LA PROPIEDAD DE MIDY

FULVIO DAVID COLIMBA ANRANGO

FACULTAD DE CIENCIAS EXACTAS Y NATURALES
DEPARTAMENTO DE MATEMÁTICAS Y ESTADÍSTICA
UNIVERSIDAD DE NARIÑO
SAN JUAN DE PASTO
2016

LA PROPIEDAD DE MIDY

FULVIO DAVID COLIMBA ANRANGO

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

Asesor
John Hermes Castillo Gómez
Doctor en Matemáticas

FACULTAD DE CIENCIAS EXACTAS Y NATURALES
DEPARTAMENTO DE MATEMÁTICAS Y ESTADÍSTICA
UNIVERSIDAD DE NARIÑO
SAN JUAN DE PASTO
2016

Nota de Responsabilidad

Todas las ideas y conclusiones aportadas en el siguiente trabajo son responsabilidad exclusiva de los autores.

Artículo 1^{ro} del Acuerdo No. 324 de octubre 11 de 1966 emanado por el Honorable Consejo Directivo de la Universidad de Nariño.

Nota de Aceptación

_____

_____

_____

_____

_____

Jurado 1

_____

Jurado 2

_____

Director

San Juan de Pasto, Diciembre de 2015

Este trabajo está dedicado a:
Familiares, profesores y amigos que estuvieron al tanto de mi progreso durante estos últimos cinco años.

Agradecimientos

Al termino de esta etapa quisiera agradecerle en primer lugar a Dios, por haberme brindado protección, compañia y sabiduria durante el tiempo que tomó realizar este trabajo.

Al profesor John Castillo le agradezco de forma muy especial, puesto que con su calidad profesional y humana siempre mostró buena disposición al momento asesorar este trabajo.

Además agradezco a mi universidad que tanto quiero y respeto y a los profesores de la planta de docentes del departamento de matemáticas y estadística que con sus conocimientos y actitudes contribuyeron a mi formación tanto profesional como humana.

Finalmente agradezco a mi familia que con sus buenos deseos y consejos se convirtieron en mi mejor motivación a la hora de desarrollar este trabajo.

Fulvio David Colimba Anrango

Universidad de Nariño
Diciembre de 2015.

Resumen

En matemáticas, es común encontrar conjuntos de números que satisfacen ciertas propiedades, una de tantas y por cierto muy fascinante nos dice que si el período del recíproco de un número primo tiene un número par de dígitos, lo podemos dividir en dos bloques, sumar los números correspondientes y obtener siempre una cadena de nueves. Esta bella propiedad ha sido objeto de estudio de diversos matemáticos, quienes con sus dudas y la necesidad de darles respuestas han contribuido con su formalización y generalización, que hoy se conoce como la propiedad de Midy en honor al matemático francés E. Midy, de quien se tiene la primera publicación formal en 1836 sobre esta curiosidad. En la actualidad, su generalización abarca más que recíprocos de números primos, no solo dos bloques y una base arbitraria. En esta monografía se presentan de forma organizada y se analizan algunos avances teóricos alrededor de esta propiedad, además se presentan algunos algoritmos implementados en el sistema de álgebra computacional SAGE con el fin de ejemplificar la teoría.

Abstract

In mathematics, it is common to find sets of numbers that satisfies certain properties, one of many and certainly very fascinating tells us that if the period of the reciprocal of a prime number has an even number of digits, we can divided it in two blocks, add the corresponding numbers and always get a string of nines. This beautiful property has been the subject of study of several mathematicians, who with their doubts and need to give them answers have contributed to their formalization and generalization. This property it is knwon today as the Midy's property, name after the French mathematician, who made the first formal publication in 1836 about this curiosity. Nowadays, its generalization includes more than reciprocals of prime numbers, not just two blocks and arbitrary basis. In this monograph are presented, in an organized way, and discussed some theoretical developments around this property. Additionally, some algorithms were implemented in the computational algebra system SAGE in order to exemplify the theory presented.

Índice general

Introducción

Sea p un número primo tal que la expansión decimal de la fracción $\frac{1}{p}$ tiene un número par de dígitos en su período, entonces al dividirlo en dos bloques de igual longitud y sumar los números correspondientes a cada uno, se obtiene como resultado un número conformado solo de nueves. De acuerdo a [2], este resultado fue estudiado por Carl Friedrich Hindenburg en 1776 y en la actualidad es conocido por algunos como la propiedad de Midy, en honor al Matemático francés E. Midy quien fue el primero en publicar, en 1836, formalmente esta curiosidad.

Esta propiedad ha sido estudiada y expandida en diversos documentos, [4, 7, 6, 3, 1]. Así por ejemplo, se puede encontrar la generalización de esta propiedad para bases, denominadores, numeradores y longitud del período en [6].

El objetivo de este trabajo es presentar de forma organizada avances teóricos al rededor de la propiedad de Midy que se han recopilado de diferentes investigaciones, y en base a ellos implementar algunos algoritmos mediante los cuales sea posible ejemplificar algunas de sus características y propiedades.

Este trabajo está dividido en 4 capítulos. En el primero se muestran algunos resultados que son necesarios para la comprensión de los capítulos subsecuentes. En el segundo y tercer capítulo se recopilan y organizan algunos resultados que han obtenido diferentes investigadores en el estudio del siguiente interrogante: ¿Cuáles son las condiciones para que un número satisfaga la propiedad de Midy?; En el segundo capítulo para base decimal y en el tercero se generaliza para una base arbitraria, además, se incluye en el tercer capítulo un breve estudio sobre la propiedad de Midy desde un punto de vista geométrico. En el último capítulo se presentan algunas implicaciones que surgen de el hecho de satisfacer la propiedad de Midy, específicamente se hace referencia al multiplicador, del cual se va adquiriendo conciencia en el transcurso del segundo y tercer capítulo y que finalmente en el último capítulo se lo muestra de forma explícita junto con algunos resultados sobre éste que se pueden encontrar en [6], y a partir de dichos resultados se proponen cotas para el multiplicador teniendo en cuenta ciertas condiciones.

Finalmente, los algoritmos que permiten ejemplificar los resultados presentados en este trabajo y que fueron implementados en el sistema de álgebra computacional SAGE se encuentran en el Apéndice.

Capítulo 1

Preliminares

En este capítulo se presentan algunas definiciones y resultados que permiten abordar con mayor propiedad la temática expuesta en los capítulos siguientes. Gran parte de los resultados de este capítulo se pueden encontrar en la mayoría de libros de Teoría elemental de números, como por ejemplo en [9], de esta forma no se presenta la demostración de los resultados de este capítulo al no considerarse relevantes para el cumplimiento de los objetivos de este trabajo.

1.1. Divisibilidad

Definición 1.1. Sean a, b números enteros con $a \neq 0$. Decimos que a divide a b si existe un entero k tal que $b = ak$. En tal caso escribimos $a|b$. Decimos también que a es un divisor de b o que b es un múltiplo de a.

Para indicar que a no divide a b escribimos $a \nmid b$. Es fácil verificar que para todo entero k, $1|k$ y si $k \neq 0$, $k|k$.

Teorema 1.1. *Supongamos que a, b y c son números enteros. Entonces.*

1. *Si $a \neq 0$ entonces $a|0$, $a|a$, $a|(-a)$.*
2. *$1|a$, $(-1)|a$.*
3. *Si $a|b$ entonces $a|bc$.*
4. *Si $a|b$ y $b|c$ entonces $a|c$.*
5. *Si $a|b$ y $a|c$ entonces para todo $x, y \in Z$, $a|(bx + cy)$.*
6. *Si $a|b$ y $b \neq 0$ entonces $|a| \leq |b|$.*
7. *Si $a|b$ y $b|a$ entonces $a = b$ o $a = (-b)$.*

Definición 1.2 (Máximo Común Divisor (gcd))**.** Sean a y b dos enteros con al menos uno de ellos diferente de cero. m se denomina máximo común divisor de a y b si $m|a$, $m|b$ y para todo d tal que $d|a$ y $d|b$ se tiene que $d|m$.

Se va a denotar con $\gcd(a, b)$ al máximo común divisor de a y b.

Teorema 1.2. *Si* $a = bq + r$ *entonces* $\gcd(a, b) = \gcd(b, r)$.

Teorema 1.3. *Si* $\gcd(a, b) = d$*, entonces* d *es la mínima combinación lineal positiva en enteros entre* a *y* b.

Corolario 1.1. *Si* $d = \gcd(a, b)$*, entonces* $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Teorema 1.4. *Si* $k \neq 0$ *entonces* $\gcd(ka, kb) = |k| \gcd(a, b)$.

Teorema 1.5. *Si* $a|bc$ *y* $\gcd(a, b) = 1$*, entonces* $a|c$.

Como consecuencias del anterior resultado se obtienen los siguientes corolarios.

Corolario 1.2 (Lema de Euclides)**.** *Si* p *es primo y* $p|ab$*, entonces* $p|a$ *o* $p|b$.

Corolario 1.3. *Si* p *es primo y* $p|a_1a_2 \cdots a_n$*, entonces* $p|a_i$ *para algún* i*,* $1 \leq i \leq n$.

Corolario 1.4. *Si* p*,* $p_1, p_2, ..., p_n$ *son números primos y* $p|p_1p_2 \cdots p_n$*, entonces* $p = p_i$ *para algún* $i, 1 \leq i \leq n$.

Corolario 1.5. *Si* $a_1, a_2, ..., a_n$ *son enteros primos relativos dos a dos y para cada* $i = 1, 2, ..., n$ $a_i|c$*, entonces* $a_1a_2 \cdots a_n|c$.

1.2. Congruencias

Definición 1.3. Sean a y b enteros cualesquiera y n un entero positivo. Si $n|(a - b)$ se escribe a es congruente con b módulo n y se escribe,

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

Si a no es congruente con b módulo n, se dice que $a \not\equiv b(modn)$.

Lema 1.1. *Para todo par de enteros* a *y* b*, se tiene*

1. $a \equiv b \pmod{1}$.
2. *Si* $d|n$ *y* $a \equiv b \pmod{n}$ *entonces* $a \equiv b \pmod{d}$.

Teorema 1.6. *Si* $a \equiv b \pmod{n}$ *y* $c \equiv d \pmod{n}$ *entonces*

1. *Para todo par de enteros* r *y* s, $ar + cs \equiv br + ds \pmod{n}$.
2. $ac \equiv bd \pmod{n}$.
3. *Para todo entero positivo* k, $ak \equiv bk \pmod{n}$.
4. *Para todo entero* r, $a + r \equiv b + r \pmod{n}$.
5. *Para todo entero* r, $ar \equiv br \pmod{n}$.

Teorema 1.7 (Pequeño teorema de Fermat)**.** *Si* p *es un primo, entonces para cada entero* a *tal que* p *no divide a* a, $a^{p-1} \equiv 1 \pmod{p}$

Corolario 1.6. *Si* p *es un primo, entonces* $a^p \equiv a \pmod{p}$, *para cualquier entero* a.

1.3. Orden de b módulo N

Definición 1.4. Se conoce como el orden de b módulo N y se denota con $|b|_N$ al menor entero tal que

$$b^{|b|_N} \equiv 1 \pmod{N}.$$

A partir de esta definición puede demostrarse que, si $b^f \equiv 1 \pmod{N}$, entonces $|b|_N$ divide a f.

Teorema 1.8. *Sea* p *un primo impar no divisible por* b, m *el mayor exponente de* p *en la factorización prima de* N *y sea* t *un entero positivo, entonces*

$$|b|_{p^t} = \begin{cases} |b|_p & if\ t \leq m, \\ \\ p^{t-m}|b|_p & if\ t > m. \end{cases}$$

El siguiente resultado se demuestra de forma implícita en el Capítulo 3.

Teorema 1.9. *Sean* x, N *y* b *enteros positivos, con* $N, b > 1$, $\gcd(x, N) = 1$, $\gcd(N, b) = 1$ *y* $1 \leq x < N$. *Entonces la expansión en base* b *de la fracción* x/N *puede representarse de la forma*

$$\frac{x}{N} = 0.\overline{a_1 a_2 ... a_{|b|_N}} = \frac{[a_1 a_2 ... a_{|b|_N}]}{b^{|b|_N} - 1},$$

con la barra indicando el período. Además, el número de dígitos en el período es igual al orden de b *módulo* N.

Capítulo 2

La propiedad de Midy para base 10

En este capítulo se presentan resultados que establecen condiciones para determinar si un entero N satisface la propiedad de Midy en base decimal para un divisor d de $|10|_N$ (orden de 10 módulo N, Definición 1.4). Algunos de estos resultados están relacionadas con la caracterización de los enteros que satisfacen dicha propiedad teniendo en cuenta su descomposición en factores primos. Los ejemplos que se presentan en donde se determina si un entero satisface la propiedad de Midy se verifican a través del *algoritmo para determinar si un entero N satisface la propiedad de Midy*, implementado en SAGE y que se encuentra en el Apéndice A2.

El objetivo principal de este capítulo es examinar bajo que condiciones se cumple la propiedad de Midy en base decimal.

Para dar una idea inicial de a que se refiere la propiedad de Midy, se va a empezar observando la expansión decimal de $\frac{1}{7}$ que es $0.\overline{142857}$, cuyo período 142857 tiene un número par de dígitos. Si se suma la primera mitad de los dígitos, 142, a la segunda, 857, el resultado es 999. Para sorpresa de muchos, éste no es un fenómeno único. Como ejemplos se tienen:

$$\begin{aligned}
&\frac{2}{11} = 0.\overline{18} && \text{donde} && 1+8 = 9 = 10-1,\\
&\frac{1}{13} = 0.\overline{076923} && \text{donde} && 076+923 = 999 = 10^3-1,\\
&\frac{3}{13} = 0.\overline{230769} && \text{donde} && 27+07+69 = 99 = 10^2-1,\\
&\frac{17}{21} = 0.\overline{809523} && \text{donde} && 80+95+23 = 198 = 2(99) = 2(10^2-1).
\end{aligned}$$

En estos ejemplos se dividió el período de la expansión decimal de varias fracciones en bloques con igual número de dígitos, se sumó los números correspondientes a cada bloque y se obtuvo un múltiplo de la diferencia entre una potencia de diez y uno. La formalización de esta curiosidad que se presenta a lo largo de este trabajo es lo que se conoce como la propiedad de Midy. De acuerdo a

[2], su nombre es en honor al matemático francés E. Midy, quien fue el primero en publicar, en un documento de 21 páginas en 1836, [8], esta curiosidad.

2.1. Propiedad de Midy para números primos

Los números primos han sido objeto de estudio en numerosos trabajos, este trabajo no es la excepción, una razón de ésto es que las primeras ideas relacionadas con la propiedad de Midy, surgieron a partir del estudio de fracciones con denominadores primos que cumplían ciertas condiciones, con el fin de abreviar el proceso para determinar su expansión decimal, ver [2].

Conocer las condiciones bajo las cuales los números primos satisfacen la propiedad de Midy es el objetivo central de esta sección.

En relación a esta propiedad se empieza abordando el primer resultado, al que se le conoce como el Teorema de Midy y cuya prueba se encuentra en [4].

Teorema 2.1. *Sea $p > 5$ un número primo y x un entero positivo menor que p tal que la expansión decimal de la fracción $\frac{x}{p}$ tenga un número par de dígitos en su período, es decir,*

$$\frac{x}{p} = 0.\overline{a_1 a_2 \dots a_{2k}} \quad \textit{para algún } k \textit{ en } \mathbb{Z}^+,$$

entonces $A + B = 10^k - 1$, donde $A = a_1 a_2 \dots a_k$ y $B = a_{k+1} a_{k+2} \dots a_{2k}$.

Demostración. Por el Teorema 1.9 se tiene que

$$\frac{x}{p} = \frac{10^k A + B}{10^{2k} - 1},$$

entonces, usando diferencia de cuadrados

$$\frac{x}{p} = \frac{10^k A + B}{10^{2k} - 1} = \frac{10^k A + B}{(10^k - 1)(10^k + 1)},$$

que es equivalente a

$$(10^k A + B)p = x(10^k - 1)(10^k + 1).$$

Puesto que p es primo, por el Corolario 1.3, p divide a x, o a $10^k - 1$, o a $10^k + 1$. Por hipótesis p no divide a x. Si p divide a $10^k - 1$ entonces $10^k \equiv 1 \pmod{p}$, pero del Teorema 1.9, $2k = |10|_p$, donde $|10|_p$ es el orden de 10 módulo p (Definición 1.4) de esta misma definición también se sigue que $2k$ divide a k, lo cual es una contradicción puesto que k está en $\mathbb{Z}^+$. Por lo tanto p divide a $10^k + 1$.

Reordenando la última ecuación, se tiene que

$$\begin{aligned}\frac{x(10^k+1)}{p} &= \frac{10^kA+B}{10^k-1}\\ &= \frac{10^kA-A+A+B}{10^k-1}\\ &= A+\frac{A+B}{10^k-1}.\end{aligned}$$

Dado que p divide a (10^k+1), el lado izquierdo de la ecuación es un número entero, así el lado derecho también lo es. Entonces como A es un número entero, $\frac{A+B}{10^k-1}$ también lo es. Se puede observar que 10^k-1 es el mayor entero con k dígitos, y ya que A y B tienen k dígitos, entonces A y B pueden ser a lo sumo 10^k-1, así

$$A+B \leq 2(10^k-1).$$

Supóngase que $A+B=2(10^k-1)$, es decir $A=B=10^k-1$, entonces

$$10^kA+B = 10^k(10^k-1)+(10^k-1) = 10^{2k}-1,$$

lo cual nos lleva a una contradicción, puesto que de ser así se obtiene

$$\frac{x}{p} = \frac{10^{2k}-1}{10^{2k}-1} = 1,$$

por lo tanto

$$A+B < 2(10^k-1),$$

y como $\frac{A+B}{10^k-1}$ es un número entero, entonces 10^k-1 divide a $A+B$, ésto implica que

$$A+B = 10^k-1.$$

□

Se puede observar que el resultado anterior se cumple independientemente del valor que tome x siempre que éste sea un entero positivo menor que p, en este caso se dice que ***p* satisface la propiedad de Midy para *d* = 2 en base 10**, se manifiesta que es para $d=2$ puesto que se ha dividido el período en dos bloques.

En general, como se había mencionado a comienzos de éste capítulo, esta propiedad también se cumple si se divide el período en cualquier número de bloques, siempre y cuando el número de bloques a considerar sea un divisor de $|10|_p$ mayor que 1, este resultado se expone formalmente en el Teorema 2.2, pero antes se realizan algunas consideraciones.

Sea N en $\mathbb{Z}^+$ tal que $\gcd(N,10)=1$. Con $\mathbb{U}_N$ se va a denotar al conjunto de enteros positivos

primos relativos y menores a N. Sean d y k enteros positivos tales que $|10|_N = dk$ con $d > 1$. Se toma x en $\mathbb{U}_N$, se considera la fracción $\frac{x}{N}$ con período $a_1a_2\ldots a_{|10|_N}$ (ver Teorema 1.9) que se divide en d bloques de igual longitud k, donde

$$A_j = a_{(j-1)k+1}a_{(j-1)k+2}\ldots a_{jk}, \quad \text{con} \quad 1 \leq j \leq d, \tag{2.1.1}$$

corresponde al j-ésimo bloque, y

$$S_d(x) = A_1 + A_2 + \cdots + A_d = \sum_{j=1}^{d} A_j,$$

corresponde a la suma de los d bloques conformados. Teniendo en cuenta estas consideraciones se presenta la siguiente definición, que ha sido adaptada para base decimal de la definición propuesta en [6].

Definición 2.1. Sea N un entero positivo primo relativo con 10. Se dice que N tiene o satisface la propiedad de Midy para un divisor $d > 1$ de $|10|_N$, si $S_d(x)$ es un múltiplo de $10^k - 1$ para todo x en $\mathbb{U}_N$.

El siguiente resultado es un caso particular del Teorema 3.3, sin embargo se incluye con el fin de exponer su demostración que se construyo siguiendo las mismas ideas de la prueba del Teorema 2.1

Teorema 2.2. *Sea $p > 5$ un número primo y $|10|_p = dk$ el orden de 10 módulo p, donde $d > 1$ es un divisor de $|10|_p$ y $k = \frac{|10|_p}{d}$. Entonces, p satisface la propiedad de Midy para todo divisor $d > 1$ de $|10|_p$.*

Demostración. Sea x en el conjunto de enteros positivos menores que p, $\mathbb{U}_p$. Del Teorema 1.9 se sabe que la longitud del período de la fracción $\frac{x}{p}$ es $|10|_p$, además, por la ecuación (2.1.1) se puede escribir la fracción $\frac{x}{p}$ de la forma

$$\frac{x}{p} = 0.\overline{a_1a_2\ldots a_{dk}} = 0.\overline{A_1A_2\ldots A_d},$$

para indicar que se ha dividido el período de longitud $|10|_p$ en d bloques de igual longitud k. Por el Teorema 1.9 se tiene

$$\begin{aligned}\frac{x}{p} &= \frac{A_1A_2\ldots A_d}{10^{dk}-1} \\ &= \frac{A_1A_2\ldots A_d}{(10^k-1)\left(10^{(d-1)k} + 10^{(d-2)k} + \cdots + 10^k + 1\right)},\end{aligned}$$

que es equivalente a

$$x(10^k-1)\left(10^{(d-1)k} + 10^{(d-2)k} + \cdots + 10^k + 1\right) = p(A_1A_2\ldots A_d).$$

De forma análoga a la prueba del Teorema 2.1 se obtiene que p divide a $\left(10^{(d-1)k}+10^{(d-2)k}+\cdots+10^k+1\right)$. Reordenando esta última ecuación se tiene

$$\begin{aligned}
&\frac{x(10^k-1)\left(10^{(d-1)k}+10^{(d-2)k}+\cdots+10^k+1\right)}{p}\\
&=\frac{(A_1A_2\ldots A_d)}{10^k-1}\\
&=\frac{10^{k(d-1)}A_1+10^{k(d-2)}A_2+\cdots+A_d}{10^k-1}\\
&=\frac{\left(10^{k(d-1)}-1\right)A_1+\left(10^{k(d-2)}-1\right)A_2+\cdots+\left(10^k-1\right)A_{d-1}+S_d(x)}{10^k-1}\\
&=\underbrace{\frac{\sum_{j=1}^{d-1}(10^{k(d-j)}-1)A_j}{10^k-1}}_{(*)}+\underbrace{\frac{S_d(x)}{10^k-1}}_{(**)}.
\end{aligned}$$

Puesto que p divide a $\left(10^{(d-1)k}+10^{(d-2)k}+\cdots+10^k+1\right)$ entonces el lado izquierdo de la ecuación es un número entero, así el lado derecho también lo es. Como (10^k-1) divide a $(10^{k(d-j)}-1)$ para $1\leq j\leq d-1$, entonces $(*)$ es un número entero, lo que implica que $(**)$ también es un número entero, es decir 10^k-1 divide a $S_d(x)$. □

Ejemplo 2.1. Teniendo en cuenta el Teorema 2.2, en la siguiente tabla se muestra que para diferentes números primos p, se tiene que p satisface la propiedad de Midy para todos los divisores d de $|10|_p$.

p	$\|10\|_p$	d
13	6	$2,3,6$
19	18	$2,3,6,9,18$
31	15	$3,5,15$
73	8	$2,4,8$

Tabla 2.1: Divisores d para los cuales p satisface la propiedad de Midy en base 10.

Obsérvese que independientemente del valor de x en $\mathbb{U}_p$, $S_d(x)$ es múltiplo de 10^k-1, sin embargo las sumas $S_d(x_1)$ y $S_d(x_2)$ con $x_1\neq x_2$ en $\mathbb{U}_p$ no necesariamente son iguales, como se ilustra en el siguiente ejemplo.

Ejemplo 2.2. En la siguiente tabla se presentan los valores de $S_d(x)$ para algunos x en $\mathbb{U}_p$, con $p=157$ y $d=26$.

x	$S_d(x)$
1	$5994 = 6(10^3 - 1)$
5	$4995 = 5(10^3 - 1)$
107	$6993 = 7(10^3 - 1)$

Tabla 2.2: $S_d(x)$ para $d = 26$, $p = 157$ y distintos valores de x.

Las cuestiones sobre la obtención de diferentes sumas $S_d(x)$, para un mismo divisor d de $|10|_p$ y distintos x en $\mathbb{U}_p$ como se observa en la Tabla 2.2, están relacionadas con el multiplicador, que no es más que el factor que multiplica a $10^k - 1$ en $S_d(x)$ y cuyo estudio se presenta en detalle en el Capítulo 4.

2.2. Propiedad de Midy para números compuestos

Al referirse a la propiedad de Midy, no únicamente se puede pensar que el denominador N de las fracciones a considerar sea un número primo. En esta sección se mostrarán algunos resultados que permiten determinar cuando un número N no necesariamente primo satisface la propiedad de Midy para un divisor $d > 1$ de $|10|_N$.

En lo que sigue, con $D_{10}(x, N)$ se va a denotar el período en la expansión decimal de la fracción $\frac{x}{N}$.

Ejemplo 2.3. Para la fracción $\dfrac{5}{21} = 0.\overline{238095}$, se tiene que

$$D_{10}(5, 21) = 238095.$$

Del Teorema 1.9 se tiene la siguiente relación:

$$ND_{10}(x, N) = x(10^{|b|_N} - 1). \tag{2.2.1}$$

Ahora, para d y k en $\mathbb{Z}^+$, tal que $|b|_N = dk$, se define $N(d, k)$ como

$$N(d, k) = \frac{10^{|b|_N} - 1}{10^k - 1} = 10^{|b|_N - k} + 10^{|b|_N - 2k} + \cdots + 10^k + 1. \tag{2.2.2}$$

De las ecuaciones (2.2.1) y (2.2.2), se tiene la siguiente relación:

$$x\left(10^k - 1\right) N(d, k) = ND_{10}(x, N). \tag{2.2.3}$$

El siguiente resultado que se puede encontrar en [7], proporciona una condición necesaria y suficiente para que un entero N satisfaga la propiedad de Midy.

Teorema 2.3. *Sean N, d y k en $\mathbb{Z}^+$, tales que $d > 1$ y $|b|_N = dk$. Entonces N satisface la propiedad de Midy para d si y sólo si $N(d, k) \equiv 0 \pmod{N}$.*

Demostración. Sea $D_{10}(x,N) = a_1a_2\ldots a_{|b|_N}$ el período en la expansión decimal de la fracción $\frac{x}{N}$ para x en $\mathbb{U}_N$. De la ecuación (2.1.1) se tiene que

$$\begin{aligned} D_{10}(x,N) &= A_1A_2\ldots A_d = 10^{(|b|_N-k)}A_1 + 10^{(|b|_N-2k)}A_2 + \cdots + A_d \\ &= \left(10^{(|b|_N-k)} - 1\right)A_1 + \left(10^{(|b|_N-2k)} - 1\right)A_2 + \cdots + \left(10^k - 1\right)A_{d-1} + S_d(x) \\ &= \sum_{j=1}^{d-1}(10^{(|b|_N-jk)} - 1)A_j + S_d(x), \end{aligned}$$

puesto que $10^k - 1$ divide a $10^{(|b|_N-ik)} - 1$ para todo i entero tal que $1 \leq i < d$, se puede afirmar que:

$$10^k - 1 \text{ divide a } D_{10}(x,N) \text{ si y sólo si } 10^k - 1 \text{ divide a } S_d(x). \tag{2.2.4}$$

Supóngase que para todo x en $\mathbb{U}_N$, $10^k - 1$ divide a $S_d(x)$, al reorganizar la ecuación (2.2.3) en la forma

$$\frac{xN(d,k)}{N} = \frac{D_{10}(x,N)}{10^k - 1}, \tag{2.2.5}$$

por la afirmación (2.2.4), el lado derecho de esta ecuación es un número entero, por tanto el lado izquierdo también lo es, y como $\gcd(x,N) = 1$, entonces N divide a $N(d,k)$.

Recíprocamente, al suponer que N divide a $N(d,k)$, de la ecuación (2.2.5) se sigue que $10^k - 1$ divide a $D_{10}(x,N)$, y por la afirmación (2.2.4), $10^k - 1$ divide a $S_d(x)$ para todo x en $\mathbb{U}_N$. □

Como consecuencia del teorema anterior se tiene el siguiente resultado.

Teorema 2.4. *Sean N, d y k en $\mathbb{Z}^+$, tales que $d > 1$ y $|b|_N = dk$. Si $\gcd(N, 10^k - 1) = 1$, entonces N satisface la propiedad de Midy para d.*

Demostración. Se reorganiza la ecuación (2.2.3) en la forma

$$xN(d,k) = \frac{ND_{10}(x,N)}{10^k - 1}.$$

Así $\gcd(N, 10^k - 1) = 1$, entonces $10^k - 1$ divide a $D_{10}(x,N)$, y de la afirmación (2.2.4), $10^k - 1$ divide a $S_d(x)$ para todo x en $\mathbb{U}_N$. □

Otro resultado que se deriva del Teorema 2.3 es el siguiente.

Teorema 2.5. *Sean N, d y k en $\mathbb{Z}^+$, tales que $d > 1$ y $|10|_N = dk$. Sea $\prod_{p|N} p^i$ la factorización prima de N. Si para cada factor primo p de N, el entero k no es múltiplo de $|10|_p$, entonces N satisface la propiedad de Midy para d.*

Demostración. Supóngase que para cada factor primo p de N, el entero k no es múltiplo de $|10|_p$, entonces $\gcd(p, 10^k - 1) = 1$, por lo tanto $\gcd(p^i, 10^k - 1) = 1$, pero N divide a $10^{|10|_N} - 1$ y así p^i también divide a $10^{|10|_N} - 1$. Por la ecuación 2.2.2 y el hecho de que $\gcd(p^i, 10^k - 1) = 1$, se tiene que p^i es un divisor de $N(d, k)$. Por lo tanto N también es un divisor de $N(d, k)$, y del Teorema 2.3 se sigue que N satisface la propiedad de Midy para d. □

Ejemplo 2.4. Sea $N = 217 = 7 \cdot 31$, $|10|_7 = 6$, $|10|_{31} = 15$ y $|10|_{217} = 30$. En particular, $D_{10}(1, 217)$ está dado por

$$D_{10}(1, 217) = 004608294930875576036866359447.$$

En la siguiente tabla se indica para cuales valores de d, 217 satisface la propiedad de Midy. Cuando el entero k no es múltiplo de 6 o 15, entonces el Teorema 2.5 garantiza que N satisface la propiedad de Midy para d. Por lo tanto, todos los casos en la siguiente tabla, excepto $k = 6$ y $k = 15$, son garantizados por el teorema.

k	d	N tiene la propiedad de Midy para d
1	30	si
2	15	si
3	10	si
5	6	si
6	5	no
10	3	si
15	2	no

Tabla 2.3: Divisores $d > 1$ de $|10|_{217}$ para los cuales 217 tiene o no tiene la propiedad de Midy.

2.3. Propiedad de Midy para $d = 2$

Los resultados en esta sección establecen condiciones para que un entero N satisfaga la propiedad de Midy para $d = 2$, además en el Teorema 2.8 se caracteriza los enteros que satisfacen la propiedad de Midy para $d = 2$ en relación a sus factores primos. De ahí que se consideran únicamente los enteros positivos N tales que $|10|_N = 2k$, con k en los enteros positivos. Esta caracterización se puede encontrar en [7].

Teorema 2.6. *Sea $N > 1$ un número entero talque $\gcd(N, 10) = 1$ y $|10|_N = 2k$ con k en los enteros positivos. Se tiene que N satisface la propiedad de Midy para $d = 2$ si y sólo si existe algún entero positivo j tal que N divide a $10^j + 1$.*

Demostración. Supóngase que N tiene la propiedad de Midy para $d = 2$. Del Teorema 2.3 se tiene que N divide a $10^k + 1$.

Recíprocamente, supóngase que N divide a $10^j + 1$ para algún j en los enteros positivos. De este supuesto, se tiene que N divide a $10^{2j} - 1$. De la Definición 1.4, $|10|_N$ divide a $2j$ y así k divide a j; es decir $j = rk$ con $r \in \mathbb{Z}^+$. Supóngase que r es par, es decir, $r = 2m$, entonces $j = 2mk = |10|_N m$, así, puesto que j es múltiplo de $|10|_N$, entonces $10^j \equiv 1 \pmod{N}$, pero además, por hipótesis, $10^j \equiv -1 \pmod{N}$, restando estas últimas dos congruencias se tiene que N divide a 2, así, $N = 1$ o $N = 2$; pero si $N = 1$ se contradice la condición de que $N > 1$ y si $N = 2$ se contradice la condición de que $\gcd(N, 10) = 1$, por lo tanto r es impar. Teniendo en cuenta que r es impar entonces j se puede escribir de la forma $j = k(2m + 1)$ para algún entero $m \geq 0$. Si $m = 0$, el teorema queda demostrado. Se toma entonces $m > 0$, y se va a suponer que N no divide a $10^k + 1$, entonces,

$$10^k \not\equiv -1 \pmod{N},$$

y como $10^{2k} \equiv 1 \pmod{N}$ entonces,

$$10^{3k} \not\equiv -1 \pmod{N},$$

del mismo modo

$$10^{5k} \not\equiv -1 \pmod{N},$$

y en general

$$10^{k(2i+1)} \not\equiv -1 \pmod{N},$$

para $i > 0$, particularmente esta relación se cumple para $i = m$, lo cuál contradice el hecho de que N divide a $10^j + 1$. Por lo tanto, N divide a $10^k + 1$, y del Teorema 2.3 se concluye que N satisface la propiedad de Midy para $d = 2$. □

El siguiente resultado muestra que si N satisface la propiedad de Midy para $d = 2$ entonces, cualquier potencia de N también la satisface.

Teorema 2.7. *Si N satisface la propiedad de Midy para $d = 2$, entonces, para todo entero positivo i, N^i satisface la propiedad de Midy para $d = 2$.*

Demostración. Sea $|10|_N = 2k$. Por la hipótesis, del Teorema 2.3, se tiene que N divide a $10^k + 1$. Por otra parte, para cualquier entero positivo impar j, $10^k + 1$ divide a $10^{jk} + 1$ y además,

$$10^{jk} + 1 = (10^k + 1) \underbrace{\left(10^{(j-1)k} - 10^{(j-2)k} + 10^{(j-3)k} - \cdots - 10^k + 1\right)}_{(*)}. \tag{2.3.1}$$

Para simplificar, se va a denotar con $E(j)$ el factor marcado con $(*)$ en la ecuación anterior. Además, para cada entero positivo impar j, si se toma

$$Q(j) = 10^{(j-2)k} - 2 \cdot 10^{(j-3)k} + 3 \cdot 10^{(j-4)k} - \cdots - (j-3)10^{2k} + (j-2)10^k - (j-1),$$

se tiene que,

$$E(j) = Q(j)(10^k + 1) + j. \tag{2.3.2}$$

Para $j = 10^k + 1$, se tiene que $E(j)$ es divisible por $(10^k + 1)$. Así, de la ecuación (2.3.1) se tiene que $\left(10^k + 1\right)^2$ divide a $10^t + 1$ cuando $t = k(10^k + 1)$, y como N divide a $10^k + 1$, entonces N^2 divide a $10^t + 1$. En consecuencia, del Teorema 2.6, N^2 satisface la propiedad de Midy para $d = 2$. Aplicando este resultado a N^2 se muestra que N^4 satisface la propiedad de Midy para $d = 2$, y en general, por iteración, si $q > 1$ es una potencia de 2 se tiene que N^q satisface la propiedad de Midy para $d = 2$. Por otro lado, para cualquier entero positivo i, existe un entero u que es una potencia de 2 tal que $i \leq u$. Puesto que N^u divide a $10^v + 1$ para algún entero positivo v y N^i divide a N^u, entonces N^i también divide a $10^v + 1$, y así por el Teorema 2.6 N^i satisface la propiedad de Midy para $d = 2$. □

En el siguiente ejemplo se observa que el entero t en la prueba anterior no necesariamente es el menor de los enteros positivos j tales que N^2 divide $10^j + 1$.

Ejemplo 2.5. Para $N = 11$, con $k = 1$, se tiene que $t = 1(10^1 + 1) = 11$, es decir, $11^2 = 121$ divide a $10^{11} + 1$, y puesto que $|10|_{11} = 22$, efectivamente t es el menor de los enteros j tales que 121 divide a $10^j + 1$. Sin embargo, para $N = 7$, con $k = 3$, se tiene que $t = 3(10^3 + 1) = 3003$, es decir, $7^2 = 49$ divide a $10^{3003} + 1$, pero $|10|_{49} = 42$, así 49 también divide a $10^{21} + 1$.

El Teorema 2.7 se usa en la prueba del Teorema 2.8, el cual caracteriza los enteros N que satisfacen la propiedad de Midy en términos de cierta relación entre los factores primos de N. Esencialmente el Teorema 2.7 permite centrar la atención en la relación entre los factores primos de N sin tener que preocuparse por sus exponentes.

El número 1507 no tiene la propiedad de Midy para $d = 2$ aunque $|10|_{1507} = 8$. Un análisis de por qué 1507 no satisface la propiedad de Midy para $d = 2$ ayudará en la comprensión de la demostración del Teorema 2.8. Se tiene que $D_{10}(1, 1507) = 00066357$. Por el Teorema 2.3, 1507 satisface la propiedad de Midy para $d = 2$ si y soló si 1507 divide a $10^4 + 1 = 10001$, en efecto esto no sucede. Conocer las causas por las que esto no sucede es lo importante de este análisis. Los factores primos de 1507 son 11 y 137, 11 divide a $10^1 + 1$ y 137 divide a $10^4 + 1$, además 11 divide a $10^u + 1$ para $u = 1, 3, 5, \ldots$, y 137 divide a $10^v + 1$ para $v = 4, 12, 20, \ldots$. El conjunto de los enteros u y de los v son disjuntos, por lo tanto, cuando 11 divide a $10^t + 1$, 137 no lo divide, y viceversa, de donde se tiene que su producto, 1507, nunca puede dividir a un número de la forma $10^t + 1$, así, por el Teorema 2.6, el número 1507 no satisface la propiedad de Midy para $d = 2$.

Previamente, en la demostración del Teorema 2.6, se probó implícitamente el siguiente Lema, que será importante en la demostración del Teorema 2.8 que le sigue.

Lema 2.1. *Sea N un entero positivo tal que $|10|_N = 2k$ con k en los enteros positivos y además que satisface la propiedad de Midy para $d = 2$. Entonces N divide a $10^t + 1$ si y sólo si, $t = k(2i+1)$ para todo entero $i \geq 0$.*

Teorema 2.8. *Sea N un entero positivo. Con p_i se va a denotar cada factor primo de N, donde $1 \leq i \leq r$ y r es el número de factores primos que tiene N. Entonces N satisface la propiedad de Midy para $d = 2$, si y sólo si, se cumple la siguiente condición:*

(*) Existe un entero positivo s tal que para cada entero i con $1 \leq i \leq r$, $|10|_{p_i} = 2^s \cdot q_i$, donde q_i es un entero impar (El entero q_i puede ser diferente para distintos valores de i, pero para cada i el factor 2^s es el mismo).

Demostración. Sea p un número primo que satisface la propiedad de Midy para $d = 2$. Supóngase que $|10|_p = 2r$. Por el Lema 2.1, p divide a $10^j + 1$ siempre que j sea de la forma $j = r(2i+1)$ para $i = 0, 1, 2, \ldots$.

Supóngase que la condición $(*)$ no se cumple. Una posibilidad es que $s = 0$ para algún i, de donde $|10|_{p_i} = q_i$, es decir, $|10|_{p_i}$ es impar, así el factor primo p_i de N no satisface la propiedad de Midy; en este caso N no puede satisfacer la propiedad de Midy para $d = 2$. Puesto que si lo hace, entonces N divide a $10^{\frac{|10|_N}{2}} + 1$, pero entonces cada factor primo de N también dividiría a este número, y así, por el Teorema 2.6 cada factor primo debería satisfacer la propiedad de Midy para $d = 2$, lo cual contradiría el hecho de que p_i como factor primo de N no satisface la propiedad de Midy.

Ahora, supongamos que la condición $(*)$ se cumple. Sea $k_i = \frac{|10|_{p_i}}{2}$ y m_i la mayor potencia de p_i en la factorización de N. Del Teorema 2.1 se sigue que p satisface la propiedad de Midy para $d = 2$, y del Teorema 2.7 se tiene que $p_i^{m_i}$ también satisface la propiedad de Midy para $d = 2$. Pero de la prueba del Teorema 2.7, se tiene que $p_i^{m_i}$ divide a $10^{t_i} + 1$, donde $t_i = k_i v_i$ con v_i impar. De la condición $(*)$, $k_i = 2^{s-1} q_i$. Como q_i es impar, el producto $q = \prod_{i=1}^{r} q_i$ es impar, del mismo modo $v = \prod_{i=1}^{r} v_i$ es impar. Sea $e = vq2^{s-1}$. Del Lema 2.1, para cada i se tiene que $p_i^{m_i}$ es un divisor de $10^e + 1$ ya que e se puede expresar de la forma de la forma $e = k_i w_i$, con $w_i = \dfrac{qv}{q_i}$ impar. En consecuencia N también es un divisor de $10^e + 1$. Por lo tanto, del Teorema 2.6 se concluye que N satisface la propiedad de Midy para $d = 2$. □

Capítulo 3

Generalización de la propiedad de Midy para una base arbitraria

En este capítulo se muestra la generalización de la propiedad de Midy para una base arbitraria $b > 1$ que propone J. Lewittes [6], complementándolo con resultados que se encuentran en [1]. Varios de los resultados que se presentan en este capítulo son generalizaciones de resultados expuestos en el Capítulo 2, sin embargo se incluyen puesto que la dinámica en sus demostraciones es diferente. Se pone especial interés en los residuos que se obtienen al determinar la expansión en base b de la fracción $\frac{x}{N}$, donde x y N son enteros positivos tales que $\gcd(N, b) = 1$, $N > 1$ y x está en $\mathbb{U}_N$; cabe mencionar que dichos residuos no se consideraron en la construcción del Capítulo 2. Del mismo modo que en el capítulo anterior, los ejemplos que aparecen, en donde se determina si un entero satisface la propiedad de Midy se verifican a través del *algoritmo para determinar si un entero N satisface la propiedad de Midy* implementado en SAGE y que se encuentra en el Apéndice A2..

3.1. Expansión en base b

En esta sección se presenta el algoritmo que permite determinar la expansión en base b de la fracción antes mencionada. Para ello, se empieza usando el algoritmo de la división como sigue. Sea $x_1 = x$, a_1 el cociente y x_2 el residuo de dividir bx_1 entre N. Es decir,

$$bx_1 = a_1N + x_2,\ 0 \leq x_2 < N \text{ y } a_1 = \left\lfloor \frac{bx_1}{N} \right\rfloor.$$

Sea a_2 el cociente y x_3 el residuo de dividir bx_2 entre N. Es decir,

$$bx_2 = a_2N + x_3,\ 0 \leq x_3 < N \text{ y } a_2 = \left\lfloor \frac{bx_2}{N} \right\rfloor.$$

Continuando con este proceso, se obtiene la siguiente secuencia infinita de ecuaciones

$$\begin{aligned} bx_1 &= a_1N + x_2 \\ bx_2 &= a_2N + x_3 \\ &\vdots \\ bx_i &= a_iN + x_{i+1} \\ &\vdots \end{aligned} \tag{3.1.1}$$

donde a_i es el cociente y x_{i+1} el residuo de dividir bx_i entre N, para todo $i \geq 1$. Además, como $0 < \frac{x_1}{N} < 1$, se tiene que $\frac{bx_1}{N} < b$, por tanto $a_1 = \left\lfloor \frac{bx_1}{N} \right\rfloor < b$, así a_1 es un b-dígito. También, al ser b y x_1 primos relativos con N, entonces del hecho de que $bx_1 \equiv x_2 \pmod{N}$ implica que $\gcd(x_2, N) = 1$, así x_2 está en $\mathbb{U}_N$. De la misma forma, para todo $i \geq 1$, a_i es un b-dígito y x_i está en $\mathbb{U}_N$. Dividiendo la primera ecuación por bN, la segunda por b^2N, y en general la i-ésima por b^iN se obtiene

$$\frac{x_1}{N} = \frac{a_1}{b} + \frac{a_2}{b^2} + \cdots + \frac{a_i}{b^i} + \frac{x_{i+1}}{b^iN}.$$

Puesto que $0 < \frac{x_{i+1}}{b^iN} < \frac{1}{b^i}$ y $\frac{1}{b^i}$ tiende a 0 cuando i tiende a infinito, se tiene que $\frac{x_1}{N} = \sum_{i=1}^{\infty} \frac{a_i}{b^i}$ que también se puede escribir como $\frac{x_1}{N} = 0.a_1a_2 \ldots a_i \ldots$ que corresponde a la expansión en base b de $\frac{x_1}{N}$.

De (3.1.1), se obtiene que para todo $i \geq 1$,

$$x_{i+1} \equiv bx_i \equiv b^2x_{i-1} \equiv \cdots \equiv b^ix_1 \pmod{N} \tag{3.1.2}$$

Por la ecuación (3.1.2) y la definición de $|b|_N$,

$$x_{|b|_N+1} \equiv b^{|b|_N}x_1 \equiv x_1 (\text{mód } N) \text{ y}$$

$$x_{i+1} \not\equiv x_1 (\text{mód} N) \text{ para } 1 \leq i < |b|_N.$$

Ya que x_1, $x_{|b|_N+1}$ están en $\mathbb{U}_N$, se tiene que,

$$\left|x_1 - x_{|b|_N+1}\right| < N,$$

así su congruencia lleva a que $x_{|b|_N+1} = x_1$.
Entonces $a_{|b|_N+1} = a_1$, $x_{|b|_N+2} = x_2$ y en general $x_{|b|_N+i} = x_i$, $a_{|b|_N+i} = a_i$, $i \geq 1$. Así la secuencia de ecuaciones (3.1.1) se reduce a las primeras $|b|_N$ ecuaciones, las cuales se repiten indefinidamente. De esta forma, la expansión en base b de $\frac{x}{N}$ es periódica, con período de longitud $|b|_N$ (Teorema 1.9), la cual se escribe como

$$\frac{x}{N} = 0.\overline{a_1a_2 \ldots a_{|b|_N}}.$$

Puesto que $|b|_N$ depende de unicamente de N y b, y no de x_1, entonces cada fracción $\frac{x}{N}$ con x en $\mathbb{U}_N$ tiene período de longitud $|b|_N$.

Ejemplo 3.1. Encontrar la expansión de $\frac{1}{22}$ en base 5.
$N = 22$, $b = 5$, $x_1 = 1$; no es necesario conocer $|5|_{22}$ para avanzar. Las ecuaciones (3.1.1) ahora son

$$\begin{aligned} 5 \cdot 1 &= 0 \cdot 22 + 5 \\ 5 \cdot 5 &= 1 \cdot 22 + 3 \\ 5 \cdot 3 &= 0 \cdot 22 + 15 \\ 5 \cdot 15 &= 3 \cdot 22 + 9 \\ 5 \cdot 9 &= 2 \cdot 22 + 1 \end{aligned}$$

y puesto que $x_6 = 1 = x_1$, se tiene que $|5|_{22} = 5$ y $\frac{1}{22} = 0.\overline{01032}$ en base 5.

También se puede obtener este mismo resultado utilizando el *algoritmo de la división* implementado en SAGE, que se encuentra en el apéndice A1 y que permite determinar la lista de residuos x_i y cocientes a_i, de la siguiente forma:

```
resi_exp(1,22,5)
[[1, 5, 3, 15, 9], [0, 1, 0, 3, 2]]
```

La primera lista corresponde a los residuos x_i y la segunda a los cocientes a_i del algoritmo antes mencionado.

3.2. Propiedad de Midy para una base arbitraria

Sea $d > 1$ un divisor de $|b|_N$, es decir $|b|_N = dk$ con k en $\mathbb{Z}^+$. Se separa las primeras $|b|_N$ ecuaciones de (3.1.1) en d grupos de k ecuaciones cada uno. Para $1 \leq j \leq d$, el j-ésimo grupo consiste de las siguientes k ecuaciones

$$\begin{aligned} bx_{(j-1)k+1} &= a_{(j-1)k+1}N + x_{(j-1)k+2} \\ bx_{(j-1)k+2} &= a_{(j-1)k+2}N + x_{(j-1)k+3} \\ &\vdots \\ bx_{jk} &= a_{jk}N + x_{jk+1}. \end{aligned} \tag{3.2.1}$$

Multiplicando la primera ecuación por b^{k-1}, la segunda por b^{k-2},..., la $(k-1)$-ésima por b, y la k-ésima por $b^0 = 1$ se obtiene

$$\begin{aligned} b^k x_{(j-1)k+1} &= a_{(j-1)k+1}b^{k-1}N + \underline{b^{k-1}x_{(j-1)k+2}} \\ b^{k-1}x_{(j-1)k+2} &= a_{(j-1)k+2}b^{k-2}N + \underline{b^{k-2}x_{(j-1)k+3}} \\ &\vdots \\ bx_{jk} &= a_{jk}N + x_{jk+1}. \end{aligned} \tag{3.2.2}$$

En (3.2.2) se puede observar que cada término subrayado puede ser remplazado por el lado derecho de la ecuación que le sigue. Haciendo este remplazo se tiene que

$$b^k x_{(j-1)k+1} = (a_{(j-1)k+1}b^{k-1} + a_{(j-1)k+2}b^{k-2} + \cdots + a_{jk})N + x_{jk+1}. \tag{3.2.3}$$

La número en paréntesis es $\left[a_{(j-1)k+1}a_{(j-1)k+2}\ldots a_{jk}\right]_b$ y corresponde al j-ésimo bloque de k b-dígitos del período; este número ase denota por A_j. Así la ecuación (3.2.3) se puede escribir como $b^k x_{(j-1)k+1} = A_j N + x_{jk+1}$ y al sumar las ecuaciones de esta forma para $j = 1, 2, \ldots d$, se obtiene

$$\underbrace{b^k \sum_{j=1}^{d} x_{(j-1)k+1}}_{(*)} = N \sum_{j=1}^{d} A_j + \underbrace{\sum_{j=1}^{d} x_{jk+1}}_{(**)}. \tag{3.2.4}$$

Pero $(*)$ y $(**)$son iguales, ya que $x_{dk+1} = x_{|b|_N+1} = x_1$. De esta manera (3.2.4) puede ser reescrita como

$$(b^k - 1)\sum_{j=1}^{d} x_{(j-1)k+1} = N \sum_{j=1}^{d} A_j. \tag{3.2.5}$$

Esta relación entre las dos sumas es la clave de todo lo que sigue, de esta forma es conveniente definir

$$R_d(x) = \sum_{j=1}^{d} x_{(j-1)k+1} \quad \text{y} \quad S_d(x) = \sum_{j=1}^{d} A_j. \tag{3.2.6}$$

Al conjunto $\left\{x_1, x_{k+1}, \ldots, x_{(d-1)k+1}\right\} = \{x_{jk+1} : j \mod d\}$ se llama el d-ciclo de x; en general, para cada $i \geq 1$ el conjunto $\left\{x_i, x_{k+i}, \ldots, x_{(d-1)k+i}\right\} = \{x_{jk+i} : j \mod d\}$ se llama el d-ciclo de x_i. Para cualquier par de índices s y t, x_s y x_t tienen el mismo d-ciclo si y si sólo si $s \equiv t \pmod k$. El siguiente resultado resume lo que hasta el momento se ha tratado en esta sección.

Teorema 3.1. *Sean N y $b > 1$ enteros positivos, sea $|b|_N$ el orden de b módulo N tal que $|b|_N = dk$, con $d > 1$ y k enteros positivos. Sea x en $\mathbb{U}_N$ y $x/N = 0.\overline{a_1 a_2 \ldots a_{|b|_N}}$ en base b. Se separa el período $a_1 a_2 \ldots a_{|b|_N}$ en d bloques de longitud k cada uno. Para $j = 1, 2, \ldots, d$, $A_j = [a_{(j-1)k+1} \ldots a_{jk}]_b$ es el número en base b que representa el j-ésimo bloque. Sean $x_1 = x$, $x_2, x_3, \ldots$ los residuos en el algoritmo de la división (3.1.1) para x/N. Entonces se cumple lo siguiente:*

$$S_d(x) = (R_d(x)/N)(b^k - 1), \tag{3.2.7}$$

$$S_d(x) \equiv 0 \pmod{b^k - 1} \quad \textit{si y sólo si} \quad R_d(x) \equiv 0 \pmod N. \tag{3.2.8}$$

Demostración. Para probar (3.2.7), es cuestión de reescribir (3.2.5) en la notación (3.2.6) y entonces la relación (3.2.8) es inmediata. □

La siguiente definición corresponde a la generalización de la propiedad de Midy para una base arbitraria.

Definición 3.1. Sean x, N, b y $|b|_N$ enteros positivos, con $N, b > 1$, $\gcd(N, b) = 1$, x en $\mathbb{U}_N$ y $|b|_N = dk$ el orden de b módulo N, con $d > 1$ y k enteros positivos. Se dice que N tiene la propiedad de Midy en base b para el divisor d, si para cada x, $S_d(x) \equiv 0 \pmod{b^k - 1}$. Se denota con $M_d(b)$ el conjunto de enteros que tienen la propiedad de Midy en base b para el divisor d.

Teorema 3.2. *Las siguientes afirmaciones son equivalentes:*

(i) $N \in M_d(b)$.

(ii) Para algún $x \in \mathbb{U}_N$, $S_d(x) \equiv 0 \pmod{b^k - 1}$.

(iii) Para algún $x \in \mathbb{U}_N$, $R_d(x) \equiv 0 \pmod{N}$.

(iv) $\frac{b^{|b|_N}-1}{b^k-1} = b^{k(d-1)} + b^{k(d-2)} + \cdots + b^k + 1 \equiv 0 \pmod{N}$.

Además, $\gcd(b^k - 1, N) = 1$ *implica que* $N \in M_d(b)$.

Demostración. Del Teorema 3.1 se sigue que (iii) es equivalente con (ii). De (3.1.2) se tiene

$$R_d(x) = \sum_{j=1}^{d} x_{(j-1)k+1} \equiv \left(\sum_{j=1}^{d} b^{(j-1)k} \right) x \pmod{N},$$

y puesto que $\gcd(x, N) = 1$, entonces $R_d(x) \equiv 0 \pmod{N}$ si y sólo si $\sum_{j=1}^{d} b^{k(j-1)} \equiv 0 \pmod{N}$ de donde se tiene que (iv) es equivalente con (ii) y (iii).

Se observa que (iv) es independiente del valor que tome x en $\mathbb{U}_N$, de lo que sigue que (iv) es equivalente a $S_d(x) \equiv 0 \pmod{b^k - 1}$ para cada x en $\mathbb{U}_N$, lo cual por Definición 3.1 es (i).

Ahora se va a demostrar la última parte de este resultado. Por definición de $|b|_N$ se tiene que

$$\left(b^k - 1\right)\left(b^{k(d-1)} + b^{k(d-2)} + \cdots + b^k + 1\right) = b^{|b|_N} - 1 \equiv 0 \pmod{N},$$

y si se asume que $\gcd(b^k - 1, N) = 1$, entonces $b^{k(d-1)} + b^{k(d-2)} + \cdots + b^k + 1 \equiv 0 \pmod{N}$, y así, de (iv), se concluye que N está en $M_d(b)$. □

Ejemplo 3.2. Tomando $N = 14$, $b = 5$, $|b_N| = 6$, $x = 1$ como en el Ejemplo 3.1. El periodo es 013431 y los residuos $x_1, \ldots, x_6$ son 1, 5, 11, 13, 9, 3, respectivamente.

Con $d = 2$, $k = 3$, se tiene $S_2(1) = A_1 + A_2 = [013]_5 + [431]_5 = [444]_5 = 5^3 - 1$ y

$R_2(1) = x_1 + x_4 = 1 + 13 = 14$; así por la equivalencia entre (i) y (ii), o (i) y (iii) del Teorema 3.2, 14 está en $M_2(5)$.

Con $d = 3$, $k = 2$, $S_3(1) = A_1 + A_2 + A_3 = [01]_5 + [34]_5 + [31]_5 = [121]_5 = 36 \not\equiv 0 \pmod{5^2 - 1}$, por lo tanto 14 no está en $M_3(5)$. Calculando además $R_3(1) = x_1 + x_3 + x_5 = 1 + 11 + 9 = 21$, se puede observar que la relación (3.2.7) se cumple: $36 = \frac{21}{14}(5^2 - 1)$.

El siguiente ejemplo muestra que $\gcd(b^k - 1, N) = 1$ es condición suficiente pero no necesaria para que N esté en $M_d(B)$.

Ejemplo 3.3. Tomando $b = 10$, $N = 21$, $\frac{1}{21} = 0.\overline{047619}$, $|b|_N = 6$. Con $d = 3$, $k = 2$,

$$S_3(1) = 04 + 76 + 19 = 99 \equiv 0 \pmod{10^2 - 1},$$

así, por la equivalencia entre (i) y (ii) del Teorema 3.2, 21 está en $M_3(10)$, pero $\gcd(10^2 - 1, 21) = 3$.

Observaciones: De la Definición 3.1, no se considera la opción de que un entero N satisfaga la propiedad de Midy en base b para el divisor $d = 1$ de $|b|_N$. Cualquiera de las siguientes dos observaciones permiten ver que sucedería si se supone que N está en $M_1(b)$ y así, dar razones al lector de por que no se considera esta posibilidad.

- Si N está en $M_1(b)$, entonces para cualquier x en $\mathbb{U}_N$, $S_1(x) \equiv 0 \pmod{b^{|b|_N} - 1}$. Sea $D_b(x, N) = S_1(x) = [a_1 a_2 \dots a_{|b|_N}]_b$. Del Teorema 1.9,

  $$\frac{D_b(x, N)}{b^{|b_N|} - 1} = \frac{x}{N},$$

  y del hecho de que N está en $M_1(b)$ se tiene que $b^{|b_N|} - 1$ divide a $D_b(x, N) = S_1(x)$, de donde se concluye que N divide a x, lo que contradice el hecho de que x está en $\mathbb{U}_N$.

- Si N está en $M_1(b)$ se tiene que, $R_1(1) = 1 \equiv 0 \pmod{N}$, lo cual no es posible ya que $N > 1$.

Los siguientes resultados describen los números N que satisfacen la propiedad de Midy en base b para el divisor d de $|b|_N$ teniendo en cuenta la descomposición en factores primos de N.

Teorema 3.3. *Sea p primo que no divide a b y sea $d > 1$ un divisor de $|b|_p$, entonces p está en $M_d(b)$. Además p^h está en $M_d(b)$ para todo entero $h > 0$.*

Demostración. Sea $|b| = dk$, con $k < |b|_N$ ya que $d > 1$, así $b^k \not\equiv 1 \pmod{p}$, por lo tanto $\gcd(b^k - 1, p) = 1$, lo cual por el Teorema 3.2 implica que p está en $M_d(b)$. Se puede observar que p no es 2, de ser así b sería impar y $b^1 \equiv 1 \pmod{2}$, por tanto $|b|_2 = 1$, que no corresponde a un múltiplo de $d > 1$. Se tiene que $|b|_{p^h} = p^g |b|_p$, donde g es un entero no negativo que depende de la factorización prima de p^h como se pude observar en el Teorema 1.8 y cuyo valor no es relevante en este momento. Así $|b|_{p^h} = dK$, donde $K = kp^g$. Por el Corolario 1.6 (Pequeño teorema de Fermat), se tiene que $b^K = \left(b^k\right)^{p^g} \equiv b^k \not\equiv 1 \pmod{p}$, así $\gcd(b^K - 1, p^h) = \gcd(b^k - 1, p) = 1$ y así por el Teorema 3,2 p^h está en $M_d(b)$. □

Teorema 3.4. *Sean d_1, d_2 tales que $d_1|d_2$ y $d_2||b|_N$. Si N está en $M_{d_1}(b)$, entonces N está en $M_{d_2}(b)$.*

A continuación se presentan dos demostraciones de este resultado; la primera en relación a la segunda es más simple, pero la segunda demostración se incluye puesto que se usa para demostrar el Teorema 4.1 del capítulo 4.

1. *Demostración.* Sean k_1, k_2 enteros positivos tales que $|b|_N = k_1 d_1 = k_2 d_2$, entonces,

$$\frac{b^{|b|_N}-1}{b^{k_2}-1} = \underbrace{\left(\frac{b^{|b|_N}-1}{b^{k_1}-1}\right)}_{(*)}\underbrace{\left(\frac{b^{k_1}-1}{b^{k_2}-1}\right)}_{(**)}.$$

   Las fracciones $(*)$y $(**)$ son enteros ya que k_1 divide a $|b|_N$ y k_2 divide a k_1. Como N está en $M_{d_1}(b)$, por la equivalencia entre (i) y (iv) del Teorema 3.2,

$$\left(\frac{b^{|b|_N}-1}{b^{k_1}-1}\right) \equiv 0 \pmod{N}.$$

   De este modo

$$\frac{b^{|b|_N}-1}{b^{k_2}-1} \equiv 0 \pmod{N}$$

   de donde N está en $M_{d_2}(b)$, también por la equivalencia entre (i) y (iv) del Teorema 3.2. □

2. *Demostración.* Se tiene que $|b|_N = d_1k_1 = d_2k_2$. Sea $c = \frac{d_2}{d_1} = \frac{k_1}{k_2}$. Puesto que N está en $M_{d_1}(b)$, $R_{d_1}(x) \equiv 0 \pmod{N}$ para cada x en $\mathbb{U}_N$. Por definición, $R_{d_2}(x) = \sum_{j=0}^{d_2-1} x_{jk_2+1}$. Se va a probar que

$$R_{d_2}(x) = \sum_{r=1}^{c} R_{d_1}(x_{(r-1)k_2+1}), \tag{3.2.9}$$

   es decir $R_{d_2}(x)$ como una suma de términos congruentes con 0 módulo N, donde esta suma también es congruente con 0 módulo N, lo que implica que $S_{d_2}(x) \equiv 0 \pmod{b^{k_2}-1}$ y que N está en $M_{d_2}(b)$.
   Los números $j = 0, 1, \ldots, d_2 - 1 = cd_1 - 1$ pueden escribirse como $j = ic + r$, donde $i = 0, 1, \ldots, d_1 - 1$ y $r = 0, 1, \ldots, c-1$; entonces $jk_2 + 1 = ick_2 + rk_2 + 1 = ik_1 + rk_2 + 1$. Así

$$R_{d_2}(x) = \sum_{r=0}^{c-1}\sum_{i=0}^{d_1-1} x_{ik_1+rk_2+1},$$

   que de acuerdo a la notación que se ha venido utilizando, es equivalente a

$$R_{d_2}(x) = \sum_{r=1}^{c}\sum_{i=1}^{d_1} x_{(i-1)k_1+(r-1)k_2+1},$$

en donde $\sum_{i=1}^{d_1} x_{(i-1)k_1+(r-1)k_2+1}$ corresponde a $R_{d_1}(x_{(r-1)k_2+1})$ y esto completa la prueba. □

La idea base aquí es que el d_2-ciclo de x es la unión de c d_1-ciclos.

El siguiente resultado establece una condición necesaria y suficiente para que N esté en $M_d(b)$.

Teorema 3.5. *Sea $|b|_N = dk$ con d, k en los enteros. Si para cada factor primo p de N se tiene que k no es múltiplo de la longitud del periodo de $\frac{1}{p}$, entonces N está en $M_d(b)$.*

Demostración. De la hipótesis se tiene que si p es un factor primo de N, entonces $\gcd(N, b^k - 1) = 1$ y por lo tanto $\gcd(p^s, b^k - 1) = 1$, para cada entero s. Así, $\gcd(N, b^k - 1) = 1$ y el resultado es consecuencia del Teorema 3.2. □

Anteriormente, en una de las observaciones que le siguen al Ejemplo 3.2.1, se denotó con $D_b(x, N)$ al período $a_1 a_2 \dots a_{|b|_N}$ de la fracción $\frac{x}{N}$, para x en $\mathbb{U}_N$. Siguiendo con esta notación, en el siguiente resultado, se va a denotar con $D_b(N)$ el período de la fracción $\frac{1}{N}$.

Teorema 3.6. *N está en $M_d(b)$ si y sólo si $D_b(N) \equiv 0 \pmod{b^k - 1}$. Además, si N está en $M_d(b)$ y $\frac{b^{|b|_N}-1}{b^k-1} = Nt$ para algun entero t, entonces $D_b(N) = (b^k - 1)t$.*

Demostración. De acuerdo al Teorema 3.2, N está en $M_d(b)$ si y sólo si $\frac{b^{|b|_N}-1}{b^k-1} \equiv 0 \pmod{N}$, es decir $\frac{b^{|b|_N}-1}{b^k-1} = tN$ para algún entero t, de donde se tiene que $\frac{1}{N} = \frac{t(b^k-1)}{b^{|b|_N}-1}$ y por el Teorema 1.9 se tiene que $\frac{D_b(N)}{b^{|b|_N}-1} = \frac{t(b^k-1)}{b^{|b|_N}-1}$, de donde $D_b(N) = t(b^k - 1)$, es decir $D_b(N) \equiv 0 \pmod{b^k - 1}$. Del mismo modo, del Teorema 1.9, $ND_b(N) = b^{|b|_N} - 1$ y dividiendo esta igualdad entre $b^k - 1$ se tiene que $Nr = \frac{b^{|b|_N}-1}{b^k-1}$ donde $r = \frac{D_b(N)}{b^{|b|_N}-1}$ es un entero siempre que $D_b(N) \equiv 0 \pmod{b^k - 1}$, de ser así y por el Teorema 3.2, N está en $M_d(b)$. □

De este resultado se puede concluir inmediatamente que si $b - 1$ no es un divisor de $D_b(N)$, entonces para cualquier factor d de $|b|_N$, N no está en $M_d(b)$.

3.3. Análisis gráfico de la propiedad de Midy para $d = 2$

En esta sección se presenta una representación gráfica de fracciones cuya expansión en base b es periódica, representación que permite dar una condición necesaria y suficiente bajo la cual un entero N satisface la propiedad de Midy en base b para $d = 2$. Esta representación fue tomada de [5].

Sean $x = x_1, x_2, \dots, x_{|b|_N}$ los residuos en el algoritmo de la división usado para determinar la expansión en base b de la fracción $\frac{x}{N}$ (sección 3.1), donde x y N son enteros positivos tales que $\gcd(N, b) = 1$, $N > 1$ y $x \in \mathbb{U}_N$. A partir de los residuos antes mencionados y empezando con $i = 1$ se procede a realizar el siguiente procedimiento:

- En el plano cartesiano se trazan dos segmentos, el primero desde el punto (x_i, x_i) hasta el punto (x_i, x_{i+1}) y el segundo desde el punto (x_i, x_{i+1}) hasta el punto (x_{i+1}, x_{i+1}).
- Se incrementa i en 1 y se repiten estos dos pasos hasta que $i = |b|_N$.

Se llama **gráfica de la fracción** $\frac{x}{N}$ en base b a la construida a partir de los anteriores pasos.

Ejemplo 3.4. Se va a determinar la gráfica de la fracción $\dfrac{1}{17}$ en base 10. Inicialmente se calcula los residuos que se obtienen del algoritmo de la división que determina la expansión decimal de dicha fracción; para ello utiliza el *algoritmo de la división* implementado en SAGE y expuesto en el Apéndice A1.

```
resi_exp(1,17,10)[0]
  [1, 10, 15, 14, 4, 6, 9, 5, 16, 7, 2, 3, 13, 11, 8, 12]
```

Con esta lista se procede realizar la construcción de la gráfica de la fracción pedida, obteniendo y uniendo los puntos de acuerdo al procedimiento propuesto para dicha construcción.

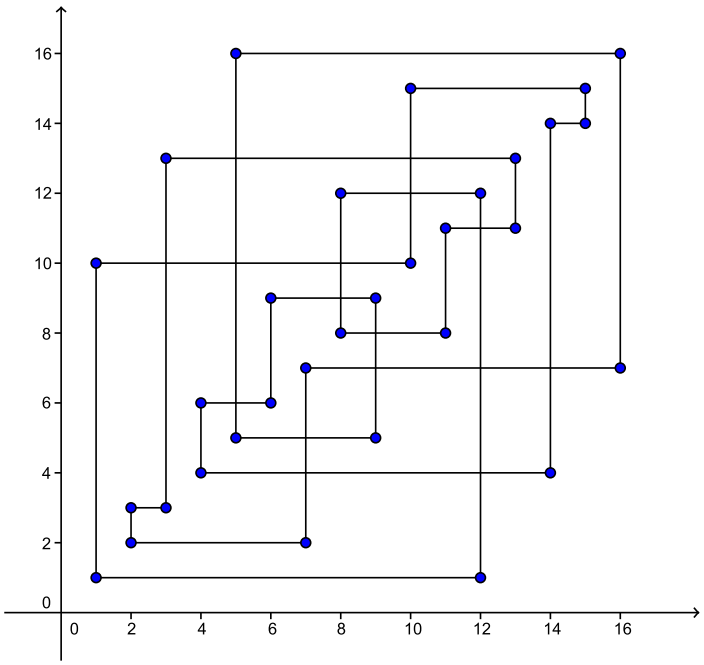

Figura 3.1: Gráfica de fracción $\frac{1}{17}$ en base 10

Ejemplo 3.5. Se va a tomar la fracción $\dfrac{1}{22}$ en base 5 como en el Ejemplo 3.1. Así, se tiene que $|5|_{22} = 5$, además, $x_1 = 1$, $x_2 = 5$, $x_3 = 3$, $x_4 = 15$, $x_5 = 9$. Los puntos que se obtienen y se deben unir de acuerdo al procedimiento propuesto para la construcción de la gráfica de esta fracción

son: $(1,1)$, $(1,5)$, $(5,5)$, $(5,3)$, $(3,3)$, $(3,15)$, $(15,15)$, $(15,9)$, $(9,9)$ y $(9,1)$. Dicha construcción se presenta en la siguiente figura.

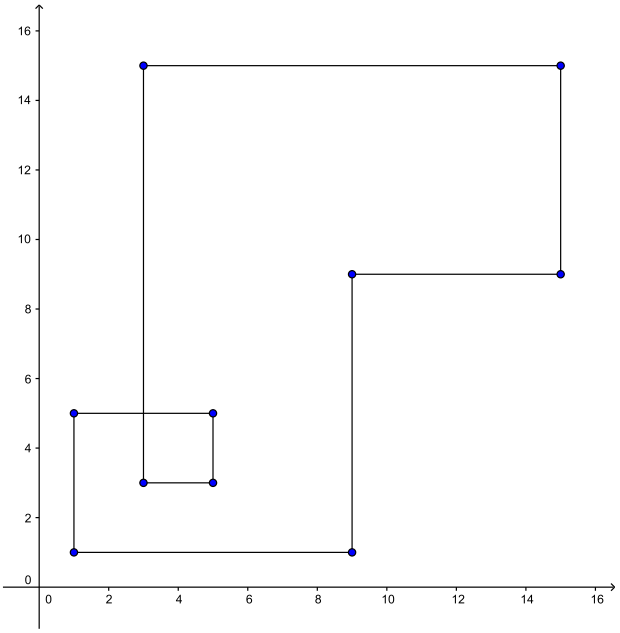

Figura 3.2: Gráfica de fracción $\frac{1}{22}$ en base 5

Definición 3.2. Se dice que la gráfica de una fracción $\frac{x}{N}$ en base b tiene simetría rotacional si al rotar la gráfica 180° alrededor del punto $\left(\frac{N}{2}, \frac{N}{2}\right)$ se consigue la misma gráfica.

Se puede observar que la gráfica de la fracción que se presenta en el Ejemplo 3.4 tiene simetría rotacional, mientras que la que se presenta en el Ejemplo 3.5 no tiene dicha simetría.

También se puede apreciar que el número total de puntos que se necesitan para determinar la gráfica de una fracción $\frac{x}{N}$ es igual a $2|b|_N$, donde la mitad corresponden a los puntos de la forma (x_i, x_i) y la otra mitad a los puntos de la forma $(x_i, x_i + 1)$, con $1 \leq i \leq |b|_N$. Además, de su construcción, se puede deducir que la gráfica de la fracción tiene simetría rotacional, si y sólo si para cada $1 \leq i \leq \frac{|b|_N}{2}$, el punto (x_i, x_i) rota al punto $\left(x_{i+\frac{|b|_N}{2}}, x_{i+\frac{|b|_N}{2}}\right)$ y viceversa, y el punto (x_i, x_{i+1}) rota al punto $\left(x_{i+\frac{|b|_N}{2}}, x_{i+1+\frac{|b|_N}{2}}\right)$y viceversa.

Particularmente, y teniendo en cuenta el objetivo de esta sección se va a considerar los enteros N tales que $|b|_N = 2k$ con $k \in \mathbb{Z}^+$. De esta forma, la gráfica de la fracción $\frac{x}{N}$ tiene simetría rotacional si y sólo si para cada $1 \leq i \leq k$ el punto (x_i, x_i) rota al punto (x_{i+k}, x_{i+k}) y viceversa, y

el punto (x_i, x_{i+1}) rota al punto (x_{i+k}, x_{i+1+k}). Puesto que la rotación se hace alrededor del punto $\left(\frac{N}{2}, \frac{N}{2}\right)$, este punto corresponde al punto medio de los puntos (x_i, x_i) y (x_{i+k}, x_{i+k}), es decir

$$\frac{x_i + x_{i+k}}{2} = \frac{N}{2},$$

en consecuencia $x_i + x_{i+k} = N$, que es equivalente a $R_2(x_i) = N$, así del Teorema 3.2 N tiene la propiedad de Midy para $d = 2$. Este resultado se enuncia formalmente en el siguiente Teorema.

Teorema 3.7. *N está en $M_2(b)$ si y sólo si la gráfica de la fracción $\frac{x}{N}$ tiene simetría rotacional.*

Ejemplo 3.6. De forma análoga a los Ejemplos 3.4 y 3.5 se obtiene la gráfica de la fracción $\frac{1}{23}$ en base 10 y se verifica que 23 satisface la propiedad de Midy para $d = 2$, observando que la gráfica tiene simetría rotacional.

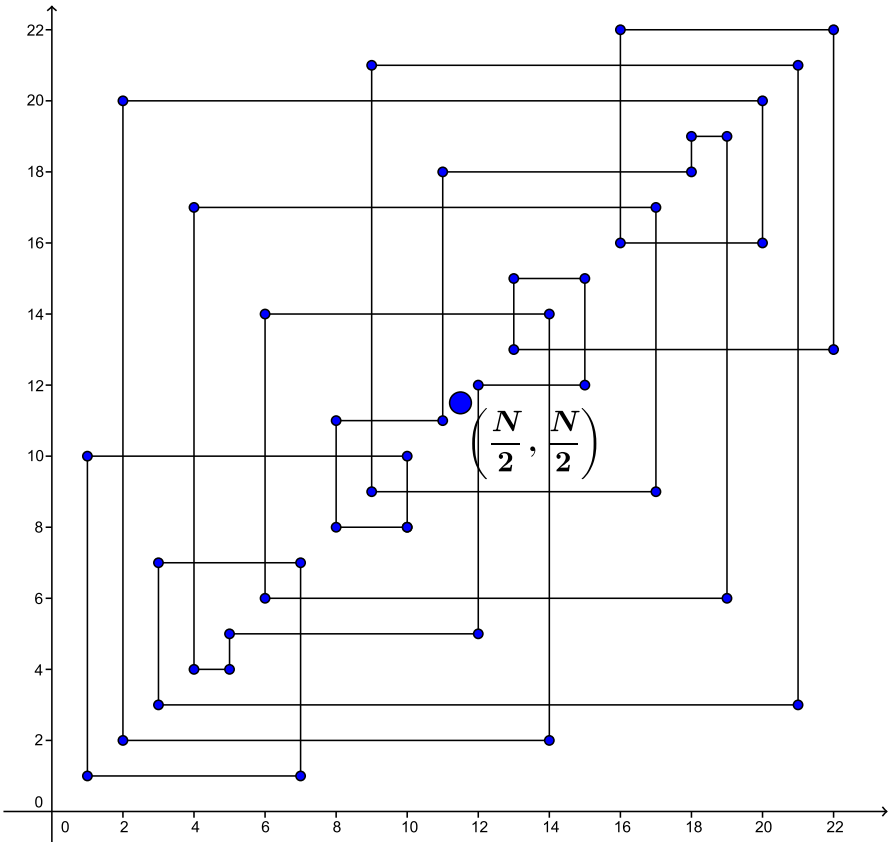

Figura 3.3: Gráfica de la fracción $\frac{1}{23}$ en base 10

.

Capítulo 4

El Multiplicador

En la Tabla 2.2, el Ejemplo 2.2 del Capítulo 2, tomando $b = 10$ se presentaron las sumas $S_d(x)$, para $d = 26$, $N = 127$ y distintos valores de x en $\mathbb{U}_{127}$. Ahí se puede observar que aunque todas las sumas son múltiplos de $10^k - 1$, éstas no son necesariamente iguales. En este capítulo se estudiará lo relacionado a estas sumas, partiendo del hecho de que N satisface la propiedad de Midy para un divisor d del orden de b, mayor que 1. Específicamente se restringe el estudio al número que multiplica a $b^k - 1$ en $S_d(x)$, a este número es al que se le denomina multiplicador. A lo largo de este capítulo se van a presentar resultados sobre el multiplicador obtenidos por J. Lewitess [6], y además se presentan dos resultados conseguidos durante el desarrollo de este trabajo de grado sobre los máximos que el multiplicador puede alcanzar.

De la Definición 3.1 se tiene que si N satisface la propiedad de Midy en base b para un divisor $d > 1$ de $|b|_N$, entonces para cada x en $\mathbb{U}_N$ se tiene que la suma $S_d(x)$ es un múltiplo de $b^k - 1$, es decir,

$$S_d(x) = m_d(x)(b^k - 1),$$

donde $m_d(x)$ es un entero al que se denomina **el multiplicador**. De la ecuación (3.2.7),

$$m_d(x) = \frac{R_d(x)}{N}. \tag{4.0.1}$$

Para la demostración de los resultados presentados en este capítulo hay que tener en cuenta el algoritmo de la división mediante el cuál se determinó la expansión en base b de la fracción $\frac{x}{N}$ que se presentó en la sección 3.1. Además se implementó en SAGE el *Algoritmo para calcular el Multiplicador* que se encuentra en el Apéndice A3.

Los dos siguientes resultados, ver [6], corresponden a casos en los cuales se puede determinar explícitamente el valor del multiplicador.

Teorema 4.1. *Si N está en $M_2(b)$ entonces para cada entero positivo par d divisor de $|b|_N$, N está en $M_d(b)$ y $m_d(x) = \frac{d}{2}$ para todo x en $\mathbb{U}_N$.*

Demostración. Sean $|b|_N = 2k$ y $x_1 = x$. Por el Teorema 3.2 se tiene que $b^k + 1 \equiv 0 \pmod{N}$, o equivalentemente $b^k \equiv -1 \pmod{N}$, multiplicando esta congruencia por x_1 y usando la relación (3.1.2) con $i = k$ se tiene que $x_{k+1} \equiv -x_1 \pmod{N}$. Pero el único elemento en $\mathbb{U}_N$ que es congruente a $-x_1$ es $N - x_1$, por lo tanto $x_{k+1} = N - x_1$. Así,

$$R_2(x) = x_1 + x_{k+1} = x_1 + (N - x_1) = N,$$

de donde se tiene que $m_2(x) = \frac{R_2(x)}{N} = 1$; esto prueba el caso para $d = 2$. Ahora se considera d, cualquier divisor par de $|b|_N$ mayor que 2. Supóngase que $d = 2c$ con $c \in \mathbb{Z}^+$, y $k' = \frac{|b|_N}{2}$. De la ecuación (3.2.9) se tiene que,

$$R_d(x) = \sum_{r=0}^{c-1} R_2\left(x_{rk'+1}\right) = \sum_{r=0}^{c-1} N = \frac{d}{2}N,$$

por lo tanto $m_d(x) = \dfrac{d}{2}$. □

En el siguiente ejemplo se observa que la condición $N \in M_2(b)$ no puede ser omitida.

Ejemplo 4.1. Para $N = 69307$, $b = 10$, $|b|_N = 12$, N no está en $M_2(10)$, pero si en $M_4(10)$ y usando el *algoritmo para calcular el multiplicador* del Apéndice A3 para determinar $m_4(1)$ se tiene que,

```
m(1,69307,10,4)
     1
```

El siguiente resultado hace referencia al multiplicador cuando N satisface la propiedad de Midy para el divisor $d = 3$ de $|b|_N$, este resultado fue demostrado en el 2004 por Ginsburg [4].

Teorema 4.2. *Sean $N \in M_3(b)$. Entonces:*

(i) $m_3(1) = 1$.

(ii) Si N es impar, $m_3(2) = 1$.

(iii) Si 3 no divide a N y $N \neq 7$, $m_3(3) = 1$.

Demostración. Supóngase que $|b|_N = 3k$ con $k \in \mathbb{Z}^+$. Para x en $\mathbb{U}_N$ se tiene que,

$$R_3(x) = x_1 + x_{k+1} + x_{2k+1} < N + N + N.$$

Puesto que $R_3(x) \equiv 0 \pmod{N}$, los posibles valores de $R_3(x_1)$ son N o $2N$. Si $x = 1$ o 2, entonces x_{k+1}, x_{2k+1} son a lo sumo $N-1$, $N-2$ (en algún orden dado que son diferentes). Así,

$$R_3(x) \leq 2 + (N-1) + (N-2) = 2N - 1 < 2N,$$

lo cual lleva a que $R_3(x_1) = N$ y por tanto $m_d(x_1) = 1$, probando (i) y (ii).

Ahora se toma $x = 3$;

$$R_3(x) \leq 3 + (N-1) + (N-2) \leq 2N,$$

donde la igualdad se cumple si y sólo si $x_{k+1} = N-1$ y $x_{2k+1} = N-2$, ó $x_{k+1} = N-2$ y $x_{2k+1} = N-1$. En el primer caso, por la relación (3.1.2), $N - 1 \equiv 3b^k \pmod{N}$ y $N - 2 \equiv 3b^{2k} \pmod{N}$, multiplicando estas dos últimas congruencias,

$$9b^{3k} \equiv 2 \pmod{N}, \tag{4.0.2}$$

pero $|b|_N = 3k$, es decir $b^{3k} \equiv 1 \pmod{N}$, así, de (4.0.1), $9 \equiv 2 \pmod{N}$, de donde $N = 7$. En el segundo caso el argumento es el mismo, intercambiando $N-1$ con $N-2$. Esto prueba (iii). □

Ejemplo 4.2. Para N=7, $b = 10$, $x = 3$, $|b|_N = 7$ y $d = 3$. Usando el *algoritmo para calcular el multiplicador* del Apéndice A3 se tiene

```
m(3,7,10,3)
     2
```

Siguiendo las ideas de Lewittes y presentadas en las demostraciones de los anteriores teoremas, se puede encontrar una cota superior para el valor de $m_d(x)$.

Sea N que está en $M_d(b)$, siendo d divisor de $|b|_N$ y sea x en $\mathbb{U}_N$. De la ecuación (4.0.1) y haciendo $x_1 = x$ se tiene que

$$m_d(x) = \frac{R_d(x)}{N} = \frac{\sum_{i=1}^{d} x_{(j-1)k+1}}{N}.$$

Teniendo en cuenta que todos los números $x_{(j-1)k+1}$ están en $\mathbb{U}_N$ y son diferentes para diferentes valores de j con $1 \leq j \leq d$, entonces pueden ser a lo sumo iguales a $N-1$, $N-2, \ldots, N-(d-1)$ y $N-d$ en algún orden. Sin pérdida de generalidad supóngase que $x_1 = N-1$, $x_{k+1} = N-2, \ldots$, $x_{(d-1)k+1} = N-d$, entonces,

$$m_d(x) = \frac{N-1+N-2+\cdots+N-d}{N} = \frac{dN - \frac{d(d-1)}{2}}{N} = d - \frac{d(d-1)}{2N} < d. \tag{4.0.3}$$

De esta última ecuación se concluye el siguiente resultado.

Teorema 4.3. *Sea $N \in M_d(b)$, entonces $m_d(x) \leq d-1$ para todo x en $\mathbb{U}_N$.*

Es posible seguir acotando los valores entre los cuales está el multiplicador siempre y cuando se cumplan ciertas condiciones, este hecho se presenta en los dos siguientes resultados.

Teorema 4.4. *Sea $N \in M_d(b)$ y x en $\mathbb{U}_N$, se tiene que:*

(i) Si $x < \frac{d(d-1)}{2}$ y $d > 2$, entonces $m_d(x) \leq d-2$.

(ii) Si $N > \frac{d(d-1)}{2}$, $x = \frac{d(d-1)}{2}$ y $m_d(x) = d-1$, entonces si d es impar, ó d es par con $b^{\frac{|b|_N}{2}} \not\equiv 1 \pmod{N}$, se cumple que $x^{d-1} \equiv (d-1)! \pmod{N}$.

Demostración.

(*i*) Supóngase que $|b|_N = dk$ con $k \in \mathbb{Z}^+$. Como $x < \frac{d(d-1)}{2}$, entonces

$$R_d(x) < \frac{d(d-1)}{2} + x_{k+1} + x_{2k+1} + \cdots + x_{(d-1)k+1}.$$

Se sabe que $x_i \neq x_j$ siempre que $|i-j| < |b|_N$, de esta forma x_{k+1}, x_{2k+1}, …, $x_{(d-1)k+1}$ son a lo sumo $N-1$, $N-2$, …, $N-(d-1)$ en algún orden. Así,

$$\begin{aligned} R_d(x) &< \frac{d(d-1)}{2} + N - 1 + N - 2 + \cdots + N - (d-1) \\ &= \frac{d(d-1)}{2} - \frac{d(d-1)}{2} + (d-1)N = (d-1)N, \end{aligned}$$

por lo tanto $R_d(x) \leq (d-2)N$ y así

$$m_d(x) = \frac{R_d(x)}{N} \leq d-2.$$

(*ii*) La condición $N > \frac{d(d-1)}{2} = x$ tiene que cumplirse para que x este en $\mathbb{U}_N$ y así tenga sentido hablar del multiplicador que en este caso es $m_d(x) = d-1$, de esta forma se tiene que

$$R_d(x) = \frac{d(d-1)}{2} + x_{k+1} + x_{2k+1} + \ldots + x_{(d-1)k+1} = N(d-1).$$

La igualdad se cumple si x_{k+1}, x_{2k+1}, …, $x_{(d-1)k+1}$ son $N-1$, $N-2$, …, $N-(d-1)$ en algún orden. Sin pérdida de generalidad, supóngase que $x_{k+1} = N-1$, $x_{2k+1} = N-2$, …, $x_{(d-1)k+1} = N-(d-1)$. Por la relación (3.1.2) se tiene

$$\begin{aligned} N - 1 &\equiv xb^k \pmod{N}, \\ N - 2 &\equiv xb^{2k} \pmod{N}, \\ &\vdots \\ N - (d-1) &\equiv xb^{(d-1)k} \pmod{N}. \end{aligned}$$

Al multiplicar las $d-1$ ecuaciones anteriores se tiene

$$(-1)^{d-1}(d-1)! \equiv x^{d-1} b^{\frac{(d-1)dk}{2}} \pmod{N}.$$

- Si d es impar, es decir $d = 2q + 1$ con $q > 0$ entero positivo, se tiene

$$(-1)^{2q+1-1}(2q+1-1)! \equiv x^{2q+1-1} b^{\frac{(2q+1-1)(2q+1)k}{2}} \pmod{N},$$

así

$$(2q)! \equiv x^{2q} b^{q(2q+1)k} \pmod{N},$$

de donde

$$(d-1)! \equiv x^{d-1} b^{dkq} \pmod{N},$$

y como $|b|_N = dk = (2q+1)k$, entonces

$$(d-1)! \equiv x^{d-1} \left(b^{|b|_N}\right)^q \pmod{N}.$$

Y puesto que $b^{|b|_N} \equiv 1 \pmod{N}$ se concluye que

$$(d-1)! \equiv x^{d-1} \pmod{N}.$$

- Si d es par, es decir $d = 2q$ con $q > 1$ entero positivo y $b^{\frac{|b|_N}{2}} \not\equiv 1 \pmod{N}$, entonces

$$(-1)^{2q-1}(2q-1)! \equiv x^{2q-1} b^{\frac{(2q-1)2qk}{2}} \pmod{N},$$

así

$$-(2q-1)! \equiv x^{2q-1} b^{(2q-1)qk} \pmod{N}$$

y como $|b|_N = dk = 2qk$ entonces

$$-(d-1)! \equiv x^{d-1} \left(b^{\frac{|b|_N}{2}}\right)^{2q-1} \pmod{N}.$$

Y puesto que $b^{|b|_N} \equiv 1 \mod N$ entonces $b^{|b|_N} - 1 \equiv 0 \pmod{N}$ y factorizando se tiene $\left(b^{\frac{|b|_N}{2}} - 1\right)\left(b^{\frac{|b|_N}{2}} + 1\right) \equiv 0 \pmod{N}$, pero por hipótesis N no divide a $\left(b^{\frac{|b|_N}{2}} - 1\right)$, de esta manera, $b^{\frac{|b|_N}{2}} + 1 \equiv 0 \pmod{N}$, es decir $b^{\frac{|b|_N}{2}} \equiv -1 \pmod{N}$, por lo tanto,

$$-(d-1)! \equiv -x^{d-1} \pmod{N},$$

es decir

$$(d-1)! \equiv x^{d-1} \pmod{N}.$$

□

En el siguiente ejemplo se ilustra que sí es posible alcanzar el máximo valor propuesto para el multiplicador en la primera parte del resultado anterior.

Ejemplo 4.3. Se tiene que 39 satisface la propiedad de Midy para $d = 6$ en base $b = 10$ y usando el *algoritmo para calcular el multiplicador* del Apéndice A3

```
m(7,39,10,6)
     4
```

El Teorema 4.2 es un caso particular del teorema 4.4, para $d = 3$.

El siguiente corresponde al último de los resultados que surgieron de la investigación realizada sobre la Propiedad de Midy, específicamente de las cotas del multiplicador.

Teorema 4.5. *Sea $N \in M_d(b)$ y rd múltiplo de d y divisor de $|b|_N$ donde r es entero positivo, entonces $N \in M_{rd}(b)$ y $m_{rd}(x) \leq r(d-1)$.*

Demostración. La primera parte de este resultado corresponde al Teorema 3.4. Bajo las condiciones expuestas se procede entonces a demostrar que $m_{rd}(x) \leq r(d-1)$.

Se tiene que $|b|_N = drk' = dk$ con $k = rk'$, r y k' enteros positivos. Se sabe que

$$R_{dr}(x) = \sum_{j=1}^{dr} x_{k'(j-1)+1}.$$

De la ecuación (3.2.9) se tiene que

$$R_{dr}(x) = \sum_{j=1}^{r} R_d(x_{(j-1)k'+1}).$$

Por lo tanto,

$$m_{rd}(x) = \frac{\sum_{j=1}^{r} R_d(x_{(j-1)k'+1})}{N} = \sum_{j=1}^{r} m_d(x_{(j-1)k'+1}) \underbrace{\leq}_{(*)} \sum_{j=1}^{r}(d-1) = r(d-1).$$

La relación $(*)$ se justifica por el Teorema 4.3. □

Conclusiones

- En este trabajo se recopilaron y organizaron algunos de los avances teóricos alrededor de la propiedad de Midy y en base a ellos se construyeron algoritmos en el sistema de álgebra computacional SAGE que permitieron ejemplificar algunas de sus características y propiedades. Específicamente los algoritmos implementados en el software antes mencionado sirven para determinar si un entero satisface la propiedad de Midy y calcular el multiplicador.
- En la Sección 3.3 se pudo observar que es posible realizar un estudio de la propiedad de Midy desde un punto de vista geométrico. En este caso, a través de la construcción de una representación gráfica de fracciones se presentó una forma alternativa de probar si un entero positivo N satisface la propiedad de Midy para $d = 2$.
- Mediante observaciones realizadas en otras investigaciones es posible proponer algunas condiciones que permiten generalizar resultados de estas, tal es el caso del Teorema 4.4 que viene a ser una generalización del Teorema 4.2 citado del artículo de Joseph Lewittes [6].
- Aún se pueden encontrar problemas abiertos respecto a la temática tratada en este trabajo e investigadores como J. H Castillo, G. García-Pulgarín, J. M. Velásquez-Soto, continúan trabajando en sus posibles soluciones. Por lo tanto este es un campo en el que se pueden desarrollar futuras investigaciones, como por ejemplo la búsqueda de fórmulas explícitas para el multiplicador.

Apéndice

En este apartado se presentan algoritmos implementados en el sistema de álgebra computacional SAGE que permitieron ejemplificar algunas características referentes a la teoría abordada en este trabajo.

A.1. Algoritmo de la división

Dados los enteros positivos N, x en $\mathbb{U}_N$, y la base b. Este algoritmo retorna las listas A y L de cocientes y residuos respectivamente, que se obtienen del algoritmo de la división que permite determinar la expansión en base b de la fracción $\frac{x}{N}$ que se presentó en la sección 3.1.

```
def resi_exp(x,N,b):
    x0=x
    L=[ ]
    A=[ ]
    L.append(x)
    a=(b*x) // N
    A.append(a)
    while b*x % N <> x0:
        x=(b*x) % N
        a=(b*x) // N
        A.append(a)
        L.append(x)
    return [L,A]
```

A.2. Algoritmo para determinar si un entero N satisface la propiedad de Midy

Dados los enteros positivos N, la base b y un divisor d de $|b_N|$. Este algoritmo retorna o bien "N tiene la propiedad de Midy" o "N no tiene la propiedad de Midy". Este algoritmo fue implementando en SAGE haciendo uso de la equivalencia (iv) del Teorema 3.2.

```
def bmidy(b,N,d):
    e=multiplicative_order(mod(b,N))
    k=e/d
    r=(b^(e)-1)/(b^(k)-1)
```

```
    m=mod(r,N)
    if m==0:
        return 'N tiene la propiedad de Midy'
    else:
        return 'N no tiene la propiedad de Midy'
```

A.3. Algoritmo para calcular el Multiplicador

Dados los enteros positivos N, b, d divisor de $|b|_N$, y x en $\mathbb{U}_N$; tales que N está en $M_d(b)$. Este algoritmo retorna el multiplicador:

$$m_d(x) = \frac{R_d(x)}{N} = \frac{\sum_{j=1}^{d} x_{(j-1)k+1}}{N}, \quad \text{con} \quad |b|_N = dk.$$

```
def rd(x,N,b,d):
    L=resi_exp(x,N,b)[0]
    v=len(L)
    k=v/d
    s=0
    for i in [1..d]:
        r=k*i-k
        s=L[r]+s
    return s/N
```

Bibliografía

[1] J. H. Castillo, G. García-Pulgarín, and J. M. Velásquez-Soto. Structure of associated sets to Midy's Property. *Mat. Enseñ. Univ. (N. S.)*, XX(1):21–28, 2012.

[2] L. Dickson. *History of the theory of numbers*. Chelsea, New York, 1992.

[3] G. García-Pulgarín and H. Giraldo. Characterizations of Midy's property. *Integers*, 9:A18, 191–197, 2009.

[4] B. D. Ginsburg. Midy's (nearly) secret theorem—an extension after 165 years. *College Math. J.*, 35(1):26–30, 2004.

[5] R. Jones and J. Pearce. A postmodern view of fractions and the reciprocals of fermat primes. *Math. Mag.*, 73(2):83–79, 2000.

[6] J. Lewittes. Midy's theorem for periodic decimals. *Integers*, 7:A2, 11 pp. (electronic), 2007.

[7] H. W. Martin. Generalizations of Midy's theorem on repeating decimals. *Integers*, 7:A3, 7 pp. (electronic), 2007.

[8] E. Midy. De quelques propriétés des nombres et des fractions décimales peŕiodiques. *Nantes*, page 21, 1836.

[9] A. Vazzana, M. Erickson, and D. Garth. *Introduction to Number Theory*. Textbooks in Mathematics. Taylor & Francis, 2007.