exterior de $R$ y usando las dos traslaciones anteriores se obtiene una cadena de puntos látices congruentes con coordenadas no negativas para los cuales los valores de $H(x, y)$ son decrecientes, cuyo último punto está en $R$. De aquí, $H(x, y)$ toma valores en cada clase residual módulo $a$ en $R$.

Comenzando en particular con $(x_0, y_0)$ el cual es congruente con $(0, 0)$ se obtiene una cadena cuyo último elemento no puede ser el punto $(0, 0)$, dado que en cada paso en la construcción de la cadena una de las coordenadas ha sido incrementado y la otra disminuida. Así, debe existir en $R$ al menos un punto látice congruente al punto $(0, 0)$ y diferente de este punto.

Supóngase que existen dos de estos puntos $(\sigma_1, \lambda_1)$ y $(\sigma_2, \lambda_2)$ que son congruentes a $(0, 0)$ con $\sigma_2 > \sigma_1$. Entonces, $(\sigma_2 - \sigma_1)b + (\lambda_2 - \lambda_1)c \equiv 0(\,\mathrm{mód}\, a)$. De donde $\lambda_2 - \lambda_1$ debe ser positivo, puesto que de otra forma se obtiene una contradicción a la escogencia de $x_1$ si $(\sigma_2 - \sigma_1)b + (\lambda_2 - \lambda_1)c$ es positivo y una contradicción a la escogencia de $y_2$ si es negativo. De esta forma $\sigma_1 < \sigma_2$ y $\lambda_1 < \lambda_2$.

Sea $(x_3, y_3)$ el punto de $R$ congruente con $(0, 0)$ con las menores coordenadas positivas. Ahora se prueba que este punto se puede obtener a partir de $(x_1, y_1)$ y $(x_2, y_2)$. Como $bx_1 - cy_1 > 0$ y $-(bx_2 - cy_2) > 0$, entonces $(bx_1 - cy_1) - (bx_2 - cy_2) > 0$ y además es congruente con cero módulo $a$. Si $y_2 - y_1 < 0$, se tiene una contradicción a la escogencia de $x_1$ y si $x_1 - x_2 < 0$ una contradicción a la escogencia de $y_2$. De esta forma $x_1 - x_2$ y $y_2 - y_1$ son positivos y el punto $(x_1 - x_2, y_2 - y_1)$ es congruente al punto $(0, 0)$ y está en $R$. Si $x_3 \neq x_1 - x_2$, supóngase sin pérdida de generalidad

$$x_3 < x_1 - x_2, \qquad y_3 < y_2 - y_1$$

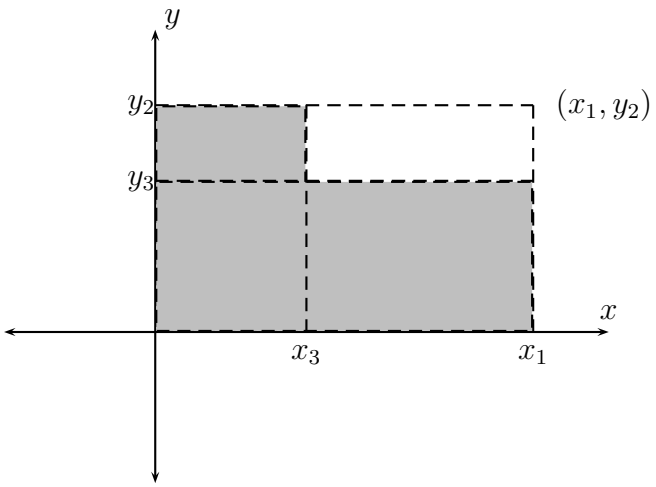
y

$$(x_2 + x_3)b - (y_2 - y_3)c \equiv 0(\mathrm{mód} a)$$

Dado que, $x_2 + x_3 < x_1$ y $0 < y_2 - y_3 < y_2$ se tiene una contradicción a la escogencia de $x_1$ ó $y_2$. En conclusión $x_3 = x_1 - x_2$ y $y_3 = y_2 - y_1$.

Sea $U$ la unión de las regiones $0 \leq x < x_1$, $0 \leq y < y_3$ y $0 \leq x < x_3$, $0 \leq y < y_2$.

Figura 2.3: Gráfica de la región en forma de $L$.




Si $(\sigma, \lambda)$ es un punto de $R$ que no está en $U$ entonces

$$H(\sigma, \lambda) \equiv H(\sigma - x_3, \lambda - y_3)(\text{mód} a)$$

y

$$H(\sigma, \lambda) > H(\sigma - x_3, \lambda - y_3).$$

De aquí los puntos látice en $U$ representan todas las clases residuales módulo $a$. Además, los puntos látices en $U$ son incongruentes módulo $a$. De otra forma si existen puntos látices congruentes $(\sigma_1, \lambda_1)$ y $(\sigma_2, \lambda_2)$ en $U$, entonces

$$0 < |\sigma_1 - \sigma_2| < x_1, 0 < |\lambda_1 - \lambda_2| < y_2$$

y

$$0 < |\sigma_1 - \sigma_2| < x_3 \quad \text{ó} \quad 0 < |\lambda_1 - \lambda_2| < y_3$$

Como $(\sigma_1 - \sigma_2)b + (\lambda_1 - \lambda_2)c \equiv 0(\text{mód} a)$ se sigue que $\sigma_1 - \sigma_2$ y $\lambda_1 - \lambda_2$ deben tener el mismo signo pues podrían llevar a la contradicción de la escogencia de $x_1$ y $y_2$. Esto no se puede tener dado que $(x_3, y_3)$ es el punto con las menores coordenadas positivas congruente con $(0, 0)$. De aquí los puntos látices de $U$ son incongruentes módulo $a$ y representan todas las clases residuales. Además los valores $H(x, y)$ que se tienen en estos puntos látices son los más pequeños para cada clase residual módulo $a$. Así, del teorema 1.6, basta con calcular el punto de $U$ donde la función $H$ alcance el máximo. Ahora $H(x, y)$, alcanza el máximo en $U$ en $(x_1 - 1, y_3 - 1)$ o en $(x_3 - 1, y_2 - 1)$. Así,

$$f(a, b, c) = \text{máx}\{x_1 b + y_3 c, x_3 b + y_2 c\} \tag{2.26}$$

$$g(a, b, c) = \text{máx}\{x_1 b + y_3 c, x_3 b + y_2 c\} - a - b - c \tag{2.27}$$

**2.4.2. Algoritmo de Davison** En lo que sigue se muestra la implementación del método de Brauer en un algoritmo computacional realizado por Davison[12].

Primero se presenta unos resultados previos necesarios en el algoritmo de Davison.

**Lema 2.3.** *Supóngase que*

$$\begin{array}{lll} 0 < x'' < x' < a, & bx' \equiv cy'(\text{mód}a), & bx' > cy', \\ 0 < y' < y'' < a, & bx'' \equiv cy''(\text{mód}a), & bx'' < cy'', \\ & x'y'' - x''y' = a. & \end{array}$$

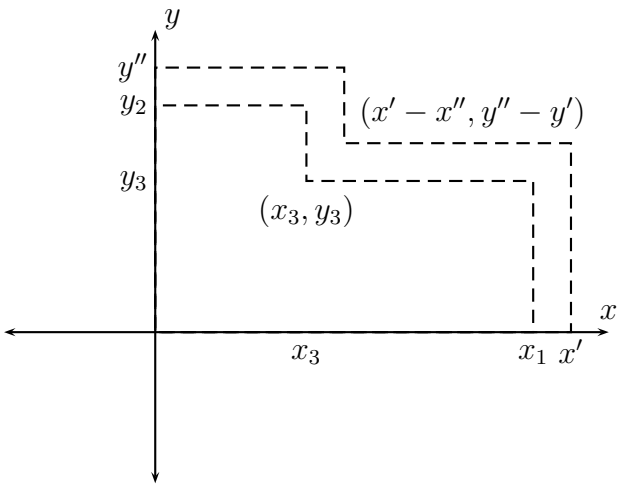
*Entonces*

$$(x', y', x'', y'') = (x_1, y_1, x_2, y_2)$$

*En la notación de la sección anterior.*

*Demostración.* Por definición $x_1 \leq x'$ y $y_2 \leq y''$. Además, $b(x' - x'') + c(y' - y'') \equiv 0(\text{mód}a)$. Del análisis hecho en el resultado de Brauer, se sigue que
$x_3 \leq x' - x'', y_3 \leq y'' - y'$. Se representa esta información en la siguiente gráfica.

Figura 2.4: Gráfica del área de la región en forma de $L$.




El área interna en forma de $L$, tiene área igual a $x_1y_2 - x_2y_1 = a$, y el área de la figura exterior en forma de $L$ tiene área $x'y'' - x''y' = a$, de esta forma las dos figuras deben ser iguales, de donde se tiene el resultado del lema. □

**Algoritmo 1** (Algoritmo de Davison)**.** *Sean $a, b, c$ tres enteros positivos.*

[12]DAVISON, J.L. (1994) *On the linear Diophantine problem of Frobenius.*

1. *Calcular* $\gcd(a,b,c)$. *Si* $\gcd(a,b,c) \neq 1$, *entonces* $f(a,b,c)$ *no existe.*

2. *Sean* $d_{12} = \gcd(a,b), d_{13} = \gcd(a,c), d_{23} = \gcd(b,c)$ *y* $a := \dfrac{a}{d_{12}d_{13}}$, $b := \dfrac{a}{d_{23}d_{12}}, c := \dfrac{c}{d_{13}d_{23}}$.

3. *Ordenar* $a, b, c$, *de tal forma que* $a < b < c$.

4. *Resolver la congruencia lineal* $bs \equiv c(\text{móda})$, *con* $0 < s < a$. *Si* $bs < c$ *entonces* $c$ *es representable por* $a, b$; *y entonces* $f(a,b,c) = ab + c$.

5. *Usar el algoritmo de Euclides en la pareja* $(s, a)$

$$\begin{aligned} a &= a_1 s + r_1 \\ s &= a_2 r_1 + r_2 \\ r_1 &= a_3 r_2 + r_3 \\ &\vdots \\ r_{m-2} &= a_m r_{m-1} + r_m, \end{aligned}$$

   *donde* $s := r_0 > r_1 > r_2 > \cdots > r_{m-1} = 1 > r_m = 0$. *De esta forma,* $s/a = [0, a_1, a_2, \ldots, a_m]$. *Y se denotan los convergentes de la fracción* $s/a$ *por* $p_i/q_i$ *para* $i = 0, \ldots, m$.

6. *Encontrar* $k$, *tal que*

$$\frac{r_{2k}}{q_{2k}} < \frac{c}{b} < \frac{r_{2k-2}}{q_{2k-2}}$$

   *Como* $bs > c$, *se tiene que* $k \geq 1$.

7. *Sea*

$$\phi(t) = \frac{r_{2k-2} - t r_{2k-1}}{q_{2k-2} + t q_{2k-1}}$$

   *Usar el método de bisección para encontrar el valor* $t^*$ *que satisface que* $\phi(t^*) < c/b < \phi(t^* - 1)$, *donde* $1 \leq t^* \leq a_{2k}$. $\phi$ *es decreciente en el intervalo* $[0, a_{2k}]$.

8. *Sea*

$$\begin{aligned} x' &= r_{2k-2} - (t^* - 1) r_{2k-1}, & y' &= q_{2k-2} + (t^* - 1) q_{2k-1}, \\ x'' &= r_{2k-2} - t^* r_{2k-1}, & y'' &= q_{2k-2} + t^* q_{2k-1}. \end{aligned}$$

   *Entonces* $f(a,b,c) = \text{máx}\{bx' + cq_{2k-1}, br_{2k-1} + cy''\}$.

**Lema 2.4.** *Con la notación del algoritmo, se tienen las siguientes identidades.*

1. $br_{2k} \equiv cq_{2k}(\text{móda})$, *para* $0 \leq k \leq \left[\dfrac{m}{2}\right]$.

2. $br_{2k-1} + cq_{2k-1} \equiv 0(\text{mód}a)$, *para* $1 \leq k \leq \left[\frac{m}{2}\right]$.

3. $r_k q_{k+1} + r_{k+1} q_k = a$, *para* $0 \leq k \leq m-1$.

*Demostración.* Las sucesiones $\{p_i\}$ y $\{q_i\}$ satisfacen las ecuaciones de recurrencia $q_{i+1} = a_{i+1}q_i + q_{i-1}, p_{i+1} = a_{i+1}p_i + p_{i-1}$ donde $q_0 = 1, q_1 = a_1, p_0 = 0$, $p_1 = 1$. Por inducción se puede demostrar que $r_i = (-1)^i(q_i s - p_i a)$, para $0 \leq i \leq m$. Como $bs \equiv c(\text{mód}a)$ y de la fórmula de $r_i$ se obtienen las partes a) y b). Para la parte c) se tiene que

$$r_k q_{k+1} + r_{k+1} q_k = (-1)^{k+1} a(p_k q_{k+1} - p_{k+1} q_k) = a$$

donde se usa que $p_k q_{k+1} - p_{k+1} q_k = (-1)^{k+1}$. □

**Teorema 2.5.** *El Algoritmo de Davison calcula* $f(a, b, c)$.

*Demostración.* Dado que $\{r_i\}$ es una sucesión decreciente y $\{q_i\}$ es creciente, se tiene que $r_i/q_i$ es una sucesión decreciente, con $r_0/q_0 = s$ y $r_{m-1}/q_{m-1} = 1/q_{m-1} \leq 1 < c/b$. Además, como, $\gcd(b, c) = 1$, es imposible que $r_i/q_i = c/b$. Así, existirá un entero $k \geq 1$, tal que

$$\frac{r_{2k}}{q_{2k}} < \frac{c}{b} < \frac{r_{2k-2}}{q_{2k-2}}$$

La demostración estará completa si se puede establecer que los valores $x', y', x'', y''$ que se encuentran en el algoritmo satisfacen las condiciones del lema 2.3 y del lema 2.4, se tiene que $bx' \equiv (cy' \text{ mód } a), bx'' \equiv cy''(\text{mód}a)$ y de su definición $bx' > cy', \quad bx'' < cy''$. Finalmente

$$\begin{aligned} x'y'' - x''y' = &(r_{2k-2} - (t^* - 1)r_{2k-1})(q_{2k-2} + t^* q_{2k-1}) \\ &- (r_{2k-2} - t^* r_{2k-1})(q_{2k-2} + (t^* - 1)q_{2k-1}) \\ =&r_{2k-2}q_{2k-1} + r_{2k-1}q_{2k-2} = a \end{aligned}$$

del lema 2.4. □

## 3. CASOS ESPECIALES

A continuación se presentará el cálculo del número de Frobenius en algunos conjuntos numéricos particulares como son: sucesiones aritméticas finitas, casi-sucesiones aritméticas finitas y una terna de números de Fibonacci.

Para el cálculo del número de Frobenius en los conjuntos de números mencionados se tendrán en cuenta propiedades de cada conjunto, posteriormente se encontrarán los $t_l$, y se aplicará el teorema 1.6.

En lo que sigue $[x]$ se entenderá como la parte entera de $x$.

### 3.1. SUCESIONES ARITMÉTICAS[1]

La sucesión $a_1, \ldots, a_n$ se denomina sucesión aritmética si $a_{i+1} = a_i + d$ para cada $i = 1, \ldots, n-1$, con $d \in \mathbb{Z}^+$.

El siguiente teorema presenta una forma para calcular el número de Frobenius de un conjunto cuyos elementos forman una sucesión aritmética. A continuación se presentan dos versiones del mismo resultado. La primera se debe a Selmer [2] en 1977 y la segunda a Bateman[3] en 1958.

**Teorema 3.1** (Selmer). *Sean $a, d$ y $k-1$ enteros positivos con $gcd(a, d) = 1$. Entonces,*

$$g(a, a+d, \ldots, a+(k-1)d) = \left[\frac{a-2}{k-1}\right] a + (a-1)d.$$

*Demostración.* Sean

$$a_1 = a, \quad a_2 = a + d, \quad a_3 = a + 2d, \ldots, a_k = a + (k-1)d, \tag{3.1}$$

donde $d > 0$, $\gcd(a, d) = 1$, y $k \leq a_1$ por el teorema 1.7. Es fácil ver que $a_1, a_2, \ldots, a_k$ son independientes.

Por el algoritmo de la división se tiene que existen enteros $t$ y $m$ tales que

$$a - 1 = t(k-1) + m; \qquad 0 \leq m < k - 1. \tag{*}$$

En el diagrama (3.2) hay $k-1$ columnas, $t$ filas completas y una fila incompleta de $m$ elementos, así se tienen $t(k-1) + m = a - 1$ elementos los cuales son representables

[1] GÓMEZ, Sergio. PALACIOS, Claudia. (2008) *El número de Frobenius en Sucesiones Aritméticas.*
[2] SELMER, Ernst. (1977) *On the linear Diophantine problem of Frobenius.*
[3] RAMIREZ, J.L. (2005) *The Diophantine Frobenius problem.*

por $a_2, a_3, \ldots, a_k$. Estos elementos son los menores enteros positivos representables por $a_2, a_3, \ldots, a_k$; en otras palabras, los elementos del sistema forman un sistema minimal $\{t_l\}$ módulo $a_1$.

$$\left.\begin{array}{lllll} a_2 & a_3 & \cdots\cdots\cdots & a_{k-1} & a_k \\ a_2+a_k & a_3+a_k & \cdots\cdots\cdots & a_{k-1}+a_k & 2a_k \\ \cdots\quad\cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots \\ a_2+(t-1)a_k & a_3+(t-1)a_k & \cdots\cdots\cdots & a_{k-1}+(t-1)a_k & ta_k \\ a_2+ta_k & a_3+ta_k\cdots & a_{m+1}+ta_k & & \end{array}\right\} \tag{3.2}$$

Sí $m > 0$, la última linea aparece, en este caso el elemento máximo de $\{t_l\}$ es el último elemento de la fila incompleta así aplicando el teorema 1.6 se tiene

$$\begin{aligned} g(a_1,a_2,a_3) = \max t_l - a_1 = a_{m+1} + ta_k - a_1 &= a + md + t(a+(k-1)d) - a \\ &= md + ta + t(k-1)d \quad \text{por} \quad (*) \\ &= md + ta + (a-1-m)d \\ &= md + ta + (a-1)d - md \\ &= ta + (a-1)d \end{aligned} \tag{a}$$

Sí $m = 0$, el elemento máximo es el último elemento de la fila completa así

$$\begin{aligned} g(a_1,a_2,a_3) = \max t_l - a_1 = ta_k - a_1 &= t(a+(k-1)d) - a \\ &= ta + t(k-1)d - a \quad \text{por} \quad (*) \\ &= a(t-1) + (a-1)d \end{aligned} \tag{b}$$

Como $a - 1 = t(k-1) + m$; $\quad 0 \leq m < k-1$; se tiene, sí $m > 0$ entonces $m - 1 \geq 0, \quad 0 \leq m - 1 < k - 2$.

Restando 1 a ambos lados de $a - 1 = t(k-1) + m$ se tiene

$$a - 2 = t(k-1) + m - 1.$$

Dividiendo por $k - 1$ se obtiene

$$\frac{a-2}{k-1} = t + \frac{m-1}{k-1}$$

dado que $\dfrac{m-1}{k-1} < 1$

$$\left[\frac{a-2}{k-1}\right] = t. \tag{3.3}$$

Sí $m = 0$ entonces, restando 1 a ambos lados de $a - 1 = t(k-1)$ resulta

$$a - 2 = t(k-1) - 1 = (t-1)(k-1) + (k-2).$$

Dividiendo por $k-1$ se deduce

$$\frac{a-2}{k-1} = t - 1 + \frac{k-2}{k-1}$$

dado que $\dfrac{k-2}{k-1} < 1$

$$\left[\frac{a-2}{k-1}\right] = t - 1. \tag{3.4}$$

En efecto, por las ecuaciones (3.3) y (3.4), las expresiones (a) y (b) para el cálculo de $g(a, a+d, \ldots, a+(k-1)d)$ pueden ser resumidas como sigue

$$g(a, a+d, \ldots, a+(k-1)d) = \left[\frac{a-2}{k-1}\right] a + (a-1)d$$

□

**Teorema 3.2** (Bateman ). *Sean $a, d$ y $s$ enteros positivos con $gcd(a,d) = 1$. Entonces,*

$$g(a, a+d, \ldots, a+sd) = \left(\left[\frac{a-2}{s}\right] + 1\right) a + (d-1)(a-1) - 1.$$

*Demostración.* Sea $y_i = \sum_{j=i}^{s} x_j$ para $i = 0, 1, \ldots, s$. Un entero positivo $L$ tiene representación por $\sum_{i=0}^{s}(a+id)x_i$ si y sólo si $L = ay_0 + d(y_1 + y_2 + \cdots + y_s)$ con $y_0 \geq y_1 \geq \cdots \geq y_s$.

Se demostrará primero que si $L$ tiene representación por $\sum_{i=0}^{s}(a+id)x_i$ entonces $L = ay_0 + d(y_1 + y_2 + \cdots + y_s)$

$$\begin{aligned}
L = \sum_{i=0}^{s}(a+id)x_i &= \sum_{i=0}^{s}(ax_i + idx_i) \\
&= a\sum_{i=0}^{s} x_i + d\sum_{i=0}^{s} ix_i \\
&= ay_0 + d(x_1 + 2x_2 + \cdots + sx_s) \\
&= ay_0 + d[(x_1 + x_2 + \cdots + x_s) + (x_2 + \cdots + x_s) \\
&+ (x_3 + x_4 + \cdots + x_s) + \cdots + x_s] \\
&= ay_0 + d\left[\sum_{i=1}^{s} x_i + \sum_{i=2}^{s} x_i + \cdots + \sum_{i=s}^{s} x_s\right] \\
&= ay_0 + d(y_1 + y_2 + \cdots + y_s).
\end{aligned}$$

Ahora se demostrará que sí $L = ay_0 + d(y_1 + y_2 + \cdots + y_s)$ entonces $L$ tiene una representación por $\sum_{i=0}^{s}(a + id)x_i$.

$$\begin{aligned}
L &= ay_0 + d(y_1 + y_2 + \cdots + y_s) \\
&= a\left(\sum_{j=0}^{s} x_j\right) + d\left(\sum_{j=1}^{s} x_j + \cdots + \sum_{j=s}^{s} x_j\right) \\
&= a\left(\sum_{j=0}^{s} x_j\right) + d\left(\sum_{j=1}^{s} x_j\right) + \cdots + d\left(\sum_{j=s}^{s} x_j\right) \\
&= a\left(\sum_{i=0}^{s} x_i\right) + d((x_1 + x_2 + \cdots + x_s) + (x_2 + \cdots + x_s) \\
&+ (x_3 + x_4 + \cdots + x_s) + \cdots + x_s) \\
&= \sum_{i=0}^{s} ax_i + d((x_1 + x_2 + \cdots + x_s) + (x_2 + \cdots + x_s) \\
&+ (x_3 + x_4 + \cdots + x_s) + \cdots + x_s) \\
&= \sum_{i=0}^{s} ax_i + d(x_1 + 2x_2 + \cdots + sx_s) \\
&= \sum_{i=0}^{s} ax_i + \sum_{i=0}^{s} dix_i \\
&= \sum_{i=0}^{s}(a + id)x_i.
\end{aligned}$$

Ahora para un entero positivo dado $y_0$, los enteros positivos $z$ que se pueden representar como

$$z = y_1 + y_2 + \cdots + y_s$$

con $y_0 \geq y_1 \geq \cdots \geq y_s$, son precisamente los enteros $z$ tales que $0 \leq z \leq sy_0$. Efectivamente, si $z = y_1 + y_2 + \cdots + y_s$, entonces

$$0 \leq z = y_1 + y_2 + \cdots + y_s \leq y_0 + y_0 + \cdots + y_0 = sy_0.$$

En consecuencia un entero $L$ es representable por $a, a + d, \ldots, a + sd$ si y sólo si $L = ay + dz$ con $0 \leq z \leq sy$.

Como resultado de la anterior afirmación, demostrar que un entero $L$ es representable por $a, a + d, \ldots, a + sd$, es equivalente a demostrar que se puede escribir en la forma $ay + dz$ con $0 \leq z \leq sy$.

Sea $R = \left(\left[\frac{a-2}{s}\right]+1\right)a+(d-1)(a-1)$; se probará que $g(a, a+d, \ldots, a+sd) = R-1$. De esta forma se mostrará que todo entero mayor o igual que $R$ es representable por $a, a+d, \ldots, a+sd$ y que $R-1$ no lo es. Entonces basta demostrar lo siguiente

1. Para todo $r \geq R$, $r = ay + dz$ con $0 \leq z \leq sy$.

2. $R-1$ no se puede representar como $ay + dz$ con $0 \leq z \leq sy$.

En efecto,

1. Sea $r \geq R$. Dado que $\gcd(a, d) = 1$ entonces existe un entero $z$ tal que $dz \equiv r(\text{mód}a)$ y $0 \leq z \leq a-1$. De aquí, $r - dz = ay$ donde $y$ es un entero. Además,

$$\begin{aligned} ay = r - dz &\geq r - d(a-1) \\ &\geq R - d(a-1) \\ &= \left(\left[\frac{a-2}{s}\right]+1\right)a + (d-1)(a-1) - d(a-1) \\ &= \left[\frac{a-2}{s}\right]a + a + d(a-1) - (a-1) - d(a-1) \\ &= \left[\frac{a-2}{s}\right]a + 1 \\ &> \left[\frac{a-2}{s}\right]a. \end{aligned}$$

   Así, $y > \left[\frac{a-2}{s}\right]$; esto es, $y \geq \left[\frac{a-2}{s}\right]+1$.

   Como

$$\frac{a-2}{s} - 1 < \left[\frac{a-2}{s}\right] \leq \frac{a-2}{s}$$

$$\frac{a-2}{s} < \left[\frac{a-2}{s}\right]+1$$

   se tiene

$$a - 2 < s\left(\left[\frac{a-2}{s}\right]+1\right) \leq sy$$

   entonces

$$sy \geq s\left(\left[\frac{a-2}{s}\right]+1\right) \geq a-1 \geq z$$

   Así, $r = ay + dz$ con $0 \leq z \leq sy$.

2. Sea $r = R-1$ y supóngase que $y$ y $z$ son enteros tales que $r = ay + dz$ con $z \geq 0$. Dado que

$$\begin{aligned} R - 1 &= \left( \left[ \frac{a-2}{s} \right] + 1 \right) a + (d-1)(a-1) - 1 \\ &= \left( \left[ \frac{a-2}{s} \right] + 1 \right) a + d(a-1) - a. \end{aligned}$$

Entonces como $r = R - 1$ se tiene que

$$ay + dz = \left( \left[ \frac{a-2}{s} \right] + 1 \right) a + d(a-1) - a$$

implica que

$$\begin{aligned} dz &\equiv \left( \left[ \frac{a-2}{s} \right] + 1 \right) a + d(a-1) - a(\text{mód} a) \\ &\equiv d(a-1)(\text{mód} a) \quad \text{y como} \quad (d,a) = 1 \\ z &\equiv (a-1)(\text{mód} a). \end{aligned}$$

De aquí, $z \geq a - 1$ y entonces,

$$\left( \left[ \frac{a-2}{s} \right] + 1 \right) a + d(a-1) - a = ay + dz \geq ay + d(a-1)$$

$$\left[ \frac{a-2}{s} \right] a \geq ay$$

$$\left[ \frac{a-2}{s} \right] \geq y.$$

Luego, $sy \leq s \left[ \frac{a-2}{s} \right] \leq a - 2 < a - 1 \leq z$. Entonces $sy < z$. Así, $r = R - 1$ no puede representarse de la forma $r = ay + dz$ con $0 \leq z \leq sy$.

Finalmente, se ha demostrado que todo entero $r \geq R$ es representable por $a, a+d. \ldots, a+sd$ y que $R-1$ no lo es, por lo tanto

$$g(a, a+d, \ldots, a+sd) = \left( \left[ \frac{a-2}{s} \right] + 1 \right) a + (d-1)(a-1) - 1.$$

□

**Teorema 3.3.** *Dados $a, h, d$ y $k$ enteros positivos con $gcd(a, d) = 1$. Entonces,*

$$g(a, ha+d, ha+2d, \ldots, ha+(k-1)d) = \left( h \left[ \frac{a-2}{k-1} \right] + h - 1 \right) a + (a-1)d.$$

*Demostración.* Sean

$$a_1 = a, \quad a_2 = ha + d, \quad a_3 = ha + 2d, \ldots, a_k = ha + (k-1)d.$$

donde $d > 0, \quad h > 1$ y $k \leq a_1$.

El diagrama (3.2) no cambia y se puede hacer un análisis similar al hecho en la demostración del teorema 3.1, para demostrar que los elementos en este diagrama forman un sistema minimal $\{t_l\}$ módulo $a_1$.

Sí $m > 0$, la última linea del diagrama aparece, en este caso el elemento máximo es el último elemento de la fila incompleta así

$$\begin{aligned} g = \text{máx}\, t_l - a_1 = a_{m+1} + ta_k - a &= a_{m+1} + t(ha + (k-1)d) - a \\ &= a_{m+1} + tha + t(k-1)d - a \\ &= a_{m+1} + tha + (a - 1 - m)d - a \\ &= ha + md + tha + (a-1)d - md - a \\ &= (ht + h - 1)a + (a-1)d. \end{aligned}$$

Si $m = 0$, el elemento máximo es el último elemento de la fila completa así

$$\begin{aligned} g = \text{máx}\, t_l - a_1 = ta_k - a_1 &= t(ha + (k-1)d) - a_1 \\ &= tha + t(k-1)d - a \\ &= tha + (a-1)d - a \\ &= (h(t-1) + h - 1)a + (a-1)d. \end{aligned}$$

En efecto, por las ecuaciones (3.3) y (3.4) las dos expresiones para el cálculo de $g(a, ha+d, \ldots, ha+(k-1)d)$ pueden ser resumidas como

$$g(a, ha+d, ha+2d, \ldots, ha+(k-1)d) = \left( h \left[ \frac{a-2}{k-1} \right] + h - 1 \right) a + (a-1)d.$$

□

## 3.2. CASI-SUCESIONES ARITMÉTICAS

En lo que sigue se presentará un teorema atribuido a Rödseth[4] que posibilita el cálculo del número de Frobenius para un conjunto de números que constituyen una casi-sucesión aritmética.

Dado el conjunto $A = \{a_0, a_1, \ldots, a_k\}$, se dice que $A$ forma una casi-sucesión aritmética si existen $e$ y $c$ en los enteros no negativos tales que

$$a_i = a_0 + ie \quad \text{para} \quad i = 1, \ldots, k \quad \text{y} \quad a_{k+1} = c.$$

En el siguiente teorema se utilizará la definición de convergentes dada en la sección (1) en la página (25) y la construcción de los residuos $s_i, \quad 1 \leq i \leq k$ dada en la sección (2), en el diagrama (2.20).

**Teorema 3.4.** *Dados $a, d, c, k$ enteros positivos con $\gcd(a, d) = 1$; Sea $s_1 = a$, y $s_0$ por $ds_0 \equiv c \bmod s_1, \quad 0 \leq s_0 < s_{-1}$. Entonces*

$g(a, a+d, a+2d, \ldots, a+kd, c) =$

$$d(s_v - 1) + c(P_{v+1} - 1) + \text{máx}\left\{a\left[\frac{s_v - s_{v+1} - 1}{k}\right] - ds_{v+1}, a\left[\frac{s_v - 2}{k}\right] - cP_v\right\}$$

*Demostración.* Sea $R_i = \dfrac{1}{a_0}(a_k s_i - kcP_i), \quad i = -1, \ldots, m+1$ que satisface la recurrencia lineal

$$R_{i+1} = q_{i+1}R_i - R_{i-1}, \qquad i = 0, \ldots, m \tag{3.5}$$

con las condiciones iniciales

$$R_0 = \frac{1}{a_0}(a_k s_0 - kcP_0) = \frac{1}{a_0}(a_k s_0 - kc).$$

ya que por definición de lo convergentes $P_0 = 1$ y

$$R_{-1} = \frac{1}{a_0}(a_k s_{-1} - kcP_{-1}) = \frac{1}{a_0}(a_k a_0) = a_k$$

debido a que $P_{-1} = 0$ y $s_{-1} = a_0$.

Como se tiene la sucesión

$$a, a+d, a+2d, \ldots, a+kd$$

con $\gcd(a, d) = 1$ se tiene que existe $s_0$ tal que

$$ds_0 \equiv c \bmod a_0 \qquad 0 \leq s_0 < s_{-1} = a_0$$

[4]RÖDSETH, Öystein. (1978) *On a linear Diophantine problem of Frobenius II.*

de este modo

$$kds_0 \equiv kc \text{ mód } a_0 \qquad 0 \leq s_0 < s_{-1} = a_0$$

se puede sumar $a_0 s_0$ sin afectar la congruencia así

$$a_0 s_0 + kds_0 \equiv kc \text{ mód } a_0 \qquad 0 \leq s_0 < s_{-1}$$

de aquí

$$(a_0 + kd)s_0 \equiv kc \text{ mód } a_0$$

como $a_k$ (el $k - simo$ término de la sucesión) es $a + kd$ resulta

$$a_k s_0 \equiv kc \text{ mód } a_0.$$

Luego $a_0|(a_k s_0 - kc)$ es decir $a_0|(a_k s_0 - kcP_0)$ de esta manera $R_0 = \dfrac{1}{a_0}(a_k s_0 - kcP_0)$ es un entero y por obvias razones $R_{-1} = a_k$ es entero.

Por lo tanto de la ecuación (3.5) se tiene que todos los $R_i$ son enteros puesto que los números enteros con las operaciones de suma y multiplicación respectivamente forma monoides.

Además por la construcción de los convergentes se sabe que $P_i \leq P_{i+1}$ es decir $P_i - P_{i+1} \leq 0$ y $s_i > s_{i+1}$ así $s_i - s_{i+1} > 0$ de donde

$$P_i - P_{i+1} \leq 0 < s_i - s_{i+1}$$

de allí se tiene lo siguiente

$$s_{i+1} < s_i$$

y multiplicando a ambos lados por $a_k$ se obtiene

$$a_k s_{i+1} < a_k s_i$$

además como $P_{i+1} \geq P_i$ se puede escribir

$$a_k s_{i+1} - kcP_{i+1} < a_k s_i - kcP_i$$

Luego

$$\frac{1}{a_0}(a_k s_{i+1} - kcP_{i+1}) < \frac{1}{a_0}(a_k s_i - kcP_i)$$

y por lo tanto

$$R_{i+1} < R_i$$

De aquí se tiene que los $R_i$ forman una sucesión decreciente

$$R_{m+1} < \ldots < R_{v+1} \leq 0 < R_v < \ldots < R_{-1}$$

Donde se usó el hecho que

$$\frac{s_{v+1}}{P_{v+1}} \leq \frac{ck}{a_k} < \frac{s_v}{P_v}$$

**Lema 3.1.** *Dados $a_o, \ldots, a_k$ enteros que satisfacen $a_i = a_0 + ie, \quad i = 1, \ldots, a_k$ para algún entero $e$. Entonces un entero $N$ es representable por $a_0, a_1, \ldots, a_k$ si y solo sí $N$ se puede representar como*

$$N = a_0 x + ey, \qquad 0 \leq y \leq kx$$

Continuando con la prueba, dado $l$, considérese ahora $t_l = t_l(a_0; a_1, \ldots, a_k, c)$ como el entero más pequeño representable por $a_1, a_2, \ldots, a_k, c$ y congruente con $l$ módulo $a_0$.

Por el lema (3.1) $t_l$ tiene una representación entera

$$t_l = a_0 x + ey + cz, \quad 0 \leq kx, z \geq 0. \tag{3.6}$$

Por la minimalidad de $t_l$, $x$ debe ser minimal con respecto a la condición $y \leq kx$, es decir $x$ debe ser el menor entero que cumpla con dicha condición.

A continuación se prueba que

1. $\dfrac{y-1}{k} - 1 < x - 1$. Como $y \leq kx$ entonces $\dfrac{y}{k} \leq x$ y por lo tanto $\dfrac{y}{k} - \dfrac{1}{k} < x$ luego $\dfrac{y-1}{k} < x$ y así $\dfrac{y-1}{k} - 1 < x - 1$.

2. $x - 1 \leq \dfrac{y-1}{k}$. Por otro lado se sabe por hipótesis que $x$ es el menor entero tal que $y \leq kx$ de este modo $k(x-1) < y$ de aquí $k(x-1) \leq y - 1$ luego $x - 1 \leq \dfrac{y-1}{k}$.

De esta manera $\dfrac{y-1}{k} - 1 < x - 1 \leq \dfrac{y-1}{k}$ y de la definición de la función parte entera

$$x - 1 = \left[\frac{y-1}{k}\right].$$

La ecuación anterior podría ser reescrita como

$$x = \left[\frac{y-1}{k}\right] + 1$$

y multiplicando a ambos lados por $a_0$

$$a_0 x = a_0 \left[\frac{y-1}{k}\right] + a_0$$

y sumando a ambos lados de la igualdad $ey + cz$ y por la ecuación (3.6) resulta

$$a_0 x + ey + cz = a_0 \left[\frac{y-1}{k}\right] + a_0 + ey + cz = t_l$$

por lo tanto

$$t_l = a_0 \left[ \frac{y-1}{k} \right] + a_0 + ey + cz. \qquad (*)$$

Se define ahora $\tau_l$ como el entero más pequeño con una representación entera

$$\tau_l = a_k y + kcz, ey + cz \equiv l \text{ mód } a_0, \quad y, z \geq 0 \qquad (3.7)$$

De donde de la ecuación $(*)$ se tiene que

$$t_l = a_0 + a_0 \left[ \frac{y}{k} - \frac{1}{k} \right] + ey + cz$$

multiplicando y dividiendo a $\frac{y}{k}$ por $a_0$ y sumando y restando dentro de $\left[ \frac{y}{k} - \frac{1}{k} \right]$ a $\frac{ey}{a_0}$ se tiene

$$t_l = a_0 + a_0 \left[ \frac{ya_0}{ka_0} - \frac{1}{k} + \frac{ey}{a_0} - \frac{ey}{a_0} \right] + ey + cz$$

Además sumando y restando $\frac{cz}{a_0}$ resulta

$$t_l = a_0 + a_0 \left[ \frac{ya_0}{ka_0} - \frac{1}{k} - \frac{ey}{a_0} + \frac{ey}{a_0} - \frac{cz}{a_0} + \frac{cz}{a_0} \right] + ey + cz$$

multiplicando y dividiendo los términos $\frac{ey}{a_0}$ y $\frac{cz}{a_0}$ por $k$ y tomando como factor común a $y$ resulta

$$t_l = a_0 + ey + cz + a_0 \left[ \frac{(a_0 + ke)y + kcz}{ka_0} - \frac{1}{k} - \frac{ey + cz}{a_0} \right]$$

como $a_0 + ke = a_k$ y por (3.7) se deduce

$$t_l = a_0 + l + a_0 \left[ \frac{a_k y + kcz}{ka_0} - \frac{1}{k} - \frac{l}{a_0} \right]$$

$$t_l = a_0 + l + a_0 \left[ \frac{1}{ka_0} \tau_l - \frac{1}{k} - \frac{l}{a_0} \right] \qquad (3.8)$$

Sea ahora $(y, z) = (y_l, z_l)$ un par de enteros que satisfacen la ecuación (3.7) y para los cuales $z_l$ es minimal.

Por la ecuación (3.7) y como $R_v = \frac{1}{a_0}(a_k s_v - kcP_v)$ se sigue que

$$\begin{aligned} \tau_l - a_0 R_v &= a_k y + kcz - a_o \left( \frac{1}{a_0}(a_k s_v - kcP_v) \right) \\ &= a_k y + kcz - a_k s_v + kcP_v \\ &= a_k(y_l - s_v) + kc(z_l + P_v) \end{aligned}$$

Por otro lado, dado que $R_i = \dfrac{1}{a_0}(a_k s_i - kcP_i) \qquad i = 1, \ldots, m+1$ y como $R_i$ es entero se deduce que $a_0|(a_k s_i - kcP_i)$ luego $a_k s_i - kcP_i \equiv 0$ mód $a_0$ de aquí $a_k s_i \equiv kcP_i$ mód $a_0$ y como $a_k = a_0 + ek$ se obtiene $(a_0 + ek)s_i \equiv kcP_i$ mód $a_0$ luego $eks_i \equiv kcP_i$ mód $a_0$ y de esta manera

$$es_i \equiv cP_i \text{ mód } a_0 \qquad i = 1, \ldots, m+1$$

De la congruencia anterior sumando $l$ a ambos lados se sigue que cuando $i = v$

$$l + es_v - cP_v \equiv l \text{ mód } a_0$$

y como $(y_l, z_l)$ cumple con la ecuación (3.7) se tiene

$$ey_l + cz_l - es_v + cP_v \equiv l \text{ mód } a_0$$

así

$$e(y_l - s_v) + c(z_l + P_v) \equiv l \text{ mód } a_0.$$

Dado que $R_v$ es un entero positivo se tiene por la definición de $\tau_l$ que $y_l - s_v < 0$ de lo contrario se tendría una contradicción ya que no puede haber un entero más pequeño, en este caso $\tau_l - a_0 R_v$, que cumpla con la definición de $\tau_l$. Donde claramente $\tau_l - a_o R_v < \tau_l$.

De manera similar se tiene

$$\tau_l + a_0 R_{v+1} = a_k(y_l + s_{v+1}) + kc(z_l - P_{v+1})$$

$z_l < P_{v+1}$ ya que $\tau_l > \tau_l + a_0 R_{v+1}$ por ser $R_{v+1} < 0$, luego por las características de $\tau_l$, $z_l < P_{v+1}$. Del mismo modo ocurre si $R_v = 0$ pero en este caso por la minimalidad de $z_l$.

Además, dado que

$$\tau_l - a_0(R_v - R_{v+1}) = a_k(y_l - s_v + s_{v+1} + kc(z_l + P_v - P_{v+1}))$$

se tiene que $y_l < s_v - s_{v+1}$ ya que $\tau_l > \tau_l - a_0(R_v - R_{v+1})$ y $\tau_l$ debe ser minimal. Por otro lado puede ocurrir $z_l < P_{v+1} - P_v$ nuevamente por las características de $\tau_l$ (ver ecuación (3.7)).

Se define ahora $A_1$ y $A_2$ como

$$\begin{aligned} A_1 =& \{(y, z) : 0 \leq y < s_v - s_{v+1}, \quad 0 \leq z < P_{v+1}\} \\ A_2 =& \{(y, z) : s_v - s_{v+1} \leq y < s_v, \quad 0 \leq z < P_{v+1} - P_v\} \end{aligned}$$

De esta manera como $y_l < s_v - s_{v+1}$ o $z_l < P_{v+1} - P_v$ se tiene que $(y_l, z_l) \in A_1 \cup A_2$ donde $A_1$ y $A_2$ son subconjuntos de puntos látices.

Sea ahora $T = \{t_l : l \in L\}$, donde $L$ es un sistema completo de residuos módulo $a_0$ y se define $S_i = \{\sigma(y,z)/(y,z) \in A_i\}, \quad i = 1,2$ donde

$$\sigma(y,z) = a_0 + a_0\left[\frac{y-1}{k}\right] + ey + cz \tag{3.9}$$

De las ecuaciones (3.7), (3.8) y (3.9) resulta

$$t_l = \sigma(y_l, z_l) \tag{3.10}$$

así

$$T \subset S_1 \cup S_2 \tag{3.11}$$

dado que $(y_l, z_l) \in A_1 \cup A_2$. Además dado que $S_iP_{i+1} - S_{i+1}P_i = a_0 \qquad i = -1, \ldots, m$ se tiene

$$|A_1 \cup A_2| = |A_1| + |A_2 \backslash A_1| = (S_v - S_{v+1})P_{v+1} + S_{v+1}(P_{v+1} - P_v) =$$

$$S_vP_{v+1} - S_{v+1}P_{v+1} + S_{v+1}P_{v+1} - S_{v+1}P_v = a_0 \tag{3.12}$$

Como $T = \{t_l : l \in L\}$ donde $L$ es un sistema completo de residuos módulo $a_0$ entonces $a_0 = |T|$ y por (3.11)

$$|T| \leq |S_1 \cup S_2| \leq |A_1 \cup A_2| = a_0$$

Por (3.12), de este modo

$$T = S_1 \cup S_2 \tag{3.13}$$

Y en consecuencia

$$g(a_0, a_0+d, a_0+2d, \ldots, a_0+kd, c) = -a_0 + \operatorname*{máx}_{l\in L} t_l = -a_0 + \text{máx}\{\sup S_1, \sup S_2\} \tag{3.14}$$

Ahora dado $a_0 = a$, $e = d$ entonces para encontrar $\sup S_1$ se debe encontrar el máximo de la función $\sigma(y,z)$ donde $(y,z) \in A_1$, por obvias razones esta función alcanza su valor máximo cuando cada coordenada $(y,z)$ sea lo más grande posible, esto ocurre precisamente según la definición de $A_1$ en $(y,z) = s_v - s_{v+1} - 1, P_{v+1} - 1$ y del mismo modo

$$\sup S_2 = \sigma(s_v - 1, s_{v+1} - s_v - 1)$$

luego de (3.9)

$$\sigma(s_v - s_{v+1} - 1, P_{v+1} - 1) = -a + a\left[\frac{s_v - s_{v+1} - 2}{k}\right] + ds_v - s_{v+1} - 1 + cP_{v+1} - 1$$

$$a\left[\frac{s_v - s_{v+1} - 2}{k}\right] - ds_{v+1} + d(s_v - 1) + c(P_{v+1} - 1) + 1$$

y

$$\sigma(s_{v-1}, P_{v+1} - P_v - 1) = a\left[\frac{s_v - 2}{k}\right] + d(s_v - 1) + c(P_{v+1} - P_v - 1)$$

$$a\left[\frac{s_v-2}{k}\right]-cP_v+d(s_v-1)+c(P_{v+1}-1)+a$$

de (3.14) y sacando el factor común $d(s_v-1)+c(P_{v+1}-1)+a$ se tiene

$$\begin{aligned} g(a,a+d,a+2d,\ldots,a+kd,c) &= -a_0+\sup\{S_1,S_2\} \\ &= -a_0+\text{máx}\{a\left[\frac{s_v-s_{v+1}-2}{k}\right]-ds_{v+1},a\lfloor\frac{s_v-2}{k}\right]-cP_v\} \end{aligned}$$

que era lo que se quería demostrar. □

## 3.3. EL NÚMERO DE FROBENIUS DE TRES NÚMEROS DE FIBONACCI

A continuación se presenta un resultado de Ramírez Alfonsín, Marín y Revuelta[5] para calcular el número de Frobenius de tres números de Fibonacci.

Los números de Fibonacci, descubiertos por Leonardo Fibonacci (1170-1240) se definen por las siguientes condiciones $F_1=1,\quad F_2=1$ y para $n\geq 2$, $F_{n+1}=F_n+F_{n-1}$.

En lo que sigue se estudiará el cálculo del número de Frobenius para una terna de números de Fibonacci, es decir $g(F_i,F_j,F_l)$ para $3\leq i<j<l$ (se asumirá que $\gcd(F_i,F_j,F_l)=1$).

Los números que son representables por $F_i,F_{i+1},F_l,\quad l\geq i+2$ también son representables por $F_i,F_{i+1}$ . En efecto, ya que los enteros que son representables por $F_i,F_{i+1}$ son de la forma $xF_i+yF_{i+1}$ con $x$ y $y$ enteros no negativos, y los enteros que son representables por $F_i,F_{i+1},F_l$ vienen descritos por la forma $xF_i+yF_{i+1}+zF_l$ con $x,y$ y $z$ enteros no negativos de allí

$$N=xF_i+yF_{i+1}+zF_l=(x+zF_{m-1})F_i+(y+zF_m)F_{i+1}.$$

Este resultado se debe al siguiente lema.

**Lema 3.2.** *Para todo* $m\geq 2$, $F_l=F_{i+m}=F_mF_{i+1}+F_{m-1}F_i$.

*Demostración.* Aplicando inducción completa sobre $m\geq 2$ se tiene

1. Se prueba para $m=2$. $F_l=F_{i+2}=F_{i+1}+F_i=1F_{i+1}+1F_i=F_2F_{i+1}+F_1F_i$
2. Supóngase que es válido para $m\leq k$ de esta manera, $F_l=F_{i+k}=F_kF_{i+1}+F_{k-1}F_i$

[5]MARÍN, J. M. RAMIREZ, J. L. REVUELTA, M. P. (2007) *On the Frobenius number of Fibonacci numerical semigroups.*

3. Ahora se demostrará para $m = k + 1$,

$$F_l = F_{i+(k+1)} = F_{i+k} + F_{i+k-1} = F_k F_{i+1} + F_{k-1} F_i + F_{k-1} F_{i+1} + F_{k-2} F_i$$

esto por el supuesto de inducción. Luego factorizando se tiene

$$F_{i+1}(F_k + F_{k-1}) + F_i(F_{k-1} + F_{k-2})$$

de allí

$$F_{i+(k+1)} = F_{i+1} F_{k+1} + F_i F_k$$

De 1, 2 y 3 se tiene que

$$F_l = F_{i+m} = F_m F_{i+1} + F_{m-1} F_i. \tag{3.15}$$

Para todo entero $m \geq 2$. □

Considérese entonces $g(F_i, F_{i+2}, F_l)$ con $l \geq i + 3$. Nótese que cuando $l = i + 3$ resulta que $\{F_i, F_{i+2}, F_{i+3}\}$ forma una sucesión aritmética dado que $F_{i+2} = F_i + F_{i+1}$ y $F_{i+3} = F_{i+1} + F_{i+2} = F_{i+1} + F_i + F_{i+1} = F_i + 2F_{i+1}$ de aquí

$$\{F_i, F_{i+2}, F_{i+3}\} = \{F_i, F_i + F_{i+1}, F_i + 2F_{i+1}\}.$$

Por tanto para el cálculo de $g(F_i, F_{i+2}, F_{i+3})$ se utiliza el teorema 3.2. Sin embargo, $\{F_i, F_{i+2}, F_{i+k}\}$ no forma una sucesión aritmética cuando $k > 3$, dado que de ser así $F_{i+k} = F_k F_{i+1} + F_{k-1} F_i = F_i + 2F_{i+1} = F_2 F_i + F_3 F_{i+1}$ de aquí al comparar coeficientes se obtiene $F_k = F_3$ y $F_{k-1} = F_2$ de esta manera lo anterior solo puede ocurrir cuando $k = 3$.

En lo que sigue se centra la atención en el cálculo de $g(F_i, F_{i+2}, F_{i+k})$ cuando $k > 3$. De esta manera se tiene el siguiente resultado

**Teorema 3.5.** *Dados los enteros $i, k > 3$ y sea $r = \left[\frac{F_{i-1}}{F_k}\right]$. Entonces*

$$g(F_i, F_{i+2}, F_{i+k}) = \begin{cases} (F_i - 1)F_{i+2} - F_i(rF_{k-2} + 1) & \text{si } r = 0 \text{ o } r \geq 1 \text{ y} \\ & F_{k-2}F_i < (F_i - rF_k)F_{i+2}, \\ (rF_k - 1)F_{i+2} - F_i((r-1)F_{k-2} + 1) & \text{en otro caso} \end{cases}$$

Sea $T^* = \{t_0^*, \ldots, t_{F_{i-1}}^*\}$ donde $t_l^*$ es el entero positivo más pequeño congruente con $l$ módulo $F_i$ que es representable como combinación lineal de $F_{i+2}$ y $F_{i+k}$ con coeficientes enteros no negativos. Por teorema 1.6 para calcular $g(F_i, F_{i+2}, F_{i+k})$ es suficiente encontrar $t_l^*$ para cada $l = 0, 1, \ldots, F_{i-1}$. Para este fin se considera todas las combinaciones enteras no negativas de $F_{i+2}$ y $F_{i+k}$. Se construye la tabla $T_1$ que tiene como entradas $t_{x,y}$ las combinaciones de la forma $xF_{i+2} + yF_{i+k}$ con enteros $x, y \geq 0$

| $x\backslash y$ | 0 | 1 | 2 | $\cdots$ |
|---|---|---|---|---|
| 0 | 0 | $F_{i+k}$ | $2F_{i+k}$ | $\cdots$ |
| 1 | $F_{i+2}$ | $F_{i+k}+F_{i+2}$ | $2F_{i+k}+F_{i+2}$ | $\cdots$ |
| 2 | $2F_{i+2}$ | $F_{i+k}+2F_{i+2}$ | $2F_{i+k}+2F_{i+2}$ | $\cdots$ |
| 3 | $3F_{i+2}$ | $F_{i+k}+3F_{i+2}$ | $2F_{i+k}+3F_{i+2}$ | $\cdots$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | |
| $F_k-1$ | $(F_k-1)F_{i+2}$ | $F_{i+k}+(F_k-1)F_{i+2}$ | $2F_{i+k}+(F_k-1)F_{i+2}$ | $\cdots$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | |

Usando la ecuación (3.15)

$$\begin{aligned} F_{i+k} &= F_kF_{i+1}+F_{k-1}F_i \\ &= F_kF_{i+1}+F_{k-1}(F_{i+2}-F_{i+1}) \\ &= F_kF_{i+1}+F_{k-1}F_{i+2}-F_{k-1}F_{i+1} \\ &= (F_k-F_{k-1})F_{i+1}+F_{k-1}F_{i+2} \\ &= F_{k-2}F_{i+1}+F_{k-1}F_{i+2} \end{aligned}$$

Luego

$$F_{i+k}=F_{k-2}F_{i+1}+F_{k-1}F_{i+2}=F_{k-2}(F_{i+2}-F_i)+F_{k-1}F_{i+2}=F_{i+2}F_k-F_{k-2}F_i$$

Así se obtiene que

$$xF_{i+2}+yF_{i+k}=xF_{i+2}+y(F_{i+2}F_k-F_{k-2}F_i)=(x+yF_k)F_{i+2}-yF_{k-2}F_i.$$

Por tanto, $T_1$ puede ser dada por la siguiente tabla, denotada por $T_2$,

| $x\backslash y$ | 0 | 1 | $\cdots$ | $r$ | $\cdots$ |
|---|---|---|---|---|---|
| 0 | 0 | $F_kF_{i+2}-F_{k-2}F_i$ | $\cdots$ | $rF_kF_{i+2}-rF_{k-2}F_i$ | $\cdots$ |
| 1 | $F_{i+2}$ | $(1+F_k)F_{i+2}-F_{k-2}F_i$ | $\cdots$ | $(1+rF_k)F_{i+2}-rF_{k-2}F_i$ | $\cdots$ |
| 2 | $2F_{i+2}$ | $(2+F_k)F_{i+2}-F_{k-2}F_i$ | $\cdots$ | $(2+rF_k)F_{i+2}-rF_{k-2}F_i$ | $\cdots$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | | $\vdots$ |
| $l$ | $lF_{i+2}$ | $(l+F_k)F_{i+2}-F_{k-2}F_i$ | $\cdots$ | $(l+rF_k)F_{i+2}-rF_{k-2}F_i$ | $\cdots$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | | $\vdots$ |
| $F_k-1$ | $(F_k-1)F_{i+2}$ | $(2F_k-1)F_{i+2}-F_{k-2}F_i$ | | $\cdots$ | |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | | $\vdots$ |

Sea $S$ el conjunto formado por las $F_k-1$ entradas de las columnas $0,1,2,\ldots$; es decir

$$S=\{t_{0,0},t_{1,0},\ldots,t_{F_k-1,0},t_{0,1},t_{1,1},\ldots,t_{F_k-1,1},\ldots,t_{0,r},t_{1,r},\ldots,t_{F_k-1,r},\ldots\}.$$

**Lema 3.3.** *Con la notación anterior se tienen las siguientes propiedades*

1. *Sean* $r = \left[\dfrac{F_i - 1}{F_k}\right]$ *y* $F_i - 1 = rF_k + l$ *para algún entero* $0 \leq l \leq F_k - 1$. *Sea*

$$S' = \{t_{0,0}, t_{1,0}, \ldots, t_{F_k-1,0}, t_{0,1}, t_{1,1}, \ldots, t_{F_k-1,1}, \ldots, t_{0,r}, t_{1,r}, \ldots, t_{l,r}\}$$

*Entonces, cada* $t_{x,y} = (x + yF_k)F_{i+2} - yF_{k-2}F_i \in S'$, *se tiene que* $0 \leq x + yF_k \leq F_i - 1$. *Además, dado que* $\gcd(F_{i+2}, F_i) = 1$, *entonces* $S'$ *constituye un sistema completo de residuos módulo* $F_i$.

2. *Los elementos de* $S$ *se pueden representar como* $s_x = xF_{i+2} - \left[\dfrac{x}{F_k}\right] F_{k-2}F_i$ *para* $x = 0, 1, 2 \ldots$.

   *De esta forma se tiene que* $S = \cup_{q\geq 0} S_q$, *donde*

$$S_q = \{s_{qF_k}, s_{qF_k+1}, \ldots, s_{(q+1)F_k-1}\} = \{t_{0,q}, \ldots, t_{F_k-1,q}\}$$

   *para cada entero* $q = 0, 1, 2, \ldots$.

3. *Si* $i \leq k$ *y* $j \leq l$, *entonces* $t_{i,j} \leq t_{k,l}$.

*Demostración.* 1. Para probar que $S'$ constituye un sistema completo de residuos módulo $F_i$ basta demostrar que $|S'| = F_i$ y que los elementos de $S'$ son incongruentes módulo $F_i$. Como los elementos de $S'$ son de la forma $t_{x,y}$ con $0 \leq x \leq F_k - 1, 0 \leq y \leq r-1$ y $t_{x,r}$ con $0 \leq x \leq l$, entonces $|S'| = rF_k + l + 1 = F_i$. Sea $t_{x,y} = (x + yF_k)F_{i+2} - yF_{k-2}F_i \in S'$, con $0 \leq x + yF_k \leq F_i - 1$. Como $\gcd(F_i, F_{i+2}) = 1$, entonces los elementos $(x + yF_k)F_{i+2}$ forman un sistema completo de residuos módulo $F_i$ y en consecuencia $S'$ también lo es.

2. Note que $S = \cup_{q\geq 0}\{t_{0,q}, \ldots, t_{F_{k-1},q}\}$. Y como

$$s_{qF_k} = qF_kF_{i+2} - \left[\frac{qF_k}{F_k}\right] F_{k-2}F_i = qF_kF_{i+2} - qF_{k-2}F_i = t_{0,q}$$

$$\begin{aligned} s_{qF_k+1} =& (qF_k + 1)F_{i+2} - \left[\frac{qF_k + 1}{F_k}\right] F_{k-2}F_i \\ =& (1 + qF_k)F_{i+2} - qF_{k-2}F_i = t_{1,q} \end{aligned}$$

$$\vdots$$

$$\begin{aligned} s_{qF_k+F_k-1} =& s_{(q+1)F_k-1} = ((q+1)F_k - 1)F_kF_{i+2} - \left[\frac{(q+1)F_k - 1}{F_k}\right] F_{k-2}F_i \\ =& (F_k - 1 + qF_k)F_{i+2} - qF_{k-2}F_i = t_{F_k-1,q} \end{aligned}$$

Entonces $S_q = \{s_{qF_k}, s_{qF_k+1}, \ldots, s_{(q+1)F_k-1}\} = \{t_{0,q}, \ldots, t_{F_k-1,q}\}$ y por lo tanto $S = \cup_{q\geq 0} S_q$.

3. De la definición de $t_{i,j}$.

□

**Lema 3.4.** *Sea $t_{u,v}$ una entrada de $T_1$, tal que $t_{u,v} \notin S'$. Entonces, existe $t_{x,y} \in S'$, tal que $t_{u,v} \equiv t_{x,y} (\text{mód} F_i)$ y $t_{u,v} > t_{x,y}$.*

*Demostración.* Se tienen los siguientes casos

1. **Caso A** Supóngase que $t_{u,v} \in S \setminus S'$. Entonces $t_{u,v}$ es de la forma $s_{pF_i+g}$ para algunos enteros $p \geq 1$ y $0 \leq g \leq F_i - 1$. Se sigue que

$$\begin{aligned} s_g &= gF_{i+2} - \left[\frac{g}{F_k}\right] F_i F_{k-2} \\ &\equiv (pF_i + g)F_{i+2} - \left[\frac{pF_i + g}{F_k}\right] F_i F_{k-2} = s_{pF_i+g} (\text{mód} F_i) \end{aligned}$$

   A continuación se prueba que $s_{pF_i+g} > s_g$. Para esto, es suficiente demostrar que $s_{F_i+g} > s_g$ (dado que $s_{pF_i+g} \geq s_{F_i+g}$). Se tienen entonces dos subcasos

   *a*) Si $r = 0$ entonces $F_k \geq F_i$. Si $F_k = F_i$, entonces

$$\begin{aligned} s_{F_i+g} =& (F_i + g)F_{i+2} - \left[\frac{F_i + g}{F_k}\right] F_{k-2} F_i \\ =& (g + F_k)F_{i+2} - F_{k-2}F_i = t_{g,1} \end{aligned}$$

   y del lema 3.3 se tiene que $t_{g,0} < t_{g,1}$. Es decir $t_{g,0} = S_g < S_{F_i+g} \leq S_{pF_i+g}$. Si $F_k > F_i$ entonces

$$\begin{aligned} s_{F_i+g} =& (F_i + g)F_{i+2} - \left[\frac{F_i + g}{F_k}\right] F_i F_{k-2} \\ =& (F_i + g + 0F_k)F_{i+2} \quad \text{Sea} \quad q = F_i + g \geq F_i \\ =& (q + 0F_k)F_{i+2} = t_{q,0} \end{aligned}$$

   $s_{F_i+g} = t_{q,0}$ para $q = F_i + g \geq F_i$ y del lema 3.3 $t_{g,0} < t_{q,0}$. Así $s_g < s_{F_i+g} \leq S_{pF_i+g}$.

   *b*) Si $r \geq 1$, entonces $s_{F_i+g} > s_g$ si y sólo si

$$(F_i + g)F_{i+2} - \left[\frac{F_i + g}{F_k}\right] F_i F_{k-2} > gF_{i+2} - \left[\frac{g}{F_k}\right] F_i F_{k-2}$$

   o equivalentemente si

$$F_{i+2} > F_{k-2} \left( \left[\frac{F_i + g}{F_k}\right] - \left[\frac{g}{F_k}\right] \right)$$

Sea $g = mF_k + n$ con $0 \leq n \leq F_k - 1$. Dado que $F_i - 1 = rF_k + l$ con $0 \leq l \leq F_k - 1$, entonces

$$\begin{aligned}\left[\frac{F_i - 1 + g + 1}{F_k}\right] = \left[\frac{rF_k + l + mF_k + n + 1}{F_k}\right] \\ \leq \frac{rF_k + l + mF_k + n + 1}{F_k} \\ \leq r + m + \frac{l + n + 1}{F_k} \\ \leq r + m + 1.\end{aligned}$$

Ahora dado que

$$g = mF_k + n$$

Dividiendo ambos lados entre $F_k$ se obtiene

$$\frac{g}{F_k} = m + \frac{n}{F_k}$$

Sea $\dfrac{n}{F_k} < 1$ entonces

$$\left[\frac{g}{F_k}\right] = m$$

y así

$$\left[\frac{F_i + g}{F_k}\right] - \left[\frac{g}{F_k}\right] \leq r + m + 1 - m = r + 1$$

En consecuencia es suficiente demostrar que $F_{i+2} > (r+1)F_{k-2}$ o lo que es equivalentemente mostrar que $F_i + F_{i+1} > (r+1)F_{k-2}$. Dado que $F_i = rF_k + l + 1$ entonces la última desigualdad se tiene si y sólo si $rF_k + l + 1 + F_{i+1} > rF_{k-2} + F_{k-2}$, y esto es cierto si y sólo si

$$r(F_k - F_{k-2}) + l + 1 + F_{i+1} = r(F_{k-1}) + l + 1 + F_{i+1} > F_{k-2}$$

lo que es cierto dado que $r \geq 1$.

2. **Caso B** Supóngase que $t_{u,v} \notin S$. Entonces se tiene que $0 \leq x \leq F_k - 1 < u$. Si $v \geq y$, entonces, del lema 3.3, $t_{x,y} < t_{x,v} < t_{u,v}$. Mientras que si $v < y$. Dado que $t_{u,v} \equiv t_{x,y} (\text{mód} F_i)$ entonces $u + vF_k \equiv x + yF_k (\text{mód} F_i)$ y del lema 3.3 como $0 \leq x + yF_k \leq F_i - 1$, entonces $u + vF_k = d(x + yF_k)$ para algún entero $d \geq 1$ y así $u + vF_k \geq x + yF_k$. Además, como $v < y$, entonces $-vF_{k-2}F_i > -yF_{k-2}F_i$. Luego, de estas dos desigualdades

$$t_{u,v} = (u + vF_k)F_{i+2} - vF_{k-2}F_i > (x + yF_k)F_{i+2} - yF_{k-2}F_i = t_{x,y}$$

□

Ahora se presenta la prueba del teorema 3.5

*Demostración del Teorema 1.* Sea $T^* = \{t_0^*, \ldots, t_{F_i-1}^*\}$ donde $t_l^*$ es el menor entero positivo congruente con $l$ módulo $F_i$ representable por $F_{i+2}, F_{i+k}$. Sea

$$s_x = xF_{i+2} - \left\lfloor \frac{x}{F_k} \right\rfloor F_{k-2}F_i$$

para $x = 0, 1, \ldots$. Del lema 3.4, se tiene que para cada $x = 0, \ldots, F_i - 1$, $s_x$ es el menor entero positivo congruente con $l$ módulo $F_i$ representable por $F_{i+2}, F_{i+k}$; es decir $S' = T^*$. Ahora del lema 3.3, si $r \geq 1$ entonces

$$t_{F_k-1,i} = \max_{0 \leq x \leq F_k - 1} \{t_{x,i} : t_{x,i} \in S'\}$$

para cada $i = 0, \ldots, r-1$. Además

$$t_{F_k-1,r-1} = \max_{0 \leq i \leq r-1} \{t_{F_k-1,i} : t_{F_{k-1},i \in S'}\}$$

y

$$t_{l,r} = \max_{0 \leq x \leq l} \{t_{x,r} : t_{x,r} \in S'\}$$

Así,

$$\max\{s : s \in S'\} = \begin{cases} t_{l,r} & \text{si } r = 0 \\ \max\{t_{F_k-1,r-1}, t_{l,r}\} & \text{en otro caso} \end{cases}$$

Ahora $t_{l,r} > t_{F_{k-1},r-1}$ si y sólo si

$$\begin{aligned} t_{l,r} = (rF_k + l)F_{i+2} - rF_{k-2}F_i &= (F_i - 1)F_{i+2} - rF_{k-2}F_i \\ &> (rF_k - 1)F_{i+2} - (r-1)F_{k-2}F_i \\ &> (rF_k + F_k - F_k - 1)F_{i+2} - (r-1)F_{k-2}F_i \\ &> (F_k - 1 + (r-1)F_k)F_{i+2} - (r-1)F_{k-2}F_i \\ &= t_{F_{k-1},r-1}. \end{aligned}$$

o de forma equivalente si

$$\begin{aligned} (F_i - 1)F_{i+2} - rF_{k-2}F_i &> (rF_k - 1)F_{i+2} - (r-1)F_{k-2}F_i \\ F_iF_{i+2} &> rF_kF_{i+2} + F_{k-2}F_i \\ F_{i+2}(F_i - rF_k) &> F_{k-2}F_i \end{aligned}$$

de donde se obtiene el resultado del teorema 3.5 es decir

- Si $r = 0$ o si $r \geq 1$ y $F_{i+2}(F_i - rF_k) > F_{k-2}F_i$ entonces

$$\begin{aligned} g(F_i, F_{i+2}, F_{i+k}) &= t_{l,r} - F_i \\ &= (rF_k + l)F_{i+2} - rF_{k-2}F_i - F_i \\ &= (F_i - 1)F_{i+2} - F_i(rF_{k-2} + 1). \end{aligned}$$

- De otra forma

$$\begin{aligned} g(F_i, F_{i+2}, F_{i+k}) =& t_{F_k-1,r-1} - F_i \\ =& (rF_k - 1)F_{i+2} - F_i((r-1)F_{k-2} + 1). \end{aligned}$$

□

# 4. PROBLEMAS ABIERTOS Y CONCLUSIONES

## 4.1. PROBLEMAS ABIERTOS

Recae en el interés de los autores mostrar algunos problemas relacionados al presente trabajo que aún están abiertos para la investigación y que se espera sean tenidos en cuenta para futuras investigaciones.

**4.1.1. Algoritmos eficientes** Todos los algoritmos que se presentan en el apéndice y en general los estudiados a lo largo de este trabajo, funcionan de manera eficiente cuando el tamaño de los números es relativamente pequeño. En general un problema difícil es encontrar algoritmos eficientes[1].

**4.1.2. Fórmulas sencillas** Además son problemas abiertos el encontrar fórmulas simples para el cálculo particularmente de $g(a_1, a_2, a_3)$ y $n(a_1, a_2, a_3)$, en donde esta última permite calcular el número de enteros no representables por $a_1, a_2$ y $a_3$. En general se requiere encontrar fórmulas simples para calcular $g(a_1, a_2, \ldots, a_k)$ y $n(a_1, a_2, \ldots, a_k)$, entendiendo por fórmula simple aquella cuya estructura sea polinomial.

**4.1.3. Generalización:** $g_k(a_1, a_2, a_3)$ En general como el lector podrá haber observado en este trabajo, no interesaba el número de representaciones que pueda tener un número, sin embargo es interesante recalcar que un número puede ser representable más de una vez por un conjunto $A = \{a_1, a_2, a_3\}$, es decir dicho número se puede escribir de diferentes manera como combinación lineal de $a_1, a_2$ y $a_3$ con coeficientes enteros no negativos. En este sentido, $g_k(a_1, a_2, a_3)$ indica el mayor número no representable por $A$ con $k + 1$ representaciones. Vale la pena mencionar que

$$g_0(a_1, a_2, a_3) = g(a_1, a_2, a_3).$$

En una manera formal sea

$$\sigma(n) = \#\{(x, y, z) : a_1x + a_2y + a_3z = n, x, y, z \geq 0\}$$

Con $g_k(a_1, a_2, a_3)$ se denota el mayor entero $n$ tal que $\sigma(n) \geq k + 1$. Encontrar $g_k(a_1, a_2, a_3)$, que es un problema que merece ser estudiado en futuras investigaciones.

[1]SHALLIT, Jeffrey. (2001) *The Computational complexity of the local pastage stamp problem.*

## 4.2. CONCLUSIONES

- A lo largo de este documento se notó la importancia del teorema 1.6 en todos los métodos para el cálculo de $g(a_1, a_2, a_3)$ puesto que en cada uno de ellos se construye un sistema completo minimal de residuos módulo $a_1$ y por consiguiente se obtienen los $t_l$, posteriormente todo se reduce a àplicar el teorema 1.6. Vale la pena recalcar que el procedimiento empleado para calcular el número de Frobenius para conjuntos de números especiales es similar al sequido en cada uno de los métodos.

- La utilización de Fracciones continuas en el desarrollo de algunos de los métodos es esencial para la implementación de estos en algoritmos que permitan el cálculo de $g(a_1, a_2, a_3)$.

- En el método de *Selmer* y *Beyer* se hace necesario la introducción de la función $M$ para simplificar su fórmula explícita para el cálculo de $g(a_1, a_2, a_3)$ lo que permite implementar este método de forma menos compleja en un algoritmo.

- Las fórmulas explícitas obtenidas por *Selmer* y *Bateman* (ver sección 3) para el cálculo del número de Frobenius en Sucesiones Aritméticas finitas son equivalentes, basta con observar que $s = k - 1$ y proceder a efectuar algunos procedimientos aritméticos.

- El cálculo del número de Frobenius para casos especiales, es decir para conjuntos de números con ciertas características, fue posible gracias a la utilización de propiedades aritméticas de cada uno de estos conjuntos.

# A. ALGORITMOS

Los algoritmos que se presentan a continuación fueron utilizados en el desarrollo del trabajo. Estos algoritmos están implementados en el sistema de álgebra computacional MuPAD.
En realidad estudiar la complejidad de estos algoritmos se sale de los objetivos del presente trabajo y podría ser estudiado en un trabajo posterior.

## A.1. ALGORITMO REPRES

Este algoritmo recibe cuatro enteros positivos $n, a, b, c$, si $n$ es representable por $a, b$ y $c$ el algoritmo muestra las ternas y el número de ellas que son de la forma $[i, j, z] \in \mathbb{Z}^+ \times \mathbb{Z}^+ \times \mathbb{Z}^+$, tales que $n = ai + bj + cz$, en caso contrario devuelve la nota 'No es representable'.

```
repres:=proc(n,a,b,c)
local i,j,z,t,l,p,q;
begin
 q:=n div a;
 l:=n div b;
 p:=n div c;
 t:=0;
  for i from 0 to q do
     for j from 0 to l do
        for z from 0 to p do
            m:=i*a+j*b+z*c;
              if m=n then
               print([i,j,z]);
               t:=t+1;
              end_if;
        end_for;
     end_for;
  end_for;
if t=0 then
 print('No es representable')
  else
 print(t)
end_if;
end_proc;
```

**Ejemplo 3.** Como 12 no es representable por 13, 5 y 17, esto significa que el algoritmo `repres` retorna 'No es representable'

```
repres(12,13,5,17)
                                'No es representable'
```

Pero como 30 es representable por $13, 5$ y 17, el algoritmo entrega la lista de ternas, además del número de veces que 30 es representable por $13, 5$ y 17 así

```
repres(30,13,5,17)
                                        [0, 6, 0]
                                        [1, 0, 1]
                                            2
```

## A.2. ALGORITMO DE HOFMEISTER

Este algoritmo recibe tres enteros positivos. Si los tres enteros no son primos relativos el algoritmo retorna "cambie de base", en caso contrario produce el número de Frobenius aplicando el método de Hofmeister.(ver sección 2).

```
hofm:=proc(a1,a2,a3)
 begin
if gcd(a1,a2,a3)>1 then
print("cambie de base")
else
M:=sort([a1,a2,a3]);
a1:=M[1];
a2:=M[2];
a3:=M[3];
d1:=igcd(a1,a2);
d2:=igcd(a1,a3);
d3:=igcd(a2,a3);
a1:=a1 div (d1*d2);
a2:=a2 div (d1*d3);
a3:=a3 div (d2*d3);
if a1=1 or a2=1 or a3=1 then
g:=-1
else
L:=numlib::lincongruence(a2,a3,a1);
s:=L[1];
t:=(s*a2-a3)/a1;
q:=a1 div s;
r:=a1 mod s;
if (q+1)*a3>=(s-r)*a2 then
g:=max((s-1)*a2+(q-1)*a3,(r-1)*a2+q*a3)-a1;
end_if;
end_if;
d1*d2*d3*g+d1*d2*a1*(d3-1)+a2*d1*d3*(d2-1)+a3*d2*d3*(d1-1);
```

```
end_if;
end_proc;
```

**Ejemplo 4.** Particularmente para 13, 25 y 26 el algoritmo `hofm` muestra que el número de frobenius de dichos números es

```
hofm(13,25,26)
287
```

## A.3. ALGORITMO DE SELMER

El siguiente algoritmo recibe tres enteros positivos. Si los tres enteros no son primos relativos el algoritmo entrega como respuesta el mensaje "cambie de base". Si los tres enteros son primos relativos el algoritmo retorna el número de Frobenius utilizando el método de Selmer y Beyer expuesto en la sección 2.

```
selmer:=proc(a1,a2,a3)
local r0,q0,r1,q1,r2,q2,r3,q3,P0,P1,P2,P3,m,g;
begin
if gcd(a1,a2,a3)>1 then
print("cambie de base")
else
M:=sort([a1,a2,a3]);
a1:=M[1];
a2:=M[2];
a3:=M[3];
d1:=igcd(a1,a2);
d2:=igcd(a1,a3);
d3:=igcd(a2,a3);
a1:=a1 div (d1*d2);
a2:=a2 div (d1*d3);
a3:=a3 div (d2*d3);
if a1=1 or a2=1 or a3=1 then
g:=-1
else
L:=numlib::lincongruence(a2,a3,a1);
s:=L[1];
r0:= a1 mod s;
q0:= a1 div s;
  if (q0+1)*a3>=(s-r0)*a2 then
  return(max((s-1)*a2+(q0-1)*a3,(r0-1)*a2+q0*a3)-a1);
  end_if;
r1:= s mod r0;
q1:= s div r0;
P0:=q0;
```

```
P1:=q0*q1+1;
m:=float(a3/a2);
q3:=q1;
P:=1;
r:=s;
r2:=r0;
P2:=P0;
 while float(r1/P1)> m do
 r2:= r0 mod r1;
 q2:= r0 div r1;
 r3:= r1 mod r2;
 q3:= r1 div r2;
 P2:=P0+q2*P1;
 P3:=P1+q3*P2;
 P:=P1;
 r:=r1;
 r0:= r2;
 q0:= q2;
 r1:=r3;
 q1:=q3;
 P0:=P2;
 P1:=P3;
 end_while;
L:=[];
for i from 0 to q3-1 do
 L:=[op(L),(r-(i+1)*r2)*a2,(P+i*P2)*a3];
 g:=-a1+(r2-1)*a2+(P0-1)*a3+op(sort(L),nops(L)/2+1);
end_for;
end_if;
d1*d2*d3*g+d1*d2*a1*(d3-1)+a2*d1*d3*(d2-1)+a3*d2*d3*(d1-1);
end_if;
end_proc;
```

**Ejemplo 5.** Particularmente para $137, 251$ y $256$ el algoritmo `selmer` muestra que el número de frobenius de dichos números es

```
selmer(137,251,256)
4948
```

## A.4. ALGORITMO DE RÖDSETH

El algoritmo de `rodseth` recibe tres enteros positivos, si estos son primos relativos retorna el número de Frobenius utilizando el método de Rödseth presentado en la sección 2, en caso contrario el algoritmo produce la nota "cambie de base".

```
rodseth:=proc(a,b,c)
local i,j,d1,d2,d3,r;
begin
if igcd(a,b,c)>1 then
print("cambie de base")
else
d1:=igcd(a,b);
d2:=igcd(a,c);
d3:=igcd(b,c);
a:=a div (d1*d2);
b:=b div (d1*d3);
c:=c div (d2*d3);
if a=1 or b=1 or c=1 then
r:=-1 else
L:=numlib::lincongruence(b,c,a);
s0:=L[1];
q1:=a div s0;
q1:=q1+1;
s1:=(a mod s0)-s0;
s:=-s1;
t:=s0;
P0:=1;
P1:=q1*P0;
P:=P1;
 while not(s/P<c/b and c/b<t/P0)  do
 q:=t div s;
 q:=q+1;
 i:=s;
 s:=(t mod s)-s;
 s:=-s;
 t:=i;
 j:=P;
 P:=q*P-P0;
 P0:=j;
 end_while;
r:=-a+b*(t-1)+c*(P-1)-min(b*s,c*P0);
end_if;
d1*d2*d3*r+d1*d2*a*(d3-1)+b*d1*d3*(d2-1)+c*d2*d3*(d1-1);
end_if;
end_proc;
```

**Ejemplo 6.** Particularmente para $137, 251$ y $256$ el algoritmo `rödseth` muestra que el número de frobenius de dichos números es

```
rodseth(137,251,256)
4948
```

## A.5. ALGORITMO DE DAVISON

**A.5.1. Algoritmo de Bisección** El algoritmo `biseccionD` se utiliza en el método de Davison y en la implementación del algoritmo `davison` presentado en esta misma sección.

```
biseccionD:=proc(s,t,c,b,r1,r2,q1,q2)
local p1,p2,m;
begin
p1:=poly(r2-x*r1);
p2:=poly(q2+x*q1);
if (p1(s)/p2(s)-c/b)<0 and (p1(s-1)/p2(s-1)-c/b)>0 then
  return(s);
end_if;
if (p1(t)/p2(t)-c/b)<0 and (p1(t-1)/p2(t-1)-c/b)>0 then
  return(t);
end_if;
m:=floor((s+t)/2);
while not ((p1(m)/p2(m)-c/b)<0 and
p1(m-1)/p2(m-1)-c/b)>0) do
 if (p1(s)/p2(s)-c/b)*(p1(m)/p2(m)-c/b)<0 then
  t:=m
else
  s:=m;
end_if;
m:=ceil((s+t)/2);
end_while;
m;
end_proc;
```

**A.5.2. Algoritmo de Davison**
El algoritmo `davison`, se basa en lo presentado en las secciones 2 y 2.3. Este algoritmo recibe tres enteros positivos primos relativos entre sí y retorna su número de Frobenius.

```
davison:=proc(a,b,c)
local s,r1,r2,q1,q2,t0,m;
begin
if igcd(a,b,c)>1 then
print("cambie de base")
else
d1:=igcd(a,b);
d2:=igcd(a,c);
d3:=igcd(b,c);
```

```
a:=a div (d1*d2);
b:=b div (d1*d3);
c:=c div (d2*d3);
if a=1 or b=1 or c=1 then
g:=-1
else
L:=numlib::lincongruence(b,c,a);
s:=L[1];
r0:=s;
q0:=1;
r1:=a mod s;
a1:=a div s;
q1:=a1;
r2:= s mod r1;
a2:= s div r1;
q2:=a2*q1+q0;
while not(r2/q2<c/b and c/b <r0/q0) do
r:= r1 mod r2;
r0:=r2;
q0:=q2;
m:= r1 div r2;
q1:=m*q2+q1;
r1:=r;
a1:=m;
r:=r2 mod r1;
m:=r2 div r1;
r2:= r;
a2:= m;
q2:=a2*q1+q2;
end_while;
t0:=biseccionD(0,a2,c,b,r1,r0,q1,q0);
 x1:=r0-(t0-1)*r1;
 x2:=r0-t0*r1; y1:=q0+(t0-1)*q1;
 y2:=q0+t0*q1;
g:=max(b*x1+c*q1,b*r1+c*y2)-a-b-c;
end_if;
d1*d2*d3*g+d1*d2*a*(d3-1)+b*d1*d3*(d2-1)+c*d2*d3*(d1-1);
end_if;
end_proc;
```

**Ejemplo 7.** Particularmente para $137, 251$ y $256$ el algoritmo `davison` muestra que el número de Frobenius de dichos números es

```
davison(137,251,256)
```

4948

## BIBLIOGRAFÍA


BEYER, Öyvind. SELMER, Ernst. (1978) *On the linear Diophantine problem of Frobenius in three variables*, J. Reine Angew. Math.301, 161-170, MR 0557015(58#27740).

BRAUER, Alfred. SHOCKLEY, James. (1962) *On a problem of Frobenius*. J. Reine Angew. Math.211, 215-220, MR 0148606(26#6116).

DAVISON, J.L. (1994) *On the linear Diophantine problem of Frobenius*. J. Number Theory 48, 353-363, MR 1293866(95j:11033).

GÓMEZ, Sergio. PALACIOS, Claudia. (2008) *El número de Frobenius en Sucesiones Aritméticas*. Revista Sigma. Universidad de Nariño. Revista en proceso de edición. Pasto.

GORDILLO, Enrique. JIMENEZ, Rafael. RUBIANO, Gustavo. (2004) *Teoria de Números*, Segunda Edición, Universidad Nacional de Colombia, Facultad de Ciencias, Ed: Pro-Offset.

HOFMEISTER, G. R. (1966) *Zu einem Problem von Frobenius*, 1-37.

MARÍN, J. M. RAMIREZ, J. L. REVUELTA, M. P. (2007) *On the Frobenius number of Fibonacci numerical semigroups*. Integers 7, A14, 7 pp. (electronic), MR 2299815.

RAMIREZ, J.L. (2005) *The Diophantine Frobenius problem*. Oxford Lecture Series in Mathematics and its Applications, 30, Oxford University Press, xvi+243 pp. ISBN: 978-0-19-856820-9, 0-19-856820-7, MR 2260521 (2007i:11052).

RÖDSETH, Öystein. (1978) *On a linear Diophantine problem of Frobenius*, J. Reine Angew. Math.301, 171-178, MR 0557016 (58 #27741).

RÖDSETH, Öystein. (1978) *On a linear Diophantine problem of Frobenius II*, J. Reine Angew. Math, 431-440, MR 0534238 (82k:10018).

SELMER, Ernst. (1977) *On the linear Diophantine problem of Frobenius*, J. Reine Angew. Math.293/294, 1-17, MR 0441855(56#246).

SHALLIT, Jeffrey. (2001) *The Computational complexity of the local pastage stamp problem*, CoRR math, NT/0112257.