Benemérita Universidad Autónoma de Puebla

Facultad de Ciencias Físico Matemáticas

La hipótesis de Riemann

Tesis presentada al

Colegio de Física

como requisito parcial para la obtención del grado de

Licenciado en Física

por

Tomás Gómez González

Asesorado por

Dr. Iván Martínez Ruiz

Puebla Pue.
30 de enero de 2024

Benemérita Universidad Autónoma de Puebla

Facultad de Ciencias Físico Matemáticas

La hipótesis de Riemann

Tesis presentada al

Colegio de Física

como requisito parcial para la obtención del grado de

Licenciado en Física

por

Tomás Gómez González

Asesorado por

Dr. Iván Martínez Ruiz

Puebla Pue.
30 de enero de 2024

Título: La hipótesis de Riemann
Estudiante: Tomás Gómez González

COMITÉ

Dr. Gilberto Tavares Velasco
Presidente

Dr. Carlos Alberto López Andrade
Secretario

M.C. Juan Francisco Estrada García
Vocal

Dr. Roberto Cartas Fuentevilla
Vocal

Dr. Iván Martínez Ruiz
Asesor

Dedicado a
La pequeña Ivana que me rescató una vez, supongo $\boldsymbol{n}$ *veces y se cumple para todas las veces...*

Agradecimientos

A mis padres y hermanos que desde siempre han sido parte medular en mi desarrollo personal y profesional, a mis amigos y profesores que estuvieron conmigo en los momentos de estrés y alegría durante este largo y retador camino. Sobre todo a mi madre que me ha inspirado amor y sacrificio que son la guía a través de este viaje por las ciencias.

Índice general

Introducción

Debido a la situación actual de las matemáticas de frontera, la hipótesis de Riemann por su carácter tan importante en la teoría analítica de los números y la variable compleja constituye un problema digno de estudiar de forma meticulosa y de igual manera algunas de sus implicaciones en la física, particularmente en la teoría de cuerdas, presentamos algunos de los avances en el entendimiento de este problema pues merece ser planteado desde un enfoque un tanto más elemental para que cualquier estudiante de licenciatura de física o matemáticas pueda comprender los conceptos necesarios para un estudio posterior más formal de esta cuestión. Con la finalidad de que más estudiantes se vean más interesados en este tipo de problemas que a veces pueden parecer muy ulteriores.

La hipótesis de Riemann es uno de los veintitrés problemas planteados por el gran matemático alemán David Hilbert y constituye el octavo en su lista, también aparece como el cuarto problema en la lista de los problemas del Milenio del Clay Matematics Institute (EE.UU.). Formulado por Bernhard Riemann en 1859, en teoría analítica de números, la hipótesis de Riemann o conjetura de Riemann es una conjetura sobre la distribución de los ceros no triviales de la función zeta de Riemann. Su importancia deriva de las consecuencias que tiene sobre la distribución de los números primos.

Riemann no discutió su hipótesis en ninguna otra publicación y no hay constancia de comunicaciones privadas en las que afirmara tener una prueba de esta conjetura. En cambio, presentó como ciertos algunos otros resultados relacionados con la cantidad y la disposición de los ceros en la tira crítica que han sido todos probados, excepto uno, por otros matemáticos en los años siguientes. En particular, Riemann, además de dar una estimación del número de ceros con parte real en el intervalo $[0, 1]$ y parte imaginaria en $[-T, T]$, afirmó que la fracción de tales ceros que se encuentra en la línea crítica tiende a 1 cuando T tiende a infinito. Riemann creía tener una prueba rigurosa de esta última afirmación que, como explica en una comunicación privada a un colega, no publicó porque aún no estaba lo suficientemente simplificada. Incluso hoy, esta forma débil de la hipótesis está esperando una prueba o una negación.

Establecer una regla matemática que demuestre la existencia o no de una lógica en ausencia de una sucesión regular en la distribución de los números primos supondría entender si hay una "arritmia" total en estos últimos o si falta; esto podría tener importantes repercusiones en las aplicaciones informáticas actuales y futuras, ya que la criptografía suele utilizar números enteros como claves cuya factorización en números primos (muy grandes) no se puede calcular en tiempos aceptables. El posible conocimiento de la distribución de esta secuencia podría, por tanto, facilitar esta factorización: habría que buscar, por tanto, otras técnicas de seguridad informática, como la criptografía con funciones elípticas modulares, pero sujeta también a una conjetura pendiente (la de Birch y Swinnerton- Dyer), o la criptografía cuántica, que por el momento parece inexpugnable y cuya primera versión (DARPA Quantum Network) ya está disponible.

A lo largo de los años, muchos matemáticos han afirmado haber probado la Hipótesis de Riemann. Un caso particular lo constituye Louis de Branges de Bourcia, un matemático ya famoso por

haber resuelto la conjetura de Bieberbach. En 1992, de Branges propuso y publicó en su sitio web una prueba basada en argumentos de análisis funcional, pero los teóricos de los números permanecieron escépticos y ocho años después, Brian Conrey y Xian-Jin Li publicaron un artículo en el que proporcionaban contraejemplos que implicaban la incorrección de la prueba. En los años siguientes, de Branges a menudo modificó la prueba, todavía basándose en el mismo tipo de ideas. Sin embargo, aunque hasta el momento nadie ha verificado la corrección de la prueba después de los cambios realizados, la nueva versión también se considera incorrecta porque los argumentos utilizados se consideran inadecuados para atacar el problema.

El gran matemático Michael Atiyah, Medalla Fields en 1966 y Premio Abel en 2004, ofreció una charla en el Heidelberg Laureate Forum el pasado lunes, 24 de septiembre de 2018. Se anunció que presentaría una demostración (sencilla) de la hipótesis de Riemann. En paralelo se publicó un artículo de cinco páginas con la (supuesta) demostración, que se basa en un artículo previo de diecisiete páginas con un (supuesto) cálculo de la constante de estructura fina; ambos manuscritos fueron rechazados en arXiv, por lo que se han publicado vía Google Drive. Tras su revisión se concluyo que la supuesta prueba estaba errada.

Dada la importancia del problema y la no trivialidad de muchos resultados previos para su entendimiento, la inmensa mayoría de libros de texto presuponen que el lector es avanzado, conoce y entiende dichos resultados como lo son: la continuación analítica, el cálculo de ceros para funciones de variable compleja, el cálculo de valores numéricos de la función zeta y cómo se relacionan los ceros no triviales de la función zeta de Riemann con la distribución de los números primos.

El enfoque de este trabajo es evidenciar la mayoría de los resultados más importantes y necesarios para entender primordialmente el enunciado de la hipótesis de Riemann, su relación con la distribución de los números primos y su conexión con algunas teorías de la física. Las principales aportaciones en este trabajo consisten en dar una construcción detallada de la continuación analítica de la función zeta de Riemann, la verificación numérica de ceros no triviales empleando la fórmula de Riemann-Siegel de forma minuciosa y la elaboración de aproximaciones cada vez mejores a la función $\pi(x)$ (contador de números primos), mediante la función $R(x)$ (contador de primos de Riemann) empleando los ceros no triviales de la función ζ (zeta).

Capítulo 1

Teoría analítica de los números

Tradicionalmente, la teoría de números es esa rama de las matemáticas puras que se ocupa de las propiedades de los números enteros y contiene muchos problemas abiertos que pueden ser entendidos incluso por aquellos que no son matemáticos. De manera más general, el tema ha llegado a tratar con una clase más amplia de problemas que han surgido naturalmente del estudio de los números enteros.

La teoría analítica de números se puede dividir en diferentes campos dependiendo de los métodos utilizados y los problemas estudiados. El término "aritmética" también se usa para referirse a la teoría de números. Este término es bastante antiguo y no es tan popular como lo era antes.

Sin embargo, el término sigue siendo frecuente, por ejemplo, en el nombre de "campos" matemáticos (geometría algebraica aritmética y aritmética de curvas y superficies elípticas). Este significado de la palabra aritmética no debe confundirse con la rama de la lógica que estudia la aritmética como un sistema formal.

En la teoría elemental de números, los números enteros se estudian sin el uso de técnicas de otras áreas de las matemáticas. Esta parte incluye las cuestiones de divisibilidad, el algoritmo de Euclides para calcular el máximo común divisor, la factorización de números enteros en números primos, el estudio de números perfectos y congruencias. Las afirmaciones típicas son el pequeño teorema de Fermat y el teorema de Euler (que es una generalización del mismo), el teorema chino del resto y la ley de reciprocidad cuadrática. Se investigan las propiedades de funciones multiplicativas como la función de Möbius y la función de Euler φ; así como secuencias de números enteros como factoriales y números de Fibonacci.

La teoría de números, un tema favorito entre los antiguos griegos, vio su renacimiento en los siglos XVI y XVII en las obras de Viète, Bachet de Méziriac y especialmente Pierre de Fermat. En el siglo XVIII Euler y Lagrange hicieron importantes aportes a la teoría, la disciplina comenzó a tener una forma científica gracias a las grandes obras de Legendre (1798), y Gauss (1801). Con *Disquisitiones Arithmeticae* de Gauss (1801) se puede decir que comenzó la teoría moderna de los números.

Chebyshev (1850) proporcionó márgenes útiles para el número de números primos entre dos límites. Riemann (1859) conjeturó una fórmula asintótica mejorada para el teorema de los números primos, introdujo un análisis complejo en la teoría de la función zeta de Riemann y, a partir de sus ceros, derivó las fórmulas explícitas de la teoría de los números primos.

La teoría de las congruencias se remonta a las *Disquisiciones* de Gauss. Introdujo la notación: $a \equiv b \pmod{c}$, y exploró la mayor parte del tema. En 1847 Chebyshev publicó un trabajo en ruso sobre el mismo tema, que fue popularizado en Francia por Serret.

Además de resumir el trabajo anterior, Legendre enunció la ley de reciprocidad cuadrática. Esta ley, descubierta por inducción matemática y enunciada por Euler, fue demostrada por primera vez por Legendre en su *Théorie des Nombres* (1798), aunque sólo para casos particulares. Independientemente de Euler y Legendre, Gauss descubrió la ley alrededor de 1795 y fue el primero en dar una prueba general. Otras personalidades destacadas que contribuyeron al tema son: Cauchy, Dirichlet, del que Vorlesungen über Zahlentheorie (Lecciones de teoría de números) es un clásico, Jacobi, quien introdujo el símbolo de Jacobi, Liouville, Eisenstein, Kummer y Kronecker. La teoría se generaliza para incluir la ley de reciprocidad cúbica y bicuadrática (Gauss, Jacobi, Kummer).

La representación de números enteros en formas cuadráticas también se debe a Gauss. Cauchy, Poinsot (1845), Lebesgue (1859, 1868), y especialmente Hermite contribuyeron al tema. La teoría de las formas ternarias fue estudiada por Eisenstein, y él y H. J. S. Smith dieron notables avances en la teoría de las formas en general. Smith dio una clasificación completa de formas ternarias cuadráticas y extendió la investigación de Gauss sobre formas cuadráticas reales a formas complejas. Los estudios sobre la representación de los números como la suma de $4, 5, 6, 7, 8$ cuadrados fueron realizados por Eisenstein y la teoría fue completada por Smith.

Dirichlet fue el primero en dar una conferencia sobre el tema en una universidad alemana. Entre sus contribuciones se encuentra la extensión del último teorema de Fermat, que Euler y Legendre habían resuelto para $n = 3, 4$; Dirichlet demostró que $x^5 + y^5 \neq az^5$. Entre los últimos escritores franceses se encuentran Borel; Poincaré, cuyos resultados son numerosos e importantes; Curtiduría y Stieltjes. Entre las personalidades más eminentes de Alemania se encuentran Kronecker, Kummer, Schering, Bachmann y Richard Dedekind. En Austria, la obra Vorlesungen über allgemeine Arithmetik de Stolz (1885-86), y en Inglaterra la Teoría de los números (Parte I, 1892) de Mathews se encuentran entre las obras más completas. Genocchi, Sylvester y Glaisher hicieron otras contribuciones a la teoría.

El matemático inglés G. H. Hardy fue uno de los defensores más apasionados de la teoría de números y dedicó gran parte de su vida a ella.

Para nuestros fines la teoría analítica de números emplea como herramientas el cálculo y el análisis complejo para abordar preguntas acerca de los números enteros. Algunos ejemplos de esta son el teorema de los números primos y la hipótesis de Riemann. El problema de Waring, la conjetura de los números primos gemelos y la conjetura de Goldbach también están siendo atacados a través de métodos analíticos.

Ahora damos la siguiente definición:

Un número es un elemento de un conjunto de símbolos sujetos a una cierta axiomática.

1.1. Números Naturales

El origen del sistema de los números naturales se pierde en la noche de los tiempos. No tenemos documentos suficientes para entender cómo el hombre los haya construido o descubierto; es posible que nuestro sistema de numeración haya nacido contemporaneamente al mismo lenguaje de la especie humana. Se han encontrado troncos fósiles más antiguos a treinta mil años, marcados con incisiones a distancias regulares. En particular, fue encontrado un hueso de babuino, llamado "Hueso de Ishago" ya que se encontró en la ciudad de Ishango en el Congo Belga entre el Nilo y el lago Eduardo, que tiene muescas dispuestas de manera que nos hace pensar que representan números o cálculos. El hueso se fecha en un período entre $20,000$ a.n.E. y $18,000$ a.n.E.

En el Congo $20,000$ a.n.E.

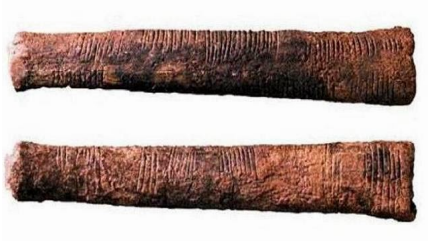


Figura 1.1: Hueso de Ishango.

Podemos imaginar que los pastores para contar los elementos del propio rebaño, hicieran marcas en sus bastones mano a mano cuando las ovejas entraban en el corral una a la vez: una marca por cada obeja. Todavía, este método de asociación uno a uno (una marca por una oveja) no es eficaz para los rebaños u objetos por contar, de grandes dimensiones. Si imaginamos, por ejemplo, la dificultad para marcar quinientas muescas en un bastón. Es posible entonces que para representar números grandes se comenzaran a usar símbolos especificos que reclamaran a la mente los grandes números y que contemporaneamente hayan sido fijadas algunas reglas para asociar estos símbolos. Sabemos que alrededor de $6,000$ años atrás los antiguos egipcios escribían los números utilizando jeroglíficos para denotar las potencias de 10 marcandolos sobre las piedras.

Números egipcios $1,500$ a.n.E.

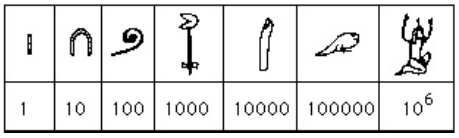


Figura 1.2: Jeroglíficos numéricos egipcios.

Los romanos usaban en cambio siete símbolos con los cuales, siguiendo determinadas reglas, representaban cualquier número.

Los símbolos son: I=1, V=5, X=10, L=50, C=100, D=500, M=1000.

El número MM representa 1000+1000 = 2000. El número VI representa $5+1=6$, mientras que el número IV representa $5-1=4$.

Números mayas 150 n.E.

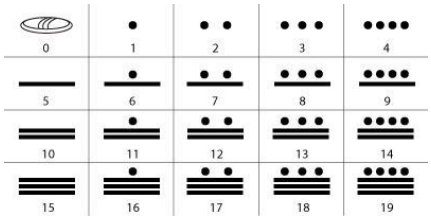


Figura 1.3: Numeración Maya.

Los primeros números que utilizamos desde pequeños para poder contar los objetos o las personas se llaman números naturales:

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, \ldots$$

El conjunto de todos estos números se representa con la letra $\mathbb{N}$. ¿Qué cosa tienen en común los dedos de una mano, con 5 manzanas, 5 rocas, 5 sillas...? Evidentemente el número 5. Una característica esto es, que es común para todos los conjuntos formados por 5 objetos. Esta característica puede ser vista como un objeto por derecho propio, un objeto abstracto de tipo matemático.

Pero los números naturales no sirven solo para indicar cuántos objetos hay (aspecto cardinal del número), también son usados para representar el orden con el cual se presentan los objetos (aspecto ordinal), el orden por ejemplo con el cual los corredores llegan a la meta: primero, segundo, tercero...

No obstante los números naturales y sus operaciones que se nos enseñan desde pequeños, la humanidad los usa desde tiempos muy antiguos y una plena comprensión no es tan simple, como demuestra el hecho que aún hoy los matemáticos los estudian. El debate sobre qué cosa sean los números y sobre qué cosa se basan ha sido particularmente animado en las primeras décadas del siglo XX, cuando los han discutido matemáticos y filósofos como Frege, Peano, Russell, Hilbert y muchos otros. Hoy existen muchos puntos de vista.

La primera y principal característica que no se puede olvidar en absoluto es que los números naturales son infinitos. La lista de números, de hecho, puede continuar indefinidamente, si consideras que puedes pensar en el número más grande que te venga a la mente pero aun así agregar una unidad y obtener uno aún mayor. No importa cuán grande sea el número más grande en el que puedas pensar, debes saber que hay infinitamente más que él.

En matemáticas hablamos de operaciones cuando, trabajando con los elementos de un conjunto, obtenemos otro elemento del mismo conjunto. La operación dentro del todo es aquella a la que se asocian dos elementos del todo para que otro elemento del mismo conjunto sea el resultado de esta operación. Las operaciones que se pueden realizar con números naturales son: (Y siempre obtendremos otro número natural)

- suma
- sustracción
- multiplicación
- exponenciación

Por su propia naturaleza cada uno de los números naturales tiene un número que le precede -que toma el nombre del anterior- y un número que le sigue -que se llama próximo o sucesivo-. En concreto, dado un número y el que le sigue (el próximo) podemos definir estos dos números consecutivos. Tomemos un ejemplo. Si tomamos el número 3, el número 2 se llamará precediendo al número y el número 4 será su consecuente. Como es fácil de adivinar, solo hay un número natural que no responde a esta regla y es el 1. Como el primero de todos los números naturales, de hecho, el uno no puede tener precedente, es decir, ningún número natural puede existir antes de uno.

Para entender cómo se comparan dos números naturales es necesario conocer los símbolos que siempre se encontrarán en la vida, los que aprendimos desde los primeros años de escuela:

- $>$
- $=$

Donde el símbolo "$>$" puede aparecer invertido "$<$" que se emplea para comparar dos números y especificar si uno es mayor que otro, donde el vértice siempre apunta al número más pequeño, por ejemplo: $3 > 2$ ó $2 < 3$. Y el símbolo "$=$" se emplea para indicar la igualdad entre ambos números: $5 = 5$.

Por tanto, acabamos de explicar cómo siempre es posible establecer si dos números del conjunto $\mathbb{N}$ son iguales o si uno es mayor o menor que el otro. Esta situación se llama propiedad y se puede definir de la siguiente manera: el conjunto de los números naturales $\mathbb{N}$ es un conjunto ordenado[1].

La representación gráfica

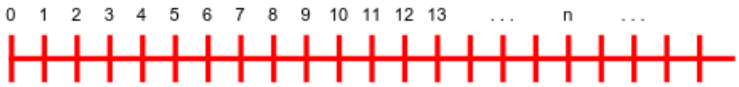


Figura 1.4: Recta de los números naturales.

El conjunto $\mathbb{N}$ de los números naturales se puede representar gráficamente en una recta horizontal y con una línea vertical vamos a marcar un segmento de recta y eso será una unidad. La primera línea corresponderá al número 1, el segundo el número 2, al tercero el número 3 y así sucesivamente. Así tendremos la representación gráfica de algunos elementos del conjunto $\mathbb{N}$.

[1] **Conjunto ordenado**:
A es un conjunto ordenado cuando la relación $\leq$ cumple las propiedades reflexiva, antisimétrica y transitiva. A saber:
Reflexiva $a \leq a$.
Antisimétrica $[a \leq b \ \wedge \ b \leq a] \ \Rightarrow \ a = b$.
Transitiva $[a \leq b \ \wedge \ b \leq c] \ \Rightarrow \ a \leq c$.

1.2. Números Enteros

Los números enteros (o enteros relativos o, simplemente, números relativos) corresponden al conjunto obtenido al unir los números naturales $\mathbb{N}$, los inversos aditivos de los números naturales $\mathbb{N}_- = \{-1, -2, -3, ...\}$ es decir, los que se obtienen colocando un signo "$-$" delante de los naturales, y el cero 0. Este conjunto en matemáticas se indica con Z o $\mathbb{Z}$, porque es la letra inicial de "Zahl" que en alemán significa número (originalmente "contar", de hecho la expresión implica el uso de números negativos).

Los números enteros se definen entonces exactamente como el conjunto de números que son el resultado de la resta de números naturales. Los números enteros se pueden sumar, restar y multiplicar y el resultado sigue siendo un número entero. Sin embargo, el inverso multiplicativo de un número entero no es un número entero en general, sino un número racional; formalmente este hecho se expresa diciendo que $\mathbb{Z}$ es un anillo conmutativo[2], pero no un campo[3].

Definición 1.2.1. Al conjunto $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \mathbb{N}_-$ se le llama conjunto de números enteros.
La representación gráfica

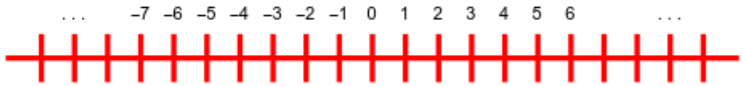


Figura 1.5: Recta de los números enteros.

El conjunto $\mathbb{Z}$ de los números enteros se puede representar gráficamente en una recta horizontal y con una línea vertical vamos a marcar un segmento de recta y eso será una unidad. Asignaremos al 0 el lugar central de nuestra gráfica, a la izquierda del cero se encontrarán los elementos del conjunto $\mathbb{N}_-$ y a la derecha del cero se encontrarán los elementos del conjunto $\mathbb{N}$. Así tendremos la representación gráfica de algunos elementos del conjunto $\mathbb{Z}$.

Luego $\mathbb{Z}$ dado por extensión: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ \ldots\}$.

Definición 1.2.2. El número $a \in \mathbb{Z}$ divide al número $n \in \mathbb{Z}$ si existe $b \in \mathbb{Z}$ tal que: $n = ab$.

Observar que no se puede dividir por cero. Si a divide a n se denota $a \mid b$ (a divide a b). Cada número n tiene siempre dos divisores triviales: 1 y el mismo: $n = 1 \cdot n$.

[2]**Anillo conmutativo**:
En teoría de anillos , un anillo conmutativo es un anillo $(R, +, \cdot)$ en el que la operación de multiplicación $\cdot$ es conmutativa; es decir, si para cualquiera $a, b \in R$, $a \cdot b = b \cdot a$.
En álgebra abstracta, un anillo es un sistema algebraico formado por un conjunto y dos operaciones binarias, llamadas usualmente «suma» y «producto», que cumplen ciertas propiedades.

[3]**Campo**:
Un campo F es un sistema algebraico en el cual las operaciones binarias llamadas adición y multiplicación cumplen las propiedades:
1. La suma es conmutativa, i.e., $\forall a, b \in F$: $a + b = b + a$.
2. La suma es asociativa, i.e., $\forall\ a, b, c \in F$: $(a + b) + c = a + (b + c) = (a + c) + b$.
3. $\exists\ 0 \in F$, $\forall a \in F$: $a + 0 = 0 + a$, el elemento 0 se llama elemento neutro de la suma.
4. $\forall a \in F$, $\exists\ -a \in F : a + (-a) = (-a) + a = 0$, $-a$ se llama inverso aditivo de a.
5. El producto es conmutativo, i.e., $\forall\ a, b \in F$: $a \cdot b = b \cdot a$.
6. El producto es asociativo, i.e., $\forall\ a, b, c \in F$: $(a \cdot b) \cdot c = a \cdot (b \cdot c) = (a \cdot c) \cdot b$.
7. $\exists\ 1 \in F$, $\forall\ a \in F$: $a \cdot 1 = 1 \cdot a = a$, además $1 \neq 0$.
8. $\forall\ a \in F : a \neq 0$, $\exists\ a^{-1} \in F : a \cdot (a^{-1}) = (a^{-1}) \cdot a = 1$.
9. $\forall\ a, b, c \in F : a \cdot (b + c) = a \cdot b + a \cdot c \ \ \wedge \ \ (a + b) \cdot c = a \cdot c + b \cdot c$.

Generalmente tenemos la división euclídea:

Proposición 1.2.3. (Algoritmo de la división)
Dados dos números enteros a, b, con $b \neq 0$, existe una única pareja de números enteros q y r tales que: $a = bq + r$ con $0 \leq r \leq b$. Además, $r = 0$, si, y sólo si, $b \mid a$. Se dice que q es el cociente y r el resto obtenido al dividir a por b.

Demostración:
Sea S el conjunto de enteros no negativos dado por

$$S = \{y : y = a - bx,\ x \in \mathbb{Z},\ y \geq 0\}.$$

Es un conjunto no vacío de enteros no negativos, por lo tanto admite mínimo, que designaremos $a - bq$. Sea $r = a - bq$, entonces $a = bq + r$ y $r \geq 0$. Ahora demostraremos que $r < b$. Supongamos $r \geq b$, entonces $0 \leq r - b < r$. Pero $r - b \in S$ ya que $r - b = a - b(q + 1)$. Por lo tanto $r - b$ es un elemento de S menor que su elemento mínimo r. Esta contradicción prueba que $r < b$. El par q, r es único, ya que si existiese otro par con estas condiciones q', r', entonces $bq + r = bq' + r'$, de donde $b(q - q') = r'$. Luego $b \mid (r' - r)$, si $r' - r \neq 0$ tendremos $b \leq |r - r'|$, que conduce a una contradicción. Por consiguiente $r' = r$ y $q' = q$. Finalmente es claro que $r = 0$ si, y sólo si, $b \mid a$.

Este teorema a pesar de ser un teorema de existencia, su demostración nos da un método para calcular el cociente q y el resto r. Restamos de a (o sumamos a a) múltiplos de b hasta obtener el menor número no negativo de la forma $a - bx$.

En lo posterior usaremos el Principio del Mínimo (que puede ser tomado como axioma):

Axioma 1.2.4. (Principio del Mínimo)
Si $X \subseteq \mathbb{N}$ es un subconjunto no vacío, entonces X tiene un elemento mínimo, esto es existe $m \in X$ tal que: $\forall x \in X,\ m \leq x$. Este principio tiene otra formulación que se conoce como el Principio del Buen Orden.

Definición 1.2.5. Un entero positivo p mayor que 1 que sólo es divisible por 1 y por p se llama un número primo. Un entero positivo mayor que 1 que no es primo es un número compuesto.

Los números primos menores o iguales a 20 son: $2, 3, 5, 7, 11, 13, 17, 19$.

El número 1 (unidad) no es considerado primo porque 1 divide a cada número $(n = 1 \cdot n)$.

Lema 1.2.6. Cada entero positivo mayor que 1 tiene un divisor primo.

Demostración:
(Por contradicción) Supongamos que existe l entero positivo que no tiene divisores primos, sea $A = \{n \in \mathbb{N} : n > 1 \text{ y } n \text{ no tiene divisores primos}\} \subseteq \mathbb{N}$, $A \neq \emptyset$ ya que $l \in A$, luego $A \subseteq \mathbb{N}$ y $A \neq \emptyset$, entonces A tiene mínimo, por el Principio del Buen Orden (P.B.O.)[4], sea $m_0 = \min A$ $(m_0 \in A)$, m_0 no tiene divisores primos y $m_0 \mid m_0$, luego m_0 no es un número primo, entonces $m_0 = ab$ para $a, b \in \mathbb{N}$ tales que $1 < a, b < m_0$, como $a < m_0$ entonces $a \notin A$ de ahí que existe p número primo tal que $p \mid a$ pero $a \mid m_0$, por consiguiente $p \mid m_0$! Lo cual es una contradicción. Por lo tanto, todo entero positivo más grande que 1 tiene al menos un divisor primo.

[4]**Principio del Buen Orden**:
En cualquier conjunto de números naturales $B \subseteq \mathbb{N}$ con $B \neq \emptyset$ existe un mínimo, es decir, un número $n \in B$ menor o igual que cualquier número del conjunto B.

1.3. Números Racionales

En el conjunto de los números naturales $\mathbb{N}$ y los números enteros $\mathbb{Z}$ no siempre es posible realizar una división. Si intentamos realizar $7/2$ obtenemos un número no entero, i.e., 3,5. Para poder hacer siempre la división, es necesario ampliar el conjunto de los enteros añadiendo los que se definen como números racionales. ¿Qué utilidad tienen en la vida real? He aquí un ejemplo concreto: "la mitad de la clase estuvo ausente hoy". La palabra *mitad* indica la división de $1/2$ que no tiene un resultado entero.

Podemos decir que el conjunto de números racionales $\mathbb{Q}$ está dado por todos los números que se pueden expresar en forma de fracción.

Definición 1.3.1. El conjunto de los números racionales es el conjunto

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z} \ \wedge \ b \neq 0 \right\}.$$

Observación: Es fácil notar que $\mathbb{Z} \subseteq \mathbb{Q}$, ya que si $a \in \mathbb{Z}$, entonces $a = \frac{a}{1} \in \mathbb{Q}$. En particular el 1 y el 0 son racionales.

Definición 1.3.2. Para cada número real x, denotaremos por $[x]$ al único número entero que cumple que $x \in [[x], [x] + 1)$ y llamaremos al entero $[x]$ la parte entera de x.

Por ejemplo: $[5] = 5$, $[-11] = -11$, $[3{,}5] = 3$, $[-3{,}5] = -4$, $\left[-\frac{1}{2}\right] = -1$.

Definición 1.3.3. La función parte entera superior de un número x, denotada $\lceil x \rceil$ devuelve el menor entero mayor o igual a x, i.e.,

$$\lceil x \rceil = \min \{ n \in \mathbb{Z} \mid n \geq x \}.$$

Por ejemplo: $\lceil 2{,}25 \rceil = 3$, $\lceil 2 \rceil = 2$, $\lceil -2{,}25 \rceil = -2$.

Definición 1.3.4. La función parte entera inferior de un número x, denotada $\lfloor x \rfloor$, devuelve el más grande entero menor o igual a x, i.e.,

$$\lfloor x \rfloor = \max \{ n \in \mathbb{Z} \mid n \leq x \}.$$

Por ejemplo: $\lfloor 2{,}8 \rfloor = 2$, $\lfloor -2 \rfloor = -2$, $\lfloor -2{,}3 \rfloor = -3$. Las definiciones 1.3.2. y 1.3.4. son dos formas distintas para enunciar el mismo concepto, aquí las enunciamos porque no se suele mencionar su equivalencia en la bibliografía y dadas las distintas notaciones se puede prestar a confusión.

Definición 1.3.5. La parte fraccionaria (también conocida como la parte fraccional o decimal) es una función que asocia a cada número real x su valor menos su parte entera: $\{x\} = x - \lfloor x \rfloor$.

Por ejemplo: $\{3{,}1416\} = 3{,}1416 - \lfloor 3{,}1416 \rfloor = 3{,}1416 - 3 = 0{,}1416$,
$\{5{,}735\} = 5{,}735 - \lfloor 5{,}735 \rfloor = 5{,}735 - 5 = 0{,}735$,
$\{-8{,}21\} = -8{,}21 - \lfloor -8{,}21 \rfloor = -8{,}21 - (-9) = 0{,}79$.

Teorema 1.3.6. (Propiedad de densidad de $\mathbb{Q}$)
Sean x, y números reales, si $x < y$, existe $r \in \mathbb{Q}$ tal que $x < r < y$.
Demostración:

Como $x < y$, se tiene que $y - x > 0$ y por la propiedad arquimediana[5], existe $n_0 \in \mathbb{N}$ tal que $1 < n_0(y - x)$ y por lo tanto $n_0 x + 1 < n_0 y$. Por otro lado si $[n_0 x]$ se denota por m, se tiene que $m \leq n_0 x < m + 1$ y entonces $n_0 x < m + 1 \leq n_0 x + 1 < n_0 y$, así que, dividiendo entre n_0, queda

$$x < \frac{m+1}{n_0} < y, \quad \text{con} \quad \frac{m+1}{n_0} \in \mathbb{Q}.$$

La representación gráfica

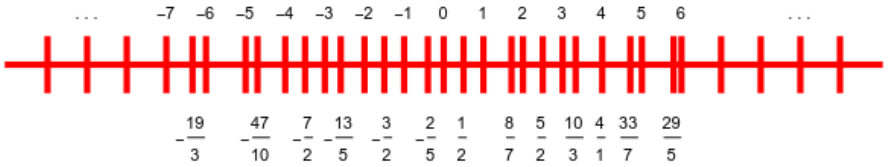


Figura 1.6: Recta de los números racionales.

El conjunto $\mathbb{Q}$ de los números racionales se puede representar gráficamente en una recta horizontal y con una línea vertical vamos a marcar un segmento de recta y eso asignara el lugar que corresponda a cada número racional. Asignaremos al 0 el lugar central de nuestra gráfica, a la izquierda del cero se encontrarán los elementos negativos $(-)$ y a la derecha del cero se encontrarán los elementos positivos $(+)$. Así tendremos la representación gráfica de algunos elementos del conjunto $\mathbb{Q}$.

1.4. Números Irracionales

Cuando se trata de operaciones entre números naturales $\mathbb{N}$, estas operaciones no siempre son internas al conjunto $\mathbb{N}$, es decir, el resultado no forma parte de los números naturales. Por ejemplo en la resta entre dos números en los que el minuendo (primer término) es menor que el sustraendo, o en la división de algunos números. Surge así la necesidad de introducir nuevos grupos numéricos; para hacer factible la resta se introdujeron los números enteros $\mathbb{Z}$, para el cociente se introdujeron los números racionales $\mathbb{Q}$, es decir, aquellos números que se pueden expresar de la forma a/b donde $a, b \in \mathbb{Z}$ y $b \neq 0$.
Parecería que todo va bien, pero no tuvimos en cuenta la extracción de raíz. ¿Qué número es, por ejemplo, la raíz cuadrada de dos?

$$\sqrt{2} = 1,414213562373095048801688724209 69\ldots$$

Es un número que no se puede expresar como a/b donde $a, b \in \mathbb{Z}$ y $b \neq 0$, y es decimal, ilimitado y no periódico. Este es un número irracional. Denotaremos el conjunto de números irracionales con $\mathbb{I}$. Sin embargo, podemos ver que este conjunto es un subconjunto de los números reales $\mathbb{R}$ como todos los demás conjuntos mencionados anteriormente.

Demostremos que la raíz cuadrada del 2 es un número irracional:
Demostración:
(Por reducción al absurdo) Supongamos que $\sqrt{2}$ no es es irracional y, por tanto, es racional. Entonces existen $p, q \in \mathbb{Z}$ tales que

$$\sqrt{2} = \frac{p}{q}, \quad p, q \in \mathbb{Z}$$

[5]**Propiedad Arquimediana**:
1. Dado cualquier número $x \in \mathbb{Q}$, existe un $n \in \mathbb{N}$ que satisface $n > x$.
2. Dado cualquier número real $y > 0$, existe un $n \in \mathbb{N}$ que satisface $\frac{1}{n} < y$.

Podemos suponer, sin pérdida de generalidad, que el máximo común divisor de p y q es 1, i.e., que no tienen factores comunes y por tanto son primos relativos. Elevamos al cuadrado y operando queda:

$$2 = \frac{p^2}{q^2} \quad \Rightarrow \quad 2q^2 = p^2$$

Por tanto p^2 debe ser múltiplo de 2, lo que implica que p también es un múltiplo de 2. i.e., $p = 2k$ para un cierto k. Sustituimos este valor de p en la expresión anterior y simplificamos un 2 de esa igualdad:

$$2q^2 = (2k)^2 \quad \Rightarrow \quad 2q^2 = 4k^2 \quad \Rightarrow \quad q^2 = 2k^2$$

La expresión anterior nos asegura que q^2 es múltiplo del 2, y por tanto también lo es q. Y aquí está el absurdo: habíamos supuesto que p y q no tenían factores comunes (i.e., $\text{mcd}(p, q) = 1$) y hemos llegado a que los dos son múltiplos del 2, i.e., que tienen al 2 como factor común, y por tanto su mcd debe ser al menos el 2. Esa es la contradicción que buscábamos. Por lo tanto la raíz cuadrada del 2 es un número irracional, i.e., $\sqrt{2} \in \mathbb{I}$.

Definición 1.4.1. Al conjunto $\mathbb{R} - \mathbb{Q} = \mathbb{I}$ se le llama conjunto de números irracionales.

Evidentemente, cabe señalar que la extracción de la raíz cuadrada no es una operación interna a los números irracionales, sino también otras raíces (tercera, cuarta, etc.). Sin embargo, cabe señalar que no todas las raíces cuadradas, cúbicas y otras dan lugar a números irracionales.
Por ejemplo: $\sqrt{81} = 9$ nueve es un cuadrado perfecto. $\sqrt[3]{8} = 2$.

Luego están los números irracionales particulares que merecen una mención aparte, debido a que no solo en las matemáticas son muy utilizados, entre estos encontramos:
Al número pi: $\pi = 3,14159265358979\ldots$.
Al número neperiano o número de Euler: $e = 2{,}718281828459045\ldots$.
Al número áureo (proporción divina): $\varphi = 1,6180339887\ldots$. Indica la relación entre dos longitudes desiguales, donde la mayor es un promedio proporcional entre la menor y la suma de las dos. Curiosidad: es posible aproximar cada vez mejor este número a partir de la relación entre dos términos sucesivos de la conocida sucesión de Fibonacci (que se define a continuación).

Definición 1.4.2. (Sucesión de Fibonacci)
Se trata de una secuencia infinita de números naturales; a partir del 0 y del 1, se van sumando a pares, de manera que cada número es igual a la suma de sus dos anteriores, de manera que: $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$. de manera más formal tenemos:

$$1, 1, 2, 3, 5, 8, 13, \ldots \; ; \quad f_1 = 1, \quad f_2 = 1, \quad f_n = f_{n-2} + f_{n-1}, \quad n \geq 3.$$

La representación gráfica

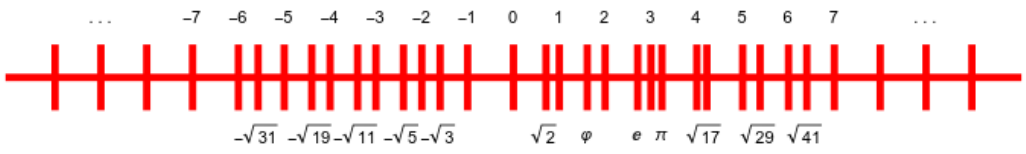


Figura 1.7: Recta de los números irracionales.

El conjunto $\mathbb{I}$ de los números racionales se puede representar gráficamente en una recta horizontal y con una línea vertical vamos a marcar un segmento de recta y eso asignara el lugar que corresponda

a cada número irracional en la parte inferior de la recta horizontal. Asignaremos al 0 el lugar central de nuestra gráfica, a la izquierda del cero se encontrarán los elementos negativos $(-)$ y a la derecha del cero se encontrarán los elementos positivos $(+)$, y en la parte superior de la recta tenemos como "guía" a los números enteros. Así tendremos la representación gráfica de algunos elementos del conjunto $\mathbb{I}$.

Teorema 1.4.3. Si p es un número primo, entonces $\sqrt{p}$ es irracional.
La demostración se hará más adelante con ayuda del teorema fundamental de la aritmética o de la factorización única, el cual establece que todo entero positivo mayor que 1 puede escribirse de forma única como un producto de potencias de números primos.

1.5. Números Trascendentales

Un número trascendente o número trascendental es un número irracional que no es un número algebraico[6], es decir, no es la solución de ninguna ecuación polinomial de la forma:

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$

donde $n \geq 1$ y los coeficientes a_i son racionales y no todos nulos. El conjunto de los números trascendentes no es cerrado con respecto a la suma o al producto; de hecho, si a es trascendente, también lo será $-a$ pero su suma, que es 0, es obviamente un número algebraico; análogamente para a y $1/a$.

El conjunto de números algebraicos es contable mientras que el conjunto de los números reales es incontable; esto implica que el conjunto de los números trascendentes es incontable, es decir, hay infinitamente más números trascendentes que algebraicos. Este resultado fue demostrado por Georg Cantor a finales del siglo XIX. Demostrar que un número dado es trascendente puede ser muy difícil. La normalidad, otra propiedad de los números, podría ayudar a determinar su trascendencia.

La existencia de números trascendentes fue demostrada por primera vez en 1844 por Joseph Liouville, quien logró construir toda una clase de números trascendentes, así llamados números de Liouville; en particular entre estos está la constante de Liouville:

$$\sum_{k=1}^{\infty} 10^{-k!} = 0{,}110001000000000000000001000\ldots$$

de los cuales el n-ésimo dígito después de la coma es igual a uno si n es un factorial (por ejemplo: $1, 2, 6, 24, 120, 720, ...$, etc.) y 0 en caso contrario. El primer número construido sin propósito que demostró ser trascendente es e; Charles Hermite lo demostró en 1873. En 1882, Ferdinand von Lindemann publicó una prueba basada en el trabajo anterior de Hermite sobre la trascendencia de π. En 1874 Georg Cantor había demostrado la existencia y no numerabilidad de los números trascendentes.

El descubrimiento de los números trascendentes permitió demostrar la imposibilidad de varios problemas geométricos antiguos relacionados con la construcción con regla y compás; la cuadratura del círculo, el más famoso de estos problemas, es imposible porque π es trascendente mientras que todos los números que se pueden construir con regla y compás son algebraicos.

[6] **Número algebraico**
En matemáticas, un número algebraico es un número real o complejo que es la solución de una ecuación polinomial de la forma:

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$

donde $n > 0$, cada a_i es un entero, y a_n es distinyo de 0.

Algunos números trascendentes:

- e^a si a es algebraico y diferente de 0. En particular, el mismo número e es trascendente. Este resultado se conoce como el teorema de Lindemann-Weierstrass.
- π la constante matemática.
- a^b donde a es algebraico distino de 1 y 0, y b es algebraico, pero no racional.
- e^π llamado constante de Gel'fond.
- La función zeta de Riemann $\zeta(n)$ para n par, ya que son múltiplos racionales de π.

Se ha conjeturado que otros números como $\zeta(n)$ para n impar o la constante de Euler-Mascheroni (que se define a continuación) γ son trascendentes, pero no se ha probado que lo son.

Constante de Euler-Mascheroni
Esta constante se define de la siguiente forma:

$$\gamma = \lim_{n\to\infty}\left(\sum_{k=1}^{n}\frac{1}{k} - \ln(n)\right)$$

Es decir, γ se define como el límite de la diferencia de la sucesión de sumas parciales de la serie armónica y el logaritmo neperiano. Otras formas de definirla son las siguientes:

$$\gamma = \int_1^\infty \left(\frac{1}{\lfloor x\rfloor} - \frac{1}{x}\right)dx \;\; = \;\; -\int_0^\infty \frac{\ln(x)}{e^x}dx$$

Su valor aproximado es: $\gamma \simeq 0{,}57721\ 56649\ 01532\ 86060\ 65120\ 90082\ldots$

1.6. Infinitud de los números primos

Uno de los temas más estudiados a lo largo de la historia de las matemáticas ha sido la infinitud de los números primos, cuya primera demostración fue elaborada por Euclides en el siglo III a.n.E. Desde esa fecha hasta nuestros días, han sido propuestas cientos de demostraciones.

Teorema 1.6.1. Hay un número infinito de números primos.
Demostración:
(Por contradicción) Supongamos que sólo existen un número finito de números primos, a saber, $p_1, p_2, \ldots, p_n$. Sea $Q = p_1, p_2, \ldots, p_n + 1$, $Q \in \mathbb{N}$ y es tal que $Q > 1$, entonces existe q número primo tal que (por el Lema 1.2.6.), $q \mid Q$, de ahí que $q = p_j$ para algún $j \in \{1, 2, \ldots, n\}$ pero $p_1p_2\cdots p_n = p_1p_2\cdots p_{j-1}p_jp_{j+1}\cdots p_n = p_j(p_1p_2\cdots p_{j-1}p_{j+1}\cdots p_n)$ entonces $p_j \mid p_1p_2\cdots p_n$, i.e., $q \mid p_1p_2\cdots p_n$ entonces $q \mid Q - p_1p_2\cdots p_n$ entonces $q \mid p_1p_2\cdots p_n + 1 - p_1p_2\cdots p_n$ entonces $q \mid 1$! En consecuencia, q es un primo que no está en la lista $p_1, p_2, \ldots, p_n$. Esta contradicción exhibe que hay un número infinito de números primos.

Otra demostración (debida a Hermite), más directa, es la siguiente. En tanto observamos el siguiente:

Lema 1.6.2. Sea $n > 1$ un entero y sea $\mathrm{Div}(n) = \{1 = d_0, d_1, \ldots, d_r = n\}$ el conjunto de sus divisores, con $1 < d_1 < d_2 < \cdots < d_{r-1} < n$. Entonces d_1 es primo.
Demostración:

Si d_1 no es primo, existe d, $1 < d < d_1$ tal que $d \mid d_1$ [7], pero $d \mid d_1$ y $d_1 \mid n$, se sigue $d \mid n$, contra la definición de d_1.

Consideramos ahora el número $n! := 1 \cdot 2 \cdot 3 \cdots n$ (n factorial). El divisor más pequeño mayor que 1 de $N := n! + 1$ es mayor que n, en efecto, si $k \leq n$, $k \nmid n! + 1$ ya que:

$$\frac{N}{k} = \frac{1 \cdot 2 \cdot 3 \cdots k \cdots n}{k} + \frac{1}{k},$$

y $\frac{1}{k} \notin \mathbb{N}$. Luego d_1 el divisor más pequeño mayor que 1 de N verifica $d_1 > n$. Por el lema 1.6.1. se sigue que: $\forall\, n \in \mathbb{N}$, $\exists\, p$, p primo con $p > n$. Por lo tanto el conjunto de números primos $\mathbb{P}$ es infinito.

Veamos una tercera demostración, usaremos dos igualdades probadas por Euler y que π^2 es irracional. Estas dos igualdades son:

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

Demostración:
Supongamos que sólo existe una cantidad finita de números primos, por lo tanto $\prod_p^{\infty} \frac{1}{1-p^{-2}}$ será siempre un número racional, al ser un producto finito de fracciones. Por otro lado, utilizando las igualdades probadas por Euler tenemos:

$$\frac{\pi^2}{6} = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots = \sum_{n=1}^{\infty} \frac{1}{n^2} = \prod_{p}^{\infty} \frac{1}{1 - p^{-2}}$$

Entonces, llegamos a que el lado izquierdo de la igualdad es un número irracional, mientras que el derecho es un número racional. Luego, llegamos a una contradicción. Por lo tanto el conjunto de números primos $\mathbb{P}$ es infinito.

1.7. El teorema fundamental de la Aritmética

Lema 1.7.1. Sean $a, b, c \in \mathbb{N}$ tales que $a \mid bc$ y $(a, b) = 1$ entonces $a \mid c$.
Demostración:
Como $(a, b) = 1$ entonces existen $s, t \in \mathbb{Z}$ tales que $1 = sa + tb$ entonces
$c = csa + ctb$ pero $a \mid bc$ entonces $a \mid ctb$ además $a \mid csa$ entonces $a \mid csa + ctb$
entonces $a \mid c$.

Lema 1.7.2. Si $p \mid a_1 a_2 \cdots a_n$ donde p es un número primo y $a_1, \ldots, a_n$ son enteros positivos, entonces $p \mid a_i$ para algún $i \in [n]$[8].
Demostración:
(Por inducción sobre el número de factores) Si $n = 1$ el resultado es inmediato; supongamos que el resultado se cumple para n factores y demostremos que el resultado se cumple para $n + 1$ factores.
Supongamos $p \mid a_1 a_2 \cdots a_n a_{n+1}$, luego $p \mid a_i(a_1 \cdots a_{i-1} a_{i+1} \cdots a_n a_{n+1})$ si p divide a $a_1 \cdots a_{i-1} a_{i+1} \cdots a_n a_{n+1}$ por hipótesis inductiva $p \mid a_j$ para algún j que pertenece a $\{1, \ldots, n+1\} \backslash \{i\}$ y el resultado se cumple si
$p \nmid a_1 \cdots a_{i-1} a_{i+1} \cdots a_n a_{n+1}$ entonces $(p, a_1 \cdots a_{i-1} a_{i+1} \cdots a_n a_{n+1}) = 1$ pero
$p \mid a_i(a_1 \cdots a_{i-1} a_{i+1} \cdots a_n a_{n+1}) \quad \Rightarrow \quad p \mid a_i$ para algún $i \in \{1, \ldots, n+1\}$.

[7] De la definición: si $n > 1$ no es primo entonces existe d, $1 < d < n$ con $d \mid n$.
[8] Aquí "$i \in [n]$" denota que i corre de 1 hasta n.

Teorema 1.7.3. (El Teorema Fundamental de la Aritmética)
Todo entero positivo más grande que 1 puede escribirse de manera única como producto de números primos, con los factores primos en el producto escritos en orden creciente.

Demostración:
(Existencia) Supongamos que existe $n \in \mathbb{N}$ con $n > 1$ tal que n no puede escribirse como un producto de números primos. Sea $A = \{k \in \mathbb{N} : k > 1$ y no puede escribirse como un producto de primos$\}$, $A \subseteq \mathbb{N}$ y $A \neq \emptyset$ ya que $n \in A$ entonces A tiene mínimo, digamos que $m = \text{mín}\, A$, por el P.B.O., m no puede ser un número primo ya que de ser así, i.e., si m es primo entonces m es un producto de primos (con m el único factor primo) lo cual es una contradicción. Entonces $m = ab$ para algunos $a, b \in \mathbb{Z}$ tales que $1 < a < b < m$, pero $a, b < m$, $m = \text{mín}\, A$, de ahí que $a = p_1 p_2 \cdots p_r$, $b = q_1 q_2 \cdots q_s$ donde p_i-primos y q_j-primos, $i \in [r]$, $j \in [s]$ y además $p_1 \leq p_2 \leq \cdots \leq p_r$, $q_1 \leq q_2 \leq \cdots \leq q_s$, de manera que $m = ab = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$! Contradicción que se deriva de suponer que existen $n \in \mathbb{N}$, $n > 1$, tal que n no se puede escribir como un producto de números primos. $\therefore \forall\, n \in \mathbb{N} : n > 1 \quad \Rightarrow \quad n = p_1 p_2 \cdots p_t$, con p_i-primos, $i \in [t] \quad \wedge \quad p_1 \leq p_2 \leq \cdots \leq p_t$.

(Unicidad) Supongamos que $n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$ con p_i, q_j primos, donde $i \in [s]$, $j \in [t]$ y $p_1 \leq p_2 \leq \cdots \leq p_s$, $q_1 \leq q_2 \leq \cdots \leq q_t$. Entonces $p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$ entonces $p_i(p_1 p_2 \cdots p_{i-1} p_{i+1} \cdots p_s) = q_1 q_2 \cdots q_t$ entonces $p_i \mid q_1 q_2 \cdots q_t$ entonces $\exists\, j \in [t] : p_i \mid q_j$ entonces $p_i = q_j$ entonces $\forall\, i \in [s]$, $\exists\, j \in [t] : p_i = q_j$, por otro lado, $q_k(q_1 \cdots q_{k-1} q_{k+1} \cdots q_t) = p_1 p_2 \cdots p_s$ entonces $q_k \mid p_1 p_2 \cdots p_s$ entonces $\exists\, l \in [s] : q_k \mid p_l$ entonces $q_k = p_l$ entonces $\forall\, k \in [t]$, $\exists\, l \in [s] : q_k = p_l$. Supóngase que $s \neq t$ entonces $s < t \quad \vee \quad t < s$:

Caso 1. Si $s < t$ y como $p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$ entonces $1 = q'_1 q'_2 \cdots q'_{t-s}$! donde $q'_u \in \{q_1, q_2, \cdots, q_t\}$, $u \in [t - s]$.

Caso 2. Si $t < s$ y como $p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$ entonces $1 = p'_1 p'_2 \cdots p'_{s-t}$! donde $p'_v \in \{p_1, p_2, \cdots, p_s\}$, $v \in [s - t]$. De ahí que $s = t$.

Definición 1.7.4. El máximo común divisor de dos números enteros a y b, no ambos iguales a cero, es el entero positivo más grande d que divide a a y b, el cual se denota por $d = \text{mcd}(a, b)$ o bien $d = (a, b)$.

Por ejemplo, los divisores comunes de 24 y 84 son: $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$, por consiguiente, $(24, 84) = 12$, también tenemos: $(15, 81) = 3$, $(100, 5) = 5$, $(17, 25) = 1$, $(0, 44) = 44$, $(-6, -15) = 3$, $(17, 289) = 17$.
En el caso del $(15, 81)$ tenemos que los divisores de 15 son: $\pm 1, \pm 3, \pm 5, \pm 15$, mientras que los divisores de 81 son: $\pm 1, \pm 3, \pm 9, \pm 27, \pm 81$, luego los divisores comunes de 15 y 81 son: $\pm 1, \pm 3$, de ahí que $(15, 81) = 3$.

Definición 1.7.5. Los enteros a y b son llamados primos relativos o coprimos si y sólo si $(a, b) = 1$.

Por ejemplo:

- 17 y 25 son primos relativos.
- 25 y 42 son primos relativos, $(25, 42) = 1$
- 19 y 34 son primos relativos, $(19, 34) = 1$
- 17 y 19 son coprimos ya que $(17, 19) = 1$

Observese que $(a,b) = (|a|,|b|)$ ya que los divisores de a y $-a$, así como los de b y $-b$ son los mismos, por lo tanto podemos restringir nuestra atención al máximo común divisor de dos enteros positivos.

Proposición 1.7.6. Sean $a,b,c \in \mathbb{Z}$ con $d = (a,b)$, entonces
i) $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$,
ii) $(a+cb, b) = (a,b)$.

Demostración:
i) Sean $a,b \in \mathbb{Z}$ tales que $d = (a,b)$, exhibiremos que $\frac{a}{d}$ y $\frac{b}{d}$ no tienen divisores comunes distintos de 1. Supongamos que $t \in \mathbb{N}$ tal que $t \mid \frac{a}{d}$ y $t \mid \frac{b}{d}$ entonces existen $k_1, k_2 \in \mathbb{Z}$ tales que $\frac{a}{d} = k_1 t$ y $\frac{b}{d} = k_2 t$ entonces $a = d(k_1 t) \ \wedge \ b = d(k_2 t)$ entonces $a = (dt)k_1 \ \wedge \ b = (dt)k_2$ entonces dt es un divisor común de a y b entonces $dt \leq d$ ya que $d = (a,b)$ entonces $t \leq 1$ entonces $t = 1$ por lo tanto $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.
ii) Sean $a,b,c \in \mathbb{Z}$. Mostraremos que los divisores comunes de a y b son exactamente los mismos divisores comunes de $a+cb$ y b. Sea $t \in \mathbb{N} : t \mid a \ \wedge \ t \mid b$ entonces $t \mid a+cb \ \wedge \ t \mid b$, de manera que t es un divisor común de $a+cb$ y b. Ahora bien, sea s un divisor común de $a+cb$ y b, i.e., $s \mid a+bc \ \wedge \ s \mid b$ entonces $s \mid cb$ entonces $s \mid (a+cb) - cb$ entonces $s \mid a$ así, $s \mid a$ y $s \mid b$, de manera que s es un divisor común de a y b, por consiguiente a,b y $a+cb$ tienen los mismos divisores comunes, por lo tanto $(a,b) = (a+cb, b)$.

Definición 1.7.7. Si a y b son enteros entonces una combinación lineal de a y b es una suma de la forma $ma+nb$ donde m,n son enteros.

Teorema 1.7.8. El máximo común divisor de los enteros a y b no ambos cero es el menor entero positivo que es una combinación lineal de a y b.

Demostración:
Sea $A = \{n \in \mathbb{N} : n = sa+tb \text{ para algunos } s,t \in \mathbb{Z}\} \subseteq \mathbb{N}$, supóngase que $a \neq 0$, luego $a < 0 \ \vee \ a > 0$ si $a < 0$ entonces $-a > 0$ entonces $0 < -a = (-1)a + 0b$ entonces $-a \in A$, de lo anterior, se sigue que $A \neq \emptyset$, luego $A \subseteq \mathbb{N} \ \wedge \ A \neq \emptyset$, entonces (por P.B.O.) A tiene mínimo, a saber, i.e., $d = \min A \ (d \in A)$ entonces existen $m,n \in \mathbb{Z} : d = ma+nb$.
$\vdash \ d \mid a \ \wedge \ d \mid b$ por el algoritmo de la división existe $q,r \in \mathbb{Z}$ tales que $a = qd + r$ con $0 \leq r < d$ entonces $r = a - qd = a + (-q)d = a + (-q)(ma+nb) = (1-qm)a + (-qn)b$ i.e., $r = (1-qm)a + (-qn)b$ con $1-qm, -qn \in \mathbb{Z}$, luego $r \in A$ pero $d = \min A$, de ahí que $r = 0$, así $d \mid a$. De manera similar, probamos que $d \mid b$.
Sea $c \in \mathbb{Z}$ tal que $c \mid a \ \wedge \ c \mid b$ veamos que $c \leq d$, como $d = ma+nb$ entonces $c \mid d$ entonces $c \leq |c| \leq |d| = d$ entonces $c \leq d \quad \therefore \ d = (a,b)$.

Corolario 1.7.9. Si a y b son primos relativos entonces existen enteros m y n tales que $ma+nb = 1$.

Demostración:
Como $(a,b) = 1$ entonces (por el Teorema 1.7.8.) existen $m,n \in \mathbb{Z}$ tales que $1 = ma+nb$.

Teorema 1.7.10. Si $a,b \in \mathbb{N}$ entonces el conjunto de combinaciones lineales de a y b es un conjunto de enteros múltiplos de (a,b).

Demostración:
Sean $d = (a,b)$, $a\mathbb{Z} + b\mathbb{Z} = \{s \in \mathbb{Z} : s = ma+nb \text{ para algunos } m,n \in \mathbb{Z}\}$ y $(d) = \{t \in \mathbb{Z} : \exists \ t \in \mathbb{Z} : t = kd\}$. veamos que $a\mathbb{Z} + b\mathbb{Z} = (d)$. Sea $s \in a\mathbb{Z} + b\mathbb{Z}$ entonces $s = ma+nb$ para algunos $m,n \in \mathbb{Z}$ pero $d = (a,b)$ luego $d \mid a$ y $d \mid b$ entonces $d \mid s$ entonces $\exists \ k \in \mathbb{Z} : s = kd \in (d)$ i.e., $s \in (d)$, así, $a\mathbb{Z} + b\mathbb{Z} \subseteq (d)$. Ahora bien, sea $t \in (d)$ entonces $\exists \ l \in \mathbb{Z} : t = ld$ entonces $t = l(ma+nb)$ donde $d = ma+nb$ para algunos $m,n \in \mathbb{Z}$ entonces $t = (lm)a + (ln)b \in a\mathbb{Z} + b\mathbb{Z}$, i.e., $t \in a\mathbb{Z} + b\mathbb{Z}$, así, $(d) \subseteq a\mathbb{Z} + b\mathbb{Z}$. $\quad \therefore \ (d) = a\mathbb{Z} + b\mathbb{Z}$.

Teorema 1.7.11. Si a y b son enteros no ambos cero, entonces un entero positivo d es el máximo común divisor de a y b si y solo si
i) $d \mid a$ y $d \mid b$,
ii) si $c \mid a$ y $c \mid b$ entonces $c \mid d$.

Demostración:
$\Rightarrow$] Supongamos que $d = (a, b)$ entonces $d \mid a \ \wedge \ d \mid b$, por definición del máximo común divisor de a y b. Además $d = ma + nb$ para algunos $m, n \in \mathbb{Z}$ si $c \mid a$ y $c \mid b$ entonces $c \mid ma$ y $c \mid nb$ entonces $c \mid ma + nb$ entonces $c \mid d$, así $c \mid a$ y $c \mid b$ entonces $c \mid d$ con lo cual hemos establecido *i*) y *ii*).
$\Leftarrow$] Supongamos que *i*) $d \mid a$ y $d \mid b$ *ii*) $c \mid a$ y $c \mid b$ implica $c \mid d$. Veamos que $d = (a, b)$. Por *i*) tenemos que d es un divisor común de a y b tal que $c \mid d$ entonces $c \leq |c| \leq |d| = d$, i.e., $c \leq d$, en consecuencia, cualquier otro divisor común de a y b, digamos c es menor o igual que d, $\quad \therefore \ d = (a, b)$.

Definición 1.7.12. Sean $a_1, a_2, \ldots, a_n$ enteros, no todos iguales a cero. El máximo común divisor de estos enteros es el entero positivo más grande que es un divisor de todos los enteros en el conjunto. El máximo común divisor de $a_1, a_2, \ldots, a_n$ es denotado por $(a_1, a_2, \ldots, a_n)$.

Ejemplo: Es fácil ver que $(12, 18, 30) = 6$ y que $(10, 15, 25) = 5$,

12	18	30	2
6	9	15	3
2	3	5	

así, $(2)(3) = 6$.

10	15	25	5
2	3	5	

Lema 1.7.13. Si $a_1, a_2, \ldots, a_n$ son enteros, no todos iguales a cero, entonces $(a_1, a_2, \ldots, a_n) = (a_1, a_2, \ldots a_{n-2}, (a_{n-1}, a_n))$.

Demostración:
Sea $s \mid a_i$ para cada $i \in [n] := \{1, 2, \ldots, n\}$, en particular $s \mid a_{n-1}$ y $s \mid a_n$ entonces (por el Teorema 1.7.11. inciso *ii*)) $s \mid (a_{n-1}, a_n)$, además $s \mid a_i$ para cada $i \in \{1, 2, \ldots, n-2\}$, luego $s \mid a_i$, $i \in \{1, 2, \ldots, n\}$. Por otro lado, si $t \mid a_i$, $i \in \{1, 2, \ldots, n-2\}$ y también $t \mid (a_{n-1}, a_n)$ entonces $(a_{n-1}a_n) \mid a_{n-1}$ y $(a_{n-1}, a_n) \mid a_n$ pero $t \mid (a_{n-1}, a_n)$ entonces $t \mid a_i$, $i \in \{1, 2, \ldots, n-2\}$ pero $t \mid a_{n-1} \ \wedge \ t \mid a_n$ entonces $t \mid a_i$, $i \in [n]$. Por lo tanto $(a_1, a_2, \ldots, a_{n-1}, a_n) = (a_1, a_2, \ldots, a_{n-2}, (a_{n-1}, a_n))$.

Ejemplo: Encontrar $\text{mcd}(105, 140, 350) = 6$ por el Lema 1.7.12. tenemos,
$\text{mcd}(105, 140, 350) = (105, (140, 350)) = (105, 70) = 35$,

140	350	2
70	175	5
14	35	7
2	5	

así, $(2)(5)(7) = 70$,

105	70	5
21	14	7
3	2	

así, $(5)(7) = 35$.

Definición 1.7.14. Los enteros $a_1, a_2, \ldots, a_n$ son primos mutuamente relativos si $(a_1, a_2, \ldots, a_n) = 1$. Estos enteros son llamados primos relativos por parejas si para cada par de enteros a_i y a_j con $i \neq j$ entonces $(a_i, a_j) = 1$, esto es, si cada par de enteros del conjunto son coprimos.

Lema 1.7.15. Si e y d son enteros y $e = dq + r$ donde $q, r \in \mathbb{Z}$ entonces $(e, d) = (d, r)$.

Demostración:
Sabemos que $(a + cb, b) = (a, b)$ $(*)$ como $e = dq + r$ entonces $r = e - dq = e + (-q)d$, luego usando $(*)$ $(e + (-q)d, d) = (e, d)$ pero $(e + (-q)d, d) = (r, d)$, así $(e, d) = (d, r)$.

Teorema 1.7.16. (El algoritmo Euclidiano)
Sean $r_0 = a$ y $r_1 = b$ enteros tales que $a \geq b > 0$. Si el algoritmo de la división es aplicado sucesivamente para obtener $r_j = r_{j+1}q_{j+1} + r_{j+2}$ con $0 < r_{j+2} < r_{j+1}$ para $j = 0, 1, 2, \ldots, n-2$ y $r_{n+1} = 0$ entones $(a, b) = r_n$, i.e. el máximo común divisor de a y b es el último residuo distinto de cero.

Demostración:
Sean $r_0 = a$ y $r_1 = b$ en $\mathbb{N}$ con $a \geq b$, por aplicación sucesiva del algoritmo de la división tenemos

$$\begin{aligned}
r_0 &= q_1 r_1 + r_2 \ , && 0 \leq r_2 < r_1 \\
r_1 &= q_2 r_2 + r_3 \ , && 0 \leq r_3 < r_2 \\
r_2 &= q_3 r_3 + r_4 \ , && 0 \leq r_4 < r_3 \\
&\vdots \\
r_{j-2} &= q_{j-1} r_{j-1} + r_j \ , && 0 \leq r_j < r_{j-1} \\
&\vdots \\
r_{n-3} &= q_{n-2} r_{n-2} + r_{n-1} \ , && 0 \leq r_{n-1} < r_{n-2} \\
r_{n-2} &= q_{n-1} r_{n-1} + r_n \ , && 0 \leq r_n < r_{n-1} \\
r_{n-1} &= q_n r_n + r_{n+1} \ , && \text{con } r_{n+1} = 0
\end{aligned}$$

i.e., $r_{n-1} = r_n q_n + 0$,
debido a que la sucesión de residuos $a = r_0 \geq r_1 \geq r_2 \geq \cdots \geq 0$ no puede contener más de a términos, entonces

$$\begin{aligned}
(a, b) &= (r_0, r_1) = (q_1 r_1, r_1) = (r_2, r_1) \\
&= (r_2, q_2 r_2 + r_3) = (r_2, r_3) = (q_3 r_3 + r_4, r_3) \\
&= (r_3, r_4) = \cdots = (r_{n-3}, r_{n-2}) \\
&= (r_{n-2} q_{n-2} + r_{n+1}, r_{n-2}) = (r_{n-2}, r_{n-1}) \\
&= (r_{n-1} q_{n-1} + r_n, r_{n-1}) = (r_{n-1}, r_n) \\
&= (r_n q_n + r_{n+1}, r_n) = (r_n, r_{n+1}) = (r_n, 0) = r_n,
\end{aligned}$$

Por lo tanto, $(a, b) = r_n$.

Definición 1.7.17. El mínimo común múltiplo de dos enteros distintos de cero a y b es un entero positivo M (único) tal que
i) $a \mid M$ y $b \mid M$,
ii) si $a \mid l$ y $b \mid l$ entonces $M \mid l$.

Notación: El mínimo común múltiplo de a y b se denota $\text{mcm}(a, b)$ ó $[a, b]$.

Ejemplo: $[15,21]=105$, $[24,36]=72$, $[2,20]=20$ y $[7,11]=77$

15	21	3
5	7	5
1	7	7
1	1	

así, $(3)(5)(7)=105$,

24	36	2
12	18	2
6	9	2
3	9	3
1	3	3
1	1	

así, $(2)(2)(2)(3)(3)=72$.

Una vez que las factorizaciones de a y b como potencias de primos son conocidas es fácil determinar (a,b) y $[a,b]$.

$(*)$ En efecto, si $a=p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}$ y $b=p_1^{b_1}p_n^{b_2}\cdots p_n^{b_n}$ donde $p_1,p_2,\cdots,p_n$ son los números primos distintos entre sí que aparecen en las factorizaciones de a y b como producto de potencias de primos, donde quizá tengamos que algunos $a_i=0$ ó $b_j=0$.

Entonces $(a,b)=p_1^{\text{mín}\{a_1,b_1\}}p_2^{\text{mín}\{a_2,b_2\}}\cdots p_n^{\text{mín}\{a_n,b_n\}}$,

mientras que $[a,b]=p_1^{\text{máx}\{a_1,b_1\}}p_2^{\text{máx}\{a_2,b_2\}}\cdots p_n^{\text{máx}\{a_n,b_n\}}$.

Lema 1.7.18. Si $x,y\in\mathbb{R}$, entonces $\text{máx}\{x,y\}+\text{mín}\{x,y\}=x+y$.

Demostración:

Supongamos que $x\geq y$:

$\Rightarrow$ $\text{máx}\{x,y\}+\text{mín}\{x,y\}=x+y$, ahora, si $x<y$:

$\Rightarrow$ $\text{máx}\{x,y\}+\text{mín}\{x,y\}=y+x=x+y$

$\therefore$ $\text{máx}\{x,y\}+\text{mín}\{x,y\}=x+y$.

Teorema 1.7.19. Si a y b son enteros positivos entonces $[a,b]=\frac{ab}{(a,b)}$.

Demostración:

Veamos que $[a,b]=\frac{ab}{(a,b)}$ ó equivalentemente $ab=(a,b)[a,b]$, sean $a=p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}$ y $b=p_1^{b_1}p_2^{b_2}\cdots p_n^{b_n}$ como en $(*)$ (párrafo anterior al lema 1.7.18.), tomemos a $M_i=\text{máx}\{a_i,b_i\}$ y $m_i=\text{mín}\{a_i,b_i\}$ entonces

$$\begin{aligned}(a,b)[a,b] &= p_1^{m_1}p_2^{m_2}\cdots p_n^{m_n}p_1^{M_1}p_2^{M_2}\cdots p_n^{M_n}\\ &= p_1^{m_1+M_1}p_2^{m_2+M_2}\cdots p_n^{m_n+M_n}=p_1^{a_1+b_1}p_2^{a_2+b_2}\cdots p_n^{a_n+b_n}\\ &= (p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n})\left(p_1^{b_1}p_2^{b_2}\cdots p_n^{b_n}\right)=ab\end{aligned}$$

$\therefore$ $ab=(a,b)[a,b]$.

A continuación exhibiremos una prueba de un caso especial del Teorema de Dirichlet[9] para la progresión $4n+3$.

Lema 1.7.20. Si a y b son enteros de la forma $4n+1$ entonces el producto de a y b también es de esta forma.

[9]Teorema de Dirichlet sobre los primos en progresiones aritméticas. Supóngase que a y b son enteros positivos que no son divisibles por el mismo número primo. Entonces la progresión aritmética $an+b$, $n\in\mathbb{N}$ contiene un número infinito de números primos. Ninguna prueba simple del teorema de Dirichlet sobre primos es progresiones aritméticas es conocida, por tal motivo se omite dicha prueba.

Demostración:
Sean $a = 4l+1$ y $b = 4m+1$ realizamos el producto de a y b, i.e., $ab = (4l+1)(4m+1)$ entonces $ab = (4l)(4m) + 4l + 4m + 1 = 16lm + 4(l+m) + 1$ entonces $ab = 4[4lm + (l+m)] + 1$, con $k = 4lm + (l+m)$ de tal manera que $ab = 4k+1$.

Teorema 1.7.21. Hay un número infinito de primos de la forma $4n+3$ donde $n \in \mathbb{N} \cup \{0\}$
Demostración:
Supongamos que hay sólo un número finito de primos de la forma $4n+3$ digamos que $p_0 = 3, p_1, p_2, \cdots, p_r$. Sea $Q = 4p_1p_2\cdots p_r + 3$, entonces hay al menos un primo en la factorización de Q de la forma $4n+3$. Sin embargo ninguno de los primos $p_0, p_1, \cdots, p_n$ divide a Q ya que si $p_0 = 3$ divide a Q, i.e., $3 \mid Q$ entonces $3 \mid Q - 3$ entonces $3 \mid 4p_1p_2\cdots p_r$!
Y si $p_j \mid Q$ para $j \in \{1, \ldots, r\}$, entonces $p_j \mid Q - 4p_1\cdots p_r$ entonces $p_j \mid 3$!

Teorema 1.7.22. Si n es un entero compuesto entonces n tiene un factor primo que no excede a $\sqrt{n}$.
Demostración:
Como n es compuesto podemos escribir $n = ab$ donde $1 < a \leq b < n$, luego $a \leq \sqrt{n}$, ya que de otro modo tendríamos que $b \geq a > \sqrt{n}$ entonces $ab \geq a^2 \ \wedge \ a^2 > \sqrt{n}\sqrt{n} = n$, así $n = ab \geq a^2 > n$! Entonces $a \leq \sqrt{n}$ pero existe $p-$número primo tal que $p \mid a$, por el lema 1.2.4., luego $|p| \leq |a|$ i.e., $p \leq a \leq \sqrt{n}$, por consiguiente $p-$primo es tal que $p \mid a$ y $a \mid n$, así $p \mid n$ pero $p \leq \sqrt{n}$.
Ahora procedemos a la demostración pendiente del Teorema 1.4.3. con ayuda del teorema fundamental de la aritmética.

Teorema 1.4.3. Si p es un número primo, entonces $\sqrt{p}$ es irracional.
Demostración:
(Por contradicción) Supongamos que $\sqrt{p}$ es racional, entonces $\sqrt{p} = \frac{a}{b}$ con $a, b \in \mathbb{Z}^+$, $b \neq 0 \ \wedge \ \text{mcd}(a,b) = 1$ entonces $p = \frac{a^2}{b^2}$ entonces $b^2p = a^2$ y como a y b son enteros positivos, pueden escribirse como productos de potencias de primos, i.e., $a = s_1^{a_1}s_2^{a_2}\cdots s_n^{a_n}$ y $b = t_1^{b_1}t_2^{b_2}\cdots t_m^{b_m}$, como a y b son coprimos, entonces los números primos de las factorizaciones son distintos, i.e., $s_i \neq t_j$, como $a^2 = pb^2$, el primo p es un divisor de a^2 y, por tanto, p debe estar en la factorización de a^2. Calculamos el cuadrado de a, i.e., $a^2 = (s_1^{a_1}s_2^{a_2}\cdots s_n^{a_n})^2 = s_1^{2a_1}s_2^{2a_2}\cdots s_n^{2a_n}$. Las potencias de la factorización de a^2 deben tener exponente par. Lo mismo ocurre con la factorización de b^2. Por un lado, como sabemos que p está en la factorización de a^2.
Por otro lado, el número pb^2 debe tener una factorización. Ahora bien, sabemos que este número es un cuadrado $pb^2 = a^2$, con lo que todos los exponentes deben ser pares, incluido el de p. Tenemos, pues, que la potencia de base p en la factorización de a^2 tiene, por un lado, exponente par; y, por otro, exponente impar!
$\therefore$ $\sqrt{p}$ es irracional.

Definición 1.7.23. Logaritmación es el proceso de hallar el exponente al cual fue elevada la base para obtener un número. Dado un número real x (argumento), la función logaritmo le asigna el exponente n (o potencia) a la que un número fijo b (base) se ha de elevar para obtener dicho argumento. Es la función inversa de b a la potencia n. Esta función se escribe como: $n = \log_b x$, lo que permite obtener n.

$$\log_b x = n \quad \Longleftrightarrow \quad b^n = x$$

Para que la definición sea válida, no todas las bases y números son posibles, la base b tiene que ser positiva y distinta de 1 ($b > 0 \ \wedge \ b \neq 1$), x tiene que ser un número positivo ($x > 0$) y n puede ser cualquier número real.
Propiedades:
1) $\log_b(xy) = \log_b(x) + \log_b(y)$.

2) $\log_b(x/y) = \log_b(x) - \log_b(y)$.
3) $\log_b(x^y) = y \log_b(x)$.

Se denomina logaritmo natural al logaritmo cuya base es el número e: El logaritmo natural suele denotarse por $\ln(x)$ o como $\log_e(x)$. El logaritmo natural es una función real con dominio de definición los números reales positivos: $\ln : \mathbb{R}^+ \to \mathbb{R}$ y tiene como función inversa a la función exponencial natural: $e^{\ln x} = x$ para todo $x > 0$, $\ln(e^x) = x$.
Definición 1.7.24. La función $\pi(x)$, donde x es un número real positivo denota el número de primos que no exceden a x.

Por ejemplo: $\pi(10) = 4$, $\pi(100) = 25$.

Teorema 1.7.25. El Teorema del número primo

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1 \ , \qquad \left(\text{o bien} \quad \lim_{x\to\infty} \frac{\pi(x)}{(x/\ln x)} = 1\right) \ .$$

El teorema del número primo fue conjeturado por Gauss en 1793 pero fue demostrado hasta 1896, cuando un matemático francés J. Hadamard y un matemático belga C.J. de la Vallé-Poussin dieron pruebas independientes.

No demostraremos el teorema del número primo aquí, las diversas pruebas conocidas son o muy complicadas o dependen de matemáticas avanzadas.

El teorema del número primo nos dice que $x/\ln x$ es una buena aproximación a $\pi(x)$ cuando x es grande. Se ha demostrado que una buena aproximación está dada por $\mathrm{li}(x) = \int_2^x \frac{dt}{\ln t}$[10], (donde $\int_2^x \frac{dt}{\ln t}$ representa el área bajo la curva $y = \frac{1}{\ln t}$ y por encima del eje x desde $t = 2$ a $t = x$).

Cada entero impar es de la forma $4n + 1$ o de la forma $4n + 3$. ¿Hay un número infinito de primos en cada forma? Los primos $5, 13, 17, 29, 37, 41, \ldots$ son de la forma $4n + 1$, mientras que los primos $3, 7, 11, 19, 23, 31, 43, \ldots$ son de la forma $4n + 3$. La evidencia sugiere que sí.

Proposición 1.7.26. Para cada $n \in \mathbb{N}$, hay al menos n enteros positivos compuestos consecutivos.

Demostración:
Consideremos los n enteros positivos consecutivos,
$(n + 1)! + 2, (n + 1)! + 3, \ldots, (n + 1)! + n + 1$, cuando $2 \leq j \leq n + 1$ tenemos que $j \mid (n + 1)!$ entonces $j \mid (n + 1)! + j$ para cada $j : 2 \leq j \leq n + 1$, por consiguiente, éstos n enteros consecutivos son todos compuestos.

Ejemplos:
1) Los 7 enteros compuestos consecutivos que comienzan con $8! + 2 = 40322$ son todos números compuestos:

$8! + 2 = 40322$ $\quad$ $8! + 5 = 40325$ $\quad$ $8! + 8 = 40328$
$8! + 3 = 40323$ $\quad$ $8! + 6 = 40326$
$8! + 4 = 40324$ $\quad$ $8! + 7 = 40327$

[10]El logaritmo integral, función integral de logaritmo o integral logarítmica $\mathrm{li}(x)$, es una función especial de relevancia significativa en problemas de física y teoría de números, ya que da una estimación de la cantidad de números primos menores que un determinado valor. Por ejemplo, el teorema de los números primos asegura que: $\pi(x) \sim \mathrm{li}(x)$.

Sin embargo, estos son mucho más grandes que los 7 enteros compuestos consecutivos más pequeños $90, 91, 92, 93, 94, 95$ y 96.
2) $n = 1$, $(1+1)! + 2 = 4$.
3) $n = 2$, $(2+1)! + 2 = 8$, $(2+1)! + 3 = 9$.
4) $n = 3$, $(3+1)! + 2 = 26$, $(3+1)! + 3 = 27$, $(3+1)! + 4 = 28$.
5) $n = 4$, $(4+1)! + 2 = 122$, $(4+1)! + 3 = 123$, $(4+1)! + 4 = 124$,
$(4+1)! + 5 = 125$.

La proposición exhibe que la brecha entre primos consecutivos es arbitrariamente grande.

Los únicos primos consecutivos son 2 y 3. Sin embargo muchos pares de primos difieren por dos unidades, estos pares de primos son llamados primos gemelos; por ejemplo 5 y 7, 11 y 13, 101 y 103, 4967 y 4969.

1.8. Congruencias

Definición 1.8.1. Fijemos $n \in \mathbb{N}$, $n > 1$ y sean $a, b \in \mathbb{Z}$. Decimos que a es congruente con b módulo n, lo cual denotamos por $a \equiv b \pmod{n}$ si y sólo si $n \mid a - b$ o bien existe $k \in \mathbb{Z} : a - b = kn$.

Teorema 1.8.2. Sea $m \in \mathbb{N}, m > 1$ y $n, a, b, c, d \in \mathbb{Z}$. Entonces
a) $a \equiv a \pmod{m}$ reflexiva,
b) si $a \equiv b \pmod{m}$ entonces $b \equiv a \pmod{m}$ simétrica,
c) si $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$ entonces $a \equiv c \pmod{m}$ transitiva,
d) si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$ entonces
$a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$ y $ac \equiv bd \pmod{m}$,
e) si $a \equiv b \pmod{m}$ entonces $ad \equiv bd \pmod{m}$,
f) si $a \equiv b \pmod{m}$ entonces $a^n \equiv b^n \pmod{m}$ para cada $n \in \mathbb{N} \cup \{0\}$.

Demostración:
a) Como $a - a = 0 = 0m$, i.e., $a - a = 0m$ para $0 \in \mathbb{Z}$ tenemos que $a \equiv a \pmod{m}$ para cada $a \in \mathbb{Z}$.
b) Supóngase que $a \equiv b \pmod{m}$ entonces $m \mid a - b$ entonces $m \mid (-1)(a - b)$ entonces $m \mid b - a$ entonces $b \equiv a \pmod{m}$ $\therefore$ $a \equiv b \pmod{m}$ entonces $b \equiv a \pmod{m}$.
c) Supóngase que $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m}$ entonces $m \mid a - b \wedge m \mid b - c$ entonces $m \mid (a-b)+(b-c)$ entonces $m \mid a - c$ entonces $a \equiv c \pmod{m}$ por lo tanto $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$ entonces $a \equiv c \pmod{m}$.
d) Supóngase que $a \equiv b \pmod{m} \wedge c \equiv d \pmod{m}$ entonces $m \mid a - b \wedge m \mid c - d$ entonces $m \mid (a - b) + (c - d)$ entonces $m \mid (a + c) - (b + d)$ entonces $a + c \equiv b + d \pmod{n}$ como $m \mid a - b$ y $n \mid c - d$ entonces $m \mid (a - b) + (d - c)$ entonces $m \mid (a - c) - (b - d)$ entonces $a - c \equiv b - d \pmod{m}$. Además, dado que $m \mid a - b \wedge m \mid c - d$ entonces $m \mid c(a - b) \wedge b(c - d)$ entonces $m \mid c(a - b) + b(c - d)$ entonces $m \mid ac - bd$ entonces $ac \equiv bd \pmod{m}$ $\therefore$ $a \equiv b \pmod{m} \wedge c \equiv d \pmod{m}$ entonces $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$, $ac \equiv bd \pmod{m}$.
e) Supóngase que $a \equiv b \pmod{m}$ entonces $\exists k \in \mathbb{Z} : a - b = km$ entonces $(a - b)d = (km)d = (kd)m$ entonces $ad - bd = (kd)m$ con $kd \in \mathbb{Z}$
entonces $m \mid ad - bd$, $ad \equiv bd \pmod{m}$ $\therefore$ $a \equiv b \pmod{m}$ entonces $ad \equiv bd \pmod{m}$.
f) Por inducción, iniciando en cero, por el inciso d) tenemos que si $c = 0$ y $d = 0$ entonces $a(0) \equiv b(0) \pmod{m}$ entonces $0 \equiv 0 \pmod{m}$ se cumple por el inciso a), luego si $c = a \wedge d = b$ entonces $a(a) \equiv b(b) \pmod{m}$ entonces $a^2 \equiv b^2 \pmod{m}$, esto se puede repetir indefinidamente, dando lugar a $a^n \equiv b^n \pmod{m}$.

En otras palabras, estamos diciendo que podemos sustituir la base por otra congruente con ella, pero en general el exponente no puede sustituirse.

Por los incisos a), b) y c) del teorema anterior tenemos que la relación de congruencia es una relación de equivalencia.

Definición 1.8.3. Sea $\chi \neq \emptyset$ y $\mathcal{F} \subseteq \mathcal{P}(\chi)$ donde $\mathcal{P}(\chi)$[11] es el conjunto potencia de χ. Diremos que $\mathcal{F}$ es una partición de χ si y sólo si
a) $\forall F \in \mathcal{F} : F \neq \emptyset$,
b) $\bigcup_{F \in \mathcal{F}} F = \chi$,
c) $\forall F_1, F_2 \in \mathcal{F} : F_1 \neq F_2 \Rightarrow F_1 \cap F_2 = \emptyset$.

Definición 1.8.4. Sea R una relación de equivalencia de χ y sea $a \in \chi$ se llama clase de equivalencia de a, lo cual se denota por $\bar{a}$ o bien $[a]$ al conjunto $\{x \in \chi | xRa\}$, i.e., $[a] = \{x \in \chi | xRa\}$. A los elementos de la clase de equivalencia de a se les llama representantes de la clase a.

Definición 1.8.5. Sea R una relación de equivalencia de χ. Al conjunto formado por las clases de equivalencia que definen R en χ, denotado por χ/R se le denomina conjunto cociente.

Sea $n \in \mathbb{N}, n > 1$ y considérese la relación de congruencia módulo n denotamos al conjunto cociente de $\mathbb{Z}$ respecto de la relación de congruencia módulo n como $\mathbb{Z}/\equiv_n$.

Veamos que $\mathbb{Z}/\equiv_n = \{[0], [1], \ldots, [n-1]\}$. Sea $a \in \mathbb{Z}$, dividamos a a por n, por el algoritmo de la división existen $q, r \in \mathbb{Z}$ tales que $a = qn + r$ con $0 \leq r < n$ entonces $a - r = qn$ entonces $n \mid a - r$ entonces $a \equiv r \pmod{n}$ entonces $[a] = [r]$ con $0 \leq r < n$. Por consiguiente, hay a lo más n clases de equivalencia, a saber $[0], [1], \ldots, [n-1]$. Pero estas son distintas, puesto que si $[i] = [j]$ con $0 \leq i < j < n$, entonces $j \in [j] = [i]$, luego $j \in [i]$, de ahí se sigue que $j \equiv i \pmod{n}$, así $n \mid j - i$ con $0 < j - i < n$, lo cual no puede suceder. Por lo tanto hay exactamente n clases de equivalencia distintas $[0], [1], \ldots, [n-1] \quad \therefore \mathbb{Z}/\equiv_n = \{[0], [1], \ldots, [n-1]\}$.

Considérese ahora la relación de congruencia módulo n, si $x \equiv a \pmod{n} \Leftrightarrow n \mid x - a \Leftrightarrow \exists k \in \mathbb{Z} : x - a = kn \Leftrightarrow a = (-kn) + x \Leftrightarrow a = qn + x$ donde $q = -k \in \mathbb{Z} \Leftrightarrow x$ es el residuo de la división de a por n.

Más aún, $x \equiv a \pmod{n} \Leftrightarrow x = a + kn \in a + n\mathbb{Z}$ donde $n\mathbb{Z} = \{kn | k \in \mathbb{Z}\}$, i.e., $x \equiv a \pmod{n} \Leftrightarrow x \in a + n\mathbb{Z}$.

Definición 1.8.6. Un sistema completo de residuos módulo n es un conjunto de enteros tales que todo entero es congruente módulo n a exactamente un entero del conjunto.

El conjunto de enteros $0, 1, 2, \ldots, n-1$ es un sistema completo de residuos módulo n. Este es llamado el conjunto más pequeño de residuos no negativos módulo n.

Problema: Encontrar un número que tiene residuo 1 cuando es dividido por 3, residuo 2 cuando es dividido por 5 y residuo 3 cuando es dividido por 7. Este problema se modela de la siguiente manera:

$x \equiv 1 \pmod{3}, \quad x \equiv 2 \pmod{5}, \quad x \equiv 3 \pmod{7}$.

[11] Un conjunto potencia es el conjunto de todos los subconjuntos de un conjunto.

Teorema 1.8.7. (El Teorema chino del residuo)
Sean $m_1, m_2, \ldots, m_r$ enteros positivos coprimos por parejas. Entonces el sistema de congruencias

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

tiene una única solución módulo $M = m_1 m_2 \cdots m_r$.

Demostración:
Primero construimos una solución simultánea al sistema de congruencias

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r}. \end{aligned}$$

Sea $M_k = \frac{M}{m_k}$ donde $M = m_1 m_2 \cdots m_r$, $M_k = m_1 m_2 \cdots m_{k-1} m_{k+1} \cdots m_k$, $k \in [r]$, tenemos que $(M_k, m_k) = 1$ ya que $(m_j, m_k) = 1$ siempre que $j \neq k$. Considérense las congruencias lineales $M_k x \equiv 1 \pmod{m_k}$, $k \in [r]$, luego, tenemos que existe y_k (el inverso de M_k) módulo m_k, de tal forma que $M_k y_k \equiv 1 \pmod{m_k}$, $k \in [r]$. Sea $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_r M_r y_r$. Veamos que el entero x es una solución de las r congruencias, por demostrar que $x \equiv a_k \pmod{m_k}$, $k \in [r]$. Como $m_k \mid M_j$ siempre que $k \neq j$ tenemos que $M_j \equiv 0 \pmod{m_k}$, $k \in [r] - \{j\}$ entonces $a_j M_j y_j \equiv 0 \pmod{m_k}$ entonces $\sum_{j=1}^{r} a_j M_j y_j \equiv 0 \pmod{m_k}$ entonces $x - a_k M_k y_k \equiv 0 \pmod{m_k}$ entonces $x \equiv a_k M_k y_k \pmod{m_k}$ pero $M_k y_k \equiv 1 \pmod{m_k}$ luego, entonces tenemos $a_k M_k y_k \equiv a_k \pmod{m_k}$ entonces $x \equiv a_k \pmod{m_k}$, $k \in [r]$. Ahora mostraremos que cualesquiera dos soluciones congruentes módulo M. Sean x_0 y x_1 soluciones simultáneas para el sistema de r congruencias, i.e., $x_0 \equiv a_k \pmod{m_k}$ y $x_1 \equiv a_k \pmod{m_k}$, $k \in [r]$, de ahí tenemos que $x_0 \equiv x_1 \pmod{m_k}$, $k \in [r]$, luego entonces, $x_0 \equiv x_1 \pmod{[m_1, m_2, \ldots, m_k]}$ pero $[m_1, m_2, \ldots, m_k] = m_1 m_2 \cdots m_k = M$, con lo cual $x_0 \equiv x_1 \pmod{M}$. Por lo tanto, la solución simultánea del sistema de r congruencias es única módulo M.

Lema 1.8.8. Sea p un número primo. Entonces $x^2 \equiv 1 \pmod{p}$ si y sólo si $x \equiv \pm 1 \pmod{p}$.

Demostración:
$\Rightarrow$] Supóngase que $x_0^2 \equiv 1 \pmod{p}$ entonces $p \mid x_0^2 - 1$ entonces $p \mid (x_0 - 1)(x_0 + 1)$ entonces $p \mid (x_0 - 1)$ ó $p \mid (x_0 + 1)$ entonces $x_0 \equiv 1 \pmod{p}$ ó $x_0 \equiv -1 \pmod{p}$.
$\Leftarrow$] Si $x \equiv 1 \pmod{p}$ entonces $x \cdot x \equiv 1 \cdot 1 \pmod{p}$ luego, entonces $x^2 \equiv 1 \pmod{p}$ si $x \equiv -1 \pmod{p}$ entonces $x \cdot x \equiv (-1)(-1) \pmod{p}$ entonces $x^2 \equiv 1 \pmod{p}$.

Teorema 1.8.9. (Teorema de Wilson)
Si p es primo, entonces $(p-1)! \equiv -1 \pmod{p}$.

Demostración:
Si $p = 2$ ó $p = 3$ el resultado se sigue de manera inmediata pues, efectivamente se tiene que $(2-1)! \equiv -1 \pmod{2}$ y $(3-1)! \equiv -1 \pmod{3}$. Así podemos suponer que $p \geq 5$, además supóngase que a es tal que $1 \leq a \leq p-1$, luego $(a, p) = 1$ de ahí que existen $x, y \in \mathbb{Z} : 1 = ax + py$ luego $1 - ax = py$, así $p \mid 1 - ax$, de ahí que $p \mid ax - 1$, en consecuencia $ax \equiv 1 \pmod{p}$, más aún, existe un único a' tal que $1 \leq a' \leq p-1$ y $aa' \equiv 1 \pmod{p}$. Así el par a y a' contribuyen a formar el producto en $(p-1)!$ y $aa' \equiv 1 \pmod{p}$. Pero si $a = a'$, entonces $a^2 = 1 \pmod{p}$ entonces $a \equiv \pm 1 \pmod{p}$ y dado que $p - 1 \equiv -1 \pmod{p}$, tenemos que $a \equiv p - 1 \pmod{p}$, que $a = 1$, es inmediato.

Sea $a : 2 \leq a \leq p-2$ entonces tenemos

$$\prod_{a=2}^{p-2} a \equiv 1 \pmod{p} \quad \text{y como} \quad 1 \equiv 1 \pmod{p} \ \text{y} \ (p-1) \equiv -1 \pmod{p}$$

$$\text{entonces} \quad 1 \cdot \prod_{a=2}^{p-2} a \cdot (p-1) \equiv 1 \cdot 1 \cdot (-1) \pmod{p}$$

$$\text{entonces} \quad (p-1)! \equiv -1 \pmod{p}.$$

Teorema 1.8.10. (El pequeño Teorema de Fermat)
Si p es un número primo y a es un entero positivo tal que $(p,a) = 1$ entonces $a^{p-1} \equiv 1 \pmod{p}$.
Demostración:
Primero vamos a demostrar que $\forall a \in \mathbb{N} : a^p \equiv a \pmod{p}$.
Para esto necesitamos exhibir que $p \mid \binom{p}{k}$ para cada $1 \leq k \leq p-1$, como

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)!}{k(k-1)!(p-k)!} =$$

$$= \frac{p}{k} \cdot \frac{(p-1)!}{(k-1)!((p-1)-(k-1))!} = \frac{p}{k}\binom{p-1}{k-1}$$

$$\text{entonces} \quad \binom{p}{k} = \frac{p}{k}\binom{p-1}{k-1} \quad \text{entonces} \quad k\binom{p}{k} = p\binom{p-1}{k-1} \quad \text{entonces} \quad p \mid k\binom{p}{k}$$

pero $(p,k) = 1$ entonces $p \mid \binom{p}{k}$ para cada $1 \leq k \leq p-1$; si $a = 1$, tenemos que $a^p = 1^p = 1 = a$ entonces $a^p = a$ entonces $a^p - a = 0$ entonces $p \mid 0$ i. e., $p \mid a^p - a$ luego $a^p \equiv a \pmod{p}$ siempre que $a = 1$.
Supongamos que $a^p \equiv a \pmod{p}$, veamos que $(a+1)^p \equiv a+1 \pmod{p}$ como

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k \cdot 1^{p-k} = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k + 1^p$$

dado que $p \mid \binom{p}{k}$ para cada $1 \leq k \leq p-1$ entonces $\binom{p}{k} \equiv 0 \pmod{p}$ para cada $1 \leq k \leq p-1$

$$\text{entonces} \quad \binom{p}{k} a^k \equiv 0 \pmod{p}, \quad k \in [p-1] \quad \text{entonces} \quad \sum_{k=1}^{p-1} \binom{p}{k} a^k \equiv 0 \pmod{p}$$

$$\text{entonces} \quad a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k \equiv a \pmod{p} \quad \text{pero} \quad 1 \equiv 1 \pmod{p}$$

$$\text{entonces} \quad a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k + 1 \equiv a+1 \pmod{p} \quad \text{entonces} \quad (a+1)^p \equiv a+1 \pmod{p},$$

lo cual queríamos demostrar. Por lo tanto $\forall a \in \mathbb{N} : a^p \equiv a \pmod{p}$, además $a^{p-1}a \equiv a \pmod{p}$ pero $(a,p) = 1$ entonces $a^{p-1} \equiv 1 \pmod{\frac{p}{(a,p)}}$ entonces $a^{p-1} \equiv 1 \pmod{p}$ para cada $a \in \mathbb{N}$.

Pero observese que $a^p \equiv a \pmod{p}$ se cumple para toda $a \in \mathbb{Z}$, ya que si $a = 0$, $a^p - a = 0^p - 0 = 0p$ luego $p \mid a^p - a$, así $a^p \equiv a \pmod{p}$ siempre que $a = 0$.
Ahora si $a \in \mathbb{Z}^-$ entonces $b = -a \in \mathbb{N}$ entonces $b^p \equiv b \pmod{p}$ entonces $(-a)^p \equiv -a \pmod{p}$ $(*)$, ahora si $p = 2$, $(-a)^2 \equiv -a \pmod{2}$ i.e., $a^2 \equiv -a \pmod{2}$ pero tenemos que $-a-a = -2a = (-a)2$ entonces $2 \mid -a-a$ entonces $-a \equiv a \pmod{2}$ entonces $a^2 \equiv a \pmod{2}$.
Si p es un primo impar, tenemos que $-a^p \equiv -a \pmod{p}$ lo cual se sigue de $(*)$ y de que p es un primo impar, entonces $a^p \equiv a \pmod{p}$ para cada $a \in \mathbb{Z}^-$. Así $\forall a \in \mathbb{Z} : a^p \equiv a \pmod{p}$.

1.9. Funciones multiplicativas

Definición 1.9.1. Una función aritmética es una función que está definida para todos los enteros positivos.

Definición 1.9.2. Una función aritmética f es llamada multiplicativa si $f(nm) = f(n)f(m)$ siempre que $m, n \in \mathbb{N}$, y $m \wedge n$ son coprimos. Es llamada completamente multiplicativa si $f(mn) = f(m)f(n)$ para cada $m, n \in \mathbb{N}$.

Ejemplos:
1) La función $f(n) = 1$, para cada $n \in \mathbb{N}$ es completamente multiplicativa, en efecto, si $m, n \in \mathbb{N}$, tenemos que $f(mn) = 1 = 1 \cdot 1 = f(m)f(n)$, i.e., $f(mn) = f(m)f(n)$, para cada $m, n \in \mathbb{N}$.
2) La función $g(n) = n$, para cada $n \in \mathbb{N}$ es completamente multiplicativa, en efecto, si $m, n \in \mathbb{N}$, tenemos que $g(mn) = mn$, i.e., $g(mn) = g(m)g(n)$ para cada $m, n \in \mathbb{N}$.

$$\text{Completamente multiplicativa} \implies \text{multiplicatica}$$

Teorema 1.9.3. Si f es una función multiplicativa y $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$ es la factorización del entero positivo n producto de potencias de primos, entonces $f(n) = f(p_1^{a_1}) f(p_2^{a_2}) \cdots f(p_s^{a_s})$.

Demostración:
(Por inducción sobre el número de primos diferentes que aparecen en la factorización de n como producto de potencias de primos.) Si $n = p_1^{a_1}$, es decir, si n tiene un primo en su factorización de producto de potencias de primo, el resultado se sigue de manera inmediata, puesto que $f(n) = f(p_1^{a_1})$.
Supongamos que el resultado es cierto para todos los enteros positivos con k diferentes primos en su factorización de potencias de primos.
Ahora supongamos que $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} p_{k+1}^{a_{k+1}}$ como

$$(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, p_{k+1}^{a_{k+1}}) = 1 \text{ entonces } f(n) = f((p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}) p_{k+1}^{a_{k+1}}) =$$

$$= f(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}) f(p_{k+1}^{a_{k+1}}) = f(p_1^{a_1}) f(p_2^{a_2}) \cdots f(p_k^{a_k}) f(p_{k+1}^{a_{k+1}})$$

esto se cumple por hipótesis inductiva. i.e.,

$$f(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} p_{k+1}^{a_{k+1}}) = f(p_1^{a_1}) f(p_2^{a_2}) \cdots f(p_k^{a_k}) f(p_{k+1}^{a_{k+1}}).$$

Definición 1.9.4. Sea n un entero positivo. La función φ de Euler, $\varphi(n)$ está definida como el número de enteros positivos menores o iguales que n, i.e., $\varphi(n) = |\{i \in [n] : (i, n) = 1\}|$. Observese la siguiente tabla:

n	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

Teorema 1.9.5. Si p es un número primo entonces $\varphi(p) = p - 1$. Recíprocamente si p es un entero positivo tal que $\varphi(p) = p - 1$, entonces p es primo.

Demostración:
$\Rightarrow$] Supongamos que p es un número primo y sea $1 \leq m \leq p - 1 < p$, entonces $(m, p) = 1$, para cada $1 \leq m \leq p - 1$, por consiguiente, $\varphi(p) = p - 1$.
$\Leftarrow$] Supongamos que p no es primo. Si p no es primo entonces $p = 1$ o p es un número compuesto. Caso 1) Si $p = 1$, entonces $\varphi(p) \neq p - 1$ ya que $\varphi(1) = 1 \neq 0 = 1 - 1$, i.e., $\varphi(p) \neq p - 1$. Caso 2) p es un número compuesto. Como p es un número compuesto existe $d \in \mathbb{Z}$ tal que $d > 1$ y $d < p$ tal que $d \mid p$, por supuesto d y p no son coprimos. Dado que sabemos

que al menos uno de los $p-1$ enteros $1,2,\ldots,p-1$, a saber d no es coprimo con p tenemos que $\varphi(p) \leq p-2$, así, $\varphi(p) \neq p-1$. Luego hemos demostrado que si $\varphi(p) = p-1$ entonces p es primo (por contra-recíproca).

Teorema 1.9.6. Sea p un primo y $a \in \mathbb{N}$ entonces $\varphi(p^a) = p^a - p^{a-1}$.

Demostración:
Como $\varphi(p^a)$ es el número de enteros m tales que $1 \leq m \leq p^a$ y $(m, p^a) = 1$, hay p^a enteros entre 1 y p^a, a saber:

1	2	.....	p
$p+1$	$p+2$	.....	$2p$
.....	.....	.....	.....
$(p-2)p+1$	$(p-2)p+2$	.....	$(p-2)p+p = p^2-p = p(p-1)$
$(p-1)p+1$	$(p-1)p+2$	.....	$(p-1)p+p = p^2$
p^2+1	p^2+2	.....	$p^2+p = p(p+1)$
$p(p+1)$	$p(p+1)+2$	.....	$p(p+1)+p = p^2+2p = p(p+2)$
.....	.....	.....	.....
			p^3
.....	.....	.....	.....
			$p^a = pp^{a-1}$

para determinar $\varphi(p^a)$ debemos considerar a todos los elementos del conjunto dado excepto a $p, 2p, 3p, \ldots, p(p-1), pp, p(p+1), \ldots, pp^2, \ldots, pp^{a-1}$, luego $\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1)$ o bien $\varphi(p^a) = p^a\left(1-\frac{1}{p}\right)$, siempre que p es primo y $a \in \mathbb{N}$.

Ejemplo: Determinar $\varphi(5^3)$, $\varphi(2^{10})$, $\varphi(11^2)$. Solución:
$\varphi(5^3) = 5^3 - 5^2 = 125 - 25 = 100$, i.e., $\varphi(5^3) = 100$,
$\varphi(2^{10}) = 2^{10} - 2^9 = 1024 - 512 = 512$, i.e., $\varphi(2^{10}) = 512$,
$\varphi(11^2) = 11^2 - 11 = 121 - 11 = 110$, i.e., $\varphi(11^2) = 110$.

Para encontrar una fórmula para $\varphi(n)$ dada la factorización prima de n es suficiente exhibir que φ es multiplicativa.

Teorema 1.9.7. Sea $n = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$ factorizado como potencias de primos, entonces $\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$.

Demostración:
Como φ es multiplicativa y $n = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$, luego
$\Rightarrow \quad \varphi(n) = \varphi(p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}) = \varphi(p_1^{a_1})\varphi(p_2^{a_2})\cdots\varphi(p_k^{a_k})$
$\Rightarrow \quad \varphi(n) = (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1})\cdots(p_k^{a_k} - p_k^{a_k-1})$
$\Rightarrow \quad \varphi(n) = p_1^{a_1}\left(1-\frac{1}{p_1}\right)p_2^{a_2}\left(1-\frac{1}{p_2}\right)\cdots p_k^{a_k}\left(1-\frac{1}{p_k}\right)$
$\Rightarrow \quad \varphi(n) = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$
$\Rightarrow \quad \varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$.

Ejemplo: Calcular $\varphi(100)$ y $\varphi(720)$. Solución:
Como $100 = 2^2\cdot 5^2$ y $720 = 2^4\cdot 3^2\cdot 5$, entonces
$\varphi(100) = \varphi(2^2\cdot 5^2) = \varphi(2^2)\varphi(5^2) = 2\cdot 20 = 40$, por otro lado
$\varphi(100) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 100\left(\frac{1}{2}\right)\left(\frac{4}{5}\right) = 50\left(\frac{4}{5}\right) = 10\cdot 4 = 40$.
$720 = 2^4\cdot 3^2\cdot 5$ entonces $\varphi(720) = \varphi(2^4\cdot 3^2\cdot 5) = \varphi(2^4)\varphi(3^2)\varphi(5) = 192$.

Definición 1.9.8. La función de Möbius, $\mu(n)$ está definida como:

$$\mu(n) = \begin{cases} 1 & \text{si} \quad n = 1, \\ (-1)^r & \text{si} \quad n = p_1 p_2 \cdots p_r, \\ 0 & \text{de otro modo.} \end{cases}$$

donde los p_i son los primos distintos, $i \in [r]$.

Definición 1.9.9. Un entero libre de cuadrados es un entero que no es divisible por cualquier cuadrado perfecto distinto de 1.

Los únicos valores de n para los cuales $\mu(n)$ es distinto de cero son aquéllos n que son libres de cuadrados.

Teorema 1.9.10. La función $\mu(n)$ es multiplicativa y

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si} \quad n = 1, \\ 0 & \text{si} \quad n > 1. \end{cases}$$

Demostración:
Veamos que $\mu(mn) = \mu(m)\mu(n)$ siempre que $(m,n) = 1$, si $m = 1$, $(m,n) = 1$ entonces $\mu(mn) = \mu(1 \cdot n) = \mu(n) = 1 \cdot \mu(n) = \mu(1)\mu(n) = \mu(m)\mu(n)$, i.e., $\mu(mn) = \mu(m)\mu(n)$, siempre que $m = 1$, si $n = 1$, $(m,n) = 1$, de manera análoga se exhibe que $\mu(mn) = \mu(m)\mu(n)$ siempre que $n = 1$.
Sean $m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ y $n = q_1^{f_1} q_2^{f_2} \cdots q_s^{f_s}$ con $(m,n) = 1$, de ahí tenemos que $p_i \neq q_j \ \forall i, j$, $i \in [r], j \in [s]$.

Caso 1. Algún $e_1 \geq 2$ y todo $f_j < 2$ (i.e., $f_j = 1$). Entonces $\mu(m) = 0$ y $\mu(n) = (-1)^s$, pero $\mu(mn) = \mu(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} q_1 q_2 \cdots q_s) = 0$ ya que $p_i^2 \mid mn$, puesto que $e_i \geq 2$, es el exponente del primo p_i.
Entonces $\mu(mn) = 0 = 0(-1)^s = \mu(m)\mu(n)$, i.e., $\mu(mn) = \mu(m)\mu(n)$.

Caso 2. Algún $f_j \geq 2$ y todo $e_1 < 2$ (i.e., $e_i = 1$), la prueba es análoga, así $\mu(mn) = \mu(m)\mu(n)$.

Caso 3. $\exists e_i \geq 2$ y $\exists f_j \geq 2$, luego $\mu(m) = 0 = \mu(n)$ y además $\mu(mn) = 0$ entonces $\mu(mn) = \mu(m)\mu(n)$.

Caso 4. Todos los $e_i = 1$, $f_j = 1$, luego $\mu(m) = (-1)^r$, $\mu(n) = (-1)^s$ y $\mu(mn) = \mu(p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s) = (-1)^{r+s}$ entonces $\mu(mn) = (-1)^{r+s}$ entonces $\mu(mn) = (-1)^r(-1)^s = \mu(m)\mu(n)$, así $\mu(mn) = \mu(m)\mu(n)$. Por lo tanto μ es multiplicativa.

Teorema 1.9.11. Si $F(n) = \sum_{d|n} f(d)$ para cada $n \in \mathbb{N}$, entonces

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

Demostración:

$$\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \left(\mu(d) \sum_{\delta | \left(\frac{n}{d}\right)} f(\delta) \right) = \sum_{d|n} \left(\sum_{\delta | \left(\frac{n}{d}\right)} \mu(d) f(\delta) \right) ,$$

observese que los pares de enteros (d,δ) con $d \mid n$ y $\delta \mid \frac{n}{d}$ son los mismos que aquéllos que satisfacen $\delta \mid n$ y $d \mid \frac{n}{\delta}$, en efecto, como $d \mid n$ y $\delta \mid \frac{n}{d}$ entonces existen $m, n \in \mathbb{Z} : n = md$ y $\frac{n}{d} = k\delta$ entonces $n = k\delta d$ y $\frac{n}{\delta} = kd$, i.e., $n = (kd)\delta$ y $\frac{n}{\delta} = kd$ entonces $\delta \mid n$ y $d \mid \frac{n}{\delta}$, y viceversa. Luego, entonces

$$\sum_{d|n}\left(\sum_{\delta|\frac{n}{d}}\mu(d)f(\delta)\right) = \sum_{\delta|n}\left(\sum_{d|\frac{n}{\delta}}\mu(d)f(\delta)\right) = \sum_{\delta|n} f(\delta)\sum_{d|\frac{n}{\delta}}\mu(d),$$

$$\text{pero} \quad \sum_{d|\frac{n}{\delta}}\mu(d) = \begin{cases} 0 & \text{si} \quad \frac{n}{\delta} \neq 1, \\ 1 & \text{si} \quad \frac{n}{\delta} = 1. \end{cases} \qquad \text{Así,}$$

$$\sum_{d|n}\mu(d)F\left(\frac{n}{d}\right) = \sum_{\delta|n}\left(f(\delta)\sum_{d|\frac{n}{\delta}}\mu(d)\right) = f(n)\cdot 1,$$

$$\text{de ahí que} \quad \sum_{d|n}\mu(d)F\left(\frac{n}{d}\right) = f(n).$$

Observación: Versión multiplicativa de la fórmula de inversión de Möbius

$$\text{Si} \quad F(n) = \prod_{d|n} f(d) \quad \text{entonces} \quad f(n) = \prod_{d|n}\left[F\left(\frac{n}{d}\right)\right]^{\mu(d)}.$$

Teorema de Euler

Definición 1.9.12. Un sistema reducido de residuos módulo n es un conjunto de $\varphi(n)$ enteros tales que cada elemento del conjunto es primo relativo a n y ningún par de elementos diferentes del conjunto son congruentes módulo n.

Ejemplo:
El conjunto $1,3,5,7$ es un sistema reducido de residuos mód 8. El conjunto $-3,-1,1,3$ también es un sistema reducido de residuos mód 8.

Definición 1.9.13. (Teorema de Euler)
Si $m \in \mathbb{N}$ y $a \in \mathbb{Z}$ donde $(a,m) = 1$ entonces $a^{\varphi(m)} \equiv 1 \pmod{m}$.
Demostración:
Sea $r_1, r_2, \ldots, r_{\varphi(m)}$ un sistema reducido de residuos módulo m de enteros positivos que no exceden a m, sabemos que $(r_j, m) = 1$, $j \in [\varphi(m)]$, luego $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ es un sistema reducido de residuos módulo m puesto que $(a,m) = 1$. Por consiguiente, cada elemento del sistema reducido de residuos módulo m $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ es congruente a algunos de los elementos $r_1, r_2, \ldots, r_{\varphi(m)}$ en consecuencia, si multiplicamos todos los términos en cada uno de estos sistema reducido de residuos obtenemos:
$(ar_1)(ar_2)\cdots(ar_{\varphi(m)}) \equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod{m}$, entonces $a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)} \equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod{m}$ entonces $a^{\varphi(m)} \equiv 1 \pmod{m}$ ya que $(r_1 r_2 \cdots r_{\varphi(m)}, m) = 1$ debido a que $(r_j, m) = 1$, $j \in [\varphi(m)]$ por lo tanto si $m \in \mathbb{N}$, $a \in \mathbb{Z}$ con $(a,m) = 1$ entonces $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Definición 1.9.14. Si $n > 0$ es un entero dado y g es coprimo con n, diremos que g es una raíz primitiva módulo n si $\mathrm{ord}_n(g) = \varphi(g)$ (el valor máximo que puede alcanzar el orden de g, por el teorema de Euler). Donde dado un número entero a y un entero positivo n coprimo con a (i.e., tal que $(a,n) = 1$), el orden multiplicativo de a módulo n es el menor entero positivo k que cumple: $a^k \equiv 1 \pmod{n}$. El orden de $a \pmod{n}$ se suele denotar $\mathrm{ord}_n a$, o bien $O_n(a)$.

Índice Aritmético

Sea r una raíz primitiva módulo el entero positivo m, sabemos que el sistema $r, r^1, \ldots, r^{\varphi(m)}$ forman un sistema reducido de residuos módulo m. A partir de este hecho, tenemos que si $(a, m) = 1$ entonces hay un número x con $1 \leq x \leq \varphi(m)$ tal que $r^x \equiv a \pmod{m}$.

Definición 1.9.15. Sea m un entero positivo ($m = 2$ ó $m = 4$ o bien $m = p^t$ ó $m = 2p^t$, donde p es un primo impar y $t \in \mathbb{N}$) con raíz primitiva r. Si a es un entero positivo con $(a, m) = 1$ entonces el único entero x con $1 \leq x \leq \varphi(m)$ y $r^x \equiv a \pmod{m}$ es llamado el índice (ó logaritmo discreto) de a en la base r módulo m y denotado por $\operatorname{ind}_r a$.

Observación: 1) Con esta definición tenemos que $r^{\operatorname{ind}_r a} \equiv a \pmod{m}$.
2) Si $a \equiv b \pmod{m}$, entonces $\operatorname{ind}_r a = \operatorname{ind}_r b$, en efecto ya que tenemos $r^{\operatorname{ind}_r a} \equiv a \pmod{m}$ y $r^{\operatorname{ind}_r b} \equiv b \pmod{m}$ entonces $r^{\operatorname{ind}_r a} \equiv r^{\operatorname{ind}_r b} \pmod{m}$ entonces $\operatorname{ind}_r a \equiv \operatorname{ind}_r b \pmod{\operatorname{ord}_m r}$ entonces $\operatorname{ind}_r a \equiv \operatorname{ind}_r b \pmod{\varphi(m)}$ entonces $\varphi(m) \mid \operatorname{ind}_r a - \operatorname{ind}_r b$ entonces $\operatorname{ind}_r a - \operatorname{ind}_r b = 0$ entonces $\operatorname{ind}_r a = \operatorname{ind}_r b$.

Teorema 1.9.16. Sea $m \in \mathbb{N}$ con raíz primitiva r y sean a, b enteros coprimos con m, entonces
a) $\operatorname{ind}_r 1 \equiv 0 \pmod{\varphi(m)}$,
b) $\operatorname{ind}_r(ab) \equiv \operatorname{ind}_r a + \operatorname{ind}_r b \pmod{\varphi(m)}$,
c) $\operatorname{ind}_r a^k \equiv k \operatorname{ind}_r a \pmod{\varphi(m)}$, siempre que $k \in \mathbb{N}$.
Demostración:
a) A partir del teorema de Euler $r^{\varphi(m)} \equiv 1 \pmod{m}$ (ya que $(r, m) = 1$). Dado que r es una raíz primitiva módulo m, ninguna potencia positiva de r más pequeña es congruente a 1 módulo m, por consiguiente tenemos que, $\operatorname{ind}_r 1 = \varphi(m) \equiv 0 \pmod{\varphi(m)}$ i.e., $\operatorname{ind}_r 1 \equiv 0 \pmod{\varphi(m)}$.
b) De la definición de índice tenemos que $r^{\operatorname{ind}_r(ab)} = ab \pmod{m}$ $(*)$, observese que como $(a, m) = 1$, $(b, m) = 1$ entonces $(ab, m) = 1$. Y también tenemos que $r^{\operatorname{ind}_r a + \operatorname{ind}_r b} = r^{\operatorname{ind}_r a}\, r^{\operatorname{ind}_r b}$ pero $r^{\operatorname{ind}_r a} \equiv a \pmod{m}$ y $r^{\operatorname{ind}_r b} \equiv b \pmod{m}$ entonces $r^{\operatorname{ind}_r a}\, r^{\operatorname{ind}_r b} \equiv ab \pmod{m}$ entonces $r^{\operatorname{ind}_r a + \operatorname{ind}_r b} \equiv ab \pmod{m}$ $(**)$, ahora por $(*)$ y $(**)$, tenemos que $r^{\operatorname{ind}_r(ab)} \equiv r^{\operatorname{ind}_r a + \operatorname{ind}_r b}$, en consecuencia tenemos $\operatorname{ind}_r(ab) \equiv \operatorname{ind}_r a + \operatorname{ind}_r b \pmod{\operatorname{ord}_m r}$, finalmente podemos concluir que $\operatorname{ind}_r(ab) \equiv \operatorname{ind}_r a + \operatorname{ind}_r b \pmod{\varphi(m)}$.
c) Por definición tenemos que $r^{\operatorname{ind}_r a^k} \equiv a^k \pmod{m}$ y también $r^{\operatorname{ind}_r a} \equiv a \pmod{m}$ pero $r^{k \operatorname{ind}_r a} = (r^{\operatorname{ind}_r a})^k$ entonces $(r^{\operatorname{ind}_r a})^k \equiv a^k \pmod{m}$, de esta forma, i.e., $r^{k \operatorname{ind}_r a} \equiv a^k \pmod{m}$, de ahí que, $r^{\operatorname{ind}_r a^k} \equiv a^k \pmod{m}$ y también $a^k \equiv r^{k \operatorname{ind}_r a} \pmod{m}$ por consiguiente, tenemos que $r^{\operatorname{ind}_r a^k} \equiv r^{k \operatorname{ind}_r a} \pmod{m}$. Por lo tanto $\operatorname{ind}_r a^k \equiv k \operatorname{ind}_r a \pmod{\varphi(m)}$.

1.10. Sucesiones y series

En nuestro camino al encuentro con la hipótesis de Riemann es necesario el estudio de las sucesiones y las series.

Si a cada entero positivo n está asociado un número real a_n entonces se dice que el conjunto ordenado $a_1, a_2, a_3, \ldots, a_n, \ldots$ define una sucesión infinita. Cada término de la sucesión tiene asignado un entero positivo, de manera que se puede hablar del primer término a_1, del segundo término a_2 y en general del término n-simo a_n. Cada término a_n tiene un siguiente a_{n+1} y por tanto no hay un "último" término.

Definición 1.10.1. Una función f cuyo dominio es el conjunto de todos los enteros positivos $n = 1, 2, 3, \ldots$ se denomina sucesión infinita. El valor $f(n)$ de la función se denomina el término n-esimo de la sucesión.

Por brevedad se utiliza la notación $\{f(n)\}$ para indicar la sucesión cuyo n-esimo término es $f(n)$.

Definición 1.10.2. Una sucesión $\{f(n)\}$ tiene límite L si, para cada número positivo ϵ, existe otro número positivo N (que en general depende de ϵ) tal que $|f(n) - L| < \epsilon$ para todo $n \geq N$. En este caso, decimos que la sucesión $\{f(n)\}$ converge hacia L y escribimos: $\lim_{n\to\infty} f(n) = L$ o $f(n) \to L$ o $n \to \infty$. Una sucesión que no converge se llama divergente.

Cuando nos referimos a "sucesión convergente" se emplea sólo para sucesiones cuyo límite es finito. Sucesiones con límite $+\infty$ o $-\infty$ se dice que son divergentes. Las reglas básicas para límites de sumas, productos, etc., son también válidas para límites de sucesiones convergentes.

Una sucesión $\{f(n)\}$ se dice que es creciente si $f(n) \leq f(n+1)$ para todo $n \geq 1$. Por otra parte, si se tiene $f(n) \geq f(n+1)$ para todo $n \geq 1$, se dice que la sucesión es decreciente. Una sucesión se llama monótona cuando es creciente o decreciente.

Teorema 1.10.3. Una sucesión monótona converge si y sólo si es acotada.
Nota: Una sucesión $\{f(n)\}$ se dice que es acotada si existe un número positivo M tal que $|f(n)| \leq M$ para todo n. Una sucesión que no está acotada se denomina no acotada.
Demostración:
Es claro que una sucesión monótona no acotada no puede converger, por tanto basta probar que una sucesión monótona y acotada es converge.
Supongamos que $\{f(n)\}$ es creciente y acotada, sea L el supremo del conjunto $\{f(n) : n \in \mathbb{N}\}$. Entonces $f(n) \leq L$ para todo n, afirmamos que la sucesión converge hacia L. Sea ϵ un número positivo arbitrario. Como $L - \epsilon$ no puede ser una cota superior del conjunto $\{f(n)\}$, entonces $L - \epsilon < f(N)$ para algún N (este N depende de ϵ). Puesto que $\{f(n)\}$ es una sucesión creciente, si $n \geq N$ entonces $f(N) \leq f(n)$, por tanto, $L - \epsilon < f(n) \leq L$ para todo $n \geq N$. De estas desigualdades tenemos que $0 \leq L - f(n) < \epsilon$ para todo $n \geq N$, lo que significa que la sucesión converge hacia L, como se quería demostrar.
Ahora, supongamos que $\{f(n)\}$ es una sucesión decreciente y acotada, sea L el ínfimo del conjunto $\{f(n) : n \in \mathbb{N}\}$. Entonces $f(n) \geq L$ para todo n, afirmamos que la sucesión converge hacia L. Sea ϵ un número positivo arbitrario. Como $L + \epsilon$ no puede ser una cota inferior del conjunto $\{f(n)\}$, entones $L + \epsilon > f(N)$ para algún N (este N depende de ϵ). Puesto que $\{f(n)\}$ es decreciente, si $n \geq N$ entonces $f(N) \geq f(n)$, por tanto, $L + \epsilon > f(n) \geq L$ para todo $n \geq N$. De estas desigualdades tenemos que $0 \leq f(n) - L < \epsilon$ para todo $n \geq N$, lo que significa que la sucesión converge hacia L, como se quería demostrar.

A partir de una sucesión de números reales, se puede formar una nueva sucesión sumando los términos sucesivamente. Así, si la sucesión dada tiene términos $a_1, a_2, \ldots, a_n, \ldots$ se forma la sucesión de las "sumas parciales" $s_1 = a_1$, $s_2 = a_1 + a_2$, $s_3 = a_1 + a_2 + a_3$, y así sucesivamente, estando definida la suma parcial de los n primeros términos como sigue:

$$s_n = a_1 + a_2 + \cdots + a_n = \sum_{k=1}^{n} a_k.$$

La sucesión $\{s_n\}$ de las sumas parciales se llama serie infinita o simplemente serie, y se indica también por los siguientes símbolos: $a_1 + a_2 + a_3 + \cdots$, $a_1 + a_2 + \cdots\ a_n + \cdots$, $\sum_{k=1}^{\infty} a_k$. En los símbolos anteriores se quiere recordar que la sucesión de sumas parciales $\{s_n\}$ se obtiene de la sucesión $\{a_n\}$ por adición de términos sucesivos.

Si existe un número real S tal que: $\lim_{n\to\infty} s_n = S$, se dice que la serie $\sum_{k=1}^{\infty} a_k$ es convergente y tiene suma S en cuyo caso se escribe: $\sum_{k=1}^{\infty} a_k = S$. Si $\{s_n\}$ diverge se dice que la serie $\sum_{k=1}^{\infty} a_k$ diverge y no tiene suma.

Las sumas finitas ordinarias tienen propiedades importantes:

$$\text{Propiedad aditiva:} \quad \sum_{k=1}^{n}(a_k + b_k) = \sum_{k=1}^{n} a_k + \sum_{k=1}^{n} b_k,$$

$$\text{Propiedad aditiva:} \quad \sum_{k=1}^{n} ca_k = c\sum_{k=1}^{n} a_k.$$

Hemos demostrado que los números primos son infinitos, el siguiente paso es entender que tan "densos" (entendiendo por densidad la proporción de números primos con relación al total de números enteros en un intervalo dado.) son los primos. Un modo para hacerlo es estudiar la suma de sus inversos, esto es: $\sum_{p}^{\infty} \frac{1}{p}$. Descubriremos así que esta suma diverge, es decir los primos son densos, más densos que los cuadrados por ejemplo:

$$\sum_{n=1}^{\infty} \frac{1}{n} \quad \text{diverge,} \qquad \sum_{n=1}^{\infty} \frac{1}{n^2} \quad \text{converge (problema de Basilea).}$$

La divergencia de $\sum \frac{1}{n}$ fue demostrada por primera vez por Nicole Oresme (1323 - 1382). Oresme demostró la divergencia de la serie armónica confrontandola con otra serie divergente (Nicole Oresme empleó el criterio de comparación[12], el cual probaremos más adelante):

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + \cdots > 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{4} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{16} + \cdots$$

En la segunda serie cada término ha sido sustituido con un término de la forma $1/2^k$ más pequeño. Es decir $1/3$ ha sido sustituido por $1/4$ mientras $1/5$, $1/6$, $1/7$ han sido sustituidos por $1/8$ y así sucesivamente. Con esta estratagema. Oresme se las arregla para reunir los términos. En particular tiene dos términos (que sumados hacen $1/2$), cuatro términos $1/8$ que sumados hacen de nuevo $1/2$ y así sucesivamente.
Por lo tanto Oresme ha logrado que aparezca un número arbitrario (y también infinito) de términos $1/2$.

$$1 + \left(\frac{1}{2}\right) + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right) + \left(\frac{1}{16} + \cdots + \frac{1}{16}\right) + \cdots =$$

$$= 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \cdots = \infty \ .$$

Dado que la serie armónica era más grande que esta serie de trabajo, también ésta serie deberá ser infinita.

$$\sum_{n=1}^{2^k} \frac{1}{n} > 1 + \frac{k}{2} \quad \text{para todo entero positivo } k.$$

Realicemos otra prueba de la divergencia de la serie armónica $\sum_{k=1}^{\infty} \frac{1}{k}$:

$$\sum_{k=1}^{\infty} \frac{1}{k} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + \cdots$$

[12]Criterio de comparación: Si $\sum_{k=1}^{\infty} b_k$ converge, y $0 \le a_k \le b_k$, entonces $\sum_{k=1}^{\infty} a_k$ converge; si $\sum_{k=1}^{\infty} c_k$ diverge y $0 \le c_k \le d_k$, entonces $\sum_{k=1}^{\infty} d_k$ diverge.

agrupando términos tenemos

$$\sum_{k=1}^{\infty}\frac{1}{k}=1+\left(\frac{1}{2}\right)+\left(\frac{1}{3}+\frac{1}{4}\right)+\left(\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}\right)+\left(\frac{1}{9}+\frac{1}{10}+\cdots+\frac{1}{16}\right)+\ \cdots$$

donde cada expresión entre paréntesis es de la forma

$$c_k=\frac{1}{2^{k-1}+1}+\frac{1}{2^{k-1}+2}+\frac{1}{2^{k-1}+2^{k-1}}=\frac{1}{2^{k-1}+1}+\frac{1}{2^{k-1}+2}+\cdots+\frac{1}{2^k}$$

para $k\geq 1$. Por ejemplo, para $k=1$ obtenemos el término $1/2$, para $k=2$ obtenemos $1/3+1/4$. La expresión anterior define la sucesión $c_1,c_2,c_3,\ldots$. El primer término de la serie es igual a 1 no está incluido en esta sucesión, para incluirlo se define $c_0=1$. Ahora, observemos que para $k\geq 1$, la fórmula para c_k tiene $2k^{-1}$ sumandos, de los cuales el menor es $\frac{1}{2^k}$, así se tiene que

$$c_k\geq 2\ k^{-1}\frac{1}{2^k}=\frac{1}{2}\qquad \text{con}\ \ k\geq 1$$

y también es cierto que, así que tenemos

$$\sum_{n=1}^{2^m}\frac{1}{n}=\sum_{k=0}^{m}c_k\geq\underbrace{\frac{1}{2}+\frac{1}{2}+\cdots+\frac{1}{2}}_{m+1\ \text{veces}}$$

es decir

$$\sum_{k=0}^{m}c_k\geq\frac{m+1}{2}\qquad\therefore\quad\lim_{m\to\infty}\sum_{k=1}^{m}c_k\geq\lim_{m\to\infty}\frac{m+1}{2}=\infty$$

de donde

$$\sum_{n=1}^{\infty}\frac{1}{n}=\lim_{m\to\infty}\sum_{k=1}^{m}c_k=\infty$$

así, la serie armónica diverge a infinito.

Teorema 1.10.4. La suma de los inversos de los números primos diverge.

Demostración:
(Por contradicción) Denotemos por p_n al n-ésimo número primo, i.e., $p_1=2$, $p_2=3$, $p_3=5,\ldots,$ y al conjunto de todos los números primos por $\mathbb{P}$. Donde la letra p siempre será asignada a un número primo. Procedemos a demostrar la divergencia de la serie:

$$\sum_{p\in\mathbb{P}}\frac{1}{p}=\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\cdots+\frac{1}{p_n}+\cdots$$

Supongamos que $\sum_{p\in\mathbb{P}}\frac{1}{p}$ converge y tiene por suma S, luego, para $\epsilon=\frac{1}{2}$, existe $N\in\mathbb{N}$ tal que

$$S-S_N=\sum_{p>N}\frac{1}{p}<\frac{1}{2}\ .$$

Ahora, sea $Q=\prod_{p\leq N}p$ el producto de todos los números primos menores o iguales que N, entonces los números de la forma $1+nQ$ con $n\in\mathbb{N}$ no son divisibles por los primos menores que N. Efectivamente, si $p\leq N$ cumple $p\mid(1+nQ)$ tendríamos que $1+nQ=pk$ con $k\in\mathbb{N}$. Por otra parte $p\mid Q$, i.e., $Q=ps$ con $s\in\mathbb{N}$, entonces $1+nps=pk$ ó $1=p(k-ns)$ lo cual es absurdo. Ahora consideremos

$$\sum_{j=1}^{\infty}\left(\sum_{p>N}\frac{1}{p}\right)^j<\sum_{j=1}^{\infty}\frac{1}{2^j}=1$$

luego, se verifica que

$$\sum_{n=1}^{\infty} \frac{1}{1+nQ} \leq \sum_{j=1}^{\infty} \left(\sum_{p>N} \frac{1}{p} \right)^j$$

porque cada término de la suma de la izquierda aparece en la suma de la derecha al menos una vez. Esto es claro, pues todo divisor primo p de $1+nQ$ es mayor que N. Además $\frac{1}{1+nQ} \leq \frac{1}{p}$, por lo tanto

$$\sum_{n=1}^{\infty} \frac{1}{1+nQ} \leq 1$$

pero la serie anterior diverge pues

$$\sum_{n=1}^{K} \frac{1}{1+nQ} \geq \frac{1}{2Q} \sum_{n=1}^{K} \frac{1}{n}$$

para todo K, y notamos que el miembro del lado derecho corresponde a la serie armónica que bien sabemos diverge cuando $K \to \infty$. Así, la suma de los inversos de los números primos diverge.

Definición 1.10.5. La serie de Taylor de una función real o compleja $f(z)$ con centro en a, es la serie:

$$f(z) = \sum_{n=0}^{\infty} \frac{1}{n!} \left. \frac{d^n f(z)}{dz^n} \right|_{z=a} (z-a)^n,$$

$$f(z) = f(a) + \frac{f'(a)}{1!}(z-a) + \frac{f''(a)}{2!}(z-a)^2 + \cdots + \frac{f^{(n)}(a)}{n!}(z-a)^n + \cdots,$$

donde $n!$ denota el factorial de n, $f^{(n)}(a)$ denota la n-ésima derivada de f evaluada en el punto a, de manera más compacta se tiene:

$$\sum_{n=0}^{\infty} \frac{f^{(n)}(a)}{n!}(z-a)^n = f(a) + f'(a)(z-a) + \frac{1}{2}f''(a)(z-a)^2 + \cdots .$$

Definición 1.10.6. La serie de Maclaurin se tiene cuando en particular $a = 0$, i.e., es un caso particular de la serie de Taylor.

Por ejemplo:
Calcular la serie de Taylor de la función $f(x) = e^x$ en $x = 0$. Como x es un número real, empleando la fórmula anterior, se tiene

$$f(x) = f(a) + \frac{f'(a)}{1!}(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \cdots + \frac{f^{(n)}(a)}{n!}(x-a)^n + \cdots ,$$

dado que nos piden la serie de Taylor en $x = 0$, por lo tanto $a = 0$ tenemos

$$f(x) = f(a) + \frac{f'(0)}{1!}(x-0) + \frac{f''(0)}{2!}(x-0)^2 + \cdots + \frac{f^{(n)}(0)}{n!}(x-0)^n + \cdots ,$$

ahora, calculamos las derivadas y las evaluamos en $x = 0$, para después sustituir en la expanción anterior

$$\begin{aligned}
f(x) = e^x &\Rightarrow f(0) = e^0 = 1, & \qquad f'''(x) = e^x &\Rightarrow f'''(0) = e^0 = 1,\\
f'(x) = e^x &\Rightarrow f'(0) = e^0 = 1, & &\vdots\\
f''(x) = e^x &\Rightarrow f''(0) = e^0 = 1, & f^{(n)}(x) = e^x &\Rightarrow f^{(n)}(0) = e^0 = 1,
\end{aligned}$$

sustituyendo

$$f(x) = 1 + \frac{1}{1!}(x-0) + \frac{1}{2!}(x-0)^2 + \frac{1}{3!}(x-0)^3 + \cdots$$

$$\Rightarrow \quad f(x) = 1 + \frac{1}{1!}x + \frac{1}{2!}x^2 + \frac{1}{3!} + \cdots \;=\; 1 + \frac{1}{1!}x + \frac{1}{2!}x^2 + \frac{1}{3!}x^3 + \cdots$$

$$\Rightarrow \quad f(x) = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots . \quad \therefore \quad f(x) = \sum_{n=0}^{\infty} \frac{x^x}{n!} \ .$$

Definición 1.10.7. Una **serie de Laurent** centrada alrededor de un punto c, es una serie de la forma:

$$\sum_{k=-\infty}^{\infty} a_k (z-c)^k$$

donde $a_k, c, z \in \mathbb{C}$. Se puede demostrar (lo cual no relizaremos) que esta serie es convergente dentro del conjunto (posiblemente nulo, $\varnothing$):

$$D := \{z \in \mathbb{C} : R_1 < |z-c| < R_2\} \ , \quad \text{donde}$$

$$R_1 := \limsup_{k\to\infty} |a_{-k}|^{1/k} \qquad \text{y} \qquad R_2 := \frac{1}{\limsup_{k\to\infty} |a_{-k}|^{1/k}} \ ,$$

toda serie de Laurent tiene vinculada una función de la forma:

$$f(z) := \sum_{-\infty}^{\infty} a_k (z-c)^k,$$

cuyo dominio es el conjunto de puntos en $\mathbb{C}$ sobre el cual es convergente. Esta función es analítica dentro de una corona D, inversamente, toda función en una corona es igual a una única serie de Laurent.

Una serie de Laurent se define con respecto a un punto particular c y un camino de integración γ. El camino de integración debe estar dentro de un disco donde $f(z)$ es una función holomorfa (a veces se usa como sinónimo el término función analítica, aunque no es estrictamente correcto, dado que una función analítica es técnicamente aquella que admite desarrollo en serie de potencias en cierto entorno de un punto, lo que ocurre es que en $\mathbb{C}$ toda función holomorfa es también analítica).
Los coeficientes de una serie de Laurent en una función analítica se pueden encontrar por medio de la fórmula integral de Cauchy y están dados por:

$$a_n = \frac{1}{2\pi i} \oint_\gamma \frac{f(z)}{(z-c)^{n+1}} dz, \quad \text{para} \ \ n = 0, 1, 2, \ldots,$$

$$a_{n-1} = \frac{1}{2\pi i} \oint_\gamma (z-c)^{n-1} f(z) dz, \quad \text{para} \ \ n = 1, 2, 3, \ldots$$

(la sucesión de constantes están definidas por un camino de integración en la generalización de la integral de Cauchy).

Si suponemos $\sum_{-\infty}^{\infty} a_n (z-c)^n$ es una serie de Laurent con coeficientes a_n y un centro complejo c. Entonces existe un radio interior r y un radio exterior R de tal forma que:

- La serie de Laurent es convergente en la corona abierta $A := \{z : r < |z-c| < R\}$, tanto para potencias de grado positivo como para potencias de grado negativo y esta convergencia define una función holomorfa $f(z)$ en la corona abierta.

- Fuera de la corona, la serie de Laurent es divergente.
- Para el disco existe al menos un punto en la frontera interior y otro en la frontera exterior para los cuales no puede ser holomorfa continua.

La serie de Laurent es muy importante en el análisis complejo, especialmente para investigar el comportamiento de funciones cerca de singularidades, pues permite saber qué tipos de singularidades tiene una función. Así, si expandimos una función en serie de Laurent, tomando como centro una singularidad y como radio interior cero, la cantidad de potencias negativas en la serie indicará que tipo de singularidad es (en el siguiente capítulo se definirán formalmente estos conceptos):

- Si la serie no tiene potencias negativas, la singularidad es evitable.
- Si la serie tiene finitas potencias negativas, la singularidad es un polo.
- Si la serie tiene infinitas potencias negativas, la singularidad es una singularidad esencial.

La serie de Laurent de una función compleja $f(z)$ es la representación de la misma función en la forma de una serie de potencias, la cual también incluye términos de grado negativo. Esta serie se puede usar para expresar funciones complejas en casos donde una expansión de la serie de Taylor no es aplicable o no se puede acoplar. La serie de Laurent fue descubierta por Karl Weierstrass en el año de 1841; pero no se divulgó en ese entonces. El matemático Pierre Alphonse Laurent fue quien la publicó en el año 1843.

Nota: En el capítulo de análisis complejo se analizaran los conceptos mencionados en la definición anterior (Definición 1.10.7.).
Esta última definición resulta útil pues será importante para una comprensión más profunda de algunos conceptos que se necesitarán para un análisis más profundo de la hipótesis de Riemann.

1.11. El problema de Basilea

Hemos llegado hasta aquí para hablar del problema di Basilea, es decir para determinar el valor de la suma de los inversos de los cuadrados. En terminos más inteligibles:

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

El problema de Basilea fue propuesto por primera vez por Pietro Mengoli en 1644 y se hace famoso cuando Jakob Bernoulli lo da a conocer en 1689. Jakob era el hermano de Johann Bernoulli, maetro de Euler, que probablemente lo mostró a Euler. En los años 30 del siglo XVIII, el problema se había vuelto extremadamente notable entre los matemáticos y es comprensible que Euler se hiciera famoso cuando lo resolvió con tan solo 28 años. Euler generalizó entonces el problema y sus ideas fueron retomadas por el mismo Riemann. Es comprensible entonces porqué el problema es llamado "de Basilea" en honor a la ciudad natal de Euler.

Euler parte de la serie de Taylor de la función seno:

$$\operatorname{sen}(x) = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots$$

dividiendo por x tenemos:

$$\frac{\operatorname{sen}(x)}{x} = \frac{x}{x} - \frac{x^3}{3!(x)} + \frac{x^5}{5!(x)} - \frac{x^7}{7!(x)} + \cdots = 1 - \frac{x^2}{3!} + \frac{x^4}{5!} - \frac{x^6}{7!} + \cdots$$

luego, las raíces de la función $\frac{\text{sen}(x)}{x}$ están en los puntos $x = n\pi$, donde $n = \pm 1, \pm 2, \pm 3, \ldots$. (Y ésta es la genialidad de Euler) que puede expresar esta función como un producto infinito de factores líneales, creando un polinomio de grado infinito, cómo haremos para un número finito de raíces; ejemplo, si yo se que las raíces de un polinomio son 1 y 3, puedo construir el polinomio como $(x-1)(x-3)$, y del mismo modo Euler crea el polinomio:

$$\frac{\text{sen}(x)}{x} = \left(1 - \frac{x}{\pi}\right)\left(1 + \frac{x}{\pi}\right)\left(1 - \frac{x}{2\pi}\right)\left(1 + \frac{x}{2\pi}\right)\left(1 - \frac{x}{3\pi}\right)\left(1 + \frac{x}{3\pi}\right)\cdots$$

$$\Rightarrow \quad \frac{\text{sen}(x)}{x} = \left(1 - \frac{x^2}{\pi^2}\right)\left(1 - \frac{x^2}{4\pi^2}\right)\left(1 - \frac{x^2}{9\pi^2}\right)\cdots ,$$

si efectuamos el producto de estos factores y comparamos los términos de x^2 vemos que el coeficiente de segundo grado de $\frac{\text{sen}(x)}{x}$ es:

$$-\left(\frac{1}{\pi^2} + \frac{1}{4\pi^2} + \frac{1}{9\pi^2} + \cdots\right) = -\frac{1}{\pi^2}\sum_{n=1}^{\infty}\frac{1}{n^2} ,$$

pero por la original expansión en serie infinita de $\frac{\text{sen}(x)}{x}$ vemos que el coeficiente de x^2 es $\frac{1}{3!} = -\frac{1}{6}$. Estos dos coeficientes deben ser iguales:

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

así, finalmente:

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

Agrego una cosa. Si se están preguntando dónde entra todo esto con la hipótesis de Riemann, sepan que la serie de los inversos de los cuadrados de los números naturales corresponde a la $\zeta(2)$ y es importante familiarizarmos con estos valores específicos de la función zeta.

Estos problemas "banales" se revelan mucho menos banales de lo que parecen dado que nadie hasta ahora ha logrado calcular el valor explícito de $\zeta(3)$ y en general de $\zeta(2n+1)$.

Capítulo 2

Análisis Complejo

Durante el estudio de las matemáticas hay una "extensión" progresiva del concepto de número, desde el conjunto de los enteros naturales $\mathbb{N}$ pasamos al de los enteros relativos $\mathbb{Z}$ para luego alcanzar a los racionales $\mathbb{Q}$, y así hasta los números reales $\mathbb{R}$. A menudo estas "extensiones" se justifican por la incapacidad de resolver dentro del conjunto de estudio un determinado problema. Por ejemplo la ecuacion

$$x^2 = 2 \ ,$$

no tiene solución en el conjunto de los racionales, mientras que tiene dos en la extensión hacia los reales $\mathbb{R}$, i.e., $\sqrt{2} \ \wedge \ -\sqrt{2}$. En cambio, surge la necesidad de ampliar aún más a los números reales, cuando intentas resolver otra ecuación cuadrática:

$$x^2 = -1 \ .$$

Ahora, el problema en este caso es común para todas las soluciones de las ecuaciones cuadráticas con discriminantes negativos y consiste en que la función raíz cuadrada real no está definido para números negativos.
Como veremos, el conjunto de los números complejos, que denotaremos con el símbolo $\mathbb{C}$, nos permitirá dar respuesta a este problema.

Los números que hoy llamamos "complejos" fueron durante muchos años motivo de polémicas y controversias entre la comunidad científica. Poco a poco, por la creciente evidencia de su utilidad, acabaron por ser comúnmente aceptados, aunque no fueron bien comprendidos hasta épocas recientes. Nada hay de extraño en ello si pensamos que los números negativos no fueron plenamente aceptados hasta finales del siglo XVII.

Los números complejos hacen sus primeras tímidas apariciones en los trabajos de Cardano (1501-1576) y Bombelli (1526-1672) relacionados con el cálculo de las raíces de la cúbica o ecuación de tercer grado. Fue René Descartes (1596-1650) quien afirmó que "ciertas ecuaciones algebraicas sólo tienen solución en nuestra imaginación" y acuñó el calificativo "imaginarias" para referirse a ellas. Desde el siglo XVI hasta finales del siglo XVIII los números complejos o imaginarios son usados con recelo, con desconfianza. Con frecuencia, cuando la solución de un problema resulta ser un número complejo se interpreta esto como que el problema no tiene solución. Para Leibnitz "el número imaginario es un recurso sutil y maravilloso del espíritu divino, casi un anfibio entre el ser y el no ser".

El éxito de Euler y Gauss al trabajar con números complejos se debió a que ellos no se preocuparon de la "naturaleza" de los mismos; no se preguntaron "¿qué es un número complejo?", sino que se dijeron "a ver, para qué sirven, qué puede hacerse con ellos". Es Gauss quien definitivamente

concede a los números complejos un lugar privilegiado dentro de las matemáticas al probar en 1799 el resultado conocido como Teorema Fundamental del Álgebra que afirma que toda ecuación polinómica de grado n con coeficientes complejos tiene, si cada raíz se cuenta tantas veces como su orden, n raíces que también son números complejos.

El término, hoy usado de "números complejos" se debe a Gauss, quien también hizo popular la letra "i" que Euler (1707-1783) había usado esporádicamente. En 1806 Argand interpreta los números complejos como vectores en el plano. La fecha de 1825 es considerada como el nacimiento de la teoría de funciones de variable compleja, pues se publica en dicho año la memoria sobre la integración compleja que Cauchy había escrito ya en 1814.

2.1. Propiedades de los números complejos

La extensión consiste en el paso de la dimensión uno de la recta (real) a la dimensión dos del plano (complejo). Por lo tanto, un número complejo z se identifica como un punto en el plano y se representa comúnmente de dos maneras: en la forma cartesiana y exponencial

Definición 2.1.1. El sistema de los números complejos, denotados por $\mathbb{C}$, es el conjunto $\mathbb{R}^2$ junto con las reglas usuales de la adición de vectores y la multiplicación escalar por un número real, a saber

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2) \ ,$$
$$a(x, y) = (ax, ay) \ ,$$

y la operación de multiplicación compleja, definida como

$$(x_1, y_1)(x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2) \ .$$

Vamos a identificar a los números reales x con puntos en el eje x; entonces x y $(x, 0)$ representan el mismo punto $(x, 0) \in \mathbb{R}^2$. El eje y será llamado el eje imaginario y el punto $(0, 1)$ será denotado por i. Así, damos la siguiente definición.

Definición 2.1.2. $i = (0, 1)$, entonces $(x, y) = x + iy$.

El lado derecho de la ecuación representa a $x(1, 0) + y(0, 1) = (x, 0) + (0, y) = (x, y)$. Usando $y = (y, 0)$ y la definición 2.1.1. de multiplicación de complejos, obtenemos $iy = (0, 1)(y, 0) = (0 \cdot y - 1 \cdot 0, y \cdot 1 + 0 \cdot 0) = (0, y) = y(0, 1) = yi$ y así también podemos escribir $(x, y) = x + iy$. Un solo símbolo tal como $z = a + ib$ se usa generalmente para indicar un número complejo. La notación $z \in \mathbb{C}$ significa que z pertenece al conjunto de los números complejos.

Nótese que $i^2 = i \cdot i = (0, 1) \cdot (0, 1) = (0 \cdot 0 - 1 \cdot 1, [1 \cdot 0 + 0 \cdot 1]) = (-1, 0) = -1$, de esta manera tenemos la propiedad:

$$i^2 = -1 \ .$$

Si recordamos esta ecuación, entonces la regla para la multiplicación de números complejos es también fácil de recordar y de motivar:

$$(a + ib)(c + id) = ac + iad + ibc + i^2bd = (ac - bd) + i(ad + bc) \ .$$

Definición 2.1.3. Los números reales x e y se llaman respectivamente parte real y parte imaginaria de z y denotada por:

$$x = \operatorname{Re} z \quad \wedge \quad y = \operatorname{Im} z \ .$$

El subconjunto de números complejos de la forma $(x,0)$ se puede identificar con el conjunto de los números reales $\mathbb{R}$, en este sentido escribimos $\mathbb{R} \subset \mathbb{C}$. A un número complejo de la forma $(0,y)$ se le llama imaginario puro.
Diremos que dos números complejos $z_1 = (x_1, y_1)$ e $z_2 = (x_2, y_2)$ son iguales si tienen las mismas partes real e imaginaria, i.e.:

$$z_1 = z_2 \qquad \Longleftrightarrow \qquad x_1 = x_2 \quad \wedge \quad y_1 = y_2 \ .$$

El número complejo i es una solución de la ecuación $x^2 = -1$.

Definición 2.1.4. El Los números $0 = (0,0)$ y $1 = (1,0)$ son respectivamente la identidad aditiva y multiplicativa, i.e.:

$$z + 0 = 0 + z = z \quad \wedge \quad z1 = 1z = z, \quad \forall z \in \mathbb{C} \ .$$

Definición 2.1.5. El inverso (aditivo) de $z = (x,y)$ se denota por el número $-z = (-x,-y)$; i.e., se tiene $z + (-z) = 0$. Usando esta noción podemos definir, para cada $z_1, z_2 \in \mathbb{C}$, la sustracción:

$$z_1 - z_2 = z_1 + (-z_2) \ , \quad \text{i.e.,}$$

$$x_1 + iy_1 - (x_2 + iy_2) = x_1 - x_2 + i(y_1 - y_2) \ .$$

Definición 2.1.6. El inverso (multiplicativo) de un número $z \neq 0$, denotado por $\frac{1}{z}$ o también z^{-1} es definido por la relación $zz^{-1} = 1$; no es dificil comprobar que:

$$\frac{1}{z} = z^{-1} = \frac{x}{x^2 + y^2} + i\frac{-y}{x^2 + y^2} \ .$$

Así que definamos la división; $\forall z_1, z_2 \in \mathbb{C}$ con $z_2 \neq 0$, como sigue:

$$\frac{z_1}{z_2} = z_1 z_2^{-1} = \frac{x_1 x_2 + y_1 y_2}{x_2^2 + y_2^2} + i\frac{x_2 y_1 - x_1 y_2}{x_2^2 + y_2^2} \ .$$

Finalmente, destacamos que el orden habitual de los números reales no es extensible al conjunto de números complejos.

Enumeramos a continuación algunas propiedades de la suma y del producto; para todo $z_1, z_2, z_3 \in \mathbb{C}$ tenemos:

Reglas de la adición:

- $z_1 + z_2 = z_2 + z_1$,
- $(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$,
- $z_1 + 0 = z_1$,
- $z_1 + (-z_1) = 0$.

Reglas de la multiplicación:

- $z_1 z_2 = z_2 z_1$,
- $(z_1 z_2) z_3 = z_1 (z_2 z_3)$.
- $1z = z$,
- $z(z^{-1}) = 1 \quad$ para $\ z \neq 0$,
- $z_1(z_2 + z_3) = z_1 z_2 + z_1 z_3$.

En resumen se tiene el siguiente teorema.

Teorema 2.1.7. Los números complejos $\mathbb{C}$ bajo las operaciones de suma y producto forman un campo.

Demostración:
La suma es conmutativa y asociativa ya que cada entrada pertenece a $\mathbb{R}$ y en $\mathbb{R}$ la suma es conmutativa y asociativa. El neutro es $(0,0)$ dado que:

$$(a,b)+(0,0)=(a+0,b+0)=(a,b)\ ,$$

para (a,b) su inverso aditivo es $(-a,-b)$. Veamos ahora el producto. Probemos que es conmutativo. Para dos complejos (a,b) y (c,d) tenemos que:

$$(a,b)(c,d)=(ac-bd,ad+bc)\quad\wedge\quad(c,d)(a,b)=(ca-db,cb+da)\ ,$$

ambos resultados son iguales ya que cada entrada pertenece a $\mathbb{R}$ y la suma y el producto son conmutativos en $\mathbb{R}$. Probemos que el producto es asociativo. Para ello tomemos tres complejos $(a,b),(c,d)$ y (e,f), tenemos que:

$$\begin{aligned}[(a,b)(c,d)](e,f)&=(ac-bd,ad+bc)(e,f)=\\&=(ace-bde-adf-bcf,acf-bdf+ade+bce)\ ,\end{aligned}$$

y también que:

$$\begin{aligned}(a,b)[(c,d)(e,f)]&=(a,b)[ce-df,cf+de]=\\&=(ace-adf-bcf-bde,acf+ade+bce-bdf)\ ,\end{aligned}$$

ambas expresiones son iguales ya que cada entrada pertenece a $\mathbb{R}$ y la suma es conmutativa en $\mathbb{R}$. El complejo $(1,0)$, actúa como neutro multiplicativo, tenemos:

$$(a,b)(1,0)=(a\cdot 1-b\cdot 0,a\cdot 0+b\cdot 1)=(a,b)\ ,$$

además, si tomamos un complejo $(a,b)\neq(0,0)$ y lo multiplicamos por $\left(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2}\right)$,:

$$(a,b)\left(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2}\right)=\left(\frac{a^2+b^2}{a^2+b^2},\frac{-ab}{a^2+b^2}+\frac{ba}{a^2+b^2}\right)=(1,0)\ ,$$

o cual muestra que tenemos inversos multiplicativos.

Finalmente probemos la propiedad distributiva, para ello, tomemos ahora tres números complejos $z_1=(a_1+ib_1),z_2=(a_2+ib_2)$ y $z_3=(a_3+ib_3)$, efectuamos $z_1(z_2+z_3)$:

$$(a_1+ib_1)[(a_2+ib_2)+(a_3+ib_3)]=(a_1+ib_1)[(a_2+a_3)+i(b_2+b_3)]\ ,$$

multiplicando:

$$\begin{aligned}&(a_1(a_2+a_3)-b_1(b_2+b_3))+i[b_1(a_2+a_3)+a_1(b_2+b_3)]=\\&\quad=(a_1a_2+a_1a_3-b_1b_2-b_1b_3)+i(b_1a_2+b_1a_3+a_1b_2+a_1b_3)\ ;\end{aligned}$$

desarrollemos ahora $z_1z_2+z_1z_3$:

$$(a_1,ib_1)(a_2+ib_2)+(a_1,ib_1)(a_3+ib_3)\ ,$$

multiplicando y sumando, tenemos:

$$\begin{aligned}&(a_1a_2-b_1b_2)+i(a_1b_2+a_2b_1)+(a_1a_3-b_1b_3)+i(a_1b_3+a_3b_1)=\\&=[(a_1a_2-b_1b_2)+(a_1a_3-b_1b_3)]+i[(a_1b_2+a_2b_1)+(a_1b_3+a_3b_1)]\ ,\end{aligned}$$

en la parte real reordenamos los términos en a_1 primero, luego los de b_1, y en la parte imaginaria los presentamos en orden inverso:

$$(a_1a_2+a_1a_3-b_1b_2-b_1b_3)+i(a_2b_1+a_3b_1+a_1b_2+a_1b_3)\ .$$

Obteniendo el desarrollo del lado izquierdo de la propiedad, de esta manera se concluye la demostración del teorema.

Nota: Si uno requiere que las propiedades de usuales de orden para los números reales se satisfagan, entonces tal orden es imposible para los números complejos. Esta afirmación puede ser probada como sigue: Supóngase que tal orden existe, entonces o $i \geq 0$, o $i \leq 0$. Supongamos que $i \geq 0$, entonces $i \cdot i \geq 0$ y, por tanto, $-1 \geq 0$, lo cual es absurdo. Alternativamente, supóngase que $i \leq 0$, entonces $-i \geq 0$, así $(-i)(-i) \geq 0$ o $-1 \geq 0$, otra vez absurdo. Si $z = a + ib$ y $w = c + id$, podemos decir que $z \leq w$ si $a \leq c$ y $b \leq d$. De cierta manera esto es un orden, pero no satisface todas las reglas que podrían ser requeridas, tales como aquellas obedecidas por los números reales. Por tanto se evitará la notación $z \leq w$ a menos que z y w resulten ser números reales.

Coordenadas cartesianas

Es natural asociar al número $z = (x, y) = x+iy$, con el punto del plano cartesiano de coordenadas x e y (ver Figura 2.1). El número z también se puede considerar como el vector desde el origen hasta el punto (x, y), el eje x se llama eje real, y el eje y eje imaginario.

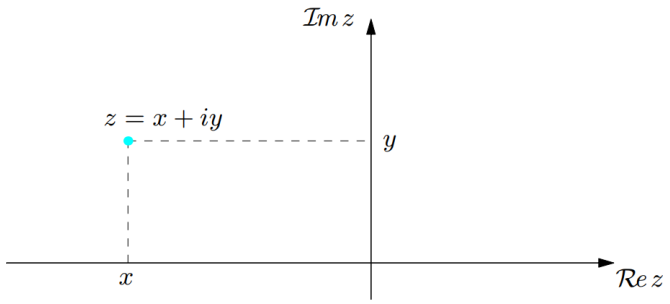


Figura 2.1: Coordenadas cartesianas del punto $z = x + iy$.

Observamos que, dados $z_1, z_2 \in \mathbb{C}$, la suma $z_1 + z_2$ corresponde al vector suma obtenido por medio de la regla del paralelogramo (ver Figura 2.2, izquierda), mientras que la diferencia $z_1 - z_2$ está representada por la diferencia (ver Figura 2.2, derecha).

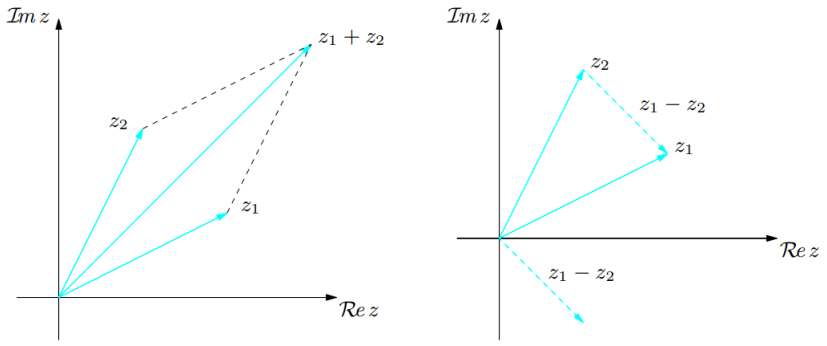


Figura 2.2: Representación gráfica de la suma, a la izquierda, y la diferencia, a la derecha, de dos números complejos z_1 y z_2.

Definición 2.1.8. El módulo o valor absoluto de $z = x + iy$, denotado por $|z|$, es el número positivo:

$$|z| = \sqrt{x^2 + y^2} \ .$$

Que representa la distancia del punto (x, y) al origen; tengamos en cuenta que esta definición se reduce al valor absoluto habitual cuando $y = 0$. Notemos que, mientras que la declaración $z_1 < z_2$ no tiene significado en general, la desigualdad $|z_1| < |z_2|$ significa que el punto correspondiente a z_1 está más cerca del origen que el punto correspondiente a z_2. La distancia entre los puntos correspondientes a z_1 y z_2 viene dada por $|z_1 - z_2|$. Para todo $z \in \mathbb{C}$, obtenemos las siguientes relaciones:

- $|z| \geq 0 \ , \quad |z| = 0 \ \Leftrightarrow \ z = 0$;
- $|z|^2 = (\operatorname{Re} z)^2 + (\operatorname{Im} z)^2$;
- $|z| \leq |\operatorname{Re} z| + |\operatorname{Im} z|$;
- $|z| \geq |\operatorname{Re} z| \geq \operatorname{Re} z$;
- $|z| \geq |\operatorname{Im} z| \geq \operatorname{Im} z$;
- $||z_1| - |z_2|| \leq |z_1 + z_2| \leq |z_1| + |z_2|$.

Definición 2.1.9. El complejo conjugado, o simplemente el conjugado, de un número complejo $z = x + iy$, denotado por $\overline{z}$, se define como:

$$\overline{z} = x - iy \ .$$

Gráficamente el conjugado $\overline{z}$ se representa por el punto $(x, -y)$ que se obtiene por la reflexión con respecto al eje real del punto (x, y). Para todo $z, z_1, z_2 \in \mathbb{C}$, son válidas las siguientes propiedades:

$* \ \overline{\overline{z}} = z$,
$* \ |\overline{z}| = |z|$,
$* \ \overline{z} = |z|^2$,
$* \ \overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2$,
$* \ \overline{z_1 - z_2} = \overline{z}_1 - \overline{z}_2$,
$* \ \overline{z_1 z_2} = \overline{z}_1 \ \overline{z}_2$,
$* \ \overline{\left(\dfrac{z_1}{z_2}\right)} = \dfrac{\overline{z}_1}{\overline{z}_2}$, con $z_2 \neq 0$.

Es inmediato comprobar que, para todo $z \in \mathbb{C}$:

$$\operatorname{Re} z = \frac{z + \overline{z}}{2} \ , \qquad \operatorname{Im} z = \frac{z - \overline{z}}{2i} \ ,$$

Forma trigonométrica y forma exponencial

Dado el punto (x, y), sean r y θ sus coordenadas polares; siempre y cuando:

$$x = r \cos\theta \quad \wedge \quad y = r \ \operatorname{sen} \ \theta \ ,$$

el número complejo $z = (x, y)$ se puede representar en la forma polar o trigonométrica como:

$$z = r(\cos\theta + i \ \operatorname{sen} \ \theta) \ .$$

Definición 2.1.10. Tenemos que $r = |z|$; el número θ es llamado el argumento de z y se denota por $\theta = \arg z$.

Geométricamente, $\arg z$ es cualquier ángulo (medido en radianes) formado por la semirecta de los reales positivos y el vector identificado por z (ver Figura 2.3.). Por lo tanto, puede asumir infinitos valores que difieren en múltiplos enteros de 2π.

Definición 2.1.11. Llamaremos al valor principal de $\arg z$, denotado por $\operatorname{Arg} z$, ese valor único θ de $\arg z$ tal que $-\pi < \theta \leq \pi$, definido por la fórmula:

$$r = \sqrt{x^2+y^2} = \begin{cases} \arctan(y/x)\ , & \text{si} \quad x > 0\ , \\ \arctan(y/x) + \pi\ , & \text{si} \quad x < 0,\ y \geq 0\ , \\ \arctan(y/x) - \pi & \text{si} \quad x < 0,\ y < 0\ , \\ \pi/2 & \text{si} \quad x = 0,\ y > 0\ , \\ -\pi/2 & \text{si} \quad x = 0,\ y < 0\ . \end{cases}$$

Ahora, observamos que dos números complejos $z_1 = r_1(\cos\theta_1 + i \operatorname{sen}\theta_1)$ y $z_2 = r_2(\cos\theta_2 + i \operatorname{sen}\theta_2)$ son iguales si y solo si $r_1 = r_2$ y θ_1, θ_2 difieren en un múltiplo entero de 2π.

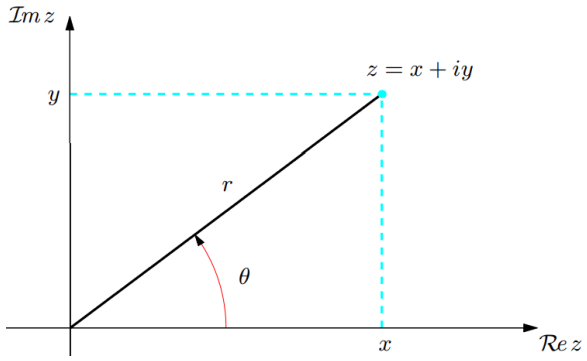


Figura 2.3: Coordenadas polares del número complejo $z = x + iy$.

La representación polar es muy útil para expresar el producto de dos números de forma sencilla y por tanto proporciona una expresión elemental para calcular potencias y raíces de un número complejo. Más precisamente, son:

$$z_1 = r_1(\cos\theta_1 + i \operatorname{sen}\theta_1) \quad \wedge \quad z_2 = r_2(\cos\theta_2 + i \operatorname{sen}\theta_2)\ ,$$

entonces, recordando las fórmulas de suma para las funciones trigonométricas, tenemos:

$$z_1 z_2 = r_1 r_2[(\cos\theta_1 \cos\theta_2 - \operatorname{sen}\theta_1 \operatorname{sen}\theta_2) + i(\operatorname{sen}\theta_1 \cos\theta_2 + \operatorname{sen}\theta_2 \cos\theta_1)]$$

$$\Rightarrow \quad z_1 z_2 = r_1 r_2[\cos(\theta_1 + \theta_2) + i \operatorname{sen}(\theta_1 + \theta_2)]\ . \quad (\star)$$

Entonces la siguiente relacion es valida:

$$\arg(z_1 z_2) = \arg z_1 + \arg z_2\ .$$

A veces es conveniente expresar un número complejo a través de la llamada forma exponencial. Con este fin, extendemos la definición de función exponencial al caso de un exponente imaginario puro.

Definición 2.1.12. Para todo $\theta \in \mathbb{R}$, $e^{i\theta} = \cos\theta + i \text{ sen } \theta$.

Esta relación, es conocida como la fórmula de Euler, encuentra una justificación (de hecho, es objeto de demostración) en el contexto de la teoría de series en un campo complejo. Pero aquí lo tomaremos como una definición. La expresión $z = r(\cos\theta + i \text{ sen } \theta)$ de un número complejo z se convierte entonces en $z = re^{i\theta}$ que es, de hecho, la forma exponencial de z.

La relación $(\star)$ nos da inmediatamente la expresión del producto de dos números complejos $z_1 = r_1 e^{i\theta_1} \ \wedge \ z_2 = r_2 e^{i\theta_2}$, como $z_1 z_2 = r_1 r_2 e^{i(\theta_1+\theta_2)}$; por lo tanto, para multiplicar dos números complejos basta con multiplicar los módulos y sumar sus argumentos. En cuanto al cociente, notamos que de $(\star)$ con $r_1 = r_2 = 1$, obtenemos $e^{i\theta_1} e^{i\theta_2} = e^{i(\theta_1+\theta_2)}$. En particular $e^{i\theta} e^{-i\theta} = 1$; y por lo tanto $e^{-i\theta}$ es el recíproco (inverso multiplicativo) de $e^{i\theta}$; por lo tanto el recíproco de un número complejo $z = re^{i\theta} \neq 0$ viene dado por $z^{-1} = \frac{1}{r} e^{-i\theta}$.

Combinando la fórmula anterior con la del producto, obtenemos la expresión de cociente de dos números complejos $z_1 = r_1 e^{i\theta_1} \ \wedge \ z_2 = r_2 e^{i\theta_2} \neq 0$ tenemos: $\frac{z_1}{z_2} = \frac{r_1}{r_2} e^{i(\theta_1-\theta_2)}$. Luego, de la expresión anterior y de $z_1 z_2 = r_1 r_2 e^{i(\theta_1+\theta_2)}$, para todo $n \in \mathbb{Z}$, obtenemos $z^n = r^n e^{in\theta}$, con $z = re^{i\theta}$ en particular, cuando $r = 1$, obtenemos la llamada **fórmula de De Moivre**:

$$(\cos\theta + i \text{ sen } \theta)^n = \cos n\theta + i \text{ sen } n\theta \ .$$

Consideremos ahora el problema de calcular la raíz n-ésima de un número complejo; dado un entero $n \geq 1$ y un número complejo $w = \rho \, e^{i\varphi}$ si queremos determinar los números complejos $z = re^{i\theta}$ satisfaciendo $z^n = w$. De ($z^n = r^n e^{in\theta}$, con $z = re^{i\theta}$), tenemos $z^n = r^n e^{in\theta} = \rho \, e^{i\varphi} = w$; y por tanto, recordando la condición de igualdad entre dos números complejos, se deben verificar las condiciones:

$$\begin{cases} r^n = \rho \\ n\theta = \varphi + 2k\pi, \quad k \in \mathbb{Z}, \end{cases}$$

o también:

$$\begin{cases} r = \sqrt[n]{\rho} \\ \\ \theta = \frac{\varphi+2k\pi}{n}, \quad k \in \mathbb{Z}. \end{cases}$$

Recordando la periodicidad de las funciones trigonométricas seno y coseno, luego para determinar las n soluciones distintas de nuestro problema:

$$z = \sqrt[n]{\rho} \, e^{\frac{\varphi+2k\pi}{n}} = \sqrt[n]{\rho} \left(\cos\frac{\varphi + 2k\pi}{n} + i \text{ sen} \frac{\varphi + 2k\pi}{n} \right), \quad k = 0, 1, 2, \ldots, n-1 \ .$$

Geométricamente estos puntos se encuentran en la circunferencia con centro en el origen y radio $\sqrt[n]{\rho}$ y son los vértices de un polígono regular de n lados (ver Figura 2.4).

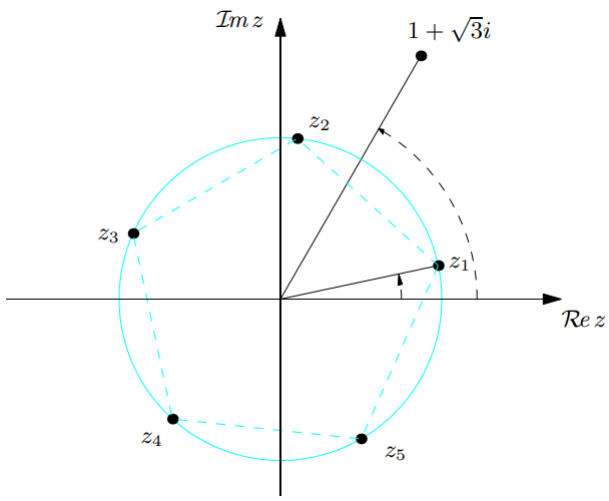


Figura 2.4: Representación gráfica del punto $1+\sqrt{3}i$ y sus raíces quintas, $z_j,\ j=1,\ldots,5$.

Ejemplos:
1) Consideremos, para $n \geq 1$, la ecuación $z^n = 1$. Escribiendo $1 = 1e^{i\theta}$, obtenemos las n raíces distintas: $z^n = z_k = e^{\frac{2ik\pi}{n}}, \quad k = 0, 1, 2, \ldots, n-1$.

Llamadas raíces n-ésimas de la unidad. Tengamos en cuenta que para n impar, tenemos una única raíz real $z_0 = 1$, mientras que para n par hay dos raíces reales $z_0 = 1 \ \wedge \ z_n/2 = -1$ (ver Figura 2.5).

2) Comprobemos que la ecuación $z^2 = -1$. Admite, como era de esperar, las dos raíces $z_\pm = \pm i$. Escribimos $-1 = 1e^{i\pi}$ de donde obtenemos:
$z_+ = z_0 = e^{\frac{i\pi}{2}} \ \wedge \ z_- = z_1 = e^{\frac{i\pi+2\pi}{2}} = e^{\frac{-i\pi}{2}} - i$.

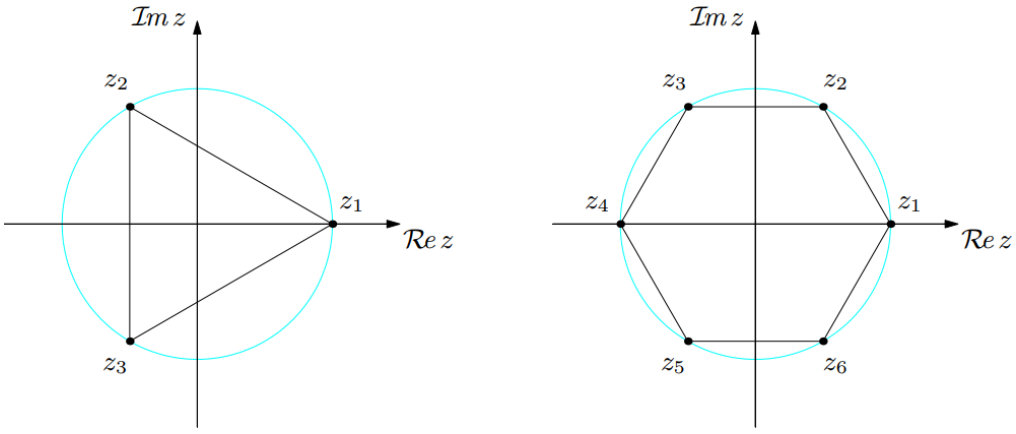


Figura 2.5: Raíces de la unidad: terceras, a la izquierda, y sextas, a la derecha.

Ecuaciones algebraicas

Ahora mostramos que la ecuación cuadrática: $az^2 + bz + c = 0$ admite dos soluciones conjugadas complejas en caso de que el discriminante sea negativo. No es restrictivo asumir que $a > 0$.

Recordando la expansión del cuadrado de un binomio, podemos escribir:

$$z^2 + \frac{b}{a}z + \frac{c}{a} = z^2 + 2\frac{b}{2a}z + \frac{b^2}{4a^2} + \frac{c}{a} - \frac{b^2}{4a^2} = 0$$

$$\Rightarrow \quad \left(z + \frac{b}{2a}\right)^2 = \frac{\Delta}{4a^2} < 0 \ , \quad \text{con} \ \ \Delta = b^2 - 4ac \ ,$$

$$\Rightarrow \quad z + \frac{b}{2a} = \pm i\frac{\sqrt{-\Delta}}{2a} \quad \Rightarrow \quad z = \frac{-b \pm i\sqrt{\Delta}}{2a} \ .$$

Esta expresión se puede escribir como $z = \frac{-b \pm \sqrt{\Delta}}{2a}$, en analogía con el caso de discriminante ≥ 0.

Las ecuaciones de tercer y cuarto grado admiten tres y cuatro, respectivamente raíces (contadas con las multiplicidades apropiadas) que se pueden expresar explícitamente mediante operaciones algebraicas y la extracción de cuadrados, cúbicos y cuartos, sin embargo, no existe una expresión analítica para las raíces de las ecuaciones de orden superior; sin embargo, el Teorema Fundamental del Álgebra garantiza que toda ecuación algebraica de orden n admite exactamente n raíces en el campo complejo, cada una con la multiplicidad adecuada.

2.2. Topología de los números complejos

Definición 2.2.1. Sea $z_0 \in \mathbb{C}$ un número complejo y $r > 0$ un número real positivo. El conjunto:

$$B_r(z_0) = \{z \in \mathbb{C} : |z - z_0| < r\} \ ,$$

se llama vecindad de centro z_0 y radio r; consta de todos los puntos $z \in \mathbb{C}$ que son menores a r desde el centro z_0 (ver Figura 2.6).

Definición 2.2.2. Sea $\Omega \subseteq \mathbb{C}$ un conjunto de números complejos; se dice que un punto $z_0 \in \Omega$ es interior a Ω si existe una vecindad $B_r(z_0)$ enteramente contenida en Ω, i.e., $B_r(z_0) \subseteq \Omega$.

Definición 2.2.3. Sea $\Omega \subseteq \mathbb{C}$ un conjunto de números complejos; se dice que un punto z_0 es externo a Ω si existe una vecindad $B_r(z_0)$ que no contiene puntos de Ω, i.e., $B_r(z_0) \cap \Omega = \emptyset$.

Definición 2.2.4. Sea $\Omega \subseteq \mathbb{C}$ un conjunto de números complejos; si z_0 no es ni interno ni externo a Ω, se llama punto frontera de Ω. En otras palabras, un punto frontera z_0 para Ω es tal que cada vecindad $B_r(z_0)$ contiene puntos tanto de Ω como de su complemento $\Omega^{\complement}$, i.e., $B_r(z_0) \cap \Omega \neq \emptyset$ y $B_r(z_0) \cap \Omega^{\complement} \neq \emptyset$. Denotaremos al conjunto de puntos de la frontera con el símbolo $\partial\Omega$, que comúnmente es llamado frontera de Ω. Por ejemplo, considere el disco unitario $\Omega_1 = \{z \in \mathbb{C} : |z| \leq 1\}$ entonces todos los puntos z de módulo < 1 son interiores a Ω y la frontera $\partial\Omega$ que consiste en la circunferencia $\{z \in \mathbb{C} : |z| = 1\}$.

Definición 2.2.5. Se dice que un conjunto $\Omega \subseteq \mathbb{C}$ es abierto si todo punto es interior, i.e., si no contiene puntos de su frontera; se dice que es cerrado si su complemento es un conjunto abierto. No es difícil verificar que un conjunto es cerrado si y solo si contiene todos sus puntos frontera. Observe que toda vecindad $B_r(z_0)$ es un conjunto abierto; el disco unitario previamente considerado Ω_1 es un conjunto cerrado. El conjunto $\Omega_2 = \{z \in \mathbb{C} : 1 \leq |z| < 2\}$, que representa la corona circular (o anillo), delimitado por las circunferencias con centro en el origen y de radios 1 y 2 respectivamente, tampoco es abierto ni cerrado (ver Figura 2.7). Observemos que la circunferencia exterior no pertenece a Ω_2 y que $\partial\Omega_2 = \{z \in \mathbb{C} : |z| = 1\} \cup \{z \in \mathbb{C} : |z| = 2\}$. El conjunto $\mathbb{C}$ es a la vez abierto y cerrado (y es el único conjunto no vacío con esta propiedad) y la frontera es vacía.

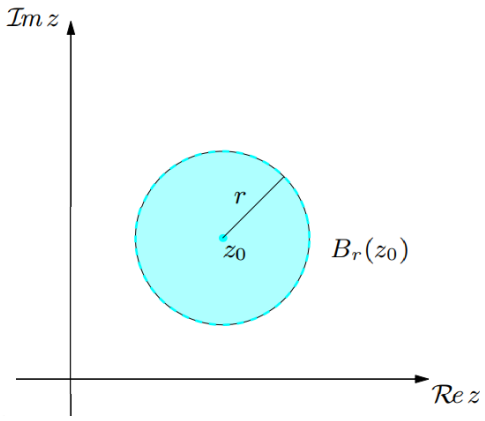


Figura 2.6: Vecindad $B_r(z_0)$ con centro en z_0 y radio $r > 0$.

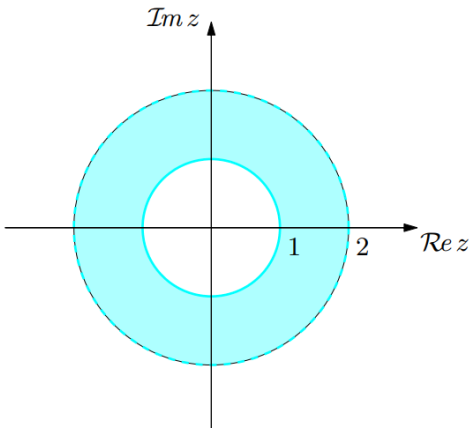


Figura 2.7: Corona circular $\Omega_2 = \{z \in \mathbb{C} : 1 \leq |z| < 2\}$.

Definición 2.2.6. Se dice que un conjunto abierto Ω es poligonal conexo si existen dos puntos cualesquiera en Ω que pueden unirse mediante una línea poligonal[13] (ver Figura 2.8).
El anillo Ω_2 es un conjunto poligonal conexo, mientras que su complemento $\Omega_2^{\complement} = \{z \in \mathbb{C} : |z| < 1 \quad \vee \quad |z| \geq 2\}$ no lo es.

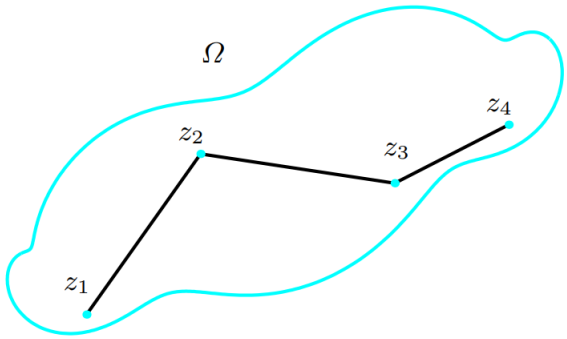


Figura 2.8: Conjunto abierto y conexo.

Definición 2.2.7. Un conjunto abierto y poligonal conexo se llama dominio. Toda vecindad $B_r(z_0)$ es un dominio.

Definición 2.2.8. Una región es un conjunto que consta de un conjunto abierto unido a todos, algunos o ningún punto de la frontera.

Definición 2.2.9. Se dice que un conjunto Ω está acotado si existe una constante $R > 0$ tal que para todo $z \in \Omega$ se satisface que $|z| < R$; i.e., $\Omega \subset B_R(0)$.

Definición 2.2.10. Una colección de conjuntos abiertos U_α para algún α en algún conjunto de indices I es una cubierta (o una cubierta abierta) de un conjunto S, si S está contenido en su unión: $S \subset \cup_{\alpha \in I} U_\alpha$; La colección de todos los discos abiertos de radio 2 es una cubierta de $\mathbb{C}$: $U_z = B(z, 2), \quad \mathbb{C} \subset \cup_{z \in \mathbb{C}} B(z, 2)$.

Definición 2.2.11. Un conjunto $S \subset \mathbb{C}$ es compacto si toda cubierta de S tiene una subcubierta finita. Se puede probar que un conjunto $\Omega \subseteq \mathbb{C}$ es compacto si y solo si es cerrado y acotado.

El semiplano $\Omega_3 = \{z \in \mathbb{C} : \operatorname{Re} z > 0\}$ es un dominio no acotado (ver Figura 2.9, izquierda); el sector $\Omega_4 = \{z \in \mathbb{C} : \frac{\pi}{4} \leq \operatorname{Arg} z \leq \frac{\pi}{3}\}$ es una región cerrada no acotada (ver Figura 2.9, derecha).

Definición 2.2.12. Un punto z_0 se llama punto de acumulación para algún $z \in \Omega : z \neq z_0$. Se sigue que si, Ω es cerrado, entonces contiene todos sus puntos de acumulación. De hecho, si un punto de acumulación z_0 no pertenecía a Ω, necesariamente sería frontera para Ω; pero esto contradice el hecho de que un conjunto cerrado contiene todos sus puntos de la frontera. No es difícil comprobar que lo contrario también es cierto y por lo tanto un conjunto es cerrado si y solo si contiene todos sus puntos de acumulación.

Todo punto de Ω_1 es de acumulación para Ω_1; el conjunto de puntos de acumulación de $B_r(z_0)$ es el conjunto $\{z \in \mathbb{C} : |z - z_0| \leq r\}$; mientras que el único punto de acumulación de $\Omega_5 = \{z \in \mathbb{C} : z = \frac{i}{n},\ n = 1, 2, \dots\}$ es el origen.

[13] Sean $z_1, z_2, \dots, z_n \in \mathbb{C}$; los $n-1$ segmentos $\overline{z_1 z_2}, \overline{z_2 z_3}, \dots, \overline{z_{n-1} z_n}$, tomados en sucesion, forman una curva llamada líneal poligonal.

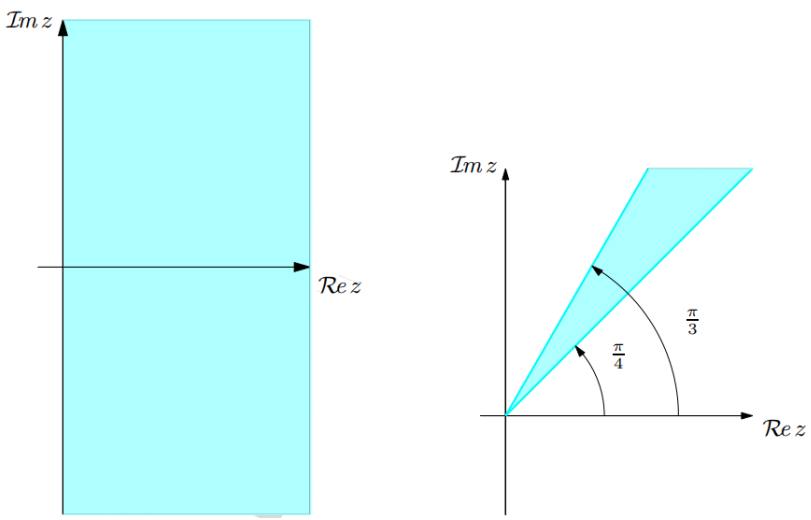


Figura 2.9: El conjunto Ω_3, a la derecha, y el conjunto Ω_4, a la izquierda.

El punto en el infinito

A veces es conveniente incluir el punto en el infinito en el plano complejo, denotado por ∞. El plano complejo con este punto ahora se llama plano complejo extendido o de Gauss. Para visualizar el punto en el infinito, podemos piense en el plano complejo como el plano que pasa por el ecuador de una esfera unidad centrada en el punto $z = 0$ (ver Figura 2.10). En cada punto z en el plano corresponde exactamente a un punto P en la superficie de la esfera. El punto P está determinada por la intersección de la línea que pasa por z y el polo norte N de la esfera con la superficie de la esfera. Por el contrario, en cada punto P de la esfera, que no es el polo norte N, corresponde exactamente a un punto z del plano. Haciendo corresponden al punto N de la esfera con el punto ∞, obtenemos una correspondencia biyectiva entre los puntos de la esfera y los puntos del plano gaussiano.
La esfera se conoce con el nombre de la esfera de Riemann y la correspondencia como proyección estereográfica.

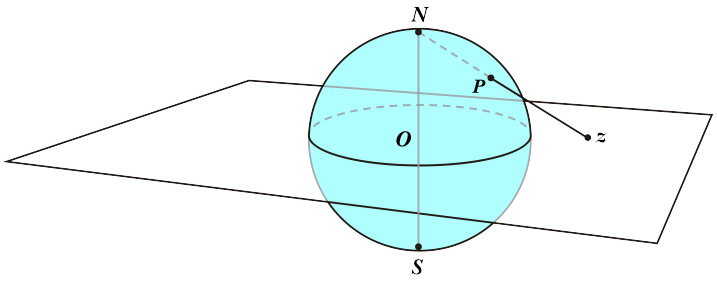


Figura 2.10: La proyección estereográfica.

Observamos que el exterior del círculo unitario centrado en el origen en el plano complejo corresponde al hemisferio superior (sin el ecuador y el polo norte). Es más, para todo $r > 0$, los

puntos del plano complejo fuera de la circunferencia $|z| = r$ corresponden a puntos de la esfera cercanos a N. Por lo tanto, llamaremos vecindad del punto al infinito a todo conjunto (abierto) $B_r(\infty) = \{z \in \mathbb{C} : |z| > r\}$.

Dado un conjunto $\Omega \subseteq \mathbb{C}$, si todo entorno de ∞ contiene al menos un punto de Ω diremos que ∞ es un punto de acumulación de Ω. Por ejemplo, ∞ es un punto de acumulación para el conjunto $\Omega_6 = \{z \in \mathbb{C} : z = ni,\ n \in N\}$, así como para el semiplano $\Omega_7 = \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$. Notamos que un conjunto Ω es no acotado si y solo si ∞ es uno de sus puntos de acumulacion. En lo siguiente z siempre denotará un punto en el plano finito, con lo cual el punto ∞ se señalará explícitamente.

2.3. Funciones complejas

Definición 2.3.1. Una función $w = f(z)$ que asigna un número complejo z a un número complejo w se llama **función de variable compleja**.
Tengamos en cuenta que su dominio de definición $\Omega \subseteq \mathbb{C}$ no es necesariamente un dominio (conjunto abierto y conexo). Por ejemplo, $f_1(z) = z$ está definida en todo $\mathbb{C}$ mientras que $f_2(z) = \frac{1}{z}$ está definida en $\mathbb{C} \setminus \{0\}$. Si el dominio de definición no se establece explícitamente, la función se entiende definida sobre el conjunto más amplio posible, compatible con la expresión de la función.

Dado que tanto el conjunto de origen como el de destino son 2-dimensionales, no es en general posible dibujar la gráfica de la función $w = f(z)$. Nos limitaremos a identificar el dominio y la imagen (cuando sea posible) de la función dibujándolos por separado. Por ejemplo, consideremos $f_3(z) = \bar{z}$ restringida al semiplano superior $\operatorname{Im} z > 0$. Entonces su imagen es el semiplano inferior $Imz < 0$ recordemos que $\bar{z} = x - iy$, (ver Figura 2.11).

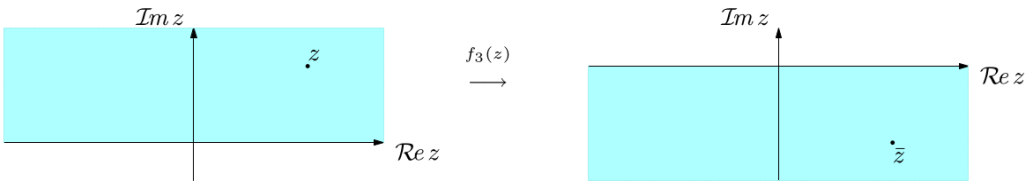


Figura 2.11: Dominio e imagen de la función $f_3(z) = \bar{z}$ restringida al semiplano superior $\operatorname{Im} z > 0$.

Ahora, sea la función $f_4(z) = z^2$ restringida a $\operatorname{Im} z \geq 0$. Entonces, usando la representación polar $z = re^{i\theta}$, $0 \leq \theta \leq \pi$, del genérico z perteneciente al dominio de definición de $f4$, vemos que $w = z^2 = r^2 e^{2i\theta} = Re^{i\varphi}$ habiendo hecho $R = r^2$ y $\varphi = 2\theta$. Por lo tanto la imagen es todo el plano complejo ya que $R \geq 0$ y $0 \leq \varphi < 2\pi$. (ver Figura 2.12).

Cada función $w = f(z)$ de variable compleja puede, por supuesto, ser pensada como una función de $\mathbb{R}^2$ a $\mathbb{R}^2$. De hecho, haciendo $z = x + iy$ y $w = u + iv$, $f(z)$ se puede escribir como

$$w = f(z) = u(x, y) + iv(x, y)\ ,$$

donde u, v son dos funciones reales de las dos variables reales x e y.

Definición 2.3.2. Llamaremos función **parte real** de f a la función $u(x, y) = \operatorname{Re} f(z)$.

Definición 2.3.3. Llamaremos función **parte imaginaria** de f a la función $v(x,y) = \operatorname{Im} f(z)$.

Algunos ejemplos:

$$f_1(z) = z = x + iy\ , \qquad u(x,y) = x\ , \qquad v(x,y) = y\ .$$

$$f_2(z) = \frac{1}{z} = \frac{x}{x^2+y^2} - i\ \frac{y}{x^2+y^2}\ , \quad u(x,y) = \frac{x}{x^2+y^2}, \quad v(x,y) = -\ \frac{y}{x^2+y^2}\ .$$

$$f_3(z) = \bar{z} = x - iy\ , \qquad u(x,y) = x\ , \qquad v(x,y) = -y\ .$$

$$f_4(z) = z^2 = x^2 - y^2 + 2ixy\ , \qquad u(x,y) = x^2 - y^2\ , \quad v(x,y) = 2xy\ .$$

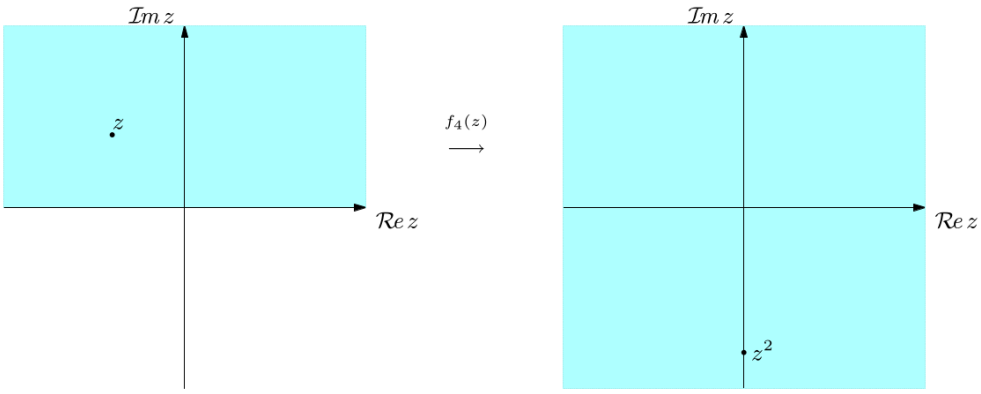


Figura 2.12: Dominio e imagen de la función $f_4(z) = z^2$ restringida al semiplano superior $\operatorname{Im} z \geq 0$.

Definición 2.3.4. Dado un entero $n \in \mathbb{N}$ y $n+1$ constantes complejas $a_j \in \mathbb{C}$, $j = 0, 1, \ldots, n$, la función $P(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_n z^n$ se dice **polinomio**; si $a_n \neq 0$, n indica el grado del polinomio. Está definida en todo $\mathbb{C}$.

Definición 2.3.5. Una **función racional** es el cociente de dos polinomios $P(z)$ y $Q(z)$

$$R(z) = \frac{P(z)}{Q(z)}$$

y está definida para todo $z \in \mathbb{C} :\ Q(z) \neq 0$.

Definición 2.3.6. Función exponencial, para $z = x + iy$, tenemos

$$e^z = e^x e^{iy} = e^x(\cos y + i\ \operatorname{sen}\ y)\ ,$$

entonces $e^z = u(x,y) + iv(x,y)$, con $u(x,y) = e^x \cos y$ y $v(x,y) = e^x \operatorname{sen}\ y$, está definida sobre todo $\mathbb{C}$. Directamente de (La definición 2.3.6.) obtenemos que, para cada $z = x + iy$, $z_1, z_2 \in \mathbb{C}$ y $n \in \mathbb{Z}$, tenemos

$$e^{z_1+z_2} = e^{z_1} e^{z_2}\ , \qquad (e^z)^n = e^{nz}\ , \qquad e^0 = 1\ ,$$
$$|e^z| = e^x\ , \qquad \arg e^z = y\ , \qquad \overline{e^z} = e^{\bar{z}}.$$

Observamos que $|e^z| = e^x > 0$ para todo z y por lo tanto

$$e^z \neq 0 \ , \qquad \forall z \in \mathbb{C} \ .$$

Por lo tanto la imagen de la función exponencial es todo $\mathbb{C}$ menos el origen. Además la función es periódica con un período imaginario igual a $2\pi i$; En efecto

$$e^{z+2\pi i} = e^z e^{2\pi i} = e^z(\cos 2\pi + 1 \text{ sen } 2\pi) = e^z \ , \qquad \forall z \in \mathbb{C} \ .$$

Definición 2.3.7. Funciones trigonométricas, sea $x \in \mathbb{R}$, de las siguientes expresiones

$$e^{ix} = \cos x + i \text{ sen } x \ , \qquad e^{-ix} \cos x - i \text{ sen } x \ ,$$

se sigue que

$$\text{sen } x = \frac{e^{ix} - e^{-ix}}{2i} \ , \qquad \cos x = \frac{e^{ix} + e^{-ix}}{2} \ .$$

Por lo tanto, es natural definir las funciones seno y coseno de la variable compleja z como

$$\text{sen } z = \frac{e^{iz} - e^{-iz}}{2i} \ , \qquad \cos z = \frac{e^{iz} + e^{-iz}}{2} \ .$$

Las otras funciones trigonométricas se definen en términos de las funciones seno y coseno según las relaciones usuales:

$$\tan z = \frac{\text{sen} z}{\cos z} \ , \qquad \cot z = \frac{\cos z}{\text{sen } z} \ ,$$

$$\sec z = \frac{1}{\cos z} \ , \qquad \csc z = \frac{1}{\text{sen } z} \ .$$

Todas las identidades trigonométricas habituales se derivan directamente de las definiciones; por ejemplo, para todo $z, z_1, z_2 \in \mathbb{C}$, tenemos

$$\text{sen } z + \cos z = 1 \ , \quad \text{sen}(z_1 + z_2) = \text{sen } z_1 \cos z_2 + \cos z_1 \text{ sen } z_2 \ .$$

La periodicidad de $\text{sen} z$ y $\cos z$ se deriva de la definición y de la periodicidad de e^z:

$$\text{sen}(z + 2\pi) = \text{sen } z \ , \quad \cos(z + 2\pi) = \cos z \ , \quad \forall z \in \mathbb{C} \ ,$$

así como el de las demás funciones trigonométricas; Por ejemplo

$$\tan(z + \pi) = \tan z \ , \quad \forall z \in \mathbb{C} \ .$$

Hacemos explícita la parte real y la parte imaginaria de la función $f(z) = \text{sen } z$; para $z = x + iy$, tenemos

$$\text{sen } z = \frac{e^{i(x+iy)} - e^{-i(x+iy)}}{2i} = \frac{e^{-y}(\cos x + i \text{ sen } x)}{2i} - \frac{e^{y}(\cos x - i \text{ sen } x)}{2i}$$

$$\Rightarrow \quad \text{sen } z = \text{sen } x \ \frac{e^y + e^{-y}}{2} + i \ \cos x \ \frac{e^y - e^{-y}}{2}$$

$$\Rightarrow \quad \text{sen } z = \text{sen } x \ \cosh y + i \ \cos x \ \text{senh } y \ ,$$

y así $u(x,y) = \text{sen } x \ \cosh y$ y $v(x,y) = \cos x \ \text{senh } y$.

Análogamente se obtiene

$$\cos z = \cos x \cosh y - i \ \text{sen } x \ \text{senh } y.$$

De estas expresiones se sigue inmediatamente que[14]

$$\overline{\text{sen } z} = \text{sen } \overline{z} \ , \quad \overline{\cos z} = \cos \overline{z} \ ,$$

$$|\text{sen } z|^2 = \text{sen}^2 z + \text{senh}^2 y \ , \quad |\cos z|^2 = \cos^2 z + \text{senh}^2 y \ .$$

Finalmente, las dos últimas igualdades nos permiten obtener los ceros de las funciones seno y coseno:

$$\text{sen } z = 0 \quad \Leftrightarrow \quad \text{sen}^2 x + \text{senh}^2 y = 0 \quad \Leftrightarrow$$

$$\text{sen } x = 0 \ \wedge \ \text{senh } y = 0 \quad \Leftrightarrow \quad x = k\pi (k \in \mathbb{Z}) \ \wedge \ y = 0 \ ,$$

así

$$\text{sen } z = 0 \quad \Leftrightarrow \quad z = k\pi \ , \quad k \in \mathbb{Z} \ ,$$

análogamente

$$\cos z = 0 \quad \Leftrightarrow \quad z = (k + 1/2)\, \pi \ , \quad k \in \mathbb{Z} \ .$$

De las dos últimas expresiones nos permiten obtener el dominio de definición de las funciones trigonométrica definidas enteriormente; por ejemplo, la función tangente se define en $\mathbb{C}$ excepto puntos $z = (k + 1/2)\pi \ , \ k \in \mathbb{Z}$.

Definición 2.3.8. Funciones hiperbólicas, generalizando las fórmulas

$$\text{senh } x = \frac{e^x - e^{-x}}{2} \ , \quad \cosh x = \frac{e^x + e^{-x}}{2} \ ,$$

válido para todo $x \in \mathbb{R}$, suponiendo de forma natural

$$\text{senh } z = \frac{e^z - e^{-z}}{2} \ , \quad \cosh z = \frac{e^z + e^{-z}}{2} \ ,$$

para todo $z \in \mathbb{C}$. Análogamente al caso real es posible definir las funciones tangente, cotangente, secante y cosecante hiperbólica. Las definiciones usuales siguen relaciones hiperbólicas como, por ejemplo

$$\cosh^2 z - \text{senh}^2 z = 1 \ , \quad \forall z \in \mathbb{C} \ .$$

El seno y el coseno hiperbólicos son funciones periódicas de período $2\pi i$, mientras que la tangente hiperbólica es de período πi.
Las funciones seno y coseno hiperbólico están estrechamente relacionadas con sus análogas funciones trigonométricas; así, obtenemos

$$\text{senh } iz = i \ \text{sin } z \ , \quad \cosh iz = \cos z \ ,$$

$$\text{sen } iz = i \ \text{senh } z \ , \quad \cos iz = \cosh z \ .$$

Además, haciendo $z = x + iy$, tenemos

$$\text{senh } z = \text{senh } x \ \cos y + i \ \cosh x \ \text{sen } y \ , \quad \cosh z = \cosh x \cos y + i \ \text{senh } x \ \text{sen } y \ ,$$

[14] Recordando que $\cosh^2 x - \text{senh}^2 x = 1 \ , \quad \forall x \in \mathbb{R}$.

$$|\text{senh } z| = \text{senh } x + \text{sen } y \ , \quad |\cosh z|^2 = \text{senh}^2 x + \cos^2 y \ .$$

Finalmente

$$\text{senh } z = 0 \quad \Leftrightarrow \quad z = k\pi i \ , \ \ k \in \mathbb{Z} \ ,$$
$$\cosh z = 0 \quad \Leftrightarrow \quad z = \left(k + \frac{1}{2}\right)\pi i \ , \ \ k \in \mathbb{Z} \ .$$

Definición 2.3.9. Función logaritmo, Denotamos por $\text{Log } r$ el logaritmo natural de un número real y positivo r, considerado $z = re^{i\theta} \neq 0$, usando formalmente las propiedades conocidas del logaritmo, tenemos

$$\log z = \log re^{i\theta} = \text{Log } r + i\theta \ , \quad \text{con} \ \ r = |z| \ \ \text{y} \ \ \theta = \arg z \ .$$

Como $\arg z = \text{Arg } z + 2k\pi \ , \ \ k \in \mathbb{Z}$, la expresión del renglón anterior no define una unívoca función única si una función multivaluada, i.e., a cada $z \neq 0$, le corresponden infinitos valores de $\log z$ que tienen todos la misma parte real ($\text{Re} \log z = \text{Log } r$) y parte imaginaria que difiere para un múltiplo entero de 2π. Llamaremos al **valor principal** de $\log z$ al valor obtenido al establecer $\theta = \text{Arg } z$. Este valor se denota $\text{Log } z$ y por lo tanto es dada por la ecuación

$$\text{Log } z = \text{Log } |r| + i \ \text{Arg } z \ .$$

La función $w = \text{Log } z$ es una función cuyo dominio de definición es $\mathbb{C}\backslash\{0\}$ y cuya la imagen es la franja $-\pi < \text{Im}\, w \leq \pi$. Observamos que $\text{Log } z$ se reduce al habitual logaritmo natural de una variable real cuando el dominio de definición está restringido al semieje de reales positivos.
Se necesita cierta cautela al extender las propiedades conocidas de los logaritmos. Primero, verifiquemos que

$$e^{\log z} = z \ .$$

Esto significa que no importa qué valor de $\log z$ elijamos, el número $e^{\log z}$ siempre será z.
Para verificar esta igualdad, escribimos $z = re^{i\theta}$ y $\log z = \text{Log } r + i\theta$. Entonces

$$e^{\log z} = e^{\text{Log } r + i\theta} = e^{\text{Log } r} e^{i\theta} = re^{i\theta} = z \ .$$

Generalmente no es cierto que $\log e^z = z$. De hecho, si $z = x + iy$, tenemos

$$\log e^z = \text{Log } |e^z| + i \ \arg e^z = x + i(y + 2k\pi) = z + 2k\pi \ , \quad k \in \mathbb{Z} \ .$$

Para cada $z_1, z_2 \in \mathbb{C}\backslash\{0\}$ las relaciones se cumplen

$$\log z_1 z_2 = \log z_1 + \log z_2 \ , \quad \log \frac{z_1}{z_2} = \log z_1 - \log z_2 \ .$$

Estas igualdades deben entenderse en el sentido de que, por ejemplo, cualquier valor de $\log z_1 z_2$ se puede expresar como la suma de un valor de $\log z_1$ y un valor de $\log z_2$, o viceversa, cada valor de $\log z_1$ sumado con un valor de $\log z_2$ es un valor de $\log z_1 z_2$.

Para verificar que $\log z_1 z_2 = \log z_1 + \log z_2$, establezcamos que $z_1 = r_1 e^{i\theta_1}$, $z_2 = r_2 e^{i\theta_2}$ recordando que $\arg(z_1 z_2) = \arg z_1 + \arg z_2$, tenemos

$$\log z_1 z_2 = \log r_1 r_2 e^{i(\theta_1 + \theta_2)} = \text{Log } r_1 r_2 + i(\theta_1 + \theta_2)$$
$$\Rightarrow \quad \log z_1 z_2 = \text{Log } r_1 + i\theta_1 + \text{Log } r_2 + i\theta_2 \quad \Rightarrow \quad \log z_1 z_2 = \log z_1 + \log z_2 \ .$$

Para $\log(z_1/z_2) = \log z_1 - \log z_2$ se demuestra de manera análoga. Nótese que (las dos igualdades que estamos demostrando para el logaritmo) no son válidos reemplazando log por Log. Por ejemplo, para $z_1 = z_2 = -1 = e^{i\pi}$ tenemos $\text{Log } z_1 = \text{Log } z_2 = \pi i$ mientras que $\text{Log } z_1 z_2 = 0$, y por lo tanto

$$\text{Log } z_1 z_2 = 0 \neq 2\pi i = \text{Log } z_1 + \text{Log } z_2 \ .$$

2.4. Límites y continuidad

Los conceptos de límite y continuidad son similares a los ya estudiados para funciones de variable real y por lo tanto nuestra discusión será concisa. Damos la siguiente definición.

Definición 2.4.1. Sea $f : \Omega \to \mathbb{C}$ y sea z_0 un punto de acumulación para el dominio Ω. Decimos que f tiene límite $l \in \mathbb{C}$ (o tiende a l) cuando z tiende a z_0 y escribimos

$$\lim_{z \to z_0} f(z) = l \ ,$$

si para todo $\epsilon > 0$ existe un $\delta > 0$ tal que

$$\forall z \in \Omega \ , \quad 0 < |z - z_0| < \delta \quad \Rightarrow \quad |f(z) - l| < \epsilon \ .$$

Con el lenguaje de vecindades: para toda vecindad $B_\epsilon(l)$ de l existe una vecindad $B_\delta(z_0)$ de z_0 tal que

$$\forall z \in \Omega \ , \quad z \in B_\delta(z_0) \backslash \{z_0\} \quad \Rightarrow \quad f(z) \in B_\epsilon(l) \ .$$

La definición de límite se ilustra gráficamente en la Figura 2.13.
La definición de límite obviamente puede extenderse al caso donde z_0 o l o ambos son el punto en el infinito ∞, usando la formulación de las vecindades. Por ejemplo

$$\lim_{z \to \infty} f(z) = l \in \mathbb{C} \ ,$$

equivale a decir que para toda vecindad $B_\epsilon(l)$ de l existe una vecindad $B_R(\infty)$ de ∞ tal que

$$\forall z \in \Omega \ , \quad z \in B_R(\infty) \quad \Rightarrow \quad f(z) \in B_\epsilon(l) \ ,$$

i.e., para todo $\epsilon > 0$ existe un $R > 0$ tal que

$$\forall z \in \Omega \ , \quad |z| > R \quad \Rightarrow \quad |f(z) - l| < \epsilon \ .$$

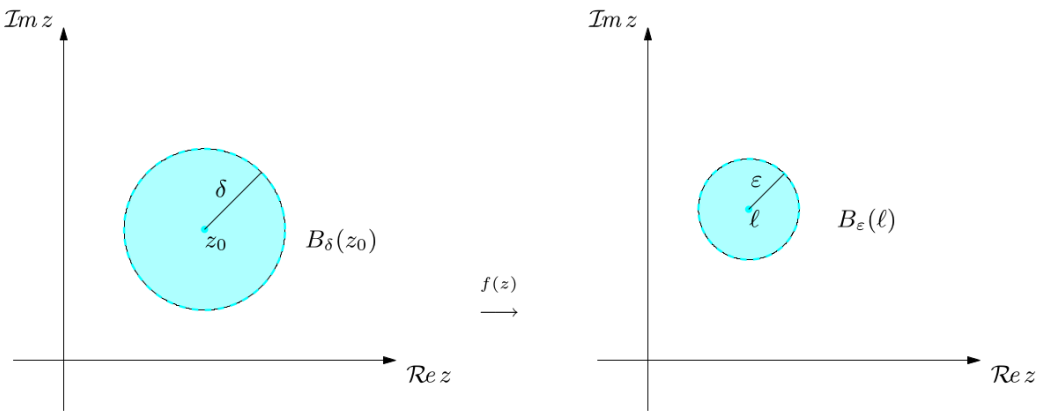


Figura 2.13: Representación gráfica de la definición de límite.

Ejemplo:

a) Comprobemos que $\lim_{z \to 1} iz = i$. Para todo $\epsilon > 0$, la condición

$$|f(z) - l| < \epsilon \quad \text{equivale a} \quad |iz - i| = |z - 1| < \epsilon \ .$$

Entonces $(\forall z \in \Omega\ ,\ 0 < |z - z_0| < \delta\ \Rightarrow\ |f(z) - l| < \epsilon)$ se verifica con $\delta = \epsilon$.

b) Comprobemos que $\lim_{z\to\infty} \frac{1}{z^2}$ dado que

$$\left|\frac{1}{z^2} - 0\right| < \epsilon \quad \text{equivale a} \quad |z| > \frac{1}{\sqrt{\epsilon}}\ .$$

$(\forall z \in \Omega\ ,\ |z| > R\ \Rightarrow\ |f(z) - l| < \epsilon)$ se satisface con $R = \frac{1}{\sqrt{\epsilon}}$.

Teorema 2.4.2. Sea z_0 un punto de acumulación para el dominio de definición de una función f, supongamos que

$$f(z) = u(x, y) + iv(x, y)\ ,\quad z_0 = x_0 + iy_0\ ,\quad l = l_{re} + il_{im}\ ,$$

entonces

$$\lim_{z\to z_0} f(z) = l \quad \Longleftrightarrow \quad \begin{cases} \lim_{(x,y)\to(x_0,y_0)}\ u(x, y) = l_{re}\ , \\ \lim_{(x,y)\to(x_0,y_0)}\ v(x, y) = l_{im}\ . \end{cases}$$

Teorema 2.4.3. Sea z_0 un punto de acumulación para el dominio de definición de dos funciones f y g, supongamos que

$$\lim_{z\to z_0} f(z) = l \quad \wedge \quad \lim_{z\to z_0} g(z) = m\ ,$$

entonces

$$\lim_{z\to z_0} [f(x) \pm g_x] = l \pm m\ ,$$
$$\lim_{z\to z_0} [f(x) \cdot g_x] = l \cdot m\ ,$$
$$\lim_{z\to z_0} \frac{f(x)}{g(x)} = \frac{l}{m}\ ,\quad m \neq 0\ .$$

Teorema 2.4.4. Sea z_0 un punto de acumulación para el dominio de definición de una función f, entonces

$$\lim_{z\to z_0} f(z) = l \quad \Rightarrow \quad \lim_{z\to z_0} |f(z)| = |l|\ .$$

Usando la definición de límite y los resultados que acabamos de exponer, inmediatamente tenemos que, si $P(z)$ y $Q(z)$ son dos polinomios, entonces

$$\lim_{z\to z_0} P(z) = P_{z_0}\ ,\qquad \lim_{z\to z_0} \frac{P_z}{Q_z} = \frac{P_{z_0}}{Q_{z_0}}\ ,\quad (Q(z_0 \neq 0))\ .$$

Continuidad

Teorema 2.4.5. Sea $\Omega \subseteq \mathbb{C}$ una región y sea $f : \Omega \to \mathbb{C}$. Decimos que f es continua en $z_0 \in \Omega$ si

$$\lim_{z\to z_0} f(z) = f(z_0)\ .$$

Diremos que f es continua en una región Ω si es continua en todo punto $z_0 \in \Omega$.
Recordando el Teorema 2.4.3., si dos funciones son continuas en un punto z_0 entonces también la suma, la diferencia, el producto son funciones continuas en $z0$, el cociente es continuo mientras la función del denominador no sea cero en $z0$. También es posible verificar, directamente de la definición, que la composición de funciones continuas es una función continua, del Teorema 2.4.2., se sigue que una función f de variable compleja es continua en $z_0 = (x_0, y_0)$ si y solo si sus partes real e imaginaria u y v son continuas en (x_0, y_0). Resumiendo y usando las definiciones dadas en la Sección 2.3, se cumple el siguiente resultado.

Teorema 2.4.6. Todas las funciones elementales (polinomios, funciones racionales, funciones exponenciales, funciones trigonométricas e hiperbólicas, funciones logarítmicas) son continuas en su dominio de definición.

2.5. Funciones analíticas

Derivabilidad

En cuanto a las funciones de variable real, también para las funciones de variable compleja se puede introducir el concepto de derivada en un punto, obtenida como límite de las razones incrementales de la función, en el punto considerado.

Definición 2.5.1. Sea f una función de variable compleja, definida en una vecindad de $z_0 \in \mathbb{C}$. Se dice que es diferenciable en z_0, y su derivada se denota $f'(z_0)$, si existe el limite finito

$$f'(z_0) = \lim_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0} \ .$$

Otros símbolos que se usan a menudo para indicar la derivada en z_0 son $\frac{df}{dz}(z_0)$, $Df(z_0)$. Haciendo $\Delta z = z - z_0$, le expresión anterior se puede reescribir en la forma:

$$f'(z_0) = \lim_{\Delta z \to 0} \frac{f(z_0 + \Delta z) - f(z_0)}{\Delta z} \ .$$

Es sencillo verificar que si una función es derivable en un punto z_0, entonces también es continua allí. En efecto

$$\begin{aligned} \lim_{z \to z_0} (f(z) - f(z_0)) &= \lim_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0}(z - z_0) \\ &= \lim_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0} \lim_{z \to z_0} (z - z_0) = f'(z_0) \cdot 0 = 0 \ , \\ \vee \quad \lim_{z \to z_0} f(z) &= f(z_0) \ . \end{aligned}$$

Definición 2.5.2. Sea $\Omega \subseteq \mathbb{C}$ un conjunto abierto no vacío, y sea $f : \Omega \to \mathbb{C}$ una función de variable compleja. Si f es diferenciable en todo punto $z_0 \in \Omega$, decimos que f es **analítica** u **holomorfa** en Ω.

Finalmente, se dice que una función f es **entera** si es holomorfa en todo el plano complejo.

Podemos decir por ejemplo que las funciones $f(z) = z$ y $f(z) = z^2$ son funciones enteras, mientras que la función $f(z) = |z|^2$ no es es analítica en cualquier conjunto abierto, ya que su derivada existe sólo en el punto $z = 0$.

Tengamos en cuenta que la definición de la derivada es formalmente idéntica a la aprendida para funciones reales de variable real. De hecho, las reglas de derivación y las derivadas de las funciones elementales son análogas a las de funciones de variable real. Con técnicas completamente análogas a las de variable real, es posible demostrar que se cumplen los siguientes resultados.

Teorema 2.5.3. Sean f y g dos funciones diferenciables en un punto $z_0 \in \mathbb{C}$. Entonces son derivables las funciones suma $f(z)+g(z)$, la función producto $f(z)g(z)$ y, si $g(z0) \neq 0$, también la función cociente $\frac{f(z)}{g(z)}$ también se tiene:

$$(f+g)'(z_0) = f'(z_0) + g'(z_0) \ ,$$

$$(fg)'(z_0) = f'(z_0)g(z_0) + f(z_0)g'(z_0) \ ,$$

$$\left(\frac{f}{g}\right)'(z_0) = \frac{f'(z_0)g(z_0) - f(z_0)g'(z_0)}{g(z_0)^2} \ .$$

Teorema 2.5.4. Sea $f(z)$ una función diferenciable en un punto $z_0 \in \mathbb{C}$. Entonces sea $g(w)$ una función diferenciable en el punto $w_0 = f(z_0)$. Entonces la función compuesta $g \circ f(z) = g(f(z))$ es diferenciable en z_0 y se tiene:

$$(g \circ f)'(z_0) = g'(w_0)f'(z_0) = g'(f(z_0))f'(z_0) \ .$$

Condiciones de Cauchy-Riemann

Supongamos que una función f está definida en un conjunto abierto $\Omega \subseteq \mathbb{C}$ de la ecuacion:

$$f(z) = u(x,y) + iv(x,y) \ , \quad z = x + iy \in \Omega \ ,$$

donde las dos funciones reales $u : \Omega \to \mathbb{R}$ y $v : \Omega \to \mathbb{R}$ son, respectivamente, la parte real y la parte imaginaria de la función f.

En esta sección estudiaremos las condiciones necesarias y suficientes de las funciones u y v, de modo que la función f es holomorfa en el conjunto abierto Ω.

Teorema 2.5.5. Sea Ω un conjunto abierto del plano complejo, y sea $f : \Omega \to \mathbb{C}$ una función de variable compleja. Luego, indicando con $u(x,y)$ y $v(x,y)$ la parte real y la parte imaginaria de f, las siguientes dos condiciones son equivalentes entre sí:

1. La función f es holomorfa en Ω.
2. Las dos funciones $u(x,y)$ y $v(x,y)$ son de clase C^1 en Ω (i.e., tienen primeras derivadas parciales continuas en Ω) y cumplen las condiciones de Cauchy-Riemann:

$$\begin{cases} \dfrac{\partial u}{\partial x}(x_0,y_0) = \quad \dfrac{\partial v}{\partial y}(x_0,y_0) \ , \\ \dfrac{\partial u}{\partial y}(x_0,y_0) = -\dfrac{\partial v}{\partial x}(x_0,y_0) \ , \end{cases}$$

para todo punto $(x_0, y_0) \in \Omega$.
Además, si f es holomorfa, la derivada compleja se expresa en función de las derivadas parciales de u y v como

$$f'(z) = \frac{\partial u}{\partial x}(x,y) + i\frac{\partial v}{\partial x}(x,y) = \frac{\partial v}{\partial y}(x,y) - i\frac{\partial u}{\partial y}(x,y) \ .$$

Demostración:
Empezamos con la implicación 1. $\Rightarrow$ 2. La idea de la prueba consiste en calcular el límite ($f'(z_0) = \lim_{\Delta z \to 0} \frac{f(z_0+\Delta z)-f(z_0)}{\Delta z}$) de dos maneras: primero a lo largo del eje real (i.e., considerando incrementos reales $\Delta z = \Delta x$) y luego a lo largo del eje imaginario (i.e., considerando incrementos

imaginarios puros, del tipo $\Delta z = i\Delta y$). Por ejemplo, tomado un punto $z_0 = x_0 + iy_0 \in \Omega$ y un incremento real $\Delta z = \Delta x$, tenemos

$$\frac{f(z_0+\Delta z)-f(z_0)}{\Delta z} = \frac{u(x_0+\Delta x, y_0)-u(x_0,y_0)}{\Delta x} + i\frac{v(x_0+\Delta x,y_0)-v(x_0,y_0)}{\Delta x}$$

y, haciendo que el incremento $\Delta z = \Delta x$ tienda a cero, encontramos

$$f'(z_0) = \frac{\partial u}{\partial x}(x_0,y_0) + i\frac{\partial v}{\partial x}(x_0,y_0)$$

(observando que el límite del primer miembro, es decir, $f'(z_0)$, existe por hipótesis y, por lo tanto, por el Teorema 2.4.2., existen también los límites correspondientes de la parte real y de la parte imaginaria presente en el miembro derecho, i.e., las derivadas parciales u_x y v_x). Análogamente, con incrementos imaginarios puros $\Delta z = i\Delta y$ tenemos

$$\begin{aligned}\frac{f(z_0+\Delta z)-f(z_0)}{\Delta z} &= \frac{u(x_0,y_0+\Delta y)-u(x_0,y_0)}{\Delta y} + i\frac{v(x_0,y_0+\Delta y)-v(x_0,y_0)}{i\Delta y} \\ &= -i\frac{u(x_0,y_0+\Delta y)-u(x_0,y_0)}{\Delta y} + \frac{v(x_0,y_0+\Delta y)-v(x_0,y_0)}{i\Delta y}\end{aligned}$$

y luego pasando al límite encontramos

$$f'(z_0) = -i\frac{\partial u}{\partial y}(x_0,y_0) + \frac{\partial v}{\partial y}(x_0,y_0)\ .$$

Comparando con $(f'(z_0) = \frac{\partial u}{\partial x}(x_0,y_0) + i\frac{\partial v}{\partial x}(x_0,y_0))$ encontramos $(f'(z) = \dfrac{\partial u}{\partial x}(x,y) + i\dfrac{\partial v}{\partial x}(x,y) = \dfrac{\partial v}{\partial y}(x,y) - i\dfrac{\partial u}{\partial y}(x,y))$, y las condiciones de Cauchy-Riemann se sigue de $(f'(z) = \dfrac{\partial u}{\partial x}(x,y) + i\dfrac{\partial v}{\partial x}(x,y) = \dfrac{\partial v}{\partial y}(x,y) - i\dfrac{\partial u}{\partial y}(x,y))$, igualando las partes real e imaginaria de las dos expresiones. No probamos aquí la continuidad de las derivadas parciales de u y v.

Ahora, la implicación $2. \Rightarrow 1.$, y por lo tanto supongamos que u y v son de clase C^1 (y por lo tanto diferenciables). Tomando un punto (x_0,y_0), supongamos por simplicidad

$$A = \frac{\partial u}{\partial x}(x_0,y_0)\ ,\quad B = \frac{\partial u}{\partial y}(x_0,y_0)\ ,\quad C = \frac{\partial v}{\partial x}(x_0,y_0)\ ,\quad D = \frac{\partial v}{\partial y}(x_0,y_0)\ ,$$

y considerando la expansión de Taylor de primer orden

$$\begin{aligned}u(x_0+h,y_0+k) &= u(x_0,y_0) + Ah + Bk + \epsilon_1(h,k)\ , \\ v(x_0+h,y_0+k) &= v(x_0,y_0) + Ch + Dk + \epsilon_2(h,k)\ ,\end{aligned}$$

donde los "errores" $\epsilon_1(h,k)$ y $\epsilon_2(h,k)$ son infinitesimales de orden superior a $\sqrt{h^2+k^2}$ para $(h,k)\to(0,0)$, i.e.

$$\lim_{(h,k)\to(0,0)} \frac{|\epsilon_1(h,k)|}{\sqrt{h^2+k^2}} = \lim_{(h,k)\to(0,0)} \frac{|\epsilon_2(h,k)|}{\sqrt{h^2+k^2}} = 0\ .$$

Por tanto, considerando el incremento complejo $\Delta z = h + ik$, tenemos que

$$f(z_0+\Delta z) - f(z_0) = Ah + Bk + \epsilon_1(h,k) + i(Ch + Dk + \epsilon_2(h,k))\ .$$

Por otro lado, tenemos $A = D$ y $B = -C$ gracias a las condiciones de Cauchy-Riemann, luego eliminando D y B obtenemos

$$f(z_0+\Delta z) - f(z_0) = A(h+ik) + C(ih-k) + \epsilon_1(h,k) + i\epsilon_2(h,k)$$

$$= A(h+ik) + iC(h+ik) + \epsilon_1(h,k) + i\epsilon_2(h,k)$$

$$= (A+iC)\Delta z + \epsilon_1(h,k) + i\epsilon_2(h,k)\ .$$

Dado que $|\Delta z| = \sqrt{h^2+k^2}$, gracias a que los límites son iguales entre sí e iguales a cero, el término $\epsilon_1 + i\epsilon_2$ es un infinitesimal de orden superior a Δz, cuando Δz tiende a cero. Por lo tanto, dividiendo por Δz en la expresión $(f(z_0+\Delta z)-f(z_0) = A(h+ik)+C(ih-k)+\epsilon_1(h,k)+i\epsilon_2(h,k))$ y pasando al límite, obtenemos que $f'(z_0)$ existe y coincide con $A+iC$ (por lo tanto también con $D-iB$), demostrando así la derivabilidad en el punto z_0 y la validez de $f'(z) = \dfrac{\partial u}{\partial x}(x,y) + i\dfrac{\partial v}{\partial x}(x,y) = \dfrac{\partial v}{\partial y}(x,y) - i\dfrac{\partial u}{\partial y}(x,y)$.

El uso que se puede hacer del Teorema 2.5.5., es doble. Por un lado, ofrece un cómodo criterio para verificar que una función dada es holomorfa: basta con verificar que la parte real y la parte imaginaria sean de clase C^1 y satisfagan las condiciones de Cauchy-Riemann. Por otro lado, si sabemos que dada cierta función $f(z)$ es holomorfa, entonces por el Teorema 2.5.5., sabemos que las condiciones de Cauchy-Riemann se satisfacen automáticamente.

Observación: La condición 2. del Teorema 2.5.5. requiere la validez de las condiciones de Cauchy-Riemann en un conjunto abierto, junto con la continuidad de las primeras derivadas parciales. De hecho, la validez de las condiciones de Cauchy-Riemann en un solo punto no implica necesariamente que la función sea diferenciable en ese punto. Revisando la prueba de la implicación 1. $\Rightarrow$ 2., vemos que la diferenciabilidad en un solo punto implica, por sí sola, las condiciones de Cauchy-Riemann en ese mismo punto. Más generalmente, si las derivadas parciales de u y v existen alrededor de un punto (x_0,y_0), son continuas y satisfacen las condiciones de Cauchy-Riemann solo en el punto (x_0,y_0), entonces la derivada de f en $z_0 = x_0+iy_0$ existe.

Forma polar de las condiciones de Cauchy-Riemann

Dado $z_0 \neq 0$, el Teorema 2.5.5., se puede reformular utilizando coordenadas polares en lugar de las cartesianas. Por esta razón reescribimos las condiciones de Cauchy-Riemann en forma polar. Usamos la transformación $x = r\cos\theta$ e $y = r\,\text{sen}\,\theta$ y su inversa $r = \sqrt{x^2+y^2}$, $\theta = \arctan\frac{y}{x} + \text{cte}$, para expresar las derivadas parciales de u y v con respecto a las variables r y θ en lugar de x e y. Resulta

$$\frac{\partial y}{\partial x} = \frac{x}{\sqrt{x^2+y^2}} = \cos\theta\ , \qquad \frac{\partial y}{\partial y} = \frac{y}{\sqrt{x^2+y^2}} = \text{sen}\ \theta\ ,$$

$$\frac{\partial \theta}{\partial x} = -\ \frac{x}{x^2+y^2} = -\ \frac{\text{sen}\ \theta}{r}\ , \qquad \frac{\partial \theta}{\partial y} = \frac{x}{x^2+y^2} = \frac{\cos\theta}{r}\ ,$$

y luego, usando la regla la cadena

$$\frac{\partial u}{\partial x} = \frac{\partial u}{\partial r}\cdot\frac{\partial r}{\partial x} + \frac{\partial u}{\partial \theta}\cdot\frac{\partial \theta}{\partial x} = \cos\theta\cdot\frac{\partial u}{\partial r} - \frac{\text{sen}\ \theta}{r}\cdot\frac{\partial u}{\partial \theta}\ ,$$

$$\frac{\partial u}{\partial y} = \frac{\partial u}{\partial r}\cdot\frac{\partial r}{\partial y} + \frac{\partial u}{\partial \theta}\cdot\frac{\partial \theta}{\partial y} = \text{sen}\ \theta\cdot\frac{\partial u}{\partial r} + \frac{\cos\theta}{r}\cdot\frac{\partial u}{\partial \theta}\ ,$$

análogamente

$$\frac{\partial u}{\partial x} = \cos\theta\cdot\frac{\partial v}{\partial r} - \frac{\text{sen}\ \theta}{r}\cdot\frac{\partial v}{\partial \theta}\ , \qquad \frac{\partial v}{\partial y} = \text{sen}\ \theta\cdot\frac{\partial v}{\partial r} + \frac{\cos\theta}{r}\cdot\frac{\partial v}{\partial \theta}\ .$$

Por lo tanto las condiciones de Cauchy-Riemann son equivalentes a

$$\begin{cases} \cos\left(\dfrac{\partial u}{\partial r} - \dfrac{1}{r}\dfrac{\partial v}{\partial \theta}\right) = \text{sen }\theta\left(\dfrac{\partial v}{\partial r} + \dfrac{1}{r}\dfrac{\partial u}{\partial \theta}\right) , \\ \cos\left(\dfrac{\partial v}{\partial r} + \dfrac{1}{r}\dfrac{\partial u}{\partial \theta}\right) = -\text{sen }\theta\left(\dfrac{\partial u}{\partial r} - \dfrac{1}{r}\dfrac{\partial v}{\partial \theta}\right) . \end{cases}$$

Estas relaciones se verifican sólo si

$$\begin{cases} \dfrac{\partial u}{\partial r} = \dfrac{1}{r}\dfrac{\partial v}{\partial \theta} , \\ \dfrac{1}{r}\dfrac{\partial u}{\partial \theta} = -\dfrac{\partial v}{\partial r} . \end{cases}$$

y estas corresponden a las condiciones de Cauchy-Riemann en forma polar. El Teorema 2.5.5., se puede expresar entonces de manera equivalente en la siguiente forma.

Teorema 2.5.6. Sea $f(z) = u(r,\theta) + iv(r,\theta)$ definida en una vecindad del punto $z_0 = r_0 e^{i\theta_0} \neq 0$. Supongamos que las derivadas parciales de u y v, con respecto a r y θ, existen en dicha vecindad y son continuas en (r_0,θ_0). Entonces, si se cumplen las condiciones $(\frac{\partial u}{\partial r} = \frac{1}{r}\frac{\partial v}{\partial \theta} \wedge \frac{1}{r}\frac{\partial u}{\partial \theta} = -\frac{\partial v}{\partial r})$ en (r_0,θ_0), la derivada de $f'(z_0)$ de f en z_0 existe y

$$f'(z_0) = e^{-i\theta_0}\left(\frac{\partial u}{\partial r}(r_0,\theta_0) + i\frac{\partial v}{\partial r}(r_0,\theta_0)\right) = \frac{e^{-i\theta_0}}{r_0}\left(\frac{\partial v}{\partial \theta}(r_0,\theta_0) - i\frac{\partial u}{\partial \theta}(r_0,\theta_0)\right).$$

Demostración:
La existencia sigue como se indicó anteriormente. Comprobemos que es válido

$$f'(z_0) = e^{-i\theta_0}\left(\frac{\partial u}{\partial r}(r_0,\theta_0) + i\frac{\partial v}{\partial r}(r_0,\theta_0)\right) , \quad \text{dado } z_0 = r_0 e^{i\theta_0} = x_0 + iy_0 ,$$

tenemos

$$f'(z_0) = \frac{\partial u}{\partial x}(x_0,y_0) + i\frac{\partial v}{\partial x}(x_0,y_0)$$

$$= \cos\theta_0\frac{\partial u}{\partial r}(r_0,\theta_0) - \frac{\text{sen }\theta_0}{r_0}\frac{\partial u}{\partial \theta}(r_0,\theta_0) + i\cos\theta_0\frac{\partial u}{\partial r}(r_0,\theta_0) - i\frac{\text{sen }\theta_0}{r_0}\frac{\partial v}{\partial \theta}(r_0,\theta_0)$$

$$= (\cos\theta_0 - i\text{ sen }\theta_0)\frac{\partial u}{\partial r}(r_0,\theta_0) + (\text{sen }\theta_0 + i\cos\theta_0)\frac{\partial v}{\partial r}(r_0,\theta_0)$$

$$\Rightarrow \quad f'(z_0) = e^{-i\theta_0}\left(\frac{\partial u}{\partial r}(r_0,\theta_0) + i\frac{\partial v}{\partial r}(r_0,\theta_0)\right) .$$

La segunda igualdad se verifica de manera análoga.

Definición 2.5.7. Una función real de dos variables reales $h : \Omega \subseteq \mathbb{R}^2 \to \mathbb{R}$ se dice **función armónica** en Ω si es de clase[15] $C^2(\Omega)$ y satisface en Ω la ecuación diferencial

$$h_{xx}(x,y) + h_{yy}(x,y) = 0.$$

Esta ecuación se conoce en la literatura como la ecuación de Laplace y el operador

$$\nabla^2 = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}$$

[15]Recordamos que $h \in C^2(\Omega)$ significa que h admite derivadas parciales continuas hasta el segundo orden en Ω.

se llama operador de Laplace o laplaciano. Entonces podemos reescribir la ecuación $(h_{xx}(x,y) + h_{yy}(x,y) = 0)$ en la forma

$$\nabla^2 = (x,y) = 0 \qquad \forall (x,y) \in \Omega \ .$$

El vínculo entre las funciones armónicas y las funciones analíticas se expresa en el siguiente resultado.

Teorema 2.5.8. Sea $f(z) = u(x,y) + iv(x,y)$ analítica en $\Omega \subseteq \mathbb{C}$, entonces las funciones $u(x,y)$ y $v(x,y)$ son armónicas en Ω.

Demostración:

Utilizaremos un resultado que se demostrará más adelante (sección Integral de Cauchy) que garantiza que, si una función de variable compleja f es analítica, entonces las funciones parte real u y parte imaginaria v son de clase $C^2(\Omega)$.

Para probar el teorema es suficiente verificar que las funciones $u(x,y)$ y $v(x,y)$ satisfacen la ecuación de Laplace en Ω. En efecto, a partir de las condiciones de Cauchy-Riemann, $ux = vy$ y $uy = -vx$, derivando ambas ecuaciones con respecto a x e y, obtenemos

$$\begin{cases} u_{xx} = v_{yx} \\ u_{yx} = -v_{xx} \end{cases} \qquad \wedge \qquad \begin{cases} u_{xy} = v_{yy} \\ u_{yy} = -v_{xy} \ . \end{cases}$$

Por el Teorema de Schwartz[16] aplicado a las funciones u y v, tenemos

$$u_{xx} + u_{yy} = v_{yx} - v_{xy} = 0 \ , \quad v_{xx} + v_{yy} = -u_{yx} + u_{xy} = 0 \ ,$$

y por tanto u y v son armónicas en Ω.

Si dos funciones u y v son armónicas en Ω y satisfacen las condiciones de Cauchy Riemann en Ω, se dice que v es una **función armónica conjugada** de u. Claramente si $f(z) = u(x,y) + iv(x,y)$ es una función analítica en Ω, entonces $v(x,y)$ es una armónica conjugada de u. Por el contrario, si v es una armónica conjugada de u en Ω, necesariamente la función $f(z) = u(x,y) + iv(x,y)$ es analítica en Ω (Teorema 2.5.5.).

Tengamos en cuenta que si v es una armónica conjugada de u en Ω, esto no es cierto en general que u es una armónica conjugada de v. Por ejemplo, consideremos

$$u(x,y) = x^2 - y^2 \quad \wedge \quad v(x,y) = 2xy.$$

Como $f(z) = u(x,y) + iv(x,y) = z2$ es una función entera, v es una armónica conjugada de u. Pero u no es una armónica conjugada de v, intercambiando los roles de u y v, las condiciones de Cauchy Riemann no se cumplen. Observamos que si Ω es un conjunto conexo y u y v son conjugadas entre sí, entonces necesariamente son funciones constantes. En efecto, si son válidas simultáneamente

$$\begin{cases} u_x = v_y \\ u_y = -v_x \end{cases} \qquad \wedge \qquad \begin{cases} v_x = u_y \\ u_y = -u_x \ , \end{cases}$$

tenemos $u_x = -u_x$ y $u_y = -u_y$, i.e., $u_x = u_y = 0$. Por lo tanto, $u(x,y)$ es constante, análogamente obtenemos que $v(x,y)$ es constante.

Dada una función armónica $u(x,y)$ en Ω nos planteamos el problema de encontrar una función armónica conjugada $v(x,y)$ de u en Ω, i.e., nos preguntamos si es posible identificar una función analítica a la que se le asigne una parte real.

[16] **Teorema de Schwartz**. Sea $h(x,y)$ de clase $C^2 \in \Omega \subseteq \mathbb{R}^2$, entonces las derivadas parciales mixtas h_{xy} y h_{yx} coinciden.

2.6. Arcos y trayectorias

Como se sabe de los cursos de cálculo, el término "curva" generalmente indica una aplicación $\gamma : I \to \mathbb{R}^n$, donde $I = [a, b]$ es un intervalo de la recta real y $\mathbb{R}^n$ es el espacio euclidiano. La idea intuitiva es la siguiente: podemos imaginar $[a, b]$ como un intervalo de tiempo, y el valor $\gamma(t)$ de la función γ en el punto t como una posición en el espacio euclidiano (por ejemplo, en el plano o en el espacio tridimensional), i.e., la "posición en el tiempo t". En otras palabras, en el instante inicial $t = a$ estamos en el punto $\gamma(a)$, en el instante final $t = b$ nos encontramos en el punto $\gamma(b)$ y así sucesivamente, para todo los instantes intermedios del tiempo.

Aquí nos interesa el caso de las curvas[17] en el plano, i.e., en aplicaciones del tipo $\gamma : [a, b] \to \mathbb{R}^2$, en relación con la teoría de funciones de variable compleja y especialmente funciones holomorfas. Por lo tanto, es aconsejable identificar el plano $\mathbb{R}^2$ con el plano complejo $\mathbb{C}$, y damos la siguiente definición:

Definición 2.6.1. Se llama **curva en el plano** o **trayectoria** a una aplicación $[a, b] \to \mathbb{C}$ continua y de clase C^1 a trozos, donde $[a, b]$ es un intervalo acotado de la recta real. Sea $z(t)$ el punto imagen de $t \in [a, b]$ a través de γ, el conjunto

$$C = \{z(t) \in \mathbb{C} : t \in [a, b]\} \ ,$$

i.e., la imagen de la aplicación γ, se llama traza o soporte de la curva.

Como para todas las funciones de variable compleja, dada una curva $z(t)$ podemos considere su parte real $x(t)$ y su parte imaginaria $y(t)$. En otras palabras, podemos escribir

$$z(t) = x(t) + iy(t) \ ,$$

donde $x(t)$ e $y(t)$ son dos funciones reales, ambas definidas en el intervalo $[a, b]$. Y es importante remarcar que en la definición anterior, cuando decimos que $z(t)$ es continua y C^1 a trozos, queremos decir que cada una de las dos funciones $x(t)$ e $y(t)$ es continúa y C^1 a trozos en $[a, b]$. Entonces podemos hablar de la derivada $z'(t_0)$ de una curva en el punto t_0, i,e., queriendo decir con esto el número complejo

$$z'(t_0) = x'(t_0) + iy'(t_0) \ ,$$

siempre que las funciones $x(t)$ e $y(t)$ sean derivables en el punto t_0 (nótese que esto ocurre en todo $[a, b]$ excepto posiblemente en un número finito de puntos, habiendo requerido que $z(t)$ sea C^1 a trozos).

El requisito de que $z(t)$ sea continua y C^1 a trozos tiene en parte razones técnicas, mientras que es esencial entender la diferencia entre una curva $z(t)$ y su traza C. La curva $z(t)$ es una función (de variable real y con valores complejos), mientras que su traza C es un conjunto de puntos en el plano (i.e., la imagen de la misma curva). Si imaginamos la curva como la descripción del movimiento de una partícula en el plano, la función $z(t)$ representa la ley de movimiento en el sentido de las manecillas del reloj, mientras que la traza C representa el conjunto de todos los puntos por los que ha pasado la partícula al menos una vez.

También se puede pensar en una curva $z(t)$ como una forma de parametrizar su traza C, asociando a cada valor del parámetro $t \in [a, b]$ un único punto de la traza C. Sin embargo, el conjunto

[17] La terminología utilizada aquí no es exactamente la clásica. De hecho, normalmente se define "curva en el plano" una aplicación $\gamma : I \to \mathbb{C}$, donde I es cualquier intervalo real, con la única suposición de que γ es continua: lo que luego se especifica por separado que se entiende por una curva regular, o regular a trozos, a veces llamanda "arcoüna curva regular a trozos cuyo dominio I es un intervalo cerrado y acotado, como en el nuestro caso. Para no sobrecargar la terminología, hemos preferido proporcionar la definición de curva un caso particular, limitándonos a lo necesario a continuación.

C puede la traza de diferentes curvas, i.e., se puede parametrizar de diferentes maneras: con una imagen del mundo real, si pensamos a C como el diseño de una pista de automóviles, y a $z(t)$ como una de las múltiples formas en que se puede recorrer esta ruta (teniendo así en cuenta de eventuales aceleraciones, paradas, retrocesos, etc.).

Por ejemplo, la curva $z(t) = t(1+i)$ con $t \in [0,1]$ tiene como traza el segmento de extremos $w_1 = 0$ y $w_2 = 1+i$ en el plano complejo. Sin embargo, este segmento también es la traza de otras curvas, por ejemplo de la curva $h(t) = t2(1+i),\ t \in [0,1]$. Las dos curvas constituyen dos parametrizaciones diferentes del mismo segmento $\overline{w_0 w_1}$. Por ejemplo, el punto medio del segmento se identifica por el parámetro $t = 1/2$ en el primer caso, y $t = \sqrt{2}/2$ en el segundo.

Sin embargo, hay que decir que el término "curva" o "arco" frecuentemente indica un subconjunto del plano (por ejemplo, comúnmente hablamos de un "arco de circunferencia"); en este caso se implica una parametrización del objeto geométrico, generalmente definida de la manera más natural.

Definición 2.6.2. Se dice que una curva γ es simple si γ es una aplicación inyectiva, i.e., si valores de diferentes puntos del parámetro identifican diferentes puntos de la traza.

Definición 2.6.3. Una curva $\gamma : [a,b] \to \mathbb{C}$ es **cerrada** si $z(a) = z(b)$: tengamos en cuenta que, obviamente, una curva cerrada no puede ser simple (aparte del caso degenerado en donde $a = b$ y el intervalo se reduce a un solo punto).

Definición 2.6.4. Una curva $\gamma : [a,b] \to \mathbb{C}$ se dice **curva de Jordan** si cumple con las siguientes condiciones:

1. Es una curva cerrada, i.e., $z(a) = z(b)$.

2. El punto $z(a) = z(b)$ es el único punto de la traza que es imagen de dos diferentes valores del parámetro.

Intuitivamente, una curva de Jordan es la parametrización de un camino cerrado que nunca pasa por segunda vez sobre los puntos ya recorridos, excepto por supuesto para el punto final $z(b)$ que coincide con $z(a)$.

Ahora establecemos un resultado intuitivamente verdadero, llamado Teorema de Jordan, cuya demostración está lejos de ser inmediata (la cual no realizaremos).

Teorema 2.6.5. (Teorema de Jordan)
Asociados a cada curva de Jordan γ hay dos dominios cada uno de los cuales cuya frontera coincide con la traza C de la curva. Uno de estos dominios, llamado el **interior** de γ, está acotado, el otro, el **exterior** de γ, no está acotado.

2.7. Integrales de línea

En esta sección vamos a definir la integral de una función de variable compleja a lo largo de una trayectoria.
En esta sección vamos a definir la integral de una función de variable real y de variable compleja $g : [a,b] \to \mathbb{C}$. Podemos escribir

$$g(t) = u(t) + iv(t)\ , \quad a \le t \le b\ ,$$

con u y v funciones reales que suponemos continuas a trozos en $[a,b]$. Así que vamos a definir la integral de g sobre $[a,b]$ como

$$\int_a^b g(t)dt = \int_a^b u(t)dt + i\int_a^b v(t)dt \ .$$

En otras palabras, la integral es un número complejo: su parte real es la integral de la parte real de g, mientras que su parte imaginaria es la integral de la parte imaginaria de g. En fórmulas

$$\mathrm{Re}\int_a^b g(t)dt = \int_a^b \mathrm{Re}\, g(t)dt \ , \qquad \mathrm{Im}\int_a^b g(t)dt = \int_a^b \mathrm{Im}\, g(t)dt \ .$$

Además, es fácil comprobar que

$$\int_a^b \lambda g(t)dt = \lambda\int_a^b g(t)dt \ , \quad \forall\lambda\in\mathbb{C} \ .$$

Consideremos ahora una curva $\gamma:[a,b]\to\mathbb{C}$, y una función $f(z)$ de variable compleja y de valor complejo, que suponemos continua sobre la traza de C de la curva.

Definición 2.7.1. La **integral de línea** de f a lo largo de C está dada como

$$\int_\gamma f(z)dz = \int_a^b f(z(t))z'(t)dt \ .$$

Tengamos en cuenta que, por definición, la integral a lo largo de una curva se reduce a la integral, en el intervalo real $[a,b]$, de la función $g(t)=f(z(t))z'(t)$, que por lo tanto debe entenderse en el sentido de $(\int_a^b g(t)dt = \int_a^b u(t)dt + i\int_a^b v(t)dt)$.

Vale la pena escribir explícitamente el lado derecho de (Definición 2.7.1.). Haciendo $f(z) = u(x,y)+iv(x,y)$ y $z(t)=x(t)+iy(t)$, tenemos que $z'(t)=x'(t)+iy'(t)$ y luego desenrollando el producto se encuentra

$$\begin{aligned} f(z(t))z'(t) = u(x(t),y(t))x'(t) - v(x(t),y(t))y'(t)+ \\ +i(v(x(t),y(t))x'(t)+u(x(t),y(t))y'(t)) \ . \end{aligned}$$

La segunda integral en la igualdad de la (Definición 2.7.1.) está por tanto bien definida gracias a las hipótesis formuladas sobre la función f, y gracias al hecho de que $z(t)$ es (por definición de la propia curva) C^1 a trozos, por lo tanto, las funciones $x'(t)$ e $y'(t)$ son continuas a trozos en $[a,b]$.
Además, usando (el desarrollo del producto), tenemos

$$\mathrm{Re}\int_\gamma f(z)dz = \int_a^b (u(x(t),y(t))x'(t) - v(x(t),y(t))y'(t))dt \ ,$$

$$\mathrm{Im}\int_\gamma f(z)dz = \int_a^b (v(x(t),y(t))x'(t) + u((x(t),y(t))y'(t))dt \ .$$

Podemos reescribir las integrales en la (Definición 2.7.1.) como

$$\int_\gamma f(z)dz = \int_\gamma (u\ dx - v\ dy) + i\int_\gamma (v\ dx + u\ dy) \ ,$$

expresión que también puede deducirse formalmente de la (Definición 2.7.1.) sustituyendo f con $u+iv$ y dz con $dx+idy$.

Para motivar la Definición 2.7.1, tratemos de entender qué sucede si uno busca construir la integral compleja como límite de las sumas de Riemann. dividimos entonces el intervalo $[a, b]$ en n intervalos congruentes, de extremos

$$a = t_0 < t_1 < \cdots < t_n = b \ , \quad \text{donde} \ \ t_j - t_{j-1} = \frac{b-a}{n} \ ,$$

consideramos los puntos de la curva

$$z_0 = z(t_0), z_1 = z(t_1), \cdots, z_n = z(t_n) \ ,$$

correspondientes a los extremos de los intervalos, y construimos la suma de Riemann

$$\sum_{j=1}^{n} f(z_j) \cdot (z_j - z_{j-1}) \ .$$

Se podría pensar en definir la integral de f a lo largo de γ como el límite de las sumas de Riemann, i.e., poner

$$\int_\gamma f(z)dz = \lim_{n\to\infty} \left(\sum_{j=1}^{n} f(z_j) \cdot (z_j - z_{j-1}) \right) \ ,$$

(los puntos t_j y sus imágenes z_j obviamente también dependen del valor de n: no indicamos explícitamente esta dependencia, para no añadir demasiado a la notación). De hecho, esta segunda definición simplemente no sería perfectamente legal, pero estaría en total acuerdo con la (Definición 2.7.1.). De hecho, si en cualquier suma de Riemann multiplicamos y dividimos cada término por el correspondiente incremento temporal $t_j - t_{j-1}$, obtenemos

$$\int_\gamma f(z)dz = \lim_{n\to\infty} \left(\sum_{j=1}^{n} f(z(t_j)) \frac{z(t_j) - z(t_{j-1})}{t_j - t_{j-1}} (t_j - t_{j-1}) \right) \ .$$

Se puede demostrar no sólo que el límite existe, sino que coincide con el miembro de la derecha de la (Definición 2.7.1.): la presencia de la derivada $z'(t)$ en la (Definición 2.7.1.), de hecho, se debe precisamente a las razones incrementales en la suma de Riemann, escrita en el resultado anterior. Sin embargo, mantengamos como en la (Definición 2.7.1.), porque se presta más al cálculo directo del valor de la integral.

Sin embargo, es útil tener en cuenta que la caracterización $(\int_\gamma f(z)dz = \lim_{n\to\infty} \left(\sum_{j=1}^{n} f(z_j) \cdot (z_j - z_{j-1}) \right))$ se cumple, porque es adecuada para interpretar el significado de la integral compleja desde un punto de vista de la física y de la geométrica. De hecho, al colocar

$$\Delta z_j = z_j - z_{j-1} = \Delta x_j + i\Delta y_j \ ,$$

la suma de Riemann $(\sum_{j=1}^{n} f(z_j) \cdot (z_j - z_{j-1}))$ se puede escribir como

$$\sum_n (u(z_j) + iv(z_j))(\Delta x_j + i\Delta y_j) = \sum_n (u(z_j)\Delta x_j - v(z_j)\Delta y_j) +$$

$$+ i \sum_n (v(z_j)\Delta x_j + u(z_j)\Delta y_j) \ .$$

Consideramos, por ejemplo, la parte real de esta suma.
$u(z_j)\Delta x_j - v(z_j)\Delta y_j$ se puede interpretar como el producto escalar entre los dos vectores

$$\vec{E}_j = \begin{pmatrix} u(z_j) \\ \\ -v(z_j) \end{pmatrix} \qquad \wedge \qquad \Delta\vec{l_j} = \begin{pmatrix} \Delta x_j \\ \\ \Delta y_j \end{pmatrix} \ .$$

Pensando en el vector E_j como el campo vectorial

$$\vec{E}(x,y) = \begin{pmatrix} u(x,y) \\ \\ -v(x,y) \end{pmatrix} \ ,$$

calculada en el punto z_j de la curva[18], y al vector $\Delta\vec{l_j}$ como un incremento (que, al pasar al límite, se hará infinitesimal) de posición a lo largo de la curva, es claro, en base a ($\int_\gamma f(z)dz = \lim_{n\to\infty}\left(\sum_{j=1}^n f(z_j)\cdot(z_j - z_{j-1})\right)$), que el parte real de la integral compleja de f a lo largo de γ no es nada más que la integral de línea (también llamada circuito si γ es una curva cerrada) del campo vectorial $\vec{E}$ a lo largo de la trayectoria γ. Por ejemplo, si $\vec{E}$ representa un campo de fuerza, la parte real de la integral compleja representa el trabajo realizado por el campo de fuerza a lo largo de la trayectoria γ. También notamos que, al identificar números complejos con vectores, el campo $\vec{E}$ se obtiene de $f(z)$ pasando a la función conjugada. En fórmulas

$$\mathrm{Re}\int_\gamma f(z)dz \oint_\gamma \vec{E}\cdot d\vec{l}\ , \qquad \vec{E}(x,y) = \overline{f(x+iy)}\ .$$

Ahora llegamos a la interpretación de la parte imaginaria de la integral. En el segundo sumando (de la forma explícita en la suma de Riemann), análogamente, la cantidad $v(z_j)\Delta x_j + u(z_j)\Delta y_j$ se puede interpretar como el producto punto de dos vectores

$$\vec{E}_j = \begin{pmatrix} u(z_j) \\ \\ -v(z_j) \end{pmatrix} \qquad \wedge \qquad \Delta\vec{n}_j = \begin{pmatrix} \Delta y_j \\ \\ -\Delta x_j \end{pmatrix} \ .$$

Observamos que el vector $\vec{n}_j$ es ortogonal al vector Δl_j, de hecho $\vec{n}_j$ se obtiene girando $\Delta\vec{l_j}$ noventa grados en el sentido de las agujas del reloj. Por lo tanto, si denotamos por ν_j al vector normalizado

$$\nu_j = \frac{\vec{n}_j}{\Delta l_j}\ , \qquad \Delta l_j = \sqrt{(\Delta x_j)^{2+(\Delta y_j)^2}}\ ,$$

representa una aproximación del versor normal a la curva, en el punto z_j (de hecho es perpendicular al segmento de extremos z_{j-1} y z_j), y podemos escribir

$$v(z_j)\Delta x_j + u(z_j)\Delta y_j = \vec{E}_j\cdot\vec{n}_j = \vec{E}_j\cdot\vec{\nu}_j\Delta l_j\ .$$

Esta cantidad por lo tanto representa el flujo del vector $E(z_j)$ a través del segmento $\Delta\vec{l_j}$ (con la normal orientada a la derecha, con respecto a la orientación del segmento). Sumando y pasando al límite, obtenemos así que

$$\mathrm{Im}\int_\gamma f(z)dz = \int_\gamma \vec{E}\cdot\nu\ dl\ , \qquad \vec{E}(x,y) = \overline{f(x+iy)}\ ,$$

i.e., la parte imaginaria de la integral compleja de $f(z)$ a lo largo de γ, representa el flujo del campo vectorial $\vec{E}$ a través de la curva γ (en la fórmula, ν denota la normal a la curva, orientada a la derecha con respecto al sentido de recorrido de la curva).

[18]Como de costumbre, por conveniencia, identificamos los números complejos con los vectores en el plano.

Asociada a la traza C, parametrizada por la curva $\gamma : [a, b] \to \mathbb{C}$, está la curva denotada por $-\gamma$ que tiene la misma traza que γ en la dirección inversa. En otras palabras, la curva $-\gamma$ une el punto $z(b)$ con el punto $z(a)$ y se describe por la parametrización $z = z(-t)$, con $-b \leq t \leq -a$.

Definición 2.7.2. Dada la curva $\gamma : [a, b] \to \mathbb{C}$, introducimos una subdivisión de $[a, b]$ mediante los puntos $a = t_0 < t_1 < \cdots < t_n = b$ y consideramos los puntos $z(t_0), z(t_1), \ldots, z(t_n)$ perteneciente a la traza,

$$\sup_{a=t_0<t_1<\cdots<t_n=b} (|z(t_1) - z(t_0)| + |z(t_2) - z(t1)| + \cdots + |z(t_n) - z(t_{n-1})|) \ ,$$

donde el límite superior se hace variando todas las opciones de números reales t_i se llama la **longitud de la curva**.

Notemos que, para una elección dada de números t_i, la suma anterior representa la longitud de la línea quebrada que se obtiene uniendo entre sí, mediante segmentos, los puntos de la traza $z(t_0), z(t_1), \ldots, z(t_n)$, tomados en ese orden.

Imaginemos, para fijar las ideas, que $z(t)$ es una curva simple. Intuitivamente, está claro que la longitud de cualquier curva a trozos obtenida de esta manera proporciona una aproximación de la longitud de la curva (donde la palabra "longitud" se usa aquí en el sentido intuitivo de la palabra). Por otro lado, se entiende que, haciendo la línea quebrada más gruesa (i.e., considerando un número gradualmente mayor que puntos de la traza), se obtiene una aproximación cada vez mejor de la longitud efectiva de la curva. Estas consideraciones intuitivas justifican la presencia del límite superior, en la definición de la longitud.

De hecho, en el caso en el cual $z(t)$ sea una curva simple, se puede probar que su longitud depende únicamente de la traza C, y no de la forma en la cual C está parametrizada (siempre que la parametrización sea inyectiva). En otras palabras, la longitud es en realidad una característica geométrica de la traza C. En cualquier caso, sobre la base de nuestra definición de una curva, se puede demostrar que la longitud L siempre es finita y se puede calcular utilizando la siguiente integral:

$$L = \int_a^b |z'(t)| dt \ .$$

Para interpretar el significado de esta integral notemos que, por lo dicho en esta sección, la derivada $z'(t)$ representa la velocidad instantánea con la que la curva se recorre en el tiempo t. Su módulo $|z'(t)|$ representa la velocidad escalar en el tiempo t: al integrar la velocidad escalar con respecto al tiempo, obtenemos la "longitud de la ruta", o más precisamente la longitud de la curva.

Proposición 2.7.3. Sea γ un camino y sean f y g dos funciones continuas a trozos en C, traza de γ, entonces

a) para todo $\lambda, \mu \in \mathbb{C}$,

$$\int_\gamma (\lambda f(z) \mu g(z)) dz = \lambda \int_\gamma f(z) dz + \mu \int_\gamma g(z) dz \ ,$$

b)

$$\int_{-\gamma} f(z) dz = -\int_\gamma f(z) dz \ ,$$

c) sea $M \geq 0$ tal que $|f(z)| \leq M$ sobre C y sea L la longitud de γ, tenemos

$$\left| \int_\gamma f(z)dz \right| \leq ML \ ,$$

d) si C es la unión de las trazas C_1 y C_2 de dos curvas $\gamma_1 : [a_1, b_1] \to \mathbb{C}$ y $\gamma_2 : [a_2, b_2] \to \mathbb{C}$ tales que $z_1(b_1) = z_2(a_2)$, tenemos que

$$\int_\gamma f(z)dz = \int_{\gamma_1} f(z)dz + \int_{\gamma_2} f(z)dz \ .$$

2.8. Teorema de Cauchy-Goursat

El siguiente teorema es uno de los resultados fundamentales de la teoría de funciones holomorfas. Cauchy lo probó con el supuesto adicional de continuidad de la derivada y, más tarde, por Goursat en su forma más general que mostramos aquí.

Teorema 2.8.1. (de Cauchy-Goursat)
Sea γ una curva de Jordan, contenida en un conjunto abierto Ω, tal que su interior A todavía está contenido en Ω. Si $f(z)$ es una función holomorfa en Ω, entonces tenemos

$$\int_\gamma f(z)dz = 0 \ .$$

Es necesario reflexionar detenidamente sobre el significado de este teorema y sus hipótesis. El valor de la integral de f a lo largo de γ depende únicamente de los valores que asumamos f en los puntos de la traza C, sin embargo, las suposiciones requieren que f sea holomorfa en un abierto Ω que contiene tanto a C como a la región A delimitada por C.

Aquí probaremos este resultado bajo la hipótesis más restrictiva que la primera derivada $f'(z)$ es también una función continua en el conjunto abierto Ω. partiendo del teorema de Cauchy-Goursat desde el siguiente teorema importante, que no probaremos.

Definición 2.8.2. Si $\vec{E}(x, y) = (a, b)$ es un campo vectorial plano que tiene por componentes dos funciones $a(x, y)$ y $b(x, y)$ de clase C^1, se llama **divergencia** de $\vec{E}$ a la función

$$\text{div } \vec{E} = \frac{\partial a}{\partial x} + \frac{\partial b}{\partial y} \ ,$$

mientras que el **rotacional** de $\vec{E}$ es

$$\text{rot } \vec{E} = \frac{\partial a}{\partial y} - \frac{\partial b}{\partial x} \ .$$

Teorema 2.8.3. (Fórmula de Gauss-Green)
Sea γ una curva de Jordan, contenida en un conjunto abierto Ω, tal que la parte del plano A delimitada por la traza C está contenida en Ω. Si $\vec{E}(x, y) : \Omega \to \mathbb{C}$ es un campo vectorial que tiene por componentes dos funciones de clase C^1 , entonces tenemos

$$\int_\gamma \vec{E} \cdot \vec{dl} = \iint_A \text{rot } \vec{E} \ dxdy \ ,$$

$$\int_\gamma \vec{E}\cdot\nu\ dl = \iint_A \text{div}\ \vec{E}\ dxdy\ .$$

En otras palabras, la circulación de $\vec{E}$ a lo largo de γ es igual a la integral del rotacional de $\vec{E}$ al interior de γ, mientras que el flujo de $\vec{E}$ saliendo de γ es igual a la integral de la divergencia de $\vec{E}$ en el interior de γ.

Para demostrar el Teorema de Cauchy-Goursat bajo el supuesto de que $f'(z)$ es continua, basta considerar el campo vectorial

$$\vec{E}(x,y) = \begin{pmatrix} u(x,y) \\ \\ -v(x,y) \end{pmatrix}\ ,$$

donde u y v, son las partes real e imaginaria de f. Calculamos la divergencia el y rotacional de $\vec{E}$, tenemos

$$\text{div}\ \vec{E}(x,y) = \frac{\partial u}{\partial x} - \frac{\partial v}{\partial y}\ , \qquad \text{rot}\ \vec{E}(x,y) = \frac{\partial u}{\partial y} + \frac{\partial v}{\partial x}\ ,$$

y por lo tanto, aplicando las condiciones de Cauchy-Riemann, obtenemos que el campo $\vec{E}$ tiene divergencia cero y rotacional cero. Así, de la fórmula de Gauss-Green, se deduce que tanto la circulación de $\vec{E}$ (la parte real de la integral compleja de f) a lo largo de γ sea el flujo de $\vec{E}$ (la parte imaginaria de la integral compleja de f) a través de γ son nulos. En consecuencia, la integral compleja de f a lo largo de γ es cero, y obtenemos el teorema de Cauchy-Goursat.

Recordemos que un campo con rotacional cero se dice irrotacional, mientras que un campo con divergencia cero se dice solenoidal (por ejemplo, el campo eléctrico debido a un distribución estacionaria de cargas es en todas partes irrotacional y solenoidal, en los puntos fuera de las cargas que lo generan). De lo que se acaba de decir se sigue inmediatamente que el campo $\vec{E}$ asociado a $\overline{f(z)}$ es irrotacional y solenoidal, en las regiones donde $f(z)$ es analítica.

Observamos que el camino considerado puede ser reemplazado por un camino cerrado no necesariamente simple. De hecho, si γ se interseca a sí mismo sólo un número finito de veces, entonces está formado por un número finito de caminos simples y cerrados. Por lo tanto, es posible aplicar el teorema a cada uno de ellos y obtener el resultado para el camino γ.

El teorema se puede extender a dominios más generales. Comenzamos introduciendo el noción de un dominio simplemente conexo, i.e., un dominio al que se aplica el teorema de Cauchy-Goursat.

Definición 2.8.4. Un **dominio simplemente conexo** D es un dominio tal que el interior de todo camino simple y cerrado está enteramente contenido en D.

Intuitivamente, un dominio simplemente conexo es un conjunto sin huecos. Por ejemplo, los contornos y los polígonos están simplemente conectados, mientras no lo es una corona circular.

Definición 2.8.5. Llamaremos **dominio con frontera** a un dominio Ω cuya frontera $\partial\Omega$ es la unión de un número finito de trazas $C_1, C_2, \ldots, C_n$, en parejas disjuntas, de caminos cerrados y simples, $\gamma_1, \gamma_2, \ldots, \gamma_n$.

Cada uno de estos caminos está orientado de tal manera que un observador ideal que recorra la frontera ve a Ω a su izquierda. Llamaremos a esta orientación, **orientación positiva**.

Teorema 2.8.6. Sea Ω un dominio con frontera y sea γ la unión de caminos cuyas trazas coinciden con la frontera Ω orientada positivamente. Sea f analítica en un conjunto abierto que

contiene la unión de Ω con su frontera, entonces

$$\int_\gamma f(z)dz = 0 \ .$$

Demostración:
Sea C_0 el camino externo y $C_1, \ldots, C_n$ aquellos contenidos en el interior de C_0. Consideremos un camino que descomponga Ω en dos partes Ω_1 y Ω_2 mediante los caminos $L_1, \ldots, L_{n+1}$ uniendo C_0 a C_1, C_1 a $C_2, \ldots C_{n-1}$ a C_n y C_n a C_0 (con traza en Ω). Sea K_j el camino cuya traza coincide con la frontera de Ω_j, $j = 1, 2$. K_1 y K_2 consisten en caminos L_j o $-L_j$ y partes de C. El teorema de Cauchy-Goursat 2.27 se puede aplicar a f sobre K_1 y K_2 y la suma de las integrales en estos caminos es nula. Dado que las integrales en direcciones opuestas a lo largo L_j se cancelan, resulta

$$0 = \int_{K_1} f(z)dz + \int_{K_2} f(z)dz = \int_\gamma f(z)dz \ .$$

Observación: Si f es analítica en Ω, dominio simplemente conexo, entonces, para todo $z_1, z_2 \in \Omega$, está bien definida $\int_{z_1}^{z_2} f(z)dz$, es el único número correspondiente al valor de la integral de f a lo largo de cualquier camino, con traza en Ω, uniendo z_1 a z_2. De hecho, si γ_1 y γ_2 son dos caminos que se unen z_1 a z_2, la integral de f a lo largo del camino cerrado obtenido uniendo γ_1 a $-\gamma_2$ es cero, entonces

$$0 = \int_{\gamma_1} f(z)dz + \int_{-\gamma_2} f(z)dz = \int_{\gamma_1} f(z)dz - \int_{\gamma_2} f(z)dz$$

y luego

$$\int_{\gamma_1} f(z)dz = \int_{\gamma_2} f(z)dz$$

donde las trazas C_1 y C_2 se recorren en sentido antihorario.

Es posible probar un resultado que puede considerarse el inverso del Teorema por Cauchy-Goursat. De hecho, se cumple el siguiente teorema de Morera.

Teorema 2.8.7. (de Morera)
Si f es una función continua en un dominio simplemente conexo D y si, para cualquier camino simple y cerrado γ cuya traza está contenida en D, resulta

$$\int_\gamma f(z)dz = 0 \ ,$$

entonces f es analítica en D.

2.9. Fórmula integral de Cauchy

Ahora establecemos el siguiente resultado fundamental.

Teorema 2.9.1. (Fórmula integral de Cauchy)
Sea f analítica en un abierto que contiene a $\Omega \cup \partial\Omega$, con dominio Ω y traza $\partial\Omega$ de un camino cerrado y simple γ en sentido antihorario. Si $z_0 \in \Omega$, entonces

$$f(z_0) = \frac{1}{2\pi i} \int_\gamma \frac{f(z)}{z - z_0} \ dz \ .$$

Demostración:
Como Ω es abierto, existe $r_0 > 0$ tal que $B_{r_0}(z_0) \subset \Omega$, sea γ_0 el camino cerrado y simple, recorrido en sentido antihorario cuya traza es la circunferencia $C_0 = \{|z - z_0| = r_0\}$. Consideremos la función $g(z) = \frac{f(z)}{z-z_0}$ analítica en $(\Omega \setminus \{z_0\}) \cup \partial\Omega$ y por lo tanto, por la observación anterior, resulta

$$\int_\gamma g(z)dz = \int_{\gamma_0} g(z)dz = f(z_0)\int_{\gamma_0} \frac{1}{z - z_0}dz + \int_{\gamma_0} \frac{f(z) - f(z_0)}{z - z_0}\ dz\ .$$

Recordando el Teorema 2.8.1. (de Cauchy-Goursat), tenemos

$$\int_\gamma g(z)dz = 2\pi i f(z_0) + \int_\gamma \frac{f(z) - f(z_0)}{z - z_0}\ dz\ .$$

Verifiquemos ahora que la última integral es cero, obteniendo así $(f(z_0) = \frac{1}{2\pi i}\int_\gamma \frac{f(z)}{z-z_0}dz)$. Siempre y cuando f sea continua, fijando $\epsilon > 0$ existe $\delta > 0$ tal que para todo $z \in \Omega$ con $|z - z_0| < \delta$ se tiene $|f(z) - f(z_0)| < \epsilon$. No es restrictivo suponer que $r_0 \leq \delta$. Ahora, calculemos $\int_\gamma z^n dz$ donde $n \in \mathbb{Z}$ y γ es el camino recorrido en sentido antihorario, cuya traza es la circunferencia $\{|z| = 1\}$. Usamos la parametrización $(z(t) = w_0 + Re^{it},\ \ t \in [0, 2\pi])$ para una circunferencia con centro w_0 y radio R, con una curva $\gamma : [a, b] \to \mathbb{C}$, entonces $z'(t) = ie^{it}$ y por lo tanto

$$\int_\gamma z^n dz = \int_0^{2\pi} e^{int} ie^{it}dt = i\int_0^{2\pi} e^{i(n+1)t}dt$$

$$\Rightarrow \quad \int_\gamma z^n dz \ = \begin{cases} \dfrac{1}{n+1}e^{i(n+1)t}\Big|_0^{2\pi} = 0\ , & n \neq -1\ , \\ \\ 2\pi i\ , & n = -1\ . \end{cases}$$

Un resultado análogo es válido si γ es el camino, recorrido en sentido antihorario, cuya traza es la circunferencia centrada en $z_0 \in \mathbb{C}$ y de radio $r > 0$. Precisamente tenemos

$$\int_\gamma (z - z_0)^n dz \ = \begin{cases} 0\ , & n \neq -1\ , \\ \\ 2\pi i\ , & n = -1\ . \end{cases}$$

Por lo tanto, gracias al resultado anterior, tenemos

$$\left|\int_\gamma \frac{f(z) - f(z_0)}{z - z_0}dz\right| \leq \sup_{z\in\mathbb{C}_0}\left|\frac{f(z) - f(z_0)}{z - z_0}dz\right| \cdot 2\pi r_0$$

$$= 2\pi \sup_{z\in\mathbb{C}_0} |f(z) - f(z_0)| < 2\pi\epsilon\ .$$

Por la arbitrariedad de ϵ, obtenemos la afirmación.

Teorema 2.9.2. Sea f analítica en z_0, entonces existen sus derivadas de cualquier orden en z_0. Además, para todo entero $n \geq 1$ y para todo camino γ simple y cerrado (con sentido antihorario) cuya traza está contenida en la vecindad de z_0 en el que f es diferenciable, tenemos

$$f^{(n)}(z_0) = \frac{n!}{2\pi i}\int_\gamma \frac{f(z)}{(z - z_0)^{n+1}}\ dz\ .$$

Observación: Recordando el Teorema 2.8.6., es inmediato verificar que el las fórmulas $(f(z_0) = \frac{1}{2\pi i}\int_\gamma \frac{f(z)}{z-z_0}\ dz)$ y $(f^{(n)}(z_0) = \frac{n!}{2\pi i}\int_\gamma \frac{f(z)}{(z-z_0)^{n+1}}\ dz)$ se pueden extender al caso en el que el camino cerrado y simple γ se reemplaza por la frontera orientada de un dominio con frontera.

Damos ahora una serie de resultados que se refieren al comportamiento de una función en una región (o incluso en todo el plano complejo).
Primero mostramos que el valor de una función en el centro de un círculo sobre el cual es analítica depende solo de los valores de la función en la frontera de ese círculo. Precisamente, tenemos

Teorema 2.9.3. Sea f analítica en un conjunto D simplemente conexo unido a su frontera. Sean $z_0 \in D$ y $r > 0$ tales que $B_r(z_0) \subset D$, entonces

$$f(z_0) = \frac{1}{2\pi} \int_0^{2\pi} f(z_0 + re^{it})\ dt\ .$$

Demostración:
Sea γ el camino simple y cerrado, recorrido en sentido antihorario, descrito por la parametrización $z = z(t) = z_0 + re^{it},\ 0 \le t \le 2\pi$, entonces, aplicando $(f(z_0) = \frac{1}{2\pi i} \int_\gamma \frac{f(z)}{z - z_0} dz)$, obtenemos

$$f(z_0) = \frac{1}{2\pi i} \int_\gamma \frac{f(z)}{z - z_0}\ dz = f(z_0) = \frac{1}{2\pi i} \int_0^{2\pi} \frac{f(z_0 + re^{it})}{re^{it}} rie^{it}\ dt$$

$$\Rightarrow \quad f(z_0) = \frac{1}{2\pi i} \int_0^{2\pi} f(z_0 + re^{it})\ dt\ .$$

Enunciamos ahora el llamado principio del módulo máximo que se puede deducir de propiedad de la media.

Teorema 2.9.4. (Principio del módulo máximo)
Sea f analítica y no constante en un dominio Ω, que también es continua en $\Omega \cup \partial\Omega$, entonces $|f(z)|$ alcanza su valor máximo en la frontera $\partial\Omega$.

De igual forma propiedades análogas se pueden deducir para las funciones armónicas $u(x, y) = \operatorname{Re} f(z)$ y $v(x, y) = \operatorname{Im} f(z)$.

Teorema 2.9.5. (de Liouville)
Sea f entera y acotada para todo $z \in \mathbb{C}$, entonces $f(z)$ es constante.
Demostración:
Sean $z_0 \in \mathbb{C}$, $r_0 > 0$ y γ_0 el camino de traza C_0 parametrizado por $z = z(t) = z_0 + r_0 e^{it},\ t \in [0, 2\pi]$. Por hipótesis, existe $M > 0$ tal que $|f(z)| \le M$ para cada z. De la fórmula $(f^{(n)}(z_0) = \frac{n!}{2\pi i} \int_\gamma \frac{f(z)}{(z - z_0)^{n+1}} dz)$ con $n = 1$, usando (inciso *c)* de la Proposición 2.7.3.), tenemos

$$|f'(z_0)| = \frac{1}{2\pi} \left| \int_{\gamma_0} \frac{f(z)}{(z - z_0)^2} dz \right| \le \frac{1}{2\pi} \sup_{z \in \mathbb{C}_0} \left| \frac{f(z)}{(z - z_0)^2} \right| \cdot 2\pi r_0$$

$$\Rightarrow \quad |f'(z_0)| = \frac{1}{r_0} \sup_{z \in \mathbb{C}_0} |f(z)| \le \frac{M}{r_0}\ .$$

Como r_0 es arbitrario y $f'(z_0)$ es un número fijo, la desigualdad $|f'(z_0)| \le \frac{M}{r_0}$ puede cumplirse solo si $f'(z_0) = 0$. Por lo tanto $f'(z) = 0$, para todo $z \in \mathbb{C}$ y por lo tanto $f(z)$ es constante.

Una consecuencia demasiada interesante (pues conecta a las funciones de variable compleja con la teoría analítica de los números) del Teorema de Liouville es el Teorema Fundamental del Álgebra, el cual establece que todo polinomio $P(z) = a_0 + a_1 z + \cdots + a_n z^n,\ a_n \neq 0,\ n \ge 1$, tiene al menos un cero; i.e., existe $z_0 \in \mathbb{C} : P(z_0) = 0$. En efecto, procediendo por contradicción, si $P(z)$ fuera distinto de cero para todo $z \in \mathbb{C}$ entonces la función $f(z) = 1/P(z)$ sería entera y acotada en $\mathbb{C}$.

Llegamos así a un absurdo ya que, por el Teorema de Liouville, se sigue que $f(z)$ es constante y por lo tanto el polinomio $P(z)$ también lo es.

2.10. Sucesiones y series

Una sucesión $\{c_n\}_{n\in\mathbb{N}}$ de números complejos es una aplicación de $\mathbb{N}$ en $\mathbb{C}$. Diremos que la sucesión $\{c_n\}_{n\in\mathbb{N}}$ tiene límite $l \in \mathbb{C}$ si para todo $\epsilon > 0$ existe un número $n_\epsilon \in \mathbb{N}$ tal que para todo $n > n_\epsilon$ tenemos $|c_n - l| < \epsilon$, en símbolos

$$\lim_{n\to\infty} c_n = l \quad \Longleftrightarrow \quad \forall \epsilon > 0, \exists n_\epsilon \in \mathbb{N} : \forall n > n_\epsilon \text{ se tiene } |c_n - l| < \epsilon \ .$$

Geométricamente, esto significa que para valores de n suficientemente grandes los puntos c_n están arbitrariamente cerca del límite l. No es difícil comprobar que el límite, si existe, es único. Cuando el límite existe, diremos que la sucesión **converge a** l, en todos los demás casos diremos que la sucesión **no converge**.

En cuanto a los límites de funciones de variable compleja, se cumple un resultado análogo a los Teoremas 2.4.2 y 2.4.4.

Teorema 2.10.1. Supongamos que $c_n = a_n + ib_n \ \wedge \ l = l_{re} + il_{im}$, entonces

$$\text{a)} \qquad \lim_{n\to\infty} c_n = l \quad \Longleftrightarrow \quad \begin{cases} \lim_{n\to\infty} a_n = l_{re} \ , \\ \lim_{n\to\infty} b_n = l_{im} \ . \end{cases}$$

$$\text{b)} \qquad \lim_{n\to\infty} c_n = l \quad \Longleftrightarrow \quad \lim_{n\to\infty} |c_n - l| = 0 \ .$$

$$\text{c)} \qquad \lim_{n\to\infty} c_n = l \quad \Longleftrightarrow \quad \lim_{n\to\infty} |c_n| = l \ .$$

Demostración:
a) Supongamos primero que $\lim_{n\to\infty} c_n = l$. Por definición, para todo $\epsilon > 0$, existe $n_\epsilon \in \mathbb{N}$ tal que

$$\forall n > n_\epsilon \quad \Rightarrow \quad |a_n - l_{re} + i(b_n l_{im})| < \epsilon \ .$$

Pero $|a_n - l_{re}| \le |a_n - l_{re} + i(b_n - l_{im})|$ y $|b_n - l_{im}| \le |a_n - l_{re} + i(b_n - l_{im})|$. En consecuencia, para todo $n > n_\epsilon$, resulta

$$|a_n - l_{re}| < \epsilon \quad \wedge \quad |b_n - l_{im}| < \epsilon \ ,$$

i.e.,

$$\lim_{n\to\infty} a_n = l_{re} \quad \wedge \quad \lim_{n\to\infty} b_n = l_{im} \ .$$

Y de forma inversa se cumple la expresión anterior, para todo $\epsilon > 0$ existen $n_1, n_2 \in \mathbb{N}$ tales que

$$\forall n > n_1 \quad \Rightarrow \quad |a_n - l_{re}| < \frac{\epsilon}{2} \qquad \wedge \qquad \forall n > n_1 \quad \Rightarrow \quad |b_n - l_{im}| < \frac{\epsilon}{2} \ .$$

Por lo tanto, si $n_\epsilon = \text{máx}(n_1, n_2)$, tenemos

$$\forall n > n_\epsilon \quad \Rightarrow \quad |a_n - l_{re} + i(b_n - l_{im})| \le |a_n - l_{re}| + |b_n - l_{im}| < \epsilon \ ,$$

i.e.,

$$\forall n > n_\epsilon \quad \Rightarrow \quad |c_n - l| < \epsilon \quad \Rightarrow \quad \lim_{n\to\infty} c_n = l \ .$$

b) Observamos que, directamente de la definición, tenemos

$$\lim_{n\to\infty} z_n = l \quad \Longleftrightarrow \quad \lim_{n\to\infty} (z_n - l) = 0 \quad \Longleftrightarrow \quad \lim_{n\to\infty} |z_n - l| = 0 \ .$$

c) El resultado se sigue inmediatamente al observar que

$$||c_n| - |l|| \leq |c_n - l| \ .$$

Observamos que en el punto c) la implicación inversa generalmente no se cumple. Si pensemos, por ejemplo, en la sucesión $c_n = (-1)^n$. Resulta que $|c_n| = 1$ y luego la sucesión de módulos $\{|c_n|\}$ converge a 1 mientras que la sucesión inicial $\{c_n\}$, no converge.

Como en el caso real, la suma de infinitos números complejos (estudio de la convergencia de una serie) se define a partir de las sucesiones.De forma más precisa, sea $\{c_n\}$ una sucesión de números complejos. Consideremos la sucesión las sumas parciales $\{s_n\}$ definidas, para todo $n \geq 0$, como

$$s_0 = c_0 \ , \qquad s_n = \sum_{k=0}^{n} c_k = s_{n-1} + c_n \ , \quad n \geq 1 \ .$$

Diremos que la serie $\sum_{n=0}^{\infty} c_n$ converge a $s \in \mathbb{C}$ si $\lim_{n\to\infty} s_n = s$. En todos los otros casos diremos que la serie no converge. El número s, si existe, se llama **suma** de la serie.
Del Teorema 2.10.1., obtenemos el siguiente resultado.

Teorema 2.10.2. Supongamos que $c_n = a_n + ib_n$ y $s = s_{re} + is_{im}$, entonces la serie $\sum_{n=0}^{\infty} c_n$ converge a s si y solo si las serie $\sum_{n=0}^{\infty} a_n$ y $\sum_{n=0}^{\infty} b_n$ converger a s_{re} y s_{im}, respectivamente.

Notemos también que el término general c_n de una serie convergente tiende necesariamente a 0, ya que ambas partes real a_n e imaginaria b_n tienden a 0. En particular, la sucesión $\{c_n\}$ está acotada, i.e., hay una constante $M > 0$ tal que $|c_n| \leq M$, para todo n.

Ejemplo:
Consideremos la serie geométrica $\sum_{n=0}^{\infty} z^n$ al variar $z \in \mathbb{C}$. Si $z = 1$ sabemos que la serie no converge. Sea ahora $z \neq 1$, escribimos

$$s_n = 1 + z + z^2 + \cdots + z^n = \frac{1 - z^{n+1}}{1 - z} \ ,$$

y usamos el Teorema 2.10.1., para concluir que

$$\lim_{n\to\infty} s_n = \begin{cases} \dfrac{1}{1-z} \ , & |z| < 1 \ , \\ \\ \text{No converge}, & \text{en otro caso.} \end{cases}$$

En conclusión, la serie converge y su suma es $\dfrac{1}{1-z}$ si y solo si $|z| < 1$.

Al igual que con las series de valores reales, diremos que la serie $\sum_{n=0}^{\infty} c_n$ converge absolutamente si converge la serie $\sum_{n=0}^{\infty} |c_n|$. La convergencia absoluta implica la convergencia y tenemos

$$\left| \sum_{n=0}^{\infty} c_n \right| \leq \sum_{n=0}^{\infty} |c_n| \ .$$

Tengamos en cuenta que la serie $\sum_{n=0}^{\infty} |c_n|$ es una serie con términos reales positivos y por lo tanto, a ella se le pueden aplicar todos los criterios ya estudiados en los cursos básicos de matemáticas.

Serie de potencias

Particularmente importantes en el estudio de funciones de variable compleja son las series de potencias. Una serie de potencias tiene la forma

$$\sum_{n=0}^{\infty} a_n (z - z_0)^n \ ,$$

con $\{a_n\}$ sucesión de números complejos, llamados **coeficientes** de la serie y $z_0 \in \mathbb{C}$ llamado el **centro** de la serie. Las siguientes definiciones y resultados se refieren a series con centro en el origen, volvemos al caso general por medio de sustitución $w = z - z_0$. Tengamos en cuenta que una serie de potencias siempre converge al menos en su propio centro z_0.

El primer ejemplo de una serie de potencias es la serie geométrica, considerada anteriormente recordamos que

$$\sum_{n=0}^{\infty} z^n = \frac{1}{1-z} \qquad \text{si} \ \ |z| < 1 \ ,$$

y la serie no converge para $|z| \geq 1$.

Y la serie no converge para $|z| \geq 1$. Veremos que el comportamiento de tales series es típico: de hecho, probaremos que toda serie de potencias converge dentro de un círculo y no converge fuera de él, excepto en los casos límite en los que sólo hay convergencia en el centro de la serie o para cada valor de z. Más precisamente, se cumple el siguiente resultado debido a Abel.

Teorema 2.10.3. Para toda serie de potencias $\sum_{n=0}^{\infty} a_n z^n$ existe un número R, con $0 \leq R \leq +\infty$, llamado **radio de convergencia** con las siguientes propiedades:

a) si $R = 0$, la serie converge solo para $z = 0$.
b) si $R > 0$, la serie converge absolutamente para todo z con $|z| < R$,
si $0 < \rho < R$, la serie converge uniformemente en el círculo $\{|z| \leq \rho\}$.
c) si $R = +\infty$, la serie converge absolutamente para todo $z \in \mathbb{C}$ y
uniformemente para todo círculo $\{|z| \leq \rho\}$ con $\rho > 0$.

Para probar el teorema, asumimos un resultado técnico:

Lema 2.10.4. Dada la serie $\sum_{n=0}^{\infty} a_n z^n$.

a) Si existe $z_1 \neq 0$ donde la serie converge, entonces la serie converge
absolutamente para todo z con $|z| < |z_1|$.
b) Si existe $z_2 \neq 0$ donde la serie no converge, entonces la serie no
converge para todo z con $|z| > |z_2|$.

Demostración:
a) Como la serie $\sum_{n=0}^{\infty} a_n z_1^n$ converge, su termino general $a_n z_1^n$ tiende a 0 cuando $n \to \infty$ y, por lo tanto, la sucesión $\{|a_n z_1^n|\}$ está acotada. Entonces existe una constante $M > 0$ tal que $|a_n z_1^n| \leq M$, para todo n. Sea ahora $z \neq 0$ tal que $|z| < |z_1|$, resulta

$$|a_n z^n| = |a_n z_1^n| \left|\frac{z}{z_1}\right|^n \leq M \left|\frac{z}{z_1}\right|^n \ .$$

La serie $\sum_{n=0}^{\infty} \left|\frac{z}{z_1}\right|^n$ converge ya que es una serie geométrica con $\left|\frac{z}{z_1}\right| < 1$, por lo tanto, aplicando el criterio de comparación válido para series numéricas reales, la serie $\sum_{n=0}^{\infty} a_n z^n$ converge absolutamente.

b) Si la serie convergiera en z con $|z| > |z_2|$, entonces por la primera parte del lema, también debería converger en z_2, contrariamente a la hipótesis.

El lema que acabamos de probar nos permite definir el radio de convergencia de la serie $\sum_{n=0}^{\infty} a_n z^n$ como el límite superior de los módulos de los puntos donde converge la serie.

$$R = \sup \left\{ |z| : \sum_{n=0}^{\infty} a_n z^n \text{ converge} \right\} .$$

Volvamos ahora a la demostración del Teorema 2.10.3.

Demostración: (del Teorema 2.10.3.)
a) Es inmediata a partir de la definición de radio de convergencia (inciso *b)* del Lema 2.10.4.).
b) Sea z con $|z| < R$ por (inciso *b)* del Lema 2.10.4.), existe z_1 con $|z| < |z_1| < R$ en el cual la serie converge. Por el punto a) del Lema 2.10.4., la serie converge absolutamente en z. Ahora sea ρ tal que $0 < \rho < R$. Por lo que acabamos de demostrar, la serie converge absolutamente en el punto $z = \rho$, i.e., la serie $\sum_{n=0}^{\infty} |a_n| \rho^n$ converge. Entonces si $|z| \leq \rho$ tenemos $|a_n z^n| \leq |a_n| \rho^n$. Por el Criterio di Weiertrass[19], la serie converge uniformemente en $\{|z| \leq \rho\}$.
c) La demostración es análoga a la del inciso anterior (*b)*).

Tengamos en cuenta que el teorema no da ninguna indicación de la convergencia de la serie en los puntos de la circunferencia $\{|z| = R\}$.

Ejemplo:
Como se vio anteriormente, la serie geométrica $\sum_{n=0}^{\infty} z^n$ tiene radio de convergencia $R = 1$, al igual que la serie $\sum_{n=0}^{\infty} n z^n$. De hecho, aplicando el criterio del cociente por paso al límite a la serie de módulos, tenemos

$$\lim_{n\to\infty} \frac{(n+1)|z|^{n+1}}{n|z|^n} = |z| ,$$

entonces la serie converge para todo z con $|z| < 1$, además no converge si $|z| > 1$ ya que el término general no tiende a 0.

Para determinar el radio de convergencia de una serie de potencias sin recurrir al estudio directo de la propia serie, es posible utilizar los llamados criterios del cociente y de la raíz. No daremos las demostraciones de estos teoremas ya que son completamente análogas a las ya vistas en cursos de matemáticas anteriores válidas para series de potencias reales $\sum_{n=0}^{\infty} a_n x^n$ con coeficientes $a_n \in \mathbb{R}$ y variable $x \in \mathbb{R}$.

Teorema 2.10.5. Criterio de d'Alembert (Criterio del cociente o de la razón)
Sea $\sum_{n=0}^{\infty} a_n z^n$ una serie de potencias y sea $a_n \neq 0$ para todo n, si existe

$$\lim_{n\to\infty} \left| \frac{a_{n+1}}{a_n} \right| = l ,$$

[19]Sea $\{f_n\}$ una sucesión de funciones de variable real o compleja definidas en un conjunto A. Si para cada $n \in \mathbb{N}$ existe un $M_n \geq 0$ tal que $|f_n(x)| \leq M_n$, $\forall x \in A$ y la serie $\sum_{n\geq 1} M_n$ converge, entonces la serie $\sum_{n\geq 1} f_n$ converge uniformemente en A.

entonces el radio de convergencia R viene dado por

$$R = \begin{cases} 0 & \text{si} \quad l = +\infty \ , \\ \dfrac{1}{l} & \text{si} \quad 0 < l < +\infty \ , \\ +\infty & \text{si} \quad l = 0 \ . \end{cases}$$

Teorema 2.10.6. (Criterio de la raíz)
Sea $\sum_{n=0}^{\infty} a_n z^n$ una serie de potencias y supongamos que existe

$$\lim_{n\to\infty} \sqrt[n]{|a_n|} = l \ ,$$

entonces el radio de convergencia R viene dado por el Teorema 2.10.5.

Ejemplos:
1) Calculemos el radio de convergencia de la serie $\sum_{n=0}^{\infty} \frac{n!}{n^n} z^n$. Usamos el criterio de la razón:

$$\lim_{n\to\infty} \frac{(n+1)!}{(n+1)^{n+1}} \frac{n^n}{n!} = \lim_{n\to\infty} \left(\frac{n}{n+1}\right)^n = \lim_{n\to\infty} \left[\left(1+\frac{1}{n}\right)^n\right]^{-1} = e^{-1} \ ,$$

entonces $R = e$.

2) Sea $\sum_{n=0}^{\infty} n^n$. Aplicando el criterio de la raíz, tenemos:

$$\lim_{n\to\infty} \sqrt[n]{n^n} = \lim_{n\to\infty} n = +\infty \ ,$$

por lo tanto $R = 0$.

Nuestro interés en las series de potencias surge de su comportamiento como funciones. Como ya hemos dicho, una serie de potencias $\sum_{n=0}^{\infty} a_n z^n$, con radio de convergencia $R \neq 0$, converge para $|z| < R$ y por lo tanto define una función $f(z)$. Mostraremos que f es analítica en tal disco. La idea es probar que la derivación término a término es legítima. Empezamos con el siguiente resultado técnico.

Lema 2.10.7. Las dos series de potencias

$$\sum_{n=0}^{\infty} a_n z^n \qquad \wedge \qquad \sum_{n=0}^{\infty} n a_n z^{n-1} \ ,$$

tienen el mismo radio de convergencia.

Demostración:
Primero verificamos que si $\sum_{n=0}^{\infty} a_n z^n$ converge absolutamente en $|z| < R$ $(R \neq 0)$, entonces también la serie $\sum_{n=0}^{\infty} n a_n z^{n-1}$ converge absolutamente allí.

Fijamos z con $0 < |z| < R$ y se elege ρ tal que $|z| < \rho < R$, tenemos

$$|n a_n z^{n-1}| = \frac{n}{|z|} \left(\frac{|z|}{\rho}\right)^n |a_n \rho^n| \ .$$

La serie $\sum_{n\to\infty} n \left(\frac{|z|}{\rho}\right)^n$ converge (como se vio en el ejemplo de la convergencia de la serie geométrica y que $|z| < \rho$), por lo tanto $\lim_{n\to\infty} n \left(\frac{|z|}{\rho}\right)^n = 0$ y por lo tanto existe una constante

$M \geq 0$ tal que $n\left(\frac{|z|}{\rho}\right)^n \leq M$, para toda n, definitivamente

$$\left|na_n z^{n-1}\right| \leq \frac{M}{|z|}|a_n\rho^n| \ ,$$

y, por el criterio de de la razón para series numéricas, la serie $\sum_{n=0}^{\infty} na_n z^{n-1}$ converge absolutamente.
Y viceversa, si la serie $\sum_{n=0}^{\infty} na_n z^{n-1}$ converge absolutamente en $|z| < R$, para todo $z \neq 0$, resulta

$$|a_n z^n| \leq \frac{1}{|z|}\left|na_n z^{n-1}\right| \ ,$$

por lo tanto también la serie $\sum_{n=0}^{\infty} a_n z^n$ converge absolutamente en $|z| < R$.

Teorema 2.10.8. Una serie de potencias $\sum_{n=0}^{\infty} a_n z^n$, con radio de convergencia $R > 0$, representa una función $f(z)$ analítica en el disco $\{|z| < R\}$.

Demostración:
Para $|z| < R$, escribimos

$$f(z) = \sum_{n=0}^{\infty} a_n z^n = s_n(z) + r_n(z) \ ,$$

donde

$$s_n(z) = \sum_{k=0}^{n} a_k z^k \ , \qquad r_n(z) = \sum_{k=n+1}^{\infty} a_k z^k$$

y

$$g(z) = \sum_{n=1}^{\infty} na_n z^{n-1} = \lim_{n\to\infty} s_n'(z) \ .$$

Tenemos que comprobar que $f'(z_0) = g(z_0)$ para todo z_0 con $|z_0| < R$. Sean z y ρ tales que $|z|,\ |z_0| < \rho < R$, podemos escribir

$$\frac{f(z) - f(z_0)}{z - z_0} - g(z_0) = \left(\frac{s_n(z) - s_n(z_0)}{z - z_0} - s_n'(z_0)\right) + (s_n'(z_0) - g(z_0)) + \\ + \left(\frac{r_n(z) - r_n(z_0)}{z - z_0}\right) \ .$$

Además, recordando que $z^k - z_0^k = (z - z_0)(z^{k-1} + z^{k-2}z_0 + \cdots + zz_0^{k-2} + z_0^{k-1})$, tenemos

$$\frac{r_n(z) - r_n(z_0)}{z - z_0} = \frac{1}{z - z_0}\sum_{k=n+1}^{\infty} a_k\left(z^k - z_0^k\right)$$

$$\Rightarrow \quad \frac{r_n(z) - r_n(z_0)}{z - z_0} = \sum_{k=n+1}^{\infty} a_k\left(z^{k-1} + z^{k-2}z_0 + \cdots + zz_0^{k-2} + z_0^{k-1}\right) \ .$$

Usando la desigualdad del triángulo y la condición $|z|,\ |z_0| < \rho$, resulta

$$\left|z^{k-1} + z^{k-2}z_0 + \cdots + zz_0^{k-2} + z_0^{k-1}\right| \leq \\ \leq |z|^{k-1} + |z|^{k-2}|z_0| + \cdots + |z||z_0|^{k-2} + |z_0|^{k-1} \leq k\rho^{k-1}$$

luego

$$\left|\frac{r_n(z) - r_n(z_0)}{z - z_0}\right| \leq \sum_{k=n+1}^{\infty} k|a_k|\rho^{k-1} \ .$$

Esta última expresión es el resto[20] de una serie convergente y tiende a 0 cuando $n \to \infty$. Por lo tanto, dado $\epsilon > 0$, podemos encontrar $n_0 \in \mathbb{N}$ tal que, para todo $n \geq n_0$,

$$\left| \frac{r_n(z) - r_n(z_0)}{z - z_0} \right| < \frac{\epsilon}{3} \ .$$

Además, dado que $\lim_{n\to\infty} s' = g(z_0)$, existe $n_1 \in \mathbb{N}$ tal que, para todo $n \geq n1$,

$$\left| s_n'(z_0) - g(z_0) < \frac{\epsilon}{3} \right| \ .$$

Sea $n \geq n_0,\ n_1$, por definición de derivada, existe $\delta > 0 :\ 0 < |z - z_0| < \delta$ implica

$$\left| \frac{s_n(z)s_n(z_0)}{z - z_0} - s_n'(z_0) \right| < \frac{\epsilon}{3} \ .$$

Finalmente, tenemos

$$\left| \frac{f(z) - f(z_0)}{z - z_0} - g(z_0) \right| < \epsilon \ ,$$

cuando $0 < |z - z_0| < \delta$. Hemos probado que $f'(z_0)$ existe y es igual a $g(z_0)$. Dado que el razonamiento puede repetirse, en realidad hemos demostrado que

$$\begin{aligned} f(z) &= a_0 + a_1 z + a_2 z^2 + \cdots \\ f'(z) &= a_1 + 2a_2 z + 3a_3 z^2 + \cdots \\ &\vdots \\ f^n(z) &= n! a_n + \frac{(n+1)!}{1!} a_{n+1} z + \frac{(n+2)!}{2!} a_{n+2} z^2 + \cdots \\ &\vdots \end{aligned}$$

En particular, $a_n = \dfrac{f^n(0)}{n!}$ y la serie de potencias tiene la forma

$$f(z) = \sum_{n=0}^{\infty} a_n z^n = \sum_{n=0}^{\infty} \frac{f^n(0)}{n!} z^n \ .$$

2.11. Serie de Taylor

La serie $(f(z) = \sum_{n=0}^{\infty} a_n z^n = \sum_{n=0}^{\infty} \frac{f^n(0)}{n!} z^n)$ no es más que el desarrollo en serie de Maclaurin, pero lo hemos obtenido bajo la hipótesis de que $f(z)$ tiene un desarrollo en serie. Sabemos que, si existe, el desarrollo es único; la propiedad fundamental, i.e., que toda función analítica en un punto z_0 admite un desarrollo en serie de Taylor centrado en z_0 y se probará en el siguiente resultado.

[20] **Resto de una serie**: Dada una serie $\sum_{n=1}^{\infty} a_n$ se denomina resto de orden k, y se denota R_k, a la suma $R_k = \sum_{n=k+1}^{\infty} a_n$.

Teorema 2.11.1. (Desarrollo en serie de Taylor)
Sea f analítica en un dominio Ω. Dado $z_0 \in \Omega$, sea $B_{r_0}(z_0)$ una vecindad de z_0 contenida en Ω, entonces para todo $z \in B_{r_0}(z_0)$, tenemos

$$f(z) = \sum_{n=0}^{\infty} \frac{f^{(n)(z_0)}}{n!}(z-z_0)^n = f(z_0) + f'(z_0)(z-z_0) + \frac{1}{2}f''(z_0)(z-z_0) + \cdots ,$$

(i.e., la serie de potencias converge a $f(z)$ si $|z-z_0| < r_0$).

Demostración:
Sea $z \in B_{r_0}(z_0)$, haciendo $|z-z_0| = r < r_0$. Sea r_1 tal que $r < r_1 < r_0$. Sea s cualquier punto de la circunferencia C_1 con centro z_0 y radio r_1, entonces $|s-z_0| = r_1$.
Como f es analítica en $\{|z-z_0| \leq r_1\}$, por la fórmula integral de Cauchy $(f(z_0) = \frac{1}{2\pi i}\int_\gamma \frac{f(z)}{z-z_0}\, dz)$, tenemos

$$f(z) = \frac{1}{2\pi i}\int_{C_1} \frac{f(s)}{s-z}\, ds ,$$

pero

$$\frac{1}{s-z} = \frac{1}{(s-z_0)-(z-z_0)} = \frac{1}{s-z} \quad \frac{1}{1-\dfrac{z-z_0}{s-z_0}} ,$$

recordando que

$$\frac{1}{1-q} = 1 + q + \cdots + q^{n-1} + \frac{q^n}{1-q} ,$$

la expresión anterior con $q = \dfrac{z-z_0}{s-z_0}$ se convierte en

$$\frac{1}{s-z} = \frac{1}{s-z_0}\left(1 + \frac{z-z_0}{s-z_0} + \cdots + \left(\frac{z-z_0}{s-z_0}\right)^{n-1} + \left(\frac{z-z_0}{s-z_0}\right)^n \frac{1}{1-\dfrac{z-z_0}{s-z_0}}\right)$$

entonces

$$\frac{f(s)}{s-z} = \frac{f(s)}{s-z_0} + \frac{f(s)}{(s-z_0)^2}(z-z_0) + \cdots +$$
$$+ \frac{f(s)}{(s-z_0)^n}(z-z_0)^{n-1} + \frac{f(s)}{(s-z)(s-z_0)^n}(z-z_0)^n ,$$

integremos ahora sobre C_1 y dividimos por $2\pi i$, obtenemos

$$f(z) = \frac{1}{2\pi i}\int_{C_1}\frac{f(s)}{s-z}\, ds = \frac{1}{2\pi i}\int_{C_1}\frac{f(s)}{s-z_0}\, ds + \frac{z-z_0}{2\pi i}\int_{C_1}\frac{f(s)}{(s-z_0)^2}\, ds + \cdots +$$
$$+\frac{(z-z_0)^{n-1}}{2\pi i}\int_{C_1}\frac{f(s)}{(s-z_0)^n}\, ds + \frac{(z-z_0)^n}{2\pi i}\int_{C_1}\frac{f(s)}{(s-z)(s-z_0)^n}\, ds .$$

Recordando $(f^{(n)}(z_0) = \frac{n!}{2\pi i}\int_\gamma \frac{f(z)}{(z-z_0)^{n+1}}\, dz)$, tenemos

$$f(z) = f(z_0) + f'(z_0)(z-z_0) + \cdots + \frac{f^{(n-1)}(z_0)}{(n-1)!}(z-z_0)^{n-1} + r_n(z) ,$$

con

$$r_n(z) = \frac{(z-z_0)^n}{2\pi i}\int_{C_1}\frac{f(s)}{(s-z)(s-z_0)}\, ds .$$

Para estimar $r_n(z)$, sea $M = \text{máx}_{s\in C_1} |f(s)|$ y observamos que

$$|s - z| = |s - z_0 - (z - z_0)| \geq |s - z_0| - |z - z_0| = r_1 - r \ ,$$

allora, usando $(|\int_\gamma f(z)dz| \leq ML)$, tenemos

$$|r_n(z)| \leq \frac{r^n}{2\pi} \frac{M2\pi r_1}{(r_1 - r)r_1^n} = \frac{Mr_1}{r_1 - r} \left(\frac{r}{r_1}\right)^n \ .$$

Como $\frac{r_1}{r} < 1$, tenemos $\lim_{n\to\infty} r_n(z) = 0$. Así para cada punto $z \in B_{r_0}(z_0)$, el límite cuando $n \to \infty$ de la suma de los primeros n términos en $(f(z_0) + f'(z_0)(z - z_0) + \cdots + \frac{f^{(n-1)}(z_0)}{(n-1)!}(z - z_0)^{n-1} + r_n(z))$ es $f(z)$ y esto concluye la demostración.

Tengamos en cuenta que el desarrollo en serie de Taylor (Teorema 2.11.1.) es válido en el disco abierto más grande centrado en z_0 y contenido en Ω. El radio de convergencia de la serie de Taylor es, por lo tanto, al menos igual a la distancia de z_0 a la frontera de Ω. Por supuesto, como hemos visto en el Teorema 2.10.8., toda serie de potencias convergente coincide con su propio desarrollo en serie de Taylor.

Como en el caso real, si $z_0 = 0$ hablaremos de la serie o desarrollo de Maclaurin.

Ejemplos:

a) Consideramos la serie geométrica

$$\sum_{n=0}^{\infty} z^n = \frac{1}{1 - z} \ , \qquad |z| < 1 \ .$$

La función $f(z) = \dfrac{1}{1 - z}$ es analítica en $|z| < 1$, y su desarrollo de Maclaurin es

$$\sum_{n=0}^{\infty} z^n \ , \quad \text{de donde también se deriva } f^{(n)}(0) = n! \ .$$

b) Sean $f(z) = e^z$ y $z_0 = 0$. Recordando que todas sus derivadas coinciden con e^z, tenemos que $f^{(n)}(0) = 1$ para todo $n \geq 0$. Por lo tanto, el desarrollo de la serie de Maclaurin de la función es

$$e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!} \ ,$$

y es fácil calcular (por el criterio de la razón) que el radio de convergencia de tal la serie es $R = +\infty$, entonces la igualdad se cumple para todo $z \in \mathbb{C}$.

b) Procediendo como en el inciso anterior, tenemos que las funciones trigonométricas $\text{sen } z$ y $\cos z$ y las funciones hiperbólicas $\text{senh } z$ y $\cosh z$ admiten los siguientes desarrollos en serie de Maclaurin con radio de convergencia $R = +\infty$:

$$\text{sen } z = \sum_{n=0}^{\infty} (-1)^n \frac{z^{2n+1}}{(2n+1)!} \ , \qquad \text{senh } z = \sum_{n=0}^{\infty} \frac{z^{2n+1}}{(2n+1)!} \ ,$$

$$\cos z = \sum_{n=0}^{\infty} (-1)^n \frac{z^{2n}}{(2n)!} \ , \qquad \cosh z = \sum_{n=0}^{\infty} \frac{z^{2n}}{(2n)!} \ .$$

2.12. Serie de Laurent

En muchas aplicaciones encontraremos funciones que no son analíticas en algunos puntos o en algún subconjunto del plano complejo. En consecuencia, no admiten desarrollo en series de Taylor en estos entornos a estos puntos. No obstante, es posible construir representaciones en series de potencias, centradas en un punto de no analiticidad z_0, que contiene potencias positivas y negativas de $(z - z_0)$. De hecho, la descomposición en serie de Laurent permite representar una función analítica en un anillo $\{r_1 < |z - z_0| < r_2\}$ (con $0 \leq r_1 < r_2$) como la suma de una función analítica en el anillo y una analítica en el exterior. En efecto, se cumple el siguiente teorema.

Teorema 2.12.1. Sea f analítica en el anillo $\Omega = \{z \in \mathbb{C} : r_1 < |z - z_0| < r_2\}$ con $z_0 \in \mathbb{C}$ y $0 \leq r_1 \leq r_2$, entonces para todo $z \in \Omega$, tenemos

$$f(z) = \sum_{-\infty}^{+\infty} c_n (z - z_0)^n \ ,$$

donde

$$c_n = \frac{1}{2\pi i} \int_C \frac{f(s)}{(s - z_0)^{n+1}} \, ds \ ,$$

y C es el camino, recorrido en sentido antihorario, cuya traza es la circunferencia $s \in \mathbb{C} : |s - z_0| = r$ con $r_1 < r < r_2$.

Demostración:
Dados $z \in \Omega$ y $|z - z_0| = r$, sea $t > 0$ tal que $r_1 < t < r < r_2$ y denotamos por C_t el camino, recorrido en sentido antihorario, cuya traza es la circunferencia $\{|z - z_0| = t\}$, entonces, recordando la Observación (en la sección de la fórmula integral de Cauchy), la fórmula integral de Cauchy se convierte en

$$f(z) = \frac{1}{2\pi i} \int_C \frac{f(s)}{s - z} \, ds - \frac{1}{2\pi i} \int_{C_t} \frac{f(s)}{s - z} \, ds \ ,$$

como en la demostración del Teorema 2.11.1, en la primera integral escribimos

$$\frac{f(s)}{s - z} = \frac{f(s)}{s - z_0} + \frac{f(s)}{(s - z_0)^2}(z - z_0) + \cdots + \\ + \frac{f(s)}{(s - z_0)^n}(z - z_0)^{n-1} + \frac{f(s)}{(s - z)(s - z_0)^n} \ .$$

Para la segunda integral, notamos que

$$- \frac{1}{s - z} = \frac{1}{(z - z_0) - (s - z_0)} = \frac{1}{z - z_0} \ \frac{1}{1 - \dfrac{s - z_0}{z - z_0}} \ ,$$

y obtenemos la identidad

$$- \frac{f(s)}{s - z} = f(s) \frac{1}{z - z_0} + \frac{f(s)}{(s - z_0)^{-1}} \frac{1}{(z - z_0)^2} + \cdots + \\ + \frac{f(s)}{(s - z_0)^{-n+1}} \frac{1}{(z - z_0)^n} + \frac{(s - z_0)^n f(s)}{(z - s)} \frac{1}{(z - z_0)^n} \ .$$

Como las funciones $f(s)/(s - z_0)^{k+1}$ con $k = -n, \ldots, n$ son analíticas en la región $\{t \leq |z - z_0| \leq r\}$, la integral sobre el camino C coincide con la del camino C_t. Así, tenemos que

$$f(z) = \sum_{k=-n}^{n} c_k (z - z_0)^k + r_n(z) + q_n(z) \ ,$$

con $c_k, k = -n, \ldots, n,$ dada por la fórmula ($c_n = \frac{1}{2\pi i}\int_C \frac{f(s)}{(s-z_0)^{n+1}}\, ds$) y

$$r_n(z) = \frac{(z-z_0)^n}{2\pi i}\int_C \frac{f(s)}{(s-z)(s-z_0)^n}\, ds\ ,$$

$$q_n(z) = \frac{1}{2\pi i(z-z_0)}\int_C \frac{(s-z_0)^n f(s)}{z-s}\, ds\ .$$

La prueba de que $r_n(z) \to 0$ cuando $n \to +\infty$ es idéntica a la vista en el Teorema 2.11.1. De manera similar, para calcular $q_n(z)$, y ahora sea $M = \text{máx}_{s\in C_t}|f(s)|$, entonces

$$|z-s| = |z-z_0-(s-z_0)| \geq |z-z_0| - |s-z_0| = r-t$$

y

$$|q_n(z)| \leq \frac{1}{2\pi r^n}\frac{t^n M 2\pi t}{r-t} = \frac{Mt}{r-t}\left(\frac{t}{r}\right)^n\ .$$

Como $t < r$, $\lim_{n\to\infty} q_n(z) = 0$ y el teorema queda probado.

La serie ($f(z) = \sum_{-\infty}^{+\infty} c_n(z-z_0)^n$) se llama **serie de Laurent**. Nótese que si f es analítica en $\{|z-z_0| < r_2\}$ excepto en el punto z_0, el radio r_1 se puede elegir arbitrariamente pequeño y la expansión se cumple para $0 < |z-z_0| < r_2$. Si f es analítica en todo el disco $\{|z-z_0| < r_2\}$, para $n+1 \leq 0$ también la función $f(z)/(z-z_0)^{n+1}$, entonces todos los coeficientes c_n con n entero negativo son cero y la expansión se reduce al desarrollo de Taylor. Finalmente, no es difícil verificar que la serie de Laurent converge uniformemente en cada subanillo $\{t \leq |z-z_0| \leq r\}$ con $r_1 < t \leq r < r_2$.

2.13. Singularidades aisladas

Definición 2.13.1. Sea f una función analítica en un entorno (o vecindad) de $z_0 \in \mathbb{C}$. Se dice que z_0 es un cero de f si $f(z_0) = 0$.

Definición 2.13.2. Sea f una función analítica en z_0, entonces existe una vecindad $B_{r_0}(z_0)$ dentro de la cual f puede ser representada por su serie de Taylor

$$f(z) = \sum_{n=0}^{\infty} c_n(z-z_0)^n\ , \qquad |z-z_0| < r_0\ .$$

Si z_0 es un cero de f, entonces $c_0 = 0$, si, además,

$$f'(z_0) = f''(z_0) = \cdots = f^{(m-1)}(z_0) = 0 \quad \wedge \quad f^{(m)}(z_0) \neq 0\ ,$$

entonces z_0 se llama **cero de orden** m y

$$f(z) = (z-z_0)^m \sum_{n=0}^{\infty} c_{n+m}(z-z_0)^m = (z-z_0)^m g(z), \quad |z-z_0| < r_0,\ c_0 \neq 0.$$

Observamos que $g(z_0) \neq 0$ y como la función g es continua en z_0, se sigue que es no nula en una vecindad de z_0. Entonces se cumple el siguiente resultado.

Teorema 2.13.3. Sea f analítica en un punto z_0 que es un cero para f. Entonces existe una vecindad de z_0 donde z_0 es el único cero de f a menos que f no sea idénticamente nula. Es decir, los ceros de una función analítica (no nula) están aislados.

Definición 2.13.4. Un punto $z_0 \in \mathbb{C}$ es llamado **singularidad aislada** de f si existe una vecindad de z_0 en la que f es analítica excepto el punto z_0.

Por lo tanto si $z_0 \in \mathbb{C}$ es una singularidad aislada de f, existe $r > 0$ tal que f es analítica en $\Omega = \{z \in \mathbb{C} : 0 < |z - z_0| < r\}$. Así, para todo $z \in \Omega$, f puede ser representada por la serie de Laurent

$$f(z) = \cdots + \frac{c_{-2}}{(z - z_0)^2} + \frac{c_{-1}}{z - z_0} + c_0 + c_1(z - z_0) + c_2(z - z_2)^2 + \cdots .$$

La parte de la serie que contiene las potencias negativas de $z - z_0$ se llama **parte principal** de f en z_0. Usaremos la parte principal para clasificar el tipo de singularidades aisladas de f en z_0.

Definición 2.13.5. Si la parte principal de f en z_0, singularidad aislada de f, contiene al menos un término distinto de cero pero el número de dichos términos es finito, z_0 se llama **polo** de f. Más precisamente, si existe un entero m distinto de cero tal que $c_{-m} \neq 0$ y $c_{-m-1} = c_{-m-2} = \cdots = 0$, i.e.,

$$f(z) = \frac{c_{-m}}{(z - z_0)^m} + \frac{c_{-m+1}}{(z - z_0)^{m-1}} + \cdots + \frac{c_{-1}}{z - z_0} + c_0 + c_1(z - z_0) + \cdots ,$$

se dice que el **polo** es **de orden** m. En particular, si $m = 1$, hablaremos de **polo simple** y si $m = 2$ de polo doble.

Razonando como en el caso de un cero, podemos escribir

$$f(z) = \frac{1}{(z - z_0)^m} \sum_{n=0}^{\infty} c_{-m+n}(z - z_0)^n = \frac{g(z)}{(z - z_0)^m} , \qquad |z - z_0| < r,\ c_{-m} \neq 0,$$

donde g es una función analítica y distinta de cero en una vecindad de z_0.

Definición 2.13.6. Si la parte principal de f en z_0 contiene un número infinito de términos, entonces el punto z_0 se llama punto de **singularidad esencial**.

Definición 2.13.7. Si todos los c_{-m} son cero, decimos que el punto z_0 es una **singularidad removible**.

2.14. Residuos y polos

Definición 2.14.1. Sea z_0 una singularidad aislada de f y sea $r > 0$:

$$f(z) = \sum_{n=-\infty}^{\infty} c_n(z - z_0)^n , \qquad 0 < |z - z_0| < r .$$

Entonces el coeficiente c_{-1} se llama residuo de f en z_0 y se denota por $c_{-1} = \mathrm{Res}_f(z_0)$,

donde

$$\mathrm{Res}_f(z_0) = c_{-1} \frac{1}{2\pi i} \int_C f(z)dz .$$

donde C es una trayectoria cerrada.

Teorema 2.14.2. (Del residuo)
Sea C un camino cerrado y simple dentro del cual y sobre el cual una función f es analítica excepto por un número finito de puntos singulares $z_1, z_2, \ldots, z_n$ pertenecientes al interior de C, entonces

$$\int_C f(z)dz = 2\pi i \sum_{k=1}^{n} \text{Res}_f(z_k) \ .$$

Demostración:
Sea Ω el interior de C, pues tenemos $z_1, z_2, \ldots, z_n \in \Omega$, es posible encontrar n vecindades $B_{r_k}(z_k)$ separadas por pares y enteramente contenidas en Ω. Ahora, sean $C_1, \ldots, C_n$ los caminos cuyas trazas son las circunferencias $\{z \in \Omega : |z - z_k| = r_k\} = \partial B_{r_k}(z_k)$. La frontera del dominio con borde $\Omega_0 = \Omega \backslash \bigcup_{k=1}^{n} B_{r_k}(z_k)$ es la traza de un camino C_0 a la que podemos aplicar el Teorema 2.8.6., y obtener

$$\int_{C_0} f(z)dz = 0 \ ,$$

pero

$$0 = \int_{C_0} f(z)dz = \int_{C_0} f(z)dz - \sum_{k=1}^{n} \int_{C_k} f(z)dz =$$

$$= \int_{C_0} f(z)dz - \sum_{k=1}^{n} \text{Res}_f(z_k) \ .$$

Y así se demuestra el teorema.

Observación: Tengamos en cuenta que el teorema del residuo nos permite transformar una integral a lo largo de un camino genérico en una suma de integrales a lo largo de circunferencias.

Cálculo de residuos

Polos simples
Sea z_0 un polo simple de f, entonces

$$f(z) = \frac{c_{-1}}{z - z_0} + c_0 + c_1(z - z_0) + \cdots = \frac{g(z)}{z - z_0} \ , \qquad 0 < |z - z_0| < r \ ,$$

por lo que resulta

$$\text{Res}_f(z_0) = c_{-1} = g(z_0) \ ,$$

o, también, observando que $g(z) = (z - z_0)f(z)$,

$$\text{Res}_f(z_0) = \lim_{z \to z_0} (z - z_0)f(z) \ .$$

En general, sea $f(z) = \dfrac{n(z)}{d(z)}$, con $n(z_0) \neq 0$ y z_0 cero de orden 1 en $d(z)$,

i.e., $d(z_0) = 0$ pero $d'(z_0) \neq 0$, entonces tenemos

$$\text{Res}_f(z_0) = \frac{n(z_0)}{d'(z_0)} \ .$$

En efecto

$$\mathrm{Res}_f(z_0) = \lim_{z\to z_0}(z-z_0)\ \frac{n(z)}{d(z)} = \lim_{z-z_0}\frac{(z-z_0)}{d(z)-d(z_0)}\ n(z) = \frac{n(z_0)}{d'(z_0)}\ .$$

Polos múltiples
Sea z_0 un polo de orden m de f, entonces

$$f(z) = \frac{c_{-m}}{(z-z_0)^m} + \frac{c_{-m+1}}{(z-z_0)^{m+1}} + \cdots + \frac{c_{-1}}{z-z_0} + c_0 + c_1(z-z_0) + \cdots = \frac{g(z)}{(z-z_0)^m}\ ,$$

con

$$g(z) = c_{-m} + c_{-m+1}(z-z_0) + \cdots + c_{-1}(z-z_0)^{m_1} + \cdots\ ,$$

tenemos

$$\mathrm{Res}_f(z_0) = \frac{1}{(m-1)!}\ g^{(m-1)}(z_0) = \frac{1}{(m-1)!}\ \lim_{z\to z_0}\frac{d^{m-1}}{dz^{m-1}}\ (z-z_0)^m f(z)\ .$$

Ahora, demostremos que la función $\zeta(s)$ es analítica.

Teorema 2.14.3. La función $\zeta(s)$ de Riemann es analítica en la región $A = \{s : \mathrm{Re}(s) > 1\}$.
Demostración: Para todo $n \geq 1$, $s \in \mathbb{C}$:

$$\left|\frac{1}{n^s}\right| = \left|\frac{1}{e^{(\sigma+it)\log n}}\right| = \left|\frac{1}{(e^{(\sigma\log n)})(e^{(it\log n)})}\right| = \left|\frac{1}{e^{\sigma\log n}}\right|\left|\frac{1}{e^{it\log n}}\right| =$$

$$= \left|\frac{1}{(e^{\log n})^\sigma}\right|\cdot 1 = \left|\frac{1}{n^\sigma}\right|\ ,$$

si $\sigma = \mathrm{Re}(s) \geq 1+\delta$ con $\delta > 0$ tenemos la acotación $\left|\frac{1}{n^s}\right| \leq \frac{1}{n^{1+\delta}}$ y ya sabemos que la serie $\sum_{n=1}^{\infty}\frac{1}{n^{1+\delta}}$ es convergente.

Lo cual implica que la serie $\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s}$ es absolutamente convergente en $\mathrm{Re}(s) > 1$, y por el criterio de Weierstrass (ya mencionado, nota 19 al pie de página), también uniformemente convergente. Dado que cada función $1/n^s$ es analítica, también lo es su suma.

En la sección 1.11. (El problema de Basilea), hemos visto que $\zeta(2) = \pi^2/6$. Euler logró encontrar la fórmula para cualquier potencia par, por ejemplo $\zeta(4) = \pi^4/90$, $\zeta(6) = \pi^6/945$. Ahora estamos en condiciones de demostrar el siguiente teorema.

Teorema 2.14.4. Sea n un número entero e indiquemos con B_{2n} a los números de Bernoulli. Sea ζ la función zeta de Riemann, entonces

$$\zeta(2n) = (-1)^{n-1}\ \frac{2^{2n-1}\pi^{2n}B_{2n}}{(2n)!}\ .$$

Demostración: (Antes de realizar la demostración, necesitamos algunos resultados). Determinación de los números de Bernoulli. La función

$$f(x) = \frac{x}{e^x - 1}$$

no está definida en $x = 0$ pero esta singularidad puede ser eliminada debido a que los límites cuando $x \to 0$ por la derecha y por la izquierda son finitos y coinciden, como puede ser comprobarlo fácilmente aplicando la regla de De L'Hopital. La misma cosa ocurre con sus derivadas:

$$f'(x) = \frac{(1-x)e^x - 1}{(e^x-1)^2}\ , \qquad f''(x) = \frac{e^x((x-2)e^x + x + 2)}{(e^x-1)^3}\ ,$$

por lo tanto, podemos encontrar de la serie McLaurin en una vecindad de 0, es decir:

$$\frac{x}{e^x-1}=\sum_{n\geq 0}B_n\frac{x^n}{n!}\ ,$$

donde B_n representa el límite cuando $x\to 0$ de la $n-$ésima derivada de $f(x)$

$$B_n=\lim_{x\to 0}f^{(n)}(x)\ ,$$

con este proceder obtenemos

$$B_0=\lim_{x\to 0}\ \frac{x}{e^x-1}=1\ ,$$

$$B_1=\lim_{x\to 0}\ \frac{(1-x)e^x-1}{(e^x-1)^2}=-\frac{1}{2}\ ,$$

$$B_2=\lim_{x\to 0}\ \frac{e^x((x-2)e^x+x+2)}{(e^x-1)^3}=\frac{1}{6}\ ,$$

etcétera. Los números B_n definidos de esta manera se conocen como números de Bernoulli. Recordando las definiciones de las funciones hiperbólicas

$$\operatorname{sinh}\ z=\frac{e^z-e^{-z}}{2}\ ,\quad \cosh z=\frac{e^z+e^{-z}}{2}\ ,\quad \coth z=\frac{\cosh z}{\operatorname{senh}\ z}\ .$$

Consideremos ahora el siguiente lema.

Lemma 2.14.4.1. $\dfrac{z}{e^z-1}+\dfrac{z}{2}=\dfrac{z}{2}\coth\dfrac{z}{2}.$

Demostración:

$$\frac{z}{e^z-1}+\frac{z}{2}=\frac{2z+z(e^z-1)}{2(e^z-1)}=\frac{2z-z+z(e^z)}{2(e^z-1)}=\frac{z}{2}\cdot\frac{e^z+1}{e^z-1}=$$

$$=\frac{e^{-z/2}}{e^{-z/2}}\cdot\frac{z}{2}\cdot\frac{e^z+1}{e^z-1}=\frac{z}{2}\cdot\frac{e^{z/2}+e^{-z/2}}{e^{z/2}-e^{-z/2}}=\frac{z}{2}\coth\frac{z}{2}\ .$$

Corolario 2.14.4.2. $z\ \coth z=\sum_{n\geq 0}4^nB_{2n}\dfrac{z^{2n}}{(2n)!}.$

Demostración:
Del lema 2.14.4.1., tenemos que $\dfrac{z}{e^z-1}+\dfrac{z}{2}=\dfrac{z}{2}\coth\dfrac{z}{2}$, siempre y cuando

$$\frac{z}{e^z-1}+\frac{z}{2}=\sum_{n\geq 0,\ n\neq 1}B_n\frac{z^n}{n!}\ ,$$

como el término $B_1\dfrac{z^1}{1!}$ es igual a $-\dfrac{z}{2}$, se deduce que

$$\frac{z}{e^z-1}+\frac{z}{2}=\sum_{n\geq 0}B_{2n}\frac{z^{2n}}{(2n)!}\ ,$$

reemplazando $2z$ por z, obtenemos

$$\frac{2z}{e^{2z}-1}+z=z\coth z=\sum_{n\geq 0}B_{2n}\frac{(2z)^{2n}}{(2n)!}=\sum_{n\geq 1}4^nB_{2n}\frac{(z)^{2n}}{(2n)!}\ .$$

Lema 2.14.4.3. $\cot x = i\coth(ix)$.

Demostración:

Como $e^{ix} = i \text{ sen } x + \cos x$ podemos hacer las siguientes sustituciones

$$\cosh ix = \frac{e^{ix}+e^{-ix}}{2} = \frac{i \text{ sen } x + \cos x + i \text{ sen } (-x) + \cos(-x)}{2} =$$

$$= \frac{2\cos x}{2} = \cos x \ ,$$

$$\text{senh } ix = \frac{e^{ix}-e^{-ix}}{2} = \frac{i \text{ sen } x + \cos x - i \text{ sen } (-x) + \cos(-x)}{2} =$$

$$= \frac{2i \text{ sen } x}{2} = i \text{ sen } x \ ,$$

por lo tanto

$$i\coth ix = i\frac{\cosh ix}{\text{senh } ix} = \frac{\cos x}{\text{sen}x} = \cot x \ .$$

Lema 2.14.4.4. $z\cot z = \sum_{n\geq 0}(-4)^n B_{2n}\dfrac{z^{2n}}{(2n)!}$ donde los B_i son los números de Bernoulli.

Demostración:

Por el corolario 2.14.4.2., tenemos que $z\coth z = \sum_{n\geq 0} B_{2n}\dfrac{(2z)^{2n}}{(2n)!}$ además considerando el lema 2.14.4.3., obtenemos

$$z\cot z = zi\coth(iz) = \sum_{n\geq 0} B_{2n}\frac{(2iz)^{2n}}{(2n)!} = \sum_{n\geq 1}(-4)^n B_{2n}\frac{z^{2n}}{(2n)!} \ .$$

Lema 2.14.4.5. $\cot z = \dfrac{1}{2^n}\sum_{k=0}^{2^n-1}\cot\dfrac{z+k\pi}{2^n}$.

Demostración:

Consideremos el caso $n = 1$, tenemos

$$\frac{1}{2}\sum_{k=0}^{1}\cot\frac{z+k\pi}{2} = \frac{1}{2}\cot\frac{z}{2} + \frac{1}{2}\cot\frac{z+\pi}{2} \ ,$$

además sabemos que $\cot\left(\dfrac{z}{2}+\dfrac{\pi}{2}\right) = -\tan\dfrac{z}{2}$, así, tenemos que

$$\frac{1}{2}\cot\frac{z}{2} + \frac{1}{2}\cot\left(\frac{z}{2}+\frac{\pi}{2}\right) = \frac{1}{2}\left(\cot\frac{z}{2} - \tan\frac{z}{2}\right) = \frac{1}{2}\left(\frac{\cos(z/2)}{\text{sen}(z/2)} - \frac{\text{sen } (z/2)}{\cos(z/2)}\right) =$$

$$= \frac{1}{2}\left(\frac{\cos^2(z/2) - \text{sen}^2(z/2)}{\text{sen}(z/2)\cos(z/2)}\right) = \frac{\frac{1}{2}\cos z}{\text{sen}(z/2)\cos(z/2)} \ ,$$

considerando que $\text{sen}(2x) = 2\text{sen } x\cos x$, obtenemos

$$\frac{\frac{1}{2}\cos z}{\text{sen}(z/2)\cos(z/2)} = \frac{1}{2}\cdot\frac{\cos z}{\frac{1}{2}\text{ sen } z} = \frac{\cos z}{\text{sen } z} = \cot z \ ,$$

supongamos ahora que

$$\cot z = \frac{1}{2^n}\sum_{k=0}^{2^n-1}\cot\frac{z+k\pi}{2^n} \ , \quad \text{para } n \geq 1, \text{ usamos}$$

$$\cot(2x) = \frac{1}{2}\left(\cot x - \tan x\right) \ , \quad \text{y tenemos}$$

$$\cot z = \frac{1}{2^n}\sum_{k=0}^{2^n-1} \cot\frac{z+k\pi}{2^n} = \frac{1}{2^{n+1}}\sum_{k=0}^{2^n-1}\left(\cot\frac{z+k\pi}{2^{n+1}} - \frac{\tan z+k\pi}{2^{n+1}}\right) \ ,$$

dado que $-\tan x = \cot\left(x+\frac{\pi}{2}\right)$, obtenemos

$$\cot z = \frac{1}{2^{n+1}}\sum_{k=0}^{2^n-1}\left(\cot\frac{z+k\pi}{2^{n+1}} + \cot\left(\frac{z+k\pi}{2^{n+1}}+\frac{\pi}{2}\right)\right) =$$

$$= \frac{1}{2^{n+1}}\sum_{k=0}^{2^n-1}\left(\cot\frac{z+k\pi}{2^{n+1}} + \cot\left(\frac{z+(k+2^n)\pi}{2^{n+1}}\right)\right) =$$

$$= \frac{1}{2^{n+1}}\sum_{k=0}^{2^n-1}\left(\cot\frac{z+k\pi}{2^{n+1}}\right) + \frac{1}{2^{n+1}}\sum_{k=0}^{2^n-1}\left(\cot\frac{z+(k+2^n)\pi}{2^{n+1}}\right) =$$

$$= \frac{1}{2^{n+1}}\sum_{k=0}^{2^n-1}\left(\cot\frac{z+k\pi}{2^{n+1}}\right) + \frac{1}{2^{n+1}}\sum_{k=2^n}^{2^{n+1}-1}\left(\cot\frac{z+k\pi}{2^{n+1}}\right) =$$

$$= \frac{1}{2^{n+1}}\sum_{k=0}^{2^{n+1}-1}\left(\cot\frac{z+k\pi}{2^{n+1}}\right) \ .$$

Corolario 2.14.4.6. $z\cot z = 1 - 2\sum_{k\geq 1}\ \frac{z^2}{k^2\pi^2 - z^2}$.

Lema 2.14.4.7. $\lim_{z\to 0}\ z\cot z = 1$

Lema 2.14.4.8. $\frac{z^2}{k^2\pi^2 - z^2} = \sum_{n\geq 1}\ \frac{z^{2n}}{k^{2n}\pi^{2n}}$.

Demostración:
Recordemos que

$$\frac{1}{1-x} = 1 + x + x^2 + \cdots \ , \qquad \frac{x}{1-x} = x + x^2 + x^3 + \cdots \ ,$$

sea $x = \frac{z^2}{k^2\pi^2}$, sustituyendo, obtenemos

$$\frac{\left(\frac{z^2}{k^2\pi^2}\right)}{1-\left(\frac{z^2}{k^2\pi^2}\right)} = \frac{\left(\frac{z^2}{k^2\pi^2}\right)}{\left(\frac{k^2\pi^2-z^2}{k^2\pi^2}\right)} = \frac{z^2}{k^2\pi^2 - z^2} \ .$$

Ahora podemos demostrar el Teorema 2.14.4.

Demostración (del Teorema 2.14.4.):
Por el corolario 2.14.4.6., tenemos que

$$z\cot z = 1 - 2\sum_{k\geq 1}\frac{z^2}{k^2\pi^2 - z^2} \ ,$$

aplicando el lema 2.14.4.8., también podemos escribir

$$z\cot z = 1 - 2\sum_{k\geq 1}\left(\frac{z^2}{k^2\pi^2} + \frac{z^4}{k^4\pi^4} + \frac{z^6}{k^6\pi^6} + \cdots\right) ,$$

dado que para cada suma, k puede tomar todos los valores mayor o igual a 1, podemos reemplazar la sumatoria $\sum_{k\geq 1}$ con

$$z\cot z = 1 - 2\left(\frac{z^2\zeta(2)}{\pi^2} + \frac{z^4\zeta(4)}{\pi^4} + \frac{z^6\zeta(6)}{\pi^6} + \cdots\right) ,$$

por el lema 2.14.4.4., tenemos que

$$z\cot z = \sum_{n\geq 0}(-4)^n B_{2n}\frac{z^{2n}}{(2n)!} = B_0 + \sum_{n\geq 1}(-4)^2 B_{2n}\frac{z^{2n}}{(2n)!} =$$

$$= 1 + \sum_{n\geq 1}(-4)^n B_{2n}\frac{z^{2n}}{(2n)!} ,$$

igualando las dos últimas ecuaciones, obtenemos la relación

$$-2\left(\frac{z^2\zeta(2)}{\pi^2} + \frac{z^4\zeta(4)}{\pi^4} + \frac{z^6\zeta(6)}{\pi^6} + \cdots\right) = \sum_{n\geq 1}(-4)^n B_{2n}\frac{z^{2n}}{(2n)!} ,$$

esto último nos da que para cada término $n \geq 1$

$$-2z^{2n}\ \frac{\zeta(2n)}{\pi^{2n}} = (-4)^n B_{2n}\ \frac{z^{2n}}{(2n)!} ,$$

explícitamente para $\zeta(2n)$ tenemos

$$\zeta(2n) = (-4)^n B_{2n}\ \frac{\pi^{2n}}{(-2)(2n)!)} ,$$

$$\zeta(2n) = (-1)^{n-1}\ \frac{2^{2n-1}\pi^{2n}B_{2n}}{(2n)!} .$$

Nota: En la sección 1.5. (Números trascendentales) se definió la constante de Euler-Mascheroni, ahora mostramos la relación de γ y la función zeta de Riemann. γ también puede ser expresada como suma infinita, cuyos términos invocan la función zeta de Riemann evaluada en números positivos:

$$\gamma = \sum_{k=2}^{\infty}\frac{(-1)^k\zeta(k)}{k} = \ln\left(\frac{4}{\pi}\right) + \sum_{k=2}^{\infty}\frac{(-1)^k\zeta(k)}{2^{k-1}k} = \ln\left(\frac{4}{\pi}\right) + \sum_{k=1}^{\infty}\frac{(-1)^{k-1}\zeta(k+1)}{2^k(k+1)}.$$

2.15. Continuación analítica

La continuación analítica permite "prolongar" una función analítica (definida sobre un dominio dado) a una función analítica definida sobre un dominio mayor, y de manera única bajo ciertas condiciones. Precisamente, dadas las funciones f_1 analítica sobre el dominio D_1, y f_2 analítica sobre el dominio D_2, tales que $D_1 \cap D_2 \neq \emptyset$ y $f_1 = f_2$, sobre $D_1 \cap D_2$, entonces $f_1 = f_2$ sobre $D_1 \cup D_2$.

Consideremos ahora que tenemos una función analítica definida por una serie de potencias convergente en un cierto disco

$$f(z) = \sum_{n=0}^{\infty} a_n (z-a)^n, \quad |z-a| < R \ .$$

Esta situación no es artificial, con frecuencia la solución de muchos problemas de la física matemática viene dada por una función analítica definida por su serie de potencias. Es natural preguntarse si dicha función puede prolongarse mas allá del disco donde está inicialmente definida sin perder la analiticidad. Si se piensa un poco, caeremos en que hay un procedimiento "natural" para tratar de extender f de forma analítica, pues las funciones analíticas vienen dadas localmente por series de potencias. Entonces, la idea es considerar un punto cualquiera $b \neq a$ en el disco $D(a,R)$ donde inicialmente está definida f y desarrollar f en serie de potencias centrada en b. De esta forma obtenemos una nueva serie de potencias $\sum b_n (z-b)^n$ con radio de convergencia $R_b > 0$ que define una función

$$f_1(z) = \sum_{n=0}^{\infty} b_n (z-b)^n, \quad |z-b| < R_b \ ,$$

tal que $f_1(z) = f(z)$ para todo $z \in D(a,R) \cap D(b,R_b)$. Puede ocurrir que el disco $D(b,R_b)$ se salga fuera del disco $D(a,R)$. En tal caso, la función $F : D(a,R) \cup D(b,R_b) \to \mathbb{C}$ dada por

$$F(z) = \begin{cases} f(z) & \text{si} \quad z \in D(a,R), \\ \\ f_1(z) & \text{si} \quad z \in D(b,R_b). \end{cases}$$

Es una extensión analítica de f al dominio $D(a,R) \cup D(b,R_B)$. Lo más interesante es que esta es la única posible extensión de f a dicho dominio como se deduce fácilmente del principio de identidad[21].
Podemos repetir ahora con f_1 este mismo proceso y así podríamos continuar indefinidamente (al menos en teoría).

De esta forma lo que obtenemos es una colección de series de potencias con sus discos de convergencia, la unión de los cuales es un abierto en el que podemos definir una "función" que "prolonga analíticamente" a la función inicial. Puede ocurrir que la "función" así obtenida no sea una verdadera función sino una correspondencia, i.e, una función multiforme. Resulta así que las funciones multiformes complejas aparecen de manera completamente natural en el proceso de prolongación analítica.

Ejemplo:
Obtener una prolongación analítica del disco $|z+1| < 2$ para la función $f(z) = \dfrac{2z+3}{z-1}$, de tal manera que ahora en nuestra nueva región esté contenido el punto $z = 1+i$.

[21] Principio de identidad: Sean $f, g : G \to \mathbb{C}$ holoformas, $f = g \ \Leftrightarrow \ \{z \in G : f(z) = g(z)\}$ tiene un punto de acumulación en G.

Para prolongar analíticamente la función de manera que el punto $z = 1 + i$ esté contenido en la nueva región, basta tomar un punto adecuado del disco $|z + 1| < 2$ tal que su distancia al punto $1 + i$ sea menor que su distancia al punto donde está la singularidad mas próxima de la función. Así, por ejemplo, el punto $z = i$ está a distancia 1 de $z = 1 + i$, y a distancia $\sqrt{2}$ de la singularidad mas próxima de la función, que está en el punto $z = 1$. tenemos, entonces

$$f(z) = \frac{2z+3}{z-1} = 2 + \frac{5}{z-1} = 2 - \frac{5}{1-i-(z-i)} = 2 - \frac{\dfrac{5}{1-i}}{1 - \dfrac{z-i}{1-i}} ,$$

$$\Rightarrow \quad f(z) = 2 - \frac{5}{1-i} \sum_{n=0}^{\infty} \left(\frac{z-i}{1-i} \right)^n , \quad \text{que converge si } |z-i| < |1-i| = \sqrt{2}.$$

Definición 2.15.1. La función zeta de Riemann $\zeta(s)$ es la continuación analítica de la serie de Dirichlet[22] en el plano complejo a excepción del punto $s = 1$.

Por lo tanto, si encontramos una función analítica en $\mathbb{C} \setminus \{1\}$ que coincida con nuestra serie de Dirichlet en cualquier dominio, D, entonces podemos definir $\zeta(s)$ para todo $s \in \mathbb{C} \setminus \{1\}$.

Definir la función zeta de Riemann de esta manera es conciso y correcto, pero sus propiedades no están claras. Continuamos construyendo la función zeta encontrando la continuación analítica de $\zeta(s)$ explícitamente. Para empezar, cuando $\mathrm{Re}(s) > 1$, escribimos

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \sum_{n=1}^{\infty} n \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) = s \sum_{n=1}^{\infty} n \int_n^{n+1} x^{-s-1} dx ,$$

pues tenemos

$$\begin{aligned}
\zeta(s) = \sum_{n=1}^{\infty} n \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) &= (1) \left(\frac{1}{(1)^s} - \frac{1}{((1)+1)^s} \right) + \\
&+ (2) \left(\frac{1}{(2)^s} - \frac{1}{((2)+1)^s} \right) + (3) \left(\frac{1}{(3)^s} - \frac{1}{((3)+1)^s} \right) + \\
&+ (4) \left(\frac{1}{(4)^s} - \frac{1}{((4)+1)^s} \right) + \cdots + (n-1) \left(\frac{1}{(n-1)^s} - \frac{1}{((n-1)+1)^s} \right) + \\
&+ n \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) + (n+1) \left(\frac{1}{(n+1)^s} - \frac{1}{((n+1)+1)^s} \right) + \cdots = \\
&= \frac{1}{1^s} - \frac{1}{2^s} + (2)\frac{1}{2^s} - (2)\frac{1}{3^s} + (3)\frac{1}{3^s} - (3)\frac{1}{4^s} + (4)\frac{1}{4^s} - (4)\frac{1}{5^s} + \\
&+ (5)\frac{1}{5^s} - (5)\frac{1}{6^s} + \cdots + (n-1)\frac{1}{(n-1)^s} - (n-1)\frac{1}{n^s} + \cdots + \\
&+ (n)\frac{1}{n^s} - (n)\frac{1}{(n+1)^s} + (n+1)\frac{1}{(n+1)^s} - (n+1)\frac{1}{(n+2)^s} + \cdots = \\
&= \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4} + \frac{1}{5^s} + \cdots + n\frac{1}{(n-1)^s} - \frac{1}{(n-1)^s} - n\frac{1}{n^s} + \frac{1}{n^s} +
\end{aligned}$$

[22] Serie de Dirichlet es toda serie del tipo $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ donde s y a_n para $n = 1, 2, 3, \ldots$ son números complejos.

$$+n\frac{1}{n^s}-n\frac{1}{(n+1)^s}+n\frac{1}{(n+1)^s}+\frac{1}{(n+1)^s}-n\frac{1}{(n+2)^s}-\frac{1}{(n+2)^s}+\cdots=$$
$$=\frac{1}{1^s}+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4}+\frac{1}{5^s}+\cdots+n\frac{1}{(n-1)^s}-\frac{1}{(n-1)^s}+\frac{1}{n^s}+$$
$$+\frac{1}{(n+1)^s}-n\frac{1}{(n+2)^s}-\frac{1}{(n+2)^s}+\cdots=$$
$$=\frac{1}{1^s}+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4}+\frac{1}{5^s}+\cdots+\frac{1}{n^s}+\cdots=\sum_{n=1}^{\infty}\frac{1}{n^s}\ .$$

y también se verifica que

$$s\sum_{n=1}^{\infty}n\int_n^{n+1}x^{-s-1}dx=\ s\sum_{n=1}^{\infty}n\left[\frac{x^{-s-1+1}}{-s-1+1}\right]_n^{n+1}=s\sum_{n=1}^{\infty}n\left[\frac{x^{-s}}{-s}\right]_n^{n+1}=$$
$$=s\sum_{n=1}^{\infty}n\left[\frac{(n+1)^{-s}}{-s}-\frac{(n)^{-s}}{-s}\right]=s\sum_{n=1}^{\infty}n\left[\frac{(n+1)^{-s}-n^{-s}}{-s}\right]=$$
$$=\sum_{n=1}^{\infty}n\ \frac{s}{-s}\left[(n+1)^{-s}-n^{-s}\right]=\sum_{n=1}^{\infty}n-\left((n+1)^{-s}-n^{-s}\right)=$$
$$=\sum_{n=1}^{\infty}n\left(n^{-s}-(n+1)^{-s}\right)=\sum_{n=1}^{\infty}n\left(\frac{1}{n^s}-\frac{1}{(n+1)^s}\right)\ .$$

Sea $x=[x]+\{x\}$, donde $[x]$ y $\{x\}$ son las partes entera y fraccionaria de x, respectivamente. Como $[x]$ es siempre la constante n para cualquier x en el intervalo $[n,n+1)$, tenemos

$$\zeta(s)=s\sum_{n=1}^{\infty}\int_n^{n+1}[x]x^{-s-1}dx=s\int_1^{\infty}[x]x^{-s-1}dx\ ,$$

escribiendo $[x]=x-\{x\}$, obtenemos

$$s\int_1^{\infty}(x-\{x\})x^{-s-1}dx=s\int_1^{\infty}\left(xx^{-s-1}-\{x\}x^{-s-1}\right)dx=$$
$$=s\int_1^{\infty}xx^{-s-1}dx-s\int_1^{\infty}\{x\}x^{-s-1}dx=$$
$$=s\int_1^{\infty}x^{-s-1+1}dx-s\int_1^{\infty}\{x\}x^{-s-1}dx=$$
$$=s\int_1^{\infty}x^{-s}dx-s\int_1^{\infty}\{x\}x^{-s-1}dx=$$
$$=s\left[\frac{x^{-s+1}}{-s+1}\right]_1^{\infty}-s\int_1^{\infty}\{x\}x^{-s-1}dx=$$
$$=s\lim_{x\to\infty}\frac{x^{1-s}}{1-s}-s\ \frac{(1)^{1-s}}{1-s}-s\int_1^{\infty}\{x\}x^{-s-1}dx=$$
$$=s\cdot(0)-s\ \frac{1}{1-s}-s\int_1^{\infty}\{x\}x^{-s-1}dx=$$
$$=\frac{s}{s-1}-s\int_1^{\infty}\{x\}x^{-s-1}dx\ ,$$

$$\Rightarrow \quad \zeta(s) = \frac{s}{s-1} - s\int_1^\infty \{x\}x^{-s-1}dx \ , \quad \sigma > 0 \ .$$

Ahora observamos que como $0 \leq \{x\} < 1$, la integral impropia anterior converge cuando $\sigma > 0$ porque la integral $\int_1^\infty x^{-\sigma-1}dx$ converge. Así, la integral impropia anterior define una función analítica de s en la región $\mathrm{Re}(s) > 0$. Por lo tanto, la función meromorfa[23] del lado derecho nos da la continuación analítica de $\zeta(s)$ a la región $\mathrm{Re}(s) > 0$, y el término $\frac{s}{s-1}$ da el polo simple de $\zeta(s)$ en $s = 1$ con residuo 1.

La ecuación anterior (última implicación) extiende la definición de la función zeta de Riemann solo a la región mayor $\mathrm{Re}(s) > 0$. Sin embargo, Riemann utilizó un argumento similar para obtener la continuación analítica de todo el plano complejo. Partió de la definición clásica de la función gamma Γ.

La función gamma extiende la función factorial a todo el plano complejo con excepción de los enteros no positivos. La definición habitual de la función gamma, $\Gamma(s)$, es mediante la integral de Euler.

Definición 2.15.2. La función Gamma está definida por la fórmula integral

$$\Gamma(s) = \int_0^\infty t^{s-1}e^{-t}dt \ ,$$

la integral converge absolutamente para $\mathrm{Re}(s) > 0$, la función Gamma tiene propiedades muy interesantes.

Propiedades:

1. $\Gamma(s)$ es definida y analítica en la región $\mathrm{Re}(s) > 0$.

   Demostración:

   Primero, tengamos en cuenta que para $\mathrm{Re}(s) > 0$ la función definida por $\int_a^\infty e^{-t}t^{s-1}dt$ es analítica. Así, solo necesitamos demostrar que es uniformemente convergente y luego podemos aplicar el (**Corolario**: Sea D un conjunto abierto y $\psi : [a, \infty] \times D \to \mathbb{C}$ sea continuo con derivada parcial continua $\frac{\partial\psi}{\partial z}$. Si la integral $\int_a^\infty \psi(t, z)dt$ converge uniformemente en subconjuntos compactos de D entonces define una función analítica allí y tiene derivada $\int_a^\infty \frac{\partial\psi}{\partial z}(t, z)dt$), ya que se cumplen todas las demás hipótesis. Como era de esperar, el exponencial domina la integral dando

   $$\begin{aligned}\left|\int_a^n e^{-t}t^{s-1}dt - \int_a^\infty e^{-t}t^{s-1}dt\right| &= \left|\int_n^\infty e^{-t}t^{s-1}dt\right| \\ &\leq \int_n^\infty e^{-t}t^{\sigma-1}dt \\ &\leq C\int_n^\infty e^{-\frac{1}{2}t}dt \\ &= 2Ce^{-\frac{1}{2}n} \ ,\end{aligned}$$

   y $2Ce^{-\frac{1}{2}n} \to 0$ como $n \to \infty$ dando la convergencia uniforme. Ahora para $\sigma > 0$ tenemos

   $$f_n(s) = \int_{\frac{1}{n}}^\infty e^{-t}t^{s-1}dt \ .$$

[23] Una función se dice meromorfa si es analítica en una región A excepto en los polos y, A está contenida en el dominio de la función.

Según el argumento anterior, cada f_n es analítica. Supongamos que $\sigma \geq c > 0$. Para $0 < t \leq 1$ tenemos $e^{-t} < 1$ y $t^{\sigma-1} \leq t^{c-1}$. Por lo tanto, para $n > m$

$$\left| \int_{\frac{1}{n}}^{\frac{1}{m}} e^{-t} t^{s-1} dt \right| < \int_{\frac{1}{n}}^{\frac{1}{m}} t^{c-1} dt = \frac{1}{c} \left(\frac{1}{m^a} - \frac{1}{n^a} \right) .$$

Dado $\epsilon > 0$ podemos elegir $0 < \delta < 1 : \frac{1}{c}(\frac{1}{m^a} - \frac{1}{n^a}) < \epsilon$ siempre que $|\frac{1}{m^a} - \frac{1}{n^a}| < \delta$. Por lo tanto, f_n satisface la condición de Cauchy para la convergencia uniforme para subconjuntos compactos del semiplano $\sigma > 0$. Ahora, aplicando el (**Lema**: Supongamos que (f_n) es una secuencia de funciones analíticas en un subconjunto abierto D de $\mathbb{C}$. Si (f_n) converge uniformemente en cada subconjunto compacto (cerrado y acotado) de D a la función límite f entonces f es analítica en D. Además, la secuencia de derivadas (f_n') converge uniformemente en subconjuntos compactos de D a f'.) vemos que la función gamma es analítica para $\sigma > 0$.

Podemos demostrar que la función Γ es una extensión de la función factorial para argumentos complejos, por medio de la propiedad 3. (ecuación funcional).

2. $\Gamma(n+1) = n!$, para enteros $n \geq 0$.

3. $\Gamma(s+1) = s\Gamma(s)$ (ecuación funcional[24]), esta propiedad y la propiedad número 2 caracterizan a la función factorial. Por lo tanto, la función $\Gamma(s)$ generaliza $n!$ a los números complejos s. Algunos autores suelen escribir también $\Gamma(s+1) = s!$.

   Demostración:

   $$\Gamma(s+1) = \int_0^\infty t^{(s+1)-1} e^{-t} dt \ , \quad \text{integrando por partes,}$$

   sean $u = t^s \ \rightarrow \ du = st^{s-1}$, $dv = e^{-t} \ \rightarrow \ v = -e^{-t}$, así

   $$\Gamma(s+1) = \int_0^\infty t^s e^{-t} dt = -e^{-t} t^s \Big|_0^\infty - \int_0^\infty (st^{s-1})(-e^{-t}) dt$$

   $$= 0 \ + s \int_0^\infty t^{s-1} e^{-t} dt = s\Gamma(s) \ .$$

   Por cálculo directo $\Gamma(1) = 1$ y por lo tanto por inducción $\Gamma(n+1) = n!$ (de forma análoga como se hizo para calcular $\Gamma(s+1)$) para todos los números enteros positivos n. Esto muestra que $\Gamma(n+1)$ y $n!$ siguen la misma recurrencia y son iguales para todo n.

4. $\Gamma(s)$ puede continuarse analíticamente como meromorfa en todo el plano con polos simples en $0, -1, -2, \ldots$. Los residuos son

   $$\text{Res}_\Gamma(-n) \equiv \text{Res}(\Gamma, -n) = \frac{(-1)^n}{n!} \ .$$

   Demostración:

   Por la propiedad 3, $\Gamma(s+1) = s\Gamma(s)$, tenemos

   $$\Gamma(s+1+1) = s(s+1)\Gamma(s)$$

[24] **Definición**. Una ecuación funcional es aquella cuya incógnita es una función, que debe determinarse en todo su dominio. Por ejemplo: Determinar todas las funciones tales que $f(x+y) = f(x) + f(y)$. Si el dominio está formado sólo por números racionales, las únicas soluciones son del tipo $f(x) = k \cdot x$, donde k es una constante arbitraria.

$$\Gamma(s+1+2) = s(s+1)(s+2)\Gamma(s)$$
$$\Gamma(s+1+3) = s(s+1)(s+2)(s+3)\Gamma(s)$$
$$\vdots$$
$$\Gamma(s+1+n) = s(s+1)(s+2)(s+3)\cdots(s+n)\Gamma(s)$$
$$\Gamma(s+n) = s(s+1)(s+2)(s+3)\cdots(s+n-1)\Gamma(s)$$
$$\Gamma(s) = \frac{\Gamma(s+n)}{s(s+1)(s+2)\cdots(s+n-1)} \ ,$$

para cualquier entero positivo n. Ahora $\Gamma(s+n)$ es analítica para $\sigma > -n$ entonces la función en la derecha es meromorfa para $\sigma > -n$ con polos simples en $0, -1, -2, \ldots, -(n-1)$. Como n es arbitrario, hemos terminado. Por construcción, esta extensión de Γ satisface la propiedad 3. Para calcular los residuos, tenemos

$$\Gamma(s) = \frac{\Gamma(s+n+1)}{s(s+1)(s+2)\cdots(s+n)} \ ,$$

entonces

$$\begin{aligned}\mathrm{Res}(\Gamma, -n) &= \lim_{s\to -n} \frac{(s+n)\Gamma(s+n+1)}{s(s+1)(s+2)\cdots(s+n)} \\ &= \lim_{s\to -n} \frac{\Gamma(s+n+1)}{s(s+1)(s+2)\cdots(s+n-1)} \\ &= \frac{(-1)^n}{n!} \ ,\end{aligned}$$

donde hemos usado $\Gamma(1) = 1$ en el numerador.

5. $$\Gamma(s) = \left[s e^{\gamma s} \prod_{n=1}^{\infty} \left(1 + \frac{s}{n}\right) e^{-\frac{s}{n}} \right]^{-1} \ ,$$

   γ es la constante de Euler-Mascheroni (definida en la sección 1.5.). Tengamos en cuenta que el producto infinito aclara las posiciones de los polos de Γ.

6. $$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\mathrm{sen}(\pi s)} \ ,$$

   y con la propiedad número 5, esto da una fórmula de producto para la función $\mathrm{sen}(\pi s)$.

7. $\Gamma(s+1) \approx \sqrt{2\pi}\, s^{s+1/2} e^{-s}$ para $|s|$ grande, $\mathrm{Re}(s) > 0$. En particular, $n! \approx \sqrt{2\pi}\, n^{n+1/2} e^{-s}$. (Fórmula de Stirling).

8. $2^{2s-1}\Gamma(s)\Gamma(s+1/2) = \sqrt{\pi}\, \Gamma(2s)$. (F. de duplicación de Legendre).

Ya hemos definido a la función gamma $\Gamma(s)$, mediante la integral de Euler $\Gamma(s) = \int_0^\infty e^{-t} t^{s-1} dt$, pero esto se aplica sólo para $\mathrm{Re}(s) > 0$. Ahora con la fórmula de Weierstrass

Definición 2.15.3. Fórmula de Weierstrass

$$\frac{1}{s\Gamma(s)} := e^{\gamma s} \prod_{n=1}^{\infty} \left(1 + \frac{s}{n}\right) e^{-\frac{s}{n}} \ ,$$

donde γ es la constante de Euler-Mascheroni, se aplica en todo el plano complejo. La función Γ es analítica en todo el plano complejo con la excepción de $s = 0, -1, -2, \ldots,$ y el residuo de $\Gamma(s)$ en $s = -n$ es $\frac{(-1)^n}{n!}$ (por la propiedad número 4 de la función gamma). Notemos que para $s \in \mathbb{N}$ tenemos que $\Gamma(s) = (s-1)!$.

Para Γ de $s/2$ tenemos

$$\Gamma\left(\frac{s}{2}\right) = \int_0^\infty e^{-t} t^{\frac{s}{2}-1} dt \ ,$$

para $\sigma > 0$. Haciendo $t = n^2\pi x$, tenemos

$$\Gamma\left(\frac{s}{2}\right) = \int_0^\infty e^{-n^2\pi x}(n^2\pi x)^{\frac{s}{2}-1}(n^2\pi\ dx) = \int_0^\infty n^{s-2}\pi^{\frac{s}{2}-1}x^{\frac{s}{2}-1}e^{-n^2\pi x}n^2\pi\ dx =$$

$$= \int_0^\infty n^{s-2+2}\pi^{\frac{s}{2}-1+1}x^{\frac{s}{2}-1}e^{-n^2\pi x}\ dx = \int_0^\infty n^s\pi^{\frac{s}{2}}x^{\frac{s}{2}-1}e^{-n^2\pi x}\ dx$$

$$\Rightarrow\ \Gamma\left(\frac{s}{2}\right) = n^s\pi^{\frac{s}{2}}\int_0^\infty x^{\frac{s}{2}-1}e^{-n^2\pi x}dx\ \Rightarrow\ \Gamma\left(\frac{s}{2}\right)n^{-s}\pi^{-\frac{s}{2}} = \int_0^\infty x^{\frac{s}{2}-1}e^{-n^2\pi x}dx$$

$$\Rightarrow\quad \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)n^{-s} = \int_0^\infty x^{\frac{s}{2}-1}e^{-n^2\pi x}dx\ .$$

Ahora, con cuidado aplicando la suma sobre n en la integral respecto a x, para $\sigma > 1$, tenemos

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\sum_{n=1}^\infty n^{-s} = \int_0^\infty x^{\frac{s}{2}-1}\left(\sum_{n=1}^\infty e^{-n^2\pi x}\right)dx$$

$$\Rightarrow\quad \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \int_0^\infty x^{\frac{s}{2}-1}\left(\sum_{n=1}^\infty e^{-n^2\pi x}\right)dx\ .$$

Definición 2.15.4. Función theta de Jacobi

$$\vartheta(x) := \sum_{n=-\infty}^\infty e^{-n^2\pi x}\ .$$

ahora, por propiedades de la función theta de Jacobi:

$$\psi(x) := 1 + 2\sum_{n=1}^\infty e^{-n^2\pi x} \quad \wedge \quad 2\psi(x) = \vartheta(x) - 1\ ,$$

y también

$$\vartheta(x) = \frac{1}{\sqrt{x}}\ \vartheta\left(\frac{1}{x}\right)\ , \quad \text{(ecuación de transformación).}$$

Luego

$$\Rightarrow\quad \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \int_0^\infty x^{\frac{s}{2}-1}\ \psi(x)\ dx \quad \wedge \quad \psi(x) = \frac{1}{\sqrt{x}}\psi\left(\frac{1}{x}\right) + \frac{1}{2\sqrt{x}} - \frac{1}{2}$$

$$\Rightarrow\quad \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \int_0^1 x^{\frac{s}{2}-1}\ \psi(x)\ dx + \int_1^\infty x^{\frac{s}{2}-1}\ \psi(x)\ dx$$

sea $u = \dfrac{1}{x}\ \Rightarrow\ du = -\dfrac{1}{x^2}$; ahora si $x = 0\ \Rightarrow\ u = \infty$, si $x = 1\ \Rightarrow u = 1$,

$$\Rightarrow\quad \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \int_\infty^1 \left(\frac{1}{u}\right)^{\frac{s}{2}-1}\psi\left(\frac{1}{u}\right)\left(-\left(\frac{1}{u}\right)^2\right)du + \int_1^\infty x^{\frac{s}{2}-1}\psi(x)\ dx$$

$$\Rightarrow \quad \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = -\int_{\infty}^{1}\left(\frac{1}{u}\right)^{\frac{s}{2}-1}\psi\left(\frac{1}{u}\right)\frac{1}{u^2}\,du + \int_{1}^{\infty}x^{\frac{s}{2}-1}\psi(x)\,dx$$

$$\Rightarrow \quad \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = -\int_{\infty}^{1}\left(u^{-1}\right)^{\frac{s}{2}-1}u^{-2}\psi\left(\frac{1}{u}\right)\,du + \int_{1}^{\infty}x^{\frac{s}{2}-1}\psi(x)\,dx$$

$$\Rightarrow \quad \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = -\int_{\infty}^{1}u^{\frac{-s}{2}+1-2}\psi\left(\frac{1}{u}\right)\,du + \int_{1}^{\infty}x^{\frac{s}{2}-1}\psi(x)\,dx$$

$$\Rightarrow \quad \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = -\int_{\infty}^{1}u^{-\frac{s}{2}+1-2}\psi\left(\frac{1}{u}\right)\,du + \int_{1}^{\infty}x^{\frac{s}{2}-1}\psi(x)\,dx$$

$$\Rightarrow \quad \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \int_{1}^{\infty}u^{-\frac{s}{2}-1}\psi\left(\frac{1}{u}\right)\,du + \int_{1}^{\infty}x^{\frac{s}{2}-1}\psi(x)\,dx$$

$$\Rightarrow \quad \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \int_{1}^{\infty}x^{-\frac{s}{2}-1}\psi\left(\frac{1}{x}\right)\,dx + \int_{1}^{\infty}x^{\frac{s}{2}-1}\psi(x)\,dx$$

y, tenemos que $\psi\left(\frac{1}{x}\right) = \sqrt{x}\;\psi(x) + \frac{\sqrt{x}}{2} - \frac{1}{2}$

$$\Rightarrow \quad \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \int_{1}^{\infty}x^{-\frac{s}{2}-1}\left[\sqrt{x}\;\psi(x) + \frac{\sqrt{x}}{2} - \frac{1}{2}\right]dx +$$

$$+ \int_{1}^{\infty}x^{\frac{s}{2}-1}\;\psi(x)\,dx\;,$$

$$\Rightarrow \quad \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \int_{1}^{\infty}\left(x^{-\frac{s}{2}-1}x^{1/2}\;\psi(x) + \frac{x^{-\frac{s}{2}-1}x^{1/2}}{2} - \frac{x^{-\frac{s}{2}-1}}{2}\right)dx +$$

$$+ \int_{1}^{\infty}x^{\frac{s}{2}-1}\;\psi(x)\,dx$$

$$\Rightarrow \quad \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \int_{1}^{\infty}x^{-\frac{s}{2}-\frac{1}{2}}\;\psi(x)\,dx + \int_{1}^{\infty}\frac{x^{-\frac{s}{2}-\frac{1}{2}}}{2}\,dx - \int_{1}^{\infty}\frac{x^{-\frac{s}{2}-1}}{2}\,dx +$$

$$+ \int_{1}^{\infty}x^{\frac{s}{2}-1}\;\psi(x)\,dx$$

evaluando las integrales, segunda y tercera, tenemos

$$\Rightarrow \quad \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \int_{1}^{\infty}x^{-\frac{s}{2}-\frac{1}{2}}\;\psi(x)\,dx + \frac{1}{s-1} - \frac{1}{s} + \int_{1}^{\infty}x^{\frac{s}{2}-1}\;\psi(x)\,dx$$

$$\Rightarrow \quad \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \frac{1}{s-1} - \frac{1}{s} + \int_{1}^{\infty}x^{-\frac{s}{2}-\frac{1}{2}}\;\psi(x)\,dx + \int_{1}^{\infty}x^{\frac{s}{2}-1}\;\psi(x)\,dx$$

$$\Rightarrow \quad \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \frac{1}{s(s-1)} + \int_{1}^{\infty}\left[x^{-\frac{s}{2}-\frac{1}{2}}\;\psi(x) + x^{\frac{s}{2}-1}\;\psi(x)\right]dx$$

$$\Rightarrow \quad \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \frac{1}{s(s-1)} + \int_{1}^{\infty}\left(x^{-\frac{s}{2}-\frac{1}{2}} + x^{\frac{s}{2}-1}\right)\psi(x)\,dx$$

$$\Rightarrow \quad \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \frac{1}{s(s-1)} + \int_{1}^{\infty}\left(x^{-\frac{s}{2}-\frac{1}{2}} + x^{\frac{s}{2}-1}\right)\left(\frac{\vartheta(x)-1}{2}\right)dx$$

$$\Rightarrow \quad \zeta(s) = \frac{\pi^{\frac{s}{2}}}{\Gamma\left(\frac{s}{2}\right)}\left[\frac{1}{s(s-1)} + \int_{1}^{\infty}\left(x^{-\frac{s}{2}-\frac{1}{2}} + x^{\frac{s}{2}-1}\right)\left(\frac{\vartheta(x)-1}{2}\right)dx\right]\;.$$

Debido al decaimiento exponencial de $\vartheta(x)$, la integral impropia enterior converge para cada $s \in \mathbb{C}$ y por lo tanto define una función entera en $\mathbb{C}$. Por lo tanto, la expresión anterior nos da la continuación analítica de $\zeta(s)$ a todo el plano complejo, a excepción de $s = 1$.

Teorema 2.15.5. La función

$$\zeta(s) = \frac{\pi^{\frac{s}{2}}}{\Gamma\left(\frac{s}{2}\right)} \left[\frac{1}{s(s-1)} + \int_1^\infty \left(x^{-\frac{s}{2}-\frac{1}{2}} + x^{\frac{s}{2}-1} \right) \left(\frac{\vartheta(x)-1}{2} \right) dx \right] ,$$

es meromorfa con un polo simple en $s = 1$ con residuo 1.

Demostración:
Tanto el principio de continuación analítica así como el principio de identidad nos garantizan la validez de esta afirmación. Dado que la expresión anterior amplía el dominio de nuestra $\zeta(s)$ original, de manera única.
Ahora para encontrar el polo simple y el residuo, tenemos que

$$\lim_{s\to 1} \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) s(s-1) \cdot \zeta(s) = 1 + s(s-1) \int_1^\infty \left(x^{-\frac{s}{2}-\frac{1}{2}} + x^{\frac{s}{2}-1} \right) \left(\frac{\vartheta(x)-1}{2} \right) dx$$

$$\Rightarrow \quad \lim_{s\to 1} \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) s(s-1) \cdot \zeta(s) = 1 \ .$$

Así, finalmente encontramos que $\zeta(s)$ tiene un polo simple en $s = 1$, con residuo $\mathrm{Res}(\zeta, s) = \mathrm{Res}_\zeta(s) = 1$.

Ahora hemos logrado nuestro objetivo de continuar la serie de Dirichlet ($\zeta(s) := \sum_{n=1}^\infty \frac{1}{n^s}$) con la que comenzamos, hasta $\zeta(s)$, una función meromorfa en $\mathbb{C}$. Ahora podemos considerar todos los números complejos en nuestra búsqueda de los ceros de $\zeta(s)$. Estamos interesados en estos ceros porque codifican información sobre los números primos.
Sin embargo, no todos los ceros de $\zeta(s)$ nos interesan. Sorprendentemente, podemos encontrar, con relativa facilidad, un número infinito de ceros, todos fuera de la región $0 \leq \mathrm{Re}(s) \leq 1$. Nos referimos a estos ceros como los ceros triviales de $\zeta(s)$ y los excluimos de el enunciado de la hipótesis de Riemann.

Antes de discutir los ceros de $\zeta(s)$, desarrollemos una ecuación funcional para ello. Recordemos que la siguiente expresión no solo da la continuación analítica de $\zeta(s)$, sino que también se puede usar para derivar una ecuación funcional para $\zeta(s)$.

$$\pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s) = \frac{1}{s(s-1)} + \int_1^\infty \left(x^{-\frac{s}{2}-\frac{1}{2}} + x^{\frac{s}{2}-1} \right) \left(\frac{\vartheta(x)-1}{2} \right) dx \ ,$$

Riemann observó que el término $\frac{1}{s(s-1)}$ y la integral impropia anterior son invariantes bajo la sustitución de s por $1-s$. Así, tenemos

$$\zeta(1-s) = \frac{\pi^{\frac{1-s}{2}}}{\Gamma\left(\frac{1-s}{2}\right)} \left[\frac{1}{s(s-1)} + \int_1^\infty \left(x^{-\frac{1-s}{2}-\frac{1}{2}} + x^{\frac{1-s}{2}-1} \right) \left(\frac{\vartheta(x)-1}{2} \right) dx \right]$$

$$\Rightarrow \ \zeta(1-s) = \frac{\pi^{\frac{1-s}{2}}}{\Gamma\left(\frac{1-s}{2}\right)} \left[\frac{1}{s(s-1)} + \int_1^\infty \left(x^{\frac{s}{2}-1} + x^{-\frac{s}{2}-\frac{1}{2}} \right) \left(\frac{\vartheta(x)-1}{2} \right) dx \right]$$

así, tenemos que

$$\pi^{-\frac{1-s}{2}} \Gamma\left(\frac{1-s}{2}\right) \zeta(1-s) = \frac{1}{s(s-1)} + \int_1^\infty \left(x^{\frac{s}{2}-1} + x^{-\frac{s}{2}-\frac{1}{2}} \right) \left(\frac{\vartheta(x)-1}{2} \right) dx$$

luego, notamos que la expresión entre corchetes del Teorema 2.15.5., coincide con la del lado derecho del resultado anterior, igualando, obtenemos

$$\pi^{-\frac{s}{2}}\ \Gamma\left(\frac{s}{2}\right)\zeta(s)=\pi^{-\frac{1-s}{2}}\ \Gamma\left(\frac{1-s}{2}\right)\zeta(1-s)\ .$$

Teorema 2.15.6. (La ecuación funcional) Para todo $s\in\mathbb{C}$

$$\pi^{-\frac{s}{2}}\ \Gamma\left(\frac{s}{2}\right)\zeta(s)=\pi^{-\frac{1-s}{2}}\ \Gamma\left(\frac{1-s}{2}\right)\zeta(1-s)\ .$$

Demostración:

$$\pi^{-\frac{s}{2}}\ \Gamma\left(\frac{s}{2}\right)\zeta(s)=\pi^{-\frac{1-s}{2}}\ \Gamma\left(\frac{1-s}{2}\right)\zeta(1-s)$$

$$\Rightarrow\quad \zeta(s)=\frac{\pi^{\frac{s}{2}}}{\Gamma\left(\frac{s}{2}\right)}\left[\frac{1}{s(s-1)}+\int_1^\infty\left(x^{-\frac{s}{2}-\frac{1}{2}}+x^{\frac{s}{2}-1}\right)\left(\frac{\vartheta(x)-1}{2}\right)dx\right]$$

$$\Rightarrow\quad \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)=\frac{1}{s(s-1)}+\int_1^\infty\left[x^{-\frac{s}{2}-\frac{1}{2}}\ \psi(x)+x^{\frac{s}{2}-1}\ \psi(x)\right]dx\ .$$

Ahora, sabemos que para todo $\sigma>0$, tenemos entonces

$$\Gamma\left(\frac{s}{2}\right)=\int_0^\infty e^{-x}x^{\frac{s}{2}-1}dx$$

sea $x=n^2\pi u$, entonces

$$n^{-s}\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)=\int_0^\infty e^{-n^2\pi u}u^{\frac{s}{2}-1}du$$

$$\Rightarrow\quad n^{-s}\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)=\int_0^\infty \psi(u)u^{\frac{s}{2}-1}du$$

usando la ecuación funcional para $\vartheta(u)$

$$\psi\left(\frac{1}{u}\right)=\frac{1}{2}\left(\vartheta\left(\frac{1}{u}\right)-1\right)=\frac{1}{2}(u^{\frac{1}{2}}\ \vartheta(u)-1)=$$

$$=\frac{1}{2}(u^{\frac{1}{2}}(2\psi(u)+1)-1)=-\frac{1}{2}+\frac{u^{\frac{1}{2}}}{2}+u^{\frac{1}{2}}\psi(u)$$

$$\Rightarrow\quad n^{-s}\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)=\int_0^\infty \psi(u)u^{\frac{s}{2}-1}du=\int_0^1 \psi(u)u^{\frac{s}{2}-1}du+\int_1^\infty \psi(u)u^{\frac{s}{2}-1}du\ ,$$

ahora el cambio $u\to 1/u$, tenemos que si $u=1\ \Rightarrow\ 1/u=1$, luego si $u\to\infty\ \Rightarrow\ 1/u=0$, así

$$n^{-s}\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)=\int_1^\infty\left(-\frac{1}{2}+\frac{u^{\frac{1}{2}}}{2}+u^{\frac{1}{2}}\ \psi(u)\right)u^{-\frac{s}{2}+1}\ \frac{du}{u^2}+\int_1^\infty \psi(u)u^{\frac{s}{2}-1}du$$

$$=\int_1^\infty -\frac{u^{-\frac{s}{2}+1}}{2u^2}du+\int_1^\infty \frac{u^{-\frac{s}{2}+\frac{3}{2}}}{2u^2}du+\int_1^\infty \frac{u^{-\frac{s}{2}+\frac{3}{2}}}{u^2}\psi(u)\ du+\int_1^\infty \psi(u)u^{\frac{s}{2}-1}du$$

evaluando la primera y segunda integrales, tenemos

$$\Rightarrow\quad n^{-s}\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)=-\frac{1}{s}+\frac{1}{s-1}+\int_1^\infty u^{-\frac{s}{2}+\frac{3}{2}-2}\ \psi(u)\ du+\int_1^\infty u^{\frac{s}{2}-1}\ \psi(u)\ du$$

$$\Rightarrow\quad n^{-s}\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)=\frac{1}{s(s-1)}+\int_1^\infty\left(u^{-\frac{s}{2}-\frac{1}{2}}\ \psi(u)+u^{\frac{s}{2}-1}\ \psi(u)\right)du$$

$$\Rightarrow \quad n^{-s}\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right) = \frac{1}{s(s-1)} + \int_1^\infty \left(u^{-\frac{s}{2}-\frac{1}{2}} + u^{\frac{s}{2}-1}\right)\psi(u)\, du$$

$$\Rightarrow \quad n^{-s}\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right) = \frac{1}{s(s-1)} + \int_1^\infty \left(u^{\frac{1-s}{2}} + u^{\frac{s}{2}}\right)\psi(u)\, du\ ,$$

notamos que la última integral converge para todo s.

De la ecuación funcional

$$\pi^{-\frac{s}{2}}\ \Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-\frac{1-s}{2}}\ \Gamma\left(\frac{1-s}{2}\right)\zeta(1-s)\ .$$

Ahora, definimos la función

$$\xi(s) := \frac{s}{2}(s-1)\pi^{-\frac{s}{2}}\ \Gamma\left(\frac{s}{2}\right)\zeta(s)\ ,$$

En vista de la expresión de la continuación analítica, $\xi(s)$ es una función entera y satisface la ecuación funcional simple

$$\xi(s) = \xi(1-s)\ .$$

Esto muestra que $\xi(s)$ es simétrica alrededor de la línea vertical $\mathrm{Re}(s) = \dfrac{1}{2}$.

Ahora hemos desarrollado la función zeta lo suficiente como para comenzar a considerar sus diversas propiedades; en particular, la ubicación de sus ceros. Hay algunas afirmaciones que podemos hacer basadas en la teoría elemental que ya hemos presentado.

Comencemos nuestra discusión aislando los ceros triviales de $\zeta(s)$. Ahora, recordemos que los únicos polos de $\Gamma(s)$ son simples y están situados en $s = 0, -1, -2, -3, \ldots$. De la expresión de la continuación analítica se sigue que $\zeta(s)$ tiene ceros simples en $s = -2, -4, -6, \ldots$, (el polo $s = 0$ de $\Gamma(\frac{s}{2})$ se cancela por el término $\frac{1}{s(s-1)}$) Estos ceros, que surgen de los polos de la función gamma, se denominan ceros triviales. De la ecuación funcional y el (**Teorema**: para todo $s \in \mathbb{C}$ con $\mathrm{Re}(s) > 1$, tenemos $\zeta(s) \neq 0$.), todos los demás ceros, los ceros no triviales, se encuentran en la franja vertical $0 \leq \mathrm{Re}(s) \leq 1$. En vista de la ecuación (definición de la función $\xi(s)$), los ceros no triviales de $\zeta(s)$ son precisamente los ceros de $\xi(s)$, y por lo tanto son simétricos con respecto a la línea vertical $\mathrm{Re}(s) = \frac{1}{2}$. Además, de la expresión de la continuación analítica, son simétricos con respecto al eje real, $t = 0$. Resumimos estos resultados en el siguiente teorema.

Teorema 2.15.7. La función $\zeta(s)$ satisface lo siguiente

1. $\zeta(s)$ no tiene ceros para $\mathrm{Re}(s) > 1$.
2. El único polo de $\zeta(s)$ está en $s = 1$, tiene residuo 1 y es simple.
3. $\zeta(s)$ tiene ceros triviales en $s = -2, -4, -6, \ldots, -2n$.
4. Los ceros no triviales se encuentran dentro de la región $0 \leq \mathrm{Re}(s) \leq 1$ y son simétricos con respecto a la línea vertical $\mathrm{Re}(s) = \frac{1}{2}$ y al eje real $\mathrm{Im}(s) = 0$.
5. Los ceros de $\xi(s)$ son precisamente los ceros no triviales de $\zeta(s)$.

Demostración:
1) La función $\zeta(s)$ de Riemann no tiene ceros en la recta vertical $\sigma = 1$. La prueba se basa en la siguiente desigualdad $3 + 4\cos\theta + \cos 2\theta \geq 0$, la cual se cumple para toda θ real, pues el lado izquierdo es $2(1 + \cos\theta)^2$.

Necesitamos un resultado muy importante conocido como **La fórmula del producto de Euler** es también llamada **La forma analítica del teorema fundamental de la aritmética**. Dado $s = \sigma + it$ con $\sigma > 1$, tenemos

$$\zeta(s) \;=\; \sum_{n=1}^{\infty} \frac{1}{n^s} \;=\; \prod_{p\in\mathbb{P}} \frac{1}{1-\frac{1}{p^s}} \cdot$$

Donde la productoria se extiende a los números primos y la sumatoria a los números naturales. De esta forma

$$\zeta(s) \;=\; 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \frac{1}{6^s} + \frac{1}{7^s} + \;\cdots\;,$$

multiplicamos ambos miembros de la igualdad por un factor de $\frac{1}{2^s}$

$$\frac{1}{2^s}\zeta(s) \;=\; \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \frac{1}{10^s} + \frac{1}{12^s} + \frac{1}{14^s} + \;\cdots\;,$$

efectuamos de diferencia entre $\zeta(s)$ y $\frac{1}{2^s}\zeta(s)$

$$\begin{aligned}
\zeta(s) - \frac{1}{2^s}\zeta(s) \;&=\; 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \frac{1}{6^s} + \frac{1}{7^s} + \;\cdots \\
&\quad \cdots - \;\frac{1}{2^s} - \frac{1}{4^s} - \frac{1}{6^s} - \frac{1}{8^s} - \frac{1}{10^s} - \frac{1}{12^s} - \frac{1}{14^s} - \;\cdots\;, \\
\left(1-\frac{1}{2^s}\right)\zeta(s) \;&=\; 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \frac{1}{11^s} + \frac{1}{13^s} + \;\cdots\;,
\end{aligned}$$

multiplicamos ambos miembros de la igualdad por un factor de $\frac{1}{3s}$

$$\frac{1}{3^s}\left(1-\frac{1}{2^s}\right)\zeta(s) \;=\; \frac{1}{3^s} + \frac{1}{9^s} + \frac{1}{15^s} + \frac{1}{21^s} + \frac{1}{27^s} + \frac{1}{33^s} + \frac{1}{39^s} + \;\cdots\;,$$

efectuamos de diferencia entre $\left(1-\frac{1}{2^s}\right)\zeta(s)$ y $\frac{1}{3^s}\left(1-\frac{1}{2^s}\right)\zeta(s)$

$$\begin{aligned}
\left(1-\frac{1}{2^s}\right)\zeta(s) - \frac{1}{3^s}\left(1-\frac{1}{2^s}\right)\zeta(s) \;&=\; 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \frac{1}{11^s} + \frac{1}{13^s} + \;\cdots \\
&\quad \cdots - \frac{1}{3^s} - \frac{1}{9^s} - \frac{1}{15^s} - \frac{1}{21^s} - \frac{1}{27^s} - \frac{1}{33^s} - \frac{1}{39^s} - \;\cdots\;, \\
\left(1-\frac{1}{2^s}\right)\left(\zeta(s) - \frac{1}{3^s}\;\zeta(s)\right) \;&=\; 1 + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{11^s} + \frac{1}{13^s} + \frac{1}{17^s} + \frac{1}{19^s} + \;\cdots\;, \\
\left(1-\frac{1}{2^s}\right)\left(1-\frac{1}{3^s}\right)\zeta(s) \;&=\; 1 + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{11^s} + \frac{1}{13^s} + \frac{1}{17^s} + \frac{1}{19^s} + \;\cdots\;,
\end{aligned}$$

de igual manera para los factores de $5, 7, 11, 13, 17, 19, \ldots$ (números primos), entonces

$$\cdots \left(1-\frac{1}{13^s}\right)\left(1-\frac{1}{11^s}\right)\left(1-\frac{1}{7^s}\right)\left(1-\frac{1}{5^s}\right)\left(1-\frac{1}{3^s}\right)\left(1-\frac{1}{2^s}\right)\zeta(s) \;=\; 1\;,$$

despejamos

$$\zeta(s) \;=\; \frac{1}{\left(1-\frac{1}{2^s}\right)\left(1-\frac{1}{3^s}\right)\left(1-\frac{1}{5^s}\right)\left(1-\frac{1}{7^s}\right)\left(1-\frac{1}{11^s}\right)\left(1-\frac{1}{13^s}\right)\left(1-\frac{1}{17^s}\right)\;\cdots}\;,$$

de esta manera

$$\zeta(s) \;=\; \prod_{p\in\mathbb{P}} \frac{1}{1-\frac{1}{p^s}} \cdot$$

Ahora, con el resultado de la fórmula del producto de Euler tenemos que, para $\sigma > 1$

$$\log|\zeta(\sigma+it)| = \operatorname{Re}\log\zeta(\sigma+it) = \operatorname{Re}\log\prod_p \frac{1}{1-p^{-s}}$$

$$= -\operatorname{Re}\sum_p \log\left(1-p^{-s}\right) = \operatorname{Re}\sum_p\sum_{m=1}^{\infty}\frac{1}{mp^{ms}}$$

$$= \operatorname{Re}\sum_{n=2}^{\infty}\frac{c(n)}{n^{\sigma+it}} = \sum_{n=2}^{\infty}\frac{c(n)}{n^{\sigma}}\cos(t\log n)\ ,$$

en donde $c(n)$ es $\frac{1}{m}$ si n es una $m-$potencia de un primo, y 0 en otro caso. Por lo tanto

$$\log|\zeta^3(\sigma)\zeta^4(\sigma+it)\zeta(\sigma+2it)| = \sum_{n=2}^{\infty}\frac{c(n)}{n^{\sigma}}(3+4\cos(t\log n)+\cos(2t\log n)) \geq 0\ ,$$

pues $c(n) \geq 0$. Por lo tanto

$$\{(\sigma-1)\zeta(\sigma)\}^3\left|\frac{\zeta(\sigma+it)}{\sigma-1}\right|^4|\zeta(\sigma+2it)| \geq \frac{1}{\sigma-1}\ .$$

Supongamos ahora que $1+it$ es un cero de $\zeta(s)$. Entonces dada la siguiente. **Proposición**: Para la función Zeta de Riemann $\zeta(s)$ existe una función $h(s)$ analítica en $\sigma > 0$ tal que $\zeta(s) = \frac{1}{s-1} + h(s)$. Demostración: Para $\sigma > 1$ tenemos que

$$\zeta(s) = \int_{1^-}^{\infty} t^{-s}d[t] = \frac{1}{s-1} - \int_{1^-}^{\infty} t^{-s}d(t-[t])$$

$$= \frac{1}{s-1} + 1 - s\int_1^{\infty}\frac{t-[t]}{t^{s+1}}dt\ ,$$

puesto que la última integral converge absolutamente para $\sigma > 0$, la proposición se sigue del **Teorema** de Weierstrass. Sea $\{g_n(s)\}$ una sucesión de funciones analíticas definidas en un conjunto abierto S del plano complejo. Suponga que $\{g_n(s)\}$ converge uniformemente en todo subconjunto compacto de S hacia la función $g(s)$. Entonces $g(s)$ es analítica en S y la sucesión de derivadas $\{g_n'(s)\}$ converge uniformemente en cada subconjunto compacto de S hacia $g'(s)$. Así, la proposición anterior implica que

$$\{(\sigma-1)\zeta(\sigma)\}^3\left|\frac{\zeta(\sigma+it)}{\sigma-1}\right|^4|\zeta(\sigma+2it)|\ ,$$

tiende al límite finito

$$|\zeta'(1+it)|^4|\zeta(1+2it)|\ ,$$

cuando $\sigma \to 1^+$. Puesto que $\{(\sigma-1)\zeta(\sigma)\}^3\left|\frac{\zeta(\sigma+it)}{\sigma-1}\right|^4|\zeta(\sigma+2it)|$ tiende a $+\infty$, obtenemos una contradicción.

Ahora, la función $\zeta(s)$ de Riemann no tiene ceros en el semiplano $\sigma \geq 1$. Solo resta probar la proposición cuando $\sigma > 1$. Pero en este caso

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty}\frac{\mu(n)}{n^s} \ll \sum_{n=1}^{\infty}\frac{1}{n^{\sigma}} < \infty\ .$$

La franja $0 \leq \mathrm{Re}(s) \leq 1$ se denomina franja crítica y la línea vertical $\mathrm{Re}(s) = \frac{1}{2}$ se llama línea crítica.

2) Se probó en el teorema 2.15.5.

3) Dadas las propiedades de la función $\Gamma(s)$ podemos escribir la ecuación funcional en varias formas equivalentes.

$$\pi^{-\frac{s}{2}}\ \Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-\frac{1-s}{2}}\ \Gamma\left(\frac{1-s}{2}\right)\zeta(1-s)\ .$$

Por ejemplo:

$$\zeta(s) = \chi(s)\zeta(1-s)\ , \qquad \chi(s) = \frac{(2s)^2}{2\Gamma(s)\cos\left(\frac{\pi s}{2}\right)}\ .$$

$$\zeta(s) = 2^s\pi^{s-1}\ \mathrm{sen}\left(\frac{\pi s}{2}\right)\Gamma(-s)\zeta(1-s).$$

Con referencia a la última expresión demostraremos el siguiente corolario.

Corolario 2.15.8. (Ceros triviales)
Si $\sigma < 0$, entonces $\zeta(s) = 0$ si y solo si $s = -2n,\ n \in \mathbb{N}$.
Demostración:
La función $\Gamma(-s)$ no se anula en todo el plano complejo y $\zeta(1-s)$ tampoco lo hace para $\sigma < 0$. Puesto que el producto de Euler converge a un valor no nulo en $\Omega_a := \{s = \sigma + it :\ \sigma > 1\}$ y de la igualdad $\zeta(s) = \prod_p \frac{1}{1-1/p^s}$, se deduce que ζ no posee ceros en el semiplano $\sigma > 1$. Además, $\mathrm{sen}\left(\frac{\pi s}{2}\right) = 0$ si y solo si $s = 2n,\ n \in \mathbb{Z}$.

Estos valores pares negativos en donde la función se anula "trivialmente" son conocidos como ceros triviales de la función zeta.

Riemann comentó sobre los ceros de $\mathrm{Re}(s)$ en sus memorias (lo veremos en el siguiente capítulo). A partir de sus declaraciones se formuló su hipótesis.

Capítulo 3

La hipótesis de Riemann

Uno de los mayores desafíos de las matemáticas es sin duda la hipótesis de Riemann. El "santo grial" de las matemáticas, que, de manera más realista, se considera el problema abierto más importante de las matemáticas, ha atraído a estudiosos de todo el mundo durante 150 años, es decir, desde que Bernhard Riemann formuló la primera versión en 1859. Forma parte de los veintitrés famosos problemas de Hilbert y de los siete problemas del milenio por los que el Clay Mathematical Institute ha ofrecido un millón de dólares. Pero, sobre todo, forma parte de los sueños de los matemáticos -y no matemáticos- que, si demostraran la validez de la conjetura del gran matemático y físico alemán, verían su nombre consignado a la historia.

Recuerdemos que en el Teorema del número primo (Teorema 1.7.25.) se dijo que una estimación aproximada para una la función $\pi(x)$, el número de primos $\leq x$, viene dado por la función $x/\log(x)$. Recordemos, también, que un refinamiento de esa suposición, ofrecido por Gauss, surge de este curioso pensamiento: la "probabilidad" de que un número n sea primo es proporcional al recíproco de su número de dígitos; más precisamente, la probabilidad es $1/\log(n)$. Esto es, suponer que el valor aproximado de $\pi(x)$ sería el área de la región de 2 a x bajo la gráfica de $1/\log(x)$, una cantidad a veces referida como $\mathrm{li}(x)$, $\mathrm{Li}(x)$, "li", "Li" es la abreviatura de Integral logarítmica, porque el área de la región de 2 a x es $1/\log(x)$, recordando (la definición) $\int_2^x \frac{dt}{\log(t)}$.

La figura 3.1 muestra la gráfica de las tres funciones $\mathrm{Li}(x)$, $\pi(x)$ y $x/\log x$, para $x \leq 200$. Pero los datos, por impresionantes que sean, pueden ser engañosos. Parece que las tres gráficas nunca se cruzan para grandes valores de x, y tenemos la relación simple $x/\log(x) < \pi(X) < \mathrm{Li}(x)$ para x grande.

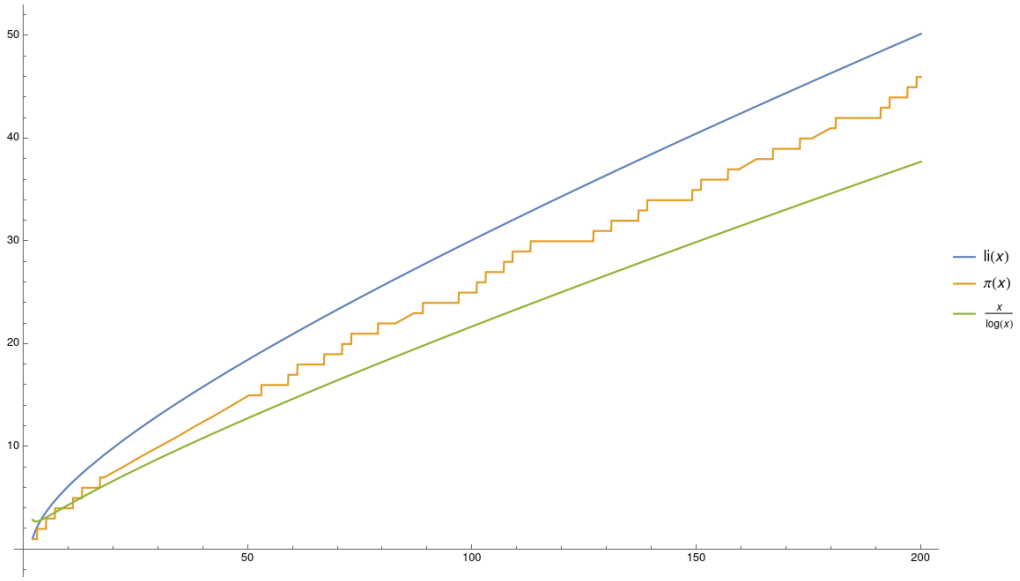


Figura 3.1: $\mathrm{Li}(x)$ (arriba), $\pi(x)$ (en medio), $x/\log(x)$ (abajo).

Es un gran desafío evaluar $\pi(x)$ para valores grandes de x. Por ejemplo, supongamos que $x = 1024$. Entonces tenemos:

$$\begin{aligned}
\pi(x) &= 18,435,599,767,349,200,867,866 \\
\mathrm{Li}(x) &= 18,435,599,767,366,347,775,143\ .\ 10580\ldots \\
x/(\log(x)-1) &= 18,429,088,896,563,917,716,962\ .\ 93869\ldots \\
\mathrm{Li}(x)-\pi(x) &= 17,146,907,277\ .\ 105803\ldots \\
\sqrt{x}\cdot\log(x) &= 55,262,042,231,857\ .\ 096416\ldots
\end{aligned}$$

De manera más imaginativa, podemos pensar en el error en esta aproximación a $\pi(x)$, i.e., $|\mathrm{Li}(x)-\pi(x)|$, (el valor absoluto) de la diferencia entre $\mathrm{Li}(x)$ y $\pi(x)$, como (aproximadamente) el resultado de una caminata que tiene aproximadamente x pasos donde te mueves bajo la siguiente regla: diríjase hacia el este una distancia[25] de $1/\log n$ pies si n no es primo y al oeste por una distancia de $1-(1/\log n)$ pies si n es primo. Tu distancia, entonces, desde el origen después de x pasos es aproximadamente $|\mathrm{Li}(x)-\pi(x)|$ pies.

No tenemos idea si esta imagen de las cosas se parece a un paseo verdaderamente aleatorio, pero al menos es razonable plantear la pregunta: ¿$\mathrm{Li}(X)$ es esencialmente una raíz cuadrada aproximada de $\pi(x)$? Podríamos decir que si. Para cualquier número real x, el número de números primos menores que x es aproximadamente $\mathrm{Li}(x)$ y esta aproximación es esencialmente la raíz cuadrada.

La hipótesis de Riemann está relacionada "genéticamente" con los números primos, que son los "átomos" de las matemáticas. Su demostración podría cambiar la forma de hacer negocios hoy en día, pues los números primos son el eje central de la seguridad en la banca y el comercio electrónico. Supondría también que habría una profundo impacto en la vanguardia de la ciencia, que afectaría a la mecánica cuántica, la teoría del caos, y el futuro de la computación. Por ello, el mismo instituto de matemáticas Clay de la Universidad de Cambridge en Massachussets, anunció durante el congreso internacional de París el 24 de mayo de 2000, en conmemoración del centenario de la conferencia

[25] En esta sección nos referiremos a la distancia euclídea, como la distancia "ordinaria" entre dos puntos de un espacio euclídeo, la cual se deduce a partir del teorema de Pitágoras. $d_E = \sqrt{(x_2-x_1)^2+(y_2-y_1)^2}$.

de David Hilbert, que premiaría con un millón de dólares a quien lograra demostrar cualquiera de los 7 problemas matemáticos abiertos del momento, denominados comúnmente del milenio, del que la hipótesis de Riemann formaba parte. Como anécdota para resaltar la importancia de la hipótesis de Riemann, cabe comentar que en una ocasión en 1943, poco antes de morir, un periodista le preguntó a David Hilbert cuál sería su primera pregunta si pudieran resucitarle 500 años después de su muerte, a lo que éste respondió sin titubeos: "¿Ha demostrado alguien la Hipótesis de Riemann?".

En el año 1900, el alemán David Hilbert pronunció una conferencia durante la celebración del congreso internacional de matemáticas en París. Esta intervención guiaría en cierto modo el devenir futuro de las matemáticas. En ella Hilbert enunció, lo que desde su punto de vista debían ser considerados los 23 problemas matemáticos aún no resueltos más importantes del momento, y en los que la comunidad matemática debería volcar todos sus esfuerzos, de ahí su famosa frase "Debemos saber, y sabremos". El problema número 8 trataba precisamente la hipótesis de Riemann, enunciada de tres modos diferentes:

- **HR.1:**

  La función $\mathrm{Li}(x)$ de Gauss está a distancia raíz cuadrada de $\pi(x)$.

- **HR.2:**

  Las funciones $\mathrm{Li}(x)$ de Gauss y $R(x)$ de Riemann están a una distancia de orden raíz cuadrada de $\pi(x)$.

- **HR.3:**

  Todos los ceros no triviales de la función zeta de Riemann, definida como continuación analítica de la forma

  $$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \ , \quad \mathrm{Re}(s) > 1 \ ,$$

  están en la franja crítica vertical, formada por los números complejos s tales que $\mathrm{Re}(s) = \frac{1}{2}$, i.e., en mitad de la franja crítica.

Conjetura 3.0.1. (La hipótesis de Riemann)
Todos los ceros no triviales de la función $\zeta(s)$ de Riemann se encuentran en la línea crítica $\mathrm{Re}(s) = \frac{1}{2}$.

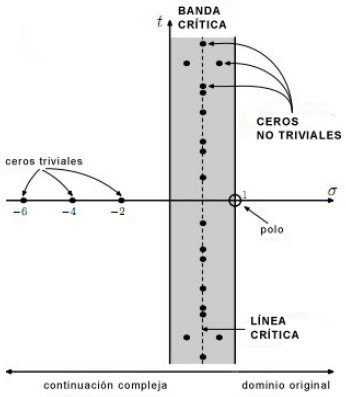
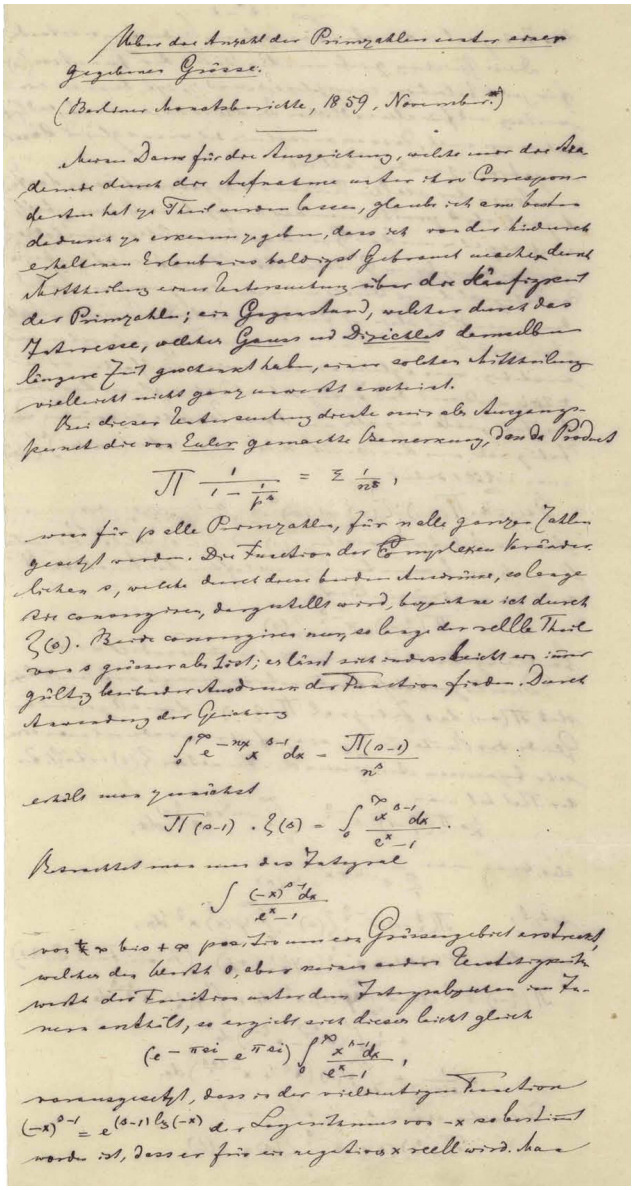


Figura 3.2: Ceros de la función zeta de Riemann.



Über die Anzahl der Primzahlen unter einer gegebenen Grösse.

(Berliner Monatsberichte, 1859, November.)

Wenn Dank für die Auszeichnung, welche mir durch die Aufnahme unter die Correspondenten hat zu Theil werden lassen, glaube ich am besten dadurch zu erweisen zu geben, dass ich von der bisher erhaltenen Erlaubniss bald zu Gebrauch machen durch Mittheilung einer Untersuchung über die Häufigkeit der Primzahlen; ein Gegenstand, welchen durch das Interesse, welches Gauss und Dirichlet demselben längere Zeit geschenkt haben, einer solchen Mittheilung vielleicht nicht ganz unwerth erscheint.

Bei dieser Untersuchung diente mir als Ausgangspunkt die von Euler gemachte Bemerkung, dass das Product

$$\prod \frac{1}{1-\frac{1}{p^s}} = \sum \frac{1}{n^s},$$

wenn für alle Primzahlen, für n alle ganzen Zahlen gesetzt werden. Die Function der complexen Veränderlichen s, welche durch diese beiden Ausdrücke, so lange sie convergiren, dargestellt wird, bezeichne ich durch $\zeta(s)$. Beide convergiren nun, so lange der reelle Theil von s grösser als 1 ist; es lässt sich jedoch leicht ein immer gültig bleibender Ausdruck der Function finden. Durch Anwendung der Gleichung

$$\int_0^\infty e^{-nx} x^{s-1} dx = \frac{\Pi(s-1)}{n^s}$$

erhält man zunächst

$$\Pi(s-1) \cdot \zeta(s) = \int_0^\infty \frac{x^{s-1} dx}{e^x - 1}.$$

Bezeichnet nun $\int \frac{(-x)^{s-1} dx}{e^x - 1}$

von $x = \infty$ bis $+\infty$ positiv um ein Grössengebiet erstreckt, welches den Werth 0, aber keinen andern Verzweigungspunkt der Function unter den Integralzeichen in sich enthält, so ergibt sich dieses Integral gleich

$$(e^{-\pi i} - e^{\pi i}) \int_0^\infty \frac{x^{s-1} dx}{e^x - 1},$$

vorausgesetzt, dass $(-x)^{s-1}$ die vieldeutige Function $e^{(s-1)\log(-x)}$ [illegible] Logarithmus von $-x$ so bestimmt worden ist, dass er für negative x reell wird. Das

3.1. Ceros triviales

La siguiente expresión nos brinda la continuación analítica de la función $\zeta(s)$ de Riemann a todo el plano complejo, a excepción de $s = 1$.

$$\zeta(s) = \frac{\pi^{\frac{s}{2}}}{\Gamma\left(\frac{s}{2}\right)} \left[\frac{1}{s(s-1)} + \int_1^{\infty} \left(x^{-\frac{s}{2}-\frac{1}{2}} + x^{\frac{s}{2}-1} \right) \left(\frac{\vartheta(x)-1}{2} \right) dx \right] ,$$

es meromorfa con un polo simple en $s = 1$ con residuo 1. Como ya se demostró en el capítulo anterior (Teorema 2.15.5.).
Recordemos que los únicos polos de $\Gamma(s)$ son simples y están situados en $s = 0, -1, -2, -3, \ldots, -n$.

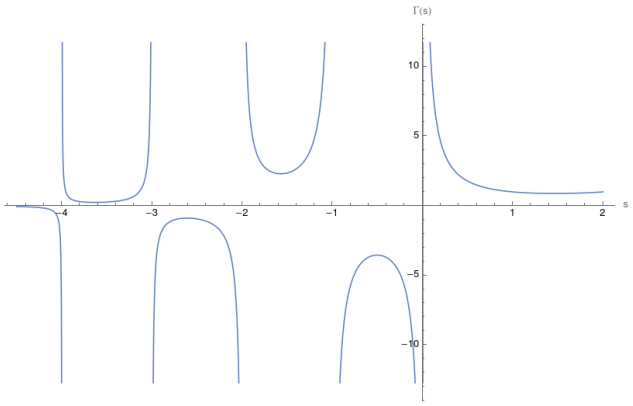


Figura 3.4: Gráfica de la función Gamma $\Gamma(s)$, donde se aprecian sus polos simples ubicados en $s = 0, -1, -2, -3, \ldots, -n$.

De la expresión de la continuación analítica se sigue que $\zeta(s)$ tiene ceros triviales en $s = -2, -4, -6, \ldots, -2n$, $n \in \mathbb{N}$, (el polo $s = 0$ de $\Gamma(\frac{s}{2})$ se cancela por el término $\frac{1}{s(s-1)}$) Estos ceros, que surgen de los polos de la función gamma, se denominan ceros triviales. Se demostro en el corolario 2.15.8.

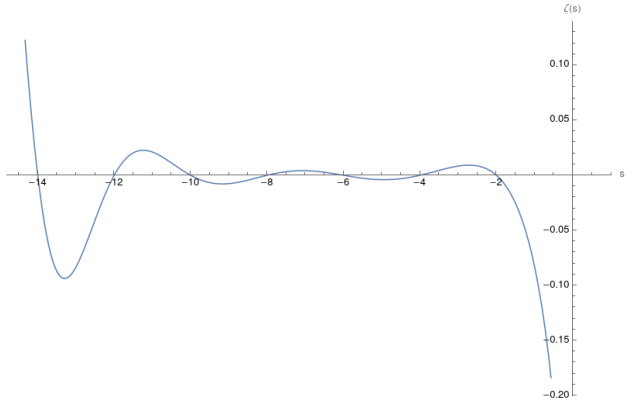


Figura 3.5: Gráfica de la continuación analítica de la función zeta $\zeta(s)$, donde se aprecian sus ceros triviales ubicados en $s = -2, -4, -6, -8, \ldots, -2n$, $n \in \mathbb{N}$.

3.2. Ceros no triviales

Se pueden encontrar por internet varias tablas sobre la ubicación de los primeros ceros no triviales de la función ζ. Desde principios del siglo pasado, donde en que comenzó el conteo metódicamente tales ceros, hasta la fecha se han calculado todos los ceros con valores de parte imaginaria del orden de 10^{13}.

Sin embargo, existen otros casos aislados de cálculo en regiones aún más lejanas al origen, la mayoría de los cuales se deben al trabajo (también teórico) del matemático Odlyzko quien, en colaboración con Schönhage, fue capaz de crear un algoritmo eficiente para calcular los valores zeta. Este mismo algoritmo es la base de los cálculos modernos, los mismos que permitieron llegar a la imagen completa de los ceros (no triviales) de ζ para valores con parte imaginaria de 0 a 10^{13}. (Luego, también de 0 a -10^{13}, pues $\zeta(\bar{s}) = \zeta(s),\ \forall s \in \mathbb{C}$).

Los ceros no triviales de la función ζ son de la forma

$$s \in \mathbb{C}\ , \quad s = \frac{1}{2} + it\ , \quad t \in \mathbb{R}\ ,$$

es decir, todos parecen confirmar la hipótesis de Riemann.

Tabla de verificaciones numéricas de HR

Año	Investigador	Número de ceros
(1859)	Riemann	≥ 3
↓	usando Euler-Maclaurin	
(1903)	Gram	15
(1916)	Backlund	79
(1925)	Hutchinson	138
↓	usando Riemann-Siegel	
(1936)	Titchmarsh y Comrie	1 041
(1953)	Turing	1 104
(1956)	Lehmer	25 000
(1958)	Meller	35 337
(1966)	Lehman	250 000
(1969)	Rosser, Yohe, Schoenfeld	3 502 500
(1979)	Brent	81 000 001
(1982)	Brent, van de Lune, te Riele y Winter	200 000 001
(1983)	van de Lune y te Riele	300 000 001
(1986)	van de Lune, te Riele y Winter	1 500 000 001
(2001)	van de Lune (no publicado)	10 000 000 000
(2003)	Wedeniwski (Zeta-grid)	250 000 000 000
	Con un nuevo método de Odlyzko y Schönhage	
(2004)	Gourdon	10 000 000 000 000

Un proverbio bastante común en matemáticas dice que "N pistas no forman una prueba" (por muy grande que sea N) y se sigue trabajando en este campo, tanto para confirmaciones adicionales o para cualquier negación.

- Si la hipótesis de Riemann es cierta, estos cálculos no son suficientes para probarla: se proporcionan tablas de ceros cada vez más grandes, pero no una demostración.
- Si la hipótesis de Riemann es falsa, suponiendo que cualquiera pueda probarla, es razonable suponer que los cálculos, tarde o temprano, acabarán identificando un cero s (no trivial) de la función ζ tal que $\mathrm{Re}(s) \neq 1/2$.

Veamos, por tanto, la ubicación de los primeros ceros no triviales de la función ζ (por tanto de los primeros ceros de la función ξ). Como ya se mencionó, $\zeta(s) = \zeta(\bar{s})$, por lo tanto, dicha tabla incluye automáticamente los valores de $\bar{s} = 1/2 - it$, partiendo de los valores $s = 1/2 + it$. Hay muchas tablas de los ceros no triviales en internet y, a menudo, en ellas, sólo se indica el valor de la parte imaginaria $t \in \mathbb{R}$ de los ceros, ya que, hasta ahora, todos tienen parte real $1/2$.

Número de cero (en orden de distancia al origen)	Valor de t (truncado a los primeros 10 decimales)
1	14.1347251417
2	21.0220396387
3	25.0108575801
4	30.4248761258
5	32.9350615877
6	37.5861781588
7	40.9187190121
8	43.3270732809
9	48.0051508811
10	49.7738324776

Recordando la función $\xi = \frac{s}{2}(s-1)\pi^{-\frac{s}{2}}\,\Gamma\left(\frac{s}{2}\right)\zeta(s)$, es una variante de la función zeta de Riemann y se define de modo que tenga una ecuación funcional particularmente simple (como se mencionó al final del Teorema 2.15.6.). Asi podemos aproximar la función $\zeta(s)$ de Riemann por medio de la función $\xi(s)$.

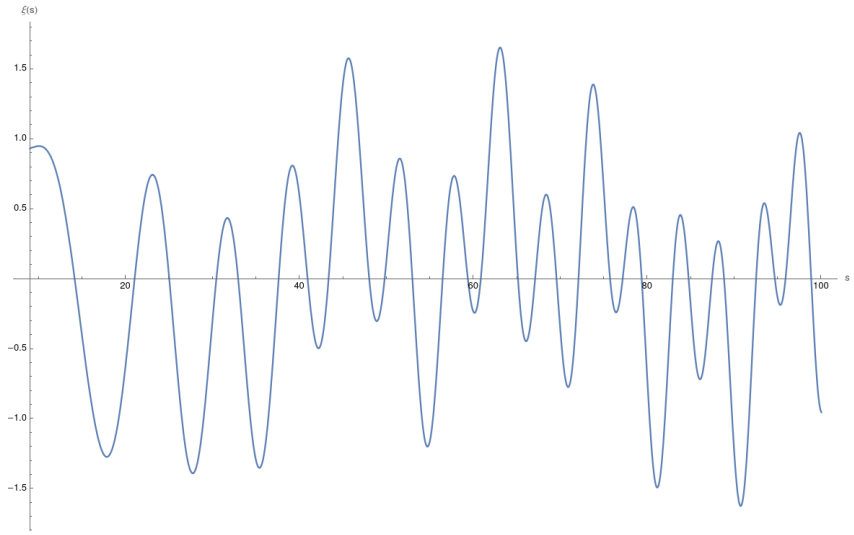


Figura 3.6: Gráfica de la función $\xi(s)$.

Para encontrar los valores de la función $\zeta(s)$ de Riemann emplearemos la Fórmula de Riemann–Siegel que es una fórmula asintótica para el error que se comete en la ecuación funcional aproximada de la función zeta de Riemann. Esta fue encontrada por Siegel (1932) en unos manuscritos no publicados de Bernhard Riemann alrededor del año 1850.

Por medio de la ecuación funcional es posible definir dos funciones reales y continuas $\vartheta(t)$ y $Z(t)$, $t \geq 0$, tales que $\zeta(\frac{1}{2} + it) = Z(t)e^{-i\vartheta(t)}$ y $\vartheta(0) = 0$.

La fórmula de Riemann-Siegel para $t > 0$

$$Z(t) = e^{-i\vartheta(t)}\ \zeta\left(\frac{1}{2} + it\right) = 2\sum_{n=1}^{\lfloor\sqrt{\frac{t}{2\pi}}\rfloor} \frac{\cos(\vartheta(t) - t\ln n)}{\sqrt{n}} + R$$

$$\Rightarrow \quad Z(t) = e^{-i\vartheta(t)} \left(2\sum_{n=1}^{\lfloor\sqrt{\frac{t}{2\pi}}\rfloor} \frac{\cos(\vartheta(t) - t\ln n)}{\sqrt{n}} + R \right) .$$

De la ecuación funcional se sigue que $\vartheta(t)$ depende sólo de la función gamma

$$\vartheta(t) := \operatorname{Im}\ln\Gamma\left(\frac{1}{4} + i\frac{t}{2}\right) - \frac{t}{2}\ln\pi\ .$$

Generalmente $\vartheta(t)$ se calcula por medio del desarrollo asintótico

$$\vartheta(t) = \frac{t}{2}\ln\frac{t}{2\pi} - \frac{t}{2} - \frac{\pi}{8} + \sum_{n=1}^{\infty} \frac{(2^{2n-1}-1)|B_{2n}|}{2^{2n}(2n-1)2n}\ \frac{1}{t^{2n-1}}\ , \quad t \to \infty\ .$$

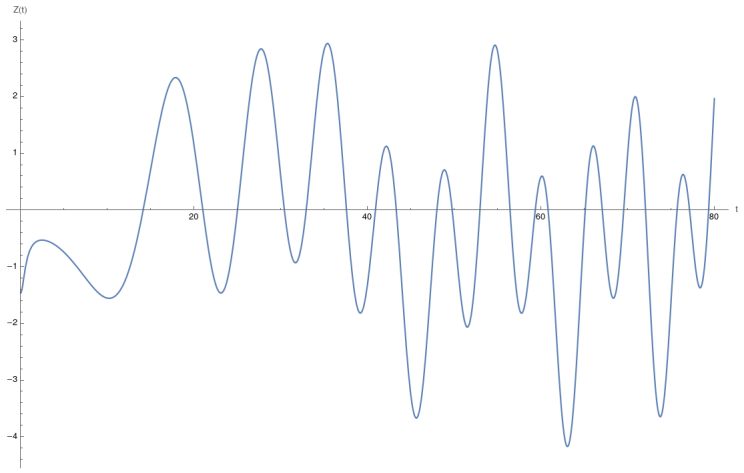


Figura 3.7: Gráfica de la función $Z(s)$.

Graficando la función $\zeta(s)$, de tal manera que sus partes real $\operatorname{Re}(s)$ e imaginaria $\operatorname{Im}(s)$, se muestren en la misma gráfica, podemos observar que cuando los ceros de ambas partes coinciden en los mismos puntos del eje horizontal, i.e., son los ceros no triviales de la función $\zeta(s)$ de Riemann.

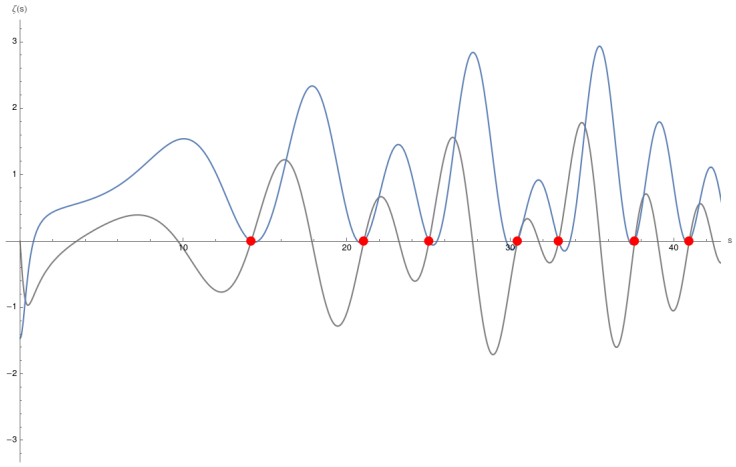


Figura 3.8: Gráfica de las partes $\text{Re}\left[\zeta\left(\frac{1}{2}+it\right)\right]$ (azul), $\text{Im}\left[\zeta\left(\frac{1}{2}+it\right)\right]$ (gris).

Con la fórmula de Riemann-Siegel podemos calcular los valores de la función $\zeta(s)$ por ejemplo para los siguientes valores de t

t	$\zeta(1/2+it)$	$\text{Re}(s)$	$\text{Im}(s)$
14,0	$\zeta(1/2+i14{,}0)$	0,02	0,10
14,2	$\zeta(1/2+i14{,}2)$	−0,01	0,05
14,6	$\zeta(1/2+i14{,}6)$	0,01	0,38

i.e.,

- $\zeta\left(\frac{1}{2}+i14{,}0\right) = (0{,}02+i0{,}10)$,
- $\zeta\left(\frac{1}{2}+i14{,}2\right) = (-0{,}01+i0{,}05)$,
- $\zeta\left(\frac{1}{2}+i14{,}6\right) = (0{,}01+i0{,}38)$.

En particular notemos que

$$\text{Im}\left[\zeta\left(\frac{1}{2}+i14{,}0\right)\right] = -0{,}10 \quad \text{i.e.,} \quad \text{Im}\left[\zeta\left(\frac{1}{2}+i14{,}0\right)\right] < 0\ ,$$

$$\text{Im}\left[\zeta\left(\frac{1}{2}+i14{,}2\right)\right] = 0{,}05 \quad \text{i.e.,} \quad \text{Im}\left[\zeta\left(\frac{1}{2}+i14{,}2\right)\right] > 0\ ,$$

la parte imaginaria de $\zeta\left(\frac{1}{2}+it\right)$ cruza el eje horizontal, i.e., debe existir un cero tal que $t \in (14,\ 14{,}2)$.

Y también notemos que

$$\text{Re}\left[\zeta\left(\frac{1}{2}+i14{,}0\right)\right] = 0{,}02 \quad \text{i.e.,} \quad \text{Re}\left[\zeta\left(\frac{1}{2}+i14{,}0\right)\right] > 0\ ,$$

$$\text{Re}\left[\zeta\left(\frac{1}{2}+i14{,}2\right)\right] = -0{,}01 \quad \text{i.e.,} \quad \text{Re}\left[\zeta\left(\frac{1}{2}+i14{,}2\right)\right] < 0\ ,$$

la parte real de $\zeta\left(\frac{1}{2}+it\right)$ cruza el eje horizontal, i.e., debe existir un cero tal que $t \in (14,\ 14{,}2)$.

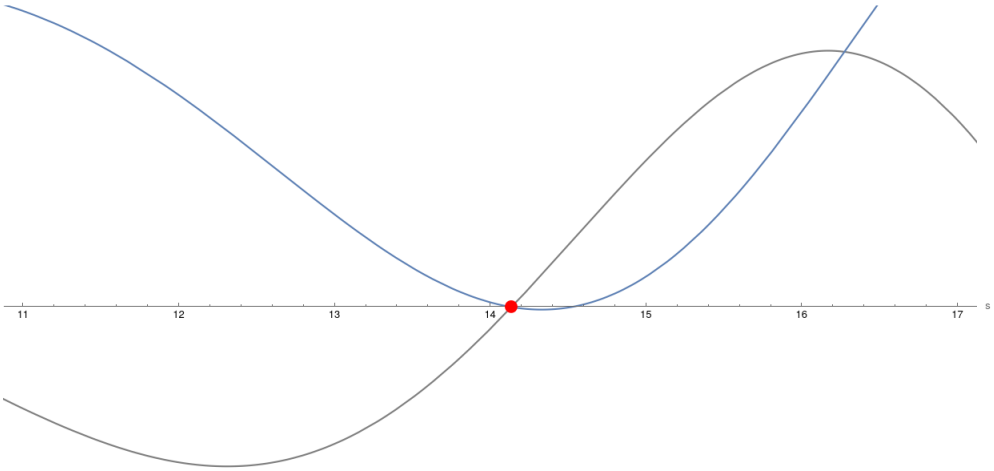


Figura 3.9: Podemos apreciar los cambios en los valores de positivo a negativo de la parte $\mathrm{Re}\left[\zeta\left(1/2+it\right)\right]$ (azul), y de negativo a positivo en la parte imaginaria $\mathrm{Im}\left[\zeta\left(1/2+it\right)\right]$ (gris).

Retomando la función theta de Riemann-Siegel

$$\vartheta(t)=\frac{t}{2}\ln\frac{t}{2\pi}-\frac{t}{2}-\frac{\pi}{8}+\sum_{n=1}^{\infty}\frac{(2^{2n-1}-1)|B_{2n}|}{2^{2n}(2n-1)2n}\ \frac{1}{t^{2n-1}}$$

$$\Rightarrow\quad \vartheta(t)=\frac{t}{2}\ln\frac{t}{2\pi}-\frac{t}{2}-\frac{\pi}{8}+\frac{(2^{2-1}-1)(1/6)}{2^2(2-1)2t^{2-1}}+\sum_{n=2}^{\infty}\frac{(2^{2n-1}-1)|B_{2n}|}{2^{2n}(2n-1)2n}\ \frac{1}{t^{2n-1}}$$

$$\Rightarrow\quad \vartheta(t)=\frac{t}{2}\ln\frac{t}{2\pi}-\frac{t}{2}-\frac{\pi}{8}+\frac{1/6}{8t}+\sum_{n=2}^{\infty}\frac{(2^{2n-1}-1)|B_{2n}|}{2^{2n}(2n-1)2n}\ \frac{1}{t^{2n-1}}$$

$$\Rightarrow\quad \vartheta(t)=\frac{t}{2}\ln\frac{t}{2\pi}-\frac{t}{2}-\frac{\pi}{8}+\frac{1}{48t}+\sum_{n=2}^{\infty}\frac{(2^{2n-1}-1)|B_{2n}|}{2^{2n}(2n-1)2n}\ \frac{1}{t^{2n-1}}$$

$$\Rightarrow\quad \vartheta(t)=\frac{t}{2}\ln\frac{t}{2\pi}-\frac{t}{2}-\frac{\pi}{8}+\frac{1}{48t}+\frac{(2^{4-1})|-1/30|}{2^4(4-1)4t^{4-1}}+\sum_{n=3}^{\infty}\frac{(2^{2n-1}-1)|B_{2n}|}{2^{2n}(2n-1)2n}\ \frac{1}{t^{2n-1}}$$

$$\Rightarrow\quad \vartheta(t)=\frac{t}{2}\ln\frac{t}{2\pi}-\frac{t}{2}-\frac{\pi}{8}+\frac{1}{48t}+\frac{(2^3)(1/30)}{16(3)4t^3}+\sum_{n=3}^{\infty}\frac{(2^{2n-1}-1)|B_{2n}|}{2^{2n}(2n-1)2n}\ \frac{1}{t^{2n-1}}$$

$$\Rightarrow\quad \vartheta(t)=\frac{t}{2}\ln\frac{t}{2\pi}-\frac{t}{2}-\frac{\pi}{8}+\frac{1}{48t}+\frac{7/30}{192t^3}+\sum_{n=3}^{\infty}\frac{(2^{2n-1}-1)|B_{2n}|}{2^{2n}(2n-1)2n}\ \frac{1}{t^{2n-1}}$$

$$\Rightarrow\quad \vartheta(t)=\frac{t}{2}\ln\frac{t}{2\pi}-\frac{t}{2}-\frac{\pi}{8}+\frac{1}{48t}+\frac{7}{5760t^3}+\cdots\ .$$

Ahora, si $t=14{,}134725141734693790457251983562 5,$ y sustituyendo en la expresión anterior

$$\vartheta(t)=\frac{14{,}134\ldots}{2}\ln\frac{14{,}134\ldots}{2\pi}-\frac{14{,}134\ldots}{2}-\frac{\pi}{8}+\frac{1}{48(14{,}134\ldots)}+\frac{7}{5760(14{,}134\ldots)^3}+\cdots$$

evaluando y simplificando, tenemos

$$\vartheta(t) \sim -1{,}728670247359832742372104349590\ .$$

Luego, necesitamos conocer el valor de n en la siguiente expresión

$$\zeta\left(\frac{1}{2}+it\right) = e^{-i\vartheta(t)}\left(2\sum_{n=1}^{\lfloor\sqrt{\frac{t}{2\pi}}\rfloor}\frac{\cos(\vartheta(t)-t\ln n)}{\sqrt{n}}+R\right)\ ,$$

entonces, tomaremos la parte entera inferior de $\lfloor\sqrt{\frac{t}{2\pi}}\rfloor$

$$\begin{aligned} n = \lfloor\sqrt{\frac{t}{2\pi}}\rfloor &= \lfloor\sqrt{\frac{14{,}134725141734693790457251983562 5}{2\pi}}\rfloor = \\ &= \lfloor 1{,}499870452923307448219125950 1034\rfloor \quad \Rightarrow \quad n=1\ , \end{aligned}$$

ahora, $\vartheta(t) \sim -1{,}728670247359832742372104349590$, $n=1$, y sustituimos

$$\begin{aligned} & \zeta\left(\frac{1}{2}+it\right) = e^{-i(-1{,}72\ldots)}\left(2\frac{\cos((-1{,}72\ldots)-t\ln(1))}{\sqrt{1}}+R\right) \\ \Rightarrow \quad & \zeta\left(\frac{1}{2}+it\right) = e^{-i(-1{,}72\ldots)}\left(2\cos((-1{,}72\ldots)-t\ln(1))+R\right) \\ \Rightarrow \quad & \zeta\left(\frac{1}{2}+it\right) = e^{i(1{,}72\ldots)}\left(2\cos((-1{,}72\ldots)-t(0))+R\right) \\ \Rightarrow \quad & \zeta\left(\frac{1}{2}+it\right) = e^{i(1{,}72\ldots)}\left(2\cos(-1{,}72\ldots)+R\right) \\ \Rightarrow \quad & \zeta\left(\frac{1}{2}+it\right) = (\cos(1{,}72\ldots)+i\ \text{sen}\ (1{,}72\ldots))\left(2\cos(-1{,}72\ldots)+R\right) \end{aligned}$$

evaluando y simplificando, tenemos $\zeta\left(\frac{1}{2}+it\right) = (a+ib)(c+R)$, donde

$$\begin{aligned} a &= -0{,}157218924494551039285826449 76 \\ b &= \ 0{,}987563775044820413868568475 12 \\ c &= -0{,}314437848989102078571652899 5 \end{aligned}$$

$N = \lfloor\sqrt{t/2\pi}\rfloor = 1$ y R es el resto, para calcularlo prodecemos de la siguiente forma

$$R \approx (-1)^{N-1}\left(\frac{t}{2\pi}\right)^{-1/4}\left[C_0+C_1\left(\frac{t}{2\pi}\right)^{-1/2}+C_2\left(\frac{t}{2\pi}\right)^{-2/2}+C_3\left(\frac{t}{2\pi}\right)^{-3/2}+C_4\left(\frac{t}{2\pi}\right)^{-4/2}\right]$$

donde

$C_0 = \Psi(p) = \frac{\cos\left(2\pi(p^2-p-1/16)\right)}{\cos(2\pi p)}$,

$C_1 = -\frac{1}{96\pi^2}\Psi^{(3)}(p)$,

$C_2 = \frac{1}{18432\pi^4}\Psi^{(6)}(p)+\frac{1}{64\pi^2}\Psi^{(2)}(p)$,

$C_3 = -\frac{1}{5308416\pi^6}\Psi^{(9)}(p) - \frac{1}{3840\pi^4}\Psi^{(5)}(p) - \frac{1}{64\pi^2}\Psi^{(1)}(p)$,

$C_4 = \frac{1}{2038431744\pi^8}\Psi^{(12)}(p) + \frac{11}{5898240\pi^6}\Psi^{(8)}(p) + \frac{19}{24576\pi^4}\Psi^{(4)}(p) + \frac{1}{128\pi^2}\Psi(p)$,

y $\Psi^{(n)}$ indica la $n-$ésima derivada, y donde p es la parte fraccionaria $p = \{\sqrt{\frac{t}{2\pi}}\}$, i.e.,

$p = \{1{,}49987045292330744821912595010 34\}$,

$p = 0{,}49987045292330744821912595010 34$.

Procedemos a calcular las derivadas y evaluar para encontrar los coeficientes $C_m,\ m = 0, 1, 2, 3$.

$C_0 = 0{,}38268346171694693660489883865$,

$C_1 = 6{,}95022701520973305446848 1 \times 10^{-6}$,

$C_2 = 0{,}00518854285106749118451846077$,

$C_3 = 3{,}47112541178474593177 \times 10^{-7}$,

$\left(\frac{t}{2\pi}\right) = \left(\frac{14{,}13\ldots}{2\pi}\right) = 2{,}24961137555236742424327071159 01$,

así, tenemos que

$R = 0{,}31436036266531701906583 5758$.

Y sustituyendo los valores en la expresión $\zeta(1/2 + it)$, tenemos

$$\zeta\left(\frac{1}{2} + it\right) = (a + ib)(c + R)\ , \quad \text{i.e.}$$

$$\zeta\left(\frac{1}{2} + i14{,}134\ldots\right) = (-0{,}15\cdots + i0{,}98\ldots)\,(-0{,}31443\cdots + 0{,}31436\ldots)$$

$$\Rightarrow\ \zeta\left(\frac{1}{2} + i14{,}134\ldots\right) = (-0{,}15\cdots + i0{,}98\ldots)\,(-0{,}3144\cdots + 0{,}3143\ldots)$$

$$\Rightarrow\ \zeta\left(\frac{1}{2} + i14{,}134\ldots\right) = (-0{,}15\cdots + i0{,}98\ldots)\,(-0{,}000077486323785059)$$

$$\Rightarrow\ \zeta\left(\frac{1}{2} + i14{,}134\ldots\right) = (-0{,}1572189244945 + i0{,}9875637750448)\,(-0{,}00007748632378)$$

$$\Rightarrow\ \zeta\left(\frac{1}{2} + i14{,}134\ldots\right) = (0{,}00001218231648852360473 - i0{,}00007652268643151862326)$$

luego, $\zeta(\frac{1}{2} + i14{,}134\ldots) = (0 + i0)$ es el primer cero no trivial de la función, tal que

$$\mathrm{Re}(s) = \frac{1}{2} \quad \wedge \quad \mathrm{Im}(s) = 14{,}134725141734693790457251983 5625\ .$$

Así, hemos verificado que la función zeta tiene un cero no trivial.

3.3. La función zeta y los números primos

La esencia de la relación entre $\zeta(s)$ y los números primos es la fórmula del producto de Euler

$$\zeta(s) = \prod_p \frac{1}{1-p^{-s}} \ , \quad \mathrm{Re}(s) > 1 \ ,$$

en la que el producto de la derecha se toman a todos los números primos. Tomando el logaritmo de ambos lados y usando la serie

$$\log(1-x) = -x - \frac{1}{2}x^2 - \frac{1}{3}x^3 - \cdots \ ,$$

obtenemos

$$\log\zeta(s) = \sum_p \sum_n \left(\frac{1}{n}\right) p^{-ns} \ , \quad \mathrm{Re}(s) > 1 \ .$$

Esta suma se puede escribir como una integral de Stieltjes[26]

$$\log\zeta(s) = \int_0^\infty x^{-s} dJ(x) \ , \quad \mathrm{Re}(s) > 1 \ ,$$

donde $J(x)$ es la función que comienza en 0 para $x = 0$ y aumenta en un salto de 1 para los primos p, con un salto de $1/2$ para los primos al cuadrado p^2, con un salto de $1/3$ para números primos al cubo p^3 y así sucesivamente. En general, tenemos un salto de $1/i$ por cada $i-$ésima potencia de un primo, i.e., p^i.

Como es habitual en la teoría de las integrales de Stieltjes, el valor de $J(x)$ cada salto se define como el punto medio entre el valor anterior y el siguiente. Entonces $J(x)$ es igual a cero para $0 \leq x < 2$, es $1/2$ para $x = 2$, es 1 para $2 < x < 3$, etcétera. Por lo tanto, una fórmula para $J(x)$ es

$$J(x) = \frac{1}{2}\left[\sum_{p^n<x} \frac{1}{n} + \sum_{p^n \leq x} \frac{1}{n}\right] \ .$$

Claramente estamos interesados en $\pi(x)$ y no en $J(x)$. Las dos funciones están relacionadas por la ecuación.

$$J(x) = \pi(x) + \frac{1}{2}\pi(x^{1/2}) + \frac{1}{3}\pi(x^{1/3}) + \cdots + \frac{1}{n}\pi(x^{1/n}) \ .$$

Simplificando la definición de $J(x)$ que debe tener en cuenta el valor en puntos de salto en la definición más simple

$$J(x) = \sum_{p^n \leq x} \frac{1}{n} \ ,$$

entonces, tenemos que

$$n = 1 \quad \Rightarrow \quad \sum_{p^1 \leq x} \frac{1}{1} \qquad \Rightarrow \quad \frac{\pi(x^1)}{1} \ ,$$

[26] La integral de Riemann-Stieltjes es una generalización de la integral de Riemann, es una herramienta inestimable para unificar formas equivalentes de teoremas estadísticos que se aplican en la probabilidad discreta y continua. A diferencia de la integral de Riemann, que depende de una sola función f llamada integrando, la integral de Riemann-Stieltjes depende de dos funciones, el integrando f y una función α llamada integrador. Para la integral de Riemann-Stieltjes se utiliza el siguiente símbolo: $\int_a^b f \ d\alpha$.

$$n=2 \quad \Rightarrow \quad \sum_{p^2\leq x}\frac{1}{2} \quad \Rightarrow \quad \frac{\pi(x^{1/2})}{2}\ ,$$

$$n=3 \quad \Rightarrow \quad \sum_{p^3\leq x}\frac{1}{3} \quad \Rightarrow \quad \frac{\pi(x^{1/2})}{3}\ ,$$

$$\vdots$$

Sumando todos los términos llegamos a la fórmula para $J(x)$. Es interesante notar que la sumatoria no es infinita ya que para "n" lo suficientemente grande tendremos $x^{1/n}<2$ y por lo tanto $\pi(x^{1/n})=0$.

Riemann invierte la relación entre $J(x)$ y $\pi(x)$ usando la "fórmula de inversión de Möbius (Teorema 1.9.11.)" para encontrar que

$$\pi(x)=\sum_n \frac{\mu(n)}{n}J(x^{1/n})\ .$$

Partiendo de la fórmula

$$J(x)=\pi(x)+\frac{1}{2}\pi(x^{1/2})+\frac{1}{3}\pi(x^{1/3})+\cdots+\frac{1}{n}\pi(x^{1/n})\ ,$$

para cada número primo "p", debemos reemplazar por ambos miembros la función $f(x)$ con $f(x)-f(x^{1/p})/p$. Entonces, repitiendo el procedimiento tenemos que

$$J(x)=\pi(x)+\frac{1}{2}\pi(x^{1/2})+\frac{1}{3}\pi(x^{1/3})+\cdots+\frac{1}{n}\pi(x^{1/n})$$

$$J(x)-\frac{J(x^{1/2})}{2}=\pi(x)+\frac{1}{3}\pi(x^{1/3})+\cdots+\frac{1}{n}\pi(x^{1/n})$$

$$J(x)-\frac{J(x^{1/2})}{2}-\frac{J(x^{1/3})}{3}+\frac{J(x^{1/6})}{2}=\pi(x)+\cdots+\frac{1}{n}\pi(x^{1/n})$$

$$\vdots$$

En el segundo paso, la $f(x)$ genérica viene dada por $J(x)-J(x^{1/2})/2$ por lo tanto se sustituye con $f(x)-f(x^{1/3})/3$ que lleva a $J(x^{1/2})/2-J(x^{1/3})/3+J(x^{1/6})/2$ donde los signos de los términos corresponden al número de factores (el signo es positivo para un número par de factores, negativo para un número impar). Llevando este razonamiento al infinito, la inversión se completa.

Por tanto, la fórmula para $\pi(x)$ viene dada por una suma de contribuciones de tres tipos

- Contribuciones que crecen monótonamente con x.
- Contribuciones que crecen en valor absoluto pero fluctúan en signo.
- Contribuciones que no aumentan cuando x aumenta.

Intuitivamente puede venir a la mente considerar sólo las contribuciones de primer tipo y en este caso tendríamos la aproximación

$$\pi(x) = \sum_{1}^{\infty} \frac{\mu}{n} \operatorname{Li}(x^{1/n}) \ .$$

Lo extraordinario es que esta aproximación demuestra empíricamente ser mucho más precisa que la aproximación de Gauss (i.e., $\operatorname{Li}(x)$).

Las dos aproximaciones son buenas pero la de Riemann está cada vez más cerca del valor real.

Riemann sugirió que al tomar sólo los términos $\operatorname{Li}(x^{1/n})$ se encontraba ya una buena aproximación, hasta diez millones, el error de Riemann en la aproximación del conteo de números primos fue de unas pocas docenas de números, mientras que el de $\operatorname{Li}(x)$ es de cuatro a diez veces mayor. Luego añadió también el término sobre los ceros de la función zeta. Entonces tenemos la función $R(x)$ que aproxima a $\pi(x)$ dada por

$$R(x) = \sum_{n=1}^{n} \frac{\mu(n)}{n} \operatorname{Li}(x^{1/n}) + \sum_{n=1}^{n} \frac{\mu(n)}{n} \left(\int_{x^{1/n}}^{\infty} \frac{dt}{(t^2-1)t \ \log t} - \log 2 \right)$$

$$- \sum_{\nu=1}^{k} \sum_{\nu=1}^{n} \frac{\mu(n)}{n} (\operatorname{Li}(x^{\rho\nu/n}) + \operatorname{Li}(x^{\bar{\rho}\nu/n})) \ .$$

Tomando sólo los primeros k pares de ceros no triviales de la función $\zeta(s)$, con ρ cero no trivial de la función zeta.

¿Y esto nos da un buen resultado? Veamos qué sucede con la función $R(x)$, con respecto a $\pi(x)$, probemos para un cero no trivial, i.e., $R_1(x)$

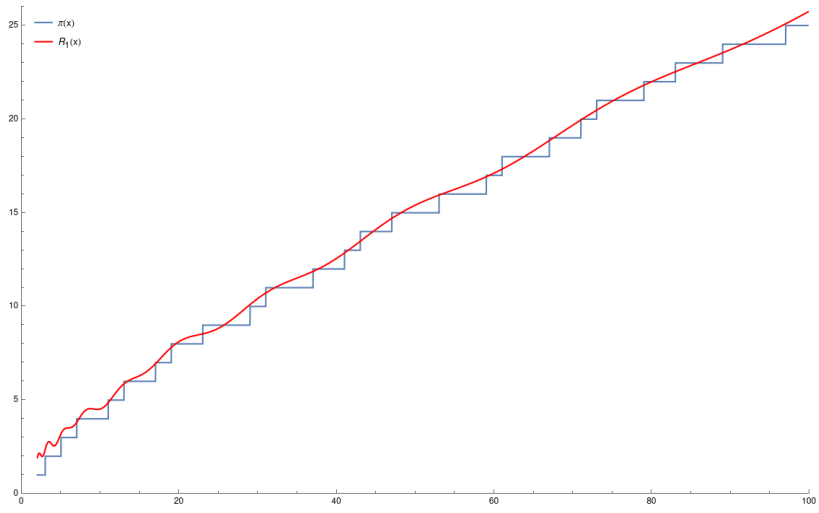


Figura 3.10: La función R_1 aproximando la escala de los números primos $\pi(x)$ hasta 100.

Probemos ahora con $R_{10}(x)$

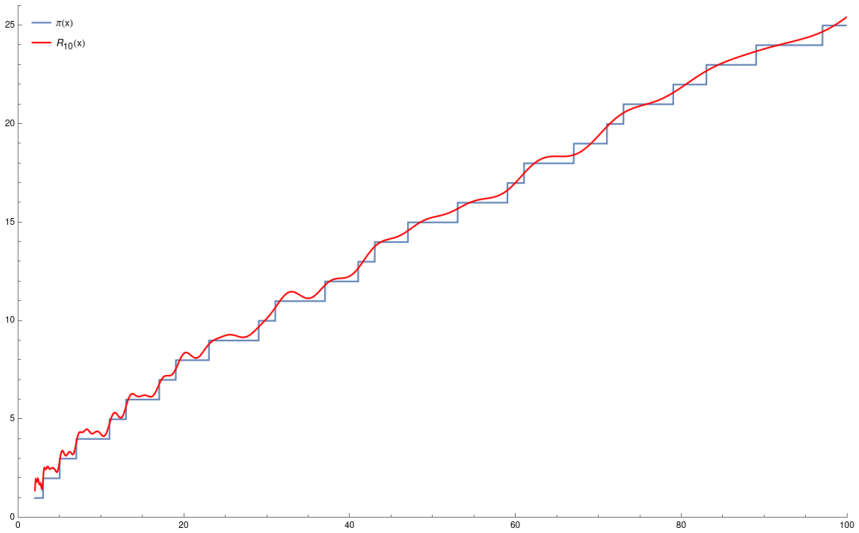


Figura 3.11: La función R_{10} aproximando a $\pi(x)$ hasta 100.

Probemos ahora con $R_{25}(x)$

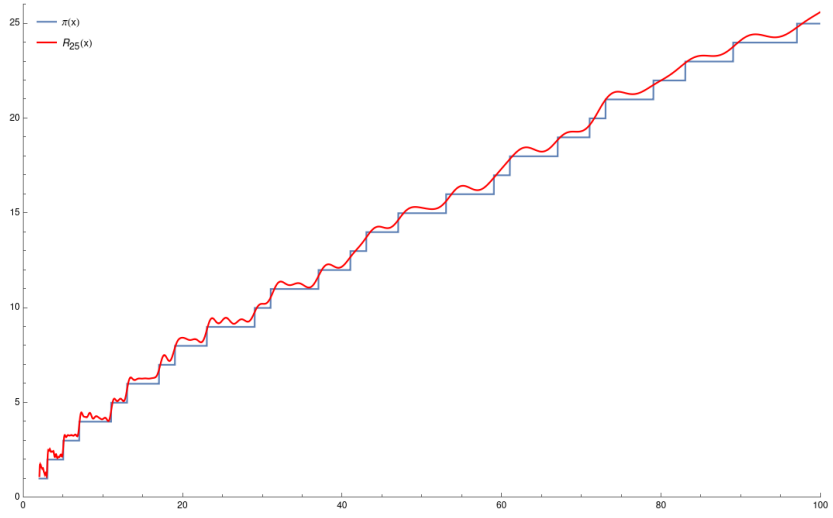


Figura 3.12: La función R_{25} aproximando a $\pi(x)$ hasta 100.

Probemos ahora con $R_{50}(x)$

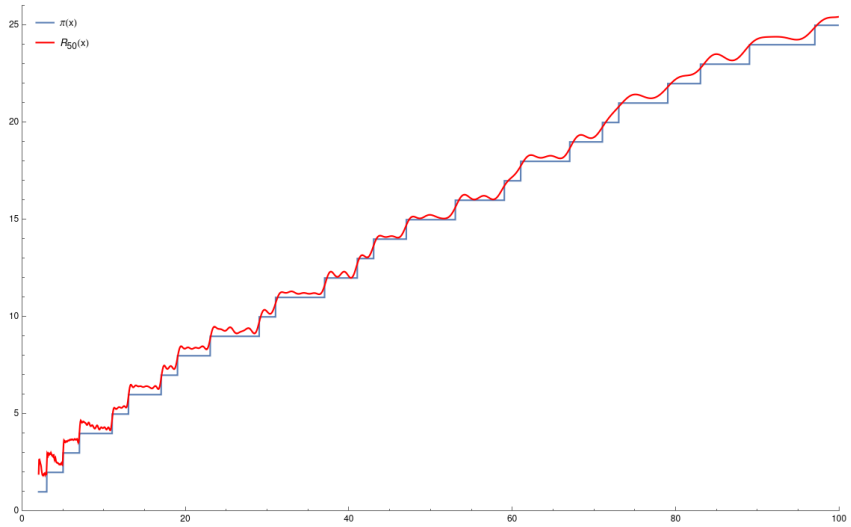


Figura 3.13: La función R_{50} aproximando a $\pi(x)$ hasta 100.

Finalmente, probemos ahora con $R_{25}(x)$

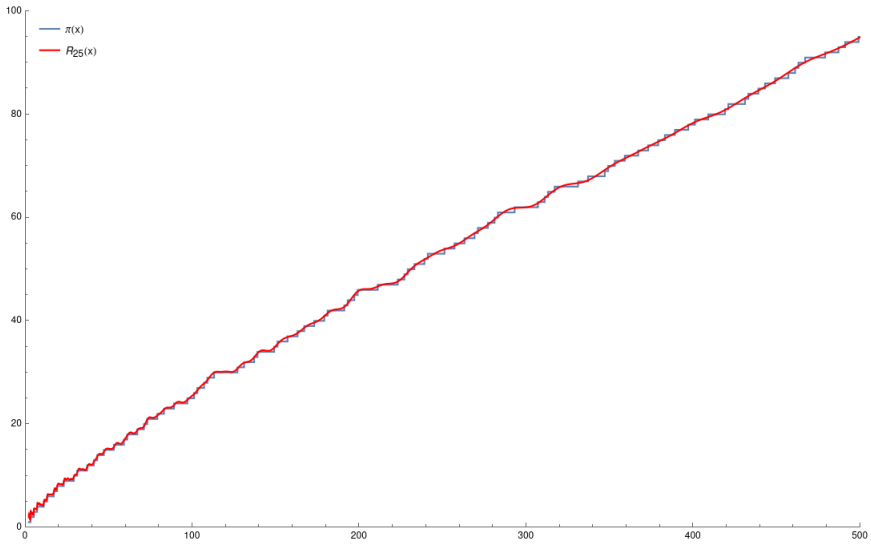


Figura 3.14: La función R_{25} aproximando a $\pi(x)$ hasta 500.

Veamos la siguiente tabla donde se muestran las estimaciones al valor real de $\pi(x)$

x	$\pi(x)$	$\mathrm{Li}(x)$	$\pi(x) - \mathrm{Li}(x)$	$R(x)$	$\pi(x) - R(x)$
100	22	30	5	26	1
1000	168	178	10	168	0
10000	1229	1246	17	1227	-2
10^6	9592	9630	38	9587	-5
10^7	78498	78638	130	78527	29
10^8	664579	664918	339	664667	88
10^9	5761455	5762209	754	5761552	97
10^{10}	50847534	50849235	1701	50847455	-79
10^{11}	455052511	455055615	3104	455050683	-1828
10^{12}	4118054813	4118066401	11588	4118052495	-2318

Como se puede observar hay oscilaciones de las dos aproximaciones pero la de Riemann está cada vez más cerca del valor real. La fórmula de Riemann proporciona una estimación del error cometido por su fórmula.

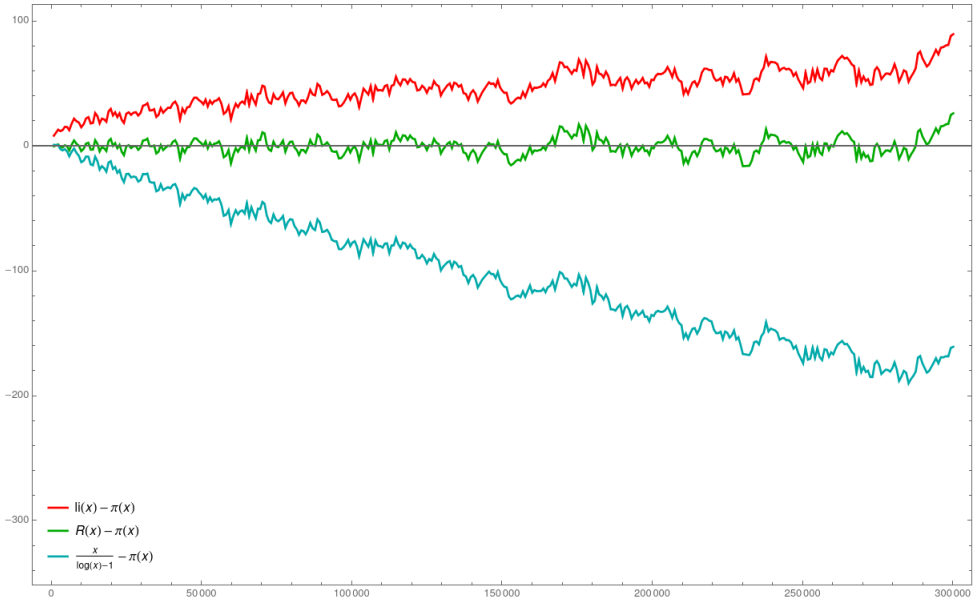


Figura 3.15: Comparación entre las funciones $\mathrm{Li}(x)$, $R(x)$, $x/(\mathrm{Log}(x) - 1)$ en diferencia con la función $\pi(x)$, de 0 a 300000.

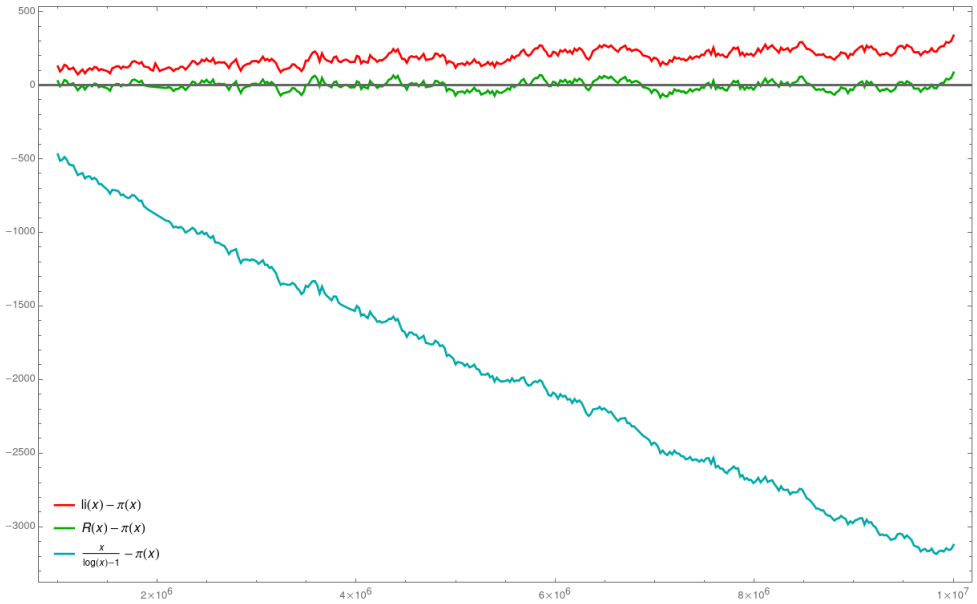


Figura 3.16: Comparación entre las funciones $\mathrm{Li}(x)$, $R(x)$, $x/(\mathrm{Log}(x)-1)$ en diferencia con la función $\pi(x)$, de 10^6 a 10^7.

Como ya se mencionó, la estimación de Gauss usando el logaritmo integral es muy buena, sin embargo, podemos concluir que la función $R(x)$ de Riemann es mucho mejor, en la cual los ceros no triviales de la función zeta son utilizados como "correctivos" en la estimación.

Capítulo 4

Relación con la Física

Todo lo que se piensa sobre el contenido Universo a grosso modo está representado por la siguiente fígura.

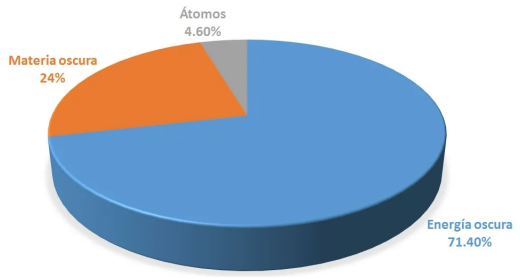


Figura 4.1: Composición del Universo.

Hoy se estima que la materia ordinaria compone alrededor de un 4,6 % del universo. Por otro lado, alrededor del 24 % está compuesto por la materia oscura, y el restante 71,4 % lo conforma la energía oscura. Estas últimas dos denominaciones tan parcas muestran, en realidad, lo poco que se sabe tanto de la materia oscura como de la energía oscura.

- Materia oscura: No emite ni absorbe radiación electromagnética. Si lo hiciera, podríamos conocer mucho más acerca de ella, ya que cada tipo de molécula reflejaría la luz de una manera diferente, e interactuaría con cada uno de los tipos de onda de forma única, revelando así algunas de sus propiedades físicas. Su existencia se deduce a partir de sus efectos gravitacionales sobre la materia que afectan el movimiento de esta, o bien la distorsionan a través de lo que se conoce como la lente gravitacional (la curvatura de un haz de luz al pasar cerca de un cuerpo), o a través de su influencia sobre la estructura a gran escala del universo (formando filamentos intergalácticos), o por sus efectos en la radiación de fondo de microondas. O sea, no se puede observar directamente, pero se pueden observar la multitud de efectos que produce sobre la materia con la que interactúa.

- Energía oscura: Tiene un efecto contrario a la gravedad, y es la causante de que el universo actual se encuentre en expansión. ¿Quizá sea la constante cosmologica de Einstein?

- Materia ordinaria o materia bariónica: Es todo aquello formado por leptones (partículas elementales) y bariones (formados por quarks, que son también partículas elementales).

Lo que entendemos es alrededor del 4 % del contenido del universo, descrito por el modelo estándar de partículas

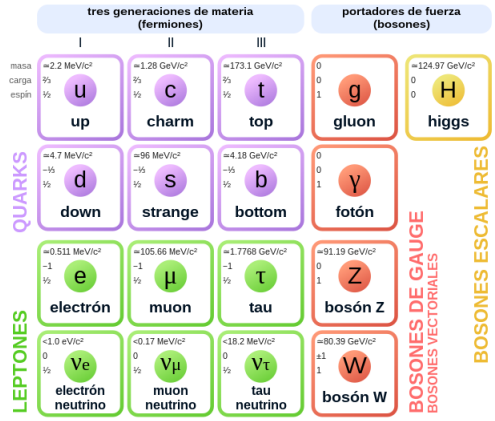


Figura 4.2: Modelo estandar de la física de partículas.

Las dos teorias fundamentales que nos ayudan a explicar todo esto son la teoría de la relatividad de Einstein y la mecánica cuántica.

Un oscilador armónico simple es una partícula o sistema que experimenta un movimiento armónico en torno a una posición de equilibrio, como un objeto con masa que vibra sobre un resorte.

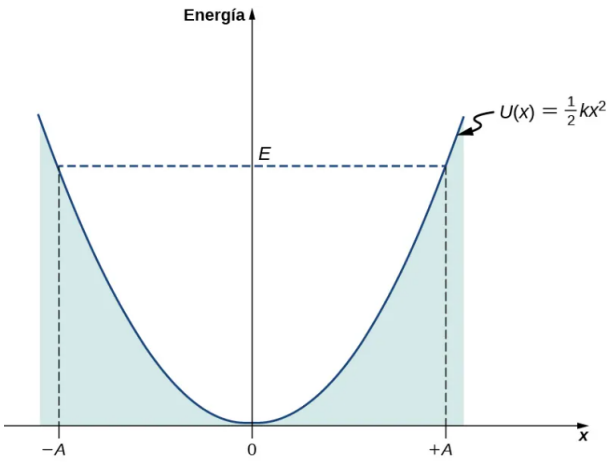


Figura 4.3: El pozo de energía potencial de un oscilador armónico clásico.

La energía de un oscilador clásico cambia de forma continua. La energía más baja que puede tener un oscilador clásico es cero, lo que corresponde a una situación en la que un objeto está en reposo en su posición de equilibrio. El estado de energía cero de un oscilador clásico significa simplemente que no hay oscilaciones ni movimiento alguno (una partícula clásica sentada en el fondo del pozo de potencial en la Figura 4.3). Cuando un objeto oscila, por muy grande o pequeña que sea su energía, pasa el mayor tiempo cerca de los puntos de inflexión, porque es ahí donde frena e invierte su dirección de movimiento. Por lo tanto, la probabilidad de encontrar un oscilador clásico entre

los puntos de giro es mayor cerca de los puntos de inflexión y menor en la posición de equilibrio. (Observe que esto no es una declaración de preferencia del objeto por ir a una energía más baja. Es una declaración sobre la rapidez con la que el objeto se mueve a través de varias regiones).

Un problema de esta formulación clásica es que no es general. No podemos utilizarla, por ejemplo, para describir las vibraciones de las moléculas diatómicas, donde los efectos cuánticos son importantes. Un primer paso hacia una formulación cuántica es utilizar la expresión clásica $k = m\omega^2$ para limitar la mención de una constante de "resorte" entre los átomos. De este modo, la función de energía potencial puede escribirse en una forma más general

$$U(x) = \frac{1}{2} m\omega^2 x^2 \ .$$

Combinando esta expresión con la ecuación de Schrödinger independiente del tiempo se obtiene

$$-\frac{\hbar}{2m}\frac{d^2\psi(x)}{dx^2} + \frac{1}{2}m\omega^2 x^2 \psi(x) = E\psi(x) \ ,$$

para resolver la ecuación anterior (es decir, para encontrar las energías permitidas E y sus funciones de onda correspondientes $\psi(x)$) necesitamos que las funciones de onda sean simétricas respecto a $x = 0$ (el fondo del pozo potencial) y normalizables. Estas condiciones garantizan que la densidad de probabilidad $|\psi(x)|^2$ deba ser finita cuando se integre en todo el rango de x desde $-\infty$ hasta $+\infty$. Las energías permitidas son

$$E_n = \left(n + \frac{1}{2}\right)\hbar\omega = \frac{2n+1}{2}\hbar\omega \ , \qquad n = 0, 1, 2, 3, \ldots \ .$$

Las funciones de onda que corresponden a estas energías (los estados estacionarios o de energía definida) son

$$\psi_n(x) = N_n e^{-\beta x^2/2} H_n(\beta x) \ , \qquad n = 0, 1, 2, 3, \ldots \ ,$$

donde $\beta = \sqrt{m\omega/\hbar} N_n$ es la constante de normalización, y $H_n(y)$ es un polinomio de grado n llamado Polinomio de Hermite. Los cuatro primeros polinomios de Hermite son

$$H_0(y) = 1 \ , \quad H_1(y) = 2y \ , \quad H_2(y) = 4y^2 - 2 \ , \quad H_3(y) = 8y^3 - 12y \ .$$

Algunos ejemplos de funciones de onda figuran en la Figura 4.4. A medida que aumenta el valor del número principal, las soluciones alternan entre funciones pares e impares alrededor de $x = 0$.

A diferencia de un oscilador clásico, las energías medidas de un oscilador cuántico solo pueden tener valores energéticos dados por la Ecuación para E_n. Los niveles de energía permitidos están espaciados de manera uniforme. Está discretizada, i.e., la enegía está cuantizada.

De la expresión de E_n tenemos la relación entre energías discretas con números enteros n.

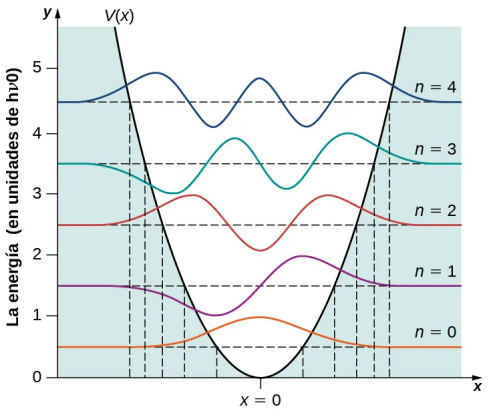


Figura 4.4: Cinco primeras funciones de onda del oscilador armónico cuántico. Los límites clásicos del movimiento del oscilador se indican con líneas verticales, correspondientes a los puntos de inflexión clásicos en $x = \pm A$ de una partícula clásica con la misma energía que la de un oscilador cuántico en el estado indicado en la figura.

Si nos ponemos filosóficos podemos pensar que:

- "El número hecho realidad es lo cuántico".
- "Lo cuántico es el número hecho realidad".
- ¿Existirá algún oscilador armónico cuántico cuyo espectro sean los números primos?

4.1. Cuántica y teoría de números

En la actualidad, lo máximo que sabemos es que al menos el 40 por ciento de los (infinitos) ceros no triviales lo satisfacen, y que es cierto para los primeros 100 mil millones de ellos. La Universidad de Bristol ha estado a la vanguardia en demostrar que existen sorprendentes similitudes entre los ceros de Riemann y los niveles cuánticos de energía de los sistemas clásicamente caóticos.

De una conferencia celebrada en 1996 en Seattle, destinada a fomentar la colaboración entre físicos y teóricos de números, surgieron pruebas tempranas de correlación entre la disposición de los ceros no triviales de Riemann y los niveles de energía de los sistemas caóticos cuánticos. Si esto fuera cierto, probaría la hipótesis de Riemann.

Ahora bien, hay ciertos atributos de la función zeta de Riemann llamados momentos que deberían dar lugar a una secuencia de números. Sin embargo, antes de la conferencia de Seattle, sólo se conocían dos de estos momentos: 1, calculado por Hardy y Littlewood en 1918; y 2, calculado por Ingham en 1926. Conrey (ahora también en Bristol) y Ghosh sugirieron que el siguiente número de la serie era 42 en 1992.

El desafío para los físicos cuánticos entonces era comprobar el número 42 con sus métodos cuánticos y calcular otros momentos de la serie, mientras que los teóricos de los números intentaban hacer lo mismo con sus métodos.

El profesor Jon Keating y la doctora Nina Snaith de Bristol describen los niveles de energía en los sistemas cuánticos utilizando la teoría de matrices aleatorias. Utilizando métodos RMT (Random Matrix Theory), produjeron una fórmula para calcular todos los momentos de la función zeta de Riemann. Esta fórmula confirmó el número 42.

Dos años después de Seattle, Keating y Snaith asistieron a una conferencia de seguimiento en el Instituto Schrodinger de Viena para presentar su fórmula. Mientras tanto, los teóricos de números Conrey y Gonek habían sugerido el siguiente momento de la serie.

Cuando se utilizó la fórmula de Keating y Snaith para calcular este momento, coincidió con la sugerencia de los teóricos de los números: 24,024. La fórmula realmente funciona.

Por lo general, las matemáticas puras apoyan a la física, proporcionando las herramientas matemáticas con las que se analizan los sistemas físicos, pero este es el caso inverso: la física cuántica está conduciendo a nuevos conocimientos sobre la teoría de números.

Ha habido un entusiasmo considerable acerca de estas conexiones entre la hipótesis de Riemann y la mecánica cuántica, pero aunque han inspirado varias líneas de ataque nuevas, el problema aún continúa resistiendo. Realmente no sabemos por qué los métodos RMT funcionan para calcular los momentos de la función zeta de Riemann. Sin embargo, se han utilizado para sugerir respuestas a algunos otros problemas importantes y de larga data relacionados con la función zeta.

4.2. La conjetura de Hilbert-Pólya

Una estrategia para demostrar la hipótesis de Riemann es la conocida como conjetura de Hilbert-Pólya. Se trata de encontrar un operador autoadjunto en un espacio de Hilbert cuyos valores propios serían las ordenadas de los ceros de la función zeta. Dado que el operador es autoadjunto, estos valores propios serían reales. En la Mecánica Cuántica un sistema está gobernado por un operador autoadjunto, el hamiltoniano. Entonces pensaron que un sistema físico adecuado tendría como hamiltoniano al operador dream de Hilbert-Pólya.

Hay que encontrar un espacio de Hilbert H y un operador D en este espacio. Entonces hay que probar dos cosas que D es autoadjunto y que los ceros de la función zeta son todos de la forma $\frac{1}{2} + i\lambda$ cuando λ recorre los valores propios de D.

4.3. Los niveles de Landau y los ceros de la funcion zeta

En 1999, Berry y Keating por un lado y Connes por otro, propusieron un modelo heurístico semiclásico que contiene la aproximación media a los ceros de Riemann. Dicho modelo describe una partícula moviéndose en una dimensión, cuyo Hamiltoniano clásico es $H = xp$, donde x es la posición y p es el momento. El trabajo de estos autores difiere sin embargo en la manera en que aparecen los ceros de Riemann. En el modelo de Berry y Keating los ceros aparecen en el espectro discreto, mientras que en el de Connes el espectro es un continuo, siendo los ceros de Riemann líneas espectrales de absorción. La diferencia entre estos dos resultados opuestos se halla en la diferente elección del espacio de fases semiclásico.

En un reciente trabajo publicado en la Revista Physical Review Letters, y titulado "Landau levels and Riemann zeros" se propone una realización física del modelo de Berry-Keating y Connes empleando una partícula cargada, por ejemplo un electrón, moviéndose en un plano bajo la acción de un campo magnético perpendicular al mismo y un campo eléctrico en forma de silla. El campo magnético hace que los electrones giren en órbitas ciclotrónicas, cuyo centro describe trayectorias hiperbólicas por el efecto del campo eléctrico. Cuando el electrón se coloca en una caja finita y en el nivel de Landau de más baja energía, se obtiene un espectro continuo corregido por la parte promedio de los ceros de Riemann, lo cual está de acuerdo con el resultado semiclásico de Connes.

Existen razones para pensar que la inclusión de niveles de Landau de más alta energía podrá dar una realización espectral de los ceros de Riemann, y no sólo de su aproximación promedio. Por otra parte, no hay que descartar que la versión de Berry y Keating sea realizable en el contexto del modelo de Landau. El sistema físico propuesto es de uso corriente en el estudio teórico y experimental del Efecto Hall cuántico, por lo que de ser cierta la conjetura de este trabajo se abriría la posibilidad de una observación experimental de los ceros de Riemann. Por otra parte la consistencia matemática del modelo posiblemente llevaría a la demostración de la Hipótesis de Riemann, aunque aún es pronto para saber si esto es así.

Últimos avances

- El gran matemático Michael Atiyah, Medalla Fields en 1966 y Premio Abel en 2004, ofreció una charla en el Heidelberg Laureate Forum en septiembre del 2018. Se anunció que presentaría una demostración (sencilla) de la hipótesis de Riemann. En paralelo se publicó un artículo de cinco páginas con la (supuesta) demostración, que se basa en un artículo previo de diecisiete páginas con un (supuesto) cálculo de la constante de estructura fina; ambos manuscritos fueron rechazados en arXiv.

- Los investigadores Germán Sierra, del Instituto de Física Teórica (centro mixto del CSIC y la Universidad Autónoma de Madrid), y Paul Townsend, de la Universidad de Cambridge (Reino Unido), proponen un modelo en el que un electrón es sometido a determinados campos electromagnéticos, en concreto, un campo eléctrico perpendicular al electrón y otro campo magnético en forma de silla.

  "En este modelo los niveles de energía del átomo coinciden, en término medio, con la posición de los ceros de la función zeta de Riemann, aunque aún no es capaz de determinar su posición exacta". Se trata de una realización física del modelo matemático propuesto en 1999 por Berry, Keating y Connes.

- Brad Rodgers y Terence Tao prueban (sin admitir ninguna hipótesis adicional) la conjetura de Newman $\Lambda \geq 0$. La prueba es por reducción al absurdo. Supongamos que $\Lambda < 0$, entonces por el resultado de Newman $H_0(x)$ tendrá todos sus ceros reales. Por tanto la hipótesis de Riemann sería válida. Y podemos admitirla en todo el razonamiento por reducción al absurdo.

Los resultados anteriores a primera vista hacen pensar que la prueba de la hipótesis de Riemann está ahora más lejos que nunca. Si la hipótesis de Riemann es cierta, la más ligera perturbación de la función $H_0(t)$ hará que aparezcan ceros complejos. Posiblemente hay o algún cero doble o una infinidad de pares de Lehmer cada vez más extremos.

Los ceros determinan la función $H_t(x)$:

$$H_t(x) = H_t(0) \prod_{j=1}^{\infty} \left(1 - \frac{x^2}{x_j(t)^2}\right) .$$

Par de Lehmer. El par de ceros reales y consecutivos $x_k(0) < x_{k+1}(0)$ de la función $H_0(x)$ se dice que es un par de Lehmer si la diferencia $\Delta_k = x_{k+1}(0) - x_k(0)$ satisface la desigualdad $\Delta_k^2 \cdot g_k(0) < 4/5$ donde

$$g_k(0) = \sum_{j \neq k,k+1} \left(\frac{1}{(x_k(0) - x_j(0))^2} + \frac{1}{(x_{k+1}(0) - x_j(0))^2}\right) .$$

Esta irregularidad de los ceros siempre ha sido la principal dificultad para probar la hipótesis de Riemann. No parece que pueda existir ninguna aproximación asintótica a ξ o a $Z(t)$ que impliquen que los ceros sean reales, ni siquiera que la mayor parte de los ceros son reales. Los métodos actuales no consiguen probar ni siquiera que el 50 % de los ceros de $\zeta(s)$ están en la recta crítica.

Bibliografía

[1] The Riemann Hypothesis A Resource for the Afficionado and Virtuoso Alike, Peter Borwein, Stephen Choi, Brendan Rooney, Andrea Weirathmueller. 2008.

[2] Matemáticas elementales, "La Comisión", FCFM-BUAP, Rev. 2015.

[3] La música de los números primos, Marcus Du Sautoy, 2003.

[4] Prime Numbers and the Riemann Hypothesis, Barry Mazur and William Stein.

[5] Breviario de teoría analica de los números, Eugenio P. Balanzario, Sociedad matemática mexicana, 2009.

[6] Introducción a la teoría de números, Felipe Zaldívar, Fondo de Cultura Económica, 2017.

[7] Introducción a la teoría analítica de los números, T.M. Apostol, Reverté, 2019.

[8] Análisis matemático, T.M. Apostol, Reverté, 1976.

[9] The Theory of The Riemann Zeta Function, E. C. Titchmarsh, Oxford, 1986.

[10] Notas del curso de teoría de números, Carlos Alberto López Andrade, FCFM-BUAP. 2022.

[11] Análisis básico de variable compleja, Jerrold E. Marsden, Trillas, 2012.

[12] Los números de Bernoulli y sus aplicaciones, Stefania Aru and Prof. Lucio Cadeddu, 2011.

[13] Introducción al análisis de variable compleja y la teoría de las distribuciones, F. Fagnani, A. Tabacco y P. Tilli, 2006.

[14] The Riemann Zeros and Eigenvalue Asymptotics, M.V.Berry and J.P.Keating, Review article from SIAM Review, 41, No.2 (1999) 236-266.

[15] La Hipótesis de Riemann, Ticiano M, 2011.

[16] Física universitaria volumen 3, William Moebs, Samuel J. Ling, Jeff Sanny, 2021.

[17] Zeros of the Zeta Function, Bachelor's project mathematics, 2020.

[18] Pure and Applied Mathematics, H. M. Edwards - Riemann's Zeta function, 1974.

[19] Quantum physics sheds light on Riemann hypothesis, The University of Bristol, School of Mathematics.

[20] BLog del Instituto de Matemáticas de la Universidad de Sevilla, institucional.us.es/blogimus.