UNIVERSIDAD NACIONAL

SANTIAGO ANTÚNEZ DE MAYOLO

FACULTAD DE CIENCIAS

ESCUELA PROFESIONAL DE MATEMÁTICA

TEOREMA DE NÚMEROS PRIMOS Y DAVENPORT COMO CASO PARTICULAR DE LA CONJETURA DE SARNAK

TESIS PARA OPTAR EL TÍTULO DE

LICENCIADO EN MATEMÁTICA

PRESENTADO POR: Bach. Julian Lázaro Aguirre

ASESOR: Msc. Dik Dani Lujerio Garcia

Huaraz - Perú

2022

Nº Registro: T016

ACTA DIGITAL DE SUSTENTACIÓN DE TESIS N° 003-2022

Los Miembros del Jurado de la Revisión y Sustentación de Tesis de la Escuela Académico Profesional de Matemática de la Facultad de Ciencias, designados mediante Resolución de Consejo de Facultad N° 069-2022-UNASAM-FC, se reunieron el día martes 22 de noviembre de 2022, a horas 08:00 a.m. en el Auditorio virtual de la Facultad de Ciencias en acto público para evaluar la Sustentación de Tesis, presentado por el:

Bachiller : **Julian Lázaro Aguirre**

Tesis Titulada : **"Teorema de Números Primos y Davenport como caso Particular de la Conjetura de Sarnak".**

Después de la Sustentación y las respuestas a las preguntas, el Jurado lo declara APROBADO POR UNANIMIDAD para optar el Título Profesional de Licenciado en Matemática, con el calificativo de DIECISIETE (17)

En señal de conformidad y para constancia, firmamos la presente ACTA, siendo las 9:36 a.m. del mismo día y año.

Huaraz, 22 de noviembre de 2022.

Mag. Hever Luis Hinostroza Encarnación
Presidente

Mag. Elí Monzón Briceño
Secretario

Mag. Víctor Alberto Pocoy Yauri
Vocal

Mag. Dik Dani Lujerio García
Asesor

LINK DE GRABACIÓN DE SUSTENCIÓN:
https://unasam.sharepoint.com/sites/UNIDADDEGRADOSYTTULOSFC-UNASAM/Documentos%20compartidos/General/Recordings/Reuni%C3%B3n%20en%20_General_-20221122_081929-Grabaci%C3%B3n%20de%20la%20reuni%C3%B3n.mp4?web=1

NOMBRE DEL TRABAJO

TEOREMA DE NÚMEROS PRIMOS Y DAV ENPORT COMO CASO PARTICULAR DE L A CONJETURA DE SARNAK

AUTOR

JULIAN LÁZARO AGUIRRE

RECUENTO DE PALABRAS

24730 Words

RECUENTO DE CARACTERES

100004 Characters

RECUENTO DE PÁGINAS

115 Pages

TAMAÑO DEL ARCHIVO

3.2MB

FECHA DE ENTREGA

May 10, 2023 8:15 AM GMT-5

FECHA DEL INFORME

May 10, 2023 8:17 AM GMT-5

17% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base d

- 14% Base de datos de Internet
- Base de datos de Crossref
- 11% Base de datos de trabajos entregados
- 8% Base de datos de publicaciones
- Base de datos de contenido publicado de Crossr

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Material citado
- Coincidencia baja (menos de 8 palabras)

Miembros del Jurado

Msc. Hever Luis HINOSTROZA ENCARNACIÓN _____

Presidente

Msc. Elí MONZÓN BRICEÑO _____

Secretario

Msc. Victor Alberto POCOY YAURI _____

Vocal

Dedicado a mis padres

y hermanos

Agradecimientos

Agradezco principalmente a Dios, por la salud, por la vida y por muchas cosas que nunca me ha faltado.

A mis padres, por darme cariño, todo amor, compresión y apoyo incondicional.

A mi orientador Dik Dani Lujerio Garcia por su amistad y su apoyo en la realización de este informe.

A la UNASAM en especial a la Escuela Profesional de Matemática por brindarme excelentes docentes en mi formación profesional.

Por último pero no por eso menos importante a todos mis familiares y amigos.

Índice

Resumen VII

Abstract VIII

Lista de símbolos 1

Índice de figuras 2

I. INTRODUCCIÓN 3

1.1. Introducción . . . 3
1.2. Justificación . . . 4
1.3. Planteamiento del problema . . . 5
1.4. Objetivos . . . 5
1.4.1. Objetivo general . . . 5
1.4.2. Objetivos específicos . . . 5
1.5. Hipótesis . . . 6

II. MARCO TEÓRICO 7

2.1. Antecedentes del problema . . . 7
2.2. Conceptos básicos de teoría de números . . . 8
2.2.1. Números Primos . . . 8
2.2.2. Algunos definiciones y resultados . . . 11
2.2.3. Notación O grande de Bachmann-Landau . . . 14
2.3. Funciones aritméticas . . . 17
2.3.1. Preliminares . . . 17
2.3.2. Función de Möbius . . . 19
2.3.3. Convoluciones de Dirichlet . . . 20
2.3.4. Función de Von Mangoldt . . . 24
2.3.5. Sumas parciales . . . 26
2.4. Identidad de Abel . . . 31

2.5. Funciones de Tchebychev 36
2.6. Nociones de sistemas dinámicos discretos 39
2.6.1. Círculo unitario 39
2.6.2. Sistemas dinámicos discretos 41
2.7. Introducción a la entropía topológica 44
2.7.1. Entropía a través de coberturas 44
2.7.2. Bola dinámica 50
2.7.3. Entropía a través de conjuntos generadores 53
2.7.4. Entropía a través de conjuntos separados 57
2.7.5. Equivalencia de las tres definiciones de la entropía 61

III. METODOLOGÍA **66**
3.1. Tipo de investigación 66
3.2. Diseño de investigación 66
3.3. Población y muestra 67

IV. RESULTADOS **68**
4.1. Teorema de Números Primos - TNP 68
4.1.1. Enunciado 68
4.1.2. Esbozo de la prueba de TNP 70
4.2. Equivalencia a TNP 72
4.2.1. Preparación 72
4.2.2. Prueba del Teorema 4.2.1 75
4.3. Teorema de Davenport 80
4.4. Aspectos dinámicos de la función de Möbius 82
4.4.1. Función libre de cuadrados 82
4.4.2. Función de Möbius no es determinsitico 84
4.4.3. La conjetura de Sarnak 88
4.4.4. Conjetura de Sarnak implica TNP 90
4.4.5. Conjetura de Sarnak implica Teorema de Davenport 91

V. CONCLUSIONES **92**

VI. RECOMENDACIONES **93**

Referencias **94**

A. ESPACIOS MÉTRICOS **96**

A.1. Espacio topológico 96

A.2. Espacio métrico 97

Resumen

En este trabajo de investigación presentamos dos ejemplos para la Conjetura de Sarnak, los cuales son el Teorema de Número Primos y el Teorema de Davenport.

Se presenta algunos resultados básicos sobre la Teoría Analítica de Números y la Entropía topológica de un sistema dinámico discreto.

Presentamos un esbozo de la prueba del Teorema de Números Primos y una demostración detallada del Teorema 4.2.1, lo cual afirma una equivalencia a este resultado.

Palabras Claves: Números primos, función de Möbius, funciones aritméticas, sistemas dinámicos, entropía topológica, aleatoriedad.

Abstrac

In this research work we present two examples for the Sarnak Conjecture, which are the Prime Number Theorem and Davenport's Theorem.

Some basic results are presented on the Analytic Number Theory and the Topological entropy of a discrete dynamical system.

We present a sketch of the proof of the Prime Number Theorem and a detailed proof of Theorem 4.2.1, which asserts an equivalence to this result.

Keywords: Prime numbers, Möbius function, arithmetic functions, dynamical systems, topological entropy, randomness.

Lista de símbolos

$\#E$	Cardinal del conjunto E
$\boldsymbol{\mu}$	Función de Möbius
$\emptyset$	Conjunto vacío
γ	Constante gamma de Euler
$\lfloor x \rfloor$	Máximo entero de x
$\ln x$	Logaritmo natural de x
$\mathbb{C}$	Conjunto de números complejos
$\mathbb{N}$	Conjunto de números naturales, es decir, $\{1, 2, 3, 4, ...\}$
$\mathbb{N}^*$	$\mathbb{N} \cup \{0\}$
$\mathbb{P}$	Conjunto de números primos, es decir, $\{2, 3, 5, 7, ...\}$
$\mathbb{R}$	Conjunto de números reales
$\mathbb{R}^+$	Conjunto de números reales positivos
$\mathbb{Z}$	Conjunto de números enteros
$\pi(x)$	Función contadora de números primos menores o iguales a x
$h_{top}(T)$	Entropía topológica de una transformación T
TNP	Teorema de Números Primos

Índice de figuras

1. Región hiperbólica. 29
2. Región de la hipérbola. 35
3. Figura de la Proposición 2.6.2. 40
4. Rotación R_α. 43
5. Conjunto generador. 54
6. Gráfico comparativo de $\pi(x)$ y $\frac{x}{\ln x}$. 69
7. Valores de $\mu(n)$ 84

I. INTRODUCCIÓN

1.1. Introducción

En el clásico libro del matemático alemán Edmundo Landau, él escribe: "Gordon dijo algo como: 'La teoría de números es útil porque, después de todo, podemos obtener un doctorado en ella' " **(Landau, 2002, pág. 40)**. Esto nos da una idea de la visión que teníamos de la teoría de números, algo hermoso y majestuoso, pero no muy útil. Sin embargo, todo eso cambió después de los años de 1940, con la aplicación en la criptografía moderna, cuya base es esencialmente la teoría de números y, en particular, la teoría de números primos.

Sabemos que desde la antigüedad los números primos representan el misterio mas fascinante que nos enfrentamos en la búsqueda de nuestro conocimiento. ¿Cómo predecir cual va ser el siguiente número primo de una serie? ¿cuál es la distancia que existen entre ellos? ¿Existe alguna fórmula que lo genere? ¿Cómo se distribuyen en los números naturales? **Du Sautoy (2007)**.

Como no es posible encontrar una fórmula general que genera los números primos, entonces tenia que ser pensando de diferente manera, así, fue conjeturado por Gauss y Legendre, lo cual fue probado casi 100 año después por Hadamard y De la Vallée Poussin (independientemente) el famoso *Teorema de Números Primos* que afirma la distribución de los números primos en los naturales.

Por otro lado, la función $\boldsymbol{\mu}$ de Möbius juega un papel importante en la distrubución de los números primos y, en 1937, Davenport demuestra la correlación del comportamiento de esta función con las funciones en el círculo unitario. Este resultado es llamado *Teorema de Davenport*.

Una de las áreas de la matemática bastante investigado en estos últimos años es *Sistemas Dinámicos* lo cual tienes sus origines con los trabajos de Kepler, Newton entre otros. Uno de los creadores de la teoría moderna de sistemas dinámicos es el matemático francés H. Poincaré. La pregunta natural que surge es: ¿Qué es un sistema dinámico?. Para responder esta pregunta tenemos: Dado un espacio X (topológico, métrico, etc.) y una transformación $T : X \to X$ lo cual puede tener diversas propiedades (continua, sobreyectiva, etc.). Entonces, básicamente la *dinámica* es tomar un punto $x \in X$ y ver por la órbita de ese punto, es decir, $\{x, T(x), T^2(x), T^3(x), ...\}$ e intentar describir lo máximo posible la estructura de esa órbita. Así, un sistema dinámico es el par (X, T), donde X es un espacio y T una transformación.

Detallado en el libro de **Iwaniec y Kowalski (2004)**, existe una antigua y famosa heurística llamado *Principio de aleatoriedad de Möbius*, que afirma que los símbolos $-1, 0$ y 1 en la sucesión generado por la función de Möbius se comportan de forma tan caótica que dicho función no tiene correlación con cualquier sucesión razonablemente simple (ver sub-sección 4.4.3). En 2010, este principio fue interpretado de forma precisa en contexto de sistemas dinámicos por P. Sarnak, lo cual es conocido como la *Conjetura de Sarnak*.

Para entender y familiarizarnos con estos resultados, vamos a presentar nociones básicas sobre la Teoría Analítica de Números y la Entropía topológica de un sistema dinámico discreto en el Capítulo II.

Finalmente, en el Capítulo IV, probamos que el Teorema de Números Primos y el Teorema de Davenport satisfacen la Conjetura de Sarnak.

1.2. Justificación

El estudio de los sistemas dinámicos tiene aplicaciones en una amplia variedad de campos como la física, la ingeniería, la biología, etc o en otras áreas de la matemática, como en este trabajo de investigación, que es aplicado a teoría de números.

La función de Möbius $\boldsymbol{\mu}$ (ver Definición 2.3.5) es definido en los números naturales que toma valores $-1, 0$ y 1 (dependiendo de como está factorizado el número natural en función de primos). Ahora, sumemos estos valores, es decir, vamos a sumar a $\boldsymbol{\mu}(1), \boldsymbol{\mu}(2), \boldsymbol{\mu}(3), ..., \boldsymbol{\mu}(n) \in \{-1, 0, 1\}$ y denotemos esa suma por S_n, o sea,

$$S_n = \sum_{k=1}^{n} \boldsymbol{\mu}(k).$$

¿Será que S_n es pequeña o grande? o ¿Podemos acotar a S_n por una constante positiva?. Al principio parece ser fácil, pero lo que hace interesante a estas preguntas es que para valores de n suficientemente grandes que ocurre. Una manera de ver que tan complejo es sumar estos valores de la función de Möbius para números grandes, es encontrar una contante $C > 0$ tal que

$$|S_n| \leq Cn^{\frac{1}{2}+\varepsilon},$$

para cualquier $\varepsilon > 0$ e n grande. Pues este resultado es equivalente a uno de los problemas del milenio, llamado la *Hipótesis de Riemann*, que dice: Todo cero no trivial de la función zeta de Riemann están localizados en la recta vertical $\{1/2 + ib : b \in \mathbb{R}\}$. En conclusión, para probar la hipótesis de Riemann, basta sumar $-1, 0, 1$ y que sucede para n grande.

Entonces, en la sucesión $\{\boldsymbol{\mu}(k)\}_{k=1}^{\infty}$ los valores $-1, 0, 1$ aparecen en cierto sentido "aleatoriamente" (esto será justificado mas adelante vía entropía topológica).

Por otro lado, los números primos tienen diversas aplicaciones, como en la criptografía moderna, y el estudio de la distribución de números primos en los naturales está íntimamente ligado a la función de Möbius (Teorema de Números Primos).

1.3. Planteamiento del problema

¿Es posible demostrar que el *Teorema de Números Primos* y *Davenport* satisfacen la *Conjetura de Sarnak*?

1.4. Objetivos

1.4.1. Objetivo general

Demostrar que el *Teorema de Números Primos* y *Davenport* satisfacen la *Conjetura de Sarnak*.

1.4.2. Objetivos específicos

- Estudiar conceptos y propiedades necesarios para entender la conjetura de Sarnak, como: Función de Möbius y la entropía topológica de un sistema dinámico discreto.
- Analizar el esbozo de la demostración del Teorema de Números Primos.

- Detallar y analizar que el Teorema de Números Primos es equivalente al valor medio de sumatorio de la función de Möbius $\boldsymbol{\mu}(n)$ para n suficientemente grande es nula.
- Analizar el enunciado del Teorema de Davenport.

1.5. Hipótesis

Considerando funciones y espacios métricos adecuados, podemos probar que el *Teorema de Números Primos* y *Teorema de Davenport* son casos particulares de la *Conjetura de Sarnak*.

II. MARCO TEÓRICO

2.1. Antecedentes del problema

En Teoría de Números, el *Teorema de Números Primos* es uno de los resultados importantes en la distribución de números primos. Este teorema fue planteado, independientemente, por Gauss en 1792 (o en 1793, publicado en *Later to Enkene* - 1849) y por Legendre en 1798 (publicado en *Essai sur la Theorie des Nombres*). En 1986, fue demostrado, independientemente, por Hadamard y De la Vallée Poussin (ver introducción historial de **Apostol (1998)**). Pruebas elementales, fue dada posteriormente, por ejemplo la prueba de Atle Selberg y Paul Erdös.

La correlación de comportamiento de la función de Möbius con las funciones en el círculo unitario fue probado por Harold Davenport en **Davenport (1937)**, este resultado es conocido como *Teorema de Davenport*. Otra prueba de este teorema puede ser consultado en **Iwaniec y Kowalski (2004)**.

Las demostraciones de los dos teoremas mencionados anteriormente son extensas, aunque sea una prueba elemental o una prueba corta, usan artillería de la Teoría Analítica de Números y Variable Compleja, como: Caracteres de Direchlet, L-funciones, función zeta de Riemann, método de Vinogradov, Teorema Integral de Cauchy, etc.

Por otro lado, el problema planteado por Peter Sarnak en **Sarnak (2011)**, que afirma que la función de Möbius es asintóticamente ortogonal a cualquier sucesión con entropía topológica cero, en los últimos años (desde 2011) se ha puesto en manifiesto por muchos matemáticos y, de hecho, se ha avanzando mucha teoría sobre ella en intento de probarlo.

2.2. Conceptos básicos de teoría de números

Las definiciones y resultados presentados en esta sección pueden encontrarse en cualquier libro de Teoría de Números, por ejemplo en **Apostol (1998)** o en **Landau (2002)**.

2.2.1. Números Primos

Usamos la notación clásica del conjunto de números enteros por $\mathbb{Z}$ y el conjunto de enteros positivos (números naturales) por $\mathbb{N}$, es decir, $\mathbb{N} = \{1, 2, 3, ...\}$. También denotamos por $\mathbb{N}^*$ el conjunto $\{0, 1, 2, 3, ...\}$, es decir, $\mathbb{N}^* = \mathbb{N} \cup \{0\}$.

Definición 2.2.1 Dados cualquier $d, n \in \mathbb{N}$, diremos que d *divide* a n, denotado por $d|n$, si $n = kd$, para algún $k \in \mathbb{N}$.

Tenemos algunas propiedades.

Proposición 2.2.1 *Para $d, n, m, n \in \mathbb{N}$, es válido,*

1. *$n|n$ (reflexiva);*
2. *$d|n$ y $n|m$ implica que $d|m$ (transitiva);*
3. *$d|n$ y $d|m$ implica que $d|(am + bn)$ (lineal).*

Demostración. 1). inmediato.

2). Si $d|n$ y $n|m$; entonces existe algún $c, k \in \mathbb{N}$ tal que $n = cd$ y $m = kn$, entonces, $m = kn = kcd = (kc)d$, esto implica que, $d|m$.

3). Si $d|n$ y $d|m$, entonces existe algún $c, k \in \mathbb{N}$ tal que $n = cd$ y $m = kd$. Luego, $am + bn = a(kd) + b(cd) = (ak + bc)d$, y sigue que $d|(am + bn)$.

■

A continuación presentamos una de las definiciones importantes, llamados *números primos*, los cuales son el análogo en matemáticas a las partículas elementales de la física.

Definición 2.2.2 (Número Primo) Un número $p \in \mathbb{N}$ mayor que 1 es llamado un *número primo* si es divisible únicamente por 1 y p.

De la definición, si $n \in \mathbb{N}$ no es un número primo, entonces es llamado *número compuesto*.

Ejemplo 2.2.1 Los números $2, 3, 5, 7, 11, 13, 17, 19$, etc. son números primos, pues son divisibles por 1 y por el mismo.

Notación. Denotamos por $\mathbb{P}$ el conjunto de números primos, es decir,

$$\mathbb{P} := \{2, 3, 5, 7, ...\}.$$

Existen infinitos números primos, como fue demostrado 300 a.C por Euclides, específicamente en el libro: *Elementos* (Libro IX - Proposición 20). Reproduzcamos esa prueba tan simple y hermosa, pero antes veamos otro teorema que también es debido a Euclides.

Teorema 2.2.1 (Teorema Fundamental de Aritmética) *Cualquier $n \in \mathbb{N}$ mayor que 1 puede ser escrito de forma única (a menos de orden de factores) como producto de números primos, es decir, existen únicos $p_1, p_2, ..., p_k \in \mathbb{P}$ tal que*

$$n = p_1 \cdot p_2 \cdots p_k.$$

Demostración. Primeramente, mostremos la existencia de una descomposición para $n \in \mathbb{N}$ mayor que 1 en producto de primos. La prueba sera hecha por inducción. Si $n = 2$, entonces existe una descomposición trivial, ya que 2 es un número primo. Suponga que existe una descomposición en producto de primos para números naturales menores que n. Mostremos que también es válido para n. Si n es un número primo, admite una descomposición trivial y acabo la demostración. Si n no es un número primo, entonces existe $1 < d < n$ tal que $n = dk$ para $1 < k < n$. Ahora, como $1 < d, k < n$, entonces por la hipótesis de inducción, existen números primos $p_1, p_2, ..., p_i$ y $q_1, q_2, ..., q_j$ tal que

$$d = p_1 \cdot p_2 \cdots p_i \quad \text{y} \quad k = q_1 \cdot q_2 \cdots q_j.$$

Luego,

$$n = dk = p_1 \cdot p_2 \cdots p_i \cdot q_1 \cdot q_2 \cdots q_j.$$

Finalmente, demostremos la unicidad de la descomposición. Probemos también por inducción para $n \in \mathbb{N}$ mayor que 1. Si $n = 2$, entonces es válido. Así, suponga que los números menores que n pueden ser escritos como producto de números primos de

forma única. Probemos que este hecho es válido para n. Si n es primo, entonces acabo la demostración. Ahora si n no es primo, entonces n es escrito de la forma

$$n = p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_m,$$

donde $p_1, ..., p_k, q_1, ..., q_m \in \mathbb{P}$. Probemos que $m = k$.

Como $p_1|(p_1 \cdot p_2 \cdots p_k)$ entonces, $p_1|(q_1 \cdot q_2 \cdots q_m)$, luego, p_1 divide a algún primo $q_1, q_2, ..., q_m$, digamos a q_1 (note que si $p_1|q_3$ podemos reordenar los sub-índices de tal manera que el primo en posición 3 quede en la posición 1), así, como $p_1, q_1 \in \mathbb{P}$, entonces $p_1 = q_1$. Luego,

$$\frac{n}{p_1} = p_2 \cdot p_3 \cdots p_k = q_2 \cdot q_3 \cdots q_m$$

Note que, $\frac{n}{p_1} \in \mathbb{N}$. Si $m > 1$ o $k > 1$, entonces $1 < \frac{n}{p_1} < n$ y por la hipótesis de inducción $\frac{n}{p_1}$ es escrito como producto de números primos de forma única. Por lo tanto, $k = m$.

■

Teorema 2.2.2 (Euclides - 300 a.C) *Existen infinitos números primos.*

Demostración. Suponga por contradicción que existe finitos números primos, digamos, $p_1, p_2, ..., p_n$, y sea, $N = 1 + p_1 \cdot p_2 \cdots p_n$. Note que $N > 1$ y por supuesto que N no es primo, pues es mayor que cada p_j, para $j = 1, 2, ..., n$. Así, debido al Teorema Fundamental de Aritmética, existe ℓ, $1 \leq \ell \leq n$ tal que $p_\ell|N$ y, como $p_\ell|(p_1 \cdot p_2 \cdots p_n)$, tenemos que $p_\ell|(N - p_1 \cdot p_2 \cdots p_n)$. Como, $N - p_1 \cdot p_2 \cdots p_n = 1$, se tiene que $p_\ell|1$, absurdo.

Por lo tanto, existen infinitos números primos.

■

Observación 2.2.1 Debido al Teorema Fundamental de Aritmética, cualquier $n \in \mathbb{N}$ mayor que 1 puede ser escrito de la forma

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k} = \prod_{j=1}^{k} p_j^{a_j},$$

donde, $p_1, p_2, ..., p_k \in \mathbb{P}$ y $a_1, a_2, ..., a_k \in \mathbb{N}$. De aquí para adelante, no mencionaremos el nombre del teorema, simplemente escribimos n como fue escrito arriba.

Comentario. Existen muchos resultados y problemas abiertos sobre números primos desde la antigüedad, por ejemplo la *Conjetura de los Primos Gemelos*[1] (planteado por Euclides - 300 a.C) que afirma: *¿Existen infinitos primos gemelos?*. Este problema lleva sin resolver mas de 2000 mil años.

Otro problema sin resolver es sobre los *primos de Mersenne* que son de la forma $2^n - 1$ para $n > 1$. *¿Existen infinitos primos de Mersenne?*. Hasta ahora es conocido un primo de Mersenne con mas de 24 millones de cifras.

Así, una de las cuestiones investigadas desde la antigüedad sobre los números primos es de como ellos se distribuyen en los enteros positivos, con que frecuencia ocurre y cual es la distancia que existe entre ellos.

2.2.2. Algunos definiciones y resultados

Denotamos por $\mathbb{R}$ el conjunto de los números reales.

Definición 2.2.3 Dado $x \in \mathbb{R}$, definimos por

$$\lfloor x \rfloor := \text{máx}\{n \in \mathbb{Z} : n \leq x\}$$

el máximo entero no mayor que x.

Observación 2.2.2 Note que,

$$\lfloor x \rfloor = \sum_{\substack{n \in \mathbb{N} \\ n \leq x}} 1,$$

pues,

$$\sum_{\substack{n \in \mathbb{N} \\ n \leq x}} 1 = \underbrace{1 + 1 + \cdots + 1}_{n \text{ veces}} = n = \text{máx}\{n \in \mathbb{Z} : n \leq x\}.$$

Proposición 2.2.2 *Para $x \in \mathbb{R}$, se tiene, $0 \leq x - \lfloor x \rfloor < 1$.*

Demostración. Sea $\lfloor x \rfloor = n$, entonces por la definición, n es el mayor entero tal que $n \leq x$. Luego, $n \leq x < n + 1$, así,

$$0 \leq x - n < 1 \Rightarrow 0 \leq x - \lfloor x \rfloor < 1.$$

■

[1] Un primo es gemelo si la diferencia entre ellos es 2, es decir, $(p, q) \in \mathbb{P} \times \mathbb{P}$ tal que $p - q = 2$. Ejemplo, $(3, 5), (5, 7), (11, 13)$, etc. son primos gemelos.

Observación 2.2.3 Para cualquier $x \in \mathbb{R}$, note que,

$$x = \lfloor x \rfloor + \{x\},$$

donde, $\{x\}$ representa la parte fraccionaria de x.

Ejemplo 2.2.2 Para $x = 2.7$, se tiene, 2.7= 2 + 0.7, pues, $\lfloor 2.7 \rfloor = 2$ y $\{2.7\} = 0.7$.

Notación. De aquí en adelante, se denota por $\mathbf{\ln x}$ el logaritmo natural de x, o sea, logaritmo de x en la base e (número de Euler).

A continuación definimos la constante de *Euler*, de hecho tal constante existe y esta acotado entre $\frac{1}{2}$ y 1.

Definición 2.2.4 (Constante de Euler) La constante γ de Euler es definida por

$$\gamma := \lim_{n\to\infty} \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \ln n\right).$$

Veamos en la siguiente proposición que este constante envuelve a una integral.

Proposición 2.2.3 *Es valido que,* $\gamma = 1 - \displaystyle\int_1^\infty \frac{\{t\}}{t^2} dt.$

Demostración. Como $\{t\} = t - \lfloor t \rfloor$, note que,

$$\begin{aligned}
\int_1^\infty \frac{\{t\}}{t^2} dt &= \sum_{k=1}^{\infty} \int_k^{k+1} \frac{t - \lfloor t \rfloor}{t^2} dt = \lim_{r\to\infty} \sum_{k=1}^{r} \int_k^{k+1} \frac{t - \lfloor t \rfloor}{t^2} dt \\
&= \lim_{r\to\infty} \sum_{k=1}^{r} \left(\int_k^{k+1} \frac{1}{t} dt - \int_k^{k+1} \frac{\lfloor t \rfloor}{t^2} dt \right) \\
&= \lim_{r\to\infty} \sum_{k=1}^{r} \left(\ln(k+1) - \ln k - k \int_k^{k+1} \frac{1}{t^2} dt \right) \text{ (pues } \lfloor t \rfloor = k \text{ en } [k, k+1)) \\
&= \lim_{r\to\infty} \sum_{k=1}^{r} \left((\ln(k+1) - \ln k + \frac{k}{k+1} - \frac{k}{k} \right) \\
&= \lim_{r\to\infty} \left(\sum_{k=1}^{r} (\ln(k+1) - \ln k) - \sum_{k=1}^{r} \frac{1}{k+1} \right) \\
&= \lim_{r\to\infty} \left(\ln(r+1) - \sum_{k=1}^{r} \frac{1}{k+1} \right) \\
&= \lim_{r\to\infty} \left(\ln(r+1) - \sum_{m=1}^{r+1} \frac{1}{m} + 1 \right), \quad \text{tomando } m = k+1.
\end{aligned}$$

Sea $r+1=n$. Note que, cuando $r\to\infty$, entonces $n\to\infty$. Luego,

$$\int_1^{\infty}\frac{\{t\}}{t^2}dt=\lim_{n\to\infty}\left(\ln n-\sum_{m=1}^{n}\frac{1}{m}+1\right).$$

Entonces,

$$\begin{aligned}1-\int_1^{\infty}\frac{\{t\}}{t^2}dt&=1-\lim_{n\to\infty}\left(\ln n-\sum_{m=1}^{n}\frac{1}{m}+1\right)=1+\lim_{n\to\infty}\left(\sum_{m=1}^{n}\frac{1}{m}-\ln n\right)-1\\&=\lim_{n\to\infty}\left(\sum_{m=1}^{n}\frac{1}{m}-\ln n\right):=\gamma.\end{aligned}$$

■

Sabemos que para $|x|<1$, la serie geométrica es convergente, es decir,

$$\sum_{n=0}^{\infty}x^n=\frac{1}{1-x}.$$

Presentamos otro resultado clásico que es la solución al *Problema de Basilea* debido al gran matemático Euler. En la actualidad, existen diversas formas de probar este resultado y una de ellas lo presentamos en la siguiente proposición.

Proposición 2.2.4 *Se tiene,*

$$\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{\pi^2}{6}.$$

Demostración. Usando técnicas de integración, calculamos que

$$\int_0^1\int_0^1\frac{1}{1-xy}dxdy=\frac{\pi^2}{6}.$$

Luego, usando la serie geométrica,

$$\begin{aligned}\frac{\pi^2}{6}&=\int_0^1\int_0^1\frac{1}{1-xy}dxdy=\int_0^1\int_0^1\sum_{n=0}^{\infty}(xy)^n dxdy\quad(\text{pues, } xy<1)\\&=\sum_{n=0}^{\infty}\left(\int_0^1 x^n dx\right)\left(\int_0^1 y^n dy\right)=\sum_{n=0}^{\infty}\frac{1}{n+1}\frac{1}{n+1}\\&=\sum_{n=0}^{\infty}\frac{1}{(n+1)^2}=\sum_{n=1}^{\infty}\frac{1}{n^2}.\end{aligned}$$

■

2.2.3. Notación O grande de Bachmann-Landau

La notación **O** grande (mayúscula) es debido a los matemáticos Edmund Landau y Paul Bachmann (conocido también como *notación asintótica*) que describe el comportamiento límite de una función cuando el argumento tiende hacia un valor particular o infinito.

Notación. Denotamos por $\mathbb{R}^+$ el conjunto de números reales positivos y por $\mathbb{C}$ el conjunto de números complejos, es decir,

$$\mathbb{R}^+ := \{x \in \mathbb{R} : x > 0\} \quad \text{y} \quad \mathbb{C} := \{a + ib : a, b \in \mathbb{R}\}.$$

Definición 2.2.5 (Notación O grande) Sean las funciones $f : \mathbb{R} \to \mathbb{R}$ (o $\mathbb{C}$) y $g : \mathbb{R} \to \mathbb{R}^+$. Si existe una constante $C > 0$ y $x_0 \in \mathbb{R}$ tal que,

$$|f(x)| \leq Cg(x) \ \ \forall\ x \geq x_0,$$

escribimos,

$$f(x) := \mathrm{O}(g(x)).$$

Ejemplo 2.2.3 Sea $f(x) = 6x^3 + 3x^2 - 7x + 50$ y $g(x) = x^3$. Entonces, $f(x) = \mathrm{O}(g(x))$, pues,

$$\begin{aligned} |f(x)| = |6x^3 + 3x^2 - 7x + 50| &\leq 6|x^3| + 3x^2 + 7|x| + 50 \\ &\leq 6x^3 + 3x^3 + 7x^3 + 50x^3 \ \ \text{para todo } x \geq 1 \\ &= 66x^3. \end{aligned}$$

Así, encontramos $C = 66$ y $x_0 = 1$.

De forma análoga, escribimos

$$f(x) = g(x) + \mathrm{O}(h(x)),$$

si existe una constante $C > 0$ y $x_0 \in \mathbb{R}$ tal que

$$|f(x) - g(x)| \leq Ch(x) \ \ \forall\ x \geq x_0.$$

Ejemplo 2.2.4 Tenemos que, $\lfloor x \rfloor = x + \mathrm{O}(1)$, pues por la Proposición 2.2.2,

$$|\lfloor x \rfloor - x| < 1,$$

donde, $C = 1$ y cualquier $x \in \mathbb{R}^+$.

Veamos algunas propiedades de O grande.

Proposición 2.2.5 *Sean las funciones* $f, f_1, f_2 : \mathbb{R} \to \mathbb{R}$ *(o* $\mathbb{C}$*)* y $g, g_1, g_2 : \mathbb{R} \to \mathbb{R}^+$. *Entonces valen las siguientes afirmaciones:*

1. $O(O(g(x))) = O(g(x))$;
2. *Si* $f_1(x) = O(g_1(x))$ y $f_2(x) = O(g_1(x))$, *entonces* $f_1(x)f_2(x) = O(g_1(x)g_2(x))$;
3. $g_1(x)O(g(x)) = O(g_1(x)g(x))$;
4. *Si* $f_1(x) = O(g_1(x))$ y $f_2(x) = O(g_1(x))$, *entonces*

$$f_1(x) \pm f_2(x) = O(\text{máx}\{g_1(x), g_2(x)\});$$

5. *Sea una constante* $K > 0$ y $f(x) = O(g(x))$, *entonces* $Kf(x) = O(g(x))$;
6. *Si* g *es integrable en* $(a, x) \subset \mathbb{R}$, *entonces*

$$\int_a^x O(g(t))dt = O\left(\int_a^x g(t)dt\right).$$

Demostración. La prueba es fácil, veamos:

1). Sea $g_1(x) = \mathrm{O}(g(x))$ y $f(x) = \mathrm{O}(g_1(x))$. Entonces, existen $C_1, C_2 > 0$ y $x_1, x_2 \in \mathbb{R}$ tal que

$$g_1(x) \leq C_1 g(x) \ \forall\ x \geq x_1 \quad \text{y} \quad |f(x)| \leq C_2 g_1(x) \ \forall\ x \geq x_2.$$

Tomando $x_0 = \text{máx}\{x_1, x_2\}$ y $C = C_1C_2$, tenemos, $|f(x)| \leq Cg(x) \ \ \forall\ x \geq x_0$. Luego,

$$\mathrm{O}(g(x)) = f(x) = \mathrm{O}(g_1(x)) = \mathrm{O}(\mathrm{O}(g(x))).$$

2). Si $f_1(x) = \mathrm{O}(g_1(x))$ y $f_2(x) = \mathrm{O}(g_1(x))$, entonces existen constantes $C_1, C_2 > 0$ y $x_1, x_2 \in \mathbb{R}$ tal que

$$|f_1(x)| \leq C_1 g_1(x) \ \ \forall\ x \geq x_1 \ \ \text{y} \ \ |f_2(x)| \leq C_2 g_2(x) \ \ \forall\ x \geq x_2.$$

Luego,

$$\begin{aligned} |f_1(x) f_2(x)| &\leq |f_1(x)||f_2(x)| \\ &\leq C_1 C_2 g_1(x) g_2(x) \ \ \forall\ x \geq x_0, \end{aligned}$$

donde, $x_0 = \text{máx}\{x_1, x_2\}$. Tomando, $C = C_1 C_2$ se concluí la prueba.

3). Sea $f_1(x) = \mathrm{O}(g(x))$, entonces existe una constante $C > 0$ y $x_0 \in \mathbb{R}$ tal que

$$|f_1(x)| \leq C g(x) \ \ \forall\ x \geq x_0 \Rightarrow |g_1(x) f_1(x)| \leq C g_1(x) g(x) \ \ \forall\ x \geq x_0.$$

4). Si $f_1(x) = \mathrm{O}(g_1(x))$ y $f_2(x) = \mathrm{O}(g_1(x))$, entonces existen constantes $C_1, C_2 > 0$ y $x_1, x_2 \in \mathbb{R}$ tal que $|f_1(x)| \leq C_1 g_1(x) \ \ \forall\ x \geq x_1 \ \ \text{y} \ \ |f_2(x)| \leq C_2 g_2(x) \ \ \forall\ x \geq x_2$. Así,

$$\begin{aligned} |f_1(x) \pm f_2(x)| &\leq |f_1(x)| + |f_2(x)| \\ &\leq C_1 g_1(x) + C_2 g_2(x) \\ &\leq C_3 \,\text{máx}\{g_1(x), g_2(x)\} \quad \forall\ x \geq x_0, \end{aligned}$$

donde, $x_0 = k \cdot \text{máx}\{x_1, x_2\}$ para algún $k > 1$ y $C_3 = K \cdot \text{máx}\{C_1, C_2\}$ para algún $K > 1$. Esto concluye la prueba.

5). Si $f(x) = \mathrm{O}(g(x))$, entonces existe una constante $C > 0$ y $x_0 \in \mathbb{R}$ tal que

$$|f(x)| \leq C g(x) \quad \forall\ x \geq x_0 \Rightarrow |K f(x)| \leq KC g(x) \ \ \forall\ x \geq x_0.$$

Tomando $C_1 = KC$ tenemos el resultado.

6). Sea $f(t) = \mathrm{O}(g(t))$, así, existen $C > 0$ y $t_0 \in \mathbb{R}$ tal que $|f(t)| \leq C g(t)$ para todo $t \geq t_0$. Por otro lado, para x suficientemente grande, se tiene,

$$\begin{aligned}\left|\int_a^x f(t)dt\right| &= \left|\int_a^y f(t)dt + \int_y^x f(t)dt\right| \\ &\leq \int_a^y |f(t)|dt + \int_y^x |f(t)|dt \\ &\leq \int_a^y |f(t)|dt + C\int_y^x g(t)dt, \quad \text{para } t_0 \geq y \\ &\leq M\int_a^y g(t) + C\int_y^x g(t)dt, \quad \text{para algún } M > 1 \\ &\leq C_1\int_a^x g(t)dt, \quad \text{donde } C_1 = \text{máx}\{M, C\}.\end{aligned}$$

Entonces,

$$\mathrm{O}\left(\int_a^x g(t)dt\right) = \int_a^x f(t)dt = \int_a^x \mathrm{O}(g(t))dt.$$

■

En general, si $f, g : \mathbb{R} \to \mathbb{R}$ (o $\mathbb{C}$), escribimos

$$f(x) := \mathrm{O}(g(x)),$$

para x suficientemente grande, si existe una constante $C > 0$ y $x_0 \in \mathbb{R}$ tal que

$$|f(x)| \leq C|g(x)| \quad \forall\ x \geq x_0,$$

y valen las mismas propiedades de la Proposición 2.2.5.

2.3. Funciones aritméticas

Los resultados presentados en esta sección son tomados de **Apostol (1998)**.

2.3.1. Preliminares

Introducimos un concepto bien usado en la Teoría de Números, llamado *Funciones aritméticas*, los cuales expresan alguna propiedad aritmética de los números naturales. Antes de definir, veamos algunos conceptos.

Definición 2.3.1 Los conjuntos A, B son *equipotentes* si existe una aplicación $h : A \to B$ que es inyectiva y sobreyectiva.

Definición 2.3.2 El *cardinal* de un conjunto E (finito o infinito) se define, intuitivamente, como el "número" de elementos (distintos) que lo compone.

Podemos definir formalmente, el "número" como la clase de conjuntos *equipotentes* al conjunto E.

Ejemplo 2.3.1 Sea $E = \{2, 5, 7, 8, 9, 4, 9\}$. Entonces el cardinal de E es 6. Note que el cardinal de $\mathbb{N}$ es infinito y de un conjunto vacío es cero.

Notación. Se denota por $\#E$ la cardinalidad del conjunto E.

Definición 2.3.3 (Función aritmética) Una *función aritmética* es una función definida sobre los números naturales que toma valores en los números naturales, reales, complejos o en algún subconjunto de ellos.

Ejemplo 2.3.2 Sea $\sigma : \mathbb{N} \to \mathbb{N}$ la función contador de divisores de $n \in \mathbb{N}$, esto es,

$$\sigma(n) := \#\{d \in \mathbb{N} : d|n \text{ para } n \in \mathbb{N}\} = \sum_{\substack{n\in\mathbb{N} \\ d|n}} 1.$$

Esta función es una función aritmética.

Mas adelante veremos mas ejemplos de funciones aritméticas.

Definición 2.3.4 Sea la función aritmética f. Entonces f es llamado

1. *multiplicativa* si para cada $n, m \in \mathbb{N}$ con $(n, m) = 1$ (máximo común divisor de m y n), tenemos que, $f(mn) = f(m)f(n)$;
2. *completamente multiplicativa* si para cada $n, m \in \mathbb{N}$, se tiene, $f(nm) = f(n)f(m)$.

Ejemplo 2.3.3 La función aritmética σ no es completamente multiplicativa, pues

$$\sigma(12) = \{1, 2, 3, 4, 6, 12\} = 6.$$

Entonces, como $\sigma(2) = 2$ y $\sigma(6) = \{1, 2, 3, 6\} = 4$, tenemos que $\sigma(12) \neq \sigma(2)\sigma(6)$. Pero, σ si es multiplicativa.

2.3.2. Función de Möbius

Ahora, presentamos la siguiente función aritmética llamado la *función de Möbius*, nombrada así en honor al matemático alemán August Ferdinand Möbius, lo cual tiene un comportamiento central en el estudio de la teoría de números primos.

Definición 2.3.5 (Función de Möbius) Definimos la función aritmética, llamado *función de Möbius* $\boldsymbol{\mu} : \mathbb{N} \to \{-1, 0, 1\}$ por

$$\boldsymbol{\mu}(n) := \begin{cases} 1, & \text{si } n = 1, \\ (-1)^k, & \text{si } n \text{ es producto de } k \text{ primos distintos}, \\ 0, & \text{caso contrario.} \end{cases}$$

Ejemplo 2.3.4 Se tiene,

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\boldsymbol{\mu}(n)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0	-1	1	1

Notación. De aquí en adelante usaremos $\boldsymbol{\mu}$ para denotaremos la función de Möbius.

Proposición 2.3.1 *La función de Möbius es una función aritmética multiplicativa, pero no es completamente multiplicativa.*

Demostración. Veamos que $\boldsymbol{\mu}$ no es completamente multiplicativa. Tenemos $\boldsymbol{\mu}(3) = -1$ y $\boldsymbol{\mu}(6) = 1$. Entonces,

$$\boldsymbol{\mu}(6 \cdot 3) = \boldsymbol{\mu}(3^2 \cdot 2) = 0 \neq -1 = \boldsymbol{\mu}(6)\boldsymbol{\mu}(3).$$

Sigue que, $\boldsymbol{\mu}$ no es completamente multiplicativa.

Veamos que $\boldsymbol{\mu}$ es multiplicativa. Es válido para $m = 1$ o $n = 1$. Sea $m, n \in \mathbb{N}$ mayor que 1 tal que $(m, n) = 1$. Ahora, si $\boldsymbol{\mu}(m) = 0$ o $\boldsymbol{\mu}(n) = 0$, si y solamente si, existe $p \in \mathbb{P}$ tal que $p^2|m$ o $p^2|n$, esto ocurre, si y solamente si, $p^2|m \cdot n$, esto es, si y solamente si, $\boldsymbol{\mu}(m \cdot n) = 0$. Así,

$$\boldsymbol{\mu}(m \cdot n) = 0 = \boldsymbol{\mu}(m)\boldsymbol{\mu}(n).$$

Si, $\boldsymbol{\mu}(m), \boldsymbol{\mu}(n) \neq 0$, entonces existen $p_1, p_2, ..., p_i \in \mathbb{P}$ (todo los p_i diferentes) y

$q_1, q_2, ..., q_j \in \mathbb{P}$ (todos los q_j diferentes) tal que

$$m = p_1 \cdot p_2 \cdots p_i \quad \text{y} \quad n = q_1 \cdot q_2 \cdots q_j.$$

Como $(m, n) = 1$, entonces $p_l \neq q_r$ para todo $l = 1, 2, ..., i$ y $r = 1, 2, ..., j$, pues si, $p_l = q_r$ para algún l y r, entonces $(m, n) > p_l > 1$, absurdo. Note que,

$$m \cdot n = p_1 \cdot p_2 \cdots p_i \cdot q_1 \cdot q_2 \cdots q_j = \prod_{s=1}^{i+j} p_s,$$

donde $p_{i+r} = q_r$ para $r = 1, 2, ..., j$. Luego,

$$\boldsymbol{\mu}(m \cdot n) = (-1)^{i+j} = (-1)^i (-1)^j = \boldsymbol{\mu}(m)\boldsymbol{\mu}(n).$$

Por lo tanto, $\boldsymbol{\mu}$ es multiplicativa.

■

2.3.3. Convoluciones de Dirichlet

A continuación definimos la convolución (una operación binaria) para funciones aritméticas introducido por el matemático alemán Peter Gustav Lejeune Dirichlet.

Definición 2.3.6 (Convolución) Sean las funciones aritméticas $f, g : \mathbb{N} \to \mathbb{R}$. Definimos el *producto de Dirichlet* (o la convolución de Dirichlet) de f y g, $f * g : \mathbb{N} \to \mathbb{R}$ por

$$(f * g)(n) := \sum_{\substack{n \in \mathbb{N} \\ d|n}} f(d) g\left(\frac{n}{d}\right).$$

Tenemos algunas propiedades de las convoluciones de Dirichlet.

Proposición 2.3.2 *La convolución de Dirichlet es asociativa y conmutativa, es decir, para funciones aritméticas f, g y h, se tiene,*

$$f * g = g * f \quad y \quad (f * g) * h = f * (g * h).$$

Demostración. Sean las funciones aritméticas $f, g, h : \mathbb{N} \to \mathbb{R}$. Veamos la asociatividad:

$$
\begin{aligned}
((f*g)*h)(n) &= \sum_{\substack{n\in\mathbb{N}\\ d|n}} (f*g)(d)h\left(\frac{n}{d}\right) = \sum_{\substack{n\in\mathbb{N}\\ d|n}} h\left(\frac{n}{d}\right)(f*g)(d) \\
&= \sum_{dc=n} h(c)(f*g)(d) = \sum_{dc=n} h(c) \sum_{b|d} f(b)g\left(\frac{d}{b}\right) \\
&= \sum_{dc=n} h(c) \sum_{ab=d} f(b)g(a) = \sum_{abc=n} h(c)f(b)g(a) \\
&= \sum_{abc=n} f(b)g(a)h(c) = \sum_{bk=n} f(b) \sum_{ac=k} g(a)h(c) \\
&= \sum_{\substack{n\in\mathbb{N}\\ b|n}} f(b) \sum_{a|k} g(a)h\left(\frac{k}{a}\right) = \sum_{\substack{n\in\mathbb{N}\\ b|n}} f(b)(g*h)(k) \\
&= \sum_{\substack{n\in\mathbb{N}\\ b|n}} f(b)(g*h)(k) = \sum_{\substack{n\in\mathbb{N}\\ b|n}} f(b)(g*h)\left(\frac{n}{b}\right) \\
&= (f*(g*h))(n).
\end{aligned}
$$

Ahora, veamos la conmutabilidad:

$$
\begin{aligned}
(f*g)(n) &= \sum_{\substack{n\in\mathbb{N}\\ d|n}} f(d)g\left(\frac{n}{d}\right) = \sum_{cd=n} f(d)g(c) \quad (\text{pues, } n = cd, \text{ para algún } c) \\
&= \sum_{cd=n} g(c)f(d) = \sum_{\substack{n\in\mathbb{N}\\ c|n}} g(c)f\left(\frac{n}{c}\right) \\
&= (g*f)(n).
\end{aligned}
$$

■

Definición 2.3.7 Defina la función aritmética $I : \mathbb{N} \to \{0, 1\}$ dada por

$$
I(n) := \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1, & \text{si } n = 1, \\ 0, & \text{si } n > 1. \end{cases}
$$

I es llamado la función identidad de la convolución de Dirichlet.

Proposición 2.3.3 *Para cualquier función aritmética f, se tiene, $I * f = f * I = f$.*

Demostración. Tenemos,

$$\begin{aligned}(I * f)(n) &= \sum_{\substack{n\in\mathbb{N}\\ d|n}} I(d) f\left(\frac{n}{d}\right) = \sum_{\substack{n\in\mathbb{N}\\ d|n}} \left\lfloor \frac{1}{d} \right\rfloor f\left(\frac{n}{d}\right) \\ &= f(n) \quad (\text{desde que } \lfloor 1/d \rfloor = 0, \text{ si } d > 1).\end{aligned}$$

Por la conmutabilidad de la convolución, $f * I = f$.

■

Proposición 2.3.4 *Dado cualquier $n \in \mathbb{N}$, tenemos,*

$$I(n) = \sum_{\substack{n\in\mathbb{N}\\ d|n}} \boldsymbol{\mu}(d).$$

Demostración. Sea

$$F(n) = \sum_{\substack{n\in\mathbb{N}\\ d|n}} \boldsymbol{\mu}(d).$$

Para $n = 1$, tenemos que, $F(n) = 1$, ya que $\boldsymbol{\mu}(1) = 1$. Sea $n > 1$ y escribimos $n = p_1^{a_1} \cdots p_k^{a_k}$, donde, $p_1, ..., p_k \in \mathbb{P}$ y $a_1, ..., a_k \in \mathbb{N}$. Por definición de $\boldsymbol{\mu}$, en

$$\sum_{\substack{n\in\mathbb{N}\\ d|n}} \boldsymbol{\mu}(d)$$

sólo contribuyen los términos para $d = 1$ y para aquellos divisores de n que son productos de primos distintos. Así,

$$\begin{aligned}\sum_{\substack{n\in\mathbb{N}\\ d|n}} \boldsymbol{\mu}(d) &= \boldsymbol{\mu}(1) + \boldsymbol{\mu}(p_1) + \cdots + \boldsymbol{\mu}(p_k) + \boldsymbol{\mu}(p_1p_2) + \cdots + \boldsymbol{\mu}(p_{k-1}p_k) \\ &\quad + \cdots + \boldsymbol{\mu}(p_1p_2\cdots p_k) \\ &= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k \\ &= (1-1)^k = 0,\end{aligned}$$

donde,

$$\begin{pmatrix} k \\ n \end{pmatrix} = \frac{k!}{n!(k-n)!}.$$

Luego, para $n > 1$, $F(n) = 0$. Por lo tanto, $F(n) = I(n)$.

■

Definición 2.3.8 (Función unitaria) Definimos la *función unitaria* $u : \mathbb{N} \to \{1\}$ dado por $u(n) = 1$ para todo $n \in \mathbb{N}$.

Corolario 2.3.1 *Tenemos que,* $I = \boldsymbol{\mu} * u = u * \boldsymbol{\mu}$.

Demostración. De la Proposición 2.3.4 se tiene,

$$I(n) = \sum_{\substack{n\in\mathbb{N}\\ d|n}} \boldsymbol{\mu}(d) = \sum_{\substack{n\in\mathbb{N}\\ d|n}} \boldsymbol{\mu}(d)u\left(\frac{n}{d}\right) = (\boldsymbol{\mu} * u)(n) = (u * \boldsymbol{\mu})(n).$$

■

Teorema 2.3.1 (Inversión de Möbius) *Para las funciones aritméticas f y g, las siguientes condiciones son equivalentes*

1. $f(n) = \sum_{\substack{n\in\mathbb{N}\\ d|n}} g(d)$;
2. $g(n) = \sum_{\substack{n\in\mathbb{N}\\ d|n}} f(d)\boldsymbol{\mu}\left(\frac{n}{d}\right)$.

Demostración. Veamos que 1) implica 2). De 1), note que,

$$f(n) = \sum_{\substack{n\in\mathbb{N}\\ d|n}} g(d) = \sum_{\substack{n\in\mathbb{N}\\ d|n}} g(d)u\left(\frac{n}{d}\right) = (g * u)(n).$$

Así, usando este resultado, la Proposición 2.3.2, Corolario 2.3.1 y la Proposición 2.3.3,

$$\begin{aligned}\sum_{\substack{n\in\mathbb{N}\\ d|n}} f(d)\boldsymbol{\mu}\left(\frac{n}{d}\right) &= (f * \boldsymbol{\mu})(n) = ((g * u) * \boldsymbol{\mu})(n) \\ &= (g * (u * \boldsymbol{\mu}))(n) = (g * I)(n) \\ &= g(n).\end{aligned}$$

Por lo tanto, probamos que, 1) implica 2).

Ahora, veamos que 2) implica 1). Note que, de 2), $g = f * \boldsymbol{\mu}$. Así, multiplicando por u a g, usando la Proposición 2.3.2, Corolario 2.3.1 y la Proposición 2.3.3,

$$g * u = (f * \boldsymbol{\mu}) * u = f * (\boldsymbol{\mu} * u) = f * I = f.$$

Luego,

$$f(n) = (g * u)(n) = \sum_{\substack{n\in\mathbb{N}\\ d|n}} g(d)u\left(\frac{n}{d}\right) = \sum_{\substack{n\in\mathbb{N}\\ d|n}} g(d).$$

Por lo tanto, 2) implica 1).

■

Corolario 2.3.2 *Tenemos que,*

$$\sum_{\substack{n\in\mathbb{N}\\ d|n}} \boldsymbol{\mu}(d)\sigma\left(\frac{n}{d}\right) = 1$$

Demostración. Se tiene que,

$$\sigma(n) = \sum_{\substack{n\in\mathbb{N}\\ d|n}} 1 = \sum_{\substack{n\in\mathbb{N}\\ d|n}} u(d).$$

Usando la Inversión de Möbius con $f = \sigma$ (función divisor) y $g = u$,

$$\begin{aligned} 1 = u(n) &= \sum_{\substack{n\in\mathbb{N}\\ d|n}} \sigma(d)\boldsymbol{\mu}\left(\frac{n}{d}\right) = (\sigma * \boldsymbol{\mu})(n) = (\boldsymbol{\mu} * \sigma)(n) \\ &= \sum_{\substack{n\in\mathbb{N}\\ d|n}} \boldsymbol{\mu}(d)\sigma\left(\frac{n}{d}\right). \end{aligned}$$

■

2.3.4. Función de Von Mangoldt

A continuación, presentamos otra función aritmética, llamado *función de Von Mangoldt* introducido por el matemático alemán Hans Von Mangoldt, que juega también un papel central en la distribución de los números primos.

Definición 2.3.9 La función aritmética $\Lambda : \mathbb{N} \to [0, \infty)$ definida por

$$\Lambda(n) := \begin{cases} \ln p, & \text{si } n = p^m \text{ para algún } p \in \mathbb{P} \text{ y } m \in \mathbb{N} \\ 0, & \text{caso contrario} \end{cases}$$

es llamado la *función de Von Mangoldt.*

Proposición 2.3.5 *Para cualquier* $n \in \mathbb{N}$,

$$\ln n = \sum_{\substack{n \in \mathbb{N} \\ d|n}} \Lambda(d).$$

Demostración. Para $n = 1$, ambas igualdades valen cero. Para $n > 1$, escribimos, $n = p_1^{a_1} \cdots p_k^{a_k}$ con $p_1, ..., p_k \in \mathbb{P}$ y $a_1, ..., a_k \in \mathbb{N}$. Tomando logaritmo natural,

$$\ln n = \sum_{i=1}^{k} a_i \ln p_i.$$

Ahora, por definición de Λ, los únicos términos distintos de cero en la suma $\sum_{d|n} \Lambda(d)$ son para los divisores d de la forma p_i^m, donde, $m \in \{1, 2, ..., a_i\}$ y $i \in \{1, 2, ..., k\}$. Luego,

$$\sum_{\substack{n \in \mathbb{N} \\ d|n}} \Lambda(d) = \sum_{i=1}^{k} \sum_{m=1}^{a_i} \Lambda(p_i^m) = \sum_{i=1}^{k} \sum_{m=1}^{a_i} \ln p_i = \sum_{i=1}^{k} a_i \ln p_i = \ln n.$$

■

Proposición 2.3.6 *Para* $n \in \mathbb{N}$, *tenemos,*

$$\Lambda(n) = \sum_{\substack{n \in \mathbb{N} \\ d|n}} \boldsymbol{\mu}(d) \ln\left(\frac{n}{d}\right) = -\sum_{\substack{n \in \mathbb{N} \\ d|n}} \boldsymbol{\mu}(d) \ln d.$$

Demostración. Por la Proposición 2.3.5, para $n \in \mathbb{N}$,

$$\ln n = \sum_{\substack{n \in \mathbb{N} \\ d|n}} \Lambda(d).$$

Note que, para cualquier $n \in \mathbb{N}$, tenemos que $\ln n \cdot I(n) = 0$, pues, $I(n) = 0$ para todo $n > 1$ y $I(n) \neq 0$ si $n = 1$, pero $\ln 1 = 0$. Así, usando este resultado y la Inversión de

Möbius (Teorema 2.3.1, ítem 1) implica ítem 2)) con $f = \ln$ y $g = \Lambda$, obtenemos

$$\begin{aligned}\Lambda(n) &= \sum_{\substack{n\in\mathbb{N}\\ d|n}} \ln(d)\boldsymbol{\mu}\left(\frac{n}{d}\right) = (\ln * \boldsymbol{\mu})(n) = (\boldsymbol{\mu} * \ln)(n) = \sum_{\substack{n\in\mathbb{N}\\ d|n}} \boldsymbol{\mu}(d)\ln\left(\frac{n}{d}\right)\\ &= \ln n \sum_{\substack{n\in\mathbb{N}\\ d|n}} \boldsymbol{\mu}(d) - \sum_{\substack{n\in\mathbb{N}\\ d|n}} \boldsymbol{\mu}(d)\ln d\\ &= \ln n \cdot I(n) - \sum_{\substack{n\in\mathbb{N}\\ d|n}} \boldsymbol{\mu}(d)\ln d, \quad \text{(por la Proposición 2.3.4)}\\ &= -\sum_{\substack{n\in\mathbb{N}\\ d|n}} \boldsymbol{\mu}(d)\ln d,\end{aligned}$$

■

Corolario 2.3.3 *Para $n \in \mathbb{N}$, tenemos,*

$$-\boldsymbol{\mu}(n)\ln n = \sum_{\substack{n\in\mathbb{N}\\ d|n}} \boldsymbol{\mu}(d)\Lambda\left(\frac{n}{d}\right).$$

Demostración. De la Proposición 2.3.6,

$$\Lambda(n) = -\sum_{\substack{n\in\mathbb{N}\\ d|n}} \boldsymbol{\mu}(d)\ln d.$$

Usando la Inversión de Möbius (Teorema 2.3.1) con $f = \Lambda$ y $g = -\boldsymbol{\mu}\ln$,

$$\begin{aligned}-\boldsymbol{\mu}(n)\ln n &= \sum_{\substack{n\in\mathbb{N}\\ d|n}} \Lambda(d)\boldsymbol{\mu}\left(\frac{n}{d}\right) = (\Lambda * \boldsymbol{\mu})(n) = (\boldsymbol{\mu} * \Lambda)(n)\\ &= \sum_{\substack{n\in\mathbb{N}\\ d|n}} \boldsymbol{\mu}(d)\Lambda\left(\frac{n}{d}\right).\end{aligned}$$

■

2.3.5. Sumas parciales

Antes de enunciar algunos resultados, vamos a generalizar la definición de la convolución de Dirichlet.

Definición 2.3.10 (Convolución generalizada) Para $F : (0, \infty) \to \mathbb{R}$ con $F(x) = 0$ si $0 < x < 1$ y la función aritmética $f : \mathbb{N} \to \mathbb{R}$, definimos la convolución de Dirichlet generalizado $f \circ F : (0, \infty) \to \mathbb{R}$ por

$$(f \circ F)(x) := \sum_{\substack{n \in \mathbb{N} \\ n \leq x}} f(n) F\left(\frac{x}{n}\right).$$

Note que, si $F(x) = 0$ para todo x no entero, la restricción de F a los enteros positivos es una función aritmética y encontramos que,

$$(f \circ F)(m) = (f * F)(m) \quad \forall\, m \in \mathbb{N}.$$

La operación $\circ$ en general, no es conmutativa ni asociativa. Sin embargo, el siguiente resultado sirve como un sustituto útil de la ley asociativa.

Proposición 2.3.7 *Para funciones aritméticas f y g, se tiene,*

$$f \circ (g \circ F) = (f * g) \circ F.$$

Demostración. Para $x > 0$,

$$\begin{aligned}
(f \circ (g \circ F))(x) &= \sum_{\substack{n \in \mathbb{N} \\ n \leq x}} f(n)(g \circ F)\left(\frac{x}{n}\right) \\
&= \sum_{\substack{n \in \mathbb{N} \\ n \leq x}} f(n) \sum_{\substack{n,m \in \mathbb{N} \\ m \leq \frac{x}{n}}} g(m) F\left(\frac{x}{nm}\right) = \sum_{\substack{n,m \in \mathbb{N} \\ nm \leq x}} f(n) g(m) F\left(\frac{x}{nm}\right) \\
&= \sum_{\substack{k \in \mathbb{N} \\ k \leq x}} \left(\sum_{\substack{n \in \mathbb{N} \\ n \mid k}} f(n) g\left(\frac{k}{n}\right) \right) F\left(\frac{x}{k}\right) \quad \text{(haciendo } mn = k\text{)} \\
&= \sum_{\substack{k \in \mathbb{N} \\ k \leq x}} (f * g)(k) F\left(\frac{x}{k}\right) \\
&= ((f * g) \circ F)(x).
\end{aligned}$$

■

Proposición 2.3.8 *Sean las funciones aritméticas f y g. Defina,*

$$H(x) := \sum_{\substack{n\in\mathbb{N}\\ n\leq x}} (f*g)(n), \quad F(x) := \sum_{\substack{n\in\mathbb{N}\\ n\leq x}} f(n) \quad y \quad G(x) := \sum_{\substack{n\in\mathbb{N}\\ n\leq x}} g(n).$$

Entonces,

$$H(x) = \sum_{\substack{n\in\mathbb{N}\\ n\leq x}} f(n)G\left(\frac{x}{n}\right) = \sum_{\substack{n\in\mathbb{N}\\ n\leq x}} g(n)F\left(\frac{n}{x}\right).$$

Demostración. Defina $U : (0,\infty) \to \{0,1\}$ por

$$U(x) := \begin{cases} 0, & \text{si } x \in (0,1) \\ 1, & \text{caso contrario} \end{cases}$$

Entonces,

$$F(x) = \sum_{\substack{n\in\mathbb{N}\\ n\leq x}} f(n) = \sum_{\substack{n\in\mathbb{N}\\ n\leq x}} f(n)U\left(\frac{x}{n}\right) = (f\circ U)(x).$$

Análogamente, $G = g\circ U$ y $H = (f*g)\circ U$. De la Proposición 2.3.7,

$$f\circ G = f\circ(g\circ U) = (f*g)\circ U = H,$$

y

$$g\circ F = g\circ(f\circ U) = (g*f)\circ U = (f*g)\circ U = H.$$

■

Observe que,

$$\begin{aligned} H(x) &:= \sum_{\substack{n\in\mathbb{N}\\ n\leq x}} \sum_{\substack{n\in\mathbb{N}\\ d|n}} f(d)g\left(\frac{n}{d}\right) = \sum_{\substack{n\in\mathbb{N}\\ n\leq x}} \sum_{qd=n} f(d)g(q) \\ &= \sum_{qd\leq x} f(d)g(q). \end{aligned}$$

Tenemos el siguiente resultado, conocido como *Principio de Hipérbola.*

Proposición 2.3.9 *Sean a y b números reales positivos tal que $ab = x$, y f, g funciones aritméticas; entonces,*

$$\sum_{qd \leq x} f(d)g(q) = \sum_{\substack{n \in \mathbb{N} \\ n \leq a}} f(n)G\left(\frac{x}{n}\right) + \sum_{\substack{n \in \mathbb{N} \\ n \leq b}} g(n)F\left(\frac{x}{n}\right) - F(a)G(b), \tag{1}$$

donde, $n = qd$.

Demostración. La suma izquierda de (1) se extiende sobre los puntos de red (puntos de coordenadas enteros) de la región hiperbólica que se muestra en la Figura 1, es decir, vamos a contar los puntos de red que se encuentran en las hipérbolas correspondientes a $n = 1, 2, ...\lfloor x \rfloor$, donde $qd = n$.

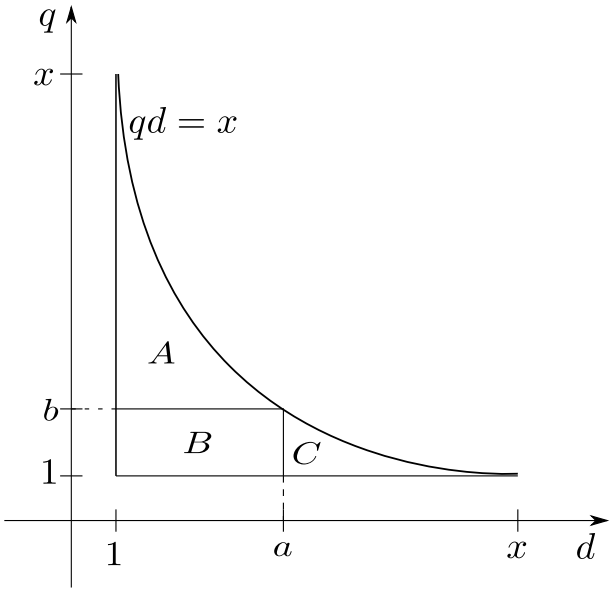


Figura 1: Región hiperbólica.

La suma izquierda de (1) se realizará en las sub regiones de la hipérbola de la Figura 1. Dividimos la suma en dos partes, una sobre los puntos de $A \cup B$ y la otra sobre aquellos puntos de $B \cup C$ y como los puntos de B están cubierto dos veces, entonces tenemos que restarlos.

La suma de puntos de red en $A \cup B$: Para cada $d \leq a$ fijo, podemos contar primero los puntos de red en el segmento vertical $1 \leq q \leq x/d$, esto es,

$$\sum_{q \leq \frac{x}{d}} f(d)g(q) = f(d) \sum_{q \leq \frac{x}{d}} g(q) = f(d)G\left(\frac{x}{d}\right)$$

y luego sumar todo los $d \leq a$, es decir,

$$\sum_{d\leq a}\sum_{q\leq \frac{x}{d}} f(d)g(q) = \sum_{d\leq a} f(d)G\left(\frac{x}{d}\right).$$

La suma de puntos de red en $B \cup C$: De forma análoga, para cada $q \leq b$ fijo, vamos a contar primero los puntos de red en el segmento horizontal $1 \leq d \leq x/q$. Esto es,

$$\sum_{d\leq \frac{x}{q}} f(d)g(q) = g(q)\sum_{d\leq \frac{x}{q}} f(d) = g(q)F\left(\frac{x}{q}\right)$$

y luego sumar todo los $q \leq b$,

$$\sum_{q\leq b}\sum_{d\leq \frac{x}{q}} f(d)g(q) = \sum_{q\leq b} g(q)F\left(\frac{x}{q}\right).$$

La suma de puntos de red en B: Fije $d \leq a$, contamos los puntos de red en el segmento vertical $1 \leq q \leq b$,

$$\sum_{q\leq b} f(d)g(q) = f(d)\sum_{q\leq b} g(q) = f(d)G(b)$$

y luego sumamos en cada $d \leq a$,

$$\sum_{d\leq a}\sum_{q\leq b} f(d)g(d) = \sum_{d\leq a} f(d)G(b) = F(a)G(b).$$

Luego, la suma de puntos de red en la región hiperbólica, es dado por los puntos en $A \cup B$ mas los puntos de red en $B \cup C$ y menos los puntos de la red en B, es decir,

$$\sum_{qd\leq x} f(d)g(q) = \sum_{d\leq a} f(d)G\left(\frac{x}{d}\right) + \sum_{q\leq b} g(q)F\left(\frac{x}{q}\right) - F(a)G(b).$$

■

Observación 2.3.1 De la Proposición 2.3.9,

$$\sum_{\substack{n\in\mathbb{N}\\ n\leq x}}(f*g)(n) = \sum_{\substack{n\in\mathbb{N}\\ n\leq a}} f(n)G\left(\frac{x}{n}\right) + \sum_{\substack{n\in\mathbb{N}\\ n\leq b}} g(n)F\left(\frac{x}{n}\right) - F(a)G(b),$$

donde $ab = x$.

2.4. Identidad de Abel

Presentamos una fórmula interesante para calcular series debido al matemático noruego Niels Henrik Abel. La bibliografía para esta sección también es **Apostol (1998)**.

Definición 2.4.1 Defina la función $A : \mathbb{R} \to \mathbb{R}$ por

$$A(x) := \sum_{\substack{n\in\mathbb{N}\\ n\leq x}} a(n),$$

donde, a es una función aritmética y $A(x) = 0$ si $x < 1$.

Lema 2.4.1 (Identidad de Abel) *Considere* $0 < y < x$ *y sea* $f : \mathbb{R} \to \mathbb{R}$ *una función continuamente diferenciable en* (y, x). *Entonces,*

$$\sum_{\substack{n\in\mathbb{N}\\ y<n\leq x}} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt.$$

Demostración. Sea $k := \lfloor x \rfloor$ y $m := \lfloor y \rfloor$. Note que,

$$A(x) = \sum_{\substack{n\in\mathbb{N}\\ n\leq x}} a(n) = \sum_{n=1}^{\lfloor x\rfloor} a(n) = \sum_{n=1}^{k} a(n) = \sum_{\substack{n\in\mathbb{N}\\ n\leq k}} a(n) = A(k)$$

$$\Rightarrow A(x) = A(k).$$

Análogamente, tenemos que,

$$A(y) = \sum_{\substack{n\in\mathbb{N}\\ n\leq y}} a(n) = \sum_{n=1}^{\lfloor y\rfloor} a(n) = \sum_{n=1}^{m} a(n) = \sum_{\substack{n\in\mathbb{N}\\ n\leq m}} a(n) = A(m)$$

$$\Rightarrow A(y) = A(m).$$

Luego, se tiene,

$$\begin{aligned}
\sum_{\substack{n\in\mathbb{N}\\ y<n\leq x}} a(n)f(n) &= \sum_{n=m+1}^{k} a(n)f(n) = \sum_{n=m+1}^{k} (A(n)-A(n-1))f(n)\\
&= \sum_{n=m+1}^{k} A(n)f(n) - \sum_{n=m}^{k-1} A(n)f(n+1)\\
&= \sum_{n=m+1}^{k-1} A(n)(f(n)-f(n+1)) + A(k)f(k) - A(m)f(m+1)\\
&= -\sum_{n=m+1}^{k-1} A(n)\int_{n}^{n+1} f'(t)dt + A(k)f(k) - A(m)f(m+1)\\
&= -\int_{m+1}^{k} A(t)f'(t)dt + A(k)f(k) + A(k)f(x) - A(k)f(x)\\
&\quad - A(m)f(m+1) + A(m)f(y) - A(m)f(y)\\
&= -\int_{m+1}^{k} A(t)f'(t)dt + A(k)f(x) - \int_{k}^{x} A(t)f'(t)dt\\
&\quad - A(m)f(y) - \int_{y}^{m+1} A(t)f'(t)dt\\
&= A(x)f(x) - A(y)f(y) - \int_{y}^{x} A(t)f'(t)dt.
\end{aligned}$$

■

Recordando, de Ejemplo 2.2.4, tenemos que

$$\lfloor x\rfloor = x + \mathrm{O}(1).$$

Veamos algunas aplicaciones de la identidad de Abel.

Proposición 2.4.1 *Se tiene,*

$$\sum_{\substack{n\in\mathbb{N}\\ n\leq x}} \ln n = x\ln x - x + O(\ln x).$$

Demostración. Usando la identidad de Abel con,

$$A(x) = \lfloor x\rfloor = \sum_{\substack{n\in\mathbb{N}\\ n\leq x}} 1,$$

$f = \ln$ y la Proposición 2.2.5, tenemos,

$$\begin{aligned}\sum_{\substack{n\in\mathbb{N}\\ n\leq x}} \ln n &= \lfloor x\rfloor \ln x - \int_1^x \frac{\lfloor t\rfloor}{t} dt \\ &= x\ln x + \mathrm{O}(\ln x) - \int_1^x dt - \mathrm{O}\left(\int_1^x \frac{1}{t} dt\right) \\ &= x\ln x - x + \mathrm{O}(\ln x).\end{aligned}$$

■

Proposición 2.4.2 *Se tiene,*

$$\sum_{\substack{n\in\mathbb{N}\\ n\leq x}} n = \frac{x^2}{2} + O(x)$$

Demostración. Nuevamente, usando la identidad de Abel, con $f(n) = n$, $A(x) = \lfloor x\rfloor$ y la Proposición 2.2.5,

$$\begin{aligned}\sum_{\substack{n\in\mathbb{N}\\ n\leq x}} n &= \lfloor x\rfloor x - 1 - \int_1^x \lfloor t\rfloor dt \\ &= x(x + \mathrm{O}(1)) - 1 - \int_1^x t dt + \mathrm{O}\left(\int_1^x dt\right) \\ &= x^2 - \frac{x^2}{2} - \frac{1}{2} + \mathrm{O}(x) = \frac{x^2}{2} + \mathrm{O}(x).\end{aligned}$$

■

Proposición 2.4.3 *Tenemos,*

$$\sum_{\substack{n\in\mathbb{N}\\ n\leq x}} \frac{1}{n} = \ln x + \gamma + O\left(\frac{1}{x}\right),$$

donde, γ es la constante de Euler.

Demostración. Para $A(x) = \lfloor x\rfloor = \sum_{n\leq x} 1$ y $f(n) = 1/n$, de la identidad de Abel y la Proposición 2.2.5,

$$\begin{aligned}\sum_{n\leq x}\frac{1}{n} &= \frac{\lfloor x\rfloor}{x} - 1 + \int_1^x \frac{\lfloor t\rfloor}{t^2}dt \\ &= \frac{\lfloor x\rfloor}{x} - 1 + \int_1^x \frac{1}{t}dt - \int_1^x \frac{\{t\}}{t^2}dt \\ &= \ln x + 1 - \int_1^\infty \frac{\{t\}}{t^2}dt + \int_x^\infty \frac{\{t\}}{t^2}dt + \mathrm{O}\left(\frac{1}{x}\right) \\ &= \ln x + \gamma + \mathrm{O}\left(\frac{1}{x}\right),\end{aligned} \tag{2}$$

donde, por la Proposición 2.2.3,

$$\gamma = 1 - \int_1^\infty \frac{\{t\}}{t^2}dt$$

y

$$0 \leq \int_x^\infty \frac{\{t\}}{t^2}dt \leq \int_x^\infty \frac{1}{t^2}dt = \frac{1}{x},$$

o sea,

$$\int_x^\infty \frac{\{t\}}{t^2}dt = \mathrm{O}\left(\frac{1}{x}\right).$$

■

Observación 2.4.1 Como $\lfloor x\rfloor \leq x$, entonces de (2),

$$\sum_{\substack{n\in\mathbb{N}\\ n\leq x}}\frac{1}{n} \leq \int_1^x \frac{1}{t}dt = \ln x < 1 + \ln x.$$

Proposición 2.4.4 *Tenemos,*

$$\sum_{\substack{n\in\mathbb{N}\\ n\leq x}}\sigma(n) = x\ln x + (2\gamma - 1)x + O(\sqrt{x}).$$

Demostración. Del Ejemplo 2.3.2,

$$\sum_{\substack{n\in\mathbb{N}\\ n\leq x}}\sigma(n) = \sum_{\substack{n\in\mathbb{N}\\ n\leq x}}\sum_{\substack{n\in\mathbb{N}\\ d\mid n}} 1 = \sum_{qd\leq x} 1 \tag{3}$$

La suma de la última igualdad de (3) se extiende sobre los puntos de red (con coordenadas enteras) en la región hiperbólica, o sea, la suma sobre los pares (q, d) tal que $qd \leq x$. Así,

vamos a contar los puntos de red que se encuentran en las hipérbolas correspondientes a $n = 1, 2, ...\lfloor x \rfloor$, donde $qd = n$.

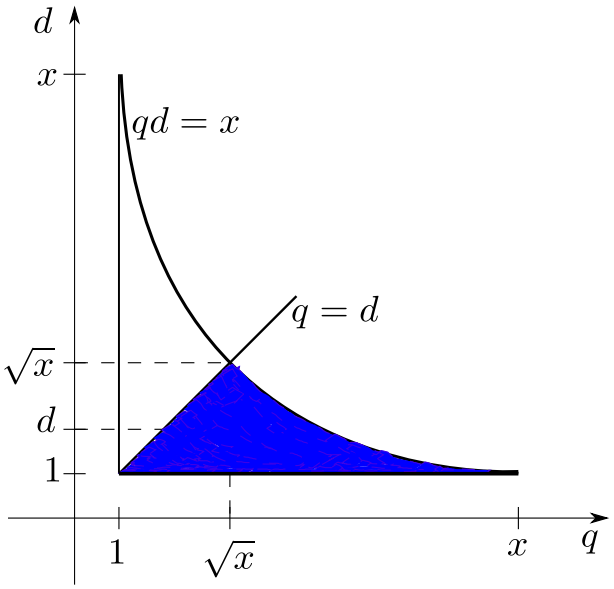


Figura 2: Región de la hipérbola.

En la Figura 2, podemos observar que la región es simétrico con respecto a la recta $q = d$. Entonces, para cada $d \leq \sqrt{x}$ fijo, podemos contar primero los puntos de red en el segmento de linea horizontal de la región sombrada de color azul,

$$1 \leq q \leq \frac{x}{d} - d,$$

luego sumarlos todo los $d \leq \sqrt{x}$. Así los punto de red en la región sombreada de color azul, es:

$$\sum_{d \leq \sqrt{x}} \sum_{q \leq \frac{x}{d} - d} 1 = \sum_{d \leq \sqrt{x}} \left(\left\lfloor \frac{x}{d} \right\rfloor - d \right).$$

Ahora, observe que, el número total de puntos de red de la región es igual al doble del número debajo de la recta $q = d$ (región sombreada de color azul) y más el número en el segmento de la línea bisectriz. Así, (3) se convierte en:

$$\begin{aligned}
\sum_{qd\le x} 1 &= 2\sum_{d\le\sqrt{x}}\left(\left\lfloor\frac{x}{d}\right\rfloor - d\right) + \lfloor\sqrt{x}\rfloor \\
&= 2\sum_{d\le\sqrt{x}}\left(\frac{x}{d} - d + \mathrm{O}(1)\right) + \mathrm{O}(\sqrt{x}) \\
&= 2x\sum_{d\le\sqrt{x}}\frac{1}{d} - 2\sum_{d\le\sqrt{x}} d + \mathrm{O}(\sqrt{x}) \\
&= 2x\left(\ln(\sqrt{x}) + \gamma + \mathrm{O}\left(\frac{1}{\sqrt{x}}\right)\right) - 2\sum_{d\le\sqrt{x}} d + \mathrm{O}(\sqrt{x}) \quad \text{(Proposición 2,4,3)} \\
&= x\ln x + 2x\gamma - 2\left(\frac{x}{2} + \mathrm{O}(\sqrt{x})\right) + \mathrm{O}(\sqrt{x}) \quad \text{(Proposición 2,4,2)} \\
&= x\ln x + (2\gamma - 1)x + \mathrm{O}(\sqrt{x}).
\end{aligned}$$

■

2.5. Funciones de Tchebychev

En esta sección, presentamos algunos resultados conforme el capítulo 1 de **Ingham (1990)**. En 1851, el matemático ruso P. L. Tchebychev introdujo las siguientes dos funciones auxiliares ψ y ϑ.

Definición 2.5.1 (Tchebychev) Sean las funciones $\psi, \vartheta : (0,\infty) \to \mathbb{R}$ definidas por

$$\psi(x) = \sum_{\substack{n\in\mathbb{N}\\ n\le x}} \Lambda(n) \quad \text{y} \quad \vartheta(x) = \sum_{\substack{p\in\mathbb{P}\\ p\le x}} \ln p.$$

Note que, $\vartheta(x) \le \psi(x)$. Es fácil ver que estas funciones son crecientes. Antes de probar un resultado interesante en esta sección , veamos el siguiente lema útil.

Lema 2.5.1 *Es válido,*

$$\sum_{\substack{p\in\mathbb{P}\\ p\le x}}\sum_{\substack{m\in\mathbb{N}\\ (p^m\le x)}} \ln p = \sum_{\substack{p\in\mathbb{P}\\ p\le x}} \left\lfloor\frac{\ln x}{\ln p}\right\rfloor \ln p.$$

Demostración. Note que, la suma sobre $m \in \mathbb{N}$ es realmente finita, pues la suma sobre $p \in \mathbb{P}$ es vacío se $\sqrt[m]{x} < 2$, esto es, si

$$m > \frac{\ln x}{\ln 2}.$$

Luego, $1 \leq m \leq \lfloor \frac{\ln x}{\ln 2} \rfloor$. Como $p \geq 2$, sigue que, $\ln p \geq \ln 2$. Así,

$$\frac{1}{\ln p} \leq \frac{1}{\ln 2} \Rightarrow \frac{\ln x}{\ln p} \leq \frac{\ln x}{\ln 2}.$$

Por lo tanto,

$$\begin{aligned}\sum_{\substack{p\in\mathbb{P}\\ p\leq x}} \sum_{\substack{m\in\mathbb{N}\\ (p^m\leq x)}} \ln p &= \sum_{\substack{p\in\mathbb{P}\\ p\leq x}} \sum_{m=1}^{\lfloor \frac{\ln x}{\ln p} \rfloor} \ln p = \sum_{\substack{p\in\mathbb{P}\\ p\leq x}} \left(\sum_{m=1}^{\lfloor \frac{\ln x}{\ln p} \rfloor} 1 \right) \ln p \\ &= \sum_{\substack{p\in\mathbb{P}\\ p\leq x}} \left\lfloor \frac{\ln x}{\ln p} \right\rfloor \ln p.\end{aligned}$$

■

Ahora, definimos la función contadora de números primos.

Definición 2.5.2 Definimos la función $\pi : [1, \infty) \to \mathbb{N}$ que cuenta la cantidad de números primos menores o iguales que $x \in [1, \infty)$ por

$$\pi(x) := \#\{p \in \mathbb{P} : p \leq x\}.$$

Ejemplo 2.5.1 $\pi(99.9) = 25$, pues, los números primos menores o iguales a 99.9 son: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$.

Teorema 2.5.1 *Tenemos*

$$\limsup_{x\to\infty} \frac{\pi(x)}{x/\ln x} = \limsup_{x\to\infty} \frac{\vartheta(x)}{x} = \limsup_{x\to\infty} \frac{\psi(x)}{x}$$

y

$$\liminf_{x\to\infty} \frac{\pi(x)}{x/\ln x} = \liminf_{x\to\infty} \frac{\vartheta(x)}{x} = \liminf_{x\to\infty} \frac{\psi(x)}{x}.$$

Demostración. Escribimos

$$A = \limsup_{x\to\infty} \frac{\pi(x)}{x/\ln x}, \quad B = \limsup_{x\to\infty} \frac{\vartheta(x)}{x} \quad \text{y} \quad C = \limsup_{x\to\infty} \frac{\psi(x)}{x}.$$

(Estos números posiblemente pueden ser $+\infty$). Ahora, para $x > 0$, usando Lema 2.5.1,

tenemos

$$\vartheta(x) \leq \psi(x) \leq \sum_{\substack{p\in\mathbb{P}\\ p\leq x}} \sum_{\substack{m\in\mathbb{N}\\ (p^m\leq x)}} \ln p = \sum_{\substack{p\in\mathbb{P}\\ p\leq x}} \left\lfloor \frac{\ln x}{\ln p} \right\rfloor \ln p \leq \sum_{\substack{p\in\mathbb{P}\\ p\leq x}} \frac{\ln x}{\ln p} \ln p$$
$$= \sum_{\substack{p\in\mathbb{P}\\ p\leq x}} \ln x = \ln x \sum_{\substack{p\in\mathbb{P}\\ p\leq x}} 1 = \ln x \ \pi(x).$$

Luego,

$$\frac{\vartheta(x)}{x} \leq \frac{\psi(x)}{x} \leq \frac{\pi(x)}{x/\ln x}. \tag{4}$$

Aplicando **lím sup** en (4), obtenemos, $B \leq C \leq A$.

Por otro lado, para cualquier $0 < \alpha < 1$ y $x > 1$,

$$\vartheta(x) \geq \sum_{\substack{p\in\mathbb{P}\\ x^\alpha < p\leq x}} \ln p \geq \sum_{\substack{p\in\mathbb{P}\\ x^\alpha < p\leq x}} \ln x^\alpha, \quad \text{pues} \quad p > x^\alpha$$
$$= \left(\sum_{\substack{p\in\mathbb{P}\\ p\leq x}} 1 - \sum_{\substack{p\in\mathbb{P}\\ p\leq x^\alpha}} 1 \right) \ln x^\alpha = (\pi(x) - \pi(x^\alpha)) \ln x^\alpha,$$

y como $\pi(x^\alpha) < x^\alpha$,

$$\frac{\vartheta(x)}{x} > \alpha \left(\frac{\pi(x)\ln x}{x} - \frac{\ln x}{x^{1-\alpha}} \right). \tag{5}$$

Fijando α, observe que

$$\lim_{x\to\infty} \frac{\ln x}{x^{1-\alpha}} = 0,$$

pues, basta usar la regla de L'Hospital. Así, aplicando **lím sup** en (5) concluimos que $B \geq \alpha A$. Finalmente, haciendo $\alpha \to 1$, tenemos $B \geq A$. Por lo tanto,

$$B \leq C \leq A \leq B \Rightarrow A = B = C.$$

La prueba de la segunda parte es análogo.

■

2.6. Nociones de sistemas dinámicos discretos

El matemático francés Henri Poincaré es considerado uno de los creadores de la teoría moderna de sistemas dinámicos, teniendo introducido en el estudio muchos aspectos cualitativos de ecuaciones diferenciales que permiten estudiar las propiedades asintóticas de las soluciones, como la estabilidad y periocidad sin ser necesario resolver explícitamente la solución de la ecuación diferencial.

El primer libro publicado en la area de sistemas dinámicos es: *Dynamical Systems* escrito por el matemático estadounidense George Birkhoff, publicado en 1927.

2.6.1. Círculo unitario

Tenemos varias formas de definir el círculo unitario para los propósitos de nuestro estudio. El círculo unitario mas conocido es el círculo Euclideano:

$$\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}.$$

Otra definición común del circulo unitario de centro 0 en $\mathbb{C}$ es dado por [2]:

$$S^1 := \{z \in \mathbb{C} : |z| = 1\} = \{z \in \mathbb{C} : z = e^{2\pi it},\ t \in \mathbb{R}\}.$$

Para definir de otro modo un círculo unitario (que va ser homeomorfo a S^1), necesitamos recordar sobre espacios cocientes, para mas detalle ver **Munkres (2000)**.

Sea X un espacio topológico y $\sim$ una relación de equivalencia [3] en X. El espacio cociente es $X/\sim$ y $P : X \to X/\sim$ es la proyección que asocia $x \in X$ en su clase de equivalencia $[x]$.

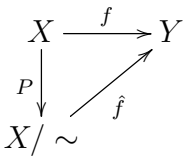
Definición 2.6.1 Definimos la *topología cociente* en $X/\sim$ definiendo $U \subseteq X/\sim$ es abierto si y solamente si, $U = X/\sim$, $U = \emptyset$ o $P^{-1}(U)$ es abierto en X.

Note que P es continua por construcción. Sean X y Y espacios topológicos, defina $f : X \to Y$ una aplicación que sea constante en las clases de equivalencia. Luego, $f(x_1) = f(x_2)$ si $x_1 \sim x_2$. Por lo tanto, podemos definir una aplicación $\hat{f} : X/\sim \to Y$ por

[2] Para $z = u + iw \in \mathbb{C}$, tenemos que $|z| = \sqrt{u^2 + v^2}$. Además, $e^{2\pi it} = \cos(2\pi t) + i\sin(2\pi t)$.

[3] **Relación de equivalencia**: Para $x, w, z \in X$, (i) $x \sim x$. (ii) Si $x \sim w$, entonces $w \sim x$. (iii) Si $x \sim w$ y $w \sim z$, entonces $x \sim z$.

$\hat{f}([x]) = f(x)$ para $x \in [x]$. Note que, el siguiente diagrama conmuta:



esto es, $\hat{f} \circ P = f$.

Proposición 2.6.1 *$\hat{f}$ es continua si y solamente si, f es continua.*

Demostración. Si $\hat{f}$ es continua, sigue que f es continua, desde que $f = \hat{f} \circ P$ (composición de dos funciones continuas).

Suponga que f sea continua. Sea $V \subset Y$ un abierto, entonces,

$$f^{-1}(V) = (\hat{f} \circ P)^{-1}(V) = P^{-1}(\hat{f}^{-1}(V)),$$

abierto, pues f es continua. Luego, por definición, $\hat{f}^{-1}(V)$ es abierto y, sigue que $\hat{f}$ es continua. ■

Sea $I = [0, 1]$ y considere la relación de equivalencia $\sim$ que identifica 0 con 1

Proposición 2.6.2 *$I/\sim$ es homeomorfo a S^1.*

Demostración. Sea $f : [0, 1] \to S^1$ dado por $f(t) = e^{2\pi it}$. Note que f es continua y constante en las clases de equivalencia (pues, $f(0) = 1 = f(1)$). Por lo tanto, definimos $\hat{f} : I/\sim \to S^1$ por $\hat{f}([x]) = f(x)$ y por la Proposición 2.6.1 $\hat{f}$ es continua. Además, $\hat{f}$ es biyectiva (inyectiva y sobreyectiva) y cerrado (pues $I/\sim = P(I)$ es compacto y S^1 es un espacio de Hausdorff). Así, $\hat{f}$ es un homeomorfismo.

■

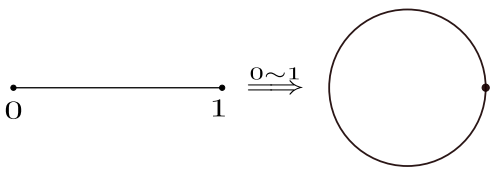


Figura 3: Figura de la Proposición 2.6.2.

Definición 2.6.2 El espacio $I/\sim$ es llamado circulo flat.

Tenemos la siguiente definición de un espacio cociente, lo cual sera identificado también con el círculo S^1.

Definición 2.6.3 Defina $\mathbb{T} := \mathbb{R}/\mathbb{Z} := \{x + \mathbb{Z} : x \in \mathbb{R}\}$, que es, la recta real con dos puntos $x, y \in \mathbb{R}$ identificado si $x - y \in \mathbb{Z}$, es decir, $\mathbb{T} = \mathbb{R}/\sim$, donde $\sim$ es una relación de equivalencia en $\mathbb{R}$ definida por: $x \sim y \Leftrightarrow x - y \in \mathbb{Z}$.

Un elemento de $\mathbb{T}$ es de la forma, $[x] = \{x + m : m \in \mathbb{Z}\}$, y las operaciones son dadas por

$$[x + y] = [x] + [y] \quad \text{y} \quad [x - y] = [x] - [y].$$

Tenemos que $p : \mathbb{R} \to \mathbb{T}$ es la proyección canónica dado por $p(x) = x \mod 1$.

Proposición 2.6.3 *$I/\sim$ es homeomorfo a $\mathbb{T}$*

Demostración. Considere $f : [0, 1] \to \mathbb{R}$ la aplicación inclusión $(f(x) = x)$ y $p : \mathbb{R} \to \mathbb{T}$ la proyección canónica $(p(x) = x \mod 1)$. Note que f y p son continuas.

Sea $h := p \circ f : [0, 1] \to \mathbb{T}$ y, observamos que h es continua constante en las clases de equivalencia (pues, $h(0) = h(1)$, desde que $0 \sim 1$). Por lo tanto, definimos $\hat{h} : I/\sim \to \mathbb{T}$ por $h([x]) = h(x)$ y nuevamente por la Proposición 2.6.1 es continua. Además, $\hat{h}$ es biyectiva y cerrado (pues, $I/\sim = P(I)$ es compacto y $\mathbb{T}$ es un espacio de Hausdorff). Así, $\hat{h}$ es un homeomorfismo.

■

Observación 2.6.1 De las Proposiciones 2.6.2 y 2.6.3, concluimos que $I/\sim$, S^1 y $\mathbb{T}$ son homeomorfos y compactos.

Notación Un elemento $[x]$ de $\mathbb{T}$ simplemente sera denotado por x.

2.6.2. Sistemas dinámicos discretos

Consideremos un conjunto X, que normalmente llamamos de espacio (topológico, métrico, etc.), es el mundo donde ocurre la dinámica y una transformación $T : X \to X$ que puede tener diversas propiedades, desde las mas básicas, por ejemplo, de ser continua, inyectiva, sobreyectiva, etc.

Notación. Dado $x \in X$ y $m, n \in \mathbb{N}^*$, denotamos por

$$T^{n+m}(x) = T^n \circ T^m(x) = T^n(T^m(x))$$

la composición de funciones y T^0 es la función identidad.

Definición 2.6.4 Definimos la *órbita positiva* de $x \in X$ por

$$\text{Orb}^+(x) := \{T^n(x) : n \in \mathbb{N}^*\} = \{x, T(x), T^2(x), ...\}.$$

De forma análoga, se T es invertible, definimos la *órbita negativa* de un punto $x \in X$ por

$$\text{Orb}^-(x) := \{T^{-n}(x) : n \in \mathbb{N}^*\}.$$

Definición 2.6.5 La *órbita* del punto $x \in X$, simplemente es definido por

$$\text{Orb}(x) := \{T^n(x) : n \in \mathbb{Z}\} = \{..., T^{-2}(x), T^{-1}(x), x, T(x), T^2(x), ...\}.$$

Entonces, básicamente la dinámica discreta es hacer lo siguiente: Tomar un punto $x \in X$ y ver por la órbita de ese punto, o sea, intentar describir lo máximo posible la estructura de las órbitas de los puntos, donde que ellas nacen, mueren, cual es el paseo que ellas hacen en el intermedio antes de converger a un cierto conjunto. Podemos ver mas conceptos y resultados de este asunto en **Robinson (1998)**.

Definición 2.6.6 Un *sistema dinámico discreto* es la dupla (X, T), donde X es un espacio y $T : X \to X$ una función que describe la dependencia temporal de la posición de un ponto en X.

Existen muchos ejemplos de sistemas dinámicos, pero de nuestro interés particular son los siguientes ejemplos.

Ejemplo 2.6.1 Sea $f : \mathbb{T} \to \mathbb{T}$ la *función doble* definido por

$$f(x) := 2x \mod 1 = \begin{cases} 2x & \text{si } x \in [0, 1/2), \\ 2x - 1 & \text{si } x \in [1/2, 1). \end{cases}$$

Note que f es continua. Así, $(\mathbb{T}, f)$ es un sistema dinámico discreto.

Y la órbita positiva de $x \in \mathbb{T}$ es dado por

$$\mathrm{Orb}^+(x) = \{f^n(x) : n \in \mathbb{N}^*\} = \{2nx \mod 1 : n \in \mathbb{N}^*\}.$$

Ejemplo 2.6.2 (Rotación) Dado $\alpha \in [0, 1)$, la *función rotación* $R_\alpha : \mathbb{T} \to \mathbb{T}$ (de ángulo α, ver Figura 4) es definido por

$$R_\alpha(x) = x + \alpha \mod 1 = \begin{cases} x + \alpha & \text{si } 0 \leq x + \alpha \leq 1, \\ x + \alpha - 1 & \text{si } x + \alpha > 1. \end{cases}$$

Entonces, $(\mathbb{T}, R_\alpha)$ es un sistema dinámico discreto.

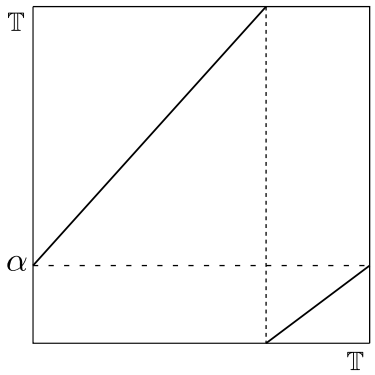


Figura 4: Rotación R_α.

La órbita de $x \in \mathbb{T}$ es dado por

$$\mathrm{Orb}(x) = \{R_\alpha^n(x) : n \in \mathbb{Z}\} = \{x + n\alpha \mod 1 : n \in \mathbb{Z}\}.$$

Observe que si $\alpha = \frac{p}{q}$, donde $p \in \mathbb{Z}$ y $q \in \mathbb{N}$ primos entre si, es decir, $(p, q) = 1$. Entonces, para $x \in S^1$,

$$R_{p/q}^q(x) = x + q \cdot \frac{p}{q} \mod 1 = x + p \mod 1 = x.$$

Esto significa que, $x \in \mathbb{T}$ es un punto periódico de periodo q por la rotación $R_{p/q}$. Si $\alpha \notin \mathbb{Q}$, entonces la órbita de $x \in \mathbb{T}$ por R_α es denso en $\mathbb{T}$, es decir, $\overline{\mathrm{Orb}(x)} = \mathbb{T}$.

2.7. Introducción a la entropía topológica

Las bibliografías que usamos para esta sección son **Walters (2000)**, **Pollicott y Yuri (1998)** y **Robinson (1998)**.

2.7.1. Entropía a través de coberturas

En 1965, R. L. Adler, A. G. Konheim y M. H. McAndrew publican un articulo llamado *Topological Entropy* (en International Business Machines Corporation, Yorktown Heights, New York) donde proponen una noción de la entropía topológica inspirado en la entropía de Kolmogorov-Sinai, pero cuya definición no envuelve medidas invariantes. Esta definición se aplica a cualquier función continua en un espacio topológico compacto. Ver Apéndice A.1 para recordar definiciones que vamos a necesitar en esta parte.

Definición 2.7.1 Para $\mathcal{U}$ una cobertura abierta de un espacio topológico compacto X, definimos,

$$N(\mathcal{U}) := \text{mín}\{n \in \mathbb{N} : \text{existe una subcobertura de } \mathcal{U} \text{ con } n \text{ elementos}\}$$

Definición 2.7.2 La *entropía de la cobertura abierta* $\mathcal{U}$ es definido por

$$H(\mathcal{U}) := \ln N(\mathcal{U}).$$

En la definición, la elección de la base del logaritmo no es esencial, porque su cambio solo da como resultado un factor de escala constante.

Ejemplo 2.7.1 Para $X = \mathbb{T} = [0,1)/\sim$ consideremos una cobertura abierta

$$\mathcal{U} = \left\{ \left(\frac{1}{4}, 1\right), \left[0, \frac{3}{4}\right), \left(\frac{1}{2}, 1\right) \cup \left[0, \frac{1}{4}\right), \left(\frac{3}{4}, 1\right) \cup \left[0, \frac{1}{2}\right) \right\}$$

Note que la subcobertura

$$\left\{ \left[0, \frac{3}{4}\right), \left(\frac{1}{4}, 1\right) \right\}$$

de $\mathcal{U}$ que cubre a $\mathbb{T}$. Luego, $N(\mathcal{U}) = 2$ y $H(\mathcal{U}) = \ln 2$.

Definición 2.7.3 (Refinamiento) Una cobertura abierta $\mathcal{U}$ es un *refinamiento* de la cobertura abierta $\mathcal{V}$, denotado por $\mathcal{V} \leq \mathcal{U}$, si todo elemento de $\mathcal{U}$ esta contenido en algún elemento de $\mathcal{V}$, o sea, dado $U \in \mathcal{U}$, existe $V \in \mathcal{V}$ tal que $U \subseteq V$.

Definición 2.7.4 (Refinamiento común) Sean las coberturas abiertas $\mathcal{U}$ y $\mathcal{V}$ de X, definimos el *refinamiento común* de ellos por,

$$\mathcal{U} \vee \mathcal{V} := \{U \cap V : U \in \mathcal{U}, V \in \mathcal{V} \text{ y } U \cap V \neq \emptyset\}.$$

Proposición 2.7.1 *Sean $\mathcal{U}$ y $\mathcal{V}$ las coberturas abiertas de X, entonces $\mathcal{U} \leq \mathcal{U} \vee \mathcal{V}$ y $\mathcal{V} \leq \mathcal{U} \vee \mathcal{V}$.*

Demostración. Sean $\mathcal{U}$ y $\mathcal{V}$ coberturas abiertas de X. Como los elementos de $\mathcal{U} \vee \mathcal{V}$ son de la forma $U \cap V \neq \emptyset$ para cualquier $U \in \mathcal{U}$, $V \in \mathcal{V}$ y, desde que, $U \cap V \subseteq U$ y $U \cap V \subseteq V$ sigue-se que, $\mathcal{U} \leq \mathcal{U} \vee \mathcal{V}$ y $\mathcal{V} \leq \mathcal{U} \vee \mathcal{V}$. ■

Definición 2.7.5 Sea $\mathcal{U} = \{U_1, U_2, ..., U_n\}$ una cobertura abierta de un espacio topológico compacto X; para $T : X \to X$ continua, definimos,

$$T^{-1}(\mathcal{U}) := \{T^{-1}(U_1), T^{-1}(U_2), ..., T^{-1}(U_n)\}.$$

Veamos algunas propiedades básicas de la entropía de una cobertura abierta.

Proposición 2.7.2 *Se tiene,*

1. $H(\mathcal{U}) \geq 0$ *y* $H(\mathcal{U}) = 0$ *si y solamente si,* $X \in \mathcal{U}$.
2. *Si* $\mathcal{V} \leq \mathcal{U}$ *entonces* $H(\mathcal{V}) \leq H(\mathcal{U})$.
3. $H(\mathcal{U} \vee \mathcal{V}) \leq H(\mathcal{U}) + H(\mathcal{V})$.
4. $H(T^{-1}(\mathcal{U})) \leq H(\mathcal{U})$.

Demostración. 1). La primera parte sigue desde que $N(\mathcal{U})$ esta formado por enteros positivos. Note que, $N(\mathcal{U}) = 1$ si y solamente si, $X = \{\mathcal{U}\}$, así probamos la segunda parte.

2). Sea $\{U_1, ..., U_N\}$ una subcobertura finita con menor cardinalidad de $\mathcal{U}$. Por hipótesis, $\mathcal{V} \leq \mathcal{U}$, entonces para cada $i \in \{1, ..., N\}$ existe $V_i \in \mathcal{V}$ tal que $U_i \subseteq V_i$. Por lo tanto, $\{V_1, ..., V_N\}$ cubre X, esto es, una subcobertura de $\mathcal{V}$ (no necesariamente con cardinalidad mínima).

Luego, $N(\mathcal{V}) \leq N(\mathcal{U})$ y, por lo tanto,

$$H(\mathcal{V}) = \ln N(\mathcal{V}) \leq \ln N(\mathcal{U}) = H(\mathcal{U})$$
$$\Rightarrow H(\mathcal{V}) \leq H(\mathcal{U}).$$

3). Sean $\{U_1, ..., U_n\}$ e $\{V_1, ..., V_m\}$ las subcoberturas finitas de menor cardinalidad de $\mathcal{U}$ y $\mathcal{V}$ respectivamente. Entonces

$$\{U_i \cap V_j : 1 \leq i \leq n,\ 1 \leq j \leq m\}$$

es una subcobertura (no necesariamente con cardinalidad mínima) de $\mathcal{U} \vee \mathcal{V}$. Luego, $N(\mathcal{U} \vee \mathcal{V}) \leq N(\mathcal{U})N(\mathcal{V})$ y, consecuentemente,

$$H(\mathcal{U} \vee \mathcal{V}) = \ln N(\mathcal{U} \vee \mathcal{V}) \leq \ln N(\mathcal{U}) + \ln N(\mathcal{V})$$
$$= H(\mathcal{U}) + H(\mathcal{V}).$$

4). Sea $\mathcal{U}$ una cobertura abierta de X y considere $\{U_1, ..., U_n\}$ una subcobertura finita de menor cardinalidad de $\mathcal{U}$, entonces, $\{T^{-1}(U_1), ..., T^{-1}(U_n)\}$ es unasubcobertura finita de $T^{-1}(\mathcal{U})$ (no necesariamente mínimo). Así, $N(T^{-1}(\mathcal{U})) \leq N(\mathcal{U})$ y, sigue que $H(T^{-1}(\mathcal{U})) \leq H(\mathcal{U})$.

■

A continuación presentamos un resultado útil de análisis de la recta.

Lema 2.7.1 (Lema de Fekete) *Sea $\{a_n\}_{n\in\mathbb{N}}$ una sucesión de números positivos tal que*

$$a_{n+m} \leq a_n + a_m \quad \forall\ m, n \in \mathbb{N}.$$

Entonces,

$$\lim_{n\to\infty} \frac{a_n}{n} = \text{ínf}\left\{\frac{a_k}{k} : k \in \mathbb{N}\right\}$$

existe.

Demostración. Tome $k \in \mathbb{N}$ fijo. Entonces por el algoritmo de Euclides, $n = qk + r$ para algún $q \in \mathbb{N}$ y $0 \leq r \leq k - 1$. Note que, $qk = k + k + \cdots + k$ (q veces) y sigue que,

$a_{qk} \leq qa_k$. Luego,

$$\frac{a_n}{n} \leq \frac{a_{qk} + a_r}{qk + r} \leq \frac{qa_k + a_r}{qk + r}.$$

Si $n \to \infty$, tenemos, $q \to \infty$. Entonces,

$$\limsup_{n\to\infty} \frac{a_n}{n} \leq \frac{a_k}{k},$$

válido para todo $k \in \mathbb{N}$. Por lo tanto,

$$\limsup_{n\to\infty} \frac{a_n}{n} \leq \left\{ \frac{a_k}{k} : k \in \mathbb{N} \right\} \leq \liminf_{n\to\infty} \frac{a_n}{n}.$$

Esto establece la existencia del límite, desde que, $\liminf \leq \limsup$.

■

Ahora, para una cobertura abierta $\mathcal{U}$ de X, una función continua $T : X \to X$ y cualquier $n \in \mathbb{N}$, definimos el siguiente conjunto:

$$\begin{aligned} \mathcal{U}^n &:= \bigvee_{j=0}^{n-1} T^{-j}(\mathcal{U}) = \mathcal{U} \vee T^{-1}(\mathcal{U}) \vee \cdots \vee T^{n-1}(\mathcal{U}) \\ &= \left\{ \bigcap_{j=0}^{n-1} T^{-j}(U_j) : U_j \in \mathcal{U} \ \text{ y } \ \bigcap_{j=0}^{n-1} T^{-j}(U_j) \neq \emptyset \right\}. \end{aligned}$$

Definición 2.7.6 La entropía de T en relación a la cobertura abierta $\mathcal{U}$ es definido por

$$h(T, \mathcal{U}) := \lim_{n\to\infty} \frac{1}{n} H(\mathcal{U}^n). \tag{6}$$

La definición nos dice, que la entropía topológica de T en relación a $\mathcal{U}$ es la cantidad promedio (por iteración) de información necesaria para describir iteraciones grandes de la transformación T. Así, cuanto hay mas información, existe mayor desorden y mayor la entropía. Cuanto menos es la información, menor la entropía.

Proposición 2.7.3 *El limite definido en (6) esta bien definida.*

Demostración. Sean $\mathcal{U}$ una subcovertura abierta de X y $a_n = H(\mathcal{U}^n)$. Probaremos que $\{a_n\}_{n\in\mathbb{N}}$ es una sucesión subaditiva.

Note que,

$$\begin{aligned}\bigvee_{j=0}^{n+m-1} T^{-j}(\mathcal{U}) &= \mathcal{U} \vee T^{-1}(\mathcal{U}) \vee \cdots \vee T^{-(n-1)}(\mathcal{U}) \vee T^{-n}(\mathcal{U}) \vee \cdots \vee T^{-(n+m-1)}(\mathcal{U}) \\ &= \bigvee_{j=0}^{n-1} T^{-j}(\mathcal{U}) \vee T^{-n}[\mathcal{U} \vee T^{-1}(\mathcal{U}) \vee \cdots T^{-(m-1)}(\mathcal{U})] \\ &= \bigvee_{j=0}^{n-1} T^{-j}(\mathcal{U}) \vee T^{-n}\left(\bigvee_{i=0}^{m-1} T^{-i}(\mathcal{U})\right).\end{aligned}$$

Así, $\mathcal{U}^{n+m} = \mathcal{U}^n \vee T^{-n}(\mathcal{U}^m)$. Luego,

$$\begin{aligned}a_{n+m} &= H(\mathcal{U}^{n+m}) = H(\mathcal{U}^n \vee T^{-n}(\mathcal{U}^m)) \\ &\leq H(\mathcal{U}^n) + H(T^{-n}(\mathcal{U}^m)) \quad \text{(Proposición 2.7.2 (3))} \\ &\leq H(\mathcal{U}^n) + H(\mathcal{U}^m) \quad \text{(Proposición 2.7.2 (4))} \\ &= a_n + a_m \quad \forall\ n, m \in \mathbb{N}.\end{aligned}$$

Por lo tanto, por el Lema de Fekete, el limite (6) existe.

■

Finalmente, tenemos la siguiente definición de la entropía topológica.

Definición 2.7.7 (Adler–Konheim–McAndrews) La *entropía topológica* de T es definido por

$$h_{top}(T) := \sup_{\mathcal{U}} h(T, \mathcal{U}).$$

Ejemplo 2.7.2 Sea $T = id : X \to X$ la función identidad. Entonces, para cualquier cobertura abierta $\mathcal{U}$, se tiene, $T^{-i}(\mathcal{U}) = \mathcal{U}$ y $\mathcal{U} = \mathcal{U}^n$. Esto significa que, $H(\mathcal{U}) = H(\mathcal{U}^n)$ y

$$h(T, \mathcal{U}) = \lim_{n\to\infty} \frac{1}{n} H(\mathcal{U}^n) = \lim_{n\to\infty} \frac{1}{n} H(\mathcal{U}) = 0.$$

Como $\mathcal{U}$ es arbitrario, $h_{top}(T) = 0$.

Definición 2.7.8 Diremos que un sistema dinámico discreto es *deterministico* si $h_{top}(T) = 0$.

Proposición 2.7.4 *Considere X y Y espacios topológicos compactos. Sean $T : X \to X$ y $S : Y \to Y$ transformaciones continuas. Si $h : X \to Y$ es continua y sobreyectora tal que $h \circ T = S \circ h$, es decir, el siguiente diagrama conmuta,*

$$\begin{array}{ccc} X & \xrightarrow{T} & X \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle h} \\ Y & \xrightarrow[S]{} & Y \end{array}$$

Entonces $h_{top}(T) \geq h_{top}(S)$.

Demostración. Como $h \circ T = S \circ h$, entonces para todo $n \in \mathbb{N}^*$, $h \circ T^n = S^n \circ h$. Luego,

$$\begin{aligned} h^{-1}(S^{-n}(A)) &:= \{x : h(x) \in S^{-n}(A)\} \\ &= \{x : S^n(h(x)) \in A\} = \{x : h(T^n(x)) \in A\} \\ &= \{x : T^n(x) \in h^{-1}(A)\} \\ &:= T^{-n}(h^{-1}(A)). \end{aligned}$$

Sea $\mathcal{V}$ la cobertura abierta de Y, como h es continua, entonces

$$h^{-1}(\mathcal{V}) := \{h^{-1}(A) : A \in \mathcal{V}\}$$

es una cobertura abierta para X. Considere $\{h^{-1}(A_1), h^{-1}(A_2), ..., h^{-1}(A_n)\}$ la subcobertura de menor cardinalidad de $h^{-1}(\mathcal{V})$ y como h es sobreyectiva, se tiene que, $\{A_1, A_2, ..., A_n\}$ es una subcobertura de $\mathcal{V}$ que cubre Y. Así, $N_Y(\mathcal{V}) \leq N_X(h^{-1}(\mathcal{V}))$, sigue que,

$$H(\mathcal{V}) \leq H(h^{-1}(\mathcal{V})).$$

De la Proposición 2.7.2 ítem (4), tenemos, $H(h^{-1}(\mathcal{V})) \leq H(\mathcal{V})$. Luego,

$$H(h^{-1}(\mathcal{V})) = H(\mathcal{V}).$$

Así, usando este resultado,

$$\begin{aligned} h(S,\mathcal{V}) &= \lim_{n\to\infty}\frac{1}{n}H(\mathcal{V}^n) = \lim_{n\to\infty}\frac{1}{n}H(h^{-1}(\mathcal{V}^n)) \\ &= \lim_{n\to\infty}\frac{1}{n}H\left(\bigvee_{j=0}^{n-1}h^{-1}(S^{-j}(\mathcal{V}))\right) \\ &= \lim_{n\to\infty}\frac{1}{n}H\left(\bigvee_{j=0}^{n-1}T^{-j}(h^{-1}(\mathcal{V}))\right) = h(T,h^{-1}(\mathcal{V})). \end{aligned}$$

Luego,

$$\begin{aligned} h_{top}(S) &:= \sup_{\mathcal{V}} h(S,\mathcal{V}) = \sup_{\mathcal{V}} h(T,h^{-1}(\mathcal{V})) \leq h_{top}(T) \\ &\Rightarrow h_{top}(S) \leq h_{top}(T). \end{aligned}$$

■

Observación 2.7.1 Tenemos:

1. Decimos que (X,T) y (S,Y) son *topológicamente conjugados*, si $h : X \to Y$ es un homeomorfismo y $h \circ T = S \circ h$. Luego, $T \circ h^{-1} = h^{-1} \circ S$ y aplicando el mismo argumenta de la prueba de la Proposición 2.7.4, se tiene que, $h_{top}(T) \leq h_{top}(S)$ y, por lo tanto, $h_{top}(T) = h_{top}(S)$.

2. De 1), concluimos que la entropía topológica es un invariante topológico, es decir, que es preservado por conjugaciones.

3. La función h en 1) es llamado aplicación *conjugado* y h en la Proposición 2.7.4 es llamado *semi-conjugado*.

2.7.2. Bola dinámica

Sean X un espacio métrico y $T : X \to X$ una transformación continua, vamos a introducir una nueva distancia.

Definición 2.7.9 Sea $n \in \mathbb{N}$, definimos,

$$d_n(x,y) := \max_{0\leq j\leq n-1} d(T^j(x),T^j(y)), \tag{7}$$

para cualquier $x, y \in X$.

Note que, para $n = 1$, $d_1 = d$ y $d_n \leq d_{n+1}$ para todo $n \in \mathbb{N}$.

Proposición 2.7.5 *La función $d_n : X \times X \to [0, \infty)$ definido en (7) es una métrica en X.*

Demostración. Sean $x, y, z \in X$, entonces, veamos que d_n satisface las condiciones de una métrica.

1. Como d es una métrica en X y por definición, sabemos que, $d_n(x, y) \geq d(T^j(x), T^j(y))$ para $0 \leq j \leq n-1$, entonces $d_n(x, y) \geq 0$. Además, $d_n(x, y) = 0$ si y solamente si $d(T^j(x), T^j(y)) = 0$ para $0 \leq j \leq n-1$, es decir, $d_n(x, y) = 0$ si y solamente si $T^j(x) = T^j(y)$ para $0 \leq j \leq n-1$, lo cual ocurre, si y solamente si $x = y$. Luego, concluimos que, $d_n(x, y) = 0$ si y solamente si $x = y$.

2. La simetría para d_n viene de la simetría de d, pues

$$d_n(x, y) = \max_{0 \leq j \leq n-1} d(T^j(x), T^j(y)) = \max_{0 \leq j \leq n-1} d(T^j(y), T^j(x)) = d_n(y, x).$$

3. Se tiene que,

$$d(T^j(x), T^j(z)) \leq d(T^j(x), T^j(y)) + d(T^j(y), T^j(z))$$

para todo $0 \leq j \leq n-1$, desde que d es una métrica. Luego,

$$\begin{aligned} \max_{0 \leq j \leq n-1} d(T^j(x), T^j(z)) &\leq \max_{0 \leq j \leq n-1} [d(T^j(x), T^j(y)) + d(T^j(y), T^j(z))] \\ &\leq \max_{0 \leq j \leq n-1} d(T^j(x), T^j(y)) + \max_{0 \leq j \leq n-1} d(T^j(y), T^j(z)). \end{aligned}$$

Así, $d_n(x, z) \leq d_n(x, y) + d_n(y, z)$.

Por lo tanto, d_n es una métrica en X.

■

Luego, concluimos que (X, d_n) es un espacio métrico.

Proposición 2.7.6 *Sea (X, d) un espacio métrico compacto. Entonces, (X, d_n) es un espacio métrico compacto.*

Demostración. Considere $\{x_k\}_{k\in\mathbb{N}}$ una sucesión de puntos en X. Como (X, d) es compacto, entonces por el Teorema A.1, existe una sub-sucesión $\{x_{k_m}\}_{m\in\mathbb{N}}$ de $\{x_k\}_{k\in\mathbb{N}}$ que es convergente, digamos que converge para $x \in X$, esto es, dado cualquier $\varepsilon > 0$, existe $m_0 \in \mathbb{N}$ tal que para todo $m \geq m_0$, se tiene que, $d(x_{k_m}, x) < \frac{\varepsilon}{2}$. Ahora, como T es una función continua, tenemos, $d(T(x_{k_m}), T(x)) < \varepsilon$ para $m \geq m_0$. Así, como T^j es continua, de forma análoga, $d(T^j(x_{k_m}), T^j(x)) < \varepsilon$ para $j = 0, 1, ..., n-1$ y para todo $m \geq m_0$. Por lo tanto, dado cualquier $\varepsilon > 0$, existe $m_0 \in \mathbb{N}$ tal que para todo $m \geq m_0$, se tiene que, $d_n(x_{k_m}, x) < \varepsilon$ para $n \in \mathbb{N}$. Luego, concluimos que (X, d_n) es un espacio métrico compacto para cada $n \in \mathbb{N}$.

■

Definición 2.7.10 (Bola dinámica) Dado $\varepsilon > 0$ y $n \in \mathbb{N}$, definimos la *bola dinámica* por,

$$B(x, n, \varepsilon) := \{y \in X : d_n(x, y) < \varepsilon\}$$

centrado en $x \in X$, de radio ε y de tamaño n.

Proposición 2.7.7 *Dado $\varepsilon > 0$ y $n \in \mathbb{N}$. Entonces, $d_n(x, y) < \varepsilon$ si y solamente si, $d(T^j(x), T^j(y)) < \varepsilon$ para todo $j = 0, 1, ..., n-1$.*

Demostración. Suponga que $d_n(x, y) < \varepsilon$, entonces por definición,

$$\max_{0\leq n\leq n-1} d(T^j(x), T^j(y)) < \varepsilon,$$

es decir, $d(T^j(x), T^j(y)) < \varepsilon$ para todo $j \in \{0, 1, ..., n-1\}$.

Ahora, suponga que $d(T^j(x), T^j(y)) < \varepsilon$ para todo $j = 0, 1, ..., n-1$. Así,

$$\max_{0\leq n\leq n-1} d(T^j(x), T^j(y)) < \varepsilon,$$

y, consecuentemente, $d_n(x, y) < \varepsilon$.

■

Corolario 2.7.1 *Tenemos,*

$$B(x,n,\varepsilon)=\bigcap_{j=0}^{n-1}T^{-j}(B(T^j(x),\varepsilon)),$$

para todo $\varepsilon>0$, $n\in\mathbb{N}$ *y* $x\in X$.

Demostración. Sigue inmediatamente de la Proposición 2.7.7.

■

Así, tenemos

$$B(x,n,\varepsilon):=\{y\in X: d(T^j(x),T^j(y)<\varepsilon \ \ \forall\ j=0,1,...,n-1\},$$

que es la intersección finita de bolas abiertas (por Corolario 2.7.1) y, por lo tanto $B(x,n,\varepsilon)$ es abierto.

2.7.3. Entropía a través de conjuntos generadores

Entre 1975 y 1979, Efin Dinabur y Rufus Bowen dan otra definición de la entropía diferente de la definición de Adler–Konheim–McAndrews, pero equivalente, para transformaciones continuas en espacios métricos compactos, a pesar de ser un poco restricto, ella tiene la ventaja de tornar mas transparente, el significado de estas definiciones es: "La entropía topológica es la tasa de crecimiento exponencial de número de órbitas que son distinguibles (o indistinguibles) dentro de cierto grado de precisión arbitrariamente grande (o pequeño)".

Entonces estas definiciones usan la métrica, pero luego veremos que la entropía depende solo de la topología ya que las métricas equivalentes conducen al mismo valor de la entropía topológica.

Vamos considerar (X,d) un espacio métrico compacto y $T: X\to X$ una transformación continua.

Definición 2.7.11 (Conjunto generador) Sea $\varepsilon>0$ y $n\in\mathbb{N}$. Un subconjunto $E\subseteq X$ diferente de vacío es llamado *conjunto* (n,ε)*-generador* si para todo $x\in X$, existe $y\in E$ tal que $d_n(T(x),T(y))<\varepsilon$.

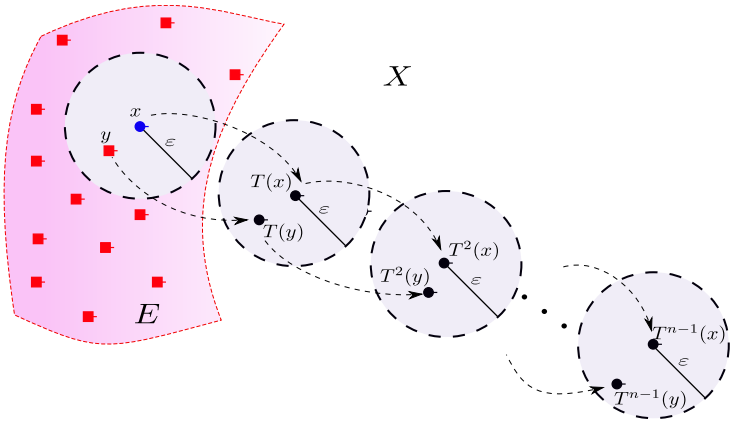


Figura 5: Conjunto generador.

Note que, un subconjunto $E \subseteq X$ ser conjunto (n, ε)-generador significa que vale,

$$X = \bigcup_{y \in E} B(y, n, \varepsilon).$$

Como X es compacto, entonces es cubierto por finitas bolas dinámicas y se concluye que siempre existen conjuntos (n, ε)-generadores E (pues tome $X = E$). Por otro lado, un conjunto (n, ε)-generador E es finito, esto viene, de la compacidad de X lo cual es cubierto por finitas bolas dinámicas.

Veamos un ejemplo de un conjunto (n, ε)-generador, pero antes, tenemos el siguiente resultado.

Lema 2.7.2 *Sea la aplicación doble f definido en el Ejemplo 2.6.1. Entonces, si*

$$d(x, y) \leq \frac{1}{4} \Rightarrow d(f(x), f(y)) = 2d(x, y).$$

Demostración. Si $|x - y| \leq 1/2$, entonces $d(x, y) = |x - y|$. Entonces sean $x, y \in S^1$ tal que $d(x, y) \leq 1/4$. Esto es, $|x - y| \leq 1/4$. Luego,

$$\begin{aligned} d(f(x), f(y)) &= d(2x \mod 1, 2y \mod 1) \\ &= \min\{|2x - 2y \mod 1|, 1 - |2x - 2y \mod 1|\} \end{aligned}$$

Note que, $|2x - 2y| \leq 1/2$, entonces, $2x - 2y \mod 1 = 2x - 2y$. Luego,

$$d(f(x), f(y)) = |2x - 2y| = 2|x - y| = 2d(x, y).$$

■

Definición 2.7.12 (Conjunto diádico) Para $k \in \mathbb{N}$, sea $S_k \subset S^1$ el *conjunto racional diádico* con denominador 2^k, esto es,

$$S_k := \left\{ \frac{i}{2^k} : 0 \leq i \leq 2^k - 1 \right\}.$$

Ejemplo 2.7.3 Para $n \in \mathbb{N}$, S_{n+k} es un conjunto (n, ε)-generador para la función doble f definido en el Ejemplo 2.6.1.

De hecho, sea $\varepsilon > 0$ fijo y escoja $k \geq 2$ tal que $1/2^{k+1} \leq \varepsilon < 1/2^k$. Observe que para cualquier $x \in S^1$, existe $i \in \{0, ..., 2^{n+k} - 1\}$ tal que

$$x \in \left[\frac{i}{2^{n+k}}, \frac{i+1}{2^{n+k}} \right).$$

Luego, sea $y \in S_{n+k}$ para que sea cualquiera de los extremos de este intervalo diádico. Entonces, $d(x, y) \leq 1/2^{n+k} < 1/4$. Usando Lema 2.7.2,

$$d(f(x), f(y)) = 2d(x, y) \leq \frac{2}{2^{n+k}} < \frac{1}{4}, \quad \text{para } n > 1.$$

Nuevamente, usando Lema 2.7.2,

$$d(f^2(x), f^2(y)) = 2d(f(x), f(y)) \leq \frac{2^2}{2^{n+k}} < \frac{1}{4}, \quad \text{para } n > 2,$$

así, aplicando el Lema 2.7.2 j veces, para $0 \leq j \leq n - 1$,

$$\begin{aligned} d(f^j(x), f^j(y)) = 2^j d(x, y) &\leq \frac{2^j}{2^{n+k}} \\ &\leq \frac{2^{n-1}}{2^{n+k}} = \frac{1}{2^{k+1}} \\ &< \varepsilon. \end{aligned}$$

Entonces,

$$d_n(x,y) = \max_{0\leq j\leq n-1} d(f^j(x), f^j(y)) < \varepsilon.$$

Por lo tanto, S_{n+k} es un conjunto (n,ε)-separado.

Queremos hacer que los conjuntos (n,ε)-generados sea los mas pequeño posible. Para eso, tenemos la siguiente definición.

Definición 2.7.13 Sea $\varepsilon > 0$ y $n \in \mathbb{N}$. Definimos la cantidad de órbitas indistinguibles de tamaño n (medidas por ε),

$$g_n(T,\varepsilon) := \min\{\#E : E \subseteq X \text{ es } (n,\varepsilon)\text{-generador}\}$$

Proposición 2.7.8 *$g_n(T,\varepsilon)$ es finito.*

Demostración. Tome $\varepsilon > 0$ y sea $n \in \mathbb{N}$. Considere E un conjunto (n,ε)-generador de X. Por la compacidad de (X,d_n) existen $x_1,...,x_m$ tales que,

$$E \subseteq X \subseteq \bigcup_{j=1}^{m} B(x_j,n,\varepsilon).$$

Por lo tanto, $\#E \leq m$.

■

Definición 2.7.14 La tasa de crecimiento exponencial medio de $g_n(T,\varepsilon)$ conforme n aumenta es definido por

$$g(T,\varepsilon) := \limsup_{n\to\infty} \frac{1}{n} \ln g_n(T,\varepsilon).$$

Proposición 2.7.9 *$\varepsilon \mapsto g(T,\varepsilon)$ es monótona creciente en ε.*

Demostración. Sean $0 < \varepsilon_1 < \varepsilon_2$ y $n \in \mathbb{N}$. Sea $E \subseteq X$ un conjunto (n,ε_1)-generador. Como $\varepsilon_1 \leq \varepsilon_2$, tenemos que $d_n(x,y) < \varepsilon_2$. Así, E es un conjunto (n,ε_2)-generador. Como E es arbitrario, $g_n(T,\varepsilon_1) \leq g_n(T,\varepsilon_2)$. Por lo tanto, $g(T,\varepsilon_1) \leq g(T,\varepsilon_2)$.

■

Definición 2.7.15 (Bowen-Dinaburg) La *entropía topológica* (a través de conjuntos generadores) de T es definido por

$$g(T) := \lim_{\varepsilon\to 0} g(T,\varepsilon).$$

Entonces, $s(T)$ es la tasa de crecimiento exponencial medio del número de segmentos de orbitas indistinguibles de tamaño n, en ese sentido, mide la complejidad del sistema dinámico topológico (X, T).

2.7.4. Entropía a través de conjuntos separados

Definición 2.7.16 (Conjunto separado) Dado $\varepsilon > 0$ y $n \in \mathbb{N}$. Un subconjunto $E \subseteq X$ diferente de vacío es llamado *conjunto* (n, ε)-*separado* para T, se para cualquier $x, y \in E$, $x \neq y$, tenemos que $d_n(x, y) \geq \varepsilon$.

Ejemplo 2.7.4 Para $n \in \mathbb{N}$, el conjunto racional diádico S_{n-1+k} es un conjunto (n, ε)-separado para la función doble f definido en el Ejemplo 2.6.1.

De hecho, sea $\varepsilon > 0$ fijado y escoja $k \geq 2$ tal que $1/2^{k+1} \leq \varepsilon < 1/2^k$. Tome dos puntos distintos $x, y \in S_{n-1+k}$. Queremos probar que $d_n(x, y) \geq \varepsilon$, es decir, queremos probar que existe $j \in \{0, 1, ..., n-1\}$ tal que $d(f^j(x), f^j(y)) \geq \varepsilon$. Suponga que existe j tal que $d(f^j(x), f^j(y)) \geq 1/4$. Como $k \geq 2$, sigue que $1/4 > \varepsilon$.

Ahora, si esto no ocurre, entonces para todo $j \in \{0, 1, ..., n-1\}$, tenemos que $d(f^j(x), f^j(y)) < 1/4$, luego aplicando el Lema 2.7.2 $n-1$ veces,

$$d(f^{n-1}(x), f^{n-1}(y)) = 2^{n-1} d(x, y).$$

Como $x, y \in S_{n-1+k}$ son distintos, tenemos que, $d(x, y) \geq 1/2^{n-1+k}$, entonces,

$$\begin{aligned} d(f^{n-1}(x), f^{n-1}(y)) &= 2^{n-1} d(x, y) \\ &\geq \frac{2^{n-1}}{2^{n-1+k}} = \frac{1}{2^k} \\ &> \varepsilon. \end{aligned}$$

Por lo tanto, S_{n-1+k} es un conjunto (n, ε)-separado.

En el siguiente resultado, veremos que dos elementos de E no pueden estar en la misma bola dinámica.

Proposición 2.7.10 *Un conjunto (n,ε)-separado $E \subseteq X$ es equivalente a,*

$$B(x,n,\varepsilon) \cap E = \{x\} \tag{8}$$

para cada $x \in E$.

Demostración. Suponga que $E \subseteq X$ sea un conjunto (n,ε)-separado. Tomemos $w, z \in B(x,n,\frac{\varepsilon}{2}) \cap E$ tal que $w \neq z$. Entonces, $d_n(w,x) < \frac{\varepsilon}{2}$ y $d_n(z,x) < \frac{\varepsilon}{2}$. Luego,

$$d_n(w,z) \leq d_n(w,x) + d_n(x,z) < \varepsilon,$$

absurdo, pues $d_n(w,z) > \varepsilon$, desde que $z, w \in E$. Por lo tanto, $B(x,n,\varepsilon) \cap E = \{x\}$, para cada $x \in E$.

El recíproco es trivial, pues si $w, z \in E$ con $w \neq z$, entonces de la ecuación (8) se tiene que, $d_n(w,z) \geq \varepsilon$.

■

Lema 2.7.3 *Un conjunto (n,ε)-separado $E \subseteq X$ es finito.*

Demostración. Suponga por contradicción, que E sea un conjunto infinito. Entonces, tome una sucesión $\{x_k\}_{k\in\mathbb{N}}$ en E dos a dos distintos. Como por la Proposición 2.7.6, (X,d_n) es compacto, existe $\{x_{k_m}\}_{m\in\mathbb{N}}$ una sub-sucesión convergente. Esto implica que $\{x_{k_m}\}_{m\in\mathbb{N}}$ es una sucesión de Cauchy, entonces, existen $l, j \in \mathbb{N}$ suficientemente grandes tal que,

$$d_n(x_{k_l}, x_{k_j}) < \varepsilon,$$

esto es una contradicción, desde que, E es un conjunto (n,ε)-separado. Por lo tanto, E es un conjunto finito.

■

Lema 2.7.4 *Se tiene que* $\sup\{\#E : E \subseteq X \text{ y } E \text{ es } (n,\varepsilon)\text{-separado}\} < \infty$.

Demostración. Como por la Proposición 2.7.6, (X,d_n) es compacto; entonces para $\varepsilon > 0$ dado, existen $x_1, x_2, ..., x_l$ tales que,

$$E \subseteq X \subseteq \bigcup_{i=1}^{l} B\left(x_i, n, \varepsilon\right).$$

Note que l no depende de E. Ahora, desde que E es (n,ε)-separado y

$$E \subseteq \bigcup_{i=1}^{l} B\left(x_i, n, \varepsilon\right);$$

entonces de la Proposición 2.7.10, tenemos que $\#E \leq l$.

■

Ahora, queremos hacer que los conjuntos (n,ε)-separados sean tan grandes como sea posible. Así definimos:

Definición 2.7.17 Dado $\varepsilon > 0$ y $n \in \mathbb{N}$. El número de órbitas distinguibles de tamaño n (medidas por ε) es definido por

$$s_n(T,\varepsilon) := \text{máx}\{\#E : E \subseteq X \text{ y } E \text{ es } (n,\varepsilon)\text{-separado}\}.$$

Observe que, de la demostración de el Lema 2.7.4, E no depende de l, así, sigue que $s_n(T,\varepsilon) \geq 1$.

Definición 2.7.18 La tasa de crecimiento exponencial medio de $s_n(T,\varepsilon)$ conforme n crece, es definido por

$$s(T,\varepsilon) := \lim_{n\to\infty} \sup \frac{1}{n} \ln s_n(T,\varepsilon).$$

Proposición 2.7.11 *Se tiene que, $\varepsilon \mapsto s(T,\varepsilon)$ es monótona en ε.*

Demostración. Tome $0 < \varepsilon_1 < \varepsilon_2$ y sea $E \subset X$ un conjunto (n,ε_2)-separado para T. Ahora, como $\varepsilon_1 < \varepsilon_2$, se obtiene que, $d_n(x,y) > \varepsilon_1$. Así, $E \subset X$ es un conjunto (n,ε_1)-separado para T. Como E es arbitrario, se concluye

$$s_n(T,\varepsilon_1) \geq s_n(T,\varepsilon_2).$$

Luego, $s(T,\varepsilon_1) \geq s(T,\varepsilon_2)$. Por lo tanto, $\varepsilon \mapsto s(T,\varepsilon)$ es monótona (decreciente) en ε

■

Definición 2.7.19 (Bowen-Dinaburg) Definimos la entropía topológica (a través de conjuntos separados) de T por

$$s(T) := \lim_{\varepsilon\to 0} s(T,\varepsilon).$$

Entonces, $s(T)$ puede interpretarse como la medida del crecimiento exponencial medio del número de segmentos de órbita distinguibles de tamaño n. En este sentido, $s(T)$ mide la complejidad del sistema dinámico topológico (X, T).

Observación 2.7.2 Bowen y Dinaburg extendieron las definiciones de entropía topológica (vía conjuntos generadores y separados) para X que no sea compacto, pero bajo el supuesto que T sea uniformemente continua.

Veamos algunas propiedades y ejemplos.

Proposición 2.7.12 *Si X es un conjunto finito, entonces la entropía de cualquier transformación continua $T : X \to X$ es cero.*

Demostración. Dado $\varepsilon > 0$ y $n \in \mathbb{N}$, existe $C > 0$ tal que $s_n(T, \varepsilon) \leq C$. Entonces,

$$s(T, \varepsilon) := \lim_{n\to\infty} \sup \frac{1}{n} \ln s_n(T, \varepsilon) \leq \lim_{n\to\infty} \sup \frac{1}{n} \ln(C) = 0.$$

Por lo tanto, $s(T) = 0$.

■

Decimos que una transformación $T : X \to X$ es una *isometria* se

$$d(x, y) = d(T(x), T(y)).$$

Proposición 2.7.13 *Sea una transformación continua $T : X \to X$ una isometria. Entonces, la entropía de T es cero.*

Demostración. Como T es una isometria, tenemos que $d_n(x, y) = d_1(x, y) = d(x, y)$ para todo $n \in \mathbb{N}$ y todo $x, y \in X$. Entonces, $s_n(T, \varepsilon) = s_1(T, \varepsilon)$. Luego,

$$s(T, \varepsilon) = \lim_{n\to\infty} \sup \frac{1}{n} \ln s_n(T, \varepsilon) = \lim_{n\to\infty} \sup \frac{1}{n} \ln s_1(T, \varepsilon) = 0.$$

Por lo tanto, $s(T) = 0$.

■

Ejemplo 2.7.5 Para la aplicación rotacional R_α definido en el Ejemplo 2.6.2, se tiene que, $s(R_\alpha) = 0$.

Primero note que $(\mathbb{T}, d)$ es un espacio métrico compacto (por el Ejemplo A.3). Vamos a ver que R_α es una transformación isometrica, así, el resultado sigue de la Proposición 2.7.13.

Note que, para $x, y \in \mathbb{T}$,

$$\begin{aligned} d(R_\alpha(x), R_\alpha(y)) &= \text{mín}\{|R_\alpha(x) - R_\alpha(y)|, 1 - |R_\alpha(x) - R_\alpha(y)|\} \\ &= \text{mín}\{|x + \alpha - y - \alpha \mod 1|, 1 - |x + \alpha - y - \alpha \mod 1|\} \\ &= \text{mín}\{|x - y|, 1 - |x - y|\} \\ &= d(x, y). \end{aligned}$$

Luego, R_α es una isometria (luego es continua[4]) y sigue que $s(R_\alpha) = 0$.

2.7.5. Equivalencia de las tres definiciones de la entropía

Ahora, nuestro objetivo es probar que estas definiciones coinciden para (X, d) un espacio métrico compacto y $T : X \to X$ una transformación continua.

Proposición 2.7.14 *Dado $\varepsilon > 0$ y $n \in \mathbb{N}$, tenemos que,*

$$g_n(T, \varepsilon) \leq s_n(T, \varepsilon) \leq g_n(T, \varepsilon/2).$$

Demostración. 1). Sea $s_n(T, \varepsilon)$ la máxima cardinalidad de un conjunto $E \subseteq X$ (n, ε)-separado. Probemos que E es un conjunto (n, ε)-generador. Suponga que E no es un conjunto (n, ε)-generador, entonces existe $y \in X$ tal que $d_n(x, y) \geq \varepsilon$ para todo $x \in E$. Luego, $E \cup \{y\}$ es un conjunto (n, ε)-separador, absurdo, pues E es un conjunto (n, ε)-separado de máxima cardinalidad. Esto significa que,

$$s_n(T, \varepsilon) \in \{\#F : F \subseteq X \text{ es } (n, \varepsilon)\text{-generador}\}.$$

Por lo tanto,

$$g_n(T, \varepsilon) := \text{mín}\{\#F : F \subseteq X \text{ es } (n, \varepsilon)\text{-generador}\} \leq s_n(T, \varepsilon).$$

[4]Dado cualquier $\varepsilon > 0$ tome $\delta = \varepsilon$, entonces si, $d(x, y) < \delta$, entonces $d(R_\alpha(x), R_\alpha(y)) < \varepsilon$ para cualquier $x, y \in \mathbb{T}$.

2). Sea E un conjunto (n,ε)-separado y F un conjunto $(n,\varepsilon/2)$-generador. Ahora, considere la transformación $\varphi : E \to F$ tal que $d_n(x,\varphi(x)) < \varepsilon/2$.

Probemos que φ es inyectiva. Sean $x, y \in E$ tal que $\varphi(x) = \varphi(y)$, mostraremos que $x = y$. Note que,

$$\begin{aligned} d_n(x,y) &\leq d_n(x,\varphi(x)) + d_n(\varphi(x),y) \\ &= d_n(x,\varphi(x)) + d_n(y,\varphi(y)) \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon. \end{aligned}$$

Como E es un conjunto (n,ε)-separado, se concluye que $x = y$. Luego, φ es inyectiva. Así, sigue que $\#E \leq \#F$. Como E y F son arbitrarios,

$$\{\#E : E \subseteq X \text{ es } (n,\varepsilon)\text{-separado}\} \subseteq \{\#F : F \subseteq X \text{ es } (n,\varepsilon/2)\text{-generador}\}.$$

Por lo tanto, $s_n(T,\varepsilon) \leq g_n(T,\varepsilon/2)$.

■

Proposición 2.7.15 *Tenemos que,* $s(T) = g(T)$.

Demostración. De la Proposición 2.7.14, $g_n(T,\varepsilon) \leq s_n(T,\varepsilon) \leq g_n(T,\varepsilon/2)$. Luego,

$$\frac{1}{n}\ln g_n(T,\varepsilon) \leq \frac{1}{n}\ln s_n(T,\varepsilon) \leq \frac{1}{n}\ln g_n(T,\varepsilon/2).$$

Aplicando lím sup,

$$\limsup_{n\to\infty} \frac{1}{n}\ln g_n(T,\varepsilon) \leq \limsup_{n\to\infty} \frac{1}{n}\ln s_n(T,\varepsilon) \leq \limsup_{n\to\infty} \frac{1}{n}\ln g_n(T,\varepsilon/2).$$

Esto es, $g(T,\varepsilon) \leq s(T,\varepsilon) \leq g(T,\varepsilon/2)$. Ahora, como $\varepsilon \mapsto g(T,\varepsilon)$ y $\varepsilon \mapsto s(T,\varepsilon)$ son monótonas en ε,

$$\lim_{\varepsilon\to 0} g(T,\varepsilon) \leq \lim_{\varepsilon\to 0} s(T,\varepsilon) \leq \lim_{\varepsilon\to 0} g(T,\varepsilon/2),$$

o sea, $g(T) \leq s(T) \leq g(T)$. Por lo tanto, $g(T) = s(T)$.

■

Dado cualquier $A \subseteq X$, definimos,

$$\operatorname{diam}(A) := \sup\{d(x,y) : x, y \in A\}.$$

Definición 2.7.20 Para una cobertura abierta de X, definimos,

$$\operatorname{diam}(\mathcal{U}) := \sup\{\operatorname{diam}(U) : U \text{ es abierto de } \mathcal{U}\}.$$

Proposición 2.7.16 *Sea $\mathcal{U}$ una cobertura abierta de X con $\operatorname{diam}(\mathcal{U}) \leq \varepsilon$. Entonces, dado $x, y \in U$, donde $U \in \mathcal{U}^n$, se tiene que, $d_n(x, y) < \varepsilon$.*

Demostración. Note que, si $U \in \mathcal{U}^n$, entonces,

$$U = \bigcap_{j=0}^{n-1} T^{-j}(U_j),$$

donde, $U_j \in \mathcal{U}$ para $j = 0, 1, ..., n-1$. Observe que, si $x, y \in U$, entonces $x, y \in T^{-j}(U_j)$, luego, $T^j(x), T^j(y) \in U_j$ para $j = 0, 1, ..., n-1$. Así,

$$d(T^j(x), T^j(y)) < \varepsilon, \quad \forall\ j = 0, 1, ..., n-1.$$

Por lo tanto, $d_n(x, y) < \varepsilon$.

■

Teorema 2.7.1 *Se tiene que, $h_{top}(T) = s(T) = g(T)$.*

Demostración. Tome $\varepsilon > 0$ y $n \in \mathbb{N}$.

1). Veamos que, $s(T) \leq h_{top}(T)$. Dado $\varepsilon > 0$, sean $E \subseteq X$ un conjunto (n, ε)-separado de máxima cardinalidad $s_n(T, \varepsilon)$ y $\mathcal{U}$ una cobertura abierta de X con $\operatorname{diam}(\mathcal{U}) \leq \varepsilon$.

Ahora, como E es un conjunto (n, ε)-separado, entonces por la Proposición 2.7.16, cada elemento de $\mathcal{U}^n$ solo puedo contener lo máximo un elemento de E, pues si contiene mas elementos distintos, digamos x y z en $E \cap U$ (donde $U \in \mathcal{U}^n$), entonces $d_n(x, z) > \varepsilon$ lo cual es una contradicción (pues $d_n(x, z) < \varepsilon$). Entonces,

$$s_n(T, \varepsilon) \leq N(\mathcal{U}^n).$$

Luego,

$$\frac{1}{n} \ln s_n(T, \varepsilon) \leq \frac{1}{n} \ln N(\mathcal{U}^n) = \frac{1}{n} H(\mathcal{U}^n).$$

Así,

$$s(T,\varepsilon) := \limsup_{n\to\infty} \frac{1}{n} \ln s_n(T,\varepsilon) \leq \limsup_{n\to\infty} \frac{1}{n} H(\mathcal{U}^n) = \lim_{n\to\infty} \frac{1}{n} H(\mathcal{U}^n) := h(T,\mathcal{U}).$$

Entonces,

$$s(T,\varepsilon) \leq h(T,\mathcal{U}) \leq \sup_{\mathcal{U}} h(T,\mathcal{U}) := h_{top}(T).$$

Por lo tanto,

$$s(T) := \lim_{\varepsilon\to 0} s(T,\varepsilon) \leq h_{top}(T).$$

2). Veamos que, $h_{top}(T) \leq g(T)$. Sea $E \subseteq X$ un conjunto (n,ε)-generador de cardinalidad mínima $g_n(T,\varepsilon)$. Como X es compacto, por el Lema A.1, toda cobertura abierta $\mathcal{U}$ de X posee un número de Lebesgue, digamos $\varepsilon > 0$.

Dado $x \in E$ y $j = 0, 1, ..., n-1$, existe $U_{x,j} \in \mathcal{U}$ tal que $B(T^j(x),\varepsilon) \subset U_{x,j}$. Entonces,

$$B(x,n,\varepsilon) \subset \bigcap_{j=0}^{n-1} T^{-j}(U_{x,j}).$$

Como E es un conjunto (n,ε)-generado,

$$X = \bigcup_{x\in E} B(x,n,\varepsilon) \subseteq \bigcup_{x\in E} \left(\bigcap_{j=0}^{n-1} T^{-j}(U_{x,j}) \right).$$

Así,

$$\mathcal{V} := \left\{ \bigcap_{j=0}^{n-1} T^{-j}(U_{x,j}) \right\}_{x\in E}$$

es una cobertura abierta de X. Note que, $\mathcal{V} \leq \mathcal{U}^n$ ($\mathcal{U}^n$ es refinamiento de $\mathcal{V}$) y $\mathcal{V}$ tiene $g_n(T,\varepsilon)$ elementos. Sabemos que,

$$N(\mathcal{U}^n) = \text{mín}\{m \in \mathbb{N} : \mathcal{U}_1 \text{ es subcobertura de } \mathcal{U}^n\}$$

(note que $\mathcal{V}$ es uno de esos subcoberturas $\mathcal{U}_1$ y m es uno de esos $g_n(T,\varepsilon)$). Entonces,

$$N(\mathcal{U}^n) \leq g_n(T,\varepsilon) \Rightarrow \frac{1}{n} H(\mathcal{U}^n) = \frac{1}{n} \ln N(\mathcal{U}^n) \leq \frac{1}{n} \ln g_n(T,\varepsilon).$$

Así,

$$\lim_{n\to\infty}\frac{1}{n}H(\mathcal{U}^n)=\limsup_{n\to\infty}\frac{1}{n}H(\mathcal{U}^n)\leq\limsup_{n\to\infty}\frac{1}{n}\ln g_n(T,\varepsilon):=g(T,\varepsilon).$$

Luego, $h(T,\mathcal{U})\leq g(T,\varepsilon)$. Ahora, si escogemos $\varepsilon_1<\varepsilon$, entonces, todo lo que hicimos anteriormente es valido (pues ε_1 es también número de Lebesgue por el Corolário A.1), o sea, $h(T,\mathcal{U})\leq g(T,\varepsilon_1)$ para toda cobertura abierta $\mathcal{U}$ con número de Lebesgue $\varepsilon_1>0$ (note que aquí, $\mathcal{U}$ está fijo, pero ε está variando). Así, haciendo $\varepsilon_1\to 0$,

$$h(T,\mathcal{U})\leq g(T).$$

Como $\mathcal{U}$ es una cobertura abierta arbitrario de X, se tiene,

$$h_{top}(T):=\sup_{\mathcal{U}}h(T,\mathcal{U})\leq g(T).$$

Luego, $s(T)\leq h_{top}(T)\leq g(T)$ y de la Proposición 2.7.15, tenemos que $s(T)=g(T)$, así, obtenemos que,

$$h_{top}(T)=s(T)=g(T).$$

■

III. METODOLOGÍA

3.1. Tipo de investigación

La investigación es de tipo explicativo y la metodología usada es inductivo - deductivo tratando de ser lo más exhaustivo posible en cada demostración.

3.2. Diseño de investigación

El presente trabajo de investigación primeramente esta dirigido a hacer un esbozo de la prueba de TNP, éste nos dice que para $x > 0$ suficientemente grande, la cantidad de números primos entre 1 y x (denotado por $\pi(x)$) es aproximadamente a $\frac{x}{\ln x}$. Para esto, primero empezamos con un Teorema que envuelve las funciones de Tchebychev, éste nos dice que el limite superior (e inferior) de $\pi(x)/x(\ln x)^{-1}$, $\vartheta(x)/x$ y $\psi(x)/x$ coinciden. El segundo paso es encontrar una formula asintótica para $\psi_1(x) = \int_0^x \psi(x)dx$ (este paso es el mas difícil, lo cual no sera demostrado, ver **Ingham (1990)**). Estos dos resultados concluyen la prueba.

Para probar que TNP es equivalente al valor medio de sumatorio de la función de Möbius $\boldsymbol{\mu}(n)$ para n suficientemente grande es nula, primero empezamos estudiar diversos resultados técnicos que envuelven la función de Möbius, la función contadora de divisores de un número natural, y función máximo entero. Con estos resultados concluimos la prueba.

El Teorema de Davenport afirma la correlación del comportamiento de la función de Möbius con las funciones definidos en el circulo unitario complejo. Presentamos una versión equivalente a este teorema, para lo cual usamos la definición de la notación O grande de Bachmann-Landau.

La conjetura de Sarnak afirma que la función de Möbius es ortogonal a cualquier sucesión realizado en un sistema dinámico discreto (X, T) con entropía topológica cero . Para entender esto, definimos la entropía topológica y estudiamos sus diversos propiedades. En realidad definimos de tres maneras y luego vemos que estas definiciones coinciden en un espacio métrico compacto.

Probamos que la sucesión formado por los valores de la función de Möbius no tiene entropía topológica cero. Para ello, primero encontramos dos sub-espacios de shift. El segundo paso es ver que las aplicaciones shifts en estos sub-espacios son semi-conjugados. Luego, se concluye la prueba.

Finalmente mostramos que el TNP y teorema de Davenport satisfacen la conjetura de Sarnak. Para esto, primero buscamos dos sistemas dinámicos específicos. El segundo paso es buscar sucesiones realizados en dichos sistemas dinámicos que tengan entropía topológica cero.

3.3. Población y muestra

Por ser nuestro trabajo netamente abstracto no existe población que estudiar, sin embargo, nuestro estudio se encuentra inmerso dentro de Sistemas Dinámicos y Teoría Analítica de Números.

IV. RESULTADOS

4.1. Teorema de Números Primos - TNP

4.1.1. Enunciado

Recordando, la función contadora de números primos $\pi : [1, \infty) \to \mathbb{N}$ es definido por

$$\pi(x) := \#\{p \in \mathbb{P} : p \leq x\}.$$

A continuación tenemos un resultado fundamental que muestra la distribución de números primos en los enteros positivos $\mathbb{N}$, conjeturado por Gauss en 1792 y por Legendre en 1798. Finalmente demostrado en 1986, independientemente, por Hadamard y De la Vallée Poussin.

Teorema 4.1.1 (TNP) *Tenemos,*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1.$$

En la siguiente tabla, tenemos la comparación de la función $\pi(x)$ con $x/\ln x$, es decir, para x suficientemente grande,

$$\frac{\pi(x)}{x/\ln x}$$

se aproxima a 1. Esto significa que, $\pi(x)$ es asintóticamente igual a $\frac{x}{\ln x}$ para x suficientemente grande.

x	$\pi(x)$	$\frac{x}{\ln x}$	$\frac{\pi(x)}{x/\ln x}$
10	4	4.3	0.93
10^2	25	21.7	1.15
10^3	168	144.9	1.16
10^4	1229	1086	1.11
10^5	9592	8686	1.10
10^6	78498	72464	1.08
10^7	664579	621118	1.07
10^8	5761455	543780	1.06
10^9	50847534	48309180	1.05
10^{10}	455052512	434294482	1.048

Tenemos el siguiente gráfico de $\pi(x)$ y $\frac{x}{\ln x}$

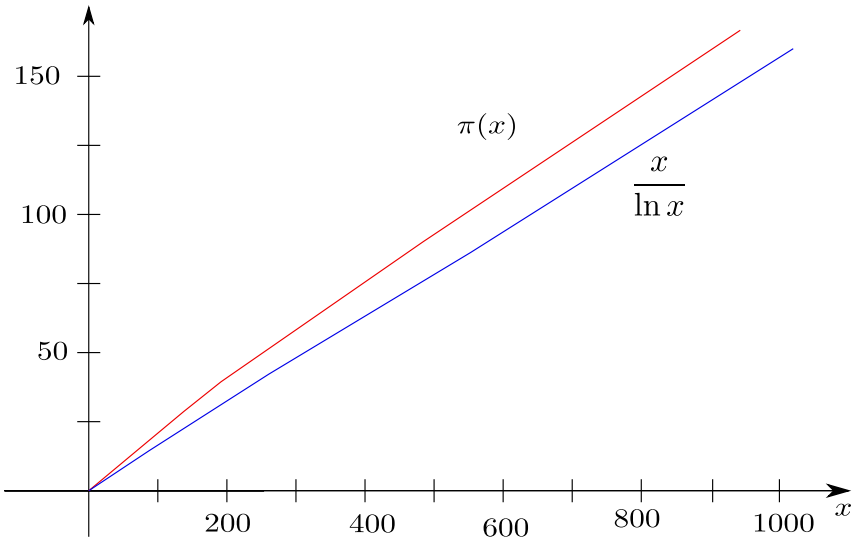


Figura 6: Gráfico comparativo de $\pi(x)$ y $\frac{x}{\ln x}$.

Definimos la función

$$\psi_1(x) = \int_0^x \psi(u)du = \int_1^x \psi(u)du,$$

donde ψ es la función auxiliar de Tchebychev,

$$\psi(x) := \sum_{\substack{n\in\mathbb{N}\\ n\leq x}} \Lambda(n),$$

y Λ es la función de Von Mangolt.

El paso principal para probar TNP es encontrar una fórmula asintótica para ψ_1 y, presentamos tal fórmula en el siguiente teorema:

Teorema 4.1.2 *Tenemos*

$$\lim_{x\to\infty} \frac{\psi_1(x)}{x^2} = \frac{1}{2}.$$

La demostración de este teorema se basa en probar que la *Función zeta de Riemann*[5] no tiene ceros de la forma $1 + it$ (números complejos), pero en este trabajo no vamos mostrar este resultado. El lector interesado puede consultar en el Capítulo 2, Teorema 11 en **Ingham (1990)**.

4.1.2. Esbozo de la prueba de TNP

Presentamos a continuación un resultado conforme **Ingham (1990)**, que es prácticamente la demostración de TNP.

Teorema 4.1.3 *Tenemos que,*

$$\lim_{x\to\infty} \frac{\psi(x)}{x} = 1.$$

Demostración. Consideremos α y β tal que $0 < \alpha < 1 < \beta$. Como $\psi(u)$ es una función creciente en u, tenemos que

$$\begin{aligned}\psi(x) &\leq \frac{1}{\beta x - x}\int_x^{\beta x} \psi(u)du = \frac{1}{\beta x - x}\left(\int_1^{\beta x} \psi(u)du - \int_1^{x} \psi(u)du\right)\\ &= \frac{1}{\beta x - x}(\psi_1(\beta x) - \psi_1(x)),\end{aligned}$$

y así,

$$\frac{\psi(x)}{x} \leq \frac{1}{(\beta-1)x^2}(\psi_1(\beta x) - \psi_1(x)) = \frac{1}{\beta - 1}\left(\beta^2\frac{\psi_1(\beta x)}{(\beta x)^2} - \frac{\psi_1(x)}{x^2}\right).$$

[5] **Función zeta de Riemann**: La función $\zeta : \mathbb{N} \to \mathbb{C}$ definido por

$$\zeta(n) := \sum_{n=1}^{\infty} \frac{1}{n^s},$$

donde $s \in \mathbb{C}$ con parte real mayor que uno, es llamdo función zeta de Riemann.

Fijando β. Como por el Teorema 4.1.2, $\lim\limits_{x\to\infty}\dfrac{\psi_1(x)}{x^2}=\dfrac{1}{2}$,

$$\begin{aligned}\limsup_{x\to\infty}\frac{\psi(x)}{x}&\leq\frac{1}{\beta-1}\left(\frac{\beta^2}{2}-\frac{1}{2}\right)=\frac{1}{2}\cdot\frac{\beta^2-1}{\beta-1}\\&=\frac{1}{2}(\beta+1).\end{aligned}\tag{9}$$

Similarmente, considerando $\int_{\alpha x}^{x}\psi(u)du$, obtenemos,

$$\begin{aligned}\liminf_{x\to\infty}\frac{\psi(x)}{x}&\geq\frac{1}{1-\alpha}\left(\frac{1}{2}-\frac{\alpha^2}{2}\right)=\frac{1}{2}\cdot\frac{1-\alpha^2}{1-\alpha}\\&=\frac{1}{2}(\alpha+1).\end{aligned}\tag{10}$$

Ahora, haciendo $\beta\to 1$ en (9) y $\alpha\to 1$ en (10),

$$\limsup_{x\to\infty}\frac{\psi(x)}{x}\leq 1\leq\liminf_{x\to\infty}\frac{\psi(x)}{x}.$$

Luego, como,

$$\liminf_{x\to\infty}\frac{\psi(x)}{x}\leq\limsup_{x\to\infty}\frac{\psi(x)}{x},$$

obtenemos que,

$$\lim_{x\to\infty}\frac{\psi(x)}{x}=1.$$

■

Por fin presentamos el esbozo de la demostración del Teorema 4.1.1

Demostración. Por el Teorema 4.1.3,

$$\begin{aligned}1&=\lim_{x\to\infty}\frac{\psi(x)}{x}=\limsup_{x\to\infty}\frac{\psi(x)}{x}=\liminf_{x\to\infty}\frac{\psi(x)}{x}\\&=\limsup_{x\to\infty}\frac{\pi(x)}{x/\ln x}=\liminf_{x\to\infty}\frac{\pi(x)}{x/\ln x},\quad\text{por el Teorema 2.5.1,}\\&=\lim_{x\to\infty}\frac{\pi(x)}{x/\ln x}.\end{aligned}$$

Por lo tanto,

$$\lim_{x\to\infty}\frac{\pi(x)}{x/\ln x}=1.$$

■

4.2. Equivalencia a TNP

En esta sección probemos el siguiente resultado (conforme **Apostol (1998)**).

Teorema 4.2.1 *TNP es equivalente a*

$$\lim_{x\to\infty}\frac{1}{x}\sum_{\substack{n\in\mathbb{N}\\ n\leq x}}\boldsymbol{\mu}(n)=0. \tag{11}$$

4.2.1. Preparación

De la Proposición 2.3.4,

$$\sum_{\substack{n\in\mathbb{N}\\ n\leq x}}\boldsymbol{\mu}(n)\left\lfloor\frac{x}{n}\right\rfloor=\sum_{\substack{n\in\mathbb{N}\\ n\leq x}}\sum_{d|n}\boldsymbol{\mu}(d)=\sum_{\substack{n\in\mathbb{N}\\ n\leq x}}\left\lfloor\frac{1}{n}\right\rfloor=1. \tag{12}$$

Tenemos el siguiente resultado útil.

Lema 4.2.1 *Para $x\geq 1$,*

$$\left|\sum_{\substack{n\in\mathbb{N}\\ n\leq x}}\frac{\boldsymbol{\mu}(n)}{n}\right|\leq 1.$$

Demostración. Si $x<2$, entonces $n=1$ y así, $\boldsymbol{\mu}(1)=1$ y vale la igualdad. Así, suponga que $x\geq 2$. Luego, de (12),

$$\begin{aligned}1&=\sum_{\substack{n\in\mathbb{N}\\ n\leq x}}\boldsymbol{\mu}(n)\left\lfloor\frac{x}{n}\right\rfloor=\sum_{\substack{n\in\mathbb{N}\\ n\leq x}}\boldsymbol{\mu}(n)\left(\frac{x}{n}-\left\{\frac{x}{n}\right\}\right)\\ &=x\sum_{\substack{n\in\mathbb{N}\\ n\leq x}}\frac{\boldsymbol{\mu}(n)}{n}-\sum_{\substack{n\in\mathbb{N}\\ n\leq x}}\boldsymbol{\mu}(n)\left\{\frac{x}{n}\right\}\\ &\Rightarrow x\sum_{\substack{n\in\mathbb{N}\\ n\leq x}}\frac{\boldsymbol{\mu}(n)}{n}=1+\sum_{\substack{n\in\mathbb{N}\\ n\leq x}}\boldsymbol{\mu}(n)\left\{\frac{x}{n}\right\}.\end{aligned}$$

Como $0\leq\{x/n\}<1$ y $|\boldsymbol{\mu}(n)|\leq 1$, tenemos que,

$$x\left|\sum_{\substack{n\in\mathbb{N}\\ n\leq x}}\frac{\boldsymbol{\mu}(n)}{n}\right| = \left|1+\sum_{\substack{n\in\mathbb{N}\\ n\leq x}}\boldsymbol{\mu}(n)\left\{\frac{x}{n}\right\}\right| \leq 1+\sum_{\substack{n\in\mathbb{N}\\ n\leq x}}\left\{\frac{x}{n}\right\}$$
$$= 1+\{x\}+\sum_{\substack{n\in\mathbb{N}\\ 2\leq n\leq x}}\left\{\frac{x}{n}\right\}$$
$$< 1+\{x\}+\lfloor x\rfloor - 1 = x.$$

Por lo tanto,

$$\left|\sum_{\substack{n\in\mathbb{N}\\ n\leq x}}\frac{\boldsymbol{\mu}(n)}{n}\right| < 1.$$

■

Presentamos la siguiente función debido al matemático polonés Franz Mertens. De hecho, la notación $\boldsymbol{\mu}(n)$ para la función de Möbius fue introducido por él.

Definición 4.2.1 La función $M : [1,\infty) \to \mathbb{Z}$ definido por

$$M(x) := \sum_{\substack{n\in\mathbb{N}\\ n\leq x}}\boldsymbol{\mu}(n)$$

es llamado la *función de Mertens*.

Ahora, sea la función $H : [1,\infty) \to \mathbb{R}$ definido por

$$H(x) := \sum_{\substack{n\in\mathbb{N}\\ n\leq x}}\boldsymbol{\mu}(n)\ln n.$$

Lema 4.2.2 *Vale la siguiente afirmación,*

$$\lim_{x\to\infty}\left(\frac{M(x)}{x}-\frac{H(x)}{x\ln x}\right) = 0.$$

Demostración. De Lema 2.4.1 (Identidad de Abel), con $a(n) := \boldsymbol{\mu}(n)$, $f(x) := \ln x$ y

$y := 1$, obtenemos,

$$H(x) = \sum_{\substack{n\in\mathbb{N}\\ n\leq x}} \boldsymbol{\mu}(n)\ln n = M(x)\ln x - M(1)\ln 1 - \int_1^x \frac{M(t)}{t}dt$$
$$= M(x)\ln x - \int_1^x \frac{M(t)}{t}dt.$$

Como, $x > 1$, tenemos,

$$\frac{M(x)}{x} - \frac{H(x)}{x\ln x} = \frac{1}{x\ln x}\int_1^x \frac{M(t)}{t}dt$$

Para finalizar la prueba, basta mostrar que,

$$\lim_{x\to\infty} \frac{1}{x\ln x}\int_1^x \frac{M(t)}{t}dt = 0. \tag{13}$$

Observe que, $M(x) = \mathrm{O}(x)$, pues,

$$\left|\sum_{\substack{n\in\mathbb{N}\\ n\leq x}} \boldsymbol{\mu}(n)\right| \leq \sum_{\substack{n\in\mathbb{N}\\ n\leq x}} |\boldsymbol{\mu}(n)| \leq \sum_{\substack{n\in\mathbb{N}\\ n\leq x}} 1 \leq x.$$

Así, por la Proposición 2.2.5,

$$\int_1^x \frac{M(t)}{t}dt = \mathrm{O}\left(\int_1^x dt\right) = \mathrm{O}(x).$$

Luego,

$$\frac{1}{x\ln x}\int_1^x \frac{M(t)}{t}dt = \mathrm{O}\left(\frac{1}{\ln x}\right).$$

Entonces, usando la definición de O grande, existe una constante $C > 0$ tal que

$$0 \leq \left|\frac{1}{x\ln x}\int_1^x \frac{M(t)}{t}dt\right| \leq \frac{C}{\ln x}$$

para x suficientemente grande. Como $\frac{C}{\ln x} \to 0$ cuando $x \to \infty$, tenemos la ecuación (13).

■

Observación 4.2.1 Note que si uno de las funciones $M(x)/x$ o $H(x)/x\ln x$ converge en el Lema 4.2.2, entonces también lo hace el otro y los dos limites coinciden.

4.2.2. Prueba del Teorema 4.2.1

Demostración. *a*). Probemos que TNP implica (11). Por el Teorema 4.1.3, TNP es equivalente a

$$\lim_{x\to\infty}\frac{\psi(x)}{x}=1.$$

Según Lema 4.2.2, basta mostrar que,

$$\lim_{x\to\infty}\frac{H(x)}{x\ln x}=0.$$

Por el Corolario 2.3.3,

$$-\boldsymbol{\mu}(n)\ln n=\sum_{d|n}\boldsymbol{\mu}(d)\Lambda\left(\frac{n}{d}\right).$$

Sumando sobre todo $n\in\mathbb{N}$ con $n\leq x$ la ecuación arriba, y usando la Proposición 2.3.8 con $f=\boldsymbol{\mu}$ y $g=\Lambda$, obtenemos,

$$\begin{aligned}-H(x)&=-\sum_{\substack{n\in\mathbb{N}\\ n\leq x}}\boldsymbol{\mu}(n)\ln n=\sum_{\substack{n\in\mathbb{N}\\ n\leq x}}\sum_{d|n}\boldsymbol{\mu}(d)\Lambda\left(\frac{n}{d}\right)\\&=\sum_{\substack{n\in\mathbb{N}\\ n\leq x}}(\boldsymbol{\mu}*\Lambda)(n)=\sum_{\substack{n\in\mathbb{N}\\ n\leq x}}\boldsymbol{\mu}(n)\sum_{m\leq x/n}\Lambda(m)\\&=\sum_{\substack{n\in\mathbb{N}\\ n\leq x}}\boldsymbol{\mu}(n)\psi\left(\frac{x}{n}\right).\end{aligned}\tag{14}$$

Como $\frac{\psi(x)}{x}\to 1$, cuando $x\to\infty$, dado $\varepsilon>0$, existe una constante $A=A(\varepsilon)>0$ tal que

$$\left|\frac{\psi(x)}{x}-1\right|<\varepsilon,\quad \text{para todo } x\geq A.$$

En otras palabras,

$$|\psi(x)-x|<\varepsilon x,\quad \text{para todo } x\geq A.\tag{15}$$

Escoja $x>A$ y escriba,

$$\sum_{\substack{n\in\mathbb{N}\\ n\leq x}}\boldsymbol{\mu}(n)\psi\left(\frac{x}{n}\right)=\sum_{\substack{n\in\mathbb{N}\\ n\leq y}}\boldsymbol{\mu}(n)\psi\left(\frac{x}{n}\right)+\sum_{\substack{n\in\mathbb{N}\\ y<n\leq x}}\boldsymbol{\mu}(n)\psi\left(\frac{x}{n}\right),\tag{16}$$

donde, $y:=\lfloor\frac{x}{A}\rfloor$. En la primera suma de (16), tenemos, $n\leq y$, así, $n\leq\frac{x}{A}$ y luego, $\frac{x}{n}\geq A$.

Por lo tanto, usando (15), escribimos,

$$\left|\psi\left(\frac{x}{n}\right)-\frac{x}{n}\right|<\varepsilon\frac{x}{n},\quad \text{para } n\leq y. \tag{17}$$

Así,

$$\begin{aligned}\sum_{\substack{n\in\mathbb{N}\\ n\leq y}}\boldsymbol{\mu}(n)\psi\left(\frac{x}{n}\right)&=\sum_{\substack{n\in\mathbb{N}\\ n\leq y}}\boldsymbol{\mu}(n)\left(\frac{x}{n}+\psi\left(\frac{x}{n}\right)-\frac{x}{n}\right)\\&=x\sum_{\substack{n\in\mathbb{N}\\ n\leq y}}\frac{\boldsymbol{\mu}(n)}{n}+\sum_{\substack{n\in\mathbb{N}\\ n\leq y}}\boldsymbol{\mu}(n)\left(\psi\left(\frac{x}{n}\right)-\frac{x}{n}\right),\end{aligned}$$

y por lo tanto,

$$\begin{aligned}\left|\sum_{\substack{n\in\mathbb{N}\\ n\leq y}}\boldsymbol{\mu}(n)\psi\left(\frac{x}{n}\right)\right|&\leq x\left|\sum_{\substack{n\in\mathbb{N}\\ n\leq y}}\frac{\boldsymbol{\mu}(n)}{n}\right|+\sum_{\substack{n\in\mathbb{N}\\ n\leq y}}|\boldsymbol{\mu}(n)|\left|\left(\psi\left(\frac{x}{n}\right)-\frac{x}{n}\right)\right|\\&<x+\varepsilon\sum_{\substack{n\in\mathbb{N}\\ n\leq y}}\frac{x}{n}\quad\text{(por Lema 4.2.1, } |\boldsymbol{\mu}(n)|\leq 1 \text{ y (17))}\\&<x+\varepsilon x(1+\ln y)\quad\text{(por la Observación 2.4.1)}\\&<x+\varepsilon x+\varepsilon x\ln x.\end{aligned}$$

En la segunda suma del lado derecho de (16), tenemos, $y<n\leq x$, así, $n\geq y+1$. Como $y\leq\frac{x}{A}<y+1$, se tiene,

$$\frac{x}{n}\leq\frac{x}{y+1}<A.$$

Entonces, $\frac{x}{n}<A$ implica que, $\psi(\frac{x}{n})<\psi(A)$. Luego,

$$\left|\sum_{\substack{n\in\mathbb{N}\\ y<n\leq x}}\boldsymbol{\mu}(n)\psi\left(\frac{x}{n}\right)\right|\leq\sum_{\substack{n\in\mathbb{N}\\ y<n\leq x}}|\boldsymbol{\mu}(n)|\psi(A)<x\psi(A).$$

Así, de (14) y (16),

$$\begin{aligned}|H(x)|=\left|\sum_{\substack{n\in\mathbb{N}\\ n\leq x}}\boldsymbol{\mu}(n)\psi\left(\frac{x}{n}\right)\right|&\leq\left|\sum_{\substack{n\in\mathbb{N}\\ n\leq y}}\boldsymbol{\mu}(n)\psi\left(\frac{x}{n}\right)\right|+\left|\sum_{\substack{n\in\mathbb{N}\\ y<n\leq x}}\boldsymbol{\mu}(n)\psi\left(\frac{x}{n}\right)\right|\\&<x+\varepsilon x+\varepsilon x\ln x+x\psi(A)<(2+\psi(A))x+\varepsilon x\ln x,\end{aligned}$$

si $\varepsilon < 1$. Luego, para $\varepsilon \in (0,1)$,

$$\frac{|H(x)|}{x \ln x} < \frac{2 + \psi(A)}{\ln x} + \varepsilon, \quad \text{si } x > A.$$

Ahora, escojamos $B > A$ tal que para $x > B$, tengamos

$$\frac{2 + \psi(A)}{\ln x} < \varepsilon.$$

Por lo tanto, para $x > B$,

$$\frac{|H(x)|}{x \ln x} < 2\varepsilon,$$

lo cual prueba que, $\frac{H(x)}{x \ln x} \to 0$, cuando $x \to \infty$. Así, probamos que TNP implica (11).

b). Veamos que, (11) implica TNP. Para probar este hecho, es suficiente mostrar que (11) implica

$$\lim_{x \to \infty} \frac{\psi(x)}{x} = 1.$$

Recordando,

$$\lfloor x \rfloor = \sum_{\substack{n \in \mathbb{N} \\ n \leq x}} 1, \quad 1 = \sum_{\substack{n \in \mathbb{N} \\ n \leq x}} \left\lfloor \frac{1}{n} \right\rfloor \quad \text{y} \quad \psi(x) = \sum_{\substack{n \in \mathbb{N} \\ n \leq x}} \Lambda(n).$$

Tenemos del Corolario 2.3.2, Proposición 2.3.4 y la Proposición 2.3.6,

$$1 = \sum_{\substack{n \in \mathbb{N} \\ d \mid n}} \boldsymbol{\mu}(d) \sigma\left(\frac{n}{d}\right), \quad \left\lfloor \frac{1}{n} \right\rfloor = \sum_{\substack{n \in \mathbb{N} \\ d \mid n}} \boldsymbol{\mu}(d) \quad \text{y} \quad \Lambda(n) = \sum_{\substack{n \in \mathbb{N} \\ d \mid n}} \boldsymbol{\mu}(d) \ln\left(\frac{n}{d}\right).$$

Defina $f : \mathbb{N} \to \mathbb{R}$ por

$$f(n) := \sigma(n) - \ln n - 2\gamma,$$

donde, γ es la constante de Euler y σ la función divisor.

Entonces,

$$\begin{aligned}
\lfloor x \rfloor - \psi(x) - 2\gamma &= \sum_{\substack{n\in\mathbb{N}\\ n\leq x}} 1 - \sum_{\substack{n\in\mathbb{N}\\ n\leq x}} \Lambda(n) - 2\gamma \sum_{n\leq x} \left\lfloor \frac{1}{n} \right\rfloor \\
&= \sum_{\substack{n\in\mathbb{N}\\ n\leq x}} \left(1 - \Lambda(n) - 2\gamma \left\lfloor \frac{1}{n} \right\rfloor \right) \\
&= \sum_{\substack{n\in\mathbb{N}\\ n\leq x}} \left(\sum_{\substack{n\in\mathbb{N}\\ d|n}} \boldsymbol{\mu}(d)\sigma\left(\frac{n}{d}\right) - \sum_{\substack{n\in\mathbb{N}\\ d|n}} \boldsymbol{\mu}(d)\ln\left(\frac{n}{d}\right) - 2\gamma \sum_{\substack{n\in\mathbb{N}\\ d|n}} \boldsymbol{\mu}(d) \right) \\
&= \sum_{\substack{n\in\mathbb{N}\\ n\leq x}} \sum_{\substack{n\in\mathbb{N}\\ d|n}} \boldsymbol{\mu}(d) \left(\sigma\left(\frac{n}{d}\right) - \ln\left(\frac{n}{d}\right) - 2\gamma \right) \\
&= \sum_{qd\leq x} \boldsymbol{\mu}(d)(\sigma(q) - \ln q - 2\gamma) \\
&= \sum_{qd\leq x} \boldsymbol{\mu}(d) f(q).
\end{aligned}$$

Esto implica que,

$$\psi(x) - x + \sum_{qd\leq x} \boldsymbol{\mu}(d) f(q) = \mathrm{O}(1).$$

Así, para finalizar la prueba, basta mostrar que,

$$\lim_{x\to\infty} \frac{1}{x} \sum_{qd\leq x} \boldsymbol{\mu}(d) f(q) = 0.$$

Ahora, usando la Proposición 2.3.9, escribimos,

$$\sum_{qd\leq x} \boldsymbol{\mu}(d) f(q) = \sum_{\substack{n\in\mathbb{N}\\ n\leq b}} \boldsymbol{\mu}(n) F\left(\frac{x}{n}\right) + \sum_{\substack{n\in\mathbb{N}\\ n\leq a}} f(n) M\left(\frac{x}{n}\right) - F(a)M(b), \tag{18}$$

donde, $a, b \in (0, \infty)$ tal que $ab = x$, $qd = n$ y

$$F(x) = \sum_{\substack{n\in\mathbb{N}\\ n\leq x}} f(n).$$

De las Proposiciones 2.4.4 y 2.4.1,

$$\begin{aligned} F(x) &= \sum_{\substack{n\in\mathbb{N}\\ n\leq x}} \sigma(n) - \sum_{\substack{n\in\mathbb{N}\\ n\leq x}} \ln n - 2\gamma \sum_{\substack{n\in\mathbb{N}\\ n\leq x}} 1 \\ &= x\ln x + (2\gamma-1)x + \mathrm{O}(\sqrt{x}) - (x\ln x - x + \mathrm{O}(\ln x)) - 2\gamma\lfloor x\rfloor \\ &= 2\gamma x + \mathrm{O}(\sqrt{x}) + \mathrm{O}(\ln x) - 2\gamma(x + \mathrm{O}(1)) \\ &= \mathrm{O}(\sqrt{x}) + \mathrm{O}(\ln x) + \mathrm{O}(1) = \mathrm{O}(\sqrt{x}). \end{aligned}$$

Esto es, existe una constante $B > 0$ tal que,

$$|F(x)| \leq B\sqrt{x},$$

para $x \geq 1$. Ahora, aplicando este resultado a la primera suma de la derecha de (18),

$$\left|\sum_{\substack{n\in\mathbb{N}\\ n\leq b}} \boldsymbol{\mu}(n) F\left(\frac{x}{n}\right)\right| \leq B\sum_{\substack{n\in\mathbb{N}\\ n\leq b}} \sqrt{\frac{x}{n}} \leq A\sqrt{xb} = \frac{Ax}{\sqrt{a}},$$

para algún constante $A > B$. Sea cualquier $\varepsilon > 0$ y escogiendo $a > 1$ tal que $\frac{A}{\sqrt{a}} < \varepsilon$. Entonces,

$$\left|\sum_{\substack{n\in\mathbb{N}\\ n\leq b}} \boldsymbol{\mu}(n) F\left(\frac{x}{n}\right)\right| < \varepsilon x, \tag{19}$$

para $x \geq 1$. Observe que, ε depende de a y no de x.

De (11), (por definición) existe una constante $C = C(\varepsilon) > 0$ tal que, para $x > C$,

$$\frac{|M(x)|}{x} < \frac{\varepsilon}{K},$$

para cualquier constante $K > 0$.

Ahora, estimamos a la segunda suma de la derecha de (18),

$$\left|\sum_{\substack{n\in\mathbb{N}\\ n\leq a}} f(n) M\left(\frac{x}{n}\right)\right| \leq \sum_{\substack{n\in\mathbb{N}\\ n\leq a}} |f(n)| \frac{\varepsilon}{K}\frac{x}{n} = \frac{\varepsilon x}{K}\sum_{\substack{n\in\mathbb{N}\\ n\leq a}} \frac{|f(n)|}{n}, \tag{20}$$

para $\frac{x}{n} > C$ y para todo $n \leq a$. Así, para $x > aC$. Tomando,

$$K := \sum_{n \leq a} \frac{|f(n)|}{n}$$

en (20), obtenemos,

$$\left| \sum_{\substack{n \in \mathbb{N} \\ n \leq a}} f(n) M\left(\frac{x}{n}\right) \right| < \varepsilon x \quad \text{para } x > aC \tag{21}$$

Finalmente,

$$|F(a)M(b)| \leq A\sqrt{a}|M(b)| \leq A\sqrt{ab} < \varepsilon\sqrt{a}\sqrt{ab} = \varepsilon ab = \varepsilon x, \tag{22}$$

si $x > a^2$ y desde que $ab = x$. Combinando, (18), (19), (21) y (22), obtenemos,

$$\left| \sum_{qd \leq x} \boldsymbol{\mu}(d) f(q) \right| < 3\varepsilon x,$$

para $x > \text{máx}\{a^2, aC\}$. Como a y C solo depende de ε, concluimos que,

$$\lim_{x \to \infty} \frac{1}{x} \sum_{qd \leq x} \boldsymbol{\mu}(d) f(q) = 0.$$

■

4.3. Teorema de Davenport

Ahora, vamos a ver la correlación del comportamiento de la función de Möbius $\boldsymbol{\mu}$ con las funciones en el círculo unitario, $S^1 := \{z \in \mathbb{C} : |z| = 1\} = \{z \in \mathbb{C} : z = e^{2\pi i t}, t \in \mathbb{R}\}$, o sea, lo que necesitamos es una estimativa para el crecimiento de las sumas

$$\sum_{\substack{n \in \mathbb{N} \\ n \leq x}} e^{2\pi i n\theta} \boldsymbol{\mu}(n),$$

donde θ es cualquier ángulo y para real $x \to \infty$.

El siguiente teorema trata sobre este asunto, lo cual fue demostrado en 1937 por el matemático inglés Harold Davenport detalladas en **Davenport (1937)** en lo cual usa Caracteres de Direchlet, L-Funciones, etc. Otra prueba posterior de este resultado usando

método de Vinogrodov se encuentra en **Iwaniec y Kowalski (2004)**.

Teorema 4.3.1 (Davenport) *Para cada $A > 0$ y para todo $\theta \in [0, 1)$, tenemos,*

$$\sum_{\substack{n\in\mathbb{N}\\ n\leq x}} e^{2\pi in\theta}\boldsymbol{\mu}(n) = \mathrm{O}(x(\ln x)^{-A}),$$

cuando $x \to \infty$, uniformemente en θ.

Para nuestro propósito de estudio, veamos otra versión de este teorema.

Teorema 4.3.2 *Para $\theta \in [0, 1)$, tenemos que,*

$$\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} e^{2\pi in\theta}\boldsymbol{\mu}(n) = 0.$$

Demostración. Note que, cuando reemplazamos $x \in \mathbb{R}$ por $N \in \mathbb{N}$ en el Teorema 4.3.1 no cambia la tasa de crecimiento de la suma. Luego, usando la definición de O grande, para cada $A > 0$, existe una constante $C_A = C(A)$ (que depende de A) tal que

$$0 \leq \left|\frac{1}{N}\sum_{n=1}^{N} e^{2\pi in\theta}\boldsymbol{\mu}(n)\right| \leq \frac{C_A}{\ln^A N}$$

para $\theta \in [0, 1)$. Como

$$\lim_{N\to\infty} \frac{C_A}{\ln^A N} = 0,$$

obtenemos que,

$$\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} e^{2\pi in\theta}\boldsymbol{\mu}(n) = 0.$$

■

4.4. Aspectos dinámicos de la función de Möbius

4.4.1. Función libre de cuadrados

El teorema que presentamos en esta sección es conforme a **Pinsky (2014)**.

Lema 4.4.1 *Tenemos que,*

$$\sum_{k=1}^{\infty} \frac{\boldsymbol{\mu}(k)}{k^2} = \frac{6}{\pi^2}.$$

Demostración. Sabemos que, por la Proposición 2.2.4,

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Considere,

$$A := \sum_{k=1}^{\infty} \frac{1}{k^2} \quad \text{y} \quad B := \sum_{k=1}^{\infty} \frac{\boldsymbol{\mu}(k)}{k^2}.$$

Entonces, la serie A es convergente y la serie B es absolutamente convergente, pues como $|\boldsymbol{\mu}(k)| \leq 1$,

$$\sum_{k=1}^{\infty} \left| \frac{\boldsymbol{\mu}(k)}{k^2} \right| \leq \sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{\pi^2}{6} < \infty.$$

Luego,

$$\begin{aligned}
\left(\sum_{n=1}^{\infty} \frac{1}{n^2}\right)\left(\sum_{k=1}^{\infty} \frac{\boldsymbol{\mu}(k)}{k^2}\right) &= \left(\sum_{n=1}^{\infty} \frac{u(n)}{n^2}\right)\left(\sum_{k=1}^{\infty} \frac{\boldsymbol{\mu}(k)}{k^2}\right) = \sum_{n,k=1} \frac{u(n)\boldsymbol{\mu}(k)}{(nk)^2} \\
&= \sum_{m=1}^{\infty} \frac{1}{m^2} \sum_{\substack{n,k \\ nk=m}} u(n)\boldsymbol{\mu}(k) = \sum_{m=1}^{\infty} \frac{1}{m^2} \sum_{k|m} \boldsymbol{\mu}(k) u\left(\frac{m}{k}\right) \\
&= \sum_{m=1}^{\infty} \frac{1}{m^2} (\boldsymbol{\mu} * u)(m) = \sum_{m=1}^{\infty} \frac{I(m)}{m^2} \quad \text{(por Corolario 2.3.1)} \\
&= 1 \quad \text{(usando la definición de } I(m)\text{)}.
\end{aligned}$$

Por lo tanto,

$$\sum_{k=1}^{\infty} \frac{\boldsymbol{\mu}(k)}{k^2} = \frac{1}{\pi^2/6} = \frac{6}{\pi^2}.$$

■

Definición 4.4.1 Un $n \in \mathbb{N}$ es *libre de cuadrados*, cuando n no es divisible por ningún otro cuadrado perfecto que no sea 1.

Ejemplo 4.4.1 Note que, $10 = 2 \cdot 5$ es libre de cuadrados y $24 = 2^2 \cdot 2 \cdot 3$ no es libre de cuadrados.

Definición 4.4.2 Definimos la función aritmética $\boldsymbol{\mu}^2 : \mathbb{N} \to \{0, 1\}$ por,

$$\boldsymbol{\mu}^2(n) = \begin{cases} 1, & \text{si } n \text{ es libre de cuadrados;} \\ 0, & \text{caso contrario.} \end{cases},$$

donde $\boldsymbol{\mu}$ es la función de Möbius.

Lema 4.4.2 *Se tiene,*

$$\boldsymbol{\mu}^2(n) = \sum_{\substack{n \in \mathbb{N} \\ d^2 | n}} \boldsymbol{\mu}(d).$$

Demostración. Sea $F(n) := \sum_{d^2|n} \boldsymbol{\mu}(d)$. Si $n \in \mathbb{N}$ es libre de cuadrados, entonces el único d que satisface $d^2|n$ es cuando $d = 1$. Entonces, $F(n) = 1$, desde que, $\boldsymbol{\mu}(1) = 1$.

Ahora, si n no es libre de cuadrados, entonces n puede ser escrito de la forma $n = m^2 k$, donde $m \in \mathbb{N}$ y $k \in \mathbb{N}$ es libre de cuadrados. Note que, $d^2|m^2 k$ si y solamente si, $d|m$. Así, tenemos,

$$\begin{aligned} F(n) &= \sum_{\substack{n \in \mathbb{N} \\ d^2 | n}} \boldsymbol{\mu}(d) = \sum_{d | m^2 k} \boldsymbol{\mu}(d) \\ &= \sum_{\substack{m \in \mathbb{N} \\ d | m}} \boldsymbol{\mu}(d) = 0 \quad \text{(prueba de la Proposición 2.3.4).} \end{aligned}$$

Por lo tanto, $F(n) = \boldsymbol{\mu}^2(n)$.

■

El siguiente resultado, muestra, en cierto sentido, que la densidad asintótica de los enteros positivos libres de cuadrados es $\frac{6}{\pi^2}$.

Teorema 4.4.1 *Tenemos,*

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} \boldsymbol{\mu}^2(n) = \frac{6}{\pi^2}.$$

Demostración. Usando Lema 4.4.2,

$$\sum_{n=1}^{N} \boldsymbol{\mu}^2(n) = \sum_{n=1}^{N} \sum_{d^2 | n} \boldsymbol{\mu}(d). \tag{23}$$

Si $d^2 > N$ entonces $\boldsymbol{\mu}(d)$ no aparecerá en el lado derecho de (23). Si $d^2 \leq N$, entonces $\boldsymbol{\mu}(d)$ aparecerá $\lfloor \frac{N}{d^2} \rfloor$ veces al lado derecho de (23), digamos, cunado $n = d^2, 2d^2, ..., \lfloor \frac{N}{d^2} \rfloor d^2$. Así,

$$\begin{aligned}\sum_{n=1}^{N} \boldsymbol{\mu}^2(n) &= \sum_{n=1}^{N} \sum_{d^2|n} \boldsymbol{\mu}(d) = \sum_{d^2 \leq N} \left\lfloor \frac{N}{d^2} \right\rfloor \boldsymbol{\mu}(d) = \sum_{d \leq \lfloor N^{1/2} \rfloor} \left\lfloor \frac{N}{d^2} \right\rfloor \boldsymbol{\mu}(d) \\ &= \sum_{d \leq \lfloor N^{1/2} \rfloor} \left\lfloor \frac{N}{d^2} \right\rfloor \boldsymbol{\mu}(d) + \sum_{d \leq \lfloor N^{1/2} \rfloor} \frac{N}{d^2} \boldsymbol{\mu}(d) - \sum_{d \leq \lfloor N^{1/2} \rfloor} \frac{N}{d^2} \boldsymbol{\mu}(d) \\ &= N \sum_{d \leq \lfloor N^{1/2} \rfloor} \frac{\boldsymbol{\mu}(d)}{d^2} + \sum_{d \leq \lfloor N^{1/2} \rfloor} \left(\left\lfloor \frac{N}{d^2} \right\rfloor - \frac{N}{d^2} \right) \boldsymbol{\mu}(d). \end{aligned} \tag{24}$$

Como $|\frac{N}{d^2} - \lfloor \frac{N}{d^2} \rfloor| < 1$ y $|\boldsymbol{\mu}(d)| \leq 1$, se tiene,

$$\left| \sum_{d \leq \lfloor N^{1/2} \rfloor} \left(\left\lfloor \frac{N}{d^2} \right\rfloor - \frac{N}{d^2} \right) \boldsymbol{\mu}(d) \right| \leq \sum_{d \leq \lfloor N^{1/2} \rfloor} 1 \leq N^{1/2}.$$

Así, la segunda suma de el lado derecho de (24) es limitado. Luego, de (24),

$$\begin{aligned}\lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} \boldsymbol{\mu}^2(n) &= \lim_{N \to \infty} \sum_{d \leq \lfloor N^{1/2} \rfloor} \frac{\boldsymbol{\mu}(d)}{d^2} = \sum_{d=1}^{\infty} \frac{\boldsymbol{\mu}(d)}{d^2} \\ &= \frac{6}{\pi^2} \qquad \text{(por el Lema 4.4.1).}\end{aligned}$$

■

4.4.2. Función de Möbius no es determinsitico

Del Ejemplo 2.3.4, para $n = 1, 2, 3, ...$ tenemos los valores de $\boldsymbol{\mu}(n)$ son:

$$1, -1, -1, 0, -1, 1, -1, 0, ...$$

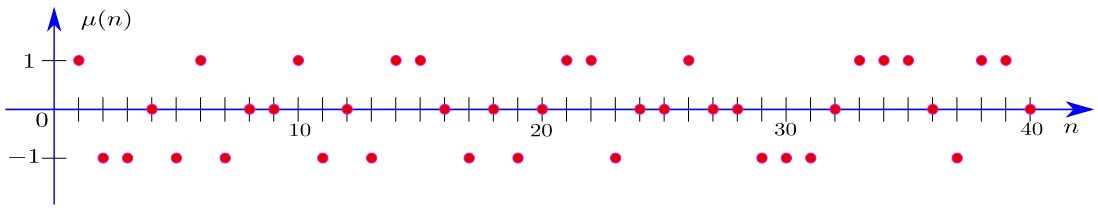


Figura 7: Valores de $\mu(n)$

La pregunta natural surge: ¿Existe algún "patrón" en esta sucesión? o ¿La sucesión $1, -1, -1, 0, -1, 1, -1, 0, 0, 1, ...$ es "aleatoria"?. Entonces, respondamos esta pregunta.

Definición 4.4.3 Dado un sistema dinámico discreto (X, T), donde X es un espacio métrico compacto y $T : X \to X$ continua, diremos que la sucesión $\{\xi(n)\}_{n\in\mathbb{N}}$ es *realizado en* (X, T), si para $x \in X$ y $f \in C(X)$,

$$\xi(n) = f(T^n(x)),$$

para todo $n \in \mathbb{N}$.

Definición 4.4.4 La sucesión $\{\xi(n)\}_{n\in\mathbb{N}}$ es determinístico si es realizado en un sistema dinámico discreto determinístico.

A continuación, vamos a ver que la sucesión $\{\boldsymbol{\mu}(n)\}_{n\in\mathbb{N}}$ no es determinístico, lo cual muestra que la función de Möbius es, en cierto sentido, aleatoria. Para probar eso, necesitamos nociones sobre *Dinámica Simbólica* (para mas detalle ver **Robinson (1998)** o **Pollicott y Yuri (1998)**).

Espacios de Shift. Sean $\Sigma_1 = \{-1, 0, 1\}^{\mathbb{N}}$ y $\Sigma_2 = \{0, 1\}^{\mathbb{N}}$; es decir,

$$\Sigma_1 = \{(w_n)_{n\in\mathbb{N}} = (w_1, w_2, w_3, ...) : w_n \in \{-1, 0, 1\}\ \forall n \in \mathbb{N}\},$$

$$\Sigma_2 = \{(w_n)_{n\in\mathbb{N}} = (w_1, w_2, w_3, ...) : w_n \in \{0, 1\}\ \forall n \in \mathbb{N}\}.$$

Sea $\Sigma := \Sigma_1$ (o Σ_2). La distancia definido (ver Ejemplo A.2) en Σ es dado por:

$$d(x, y) := \begin{cases} 0 & \text{si } x = y, \\ \left(\frac{1}{2}\right)^{N(x,y)} & \text{si } x \neq y, \end{cases}$$

donde, $x = (x_n)_{n\in\mathbb{N}}$, $y = (y_n)_{n\in\mathbb{N}}$ y $N(x, y) := \text{máx}\{N \in \mathbb{N} : x_n = y_n\ \forall\ n < N\}$. Luego, por el Ejemplo A.4, (Σ, d) es un espacios métrico compacto.

Definición 4.4.5 (Aplicación shift) Definimos la aplicación *shift* $\sigma : \Sigma \to \Sigma$ por

$$\sigma((w_n)_{n\in\mathbb{N}}) := (w_{n+1})_{n\in\mathbb{N}}.$$

Esto es,

$$\sigma(w_1, w_2, w_3, w_4, ...) = (w_2, w_3, w_4, w_5, ...).$$

Notación. Dado $x \in \Sigma$, denotamos una coordenada dada por la aplicación shift por $\sigma(x)_n = x_{n+1}$.

Proposición 4.4.1 *La aplicación shift es continua*[6].

Demostración. Sean $x, y \in \Sigma$, note que si $x \neq y$ e $d(x, y) = (\frac{1}{2})^N$, entonces $x_n = y_n$ para todo $n < N$. Luego, $\sigma(x)_n = x_{n+1} = y_{n+1} = \sigma(y)_n$ para todo $n = 1, 2, ..., N-1$. Esto significa que,

$$d(\sigma(x), \sigma(y)) = \left(\frac{1}{2}\right)^N \leq \left(\frac{1}{2}\right)^{N-1} = \frac{1}{2}d(x, y).$$

Dado cualquier $\varepsilon > 0$, tome $\delta = 2\varepsilon$. Luego, si $d(x, y) < \delta$, entonces, $d(\sigma(x), \sigma(y)) < \varepsilon$. Como $x, y \in \Sigma$ son arbitrarios, concluimos que σ es continua.

■

Ahora, para $\omega := (\boldsymbol{\mu}(1), \boldsymbol{\mu}(2), \boldsymbol{\mu}(3), \boldsymbol{\mu}(4), ...) \in \Sigma_1$, la órbita de ω por σ es:

$$\mathrm{Orb}(\omega) = \{\sigma^j(\omega) : j \in \mathbb{N}\}.$$

Sea $X := \overline{\mathrm{Orb}(\omega)} \subseteq \Sigma_1$ (clausura de la orbita de ω). Luego, en X tenemos la aplicación shift T que es la restricción de σ a X, es decir, $T := \sigma|_X$. Observe que $T(X) \subseteq X$ (esto nos dice, que tenemos un nuevo sistema dinámico (X, T)).

De forma análoga, para $\eta := (\boldsymbol{\mu}^2(1), \boldsymbol{\mu}^2(2), \boldsymbol{\mu}^2(3), \boldsymbol{\mu}^2(4), ...) \in \Sigma_2$ sucesión libre de cuadrados, la órbita de η por la aplicación σ es:

$$\mathrm{Orb}(\eta) = \{\sigma^j(\eta) : j \in \mathbb{N}\}.$$

[6]Dado un espacio métrico (X, d). Una función $f : X \to X$ es continua en $x_0 \in X$, si para todo $\varepsilon > 0$, existe $\delta > 0$ tal que $d(x, x_0) < \delta$, entonces $d(f(x), f(x_0)) < \varepsilon$. Si f es continua en todo los puntos de X, diremos que f es una función continua.

Sea $Y := \overline{\text{Orb}(\eta)} \subseteq \Sigma_2$. Entonces, en Y_1 tenemos la aplicación shift dado por $S := \sigma|_Y$. También tenemos que $S(Y) \subseteq Y$.

Sea $x = (x_1, x_2, x_3) \in \Sigma$ y defina $f : \Sigma \to \{-1, 0, 1\}$ por $f(x) = x_1$. Note que f es continua. Ahora, para $x = \omega$, tenemos que,

$$\xi(1) = f(T(x)) = f(\boldsymbol{\mu}(2), \boldsymbol{\mu}(3), \boldsymbol{\mu}(4), ...) = \boldsymbol{\mu}(2),$$
$$\xi(2) = \boldsymbol{\mu}(3), ...$$

Luego, concluimos que la sucesión $\{\xi(n)\}_{n\in\mathbb{N}} = (\boldsymbol{\mu}(2), \boldsymbol{\mu}(3), ...)$ es realizado en el sistema dinámico discreto (X, T).

Similarmente, para $x = \eta$, la sucesión $(\boldsymbol{\mu}^2(2), \boldsymbol{\mu}^2(3), \boldsymbol{\mu}^2(4), ...)$ es realizado en el sistema dinámico discreto (Y, S).

Proposición 4.4.2 *Considere la función $h : X \to Y$ dado por*

$$h(x_1, x_2, x_3, ...) = (x_1^2, x_2^2, x_3^2, ...).$$

Entonces, h semi-conjuga a T y S.

Demostración. Es fácil ver que h es continua. Como $h(\omega) = \eta$, tenemos que $h(X) = Y$ y sigue que h sobreyectiva. Note que,

$$\begin{aligned} h \circ T(\omega) &= h(\boldsymbol{\mu}(2), \boldsymbol{\mu}(3), \boldsymbol{\mu}(4), ...)) = ((\boldsymbol{\mu}^2(2), \boldsymbol{\mu}^2(3), \boldsymbol{\mu}^2(4), ...) \\ &= S(\boldsymbol{\mu}^2(1), \boldsymbol{\mu}^2(2), \boldsymbol{\mu}^2(3), ...) \\ &= S \circ h(\omega). \end{aligned}$$

Así, $h \circ T = S \circ h$. Esto es, que el siguiente diagrama conmuta

$$\begin{array}{ccc} X & \xrightarrow{T} & X \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle h} \\ Y & \xrightarrow[S]{} & Y \end{array}$$

Luego, la aplicación h es una semi-conjugación.

■

Para la prueba del siguiente teorema se necesita conocer sobre *Conjuntos Admisibles* y *Teoría Ergódica* (lo cual no será abordado aquí). Para mas detalle ver **Sarnak (2011)** y **Lemanczyk y de la Rue (2017)**.

Teorema 4.4.2 *Se tiene que,* $h_{top}(S) = \dfrac{6}{\pi^2}\ln 2$.

El siguiente resultado muestra que $\{\boldsymbol{\mu}(n)\}_{n\in\mathbb{N}}$ no es deterministico.

Proposición 4.4.3 $h_{top}(T) > 0$.

Demostración. La función $h : X \to Y$ definido en la Proposición 4.4.2 es una semi-conjugación; entonces de la Proposición 2.7.4 y el Teorema 4.4.2,

$$\begin{aligned} h_{top}(T) &\geq h_{top}(S) \\ &= \frac{6}{\pi^2}\ln 2 > 0. \end{aligned}$$

■

4.4.3. La conjetura de Sarnak

Presentamos la conjetura de Sarnak, conocido también como la *Ley de aleatoriedad de Möbius*. Pero veamos como nació las ideas de este problema.

Principio de Aleatoriedad. Una antigua y famosa heurística llamada *Principio de aleatoriedad de Möbius* **(Iwaniec y Kowalski, 2004, pág. 338)**, afirma que los padrones de los símbolos $-1, 0$ y 1 en la sucesión $\{\boldsymbol{\mu}(n)\}_{n\in\mathbb{N}}$ se comportan de forma tan caótica que $\{\boldsymbol{\mu}(n)\}_{n\in\mathbb{N}}$ no tiene correlación con cualquier sucesión $\{\xi(n)\}_{n\in\mathbb{N}}$ *acotado razonablemente simples.*

La idea intuitiva para este principio es:

- Por sucesiones "razonables" nos referimos como aquellas que no se obtienen mediante construcciones muy elaboradas.
- Por "no tiene correlación" entenderemos,

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}\xi(n)\boldsymbol{\mu}(n) = 0.$$

Por otro lado, en 2010, el matemático sud-africano (nacionalizado estadounidense) Peter Clive Sarnak en **Sarnak (2011)**, propone una interpretación precisa de este principio de aleatoriedad en contexto de sistemas dinámicos. Entonces, presentamos el famoso problema abierto que envuelve teoría de números y sistemas dinámicos (para mas información ver también **Ferenczi, Kułaga-Przymus, y Lemańczyk (2018)**):

Conjetura 4.4.1 (Sarnak - 2011) *Sea $T : X \to X$ una transformación continua en un espacio métrico compacto X, con $h_{top}(T) = 0$. Entonces para cada $x \in X$ y cualquier función $f \in C(X)$, tenemos,*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(T^n(x))\boldsymbol{\mu}(n) = 0,$$

donde $C(X) := \{f : X \to \mathbb{C} : f \text{ es continua}\}$.

Sabemos que la entropía topológica mide el crecimiento exponencial medio del número de segmentos distinguibles (o indistinguibles) de las órbitas de tamaño n, es decir, mide la cantidad de caos en un determinado sistema. Así, un sistema con entropía topológica cero parece ser determinista en un sentido a priori y $\boldsymbol{\mu}$ siendo ortogonal (ver Definición 4.4.6) a cualquier sucesión realizada en un sistema dinámico determinístico significa que $\boldsymbol{\mu}$ no actúa deterministicamente (o previsiblemente) de forma alguna.

En la Conjetura 4.4.1, mayoría de veces, pero no siempre, T será un homeomorfismo como es descrito en **Lemanczyk y de la Rue (2017)**. Sarnak señaló que esta conjetura estaba respaldada por una conjetura más antigua llamada *Conjetura de Chowla*[7] que dice que $\boldsymbol{\mu}$ no tiene auto-correlación de ningún orden.

Definición 4.4.6 Diremos que $\boldsymbol{\mu}(n)$ es ortogonal a (X, T) si

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \xi(n)\mu(n) = 0,$$

donde $\{\xi(n)\}_{n\in\mathbb{N}}$ es realizado en (X, T).

[7] **Conjetura de Chowla**. Dado cualquier número entero $r \geq 0$ y enteros $i_0, i_1, ..., i_r \geq 0$ con por lo menos i_j impar, entonces

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \boldsymbol{\mu}^{i_0}(n) \cdot \boldsymbol{\mu}^{i_1}(n+1) \cdots \boldsymbol{\mu}^{i_r}(n+r) = 0.$$

Así, de la Definición 4.4.6, otra manera de enunciar la conjetura es:

Conjetura de Sarnak: $\boldsymbol{\mu}(n)$ es ortogonal a cualquier sucesión deterministico realizado en (X, T).

Observación 4.4.1 Por la Proposición 4.4.3, la función de Möbius no es deterministico y por el Teorema 4.4.1,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \boldsymbol{\mu}^2(n) = \frac{6}{\pi^2}.$$

Así, $\boldsymbol{\mu}(n)$ no es razonablemente simple y tine correlación con el mismo para todo $n \in \mathbb{N}$.

4.4.4. Conjetura de Sarnak implica TNP

Veremos que el Teorema de Números Primos satisface la conjetura de Sarnak. Para eso vamos a buscar un espacio métrico compacto (X, d), una transformación continua $T : X \to X$ con entropía topológica cero y $f \in C(X)$.

El espacio métrico buscado es el siguiente: Considere $X = \{x\}$, entonces (X, d) es un espacio métrico compacto, donde d es la métrica trivial (la métrica discreta).

Proposición 4.4.4 *TNP satisface la conjetura de Sarnak.*

Demostración. Como $X = \{x\}$ es finito, entonces para cualquier $T : X \to X$ transformación continua (de hecho, $T(x) = x$ para todo $x \in X$) por la Proposición 2.7.12, se tiene que, $h_{top}(T) = 0$ y sea $f : X \to \mathbb{R}$ una función constante, es decir, $f(x) = c$ para todo $x \in X$. Así, estamos en las hipótesis de la conjetura de Sarnak y, como el valor de $f(T^n(x))$ no contribuye en términos de convergencia, pues es constante para todo $n \in \mathbb{N}^*$ y todo $x \in X$, basta mostrar que,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \boldsymbol{\mu}(n) = 0,$$

pero esto es inmediato, una vez que es equivalente a Teorema de los Números Primos debido al Teorema 4.2.1. Por lo tanto, la Conjetura de Sarnak implica al Teorema de Números Primos.

■

Observación 4.4.2 Para probar la Proposición 4.4.4 no es necesario que X sea un punto, pues basta considerar (X, d) cualquier espacio métrico compacto y $T : X \to X$ una transformación continua con $h_{top}(T) = 0$. Entonces, para $f \in C(X)$ constante, se tiene que, $f(T^n(x))$ no contribuye en términos de convergencia, desde que es constante para todo $x \in X$ y todo $n \in \mathbb{N}^*$.

4.4.5. Conjetura de Sarnak implica Teorema de Davenport

En esta sección, vamos a demostrar que el Teorema de Davenport satisface la conjetura de Sarnak. Sabemos que por la Observación 2.6.1, que los tres círculos unitarios $S^1, I/\sim$ y $\mathbb{T}$ son homeomorfos, así, en esta parte usamos el circulo unitario (flat) $\mathbb{T}$.

Proposición 4.4.5 *El Teorema de Davenport satisface la Conjetura de Sarnak.*

Demostración. Considere $X = \mathbb{T} = \mathbb{R}/\mathbb{Z}$ y sabemos que, por el Ejemplo A.3, (X, d) es un espacio métrico compacto. Sea $T = R_\alpha : \mathbb{T} \to \mathbb{T}$ la rotación introducido en el Ejemplo 2.6.2, es decir, para $\alpha \in [0, 1)$, $R_\alpha(x) = x + \alpha \mod 1$. Note que, para todo $n \in \mathbb{Z}$,

$$R_\alpha^n(x) = x + n\alpha \mod 1. \tag{25}$$

Por el Ejemplo 2.7.5 tenemos que, $h_{top}(R_\alpha) = 0$. Ahora, considere la función continua $f : \mathbb{T} \to \mathbb{C}$ definida por $f(z) = e^{2\pi iz}$. Luego, estamos en las hipótesis de la conjetura de Sarnak. Así, para $x = 0$ en (25), obtenemos,

$$\begin{aligned}\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(R_\alpha^n(0))\boldsymbol{\mu}(n) &= \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(n\alpha)\boldsymbol{\mu}(n) \\ &= \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e^{2\pi in\alpha}\boldsymbol{\mu}(n) \\ &= 0 \quad \text{(Teorema 4.3.2 - Davenport).}\end{aligned}$$

Por lo tanto, la conjetura de Sarnak implica al Teorema de Davenport.

■

V. CONCLUSIONES

El proyecto fue muy productivo para la comprensión de conceptos básicos de la Teoría Analítica de Números y la Entropía topológica de un sistema dinámico discreto, así, entender la motivación matemática que conecta a ellos.

En este informe final, fue posible explorar los conceptos y propiedades básicas de la Teoría de Números para entender el esbozo de la prueba del Teorema de Números Primos y cuya equivalencia que envuelve la función de Möbius (Teorema 4.2.1).

Estudiar la Función de Möbius fue muy importante para la compresión de la distribución de números primos en los naturales, para ver la correlación con las funciones en el circulo unitario y ver que no actúa previsiblemente de forma alguna a un sistema dinámico con entropía topológica cero.

El estudio de la entropía topológica de un sistema dinámico y sus respectivos propiedades fueron una buena introducción para entender la conjetura de Sarnak.

Los objetivos listados y la hipótesis planteado en el proyecto de investigación fueron cumplidos. Tenemos las siguientes conclusiones:

1. El Teorema 4.2.1 juega un rol importante para conectar el Teorema de los Números Primos y la Conjetura de Sarnak.

2. La función de Möbius en cierto sentido es aleatorio, es decir, no es deterministico.

3. El Teorema de los Números Primos y el Teorema de Davenport satisfacen la Conjetura de Sarnak.

VI. RECOMENDACIONES

Se tiene las siguientes recomendaciones:

1. Profundizar la prueba del Teorema de los Números Primos, es decir, estudiar las propiedades de la Función Zeta de Riemann.

2. Analizar a detalle la prueba del Teorema de Davenport.

3. Estudiar mas ejemplos que satisfacen la conjetura de Sarnak, por ejemplo el Teorema de Dirichlet sobre Números Primos en Progresiones Aritméticas.

4. Ver si aún es válido la conjetura de Sarnak para cualquier sucesión tomando valores en $\{-1, 0, 1\}$.

5. Ver la conjetura de Sarnak vía Teoría Ergódica.

Referencias

Apostol, T. M. (1998). *Introduction to analytic number theory.* Springer Science & Business Media.

Davenport, H. (1937). On some infinite series involving arithmetical functions (ii). *The Quarterly Journal of Mathematics*(1), 313–320.

Du Sautoy, M. (2007). *A música dos números primos: a história de um problema não resolvido na matemática.* Editora Schwarcz-Companhia das Letras.

Ferenczi, S., Kułaga-Przymus, J., y Lemańczyk, M. (2018). Sarnak's conjecture: what's new. En *Ergodic theory and dynamical systems in their interactions with arithmetics and combinatorics* (pp. 163–235). Springer.

Ingham, A. E. (1990). *The distribution of prime numbers* (n.º 30). Cambridge University Press.

Iwaniec, H., y Kowalski, E. (2004). *Analytic number theory* (Vol. 53). American Mathematical Soc.

Landau, E. (2002). *Teoria elementar dos números.* Ciência Moderna.

Lemanczyk, M., y de la Rue, T. (2017). The chowla and the sarnak conjectures from ergodic theory point of view. *DYNAMICAL SYSTEMS*, *37*(6).

Lima, E. L. (1983). *Espaços métricos* (Vol. 4). Instituto de Matemática Pura e Aplicada, CNPq Rio de Janeiro.

Munkres, J. R. (2000). *Topology.* Prentice hall Upper Saddle River.

Pinsky, R. G. (2014). Problems from the discrete to the continuous. *Springer International Publishing Switzerland*, *3*, 21–34.

Pollicott, M., y Yuri, M. (1998). *Dynamical systems and ergodic theory* (n.º 40). Cambridge University Press.

Robinson, C. (1998). *Dynamical systems: stability, symbolic dynamics, and chaos*. CRC press.

Sarnak, P. (2011). *Three lectures on the möbius function, randomness and dynamics.*

Walters, P. (2000). *An introduction to ergodic theory* (Vol. 79). Springer Science & Business Media.

A. ESPACIOS MÉTRICOS

Vamos a recordar algunos conceptos y propiedades de la topología y espacios métricos. No probaremos los resultados mencionados en este capítulo, solo veremos la demostración de algunos resultados y ejemplos que generalmente no se ve en un curso de topología o espacios métricos. Las referencias son **Munkres (2000)**, **Lima (1983)**, **Pollicott y Yuri (1998)** y **Robinson (1998)**.

A.1. Espacio topológico

Definición A.1 (Topología) Una *topología* en un conjunto X es una colección τ de partes de X, llamados *abiertos* de la topología, que satisfacen:

1. $\emptyset, X \in \tau$;
2. Si $A_1, A_2, ..., A_n \in \tau$, entonces $A_1 \cap A_2 \cap \cdots \cap A_n \in \tau$;
3. Sea la familia arbitraria $(A_\lambda)_{\lambda \in I}$, con $A_\lambda \in \tau$ para todo $\lambda \in I$, entonces,

$$\bigcup_{\lambda \in I} A_\lambda \in \tau.$$

Definición A.2 (Espacio topológico) Un *espacio topológico* es el par (X, τ) donde X es un conjunto y τ una topología en X.

Definición A.3 (Cerrado) Un subconjunto de un un espacio topológico es *cerrado* si su complemento fuera abierto.

Definición A.4 (Cobertura abierta) Una colección $\mathcal{U}$ de subconjuntos de X se llama *cobertura abierta* de X siempre que

1. cada $A \in \mathcal{U}$ sea un subconjunto abierto de X y
2. $\bigcup_{A \in \mathcal{U}} A = X$.

Definición A.5 (Subcobertura) Una subcolección $\mathcal{B}$ de la cobertura abierta $\mathcal{U}$ se denomina *subcobertura* siempre que

$$\bigcup_{A \in \mathcal{B}} A = X.$$

Definición A.6 (Espacio de Hausdorff) Un espacio topológico (X, τ) es llamado *espacio de Hausdorf* si dados cualquier dos puntos distintos tienen vecindades distintas, es decir, dado $x, z \in X$ distintos y sean U, V vecindades de x y z respectivamente, entonces $U \cap V = \emptyset$.

Definición A.7 (Compacto) Diremos que un espacio topológico es *compacto* si tiene la propiedad de Hausdorff y cualquier cobertura abierta admite una subcobertura finita.

A.2. Espacio métrico

Definición A.8 (Métrica) Sea X cualquier conjunto diferente de vacío. Una *métrica* definido en X es una función $d : X \times X \to \mathbb{R}$ tal que, para cualquier $x, y, z \in X$,

1. $d(x, y) \geq 0$ y $d(x, y) = 0 \Leftrightarrow x = y$,
2. $d(x, y) = d(y, x)$,
3. $d(x, z) \leq d(x, y) + d(y, z)$

Ejemplo A.1 La distancia natural en $[0, 1]$ induce una distancia en $\mathbb{T} = [0, 1]/\sim$ (donde $\sim$ significa que 0 está identificado con 1, ver la sub-sección 2.6.1); específicamente, definido por:

$$d(x, y) := \text{mín}\{|x - y|, 1 - |x - y|\}, \quad \forall\, x, y \in \mathbb{T}. \tag{26}$$

Entonces, la función $d : \mathbb{T} \times \mathbb{T}$ definido en (26) es una métrica.

Demostración. Probemos esto, sean $x, y, z \in \mathbb{T}$:

1). Como x, y están en $[0, 1)$, tenemos que

$$0 \leq |x - y| < 1 \quad \text{y} \quad 0 < 1 - |x - y| < 1,$$

entonces, mín$\{|x - y|, 1 - |x - y|\} \geq 0$ y sigue que $d(x, y) \geq 0$.

Si $x = y \Rightarrow$ mín$\{0, 1\} = 0$ y, sigue que $d(x, y) = 0$. Ahora, si $d(x, y) = 0$, tenemos

$$|x - y| = 0 \quad \text{o} \quad |x - y| = 1.$$

Si $|x - y| = 0$, tenemos que $x = y$. Si $|x - y| = 1$, tenemos también que $x = y$, pues 0 y 1 están identificados. Luego, en ambos casos tenemos que $x = y$.

2). Como $|x - y| = |y - x|$,

$$\begin{aligned} d(x, y) &= \text{mín}\{|x - y|, 1 - |x - y|\} \\ &= \text{mín}\{|y - x|, 1 - |y - x|\} = d(y, x). \end{aligned}$$

3). Lo mas difícil de probar es la desigualdad triangular. Antes de probar, tenemos el siguiente hecho:

Afirmación A. *Para cualquier* $x, y \in [0, 1]$, *tenemos*,

$$d(x, y) \leq \frac{1}{2}.$$

De hecho, si $d(x, y) = |x - y|$ entonces, por definición de d, $|x - y| \leq 1 - |x - y|$, luego, $|x - y| \leq 1/2$. Así, $d(x, y) \leq 1/2$.

Ahora, si $d(x, y) = 1 - |x - y|$, tenemos que, $1 - |x - y| \leq |x - y|$. Luego,

$$\begin{aligned} 2|x - y| \geq 1 \Rightarrow |x - y| &\geq \frac{1}{2} \\ \Rightarrow 1 - |x - y| &\leq \frac{1}{2}. \end{aligned}$$

Así, $d(x, y) \leq 1/2$. Esto concluye la prueba de este afirmación.

Veamos la desigualdad triangular:

Caso 1: Sea $d(x,y) = |x-y|$ y $d(y,z) = |y-z|$. Note que,

$$|x-z| \leq |x-y| + |y-z|.$$

Si $d(x,z) = |x-z|$, entonces, $d(x,z) \leq d(x,y) + d(y,z)$. Ahora, si $d(x,z) = 1 - |x-z|$, tenemos que $1 - |x-z| \leq |x-z|$. Luego,

$$1 - |x-z| \leq |x-y| + |y-z| \Rightarrow d(x,z) \leq d(x,y) + d(y,z).$$

Caso 2. Sea $d(x,y) = |x-y|$ y $d(y,z) = 1 - |y-z|$. Entonces, de la Afirmación A, note que,

$$\begin{aligned} &|x-z| + |y-z| + 1 - |x-y| \leq \frac{1}{2} + \frac{1}{2} + \frac{1}{2} \leq 2 \\ &\Rightarrow |x-z| \leq |x-y| + 1 - |y-z| \\ &\Rightarrow |x-z| \leq d(x,y) + d(y,z). \end{aligned}$$

Luego, si $d(x,z) = |x-z|$, tenemos, $d(x,z) \leq d(x,y) + d(y,z)$. Por otro lado, si $d(x,z) = 1 - |x-z|$, entonces, como por definición de d, $1 - |x-z| \leq |x-z|$, se tiene que, $d(x,z) \leq d(x,y) + d(y,z)$.

Caso 3. Sea $d(x,y) = 1 - |x-y|$ y $d(y,z) = |y-z|$. De la Afirmación A,

$$\begin{aligned} |x-z| + |x-y| + 1 - |y-z| \leq 2 &\Rightarrow |x-z| \leq 1 - |x-y| + |y-z| \\ &\Rightarrow |x-z| \leq d(x,y) + d(y,z). \end{aligned}$$

Si $d(x,z) = |x-z|$, $d(x,z) \leq d(x,y) + d(y,z)$. Ahora si, $d(x,z) = 1 - |x-z|$, entonces, $1 - |x-z| \leq |x-z|$, así, $d(x,z) \leq d(x,y) + d(y,z)$.

Caso 4. Sea $d(x,y) = 1 - |x-y|$ y $d(y,z) = 1 - |y-z|$. Entonces,

$$d(x,y) + d(y,z) = 2 - |x-y| - |y-z|.$$

Ahora, note que, usando la Afirmación A,

$$|x-y|+|y-z|+|x-z| \leq \frac{1}{2}+\frac{1}{2}+\frac{1}{2} \leq 2$$
$$\Rightarrow |x-z| \leq 2-|x-y|-|y-z|.$$

Entonces, si $d(x,z) = |x-y|$, tenemos que, $d(x,z) \leq d(x,y)+d(y,z)$. Ahora, si $d(x,y) = 1-|x-z|$, entonces, como $1-|x-y| \leq |x-y|$ (por definición de d), se tiene que $d(x,z) \leq d(x,y)+d(y,z)$.

■

Ejemplo A.2 (Espacio de sucesiones) Sea $\Sigma = \{0,1,2,...,m\}^{\mathbb{Z}}$, es decir,

$$\Sigma = \{\{x_n\}_{n\in\mathbb{Z}} = (...,x_{-2},x_{-1},x_0,x_1,x_2,...) : x_n \in \{0,1,2,...m\}\}.$$

Defina $d : \Sigma \times \Sigma \to \mathbb{R}$ por

$$d(x,y) := \begin{cases} 0 & \text{si } x = y, \\ \left(\frac{1}{2}\right)^{N(x,y)} & \text{si } x \neq y, \end{cases}$$

donde $N(x,y) := \text{máx}\{N \in \mathbb{N} : x_n = y_n \ \forall\, n < N\}$, $x = \{x_n\}_{n\in\mathbb{N}}$ y $y = \{y_n\}_{n\in\mathbb{N}}$. Entonces, d es una métrica.

Demostración. Veamos que satisface las tres condiciones de una métrica: Sean $x = \{x_n\}_{n\in\mathbb{N}}$, $y = \{y_n\}_{n\in\mathbb{N}}$ y $z = \{z_n\}_{n\in\mathbb{N}}$.

1). Si $x = y$, por definición, $d(x,y) = 0$. Ahora, si $x \neq y$, por definición se tiene,

$$d(x,y) = \left(\frac{1}{2}\right)^{N(x,y)} > 0,$$

pues $N(x,y) \in \mathbb{N}$. Luego, $d(x,y) \geq 0$.

Si $x = y$, entonces por definición, $d(x,y) = 0$. Si $d(x,y) = 0$, como no existe $k \in \mathbb{N}$ tal que $(\frac{1}{2})^k = 0$, tenemos que $x = y$. Así, $d(x,y) = 0$ si y solamente si, $x = y$.

2). Si $x = y$, $d(x, y) = 0 = d(y, x)$. Ahora si, $x \neq y$, entonces,

$$\begin{aligned} N(x, y) &= \text{máx}\{N \in \mathbb{N} : x_n = y_n \ \forall \ n < N\} \\ &= \text{máx}\{N \in \mathbb{N} : y_n = x_n \ \forall \ n < N\} \\ &= N(y, x). \end{aligned}$$

Así, $d(x, y) = d(y, x)$.

3). Antes de probar la desigualdad triangular, tenemos el siguiente hecho:

Afirmación B. *Sea* $N(x, y) = N_1$ *y* $N(y, z) = N_2$. *Entonces si* $N_1 = N_2$, *se tiene que* $N(x, z) \geq N_1$. *Si* $N_1 < N_2$, *entonces,* $N(x, z) = N_1$.

De hecho, como $N(x, y) = N_1$, entonces, $x_n = y_n$ para todo $n < N_1$. De la misma forma, como $N(y, z) = N_2$, entonces, $y_n = z_n$ para todo $n < N_2$. Luego, si $N_1 = N_2$, tenemos que $x_n = y_n = z_n$ para todo $n < N_1$, lo que implica $N(x, z) \geq N_1$.

Sea $N_1 < N_2$. Entonces suponga que $N(x, z) > N_1$, así, $x_{N_1+1} = z_{N_1+1}$ y como $N_1 < N_2$, entonces, $y_{N_1+1} = z_{N_1+1}$. Luego, $x_{N_1+1} = z_{N_1+1} = y_{N_1+1}$, es decir, $x_{N_1+1} = y_{N_1+1}$, esto es imposibles, pues contradice la maximalidad de $N_1 = N(x, y)$. Por lo tanto, $N(x, z) = N_1$.

En otras palabras, la Afirmación B nos dice que, para tres sucesiones en Σ dos de los valores de la función exponente debe ser iguales entre si y, el tercero debe ser mayor o igual que otros dos.

Si $x = z$, $x = y$ o $z = y$, la igualdad es inmediata. Entonces, suponga que $x \neq z$, $x \neq y$ y $z \neq y$. Entonces, usando la Afirmación B, sea N_1 menor valor de los exponentes $N(x, z), N(x, y)$, $N(y, z)$ y N_2 el otro valor tal que $N_1 \leq N_2$. Note que,

$$\left(\frac{1}{2}\right)^{N_1} + \left(\frac{1}{2}\right)^{N_1} = \left(\frac{1}{2}\right)^{N_1 - 1} \geq \left(\frac{1}{2}\right)^{N_2},$$

pues, $N_1 - 1 < N_1 \leq N_2$. Entonces en este caso, vale la desigualdad.

Tenemos,

$$\left(\frac{1}{2}\right)^{N_2} \geq 0 \Rightarrow \left(\frac{1}{2}\right)^{N_1} + \left(\frac{1}{2}\right)^{N_2} \geq \left(\frac{1}{2}\right)^{N_1},$$

y vale la desigualdad. Así, en los dos caso probamos la desigualdad. Por lo tanto, d es una métrica en Σ. ■

Definición A.9 (Espacio métrico) Un *espacio métrico* es el par (X, d) donde X es un conjunto y d la métrica en X.

Ejemplo A.3 Para la distancia definido en el Ejemplo A.1, tenemos que $(\mathbb{T}, d)$ es un espacio métrico. Como d genera los mismos abiertos en $[0,1]/\sim$ y $[0,1]$, así, usando la Proposición 2.6.3, tenemos que $(\mathbb{T}, d)$ es un espacio métrico compacto.

Definición A.10 (Bola abierta) Una *bola abierta* de radio $r > 0$ en un espacio métrico (X, d) centrando en $x \in X$ es definido por

$$B(x, r) := \{y \in X : d(x, y) < r\}.$$

Así, un espacio métrico tiene la estructura natural de un espacio topológico, pues la topología es generada por las bolas abiertas.

Proposición A.1 *Cualquier espacio métrico es un espacio de Hausdorff*

Notación. Un espacio topológico (X, τ) o un espacio métrico (X, d) sera denotado simplemente por X.

Teorema A.1 (Secuencialmente compacto) *Sea X un espacio métrico; entonces X es compacto si y solamente si, cualquier sucesión $\{x_n\}_{n\in\mathbb{N}}$ en X contiene una sub-sucesión convergente.*

Ejemplo A.4 (Σ, d) es un espacio métrico compacto.

Demostración. Por el Teorema A.1, basta probar que, dado $x^{(m)} = \{x_n^{(m)}\}_{n\in\mathbb{Z}}$ (donde $m \in \mathbb{N}$) cualquier sucesión en Σ, existe un $x \in \Sigma$ y una sub-sucesión $x^{(m_\ell)}$ de $x^{(m)}$ tal que $\lim_{\ell\to\infty} x^{(m_\ell)} = x$.

Note que los valores de la forma $x_0^{(m)}$ (con $m \in \mathbb{N}$) toman valores en $\{0, 1, 2, ..., k\}$ de infinitas maneras. Entonces, escoge $x_0 \in \{0, 1, 2, ..., k\}$ tal que $x_0^{(m)} = x_0$, para valores infinitos de m. De forma inductiva, tenemos: Para $\ell \geq 1$, tomemos $x_\ell \in \{0, 1, 2, ..., k\}$

y $x_{-\ell} \in \{0, 1, 2, ..., k\}$ tal que $x_{-\ell}^{(m)} = x_{-\ell}, ..., x_0^{(m)} = x_0, ..., x_\ell^{(m)} = x_\ell$, para cualquier m. Finalmente, tome $x = (x_\ell)_{\ell \in \mathbb{Z}}$ y $m_\ell := m$ tal que $x_{-\ell}^{(m)} = x_{-\ell}, ..., x_0^{(m)} = x_0, ..., x_\ell^{(m)} = x_\ell$. Entonces,

$$d(x^{(m_\ell)}, x) \leq \frac{1}{2^\ell} \Rightarrow \lim_{\ell \to \infty} d(x^{(m_\ell)}, x) = 0,$$

desde que $\lim_{\ell \to \infty} \frac{1}{2^\ell} = 0$. Así, $\lim_{\ell \to \infty} x^{(m_\ell)} = x$.

■

Definición A.11 (Número de Lebesgue) Sea un espacio métrico compacto X. Entonces dada una cobertura abierta $\mathcal{U}$ de X, decimos que $\varepsilon > 0$ es un *número de Lebesgue* para la cobertura abierta $\mathcal{U}$, cuando para todo $x \in X$, se tiene que $B(x, \varepsilon)$ esta contenido en algún abierto de $\mathcal{U}$.

Lema A.1 *Sea X un espacio métrico compacto; entonces toda cobertura abierta de X posee un número de Lebesgue*

Demostración. Supongamos que no existe ningún número de Lebesgue. Entonces, existe una cobertura abierta $\mathcal{U}$ de X tal que para todo $\varepsilon > 0$, existe $x \in X$ tal que $B(x, \varepsilon)$ no esta contenido en $U_\alpha \in \mathcal{U}$. En particular, para cada $n \in \mathbb{N}$, podemos escoger una sucesión $(x_n)_{n \in \mathbb{N}}$ en X tal que $B(x_n, 1/n)$ no está contenido en U_α para cualquier α.

Como X es compacto, entonces por el Teorema A.1, existe una subsucesión $\{x_{n_k}\}_{k \in \mathbb{N}}$ de $\{x_n\}_{n \in \mathbb{N}}$ que converge para $y \in X$. Note que, como $\mathcal{U}$ es una cobertura abierta de X, entonces existe $\varepsilon_1 > 0$ y algún $U_\beta \in \mathcal{U}$ tal que $B(y, \varepsilon_1) \subseteq U_\beta$. De forma análogo que antes, escoja $N \in \mathbb{N}$ de modo que $1/k < \varepsilon_1/2$ y $d(x_{n_k}, y) < \varepsilon_1/2$ para todo $k > N$. Así, se concluye que $B(x_{n_k}, 1/k) \subset U_\beta$ para todo $k > N$. Esto es una contradicción, desde que, $\{x_{n_k}\}_{k \in \mathbb{N}}$ es una subsucesión de $\{x_n\}_{n \in \mathbb{N}}$. Por lo tanto, existe un número de Lebesgue para cualquier cobertura abierta de X.

■

Corolario A.1 *Sea $\varepsilon > 0$ número de Lebesgue para el compacto X, entonces cualquier $\varepsilon_1 > 0$ tal que $\varepsilon_1 < \varepsilon$ es un numero de Lebesgue para X.*

Demostración. Como $\varepsilon > 0$ es un número de Lebesgue, entonces sea $A \in \mathcal{U}$ un abierto tal que $B(x, \varepsilon) \subset A$ para cualquier $x \in X$. Como $\varepsilon_1 < \varepsilon$, entonces, $B(x, \varepsilon_1) \subset B(x, \varepsilon)$ para cualquier $x \in X$. Luego, $B(x, \varepsilon_1) \subset A$ y, consecuentemente, $\varepsilon_1 > 0$ es un número de Lebesgue para el compacto X. ■