SOBRE LA PROPIEDAD DE MIDY

JUAN CAMILO CALA BARÓN

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA

2015

SOBRE LA PROPIEDAD DE MIDY

Autor

JUAN CAMILO CALA BARÓN

Trabajo de grado para optar al título de

Matemático

Director

CARLOS ARTURO RODRIGUEZ PALMA

Magíster en Ciencias

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA

2015

Universidad Industrial de Santander

NOTA DE PROYECTO DE GRADO

NOMBRE DEL ESTUDIANTE: JUAN CAMILO CALA BARÓN	2112650
TITULO DEL PROYECTO : "Sobre la propiedad de Midy"	
FACULTAD : *Ciencias*	CARRERA: ***MATEMÁTICAS***
NOTA DEFINITIVA: **CUATRO, CINCO(4.5)**	CREDITOS: *10*

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

FIRMA

Carlos A. Rodríguez.

CALIFICADORES

		FECHA
F Hector Pinedo T.	F	A 15 M 8 D 20
HÉCTOR EDONIS PINEDO T.	**EDILBERTO JOSÉ REYES**	

Universidad Industrial de Santander

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

Yo, **JUAN CAMILO CALA BARÓN**, mayor de edad, vecino de Bucaramanga, identificado con la Cédula de Ciudadanía **No 1.098.730.052** de Bucaramanga, actuando en nombre propio, en mi calidad de autor del trabajo de grado, del trabajo de investigación, o de la tesis denominada(o): **SOBRE LA PROPIEDAD DE MIDY**, hago entrega del ejemplar respectivo y de sus anexos de ser el caso, en formato digital o electrónico (CD o DVD) y autorizo a **LA UNIVERSIDAD INDUSTRIAL DE SANTANDER**, para que en los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia, utilice y use en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador de la obra objeto del presente documento.

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

EL AUTOR / ESTUDIANTE, manifiesta que la obra objeto de la presente autorización es original y la realizó sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de su exclusiva autoría y detenta la titularidad sobre la misma. PARÁGRAFO: En caso de presentarse cualquier reclamación o acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión, EL AUTOR / ESTUDIANTE, asumirá toda la responsabilidad, y saldrá en defensa de los derechos aquí autorizados; para todos los efectos la Universidad actúa como un tercero de buena fe. Para constancia se firma el presente documento en dos (02) ejemplares del mismo valor y tenor, en Bucaramanga, a los 24 días del mes de Agosto de Dos Mil quince (2015).

EL AUTOR / ESTUDIANTE:

Juan Camilo Cala Barón.
CC 1.098.730.052

Agradecimientos

Durante mi proceso de formación profesional, han habido personas que han contribuido tanto en la parte académica como en la parte personal y quisiera agradecerles por tal motivo:

- A todos y cada uno de los profesores con quien tuve la oportunidad de educarme a lo largo de mi carrera, pues de ellos aprendí lo que quiero y lo que no quiero ser como profesional; especialmente a mi director de proyecto Carlos Arturo por haber aceptado este cargo, ser mi tutor, colega y amigo.
- Al grupo "Olimpiadas Regionales de Matemáticas", del cual hago parte, por permitirme desempeñar tan maravillosa labor y a cada uno de sus integrantes por brindarme su amistad.
- A mis familiares, amigos y compañeros de aula.

De igual forma, además de agradecer quisiera dedicar este trabajo a mis padres, por haberme brindado el apoyo necesario durante este largo proceso, y a mi novia por su comprensión y paciencia hacia mi amor por la matemática. Sin ellos hubiera sido imposible estar culminando esta etapa.

Índice general

pág.

Introducción **11**

1 Preliminares **14**

1.1 Divisibilidad en $\mathbb{Z}$ 14

1.2 Teorema fundamental de la aritmética 16

1.3 Aritmética modular 17

1.3.1 Nociones básicas 17

1.3.2 Teorema de Fermat y la función ϕ de Euler 18

1.4 Estructura algebraica de $\mathbb{Z}$ 18

1.5 Representación de los números por decimales 22

2 Una prueba para el teorema de midy **28**

3 Generalizaciones del teorema de midy **37**

3.1 El teorema de midy en base 10 39

3.2 El teorema de midy en base B 47

A Algoritmos **66**

Referencias bibliográficas **72**

Índice de tablas

pág.

Tabla 1 Estudio de los primos de Mersenne. 35

Tabla 2 Verificación del Teorema 3.5 para $n = 49$. 42

Tabla 3 Uso del Teorema 3.9 para $n = 217$. 43

Tabla 4 Orden de 3 módulo 17^h para $h \leqslant 10$. 53

Tabla 5 Estudio de la propiedad de Midy para $n = 98$ y $B = 3$. 57

Resumen

TÍTULO: SOBRE LA PROPIEDAD DE MIDY[1].

AUTOR: JUAN CAMILO CALA BARÓN[2].

PALABRAS CLAVE: Teorema de Midy; propiedad de los 9's; representación por decimales.

DESCRIPCIÓN:

Sean p un número primo y e el orden de 10 módulo p, es decir, $e = \text{ord}_p(10)$. Es sabido que la fracción $1/p$ es periódica con periodo de longitud e. E. Midy demostró que si $1/p$ tiene periodo de longitud par $e = 2k$, para algún entero positivo k, y $1/p = 0.\overline{a_1 a_2 \cdots a_e}$, donde cada a_i es un dígito, entonces $a_i + a_{k+i} = 9$ para $i = 1, 2, \ldots, k$. En otras palabras, si el periodo se divide en dos mitades, su suma es igual a $10^k - 1$, una cadena de k nueves. Este resultado se conoce como el Teorema de Midy.

En este trabajo, el interés principal es el problema general que se desprende del Teorema de Midy. Dados los enteros n y una base numérica $B > 1$ con n y B primos relativos, la fracción x/n, donde $x \in \mathbb{U}_n$, es periódica en la escala de B con periodo de longitud $e = \text{ord}_n(B)$. Si $e = dk$, para algún par de enteros $d > 1$ y k, el periodo puede dividirse en d bloques cada uno de k dígitos. Si la suma de estos bloques es un múltiplo de $B^k - 1$ para cada elemento $x \in \mathbb{U}_n$, se dirá que n tiene la propiedad de Midy para el divisor d de e y la base B, y se escribirá esto por $n \in M_d(B)$.

[1]Tesis.

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

Abstract

TITLE: ABOUT MIDY'S PROPERTY[3].

AUTHOR: JUAN CAMILO CALA BARÓN[4].

KEYWORDS: Midy's theorem; 9's property; representation by decimals.

DESCRIPTION:

Let p be a prime number and e the order of 10 modulo p, that is, $e = \text{ord}_p(10)$. It is known that the fraction $1/p$ is periodic and has period lenght equals e. E. Midy proof that if $1/p$ has even period lenght $e = 2k$, for some positive integer k, and $1/p = 0.\overline{a_1 a_2 \cdots a_e}$, where each a_i is a digit, then $a_i + a_{k+i} = 9$ for $i = 1, 2, \ldots, k$. In other words, if the period is broken into two halves, their sum equals $10^k - 1$, a string of k nines. This result is known as Midy's Theorem.

In this work, the main interest is the general problem which follows from the Midy's Theorem. Given integers n and a number base $B > 1$ with n and B relatively primes, the fraction x/n, where $x \in \mathbb{U}_n$, is periodic in the scale of B with period lenght $e = \text{ord}_n(B)$. If $e = dk$, for some pair of integers $d > 1$ and k, the period can be broken into d blocks each one containing k digits. If the sum of these blocks is a multiple of $B^k - 1$ for every element $x \in \mathbb{U}_n$, it will be said that n has the Midy's property for the divisor d of e and the number base B, and this will be written by $n \in M_d(B)$.

[3]Thesis.

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

"If people do not believe that mathematics is simple, it is only because they do not realize how complicated life is."

John von Neumann

Introducción

No se puede poner en duda que los números enteros constituyen dentro del campo de las matemáticas una de las principales atracciones debido a la belleza de su simplicidad. Han sido motivo de estudio por sus particulares características, hecho que ha conllevado a los matemáticos a crear estructuras generalizadas que compartan estas mismas singularidades desde el punto de vista algebraico, como lo son los enteros algebraicos que desarrollan un papel vital en la teoría algebraica de números; son los enteros los principales protagonistas, el punto de referencia. Pudiese uno entonces emprender un viaje en búsqueda de tales propiedades y seguramente el resultado sería un total éxito, pero verdaderamente extenso.

No obstante, si nos fijamos en el caso de la operación división entre dos números enteros, aunque tenemos nuevamente un sinfín de resultados y propiedades escondidas allí, el asunto se reduce un poco. Es sabido que para cuando p es un número primo la fracción $1/p$ es periódica. Particularmente para $p = 13$,

$$\frac{1}{13} = 0.\overline{076923}$$

tiene período de longitud 6. Puede observarse que si se divide la expresión después del punto decimal en dos bloques de tres dígitos (exactamente a la mitad) y se suman, resulta que $076+923 = 999$ es una cadena de tres 9's. Del mismo modo, $1/7 = 0.\overline{142857}$ tiene período 6 y $142+857 = 999$. Igualmente, la fracción $1/19 = 0.\overline{052631578947368421}$ tiene período 18 y la suma $052631578 + 947368421 = 999999999$ es una cadena de nueve 9's. Y se puede seguir así verificando esta propiedad para muchos más casos

particulares. Sin embargo, es fácilmente verificable que para $p = 2, 3, 5$ dicha propiedad no se satisface.

Hacia mediados de 1836 el matemático francés E. Midy, según [7], publicó en su país natal un artículo referente a la propiedad mencionada en el párrafo anterior. Allí, formalizó el resultado de la siguiente forma:

Teorema de Midy. *Si para $p > 5$ un número primo la fracción $1/p$ tiene periodo de longitud par, digamos $e = 2k$ para algún entero positivo k, entonces la suma de las mitades que conforman el periodo es una cadena de k 9's.*

En el transcurso de los últimos 10 años esta propiedad ha despertado el interés de la comunidad matemática hasta tal punto que en la actualidad ya se conoce relativamente lo suficiente sobre ella. El pionero de este auge fue Ginsberg que, en [3], sube un peldaño y prueba el Teorema de Midy para el caso en que la longitud del período es de la forma $e = 3k$. Formalmente, el resultado queda enunciado así:

Teorema de Ginsberg. *Sea p un primo tal que*

$$\frac{1}{p} = 0.\overline{a_1 a_2 \dots a_e},$$

donde cada a_i es un dígito y la longitud del período es $e = 3k$ para algún entero positivo k. Si se divide el periodo en 3 bloques donde cada uno contiene k dígitos, la suma de ellos es igual a $10^k - 1$, una cadena de k 9's.

Siguiendo este camino de generalizar sobre la longitud del período, Gupta y Sury en [4] prueban el caso cuando este es de la forma $e = dk$ con $d > 1$, de modo que el período se puede dividir en d sub-bloques de k dígitos y su suma es un múltiplo de $10^k - 1$. Posteriormente, Martin en [8] desarrolla las primeras generalizaciones y caracterizaciones al utilizar las fracciones $1/n$ donde n no es necesariamente un número primo y extiende la propiedad de Midy en su estado puro, es decir, cuando la longitud del periodo es $e = 2k$. Finalemente, Lewittes y García-Pulgarín junto con Giraldo en [7] y [2], respectivamente, formalizan la propiedad de Midy y llevan el problema a otro

nivel recopilando el trabajo anterior cuando se trabaja con las fracciones x/n donde $x \in \mathbb{U}_n$, el grupo multiplicativo de la unidades de $\mathbb{Z}_n$, y su desarrollo es sobre cualquier base numérica $B > 1$.

Durante esta formalización de la propiedad de Midy surgen preguntas sobre condiciones necesarias y suficientes para las cuales las fracciones $1/n$ la cumplan, así como las caracterizaciones y generalizaciones a las que se han llegado. Por otro lado, cómo influye la base numérica en la que se desarrolle la expansión de $1/n$. La respuesta de dichas cuestiones y las extensiones que de ellas se desprendan se encuentran en la literatura y serán el motivo principal de estudio y de la realización de este trabajo monográfico.

Capítulo 1

Preliminares

En este primer capítulo vamos a enunciar algunos resultados clásicos de la Teoría de Números que serán utilizados a lo largo de este trabajo monográfico. Las demostraciones de cada uno de ellos pueden ser encontradas en cualquier libro de Teoría de Números elemental (ver por ejemplo [1] o [5]). La Sección 1.5 es la que brinda más información que está directamente relacionada con el contenido de este trabajo, por lo que invitamos al lector a revisarla, a pesar de la brevedad con la que se desarrolla.

1.1. Divisibilidad en $\mathbb{Z}$

Teorema 1.1 (Algoritmo de la División)**.** *Sean $a, b \in \mathbb{Z}$ con $b > 0$. Existen enteros únicos q y r con $0 \leqslant r < b$ tales que*

$$a = bq + r.$$

Los enteros q y r se dicen *cociente* y *residuo*, respectivamente, de la división de a entre b.

Definición 1.2. Sean $a, b \in \mathbb{Z}$ con $a \neq 0$. Diremos que b *es divisible por* a si existe un $c \in \mathbb{Z}$ tal que

$$b = ac.$$

En dicho caso decimos que a divide a b y lo denotamos por $a \mid b$. De no ocurrir esto escribimos $a \nmid b$.

Teorema 1.3. *Sean $a, b, c \in \mathbb{Z}$.*

I. *Si $a \mid b$ y $c \mid d$, entonces $ac \mid bc$.*

II. *Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.*

III. *Si $a \mid b$ y $b \neq 0$, entonces $|a| \leqslant |b|$.*

IV. *Si $a \mid b$ y $a \mid c$, entonces $a \mid (xb + yc)$ para cualesquiera $x, y \in \mathbb{Z}$.*

Cuando exista un entero d tal que $d \mid a$ y $d \mid b$, decimos que d es un *divisor común* de a y b. Puesto que el número de divisores de cualquier entero $c \neq 0$ es finito, los divisores comunes de dos enteros a y b con al menos uno no nulo es finito, lo cual garantiza la existencia del mayor de todos ellos. Esto motiva la siguiente definición.

Definición 1.4. Dados $a, b \in \mathbb{Z}$ con al menos uno de ellos distinto de cero, el mayor entero que divide a ambos a y b se denomina *máximo común divisor de a y b* y lo denotaremos por $\gcd(a, b)$. Es decir, $d = \gcd(a, b)$ si y solo si se satisface:

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

II. Si $c \mid a$ y $c \mid d$, entonces $c \leqslant d$.

Teorema 1.5. *Sean $a, b \in \mathbb{Z}$ con al menos uno distinto de cero y $d = \gcd(a, b)$. El entero d es el menor entero positivo que es combinación lineal de a y b, esto es,*

$$d = \min \{au + bv > 0 : u, v \in \mathbb{Z}\}.$$

Definición 1.6. Decimos que los enteros a y b con alguno de ellos distinto de cero son *primos relativos* cuando $\gcd(a, b) = 1$.

Teorema 1.7. *Sean $a, b \in \mathbb{Z}$ no ambos iguales a cero, entonces a y b son primos relativos si y solo si existen $x, y \in \mathbb{Z}$ tales que $1 = ax + by$.*

Corolario 1.8. *Supongamos que $a \mid c$ y $b \mid c$. Si $\gcd(a,b) = 1$ entonces $ab \mid c$.*

Lema 1.9. *Si $a \mid bc$ y $\gcd(a,b) = 1$, entonces $a \mid c$.*

Teorema 1.10 (Algoritmo de Euclides)**.** *Sean $a, b \in \mathbb{Z}$, si $a = bq + r$ para algunos $q, r \in \mathbb{Z}$ entonces $\gcd(a,b) = \gcd(b,r)$.*

Teorema 1.11. *Dado $b > 1$, todo entero n se pude expresar de forma única en términos de potencias de b como*

$$n = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_1 b + a_0, \tag{1.1}$$

donde los coeficientes toman valores $a_k = 0, 1, 2, \ldots, b-1$.

Puesto que la representación (1.1) es única, n está completamente determinado por los coeficientes $a_m, a_{m-1}, \ldots, a_1, a_0$ y escribimos la representación de n en base b como

$$n = [a_m a_{m-1} a_1 a_0]_b \,.$$

A cada uno de los a_i los llamaremos b-dígitos.

1.2. Teorema fundamental de la aritmética

Definición 1.12. Un entero $n > 1$ se denomina un número *primo* si sus únicos divisores son 1 y n. En caso contrario, decimos que n es un número compuesto.

Teorema 1.13. *Si p es primo y $p \mid ab$, entonces $p \mid a$ o $p \mid b$.*

Teorema 1.14 (Fundamental de la Aritmética)**.** *Todo entero positivo $n > 1$ es primo o es producto de primos. Esta representación es única salvo el orden en que aparecen los factores.*

Corolario 1.15. *Cualquier entero $n > 1$ se puede representar de forma única como*

$$n = p_1^{\alpha_1} \, p_2^{\alpha_2} \ldots \, p_k^{\alpha_k} \tag{1.2}$$

donde los $\alpha_i \in \mathbb{Z}^+$ *y* $p_1 < p_2 < \cdots < p_k$*, con* p_i *primo para* $i = 1, 2, \ldots, k$*.*

Usualmente la expresión (1.2) se llama la factorización prima de n o la descomposición canónica de n.

1.3. Aritmética modular

1.3.1. Nociones básicas

Definición 1.16. Sea n un entero positivo fijo. Dos enteros a y b se dicen *congruentes módulo* n, denotado $a \equiv b \pmod{n}$, si $n \mid b - a$.

Teorema 1.17. *Sean* $a, b \in \mathbb{Z}$*, entonces* $a \equiv b \pmod{n}$ *si y solo si* a *y* b *dejan el mismo residuo al dividirse por* n*.*

Teorema 1.18. *Sean* $a, b, c, d, n \in \mathbb{Z}$ *con* $n \geqslant 1$*, entonces:*

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

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

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

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

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

VI. *Si* $a \equiv b \pmod{n}$ *entonces* $a^k \equiv b^k \pmod{n}$ *para todo* $k = 1, 2, 3, \ldots$

Teorema 1.19 (Chino del Residuo)**.** *Sean* $n_1, n_2, \ldots, n_k$ *enteros positivos primos relativos dos a dos. Si* $a_1, a_2, \ldots, a_k$ *son enteros, el sistema de congruencias*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k}, \end{aligned}$$

tiene solución única módulo $n = n_1 n_2 \cdots n_k$*, esto es, si* x_1 *y* x_2 *son soluciones del sistema, entonces* $x_1 \equiv x_2 \pmod{n}$.

1.3.2. Teorema de Fermat y la función ϕ de Euler

Teorema 1.20 (Fermat)**.** *Si* p *es primo y* $p \nmid a$*, se tiene que*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Definición 1.21. Sea $n \geqslant 1$ un entero positivo. La función $\phi(n)$ denota el número de enteros positivos menores o iguales a n que son primos relativos con n. Es decir, si

$$\mathcal{S} = \left\{ x \in \mathbb{Z} : 1 \leqslant x \leqslant n \wedge \gcd(x, n) = 1 \right\}$$

entonces $\phi(n) = |\mathcal{S}|$.

Es inmediato ver que la función ϕ caracteriza a los números primos. De hecho, n es primo si y solo si $\phi(n) = n - 1$.

Teorema 1.22 (Euler-Fermat)**.** *Si* n *es un entero positivo y* $\gcd(a, n) = 1$*, entonces*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Definición 1.23. Un entero $a \neq 0$ es una *raíz primitiva módulo* n si $\varphi(n)$ es el menor exponente t para el cual $a^t \equiv 1 \pmod{n}$.

1.4. Estructura algebraica de $\mathbb{Z}$

Definición 1.24. Decimos que un conjunto $G \neq \emptyset$ dotado de una operación binaria $* : G \times G \to G$ es un *grupo* si se satisfacen los siguientes axiomas:

A1. Para cada par de elementos $a, b \in G$, $a * b \in G$.

A2. Existe un elemento $e \in G$ tal que $a * e = e * a = a$ para todo $a \in G$.

A3. Para cada $a \in G$, existe $a^{-1} \in G$ tal que $a * a^{-1} = a^{-1} * a = e$.

A4. $a * (b * c) = (a * b) * c$ para todo $a, b, c \in G$.

El axioma **A1** de la definición anterior se conoce como la *propiedad clausurativa* o *propiedad de cerradura* y puede omitirse pues se sigue inmediatamente del hecho que $*$ es una operación binaria sobre G. Los elementos e y a^{-1} se dicen neutro e inverso de a, respectivamente. Al axioma **A4** se le conoce también como la *propiedad asociativa*.
Denotamos un grupo por $\langle G, * \rangle$ o simplemente G cuando no haya confusión sobre la operación $*$.

Ejemplo 1.25. $\mathbb{Z}$ con la operación suma usual $+$ es un grupo. De hecho, los conjuntos numéricos $\langle \mathbb{Q}, + \rangle$, $\langle \mathbb{R}, + \rangle$ y $\langle \mathbb{C}, + \rangle$ son grupos bajo esta misma operación.

Ejemplo 1.26. Sea $n \geqslant 1$ un número entero. Definamos

$$n\mathbb{Z} = \{nt : t \in \mathbb{Z}\}$$

el conjunto de los múltiplos de n. Para $a, b \in \mathbb{Z}$, la relación de congruencia módulo n anteriormente introducida en la Sección 1.3 se puede establecer así: $a \equiv b \,(\text{mód } n)$ si y solo si $b - a \in n\mathbb{Z}$. Por el Teorema 1.18, esta relación es de equivalencia sobre $\mathbb{Z}$, luego las clases de equivalencia módulo n para cada $m \in \mathbb{Z}$ vienen dadas por

$$[m] = \left\{x \in \mathbb{Z} : x \equiv m \,(\text{mód } n)\right\} = \{m + nt : t \in \mathbb{Z}\}\,.$$

Observe que si $m \geqslant n$, podemos escribir por el algoritmo de la división $m = nq + r$ con $0 \leqslant r < n$, de donde $r \in [m]$ y por tanto $[m] = [r]$. De ahí que las clases de equivalencia módulo n están completamente determinadas por los residuos $0, 1, 2, \ldots, n-1$, de modo que el conjunto cociente

$$\mathbb{Z}/n\mathbb{Z} = \left\{[0], [1], [2], \ldots, [n-1]\right\}$$

se conoce como el conjunto de las clases residuales módulo n. Definamos la operación $\oplus$ en $\mathbb{Z}/n\mathbb{Z}$ mediante la regla

$$[x] \oplus [y] \coloneqq [x + y],$$

donde la suma a la derecha de la igualdad es la usual en los enteros. Entonces $\langle \mathbb{Z}/n\mathbb{Z}, \oplus \rangle$ es un grupo. Por conveniencia, nos referiremos a este grupo como $\mathbb{Z}_n$ y escribiremos

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}.$$

Ejemplo 1.27. En $\mathbb{Z}/n\mathbb{Z}$ definamos para $a, b \in \mathbb{Z}$ el producto módulo n como

$$[a] \odot [b] \coloneqq [a \cdot b],$$

entonces $\mathbb{U}_n$ es un grupo bajo el producto módulo n, donde

$$\mathbb{U}_n = \left\{ x \in \mathbb{Z}_n : \gcd(x, n) = 1 \right\}.$$

Proposición 1.28. *Si G_1 y G_2 son dos grupos, entonces $G = G_1 \times G_2 = \{(a, b) : a \in G_1 \text{ y } b \in G_2\}$ es un grupo con la operación heredada por G_1 y G_2 componente a componente, esto es, $(a, b)(c, d) = (ac, bd)$, para $a, c \in G_1$ y $b, d \in G_2$.*

Definición 1.29. Sean $\langle G, * \rangle$ un grupo y $H \subseteq G$ un subconjunto no vacío de G. Decimos que H es un *subgrupo* de G, y lo denotamos por $H \leq G$, si $\langle H, * \rangle$ es un grupo.

Dados un grupo $\langle G, * \rangle$, $a \in G$ y un entero positivo n, si definimos de manera natural $a^2 \coloneqq a * a$ es fácil probar mediante inducción matemática que

$$a^n \coloneqq \underbrace{a * a * \cdots * a}_{n-veces}.$$

Definición 1.30. Sean G un grupo y $a \in G$. El *orden* del elemento a, denotado $\mathrm{ord}_G(a)$, es el menor entero positivo m tal que $a^m = e$.

Cuando $G = \mathbb{U}_n$, $e = 1$ y si para $a \in \mathbb{Z}$ existe $m = \min\left\{ j \in \mathbb{Z}^+ : a^j \equiv 1 \pmod{n} \right\}$,

diremos que m es el orden de a módulo n y lo denotaremos mediante $m = \text{ord}_n(a)$. Así las cosas, el concepto dado en la Definición 1.23 puede establecerse ahora diciendo que un entero $a \neq 0$ es una raíz primitiva modulo n si $\text{ord}_n(a) = \varphi(n)$, donde φ es la función de Euler.

Teorema 1.31. *Sean G un grupo finito con $|G| = n$ y $a \in G$ con $\text{ord}_G(a) = m$, entonces:*

I. $m \mid n$.

II. $a^k = e$ *si y solo si* $m \mid k$. *En particular,* $a^n = e$.

Ejemplo 1.32. Sean G un grupo y $a \in G$. El conjunto $H = \left\{a^i : i \in \mathbb{Z}\right\}$ de todas las potencias de a es un subgrupo de G, llamado *subgrupo cíclico de G generado por a* y se denota mediante $\langle a \rangle$. Este ejemplo motiva la definición de grupo cíclico.

Definición 1.33. Decimos que un grupo G es cíclico si existe un elemento $a \in G$ tal que $G = \langle a \rangle$. En dicho caso, a se llama un elemento *generador de G*.

Teorema 1.34. *Sea G un grupo cíclico finito con $|G| = n$. Cada subgrupo H de G es cíclico y tiene orden d, donde d es un divisor positivo de n. Recíprocamente, dado un divisor positivo d de n, existe un único subgrupo H de orden d en G.*

Proposición 1.35. $\mathbb{U}_n$ *es cíclico si y solo si* $n \in \{2, 4, p^t, 2p^t\}$, *donde p es un número primo impar y t un entero positivo.*

Definición 1.36. Sean $\langle G_1, * \rangle$ y $\langle G_2, \cdot \rangle$ grupos. Una función $\varphi : G_1 \longrightarrow G_2$ se llama un *homomorfismo* si para cada par de elementos $a, b \in G_1$, se cumple $\varphi(a * b) = \varphi(a) \cdot \varphi(b)$.

Un homomorfismo $\varphi : G_1 \longrightarrow G_2$ que además es biyectivo (inyectivo y sobreyectivo), se dice un *isomorfismo*. En tal caso, G_1 y G_2 son llamados isomorfos, lo cual se denota $G_1 \cong G_2$.

Definición 1.37. Si $G_1, G_2, \ldots, G_n$ son n grupos, entonces su *producto directo* $G_1 \times G_2 \times \cdots \times G_n$ es el conjunto de todas las n-tuplas $(a_1, a_2, \ldots, a_n)$ donde $a_i \in G_i$ para $i = 1, 2, \ldots, n$, y el producto en $G_1 \times G_2 \times \ldots \times G_n$ se define componente a componente.

No es difícil ver que $G = G_1 \times G_2 \times \cdots \times G_n$ con la operación definida componente a componente es un grupo (la Proposición 1.28 puede ser extendida por inducción matemática para n grupos). Un resultado muy valioso que se sigue del *Teorema Chino del Residuo* establece que dada la descomposición canónica del entero $n = p_1^{t_1} p_2^{t_2} \dots p_k^{t_k}$, es posible hallar un isomorfismo entre $\mathbb{Z}_n$ y el producto directo de los $\mathbb{Z}_{p_i^{t_i}}$ para $i = 1, 2, \dots, k$. Particularmente, $\mathbb{U}_n \cong \mathbb{U}_{p_1^{t_1}} \times \mathbb{U}_{p_2^{t_2}} \times \cdots \times \mathbb{U}_{p_k^{t_k}}$.

1.5. Representación de los números por decimales

Teorema 1.38. *Cualquier número positivo puede ser escrito como un decimal, esto es, si* $\zeta > 0$ *escribimos*

$$\zeta = A_1 A_2 \dots A_s . a_1 a_2 a_3 \dots,$$

donde $0 \leqslant A_i, a_j < 10$.

Demostración. Sea $\zeta > 0$ un número positivo. Sean X el mayor entero positivo menor o igual que ζ, es decir, $X = \lfloor \zeta \rfloor$, y $x = \zeta - X$, de tal modo que podemos escribir $\zeta = X + x$, donde $0 \leqslant x < 1$. Consideremos a X y x de forma separada.
Si $X > 0$, del Teorema 1.11 es sabido que podemos escribir a X de forma única mediante

$$X = A_1 10^{s-1} + A_2 10^{s-2} + \cdots + A_{s-1} 10 + A_s,$$

donde $0 \leqslant A_i < 10$ para $i = 1, 2, \dots, s-1$, y el entero s es tal que $10^{s-1} \leqslant X < 10^s$. Entonces $X = A_1 A_2 \dots A_s$.
Ahora para x, escribamos $x = f_1$ y supongamos que $a_1 = \lfloor 10 f_1 \rfloor$, de modo que

$$\frac{a_1}{10} \leqslant f_1 < \frac{a_1 + 1}{10},$$

donde es claro que $0 \leqslant a_1 \leqslant 9$ y además,

$$10f_1 = a_1 + f_2, \text{ con } 0 \leqslant f_2 < 1.$$

De manera análoga, definamos $a_2, a_3, a_4 \ldots$ como

$$\begin{aligned}
a_2 = \lfloor 10f_2 \rfloor,\ 10f_2 = a_2 + f_3,\ \text{con } 0 \leqslant f_3 < 1,\\
a_3 = \lfloor 10f_3 \rfloor,\ 10f_3 = a_3 + f_4,\ \text{con } 0 \leqslant f_4 < 1,\\
a_4 = \lfloor 10f_4 \rfloor,\ 10f_4 = a_4 + f_5,\ \text{con } 0 \leqslant f_5 < 1,\\
\vdots\\
a_n = \lfloor 10f_n \rfloor,\ 10f_n = a_n + f_{n+1},\ \text{con } 0 \leqslant f_{n+1} < 1,\\
\vdots
\end{aligned}$$

Es claro que $0 \leqslant a_n \leqslant 9$, luego

$$x = x_n + g_{n+1}, \tag{1.3}$$

donde

$$a_n = \frac{a_1}{10} + \frac{a_2}{10^2} + \cdots + \frac{a_n}{10^n}$$

y

$$0 \leqslant g_{n+1} = \frac{f_{n+1}}{10^n} < \frac{1}{10^n}.$$

Definamos entonces el decimal $0.a_1a_2a_3 \ldots$ asociado a x. Como $a_n < 10$, la convergencia de la serie

$$\sum_{n=1}^{\infty} \frac{a_n}{10^n}$$

está garantizada y además, como $g_{n+1} \to 0$ cuando $n \to \infty$, la serie de arriba es simplemente x. Entonces $x = 0.a_1a_2a_3 \ldots$ y así concluye la prueba. □

Un decimal que nunca termina puede ser *periódico puro* o *periódico mixto*. Los casos

$$\frac{1}{3} = 0.\overline{3} \quad \text{y} \quad \frac{1}{7} = 0.\overline{142857}$$

son ejemplos de decimales periódicos puros, mientras que

$$\frac{1}{6} = 0.1\overline{6} \quad \text{y} \quad \frac{5}{14} = 0.2\overline{571428}$$

son decimales periódicos mixtos. El *periodo* es la menor secuencia de dígitos que se repite en la representación decimal y se denota con una barra encima como en los ejemplos anteriores. Decimales como

$$\frac{1}{2} = 0.5, \quad \frac{3}{5} = 0.6 \quad \text{y} \quad \frac{3}{8} = 0.375$$

se llaman *decimales exactos*. El uso de la palabra *decimal* viene motivada precisamente por la base $b = 10$ pero no hay razón alguna para no trabajar con otra distinta. Por ejemplo,

$$\begin{aligned}
&\frac{2}{3} = \frac{4}{7} + \frac{4}{7^2} + \frac{4}{7^3} + \cdots = \left[0.\overline{4}\right]_7, \\
&\frac{1}{7} = \frac{1}{11} + \frac{6}{11^2} + \frac{3}{11^3} + \frac{1}{11^4} + \frac{6}{11^5} + \cdots = \left[0.\overline{163}\right]_{11}, \\
&\frac{1}{9} = \frac{0}{3} + \frac{1}{3^2} = [0.01]_3 .
\end{aligned}$$

Cuando la base $b \neq 10$ se hará referencia a los decimales en la escala de b. Los siguientes resultados resumen todo lo que ya hemos dicho.

Teorema 1.39. *Supongamos que b es primo o producto de primos distintos. Cualquier número positivo se puede escribir de forma única como un decimal en la escala de b, es decir, si $\zeta > 0$ entonces*

$$\zeta = A_1 A_2 \ldots A_s . a_1 a_2 a_3 \ldots ,$$

donde $0 \leqslant A_i, a_j < b$ para $i = 1, 2, \ldots, s$ y $j = 1, 2, 3, \ldots$.

Observe que la prueba de este resultado se realiza de manera análoga a cómo se probó el Teorema 1.38, simplemente cambiando a 10 por b.

Teorema 1.40. *Sea $b = p_1 p_2 \cdots p_r$ donde los p_i son todos primos distintos. Supongamos que $0 < x < 1$ y*

$$x = \frac{m}{n}$$

con $\gcd(m, n) = 1$.

- **I.** *Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ y $\alpha = \max\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ entonces el decimal en la escala de b para x es exacto y termina en el $\alpha-$ésimo dígito.*

- **II.** *Si $\gcd(n, b) = 1$ y $v = \mathrm{ord}_n(b)$, entonces el decimal en la escala de b para x es periódico puro con periodo de longitud v.*

- **III.** *Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}\, q$, $q > 1$, $\gcd(q, b) = 1$ y v es el orden de $b \pmod q$ entonces el decimal en la escala de b para x es periódico mixto con α dígitos no periódicos y periodo de longitud v, donde $\alpha = \max\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$.*

Demostración. Vamos a probar el teorema para el caso en que $b = 10 = 2 \times 5$. En general, se procede de forma similar.

I. Supongamos que $n = 2^{\alpha_1} 5^{\alpha_2}$ y $\alpha = \min\{\alpha_1, \alpha_2\}$, entonces

$$x = \frac{m}{n} = \frac{2^{\alpha - \alpha_1} 5^{\alpha - \alpha_2} m}{10^{\alpha}},$$

luego $10^{\alpha} x$ es un entero y α es el menor exponente para el cual esto es cierto. De ahí que si $x = 0.a_1 a_2 \ldots$ entonces x termina en el dígito a_{α}.

II. Sea $v = \mathrm{ord}_n(10)$, entonces $10^v = tn + 1$ para algún entero t, luego

$$10^v x = \frac{10^v m}{n} = \frac{(tn+1)m}{n} = tm + \frac{m}{n} = tm + x.$$

Puesto que de la expresión (1.3) tenemos que

$$10^v x = 10^v x_v + 10^v g_{v+1} = 10^v x_v + f_{v+1}$$

y $0 < x < 1$, se sigue que $f_{v+1} = x$. Así, el proceso mediante el cual fue construido el decimal de x se repite desde f_{v+1} en adelante. De esto que x es un decimal periódico puro con periodo de longitud v.

III. Supongamos que $n = 2^{\alpha_1}5^{\alpha_2}q$, con $q > 1$ un entero primo relativo con 10. Sean α como en el inciso **I** y $v = \mathrm{ord}_q(10)$, entonces

$$10^{\alpha}x = \frac{2^{\alpha-\alpha_1}5^{\alpha-\alpha_2}m}{q} = X + \frac{M}{q},$$

donde X, M son enteros que satisfacen $0 \leqslant X < 10^{\alpha}$, $0 < M < q$ y $\gcd(M, q) = 1$. Si $X > 0$, existe un entero $s < \alpha$ tal que $10^{s-1} \leqslant X < 10^{s}$, de modo que $X = A_1A_2 \ldots A_s$. Por el ítem **II**, el decimal para la fracción M/q es periódico con periodo de longitud v, luego

$$10^{\alpha}x = A_1A_2 \ldots A_s.\overline{a_1a_2 \ldots a_v},$$

de donde se obtiene que

$$x = 0.b_1b_2 \ldots b_{\alpha}\overline{a_1a_2 \ldots a_v},$$

donde los s últimos b_i son $A_1, A_2, \ldots, A_s$ y los demás, si los hay, son 0. □

Teorema 1.41. *Supongamos que b es primo o producto de primos distintos. Si q es primo y b es una raíz primitiva módulo q entonces los decimales en la escala de b para*

$$\frac{x}{q}, \text{ donde } x = 1, 2, \ldots, q-1$$

tienen periodo de longitud $q - 1$ y difieren entre ellos únicamente por una permutación cíclica.

Ejemplo 1.42. El $\mathrm{ord}_7(10) = 6$, de modo que 10 es una raíz primitiva módulo 7. Sabemos que $1/7 = 0.\overline{142857}$, entonces el Teorema 1.41 dice que para $x = 2, 3, 4, 5, 6$, las fracciones $x/7$ son, en algún orden,

$$0.\overline{428571}, \quad 0.\overline{285714}, \quad 0.\overline{857142}, \quad 0.\overline{571428} \text{ y } 0.\overline{714285}.$$

Efectivamente, puede verificarse rápidamente que en este orden, las fracciones vienen siendo 3/7, 2/7, 6/7, 4/7 y 5/7, respectivamente.

Capítulo 2

Una prueba para el teorema de Midy

En este capítulo vamos a estudiar la primera generalización del Teorema de Midy; si la longitud del periodo de la fracción $1/p$ con p un número primo es $e = dk$, la suma de los d bloques de k dígitos que conforman el periodo es un múltiplo de $10^k - 1$. Además, la suma de los elementos del único subgrupo de orden d en $\mathbb{U}_p$ nos proporciona el valor r para el cual dicha suma es $r(10^k - 1)$.

Del Teorema 1.40 es sabido que la fracción $1/p$ es periódica y su periodo tiene longitud $e = \text{ord}_p(10)$. Un resultado más general que involucra este hecho, se dará en el Capítulo 3, al iniciar la Sección 3.2. Para empezar, vamos a probar que la suma de los elementos de un subgrupo no trivial en $\mathbb{U}_p$ es un múltiplo de p.

Lema 2.1. *Sean $p > 2$ un primo y G un subgrupo no trivial de $\mathbb{U}_p$. Entonces la suma de los elementos de G es un múltiplo de p.*

Demostración. Dado que $\mathbb{U}_p$ es un grupo finito de orden $p - 1$, podemos escribir que $G = \{g_1, g_2, \ldots, g_m\}$ con $m \leqslant p - 1$. Sea $a \in G$ con $a \neq 1$ y considere el conjunto

$$aG = \{ag_i : i = 1, 2, \ldots, m\}.$$

No es difícil ver que aG es subgrupo de $\mathbb{U}_p$ y es de hecho el mismo G. En efecto, si tomamos $ag_i \in aG$, entonces $ag_i \in G$ puesto que a y g_i están ambos en G. Además, $ag_i \neq ag_j$ para $i \neq j$, pues de lo contrario, por la ley cancelativa en G, se llegaría a que $g_i = g_j$. Por lo tanto,

$$a\sum_{i=1}^{m} g_i \equiv \sum_{i=1}^{m} g_i \text{ (mód } p),$$

de donde obtenemos

$$(a-1)\sum_{i=1}^{m} g_i \equiv 0 \text{ (mód } p)$$

y como $a \neq 1$, $a-1 \not\equiv 0$ (mód p). De ahí que $\sum_{i=1}^{m} g_i \equiv 0$ (mód p), o lo que es lo mismo, $\sum_{i=1}^{m} g_i = rp$ para algún $r \in \mathbb{Z}$. □

Si consideramos un primo p y $d > 1$ un divisor de $p-1$, existe un único subgrupo de orden d en $\mathbb{U}_p$ que notaremos por $\mathbb{U}(p,d)$. Del resultado anterior es claro que $\sum_{g\in\mathbb{U}(p,d)} g = rp$ para algún $r \in \mathbb{Z}$. Llamaremos a esta suma $s(p,d)$.

Teorema 2.2. *Sea $p > 5$ un número primo y supongamos que $\text{ord}_p(10) = dk$, con $d > 1$. Si escribimos*

$$\frac{1}{p} = 0.(A_1A_2\cdots A_d)(A_1A_2\cdots A_d)\cdots$$

donde cada A_j consiste de k dígitos, entonces

$$A_1 + A_2 + \cdots + A_d = r(10^k - 1),$$

donde $s(p,d) = rp$.

Note que $e = dk \mid p-1$, por lo cual se sigue que $d \mid p-1$ y así tiene sentido hablar de $s(p,d)$ en el teorema.

Antes de dar inicio a la prueba, sea a/b con $a, b \in \mathbb{Z}$ y $b \neq 0$ un número racional. Definimos la *parte fraccionaria de a/b*, que denotaremos por $\{a/b\}$, como

$$\left\{\frac{a}{b}\right\} := \frac{a}{b} - \left\lfloor\frac{a}{b}\right\rfloor,$$

donde $\lfloor a/b \rfloor$ denota la función parte entera del número a/b. Es inmediato de esta definición que $\{n\} = 0$ para cualquier $n \in \mathbb{Z}^+$ y por lo tanto

$$\left\{ n + \frac{a}{b} \right\} = \left\{ \frac{a}{b} \right\}.$$

Además, por el algoritmo de la división

$$\left\{ \frac{a}{b} \right\} = \frac{r}{b}, \tag{2.1}$$

donde $a \equiv r \pmod{p}$, $0 \leqslant r < b$.

Demostración. Como $\mathrm{ord}_p(10) = dk$, podemos escribir el conjunto $\mathbb{U}(p, d)$ como

$$\mathbb{U}(p, d) = \left\{ 10^{ik} \pmod{p} : 0 \leqslant i \leqslant d - 1 \right\}.$$

Sea $a_i \in \mathbb{U}(p, d)$ el elemento correspondiente a $10^{ik} \pmod{p}$ con $1 \leqslant a_i \leqslant p-1$, es decir, $10^{ik} \equiv a_i \pmod{p}$. De ahí, haciendo uso de (2.1), que

$$\left\{ \frac{10^{ik}}{p} \right\} = \frac{a_i}{p},$$

por lo cual

$$\sum_{i=0}^{d-1} \frac{a_i}{p} = \frac{s(p, d)}{p} = r. \tag{2.2}$$

Ahora bien, observemos que como cada bloque A_j contiene k dígitos, al multiplicar la fracción $1/p$ por 10^{jk} se estarán moviendo los bloques $A_1, A_2, \ldots, A_j$ a la izquierda del punto decimal con respecto a $1/p$, como se muestra a continuación:

$$\begin{aligned}
\frac{1}{p} &= 0.(A_1 A_2 \cdots A_d)(A_1 A_2 \cdots A_d) \cdots \\
\frac{10^k}{p} &= A_1.(A_2 A_3 \cdots A_d A_1)(A_2 A_3 \cdots A_d A_1) \cdots \\
\frac{10^{2k}}{p} &= A_1 A_2.(A_3 A_4 \cdots A_1 A_2)(A_3 A_4 \cdots A_1 A_2) \cdots
\end{aligned}$$

$$\vdots$$

$$\frac{10^{(d-1)k}}{p} = A_1A_2\cdots A_{d-1}.(A_dA_1\cdots A_{d-1})(A_dA_1\cdots A_{d-1})\cdots$$

Al hacer una inspección detallada se puede determinar que después del punto decimal las expresiones del lado derecho de las igualdades de arriba son la parte fraccionaria de $10^{ik}/p$ para $0 \leqslant i \leqslant d-1$, cuya suma está dada en (2.2). Veamos también que la siguiente igualdad es cierta:

$$\sum_{i=0}^{d-1}\left\{\frac{10^{ik}}{p}\right\} = \frac{A_1 + A_2 + \cdots + A_d}{10^k - 1}. \tag{2.3}$$

Puesto que para cada $0 \leqslant i \leqslant d-1$, usando el convenio $A_0 = A_d$, tenemos que

$$\left\{\frac{10^{ik}}{p}\right\} = \left(\frac{A_{i+1}}{10^k} + \frac{A_{i+2}}{10^{2k}} + \cdots + \frac{A_d}{10^{(d-i)k}} + \cdots + \frac{A_i}{10^{dk}}\right)\sum_{j=0}^{\infty}\left(\frac{1}{10^e}\right)^j,$$

y la serie del lado derecho de la igualdad tiene radio $r = 1/10^e < 1$, por lo tanto se garantiza su convergencia, a saber,

$$\sum_{j=0}^{\infty}\left(\frac{1}{10^e}\right)^j = \frac{10^{dk}}{10^{dk}-1},$$

podemos escribir que

$$\left\{\frac{10^{ik}}{p}\right\} = \frac{M_i}{10^{dk}-1}, \text{ donde } M_i = \sum_{j=1}^{d} A_{l_j}10^{(d-j)k} \text{ y } l_j \equiv j + i \,(\text{mód } d).$$

Si agrupamos convenientemente podemos ver que

$$\sum_{i=1}^{d}\left\{\frac{10^{ik}}{p}\right\} = \sum_{i=0}^{d-1}\sum_{j=1}^{d}\frac{A_j10^{ik}}{10^{dk}-1},$$

y dado que la suma finita

$$\sum_{i=0}^{d-1} 10^{ik} = \frac{10^{dk}-1}{10^k-1},$$

resulta inmediatamente la expresión (2.3) que al igualarla con (2.2) nos permite concluir que

$$A_1 + A_2 + \cdots + A_d = r(10^k - 1).$$

□

Veamos un caso ilustrativo de este teorema.

Ejemplo 2.3. Consideremos el primo $p = 19$, entonces la longitud del periodo de $1/19$ es $e = \text{ord}_{19}(10) = 18 = 2 \cdot 3^2$. Hagamos una inspección detallada de los posibles valores que puede tomar $d > 1$, o sea, todas las posibles particiones del periodo. Recordemos que en la prueba del teorema se indica la forma de construir el subgrupo $\mathbb{U}(p, d)$.
Caso $d = 2$: Tenemos que $k = 9$ y es evidente que $\mathbb{U}(19, 2) = \{1, 18\}$, por lo cual $s(19, 2) = 19$. Luego $r = 1$ y la suma de los $d = 2$ bloques de $k = 9$ dígitos que conforman el periodo es

$$10^9 - 1 = 999999999.$$

Caso $d = 3$: Tenemos que $k = 6$, por lo tanto:

$$10^0 \equiv 1 \text{ (mód 19)},$$
$$10^6 \equiv 11 \text{ (mód 19)},$$
$$10^{12} \equiv 7 \text{ (mód 19)}.$$

De ahí que $\mathbb{U}(19, 3) = \{1, 7, 11\}$ y $s(19, 3) = 19$. Luego $r = 1$ y la suma de los $d = 3$ bloques de $k = 6$ dígitos que conforman el periodo es

$$10^6 - 1 = 999999.$$

Caso $d = 6$: Tenemos que $k = 3$, por lo tanto:

$$10^0 \equiv 1 \text{ (mód 19)},$$
$$10^3 \equiv 12 \text{ (mód 19)},$$
$$10^6 \equiv 11 \text{ (mód 19)},$$
$$10^9 \equiv 18 \text{ (mód 19)},$$
$$10^{12} \equiv 7 \text{ (mód 19)},$$
$$10^{15} \equiv 8 \text{ (mód 19)}.$$

De ahí que $\mathbb{U}(19, 6) = \{1, 7, 8, 11, 12, 18\}$ y $s(19, 6) = 57 = 3 \cdot 19$. Luego $r = 3$ y la suma de los $d = 3$ bloques de $k = 6$ dígitos que conforman el periodo es

$$3(10^3 - 1) = 2997.$$

Caso $d = 9$: Tenemos que $k = 2$, por lo tanto:

$$10^0 \equiv 1 \text{ (mód 19)},$$
$$10^2 \equiv 5 \text{ (mód 19)},$$
$$10^4 \equiv 6 \text{ (mód 19)},$$
$$10^6 \equiv 11 \text{ (mód 19)},$$
$$10^8 \equiv 17 \text{ (mód 19)},$$
$$10^{10} \equiv 9 \text{ (mód 19)},$$
$$10^{12} \equiv 7 \text{ (mód 19)},$$
$$10^{14} \equiv 16 \text{ (mód 19)},$$
$$10^{16} \equiv 4 \text{ (mód 19)}.$$

De ahí que $\mathbb{U}(19, 6) = \{1, 4, 5, 6, 7, 9, 11, 17, 16\}$ y $s(19, 6) = 76 = 4 \cdot 19$. Luego $r = 4$ y

la suma de los $d = 9$ bloques de $k = 2$ dígitos que conforman el periodo es

$$4(10^2 - 1) = 396.$$

Caso $d = 18$: Tenemos que $k = 1$ y evidentemente $\mathbb{U}(19, 18) = \mathbb{U}_{19}$, por lo cual $s(19, 18) = 171 = 9 \cdot 19$. Luego $r = 9$ y la suma de los $d = 18$ bloques de $k = 1$ dígito que conforman el periodo es

$$9(10 - 1) = 81.$$

Si nos fijamos bien en el ejemplo anterior cuando $d = 2$ y $d = 3$, $s(19, d) = 19$. Esto no es de sorprender puesto que se trata del Teorema de Midy y el Teorema de Ginsberg, que surgen como consecuencia inmediata del Teorema 2.2.

Corolario 2.4. *Bajo las mismas hipótesis del Teorema 2.2 se tiene que* $s(p, 2) = s(p, 3) = p$. *En particular, el teorema de Midy y el teorema de Ginsberg se satisfacen.*

Demostración. Observe que $\mathbb{U}(p, 2) = \{1, p - 1\}$ y $\mathbb{U}(p, 3) = \{1, x, y\}$, con $x, y < p - 1$. Como $1 + x + y \equiv 0 \pmod{p}$ y es menor que $1 + 2(p - 1)$, se sigue que $1 + x + y = p$. □

El Teorema 2.2 resulta ser de gran importancia pues transforma el problema inicial de la suma de los bloques que conforman el periodo de la fracción $1/p$, a la suma de los elementos del único subgrupo de orden d en $\mathbb{U}_p$. El cálculo de $s(p, d)$ es equivalente al cálculo de la suma $A_1 + A_2 + \cdots + A_d$ y en estos momentos nuestro mayor interés es saber bajo qué condiciones tenemos que $s(p, d) = p$, para así no salirnos del contexto original del problema de Midy. Veremos a continuación lo que ocurre cuando trabajamos con los *primos de Mersenne* y con los *primos de Sophie Germain*.

Definición 2.5. Sea p un número primo.

I. Decimos que p es un *primo de Mersenne* si $p = 2^n - 1$, donde n es también un primo.

II. Decimos que p es un *primo de Sophie Germain* si $n = 2p+1$ es también un primo.

Una conjetura abierta establece que existen infinitos números primos de Mersenne. Verificar si $p = 2^n - 1$ es primo dado que n es primo no es una tarea fácil, incluso usando herramientas computacionales modernas. A la fecha solo han sido descubiertos 48 de estos números. Los cuatro primeros primos de Mersenne son fáciles de hallar: $3 = 2^2 - 1$, $7 = 2^3 - 1$, $31 = 2^5 - 1$ y $127 = 2^7 - 1$. Actualmente, el número primo más grande conocido es de Mersenne, $2^{57885161} - 1$, descubierto en 2013 por el Dr. Curtis Cooper de la University of Central Missouri bajo la contribución de la *Great Internet Mersenne Prime Search*[1], GIMPS, con un total de 17425170 cifras.

Ejemplo 2.6. Vamos a estudiar el comportamiento de $s(p, d)$, donde $p = 2^d - 1$ es un número primo de Mersenne. En la siguiente tabla dejaremos los detalles para verificar lo que sucede con los primeros tres primos mayores que 3.

Primos de Mersenne	$\text{ord}_p(10)$	d	k
7	6	3	2
31	15	5	3
127	42	7	6

Tabla 1. Estudio de los primos de Mersenne.

En el primer caso, $7 = 2^3 - 1$, de modo que $e = 3k$ y por lo tanto $s(7, 3) = 7$ en virtud del Teorema de Ginsberg (Corolario 2.4). Para $p = 31$ tenemos que $\mathbb{U}(31, 5) = \{1, 2, 4, 8, 16\}$, por lo que $s(31, 5) = 1 + 2 + 4 + 8 + 16 = 31$. Finalmente en el caso $p = 127$, $\mathbb{U}(127, 7) = \{1, 2, 4, 8, 16, 32, 64\}$, donde obtenemos que $s(127, 7) = 1+2+4+8+16+32+64 = 127$. Estos resultados nos llevan a preguntarnos si $s(p, d) = p$ siempre que $p = 2^d - 1$ es un primo de Mersenne. La forma en cómo resulta el subgrupo $\mathbb{U}(p, d)$ es precisamente la clave para que esta respuesta sea afirmativa.

[1] http://www.mersenne.org/primes/

Proposición 2.7. *Si $p = 2^d - 1$ es un primo de Mersenne, entonces $s(p, d) = p$.*

Demostración. Puesto que $2^d - 1 \equiv 0 \,(\text{mód } p)$, entonces $\text{ord}_p(2) = d$, por lo tanto $d \mid p - 1$ y $\mathbb{U}(p, d) = \left\{1, 2, 2^2, \ldots, 2^{d-1}\right\}$, luego

$$s(p, d) = \sum_{k=0}^{d-1} 2^k = 2^d - 1 = p.$$

□

Sophie Germain fue una matemática francesa que se hizo famosa a princicios del siglo XIX al permitir avances sobre la posible prueba del *Último Teorema de Fermat*[2] usando precisamente los primos p para los cuales $n = 2p+1$ también lo son. Al igual que con los primos de Mersenne, se ha conjeturado que existen infinitos primos de Sophie Germain y hasta ahora no se ha logrado probar. La razón por la cual nos interesamos en esta clase de primos nos la brinda el siguiente enunciado.

Proposición 2.8. *Si $d > 3$ es un primo de Sophie Germain tal que $p = 2d+1$ también es primo, entonces $s(p, d) > p$.*

Demostración. Como $\mathbb{U}(p, d)$ tiene evidentemente d elementos, es inmediato que si $d > 5$,

$$s(p, d) \geqslant 1 + 2 + 3 + \cdots + (d - 1) = \frac{d(d-1)}{2} = \frac{d^2 - d}{2}.$$

Como $d^2 - d > 4d + 2$ para todo $d > 5$, se sigue que $s(p, d) > p$. Para el caso $d = 5$, $p = 11$ y $\mathbb{U}(11, 5) = \{1, 3, 4, 5, 9\}$, por lo que $s(11, 5) = 22 > 11$. □

Ejemplo 2.9. El primo $d = 11$ es de Sophie Germain pues $p = 23$ es primo. Observe que $\mathbb{U}(23, 11) = \langle 3 \rangle = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$, entonces $s(23, 11) = 4 \cdot 23 = 92$.

[2]Este enunciado establece que no es posible encontrar para ningún natural $n > 2$ soluciones enteras x, y, z no triviales a la ecuación

$$x^n + y^n = z^n.$$

Capítulo 3

Generalizaciones del teorema de Midy

Con el propósito de generalizar el Teorema de Midy cuando se trabaja en una base numérica $B > 1$ cualquiera, debemos introducir una notación apropiada.
Sean $B > 1$ y n enteros positivos tales que $\gcd(n, B) = 1$. Si $e = \mathrm{ord}_n(B) = dk$, con $d, k \in \mathbb{Z}$ y $d > 1$, es la longitud del periodo de x/n, para $x \in \mathbb{U}_n$, entonces

$$\frac{x}{n} = [0.\overline{a_1 a_2 \cdots a_e}]_B,$$

donde los a_i son B-dígitos y el periodo $a_1 a_2 \cdots a_e$ se puede dividir en d sub-bloques cada uno con k dígitos. Sea A_j la representación numérica en la base B del j-ésimo sub-bloque de k B-dígitos del periodo y sea $S_d(x)$ la suma (en base B)

$$S_d(x) \coloneqq \sum_{j=1}^{d} A_j.$$

Definición 3.1. Con la notación anterior, si para cada $x \in \mathbb{U}_n$ la suma $S_d(x)$ es un múltiplo de $B^k - 1$, o lo que es lo mismo, $S_d(x) \equiv 0 \,(\mathrm{mód}\ B^k - 1)$, diremos que n tiene la propiedad de Midy para la base B y el divisor d de e. En tal caso, escribimos $n \in M_d(B)$.

Observación. En la definición anterior estamos asumiendo que los resultados referentes a la expansión en la escala de B de la fracción x/n son como se ilustran. Para sustentar este hecho, habrá que esperar hasta el inicio de la Sección 3.2, donde mostraremos un resultado que esclarecerá cualquier tipo de duda.

Ejemplo 3.2. Veamos que $7 \in M_2(5)$. Como 5 es un raíz primitiva módulo 7 se sigue que $e = 6 = 2 \cdot 3$. Para empezar,

$$\frac{1}{7} = [0.\overline{032412}]_5,$$

de modo que por el Teorema 1.41 las demás fracciones $x/7$ para $x = 2, 3, 4, 5, 6$ son en algún orden

$$[0.\overline{324120}]_5, [0.\overline{241203}]_5, [0.\overline{412032}]_5, [0.\overline{120324}]_5, [0.\overline{203241}]_5.$$

Para $1/7$, tenemos que $A_1 = [032]_5$, $A_2 = [412]_5$ y $5^3 - 1 = [444]_5$, de donde

$$S_2(1) = [032]_5 + [412]_5 = [444]_5 \equiv 0 \,(\text{mód } [444]_5).$$

Puesto que las demás fracciones difieren en su periodo con el de $1/7$ por permutaciones cíclicas, se sigue que $S_2(x) = S_2(1) \equiv 0 \,(\text{mód } [444]_5)$ para $x = 2, 3, 4, 5, 6$, luego $7 \in M_2(5)$.

Ahora, consideremos $D_B(n)$ la secuencia más corta de B-dígitos que se repiten en la expansión decimal en la escala de B de $1/n$, es decir, el periodo. Por ejemplo, $D_{10}(7) = 142857$ y $D_5(7) = 032412$. Si escribimos $1/n = 0.\overline{D_B(n)}$, suponiendo que $e = \text{ord}_n(B)$,

$$\frac{B^e - 1}{n} = D_B(n).\overline{D_B(n)} - \frac{1}{n},$$

de donde obtenemos la igualdad

$$n \cdot D_B(n) = B^e - 1. \tag{3.1}$$

Si $e = dk$, definamos $N_B(k, d)$ por

$$N_B(k, d) \coloneqq \frac{B^e - 1}{B^k - 1}, \tag{3.2}$$

de modo que al combinar las igualdades (3.1) y (3.2) obtenemos la relación

$$(B^k - 1) \cdot N_B(k, d) = n \cdot D_B(n). \tag{3.3}$$

Observación. Para el desarrollo de toda esta teoría hemos asumido que $d > 1$ y no argumentamos el motivo de esta aserción. La razón es muy simple. Supongamos que $e = \mathrm{ord}_n(B) = dk$ con $d = 1$, entonces el único bloque de $k = e$ B-dígitos en la expansión decimal de $1/n$ es $D_B(n)$. Puesto que $n \in M_1(B)$ si y solo si $S_1(x) \equiv 0 \pmod{B^e - 1}$ para cada $x \in \mathbb{U}_n$, resulta claro que $D_B(n) < B^e - 1$, de modo que $B^e - 1 \nmid S_1(1)$ y así $n \notin M_1 B$). De ahí concluimos que $M_d(B) = \emptyset$ siempre que $d = 1$.

3.1. El teorema de Midy en base 10

En esta sección estaremos interesados en estudiar bajo las condiciones de la Definición 3.1, los casos $B = 10$ y $e = 2k$, con el fin de caracterizar completamente los números que cumplen la propiedad de Midy en su estado puro. Para ello, puesto que trabajaremos con fracciones $1/n$, abusaremos un poco con la notación ya introducida y asumiremos que $n \in M_d(10)$ si y solo si $S_d(1) \equiv 0 \pmod{10^k - 1}$. Ya veremos en la Sección 3.2 que este abuso es intencional.

Puesto que $B = 10$ a lo largo de esta sección, omitiremos hacer uso de la letra B en las notaciones y definiciones ya introducidas. Por ejemplo, escribiremos $n \in M_d$ en lugar de $n \in M_d(10)$. Además, $D(n)$ es $D_{10}(n)$, por lo cual

$$n \cdot D(n) = 10^e - 1, \tag{3.4}$$

donde $e = \mathrm{ord}_n(10) = dk$, así $N_{10}(k,d)$ lo escribimos

$$N(k,d) = \frac{10^e - 1}{10^k - 1}, \tag{3.5}$$

y la relación (3.3) resulta ser

$$(10^k - 1) \cdot N(k,d) = n \cdot D(n). \tag{3.6}$$

Esta última expresión contiene demasiada información de la propiedad de Midy.

Lema 3.3. *Sean n un entero positivo primo relativo con 10 y $e = dk$. Entonces $10^k - 1 \mid D(n)$ si y solo si $10^k - 1 \mid S_d(1)$.*

Demostración. Dado que $D(n) = A_1 A_2 \ldots A_d$, podemos escribirlo de la forma

$$D(n) = \sum_{j=1}^{d} A_j 10^{e-jk}.$$

De este modo se sigue que

$$\begin{aligned} D(n) &= S_d(1) + \sum_{j=1}^{d} A_j (10^{e-jk} - 1) \\ &= S_d(1) + \sum_{j=1}^{d-1} A_j (10^k - 1) \left(1 + 10^k + 10^{2k} + \cdots + 10^{(d-j-1)k}\right) \\ &= S_d(1) + (10^k - 1) \sum_{j=1}^{d-1} A_j \left(1 + 10^k + 10^{2k} + \cdots + 10^{(d-j-1)k}\right) \end{aligned}$$

De ahí es inmediato ver que $10^k - 1 \mid D(n)$ si y solo si $10^k - 1 \mid S_d(1)$. □

Teorema 3.4. *Sea n un entero positivo con $\gcd(n, 10) = 1$ y $e = dk$, entonces $n \in M_d$ si y solo si $n \mid N(k,d)$.*

Demostración. Supongamos que $n \in M_d$, entonces $10^k - 1 \mid S_d(1)$. Por el lema anterior, $10^k - 1 \mid D(n)$, así que en virtud de (3.6) se sigue que $n \mid N(k,d)$. Recíprocamente,

supongamos que $n \mid N(k,d)$. Nuevamente por la ecuación (3.6), $10^k - 1 \mid D(n)$, pero esto implica que $10^k - 1 \mid S_d(1)$ por el lema precedente, luego $n \in M_d$ lo que completa la prueba. □

Teorema 3.5. *Sea n un entero positivo con $\gcd(n,10) = 1$ y $e = dk$. Si $\gcd(n, 10^k - 1) = 1$ entonces $n \in M_d$.*

Demostración. Puesto que de (3.6) se tiene que $(10^k - 1) \cdot N(k,d) = n \cdot D(n)$, si $\gcd(n, 10^k - 1) = 1$ debe ocurrir que $n \mid N(k,d)$ y así por el teorema anterior, $n \in M_d$. □

El Teorema 3.5 da una condición suficiente, pero no necesaria, para que $n \in M_d$. A continuación mostramos un ejemplo de ello.

Ejemplo 3.6. Sea $n = 21$, entonces $1/21 = 0.\overline{047619}$ y $e = 6$. Con $d = 3$ y $k = 2$, $S_3(1) = 99 \equiv 0 \pmod{10^2 - 1}$, luego $21 \in M_2$ pero $\gcd(21, 10^2 - 1) = 3$.

Ejemplo 3.7. Cuando $n = 13$, la fracción $1/13 = 0.\overline{076923}$ tiene período de longitud 6. En cualquiera de los casos en que $k = 1, 2, 3$, se verifica que $\gcd(13, 10^k - 1) = 1$, luego $13 \in M_6$, $13 \in M_3$ y $13 \in M_2$. Particularmente, tenemos las relaciones

$$\begin{aligned} S_6(1) &= 7 + 6 + 9 + 2 + 3 = 27 = 3(10^1 - 1), \\ S_3(1) &= 7 + 69 + 23 = 99 = 10^2 - 1, \\ S_2(1) &= 76 + 923 = 999 = 10^3 - 1. \end{aligned}$$

Ejemplo 3.8. Si tomamos ahora $n = 49$, la fracción

$$\frac{1}{49} = 0.\overline{020408163265306122448979591836734693877551}$$

tiene período de longitud $42 = 2 \cdot 3 \cdot 7$. Podemos entonces considerar siete casos distintos para valores de k, donde $42 = dk$ y verificar para cuáles de ellos se satisfacen las condiciones del teorema anterior. En la Tabla 2 se resumen estos resultados.

k	d	$\gcd(10^k - 1, 49)$	$S_d(1)$
1	42	1	$21(10^1 - 1)$
2	21	1	$10(10^2 - 1)$
3	14	1	$7(10^3 - 1)$
6	7	7	No aplica
7	6	1	$3(10^7 - 1)$
14	3	1	$10^{14} - 1$
21	2	1	$10^{21} - 1$

Tabla 2. Verificación del Teorema 3.5 para $n = 49$.

Cuando $k = 6$, $\gcd(10^6 - 1, 49) = 7 \neq 1$ y por lo tanto el Teorema 3.5 no verifica si $49 \in M_7$. Sin embargo, si hacemos una verificación rápida podemos ver que $S_7(1) = 3142854 \equiv 142857 \pmod{10^6 - 1}$, es decir, la suma de los 7 sub-bloques de 6 dígitos que conforman el período no resulta ser un múltiplo de $10^6 - 1$. De ahí que $49 \notin M_7$.

Una pregunta que podría surgir es si existe relación alguna entre los divisores primos p de n y $\mathrm{ord}_p(10)$ para que el teorema anterior siga teniendo la misma conclusión. La respuesta es afirmativa y nos la proporciona el siguiente resultado.

Teorema 3.9. *Sea n un entero positivo con $\gcd(n, 10) = 1$ y $e = dk$. Si para cada factor primo p de n el entero k no es múltiplo de $\mathrm{ord}_p(10)$, entonces $n \in M_d$.*

Demostración. Sea $t = \mathrm{ord}_p(10)$ y supongamos que para cada factor primo p de n el entero k no es un múltiplo de t, es decir, $t \nmid k$, de donde $10^k \not\equiv 1 \pmod{p}$, por lo cual $\gcd(p, 10^k - 1) = 1$. Ahora, como $n \mid 10^e - 1$ (ver ecuación (3.4)), también $p \mid 10^e - 1$ y de la igualdad (3.5) se sigue que $p \mid N(k, d)$, por ser p y $10^k - 1$ primos relativos. Sea α la multiplicidad del primo p como factor de n, entonces es claro que $\gcd(p^\alpha, 10^k - 1) = 1$ y el mismo argumento que acabamos de usar para mostrar que p es un divisor de $N(k, d)$ también prueba que $p^\alpha \mid N(k, d)$. Como esta última afirmación es válida para cada divisor primo p de n, se sigue que $n \mid N(k, d)$ y así $n \in M_d$ como consecuencia del Teorema 3.4. □

Note que la Tabla 2 se hubiese podido estudiar de igual forma haciendo uso del teorema anterior y solamente fallaría en el mismo caso en que el Teorema 3.5 falló cuando $k = 6$, pues el único factor primo de 49 es 7 y $\text{ord}_7(10) = 6$.

Ejemplo 3.10. Sea $n = 217 = 7 \cdot 31$. Tenemos que $\text{ord}_7(10) = 6$, $\text{ord}_{31}(10) = 15$ y $\text{ord}_{217}(10) = 30$, particularmente esta última afirmación se puede verificar rápidamente escribiendo

$$\frac{1}{217} = 0.\overline{004608294930875576036866359447}.$$

En la Tabla 3 mostramos cuándo la suma de los k sub-bloques con d dígitos que conforman el periodo de $1/217$, donde $30 = kd$, es múltiplo de $10^k - 1$ haciendo uso del Teorema 3.9. Cuando k no es un múltiplo de 6 ni de 15 la respuesta es afirmativa.

k	d	Múltiplo de $10^k - 1$
1	30	Sí
2	15	Sí
3	10	Sí
5	6	Sí
6	5	No aplica
10	3	Sí
15	2	No aplica

Tabla 3. Uso del Teorema 3.9 para $n = 217$.

No sabemos si $217 \in M_5$ y tampoco si $217 \in M_2$, sin embargo, podemos hacer los cálculos numéricos de $S_6(1)$ y $S_2(1)$ para saber lo que ocurre:

$$S_2(1) = 004608294930875 + 576036866359447 \equiv 580645161290322 \,(\text{mód } 10^{15} - 1),$$
$$S_5(1) = 004608 + 294930 + 875576 + 036866 + 359447 \equiv 571428 \,(\text{mód } 10^6 - 1).$$

De esto tenemos que $217 \notin M_2$ y $217 \notin M_5$.

En lo restante de esta sección vamos a enfocar nuestro interés en el estudio de la propiedad de Midy cuando la longitud del periodo de $1/n$ es par, es decir, $e = 2k$ para algún entero k. Comenzamos enunciado la siguiente caracterización.

Teorema 3.11 (Schlömilch)**.** *Sea n un entero positivo con* $\gcd(n, 10) = 1$ *y $e = 2k$. Entonces $n \in M_2$ si y solo si existe algún $j \in \mathbb{Z}^+$ tal que $n \mid 10^j + 1$.*

Demostración. Supongamos que $n \in M_2$, entonces del Teorema 3.4, $n \mid N(k, 2) = 10^k + 1$. Recíprocamente, supongamos que existe $j \in \mathbb{Z}^+$ tal que $n \mid 10^j + 1$. Es claro que $n \mid 10^{2j} - 1$, por lo que $e \mid 2j$ y de ahí que $k \mid j$. Ahora bien, para cada factor primo p de n, $p \mid 10^j + 1$ luego $p \nmid 10^j - 1$, de donde $\gcd(p, 10^j - 1) = 1$ y por lo tanto $\gcd(n, 10^j - 1) = 1$. Dado que $10^k - 1 \mid 10^j - 1$, se sigue que $\gcd(n, 10^k - 1) = 1$ y por el Teorema 3.5, $n \in M_2$. □

El Teorema 3.11 se limita a ser un test para ver si determinado número $n \in M_2$. No obstante, desarrolla un papel muy importante al momento de dar otra caracterización de la propiedad de Midy cuando la longitud del periodo de $1/n$ es par. Antes de eso, veamos que si n es cualquier número que tiene la propiedad de Midy, entonces cada potencia de n también tiene la propiedad.

Teorema 3.12. *Si $n \in M_2$ entonces $n^h \in M_2$ para todo $h \in \mathbb{Z}^+$.*

Demostración. Sea $e = 2k$, entonces $n \mid N(k, 2) = 10^k + 1$. Observe que para cualquier entero positivo impar j, $10^k + 1 \mid 10^{jk} + 1$. En efecto,

$$10^{jk} + 1 = E(j) \cdot (10^k + 1), \tag{3.7}$$

donde $E(j) = 10^{(j-1)k} - 10^{(j-2)k} + \cdots - 10^k + 1$. Además,

$$E(j) = Q(j) \cdot (10^k + 1) + j, \tag{3.8}$$

donde $Q(j) = \sum_{i=0}^{j-2} (-1)^i \, (i + 1) \, y^{j-2-i}$. Escojamos $j = 10^k + 1$ en la ecuación (3.8) de manera conveniente, entonces $10^k + 1 \mid E(j)$. Por la ecuación (3.7), $(10^k + 1)^2 \mid 10^t + 1$,

donde $t = k\cdot(10^k+1)$, así que por transitividad se sigue que como $n \mid 10^k+1$, $n^2 \mid 10^t+1$. De ahí que $n^2 \in M_2$ por el Teorema 3.11.

Como $n^2 \in M_2$, podemos aplicar el mismo procedimiento para probar que $n^4 \in M_2$ y en general, $n^q \in M_2$ para cualquiera que sea q una potencia de 2. Ahora bien, sea h un entero positivo. Existe una potencia de 2, digamos $u \in \mathbb{Z}$ tal que $h \leqslant u$. Como $n^u \mid 10^v + 1$ para algún $v \in \mathbb{Z}$ y $n^h \mid n^u$, se sigue por transitividad que $n^h \mid 10^v + 1$. Luego $n^h \in M_2$, lo que completa la prueba. □

Lema 3.13. *Sea $n \in M_2$ un entero positivo con $e = 2k$. Entonces, $n \mid 10^t + 1$ si y solo si $t = k \cdot (2i + 1)$ para todo $i = 0, 1, 2, \ldots$.*

Demostración. Supongamos que $n \mid 10^t + 1$. Como $n \in M_2$, $n \mid N(k, 2) = 10^k + 1$. Veamos que

$$k = \text{mín}\left\{j \in \mathbb{Z}^+ : n \mid 10^j + 1\right\}. \tag{3.9}$$

En efecto, supongamos que existe $\kappa \in S$ tal que $\kappa < k$. Si hacemos $\varepsilon = 2\kappa$ es evidente que $n \mid 10^\varepsilon - 1$ y como $\varepsilon = 2\kappa < 2k = e$, se contradice la definición de e. Veamos ahora que $k \mid t$. Procedamos por reducción al absurdo, supongamos que $k \nmid t$, por el algoritmo de la división existen $a, r \in \mathbb{Z}$ con $0 < r < k$ tales que $t = ka + r$. Luego

$$10^t \equiv \left(10^k\right)^a \cdot 10^r \equiv (-1)^a \cdot 10^r \equiv -1 \,(\text{mód } n).$$

Observe que si a es par entonces $10^r \equiv -1 \,(\text{mód } n)$ y como $r < k$ se contradice (3.9). Si a es impar, $10^\rho \equiv 1 \,(\text{mód } n)$ donde $\rho = 2r < 2k = e$ contradice la definición de e. Debe ocurrir entonces que $k \mid t$ como se quería, por lo tanto $t = ks$ para algún $s \in \mathbb{Z}$ y

$$10^t \equiv \left(10^k\right)^s \equiv (-1)^s \equiv -1 \,(\text{mód } n)$$

si y solo si $s = 2i + 1$ para $i = 0, 1, 2, \ldots$ □

Teorema 3.14. *Sea $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ la descomposición canónica del entero positivo n y para cada i, sea $e_i = \text{ord}_{p_i}(10)$. Entonces $n \in M_2$ si y solo si existe un $s \in \mathbb{Z}^+$ tal*

que para cada $1 \leqslant i \leqslant r$, $e_i = 2^s \cdot q_i$, *donde* q_i *es impar.*

Cabe aclarar que en este teorema los q_i pueden diferir para valores diferentes de i, sin embargo el factor 2^s es fijo para cada i.

Demostración. Supongamos que $n \in M_2$ y por reducción al absurdo supongamos que la tesis no se satisface. Esto puede ocurrir por dos razones. La primera es que $s = 0$ para algún i, de modo que $e_i = q_i$ es impar. Esto conlleva a que el factor primo $p_i \notin M_2$. Puesto que $n \mid 10^m + 1$ para algún entero m, para cada uno de los factores primos p de n tenemos que $p \mid 10^m + 1$, en particular para p_i y por el Teorema 3.11 tendríamos que $p_i \in M_2$, lo cual es absurdo. La segunda razón por la cual puede fallar la tesis ocurre si n tiene factores primos p_i y p_j con $i \neq j$ tales que $e_i = 2 \cdot (2^a\, u)$ y $e_j = 2 \cdot (2^b\, v)$, con a, b enteros positivos distintos y u, v impares. Sean $\lambda = 2^a\, u$ y $\theta = 2^b\, v$, entonces $p_i \mid 10^\lambda + 1$ y $p_j \mid 10^\theta + 1$, donde λ y θ son los menores exponentes de 10, respectivamente, para lo cual esto pasa. Dado que $p_i, p_j \mid 10^m + 1$, se sigue del Lema 3.13 que

$$m = (2^a\, u)(2x + 1), \text{ para algún } x = 1, 2, 3, \ldots \tag{3.10}$$

y también,

$$m = (2^b\, v)(2y + 1), \text{ para algún } y = 1, 2, 3, \ldots \tag{3.11}$$

Puesto que u y v son ambos impares, la multiplicidad del primo 2 en la factorización de m es a por (3.10) y también es b por (3.11). Por la unicidad, debe ocurrir que $a = b$ y esto es absurdo pues a y b se escogieron de tal forma que fueran distintos. De la contradicción se sigue que la tesis es verdadera.

Recíprocamente, supongamos que existe $s \in \mathbb{Z}^+$ tal que $e_i = 2^s \cdot q_i$, con q_i impar para $1 \leqslant i \leqslant r$. Para cada i, sea $d_i = e_i/2$. Por el Teorema 3.12 sabemos que $p_i^{\alpha_i} \in M_2$, más aún, en la prueba de este resultado se mostró que $p_i^{\alpha_i} \mid 10^{t_i} + 1$ donde t_i es un múltiplo impar de d_i. Por hipótesis tenemos que $d_i = 2^{s-1} \cdot q_i$ para cada i, y como cada uno de los q_i es impar, el producto de todos ellos, que lo denotaremos por q, también lo es. Ahora bien, sea t el producto de todos los t_i, luego $t \cdot q$ es un número impar múltiplo

de cada q_i y cada t_i. Sea $v = t \cdot q \cdot 2^{s-1}$, entonces $p_i^{\alpha_i} \mid 10^v + 1$ para todo $1 \leqslant i \leqslant r$ y como los $p_i^{\alpha_i}$ son primos relativos dos a dos, se sigue que su producto n satisface que $n \mid 10^v + 1$. De ahí que $n \in M_2$. □

Cuando $n = p$ es primo y $e = \text{ord}_p(10)$ es par, el hecho que p no tenga factores primos mas que él mismo reduce las condiciones del teorema anterior ya que siempre podremos escribir $e = 2^s \cdot q$ con q impar (en el peor de los casos $q = 1$). Con esto estamos diciendo que el Teorema de Midy puede tenerse nuevamente ahora por medio del Teorema 3.14.

Ejemplo 3.15. Vamos a ver a que $1507 \notin M_2$. Dado que los factores primos de 1507 son $p_1 = 11$ y $p_2 = 137$, tenemos que $e_1 = \text{ord}_{11}(10) = 2$ y $e_2 = \text{ord}_{137}(10) = 8$, donde la única posibilidad para s es $s = 1$ pero $q_2 = 4$ no es impar.

3.2. El teorema de Midy en base B

Al inicio de este capítulo se introdujo una notación para generalizar la propiedad de Midy cuando se trabaja con las expansiones decimales de las fracciones x/n en la escala de una base $B > 1$ cualquiera. Sin embargo, el trabajo realizado en la sección precedente no se apoya en esta definición y expande los resultados del Teorema de Midy en su 'estado puro', es decir, cuando se trabaja con la fracción $1/n$ y la longitud del periodo es $e = 2k$. En esta sección vamos a ver que los resultados obtenidos anteriormente son implicaciones inmediatas de resultados más generales.

Sean $B > 1$ y n primos relativos como es usual. Para $x \in \mathbb{U}_n$, si hacemos $x_1 = x$ existen enteros a_1 y x_2 tales que $Bx_1 = a_1 n + x_2$, con $0 \leqslant x_2 < n$. Del mismo modo, existen enteros a_2 y x_3 tales que $Bx_2 = a_2 n + x_3$ con $0 \leqslant x_3 < n$ y en general, al proceder de

manera inductiva obtenemos el siguiente sistema de ecuaciones:

$$\begin{aligned} Bx_1 &= a_1 n + x_2 \\ Bx_2 &= a_2 n + x_3 \\ &\vdots \\ Bx_i &= a_i n + x_{i+1} \\ &\vdots \end{aligned} \tag{3.12}$$

Como $0 < x_1/n < 1$, $0 < Bx_1/n < B$ y por lo tanto $a_1 < B$, luego a_1 es un B-dígito. Como B y x_1 son ambos primos relativos a n y $Bx_1 \equiv x_2 \pmod{n}$ se sigue que $\gcd(x_2, n) = 1$, es decir, $x_2 \in \mathbb{U}_n$. Usando el mismo razonamiento se muestra que a_2 es un B-dígito y $x_3 \in \mathbb{U}_n$, y en general para todo $i \geqslant 1$, a_i es un B-dígito y $x_i \in \mathbb{U}_n$. Si para cada $k \leqslant i$ dividimos la k-ésima ecuación del sistema (3.12) por $B^k n$ tenemos que

$$\frac{x_1}{n} = \frac{a_1}{B} + \frac{a_2}{B^2} + \cdots + \frac{a_i}{B^i} + \frac{x_{i+1}}{B^i n}.$$

Dado que $0 < x_{i+1}/B^i n < 1/B^i$ y $1/B^i \to 0$ cuando $i \to \infty$ se obtiene que $x/n = \sum_{i=1}^{\infty} a_i/B^i$ y escribimos esto como

$$\frac{x}{n} = 0.a_1 a_2 \ldots a_i \ldots$$

Las ecuaciones (3.12) muestran que para cada $i \geqslant 1$,

$$x_{i+1} \equiv Bx_i \equiv B^2 x_{i-1} \equiv \cdots \equiv B^i x_1 \pmod{n} \tag{3.13}$$

Sea e el orden de B módulo n. Por la ecuación (3.13), $x_{e+1} \equiv B^e x_1 \equiv x_1 \pmod{n}$ y además $x_{i+1} \not\equiv x_1$ para $1 \leqslant i < e$. Como $x_1, x_{e+1} \in \mathbb{U}_n, |x_1 - x_{e+1}| < n$ y por ser ambos congruentes módulo n la única opción posible es que $x_{e+1} = x_1$, por lo tanto $a_{e+1} = a_1$, $x_{e+2} = x_2$ y en general $x_{e+i} = x_i$, $a_{e+i} = a_i$ para cada $i \geqslant 1$. Concluimos que el decimal

de x/n en la escala de B es periódico puro con longitud e y entonces

$$\frac{x}{n} = [0.\overline{a_1 a_2 \dots a_e}]_B.$$

Dado que e depende únicamente de B y n y no de x, cada fracción x/n con $x \in \mathbb{U}_n$ es periódica de longitud e.

Observación. Todo el análisis que se acabó de hacer, sustenta que la Definición 3.1 esté, valga la redundancia, bien definida. Además, puede verse que este resultado extiende el inciso **II** del Teorema 1.40, donde la condición allí sobre la base era más fuerte.

Teorema 3.16. *Sean n y $B > 1$ primos relativos y $e = dk$. Definamos para $x \in \mathbb{U}_n$,*

$$R_d(x) \coloneqq \sum_{j=1}^{d} x_{(j-1)k+1},$$

entonces:

I. $nS_d(x) = (B^k - 1)R_d(x)$.

II. $S_d(x) \equiv 0 \pmod{B^k - 1}$ *si y solo si* $R_d(x) \equiv 0 \pmod{n}$.

Demostración. Como $e = dk$, podemos separar las primeras e ecuaciones del sistema (3.12) en d grupos con k ecuaciones. Para cada $1 \leqslant j \leqslant d$, el j-ésimo grupo consiste de las k ecuaciones

$$\begin{aligned} Bx_{(j-1)k+1} &= a_{(j-1)k+1}n + x_{(j-1)k+2} \\ Bx_{(j-1)k+2} &= a_{(j-1)k+2}n + x_{(j-1)k+3} \\ &\vdots \\ Bx_{jk} &= a_{jk}n + x_{jk+1} \end{aligned} \tag{3.14}$$

Si multiplicamos la primera de estas ecuaciones por B^{k-1}, la segunda por B^{k-2} y así sucesivamente hasta multiplicar la $(k-1)$-ésima ecuación por B y la k-ésima por $B^0 = 1$,

obtenemos

$$B^k x_{(j-1)k+1} = a_{(j-1)k+1} B^{k-1} n + B^{k-1} x_{(j-1)k+2}$$
$$B^{k-1} x_{(j-1)k+2} = a_{(j-1)k+2} B^{k-2} n + B^{k-2} x_{(j-1)k+3}$$
$$\vdots$$
$$B x_{jk} = a_{jk} n + x_{jk+1}$$

Al hacer un reemplazo escalonado del último sumando de cada una de las ecuaciones en la ecuación siguiente, tenemos la igualdad

$$B^k x_{(j-1)k+1} = \left(a_{(j-1)k+1} B^{k-1} + a_{(j-1)k+2} B^{k-2} + \cdots + a_{jk} \right) n + x_{jk+1},$$

y dado que definimos $A_j = [a_{j-1} a_{j-2} \dots a_{jk}]_B$, reescribimos la última expresión como

$$B^k x_{(j-1)k+1} = A_j n + x_{jk+1}, \tag{3.15}$$

así que al sumar las ecuaciones (3.15) para $j = 1, 2, \dots, d$ tenemos

$$B^k \sum_{j=1}^{d} x_{(j-1)k+1} = n \sum_{j=1}^{d} A_j + \sum_{j=1}^{d} x_{jk+1}.$$

Dado que $x_{dk+1} = x_{e+1} = x_1$, las sumas sobre los x_t son iguales y por lo tanto podemos reescribir la última expresión como

$$(B^k - 1) \sum_{j=1}^{d} x_{(j-1)k+1} = n S_d(x). \tag{3.16}$$

De ahí se sigue **I**. Además, **II** es consecuencia inmediata de (3.16). □

En el Ejemplo 3.2 mostramos que $7 \in M_2(5)$ y el Teorema 1.41 facilitó dicho trabajo. En general, determinar si $n \in M_d(B)$ puede volverse tedioso debido a que la condición $S_d(x) \equiv 0 \pmod{B^k - 1}$ debe cumplirse para cada $x \in \mathbb{U}_n$, es decir, tendríamos que hacer $\phi(n)$ cálculos para obtener una conclusión. Sin embargo, esta definición viene motivada por los resultados del siguiente teorema, donde se establece que la ya nombrada

condición puede debilitarse para algún $x \in \mathbb{U}_n$ y no todos. Esto ayudará el estudio de los ejemplos.

Teorema 3.17. *Bajo las mismas hipótesis del Teorema 3.16, las siguientes proposiciones 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. $N_B(k,d) = B^{k(d-1)} + B^{k(d-2)} + \cdots + B^k + 1 \equiv 0 \pmod{n}$.

Además, $n \in M_d(B)$ *siempre que* $\gcd(n, B^k - 1) = 1$.

Demostración. Observe que la cadena de implicaciones **I** $\Longrightarrow$ **II** $\Longleftrightarrow$ **III** se sigue de la Definición 3.1 y el Teorema 3.16, respectivamente. Ahora bien, de la ecuación (3.13),

$$R_d(x) = \sum_{j=1}^{d} x_{(j-1)k+1} \equiv x \sum_{j=1}^{d} B^{k(j-1)} \equiv x N_B(k,d) \pmod{n},$$

de modo que $R_d(x) \equiv 0 \pmod{n}$ si y solo si $N_B(k,d) \equiv 0 \pmod{n}$, pues $\gcd(x,n) = 1$. Esto muestra la equivalencia entre **IV** y **III** y por ende con **II**. Dado que la proposición **IV** es independiente de x, equivale a decir que $S_d(x) \equiv 0 \pmod{B^k - 1}$ para cada $x \in \mathbb{U}_n$, esto es $n \in M_d(B)$.

Para probar la última afirmación, consideremos el polinomio $F_d(t) = t^{d-1} + t^{d-2} + \cdots + t + 1$. Por definición de e, $B^e \equiv 1 \pmod{n}$, luego $B^e - 1 = (B^k - 1)F_d(B^k) \equiv 0 \pmod{n}$. Por lo tanto $F_d(B^k) = N_B(k,d) \equiv 0 \pmod{n}$ siempre que $\gcd(n, B^k - 1) = 1$ y de ahí que $n \in M_d(B)$. □

El hecho de haber trabajado toda la sección anterior únicamente con la fracción $1/n$ se explica con este teorema. De igual forma, la última proposición ya se había discutido cuando $B = 10$, donde mostrábamos que la condición era suficiente pero no necesaria

(ver Ejemplo 3.6). Con el fin de familiarizarnos un poco con la notación mostraremos otro ejemplo de este hecho.

Ejemplo 3.18. Sean $B = 7$ y $n = 39$. Para hallar el decimal de $1/39$ en la escala de 7 acudimos al algoritmo implementado en el sistema de ecuaciones (3.12):

$$\begin{aligned}
7 \cdot 1 &= 0 \cdot 39 + 7 \\
7 \cdot 7 &= 1 \cdot 39 + 10 \\
7 \cdot 10 &= 1 \cdot 39 + 31 \\
7 \cdot 31 &= 5 \cdot 39 + 22 \\
7 \cdot 22 &= 3 \cdot 39 + 37 \\
7 \cdot 37 &= 6 \cdot 39 + 25 \\
7 \cdot 25 &= 4 \cdot 39 + 19 \\
7 \cdot 19 &= 3 \cdot 39 + 16 \\
7 \cdot 16 &= 2 \cdot 39 + 34 \\
7 \cdot 34 &= 6 \cdot 39 + 4 \\
7 \cdot 4 &= 0 \cdot 39 + 28 \\
7 \cdot 28 &= 5 \cdot 39 + 1
\end{aligned}$$

Puesto que el residuo $x_{12} = 1 = x_1$, $e = 12$ y por lo tanto $1/39 = [0.\overline{011536432605}]_7$. Con $d = 6$ y $k = 2$, $S_6(1) = [165]_7 = 2 \cdot [66]_7 \equiv 0 \,(\text{mód } 7^2 - 1)$ y además $R_6(1) = x_1 + x_3 + x_5 + x_7 + x_9 + x_{11} = 78$, luego $39 \in M_6(7)$, sin embargo $\gcd(39, 7^2 - 1) = 3 \neq 1$.

Observación. El Teorema 3.17 nos brinda desde otro punto de vista una explicación sencilla y breve del por qué $d > 1$. En efecto, si tuviéramos que $n \in M_1(B)$ entonces $1 = R_1(1) \equiv 0 \,(\text{mód } n)$, lo cual es absurdo.

Ejemplo 3.19. Consideremos el número primo $p = 17$ y la base $B = 3$, de donde $e = \text{ord}_p(B) = 16$. Si hacemos $d = k = 4$ entonces $\gcd(17, 3^4 - 1) = 1$, luego $17 \in M_4(3)$.

Sea $h \in \mathbb{Z}^+$, queremos ver si es posible que $17^h \in M_4(3)$ y para ello vamos a calcular el $\text{ord}_{17^h}(3)$ para $h \leqslant 10$, como muestra la siguiente tabla.

h	$\text{ord}_{17^h}(3)$
2	$16 \cdot 17$
3	$16 \cdot 17^2$
4	$16 \cdot 17^3$
5	$16 \cdot 17^4$
6	$16 \cdot 17^5$
7	$16 \cdot 17^6$
8	$16 \cdot 17^7$
9	$16 \cdot 17^8$
10	$16 \cdot 17^9$

Tabla 4. Orden de 3 módulo 17^h para $h \leqslant 10$.

Tenemos que $\text{ord}_{17^h}(3) = 4K$ donde $K = 4 \cdot 17^{h-1}$, entonces por el teorema de Fermat, $3^K \equiv \left(3^4\right)^{17^{h-1}} \equiv 3^4 \,(\text{mód } 17)$, por lo cual $\gcd(17^h, 3^K - 1) = \gcd(17^h, 3^4 - 1) = 1$. De ahí que $17^h \in M_4(3)$ para $h \leqslant 10$. De hecho, esta última conclusión es válida para todo $h \in \mathbb{Z}^+$ y en general, cualquier número primo p tiene la propiedad de Midy para la base B y el divisor d, así como también p^h para cada $h \in \mathbb{Z}^+$, cuando p y B son primos relativos. Para probar esto, vamos a demostrar primero los siguientes dos lemas.

Lema 3.20. *Sean p un primo y $a, b \in \mathbb{Z}$.*

I. *Si $a \equiv b \,(\text{mód } p^n)$ entonces $a^{p^s} \equiv b^{p^s} \,(\text{mód } p^{n+s})$ para cada par de enteros positivos n y s.*

II. *Si $p \neq 2$ y $p \nmid b$ entonces para cada par de enteros positivos n y s, se tiene que $a^{p^s} \equiv b^{p^s} \,(\text{mód } p^{n+s})$ implica $a \equiv b \,(\text{mód } p^n)$.*

Demostración. **I**. Usemos inducción sobre s para probar el enunciado. Supongamos que

$a \equiv b \,(\text{mód } p^n)$, entonces $a = tp^n + b$ para algún entero t y así,

$$a^p = \sum_{k=0}^{p} \binom{p}{k} (tp^n)^{p-k}\ b^k.$$

Dado que $p \mid \binom{p}{k}$ para $0 < k < p$, es claro que $p^{n+1} \mid \binom{p}{k} p^{n(p-k)}$ y también $p^{n+1} \mid p^{np}$, luego $a^p \equiv b^p \,(\text{mód } p^{n+1})$ y el resultado es válido para $s = 1$ y cada $n \in \mathbb{N}$.
Supongamos ahora que el enunciado se satisface para cada $n \in \mathbb{N}$, para $s = 1, 2, \ldots, r$ y supongamos que $a \equiv b \,(\text{mód } p^n)$. Por la hipótesis de inducción para $s = 1$, $a^p \equiv b^p \,(\text{mód } p^{n+1})$. Si partimos de este hecho entonces para $s = r$ tenemos que

$$(a^p)^{p^r} \equiv (b^p)^{p^r} \,(\text{mód } p^{n+1+r}),$$

que al reescribirlo resulta $a^{p^r+1} \equiv b^{p^r+1} \,(\text{mód } p^{n+(r+1)})$. De este modo el resultado es válido para $s = r + 1$ y por lo tanto para cada par de enteros positivos s y n.
II. Vamos a probar el caso $s = 1$ por inducción sobre n. Queremos ver que si se cumple $a^p \equiv b^p \,(\text{mód } p^{n+1})$, entonces $a \equiv b \,(\text{mód } p^n)$. Para $n = 1$, si $a^p \equiv b^p \,(\text{mód } p^2)$, es inmediato que $a^p \equiv b^p \,(\text{mód } p)$ y por el teorema de Fermat, $a \equiv b \,(\text{mód } p)$. Supongamos ahora que $a^p \equiv b^p \,(\text{mód } p^m)$ implica $a \equiv b \,(\text{mód } p^{m-1})$. Si $a^p \equiv b^p \,(\text{mód } p^{m+1})$ resulta claro que $a^p \equiv b^p \,(\text{mód } p^m)$ y por la hipótesis de inducción, $a \equiv b \,(\text{mód } p^{m-1})$. Escribamos $a = up^{m-1} + b$ para algún entero u, como $p > 2$, $p \mid \binom{p}{k}$ para $0 < k < p$ y

$$a^p = \sum_{k=0}^{p} \binom{p}{k} \left(up^{m-1}\right)^{p-k} b^k,$$

se sigue que $a^p \equiv b^p + up^m b^{p-1} \,(\text{mód } p^{m+1})$. Entonces $up^m b^{p-1} = tp^{m+1}$ para algún entero t, es decir, $ub^{p-1} = tp$ y por lo tanto $p \mid u$ pues $p \nmid b$. De modo que $a = u_1 p^m + b$ para algún entero u_1 y así $a \equiv b \,(\text{mód } p^m)$.
Usemos ahora inducción sobre s para completar la prueba. Asumamos que para cada $n \in \mathbb{N}$, $a^{p^{r-1}} \equiv b^{p^{r-1}} \,(\text{mód } p^{n+r-1})$ implica $a \equiv b \,(\text{mód } p^n)$ y también que $a^{p^r} \equiv$

$b^{p^r} \pmod{p^{n+r}}$. Entonces

$$(a^p)^{p^{r-1}} \equiv (b^p)^{p^{r-1}} \pmod{p^{n+r}},$$

y por la hipótesis de inducción, $a^{p^{r-1}} \equiv b^{p^{r-1}} \pmod{p^{n+1}}$, así que por lo que ya probamos se sigue que $a \equiv b \pmod{p^n}$. Esto completa la prueba. □

Lema 3.21. *Sea p un primo impar. Si $\mathrm{ord}_p(B) = e$, $p^z \mid (B^e - 1)$ y $p^{z+1} \nmid (B^e - 1)$ entonces*

$$\mathrm{ord}_{p^h}(B) = ep^{\max\{0,h-z\}}.$$

Demostración. Supongamos cierta la hipótesis. Si $h \leqslant z$ entonces $p^h \mid (B^e - 1)$. Esto no es válido para ningún exponente $t < e$, ya que si $p^h \mid (B^t - 1)$, entonces $p \mid (B^t - 1)$ y por definición, $e \mid t$. Siendo así tenemos que $\mathrm{ord}_{p^h}(B) = e$, lo que prueba el lema cuando $h \leqslant z$.

Si $h > z$, como $B^e \equiv 1 \pmod{p^z}$ entonces del lema anterior, $B^{ep^{h-z}} \equiv 1 \pmod{p^h}$. Veamos que $B^d \not\equiv 1 \pmod{p^h}$ para cualquier divisor propio d de ep^{h-z}. Sea $d = e_1 p^r$, donde $e_1 \mid e$ y $r \leqslant h - z$, y supongamos que $B^{e_1 p^r} \equiv 1 \pmod{p^h}$. Por el lema precedente, $B^{e_1} \equiv 1 \pmod{p^{h-r}}$, de modo que $B^{e_1} \equiv 1 \pmod{p}$ y por lo tanto $e \mid e_1$. De ahí que $e_1 = e$. Dadas las condiciones de z en la hipótesis entonces como $p^{h-r} \mid (B^e - 1)$, tenemos que $h - r \leqslant z$, luego $r = h - z$, como queríamos. Por esto último, $\mathrm{ord}_{p^h}(B) = ep^{h-z}$ para $h > z$. □

Ahora sí procedemos a enunciar el resultado que ya habíamos comentado.

Teorema 3.22. *Si p es un primo que no divide a B y $e = dk$, entonces $p \in M_d(B)$. También se tiene que $p^h \in M_d(B)$ para cada $h \in \mathbb{Z}^+$.*

Demostración. Como $d > 1$, $k < e$ y por tanto $B^k \not\equiv 1 \pmod{p}$, luego $\gcd(B^k - 1, p) = 1$ y así $p \in M_d(B)$ por el Teorema 3.17. Observe que $p \neq 2$ pues de no serlo, como p y B son primos relativos, B sería impar y así $B^1 \equiv 1 \pmod{2}$, de donde $e = \mathrm{ord}_2(B) = 1$ no es posible pues e debe ser un múltiplo de d. Por el lema precedente, $e_h = \mathrm{ord}_{p^h}(B) = ep^g$

donde g depende de h, luego $e_h = dK$ con $K = kp^g$. Por el teorema de Fermat, $B^K = (B^k)^{p^g} \equiv B^k \pmod{p}$, de modo que $\gcd(B^K - 1, p^h) = \gcd(B^k - 1, p) = 1$ y del Teorema 3.17 se sigue que $p^h \in M_d(B)$. □

Una pregunta natural que nace siguiendo el mismo orden de ideas dado por el teorema anterior, es saber si $n \in M_d(B)$ implica $n^h \in M_d(B)$. En la sección precedente veíamos que cuando $B = 10$ y $e = 2k$ esto era cierto, sin embargo el siguiente ejemplo nos muestra que en general no podemos concluir lo mismo.

Ejemplo 3.23. Para la base $B = 4$, la fracción $1/21$ tiene periodo de longitud $e = \mathrm{ord}_{21}(4) = 3$; más precisamente,

$$\frac{1}{21} = [0.003]_4,$$

de donde es claro que $S_3(1) = [3]_4 \equiv 0 \pmod{4-1}$, esto es, $21 \in M_3(4)$. Sin embargo, $\mathrm{ord}_{21^2}(4) = 21$ y

$$\frac{1}{21^2} = [0.000021102123210231313],$$

de donde $S_3(1) = [1111111]_4 \equiv 5461 \pmod{4^7 - 1}$.

El siguiente resultado es una extensión del Teorema 3.9.

Teorema 3.24. *Sean n y B primos relativos y $e = kd$. Si para cada factor primo p de n se tiene que* $\mathrm{ord}_p(B) \nmid k$, *entonces $n \in M_d(B)$.*

Demostración. Sea p un factor primo de n. Como $\mathrm{ord}_p(B) \nmid k$, entonces $p \nmid B^k - 1$, luego $\gcd(p, B^k - 1) = 1$. Es claro que si $\alpha \in \mathbb{Z}^+$ es la multiplicidad del primo p como factor de n, $\gcd(p^\alpha, B^k - 1) = 1$. De ahí que $\gcd(n, B^k - 1) = 1$ y por lo tanto $n \in M_d(B)$. □

Ejemplo 3.25. Sean $n = 45 = 3^2 \cdot 5$ y $B = 2$, entonces $\mathrm{ord}_3(2) = 2$, $\mathrm{ord}_5(2) = 4$ y $e = \mathrm{ord}_{45}(2) = 12$. Cuando $d = 4$, el entero $k = 3$ no es múltiplo ni de 2 ni de 4, por lo que $45 \in M_4(2)$. De igual forma cuando $d = 12$, se verifican las mismas condiciones para el entero $k = 1$, así que $45 \in M_{12}(2)$.

Ejemplo 3.26. Consideremos los enteros $n = 98$ y $B = 3$, donde $e = \text{ord}_{98}(3) = 42$ y

$$\frac{1}{98} = [0.000021102211212102021222201120011010120201].$$

En la tabla que se muestra a continuación estudiamos la suma $S_d(1)$ para cada divisor d de $e = 42$, fijando interés en la relación que guarda la suma $S_{d_1}(1)$ cuando $d_1 \mid d$.

d	$S_d(1)$	¿$98 \in M_d(3)$?
2	$[22222222222222222222]_3$	Sí
3	$[111111111111110]_3$	No
6	$[22222220]_3$	Sí
7	$[10001211]_3$	No
14	$[20202]_3$	Sí
21	$[10010]_3$	No
42	$[1120]_3$	Sí

Tabla 5. Estudio de la propiedad de Midy para $n = 98$ y $B = 3$.

Observemos que $98 \in M_2(3)$ y para los divisores $d = 6, 14, 42$ que son múltiplos de $d_1 = 2$ también $98 \in M_d(B)$. Contrarrecíprocamente, $98 \notin M_{21}(3)$ y para los divisores $d = 3, 7$, $d \mid 21$ y $98 \notin M_d(3)$. La razón por la cual esto ocurre lo explica el siguiente teorema.

Teorema 3.27. *Sean n y B primos relativos, y d_1 y d_2 enteros positivos tales que $d_1 \mid d_2$ y $d_2 \mid e = \text{ord}_n(B)$. Si $n \in M_{d_1}(B)$ entonces $n \in M_{d_2}(B)$.*

Demostración. Supongamos que $n \in M_{d_1}(B)$ y sea $e = d_1k_1 = d_2k_2$. Podemos escribir

$$N_B(k_2, d_2) = \frac{B^e - 1}{B^{k_2} - 1} = \left(\frac{B^e - 1}{B^{k_1} - 1}\right)\left(\frac{B^{k_1} - 1}{B^{k_2} - 1}\right),$$

donde las dos fracciones al lado derecho de la igualdad son enteros ya que $k_1 \mid e$ y $k_2 \mid k_1$. Observe que el primero de los factores en la expresión es $N_B(k_1, d_1)$ y por el

Teorema 3.17, $N_B(k_1, d_1) \equiv 0 \,(\text{mód } n)$, esto implica que $N_B(k_2, d_2) \equiv 0 \,(\text{mód } n)$, de donde $n \in M_{d_2}(B)$, nuevamente por el Teorema 3.17, □

El siguiente enunciado nos brinda una sencilla pero interesante caracterización de la propiedad de Midy en términos del periodo de la fracción $1/n$ en la escala de B.

Teorema 3.28. *Sean n y B primos relativos y $e = dk$, entonces $n \in M_d(B)$ si y solo si $D_B(n) \equiv 0 \,(\text{mód } B^k - 1)$. Además, si $n \in M_d(B)$ y $N_B(k, d) = nt$ para algún $t \in \mathbb{Z}$, entonces $D_B(n) = t(B^k - 1)$.*

Demostración. Por el Teorema 3.17, $n \in M_d(B)$ si y solo si $N_B(k, d) \equiv 0 \,(\text{mód } n)$, de donde $B^e - 1 = nt(B^k - 1)$ para algún $t \in \mathbb{Z}$. Por la ecuación (3.1), $nD_B(n) = B^e - 1$, de modo que $D_B(n) = t(B^k - 1)$ si y solo si $D_B(n) \equiv 0 \,(\text{mód } B^k - 1)$. □

Teniendo a la mano esta caracterización, estudiar la propiedad de Midy para los distintos divisores d de $e = \text{ord}_n(B)$ se hace una tarea más sencilla en cuanto evita calcular las sumas en base B de los bloques que conforman el periodo de $1/n$, como hemos venido haciendo para la mayoría de ejemplos. La única consideración a tener es la conversión de $D_B(n)$ de la base B a la base decimal usual, como veremos a continuación.

Ejemplo 3.29. Del Ejemplo 3.26 sabemos que $98 \in M_d(3)$ para los divisores pares $d = 2, 6, 14, 42$ de $e = 42$. En base 10,

$$D_3(98) = 1116520297260330196$$

y en efecto se verifica que $D_3(98) \equiv 0 \,(\text{mód } 3^k - 1)$, para $k = 21, 7, 3, 1$, respectivamente.

En el Capítulo 2 estudiamos la propiedad de Midy en la base decimal usual cuando n era primo utilizando el subgrupo $\mathbb{U}(p, d)$ de $\mathbb{U}_p$ para saber la forma de la suma $S_d(1)$ como múltiplo de $10^k - 1$. En el contexto general, si n es una potencia de un primo, digamos $n = p^t$ para algún entero t, tenemos un resultado análogo. Veamos un ejemplo para dar una idea de lo que sucede y posteriormente enunciar el resultado.

Ejemplo 3.30. Vamos a denotar por $\mathbb{U}(p^t, d)$ el único subgrupo de orden d en $\mathbb{U}_{p^t}$ y por $s(p^t, d)$ la suma de sus elementos. Sean $n = 9 = 3^2$ y $B = 11$. Como $e = \mathrm{ord}_9(11) = 6$ y

$$\frac{1}{9} = [0.\overline{124986}]_{11},$$

estudiemos caso por caso la suma $S_d(1)$ para los distintos valores $d = 2, 3, 6$.

Caso $d = 2$: Tenemos que $\mathbb{U}(9, 2) = \{1, 8\}$, de donde $s(9, 2) = 9$ y $S_2(1) = [AAA]_{11} = 11^3 - 1$. De ahí que $9 \in M_2(11)$. (Aquí la letra A representa a 10 como 11-dígito.)

Caso $d = 3$: Tenemos que $\mathbb{U}(9, 2) = \{1, 4, 7\}$, de donde $s(9, 3) = 12$ y $S_3(1) = [136]_{11} \equiv 40 \pmod{11^2 - 1}$, luego $9 \notin M_3(11)$.

Caso $d = 6$: Tenemos que $\mathbb{U}(9, 6) = \mathbb{U}_9$, de donde $s(9, 6) = 27 = 3 \cdot 9$ y $S_6(1) = [28]_{11} = 3(11^1 - 1)$. De ahí que $9 \in M_6(11)$.

Consideremos ahora los enteros $n = 125 = 5^3$ y $B = 4$, de donde $e = \mathrm{ord}_{125}(4) = 50$ y

$$\frac{1}{125} = [0.\overline{00020030102123221132031103331330323121011220130223}]_4.$$

En este caso los posibles divisores de e son $d = 2, 5, 10, 25, 50$, veamos lo que ocurre para cada uno de ellos.

Caso $d = 2$: Tenemos que $\mathbb{U}(125, 2) = \{1, 124\}$, de donde $s(125, 2) = 125$ y $S_2(1) = 4^{25} - 1$. De ahí que $125 \in M_2(4)$.

Caso $d = 5$: Tenemos que $\mathbb{U}(125, 5) = \{1, 26, 51, 76, 101\}$, de donde $s(125, 5) = 1 + 26 + 51 + 76 + 101 = 255$ y $S_5(1) \equiv 41943 \pmod{4^{10} - 1}$. De ahí que $125 \notin M_5(4)$.

Caso $d = 10$: Tenemos que $\mathbb{U}(125, 10) = \{1, 24, 26, 49, 51, 74, 76, 99, 101, 124\}$, por lo tanto $s(125, 10) = 625 = 5 \cdot 125$ y $S_5(1) = [1033323]_4 = 5(4^5 - 1)$. De ahí que $125 \in M_{10}(4)$.

Caso $d = 25$: Evitamos listar $\mathbb{U}(125, 25)$ debido a la extensa cantidad de elementos que posee, pero puede verificarse que $s(125, 25) = 1525$ y $S_{25}(1) = [2313]_4 \equiv 3 \pmod{4^2 - 1}$. De ahí que $125 \notin M_{25}(4)$.

Caso $d = 50$: Nuevamente evitamos listar $\mathbb{U}(125, 50)$ pues se hace extenso, pero puede

verificarse que $s(125, 50) = 3125 = 25 \cdot 125$ y $S_{50}(1) = [1023]_4 = 25(4^1 - 1)$. De ahí que $125 \in M_{50}(4)$.

En ambos ejemplos, cuando el divisor d no es una potencia del primo p, $p^t \in M_d(B)$, mientras que si ocurre lo contrario, $p^t \notin M_d(B)$. Además, cuando $p^t \in M_d(B)$ se verifica que $S_d(1) = r(B^k - 1)$ donde $s(p^t, d) = rp^t$. Esto es precisamente todo lo que envuelven los siguientes resultados.

Lema 3.31. *Sean p un primo impar y t un entero positivo. Sea d un divisor de $\phi(p^t)$ y sea $\mathbb{U}(p^t, d)$ el único subgrupo de orden d de $\mathbb{U}_{p^t}$. Entonces d es una potencia de p, $d = p^{t-i}$, si y solo si $a \equiv 1 \pmod{p}$ para cada $a \in \mathbb{U}(p^t, d)$. Además, si denotamos por $s(p^t, d)$ la suma de los elementos de $\mathbb{U}(p^t, d)$, entonces*

$$s(p^t, d) = \begin{cases} \dfrac{p^{t-i}(p^t - p^i + 2)}{2} & \text{si } d = p^{t-i}, \\ 0 \pmod{p^t} & \text{en cualquier otro caso.} \end{cases}$$

Demostración. Supongamos que $d = p^{t-i}$ para algún $i = 1, 2, \ldots, t-1$. Sea $a \in \mathbb{U}(p^t, p^{t-i})$, dado que $a^{p^{t-i}} \equiv 1 \pmod{p^t}$, del Lema 3.20 se sigue que $a \equiv 1 \pmod{p^i}$ y de ahí que $a \equiv 1 \pmod{p}$. Si escribimos $a = 1 + mp^i$ para algún entero m, resulta evidente que

$$U(p^t, d) = \left\{1 + mp^i : m = 0, 1, 2, \ldots, p^{t-1} - 1\right\}, \tag{3.17}$$

por lo tanto

$$s(p^t, d) = \sum_{m=0}^{d-1} \left(1 + mp^i\right) = p^{t-i} + \frac{p^t(p^{t-i} - 1)}{2} = \frac{p^{t-i}(p^t - p^i + 2)}{2}.$$

Recíprocamente, si d no es un potencia de p entonces $d \nmid p^{t-1}$. Como d es un divisor de $\phi(p^t)$, $d \mid p - 1$ y existe un elemento $a \neq 1$ en $\mathbb{U}(p^t, d)$ tal que $\mathrm{ord}_{p^t}(a) \mid p - 1$ y por lo tanto $a \notin \mathbb{U}(p^t, p^{t-1})$. Por (3.17), esto implica que $a \neq 1 + mp^i$ y así $a \not\equiv 1 \pmod{p}$.

Ahora, puesto que $\mathbb{U}(p^t,d)=\left\{ag : g\in\mathbb{U}(p^t,d)\right\}$, tenemos que

$$\sum_{g\in\mathbb{U}(p^t,d)} ag = \sum_{g\in\mathbb{U}(p^t,d)} g,$$

luego

$$(a-1)\sum_{g\in\mathbb{U}(p^t,d)} g = 0,$$

y como $a\not\equiv 1 \pmod{p}$, entonces $s(p^t,d)\equiv 0 \pmod{p^t}$. □

Teorema 3.32. *Suponga que p es un primo tal que $B\not\equiv 1 \pmod{p}$. Sea t un entero positivo y $e=\operatorname{ord}_{p^t}(B)=dk$. Si*

$$\frac{1}{p^t}=\left[0.\overline{A_1A_2\ldots A_d}\right]_B,$$

entonces

$$\sum_{j=1}^{d} A_j = \begin{cases} \dfrac{(B^k-1)(p^t-p^i+2)}{2p^i} & \text{si existe } 1\leqslant i\leqslant t-1, \text{ tal que } d=p^{t-i}, \\ 0 \pmod{B^k-1} & \text{en cualquier otro caso.} \end{cases}$$

Demostración. Observemos que en base B,

$$\begin{aligned} \frac{1}{p^t} &= 0.\overline{A_1A_2\cdots A_d}, \\ \frac{B^k}{p^t} &= A_1.\overline{A_2A_3\cdots A_dA_1}, \\ \frac{B^{2k}}{p^t} &= A_1A_2.\overline{A_3A_4\cdots A_1A_2}, \\ &\vdots \\ \frac{B^{(d-1)k}}{p^t} &= A_1A_2\cdots A_{d-1}.\overline{A_dA_1\cdots A_{d-1}}. \end{aligned}$$

Al sumar cada una de las ecuaciones anteriores obtenemos:

$$\sum_{j=0}^{d-1} \frac{B^{jk}}{p^t} = \sum_{j=0}^{d-1} \left\lfloor \frac{B^{jk}}{p^t} \right\rfloor + \sum_{j=0}^{d-1} \left\{ \frac{B^{jk}}{p^t} \right\}. \tag{3.18}$$

Por un lado, si usamos un razonamiento análogo al usado en la demostración del Teorema 2.2, es claro que

$$\sum_{j=0}^{d-1} \left\{ \frac{B^{jk}}{p^t} \right\} = \frac{A_1 + A_2 + \cdots + A_d}{B^k - 1}.$$

Ahora, puesto que $B^{jk} = p^t \left\lfloor \dfrac{B^{jk}}{p^t} \right\rfloor + r_j$, donde $r_j \equiv B^{jk} \pmod{p^t}$, podemos reescribir (3.18) como

$$\sum_{j=0}^{d-1} \frac{B^{jk}}{p^t} = \sum_{j=0}^{d-1} \left(\frac{B^{jk} - r_j}{p^t} \right) + \frac{A_1 + A_2 + \cdots + A_d}{B^k - 1}$$

y así llegamos a que

$$\sum_{j=1}^{d} A_j = \frac{B^k - 1}{p^t} \sum_{j=0}^{d-1} r_j. \tag{3.19}$$

Como $\operatorname{ord}_{p^t}(B) = dk$,

$$\mathbb{U}(p^t, d) = \left\{ B^{jk} \pmod{p^t} : j = 0, 1, 2, \ldots, d-1 \right\},$$

y entonces la conclusión del teorema se sigue del Lema 3.31. □

Del teorema anterior podemos deducir que $n = p^t \in M_d(B)$ siempre y cuando d no sea una potencia de p. Más aún, nos brinda información de la suma de los bloques que conforman el periodo de $1/n$, $S_d(1)$, bajo el conocimiento del único subgrupo de orden d en $\mathbb{U}_{p^t}$, a saber $\mathbb{U}(p^t, d)$, tal como veíamos en el Ejemplo 3.30. Resumimos todo esto en el siguiente enunciado.

Teorema 3.33. *Sean t un entero positivo y p un primo que no divide a B. Sea $n = p^t$ y $e = \operatorname{ord}_n(B) = kd$. Entonces $n \in M_d(B)$ si y solo si $d \nmid p^{t-1}$. Además, si $n \in M_d(B)$*

y $s(p^t, d) = rp^t$ *para algún entero* r*, entonces* $S_d(1) = r(B^k - 1)$.

Si consideramos la fracción $1/n$ no es difícil ver que del mismo modo en que se obtuvo la expresión (3.19), denotando por $r_j \equiv B^{jk} \pmod{n}$ para $j = 1, 2, \ldots, d$, entonces

$$\sum_{j=1}^{d} A_j = \frac{B^k - 1}{n} \sum_{j=1}^{d} r_j.$$

De ahí que

$$\frac{\sum_{j=1}^{d} A_j}{B^k - 1} = \frac{\sum_{j=1}^{d} r_j}{n}. \tag{3.20}$$

Esta última expresión nos dice que a condición de tener $n \in M_d(B)$ es necesario y suficiente que la suma $\sum_{j=1}^{d} r_j$ sea múltiplo de n. Ahora bien, si $n = p_1^{t_1} p_2^{t_2} \ldots p_s^{t_s}$ es la descomposición canónica de n, es sabido que el *Teorema Chino del Residuo* garantiza de cierta forma el isomorfismo entre $\mathbb{U}_n$ y $\mathbb{U}_{p_1^{t_1}} \times \mathbb{U}_{p_2^{t_2}} \times \cdots \times \mathbb{U}_{p_s^{t_s}}$, de modo tal que $\sum_{j=1}^{d} r_j$ es un múltiplo de n si y solo si es un múltiplo de $p_i^{t_i}$ para todo $i = 1, 2, \ldots, s$. Vamos a usar este razonamiento en la prueba del siguiente teorema.

Teorema 3.34. *Sean* n *y* B *primos relativos y* $e = dk$*. Sea* p^t *la mayor potencia de* p *que divide a* n*. Entonces* $n \in M_d(B)$ *si y solo si para cada factor primo* p *de* n*,* $\mathrm{ord}_p(B) \mid k$ *implica* $p^t \mid d$.

Demostración. Sean p un factor primo de n, p^t la mayor potencia de p que divide a n y π la proyección canónica de $\mathbb{U}_n \cong \mathbb{U}_{p_1^{t_1}} \times \mathbb{U}_{p_2^{t_2}} \times \cdots \times \mathbb{U}_{p_s^{t_s}}$ sobre $\mathbb{U}_{p^t}$, esto es, π es el homomorfismo definido como sigue:

$$\begin{aligned} \pi : \mathbb{U}_n &\longrightarrow \mathbb{U}_{p^t} \\ a &\mapsto \pi(a) = a \pmod{p^t}. \end{aligned}$$

Supongamos que para cada factor primo p de n, $\mathrm{ord}_p(B) \mid k$ implica $p^t \mid d$, entonces es claro que $r_j \equiv B^{jk} \equiv 1 \pmod{p}$ para $j = 1, 2, \ldots, d$. Como el conjunto $\mathcal{B} = \{B^{jk} : j = 1, 2, \ldots, d\}$ es un subgrupo de $\mathbb{U}_n$, su imagen bajo la proyección canónica $\pi(\mathcal{B})$ es

un subgrupo de $\mathbb{U}_{p^t}$; más precisamente, por el Lema 3.31 tiene orden p^{t-i} para algún $1 \leqslant i \leqslant t$, luego $\pi(\mathcal{B}) = \mathbb{U}(p^t, p^{t-i})$. Como $d = lp^t$ para algún entero l y podemos escribir a $\mathcal{B}$ como

$$\mathcal{B} = \bigcup_{g \in \mathbb{U}(p^t, p^{t-i})} \pi^{-1}(g),$$

es claro que cada $g \in \mathbb{U}(p^t, p^{t-i})$ es imagen de l elementos en $\mathcal{B}$ incongruentes módulo n pero congruentes módulo p^t, así que por el Lema 3.31 la suma

$$\sum_{j=1}^{d} r_j = l\left(\frac{p^{t-i}(p^t - p^i + 2)}{2}\right) = \frac{d}{p^{t-i}} \times \frac{p^{t-i}(p^t - p^i + 2)}{2} = d\left(\frac{p^t - p^i + 2}{2}\right)$$

es un múltiplo de d y por hipótesis de p^t. De esto último tenemos que para cada factor primo p de n, $\sum_{j=1}^{d} r_j$ es un múltiplo de p^t. Por lo dicho antes de dar inicio a la prueba, usando el hecho que $\mathbb{U}_n \cong \mathbb{U}_{p_1^{t_1}} \times \mathbb{U}_{p_2^{t_2}} \times \cdots \times \mathbb{U}_{p_s^{t_s}}$, podemos concluir que $\sum_{j=1}^{d} A_j$ es un múltiplo de $B^k - 1$, o sea, $n \in M_d(B)$.

Recíprocamente, supongamos que $n \in M_d(B)$. Si $\mathrm{ord}_p(B) \nmid k$, no hay nada que probar. Supongamos que $\mathrm{ord}_p(B) \mid k$, luego $r_j \equiv B^{jk} \equiv 1 \pmod{p}$. Nuevamente, bajo el mismo razonamiento que usamos en el párrafo anterior, $\pi(\mathcal{B})$ es un subgrupo de $\mathbb{U}_{p^t}$ de orden p^{t-i} para algún $1 \leqslant i \leqslant t$, es decir, de la forma $\mathbb{U}(p^t, p^{t-i})$, así que al aplicar el Lema 3.31,

$$\sum_{j=1}^{d} r_j = \frac{d}{p^{t-i}} \times \frac{p^{t-i}(p^t - p^i + 2)}{2} = d\left(\frac{p^t - p^i + 2}{2}\right).$$

Por lo dicho antes de dar inicio a la prueba, $n \in M_d(B)$ si y solo si $n \mid \sum_{j=1}^{d} r_j$, de modo que que $p^t \mid \sum_{j=1}^{d} r_j$ y por transitividad $p^t \mid d$. □

Finalmente, el siguiente resultado es una consecuencia inmediata del teorema que acabamos de probar.

Corolario 3.35. *Bajo las mismas hipótesis del Teorema 3.34, $n \in M_d(B)$ si y solo si para cada divisor primo p de $\gcd(B^k - 1, n)$, se tiene que $p^t \mid d$.*

Ejemplo 3.36. El Corolario 3.35 brinda una sencilla caracterización de la propiedad de

Midy. Del Ejemplo 3.23 es sabido que $42 \in M_6(11)$, donde $e = \text{ord}_{42}(11) = 6$. El único factor primo de $\gcd(42, 11^1 - 1) = 2$ es $p = 2$ y se verifica que $\text{ord}_2(11) = 1 \mid k = 1$.

Apéndice A

Algoritmos

En el desarrollo de una teoría siempre es indispensable tener a la mano ejemplos que ayuden al entendimiento de los conceptos, así como contraejemplos. La propiedad de Midy se enriquece precisamente con el estudio de ejemplos particulares debido a la extensa cantidad de resultados obtenidos, por lo que se hace de suma importancia usar herramientas computacionales que faciliten y agilicen el trabajo. Este apéndice contiene el *pseudocódigo* de los diferentes algoritmos usados a lo largo de esta tesis para la verificación de algunos teoremas, para ayudar a plantear preguntas y para resolver dudas. Cada uno de ellos fue implementado en SAGE[1].

Vamos a considerar como es usual los enteros n, B, e, d y k tales que $\gcd(n, B) = 1$ y $e = \mathrm{ord}_n(B) = dk$. Definamos provicionalmente $D_B(x, n)$ para cada $x \in \mathbb{U}_n$ como siendo el periodo de la fracción x/n en la base B, es decir,

$$\frac{x}{n} = 0.\overline{D_B(x, n)},$$

de donde es claro que

$$D_B(x, n) = \frac{x\,(B^e - 1)}{n}. \tag{A.1}$$

Recordemos de la Definición 3.1 que $n \in M_d(B)$ si $S_d(x) \equiv 0 \pmod{B^k - 1}$ para cada

[1] http://www.sagemath.org/

$x \in \mathbb{U}_n$. El primer algoritmo se basa en esta definición, donde se calcula $S_d(x)$ para cada $x \in \mathbb{U}_n$. Como entrada, se piden n, B y d y la salida es cada una de las sumas $S_d(x)$. Puesto que el Teorema 3.17 brinda una caracterización muy útil utilizando únicamente algún $x \in \mathbb{U}_n$, el segundo algoritmo que proponemos inmediatamente debajo del que acabamos de explicar, es un test para decidir si n tiene la propiedad de Midy utilizando la fracción $1/n$, donde la entrada es la misma que antes y en la salida retorna **cierto** o **falso**. A este procedimiento lo llamaremos MIDY(n, B, d).

Algoritmo 1 Calcular $S_d(x)$ para cada $x \in \mathbb{U}_n$.

Entrada: n y B primos relativos y d tal que $d \mid \mathrm{ord}_n(B)$.
Salida: $S_d(x)$ para cada $x \in \mathbb{U}_n$

1: $e \leftarrow \mathrm{ord}_n(B)$
2: $k \leftarrow e/d$
3: **para cada** $x \in \mathbb{U}_n$ **hacer**
4: $\quad S_d(x) \leftarrow 0$
5: $\quad$ **para** $j = 1$ hasta d **hacer**
6: $\quad\quad A_j \leftarrow \lfloor D_B(x,n)/B^{(d-j)k} \rfloor$
7: $\quad\quad D_B(x,n) \leftarrow D_B(x,n) \pmod{B^{(d-j)k}}$
8: $\quad\quad S_d(x) \leftarrow S_d(x) + A_j$
9: $\quad$ **fin para**
10: $\quad$ **imprimir** $S_d(x)$
11: **fin para**

Tanto el Algoritmo 1 como el Algoritmo 2 trabajan bajo el supuesto que $e = \mathrm{ord}_n(B)$ es conocido. En la práctica, e nunca es dado salvo algunos casos particulares. De la ecuación (A.1) es claro que el conocimiento de $D_B(x, n)$ surge como consecuencia inmediata del conocimiento de e, por lo que se hace necesario implementar un algoritmo para calcular e. Al inicio de la Sección 3.2, el sistema de ecuaciones (3.12) muestra precisamente el método para hallar e y esta es de hecho toda la esencia del siguiente algoritmo.

Hay varios inconvenientes que surgen computacionalmente cuando queremos calcular (A.1) conocido e y al computar la suma $S_d(x)$ alrededor de la aritmética en base B. Por ejemplo, sean $n = 39$ y $B = 7$. Si hacemos un llamado a la función ORDEN$(7, 39)$ tenemos que $e = 12$, luego si procedemos a usar la ecuación (A.1) para calcular $D_7(1, 39)$

Algoritmo 2 Decidir si $n \in M_d(B)$.

Entrada: n y B primos relativos y d tal que $d \mid \mathrm{ord}_n(B)$.
Salida: **cierto** si $S_d(1)$ es múltiplo de $B^k - 1$ y **falso** en caso contrario.

procedimiento MIDY(n, B, d)
    $e \leftarrow \mathrm{ord}_n(B)$
    $k \leftarrow e/d$
    $S_d(1) \leftarrow 0$
    para $j = 1$ hasta d **hacer**
        $A_j \leftarrow \lfloor D_B(n)/B^{(d-j)k} \rfloor$
        $D_B(n) \leftarrow D_B(n) \pmod{B^{(d-j)k}}$
        $S_d(1) \leftarrow S_d(1) + A_j$
    fin para
    si $S_d(1) \equiv 0 \pmod{B^k - 1}$ **entonces**
        devolver cierto ▷ $n \in M_d(B)$
    si no
        devolver falso ▷ $n \notin M_d(B)$
    fin si
fin procedimiento

Algoritmo 3 Calcular $e = \mathrm{ord}_n(B)$.

Entrada: n y B primos relativos.
Salida: $\mathrm{ord}_n(B)$

procedimiento ORDEN(B, n)
    $r \leftarrow B \pmod{n}$
    $e \leftarrow 1$ ▷ En el peor de los casos, $\mathrm{ord}_n(B) = 1$.
    mientras $r \neq 1$ **hacer**
        $r \leftarrow Br \pmod{n}$
        $e \leftarrow e + 1$
    fin mientras
    devolver e
fin procedimiento

tenemos que

$$D_7(1,n) = \frac{7^{12}-1}{39} = 354904800.$$

El problema aquí es que según la definición, $D_B(x,n)$ consiste de B-dígitos, es decir, está escrito en base B, pero hemos calculado $D_7(1,n)$ usando la aritmética decimal usual y es claro que ni 8 ni 9 son 7-dígitos. Esto se soluciona fácilmente usando una función que haga el cambio de base y existe un algoritmo genérico en el mundo de la computación.

Algoritmo 4 Cambio de base decimal a base B.

Entrada: Enteros m y B.
Salida: Representación de m en base B.

```
1: procedimiento BASE(m, B)
2:     b ← 0
3:     i ← 0
4:     mientras m ≠ 0 hacer
5:         r ← m (mód B)
6:         b ← b + r10^i
7:         m ← ⌊m/B⌋
8:         i ← i + 1
9:     fin mientras
10:    devolver b
11: fin procedimiento
```

En la línea 6 de este último algoritmo estamos multiplicando cada residuo r por potencias de 10, algo que a simple vista puede parecer contradictorio. La explicación tiene que ver con que las computadoras vienen prediseñadas para uso aritmético decimal. Para ilustrar esto de una mejor manera, sigamos con $n = 39$ y $B = 7$, donde teníamos que $D_7(1,39) = 354904800$. Puede verificarse rápidamente que si $m = D_7(1,39)$ entonces los residuos son, en orden sucesivo, $r = 5,0,6,2,3,4,6,3,5,1,1,0$. Del Ejemplo 3.18 sabemos que $D_7(1,39) = 011536432605$, entonces si queremos que la computadora nos muestre este resultado, debemos calcular la suma

$$\sum_{i=0}^{11} r10^i,$$

y esto es precisamente a lo que nos referíamos.

Ahora bien, dado que $e = 12 = dk$ y $D_7(1, 39) = 011536432605$, hagamos $d = 6$ y procedamos a calcular la suma $S_d(1)$. Partamos del hecho que $39 \in M_6(7)$, así que solo queremos verificar esta afirmación. Tenemos que $A_1 = 01$, $A_2 = 15$, $A_3 = 36$, $A_4 = 43$, $A_5 = 26$ y $A_6 = 05$, por lo que $S_6(1) = 1 + 15 + 36 + 43 + 26 = 126$. Deberíamos tener que $S_6(1) \equiv 0 \pmod{7^2 - 1}$, pero $126 \equiv 30 \pmod{7^2 - 1}$. Aquí el problema es que cada uno de los bloques A_j están representados en base 7 y la definición exige que la suma $S_6(1)$ se haga en base 7. Una primer solución es implementar un algoritmo que sume en base B, pero esta cuestión no es tan simple como parece. Una segunda solución, que es la que vamos a proponer, es hacer el cambio a la base decimal de cada bloque A_j y proceder a calcular la suma de ellos, por lo que se hace necesario la función inversa de la función $\textsc{Base}(m, B)$ que llamaremos $\textsc{InversaBase}(m, B)$. De este modo, tenemos en base 10 que $A_1 = 1$, $A_2 = 12$, $A_3 = 27$, $A_4 = 31$, $A_5 = 20$ y $A_6 = 5$ y por lo tanto $S_d(1) = 96 \equiv 0 \pmod{7^2 - 1}$, como queríamos.

Algoritmo 5 Cambio de base B a base decimal.

Entrada: Enteros m y B.
Salida: Representación decimal de m.

```
1: procedimiento InversaBase(m, B)
2:     b ← 0
3:     i ← 0
4:     mientras m ≠ 0 hacer
5:         r ← m (mód 10)
6:         b ← b + rB^i
7:         m ← ⌊m/10⌋
8:         i ← i + 1
9:     fin mientras
10:    devolver b
11: fin procedimiento
```

Si escogemos el camino guiado por el Algoritmo 1 y el Algoritmo 2 para verificar si $n \in M_d(B)$, todo lo que acabamos de explicar garantiza el buen funcionamiento de los programas. Si nos fijamos bien, el Algoritmo 4 surge bajo la necesidad de escribir el periodo de la fracción x/n en base B, no obstante, en el Algoritmo 3 hubiese bastado con

implementar una línea más para solucionar este problema, pues el sistema de ecuaciones (3.12) también muestra cómo hallar $D_B(x, n)$.

De igual forma, si modificamos ligeramente el pseudocódigo mostrado en el Algoritmo 3 podemos obtener otro test para saber si $n \in M_d(B)$ usando la suma $R_d(x)$, ya que recordando el Teorema 3.17, $n \in M_d(B)$ si y solo si $R_d(x) \equiv 0 \,(\text{mód } n)$ para algún $x \in \mathbb{U}_n$. Computacionalmente esta opción es más eficiente y la razón por la que hemos puesto como primera elección los algoritmos que involucran directamente la suma de los bloques del periodo de la fracción $1/n$, no es otra que dar a conocer las bases teóricas por las cuales dichos resultados funcionan y esclarecer algunas dudas que nacen de todo este estudio. También, porque no hay que desconocer que fue así cómo inicialmente se conoció la propiedad de Midy. A continuación mostramos este test.

Algoritmo 6 Decidir si $n \in M_d(B)$ bajo la suma $R_d(1)$.

Entrada: n y B primos relativos.
Salida: **cierto** si $R_d(1)$ es múltiplo de n y **falso** en caso contrario.

```
1: procedimiento MIDY2(n, B, d)
2:     r ← B (mód n)
3:     R_d(1) ← r
4:     mientras r ≠ 1 hacer
5:         r ← Br (mód n)
6:         R_d(1) ← R_d(1) + r
7:     fin mientras
8:     si R_d(1) ≡ 0 (mód n) entonces
9:         devolver cierto                          ▷ n ∈ M_d(B)
10:    si no
11:        devolver falso                           ▷ n ∉ M_d(B)
12:    fin si
13: fin procedimiento
```

Referencias Bibliográficas

[1] BURTON, D. (2007). *Elementary Number Theory.* McGraw-Hill, Avenue of the Americas, New York, 6th edition.

[2] GARCÍA-PULGARÍN, G., GIRALDO, H. (2009). Characterizations of Midy's property. *Integers: Electronic Journal of Combinatorial Number Theory*, 9(1):191–197.

[3] GINSBERG, B. (2004). Midy's (nearly) secret theorem - an extension after 165 years. *College Mathematics Journal*, 35(1):26–30.

[4] GUPTA, A., SURY, B. (2005). Decimal expansion of $1/p$ and subgroup sums. *Integers: Electronic Journal of Combinatorial Number Theory*, 5(1):1–11.

[5] HARDY, G., WRIGHT, E. (2008). *An Introduction to the Theory of Numbers.* Oxford University Press, Great Clarendon Street, Oxford, 6th edition.

[6] LEVEQUE, W. (1956). *Topics in Number Theory.* Addison-Wesley Publishing Company, Reading, Massachusetts.

[7] LEWITTES, J. (2007). Midy's theorem for periodic decimals. *Integers: Electronic Journal of Combinatorial Number Theory*, 7(1):8–18.

[8] MARTIN, H. (2007). Generalizations of Midy's theorem on repeating decimals. *Integers: Electronic Journal of Combinatorial Number Theory*, 7(1):19–25.