Primos en progresiones aritméticas

"La matemática es la reina de las ciencias y la Teoría de Números es la reina de la matemática."

Carl Friedrich Gauss, 1777 – 1855.

$$6\mu + 1 \quad 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, \ldots$$

$$\prod \frac{1}{1 - \Theta^{\mathfrak{a}\alpha}\,\Omega^{\mathfrak{c}\gamma}\frac{1}{q^s}} = \sum \Theta^{\mathfrak{a}\alpha}\,\Omega^{\mathfrak{c}\gamma}\frac{1}{n^s} = L_{\mathfrak{a},\mathfrak{c}}$$

$$\Phi_n = \prod_{\xi \in \mathbb{G}_n^*} (X - \xi)$$

Un paseo por el Teorema de Dirichlet sobre Progresiones Aritméticas, el orígen de la Teoría Analítica de Números

Aaron Blas Pereda

Facultad de Matemática, Astronomía, Física y Computación
Universidad Nacional de Córdoba

Concurso de monografías 2024

UNION MATEMATICA ARGENTINA
FUNDADA EN 1936

Agradecimientos

A mi novia Sofía Cuva, quien me ayudó con problemas técnicos y me animó cuando dudé en abandonar la idea de esta monografía, cuando ya se encontraba iniciada.

Al profesor Diego Sulca, que me introdujo el tema y brindó su conocimiento.

A mis amigos que me escucharon cada vez que les hablaba emocionado con el tema, y aportaron útiles y sinceras opiniones.

A los profesores que divulgan sobre la competencia y se muestran serviciales a consultas.

A la UMA, por ofrecer una instancia extracurricular en la cual incursionar en temas apasionantes es más que productivo y satisfactorio.

El problema

Una *progresión aritmética* módulo k con primer elemento m es una sucesión $\mu k + m$ sobre los μ enteros no negativos. Mi elección de usar estas letras tiene motivos históricos, pues es la notación usada por Dirichlet al probar el teorema enunciado a continuación, además tampoco me pareció que actualmente halla una notación estandar.

El *Teorema de Dirichlet sobre Progresiones Aritméticas* afirma que si k y m son números naturales coprimos, entonces la progresión aritmética $\mu k + m$ contiene infinitos primos.

Como ejemplo, tomando $k = 10$ y $m = 3$, el teorema asegura que existen infinitos primos que terminan en 3 en su representación decimal. Observar que si $\text{mcd}(k, m) > 1$ entonces el teorema no se cumple, pues $(k, m) \mid \mu k + m$.

Un estudiante de sexto grado conoce suficientes matemáticas para entender esta formulación particular del teorema. Sin embargo, para demostrarlo se requieren muchas ideas profundas de álgebra y análisis [18, p. 1].

El teorema nos brindan información sobre los primos vistos en congruencias modulares, presumiendo describir un aspecto importante sobre la distribución de los misteriosos números primos, paradigma que dominó gran parte de los esfuerzos de los teóricos de números en el siglo XIX.

La *Teoría de Números* es la reina de las matemáticas (cita atribuida a Gauss), y el Teorema de Dirichlet ha sido considerado una joya de esa reina. La importancia de este teorema radica no solo en su declaración sencilla, sino también en la hermosa demostración ofrecida por Dirichlet, que de hecho sentó las bases para el estudio posterior de la *Teoría de Grupos* y la *Teoría de Representaciones* [19, p. 1]. Este teorema consolida la *Teoría Analítica de Números* como una nueva área de las matemáticas, de la cual serán protagonistas matemáticos de los más eminentes que, hasta el día de hoy, dejaron tanto descubrimientos milagrosos, por ejemplo el *Teorema de los Números Primos* (cuyos primeros intentos de prueba estimularon el desarrollo del *Análisis Complejo* [1, p. 13]), como intrigantes preguntas, por ejemplo la famosa *Hipótesis de Riemann*.

Dirichlet prueba algo más fuerte que el enunciado que dimos, obteniendo que la suma $\sum \frac{1}{p}$ sobre los primos en la progresión, diverge. Personalmente, aprecio a las expresiones que obtiene Dirichlet como los albores de las extensiones meromorfas de $\zeta(s)$ con un polo simple en $s = 1$ que obtiene Riemann, así como de otras series de interés. Si Dirichlet no concretó tales hechos, fue porque dichas expresiones eran solo una herramienta para sus objetivos, además de restringirse a variables reales a más no poder debido a su época (1837).

La elección del tema radica en considerarlo ideal por ser un resultado pilar central que relaciona múltiples herramientas y objetos, crea un nuevo paradigma, incluye nombres de matemáticos de los más populares, y con suficientes preliminares puede ser presentado, en gran parte, a la comunidad matemática con al menos un año de formación. Además la pregunta sobre posibles pruebas puramente algebraicas resulta en resultados muy atractivos e increíbles. Además, la información sobre esto la encontré muy dispersa.

Al contar esta historia, tendremos que incluir nombres como el de Euclides, Euler, Legendre, Gauss, Fourier, Dirichlet, Landau, Chebotarev, Schur, Murty, y otros numerosos matemáticos que hicieron aportes que hicieron sus aportes con versiones alternativas de pruebas o de casos particulares, como por ejemplo Lebesgue y Kronecker.

Prefacio

Mi desembarco en un tema apasionante

Ingresé a la carrera de Licenciatura en Física, en FaMAF, sin tener idea de lo que era la matemática, la imagen mental que tenía de una olimpiada en matemática era la de un montón de personas reduciendo expresiones matemáticas a su forma mas simple posible, lo mas rápido que se pueda. No tenía idea de la lo que era una demostración, de la belleza de este arte que siempre había estado ocultándose de mí. Pero rápidamente me fasciné con un objeto hermoso: los números primos. Podría pensar que esta fascinación precoz por estos números se debe a que protagonizan las primeras conjeturas que uno conoce al entrar a la universidad, pero al menos en mi caso, después de 3 años de haberme cambiado a la Licenciatura en Matemática, esa profunda intriga no se ha desvanecido.

Más precisamente, esta pasión nació en una clase de Álgebra I, cuando la profesora del teórico, mencionó la *Conjetura de los Primos Gemelos*, la cual afirma que existen infinitos pares de números primos cuya diferencia es 2. Quedé sorprendido ante la incertidumbre frente a un enunciado tan simple, y no pude evitar pensarlo en tiempos libres, buscar información y ver videos de youtube, durante varios meses, hasta comprender la complejidad subyacente al problema. "Quizás comprender la distribución de los números primos es tan difícil porque al se los ladrillos de la aritmética, no contamos con elementos previos para estudiarlos", pensé, y me fasciné aún más.

> *¿Por qué los números son hermosos? Es como preguntar por qué la novena sinfonía de Beethoven es hermosa. Si no ves por qué, nadie puede explicártelo. Yo sé que los números son hermosos. Si no lo son, nada lo es.*
>
> Paul Erdős

Continué consumiendo divulgación sobre Teoría de Números (como el canal de youtube "MathArg Papers") y leyendo algunas demostraciones que pueda entender, la que más recuerdo es la de una versión débil del *Teorema de los Números Primos* que encontré en el libro [29, chap. 8] (el cual cuenta con una versión en español), y dice que existen números $a, b > 0$ tal que

$$a\frac{x}{\ln x} < \pi(x) < b\frac{x}{\ln x} \qquad \forall x \geqslant 2$$

donde $\pi(x)$ es la *Función pi de Gauss* que a cada numero x le asocia la cantidad de números primos menores o iguales a x. La demostración, a pesar de no ser tan breve, es hermosa, ingeniosa y elemental.

Llegó el momento de cursar especialidades y no dudé al elegir la primera, "Teoría Algebraica de Números". Fue ahí cuando Diego, quién dictaba la asignatura, me comento sobre el *Teorema de Densidad de Chebotarev*, un caso general del *Teorema de Dirichlet sobre Progresiones Aritméticas*. El Teorema de Chebotarev habla de objetos algebraicos mas generales que el habitual $\mathbb{Z}$, y ofrece un importante condimento extra al describir cómo se distribuyen asintóticamente los infinitos objetos de los que habla. Me resulta paradójico haber conocido esta formulación abstracta y precisa antes de su versión primitiva.

Hoy me encuentro escribiendo sobre esos objetos que me deslumbraron en las primeras clases de Álgebra. Espero poder ofrecer respuesta a posibles preguntas y tal vez contagiar

un poco de mi pasión. He disfrutado profundamente la creación de esta monografía, desde el diseño detallista de la portada que nos recuerda a los libros clásicos envejecidos, hasta el capricho de cumplir mis objetivos ideales aunque por etapas sea bastante agotador, pero fue necesario para que sea sumamente nutritivo tanto para mi forma de comprender la matemática, como para mi capacidad de darme a entender y contar una historia después de realizar un trabajo de "minería de fuentes históricas" confiables.

Objetivos y elementos de la monografía

Me gustaría poder contar esta historia como un cuento. Fue un reto de desarmar los conceptos para extraer su esencia y presentarlas de la forma mas natural posible. Afortunadamente, la gran parte de esta monografía puede ser leída por personas con al menos un año de formación matemática, este fue un objetivo claro al recordar a mi yo de primer o segundo año de facultad buscando información apta para mi escaso conocimiento en técnicas sofisticadas.

Además del contexto histórico, la monografía incluye una demostración completa del Teorema de Dirichlet. La idea general es ir construyendo los elementos que vamos necesitando, de forma que no parezcan sacados de la nada. Personalmente, soy partidario de que, al menos en las primeras instancias, las demostraciones que presentan objetos concretos fijados con antelación y al leerlas uno simplemente tiene que chequear que todo encaja, no esclarecen mucho cómo se llegó a dicha demostración, por ende perdemos parte de la iluminación que se necesita para replicar esos enfoques en problemas nuevos. Al menos al día de hoy, creo que en el arte de la matemática debe enseñarse el camino del descubrimiento desde el desconcierto, y ser esto un fuerte complemento de las ordenadas y elegantes pruebas que consisten en verificar algorítmicamente ideas previamente cocinadas.

Aquí me hubiese gustado citar una frase de Eduardo Sáenz de Cabezón en una de sus charlas. Lamentablemente no pude rastrearla bien, pero la idea la recuerdo algo así: *"La matemática no debe enseñarse en sintonía a como nos gustaría que funcione nuestro cerebro, sino a cómo realmente funciona"*.

Hay distintos artículos que tratan diferentes aspectos específicos del teorema, algunos con bastante profundidad, pero no encontré ninguno que los integre a todos ni que satisfaga mis caprichos (y aún menos en español); esto le dio mayor motivo a la elección de este tema. Un objetivo de esta monografía es recopilar toda esa información, ofreciendo un estudio abarcativo y correlativo, y dejando las correspondientes referencias para quien quiera profundizar en los aspectos que le interesen. Algunos resultados los detallo más de los que están en las referencias, incluso a veces opto por algunas variantes sutiles.

En el proceso enfático de perseguir los hilos conectores de esta historia, inevitablemente nos veremos salpicados por varios tópicos de interés propio.

Estructura de la monografía

La Sección 1 sobre historia la pueda leer cualquiera con conocimientos muy básicos de matemática. La Sección 4 es la más técnica, aquellos con un curso de Análisis Complejo y de *Estructuras Algebraicas* estarán familiarizados con los conceptos necesarios, aunque de todos modos damos los preliminares (sin pruebas) para aquellos que aún no hayan llegado a tales cursos quieran esforzarse en seguir la prueba. El resto de las secciones (2, 3 y 5) puede seguirse con naturalidad por todo aquel que cuente con un año de buena formación

matemática; aunque por momentos usamos a los grupos como lenguaje, también daremos sus debidos preliminares breves.

En § 1.1 la idea es contar en síntesis (y sin preocuparnos excesivamente en verificar que esto sea totalmente representativo de la historia completa) la historia Teoría de Números desde su origen hasta la época en que aparece el Teorema de Dirichlet, para luego en § 1.2 despegarnos y ocuparnos del teorema en específico, aquí sí tratando de ser exhaustivos. En § 1.3 mencionamos brevemente (también, sin preocuparnos en ser olvidadizos con algunos tópicos de interés) cómo continua la Teoría Analítica de Números, presentando dos problemas pilares en la disciplina. En § 1.4 comenzamos dándole un cierre breve a esta historia analítica al presentar una exquisita refinación del Teorema de Dirichlet, y cerrados el capítulo con una historia paralela que nace de una pregunta natural: ¿Es necesario el análisis para probar este enunciado puramente algebraico?

En § 2 vamos a leer el artículo original de Euler [6] que, por cierto, está en latín, como era costumbre en su época. Este escrito constituye la semilla de la Teoría Analítica de Números, que se consolidaría exactamente un siglo después con la prueba de Dirichlet. También tratamos de dar cuenta del lenguaje empleado por Euler pero sin complicarnos demasiado. De todos modos, en § 4 veremos los resultados mas generales y masticados, con pruebas mas limpias.

En § 3 vamos a motivar y leer exhaustivamente el artículo original de Dirichlet [11, *Berlin:* 45-81, *Werke* 1: 315-342] en el que prueba el teorema. Lo vamos a resumir y presentar en su propio lenguaje, orden y notación. Esto, además de bello, nos permite entender la motivación de la teoría moderna, y saber mejor lo que él pensó.

En § 4 presentamos una prueba moderna, potente, completa y ordenada. Con este propósito, necesitaremos resultados básicos del Análisis Complejo, que derivaremos del libro de Conway [16] para quien aún no esté familiarizado con ellos.

En § 5 daremos diferentes pruebas puramente algebraicas para ciertos casos particulares, incluyendo el caso $m = 1$. También discutimos algunos vínculos de estos resultados con los *números de Mersenne* y *números de Fermat*. Luego enunciamos el *Teorema de Murty*, un resultado de 1988 que le pone un sello increíble y definitivo a la pregunta sobre el límite teórico de estos procedimientos.

En § 6 concluimos con unas breves reflexiones personales sobre esta historia en su conjunto.

En § 7 damos cierre al tema enunciando un problema abierto relacionado.

Respecto a la notación, no seremos muy creativos ni cambiantes. p y q serán siempre números primos. n y N será siempre números naturales. Las letras μ, k y m quedan reservadas a hacer referencia al enunciado que dimos del Teorema de Dirichlet en la página III.

Índice general

1. Introducción histórica

Para § 1.1 usamos más que nada el libro de T. M. Apostol [1], y nos complementamos muy bien con los libros de Sean Mahoney [2] y Ian Stewart [3]. El libro [2] ofrece un amplio y profundo estudio sobre la vida y obra de Fermat, y el contexto de la época. Para un estudio enciclopédico de la historia de la Teoría de Números en general, desde la antigüedad hasta 1972, Apostol recomienda las obras de Dickson [4] y de Le Veque [30].

En § 1.2, además de otras fuentes esporádicas que mencionaremos, continuaremos consultando a Apostol, y seguimos de cerca la obra de Dickson [4, ch. XVIII], el célebre artículo *Variae observationes circa series infinitas* de Leonhard Euler [6], los artículos de Felipe Zaldívar [7] y Fernando Chamizo [8], y la tesis [17]. Por cierto, en la página web *The Euler Archive* se pueden encontrar los artículos de Euler. También consultaremos al propio Dirichlet. Los escritos originales de Dirichlet [11] están en alemán y además parece difícil conseguir una digitalización en buen estado, por lo que es sumamente útil la redigitalización a LaTeX y traducción al inglés [12].

El artículo [13] se encarga de un análisis histórico y exhaustivo sobre la evolución del lenguaje de los caracteres que implícitamente usa Dirichlet. También discute sobre la evolución de otros conceptos, como el de función y grupo.

En § 1.4.2 usamos los artículos [27, § 3] (este increíble trabajo de recopilación histórica, también ofrece detalles con los que hemos salpicado el resto de la sección). Dickson [4, p. 418-420] ofrece abundantes referencias sobre demostraciones del Teorema de Dirichlet, así que nos complementamos con él, así como con "pellizcos" de otras fuentes interesantes. De toda la gran cantidad de pruebas mencionadas en las fuentes, expongo un salpicado de varias (y casi textualmente como en las fuentes), las que consideré relevantes para esta historia.

1.1. Origen y renacimiento de la Teoría de Números

En su origen, la teoría de Números es la rama de la Matemática que trata de las propiedades de la totalidad de los números

$$1,\ 2,\ 3,\ 4,\ 5,\ \ldots$$

llamados *números naturales* o *enteros positivos*.

Los enteros positivos constituyen, sin duda alguna, la primera creación matemática del hombre. Quizás sea esta la razón por la que Gauss (de quien hablaremos próximamente), consideraba tan especial a esta disciplina, al ser tan natural y compleja a la vez.

> *"La matemática es la reina de las ciencias y la Teoría de Números es la reina de la matemática."*
>
> Carl Friedrich Gauss, 1777-1855.

La popular cita anterior presente en nuestra portada, que tal vez no haya sido tan textual, data de años antes de la prueba de Dirichlet que impulsó el desarrollo de otras áreas, dándole mas sentido a esta apreciación de Gauss en [14].

La historia nos dice que ya en los años 5700 a.C. los antiguos sumerios disponían de un calendario, luego debían haber desarrollado ya alguna forma de Aritmética. En los años 2500 a.C. desarrollaron un sistema de numeración utilizando 60 como base. Éste pasó a los

babilonios que desarrollaron una gran habilidad calculadora. Se han encontrado tablillas de arcilla babilónicas que contienen tablas matemáticas elaboradas, y que se datan en 2000 a.C.

Cuando las antiguas civilizaciones alcanzaron un nivel que les dejaba tiempo libre para pensar sobre las cosas, algunos pueblos empezaron a especular acerca de la naturaleza y propiedades de los números. Esta curiosidad se desarrolló en un cierto misticismo numérico o "Numerología", y aún hoy números como 3, 7, 11 y 13 se consideran portadores de buena o mala suerte.

Los números se utilizaron para fijar los recuerdos y celebrarlos y para las transacciones comerciales unos 5000 años antes de que se pensase en estudiarlos en sí mismos de forma sistemática. La primera orientación científica al estudio de los enteros, es decir, el origen de la *Teoría de Números*, se atribuye generalmente a los griegos. Allá por los años 600 a.C., Pitágoras y sus discípulos efectuaron un estudio bastante completo de los enteros. Fueron los primeros en clasificar los enteros de diversas formas, por ejemplo en pares o impares, primos o compuestos (el 1 no se lo considera ni primo ni compuesto; de otra forma, enunciados como el del *Teorema Fundamental de la Aritmética* serían mas intrincados).

Los pitagóricos relacionaron además los números con la Geometría. Un ejemplo son los *números poligonales*: números triangulares, números cuadráticos, números pentagonales, etc. La razón de esta nomenclatura geométrica aparece clara cuando los números se representan por medio de puntos colocados en forma de triángulos, cuadrados, pentágonos, etc. (si hay mayor interés, esto queda visualmente mas claro con la Figura I.1 de [1, p. 2]).

Otra conexión con la Geometría procede del famoso *Teorema de Pitágoras*. Los pitagóricos se interesaron por los triángulos rectángulos cuyos lados eran enteros. Tales triángulos se conocen como *triángulos pitagóricos*. La correspondiente terna de números $(x, y, z) \in \mathbb{N}$, con $z^2 = x^2 + y^2$, que representan las longitudes de los lados se llama *terna pitagórica*.

Se ha encontrado una tablilla babilónica, datada alrededor de 1700 a.C., que contiene una lista extensa de ternas pitagóricas, algunos de cuyos números son bastante grandes. Los pitagóricos fueron los primeros en proporcionar un método para determinar infinidades (pero no todas) de ternas. En notación moderna podemos describirlo como sigue: Sea n un número impar mayor que 1, entonces

$$\left(n,\ \frac{n^2-1}{2},\ \frac{n^2+1}{2}\right)$$

es siempre una terna pitagórica con $z = y+1$. Dos ejemplos de ternas que no se obtienen de esta forma son $(8, 15, 17)$ y $(12, 35, 37)$. Estas últimas, son ternas que satisfacen $z = y+2$. Platón (430-349 a.C.) justificó un método para determinar todas las ternas de este tipo; en notación moderna viene dadas por las fórmulas

$$\left(4n,\ 4n^2-1,\ 4n^2+1\right)$$

Alrededor de 300 a.C. ocurrió, en la historia de la Matemática, un suceso realmente importante. La aparición de los *Elementos*, la popular obra de Euclides, una colección de 13 libros, en particular convirtió la Numerología en una ciencia deductiva. Euclides fue el primero en presentar hechos matemáticos junto con demostraciones rigurosas.

Tres de tales libros se hallan dedicados a la Teoría de números (libros VII, IX y X). En el libro IX Euclides da su famosa demostración sobre la infinidad de números primos. En el libro X dio un método para obtener todas las ternas pitagóricas si bien no demuestra

que este método, realmente, las da todas. El método se puede establecer sumariamente por las fórmulas

$$x = t(a^2 - b^2), \qquad y = 2tab, \qquad z = t(a^2 + b^2)$$

en donde t, a, y b, son naturales tales que $a > b$, a y b son coprimos, y uno de ellos es par (y por lo tanto el otro es impar). Las ternas se podrían escribir como

$$t\left(a^2 - b^2,\ 2ab,\ a^2 + b^2\right)$$

Además Euclides da una importante contribución a otro problema planteado por los pitagóricos: el de buscar todos los *números perfectos*. El 6 fue llamado número perfecto puesto que $6 = 1 + 2 + 3$, que es la suma de sus divisores propios. Otro número perfecto es $28 = 1 + 2 + 4 + 7 + 14$. Los griegos se referían a los divisores propios de un número llamándolos sus "partes". Los números 6 y 28 se llamaron perfectos porque eran iguales a la suma de todas sus partes.

En el libro IX Euclides da todos los números perfectos pares. Demuestra que todo número de la forma

$$2^{p-1}(2^p - 1)$$

donde p y $2^p - 1$ son primos, es un número perfecto. Dos mil años más tarde, Euler demostró el recíproco, es decir cada número perfecto par debe ser del tipo descrito por Euclides. Los cinco primeros números perfectos pares son

$$6,\ \ 28,\ \ 496,\ \ 8138 \text{ y } 33\,550\,336$$

y corresponden a los primos 2, 3, 5, 7 y 13. Los números perfectos son, realmente, muy raros, y hasta el día de hoy se conocen relativamente pocos números de estos. Son tan raros como los *números primos de Mersenne*. Los *números de Mersenne* son los de la forma $M_n = 2^n - 1$ con $n \in \mathbb{N}$, y estos son primos de Mersenne cuando tanto n como M_n son primos. Llevan su nombre en honor al francés Marin Mersenne, quien los estudió en 1644.

No se sabe si existen números perfectos impares, aunque hay algunos resultados parciales que dan cotas inferiores de estos, así como restricciones sobre sus factores primos.

Después de los Elementos no se efectuaron avances significativos en Teoría de Números hasta aproximadamente 250 d.C. en que otro matemático griego, Diofanto de Alejandría, publicó 13 libros, de los que se han conservado seis. Esta es la primera obra griega en la que se realiza un uso sistemático de los símbolos algebraicos. Si bien dicha notación algebraica parece torpe frente a la usual de hoy día, Diofanto fue hábil para resolver ecuaciones algebraicas con dos o tres incógnitas. Muchos de estos problemas se originaron en la Teoría de Números y a él le pareció natural buscar *soluciones enteras* para las ecuaciones. Las ecuaciones que deben ser resueltas por medio de valores enteros de las incógnitas se llaman hoy *ecuaciones diofánticas*, y el estudio de tales ecuaciones recibe el nombre de *Análisis diofántico*. La ecuación $x^2 + y^2 = z^2$ relativas a las ternas pitagóricas constituye un ejemplo de ecuación diofántica.

Tras Diofanto no se realizaron muchos progresos en la disciplina hasta el siglo XVII, si bien existe evidencia de que el tema empezaba a florecer en el Lejano Oriente (especialmente en la India) en el período entre los años 500 y 1200.

En el siglo XVII el tema renació en la Europa Oeste, en gran manera gracias a los esfuerzos de un matemático francés, Pierre de Fermat (Francia, 1601 - Francia, 1665),

que se conoce generalmente como el padre de la Teoría de Números moderna. Cuando el interés hacia los textos clásicos de la antigua Grecia había menguado entre los afines a la matemática, Fermat los supo utilizar como inspiración, y gran parte de esta se deriva de los trabajos de Diofanto.

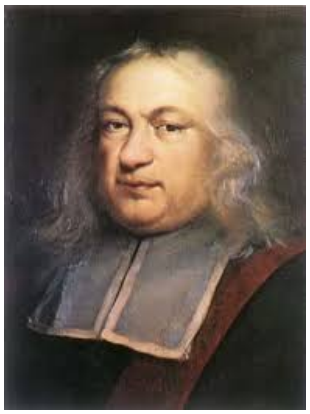

Figura 1: Fermat.

De forma contraria a la creencia popular, la matemática no era un mero pasatiempo para él. En sus tiempos no existía todavía la profesión de matemático como tal. El significado de la palabra matemática era relativo y había distintas corrientes filosóficas al respecto. Quizás solo en el momento de la muerte de Fermat en 1665, uno puede comenzar a encontrar elementos de una profesión matemática emergente.

Aunque en parte de forma desordenada e informal, mantenía una comunicación frecuente y fluida con sus colegas, proceso mediante el que compartía sus resultados. Fue el primero en descubrir propiedades realmente profundas de los enteros. Fermat demostró el siguiente teorema sorprendente:

Todo número entero es suma de a lo sumo 3 números triangulares. También, es suma de a lo sumo 4 números cuadráticos, es suma de a lo sumo 5 números pentagonales, y así sucesivamente.

Fermat descubrió que todo número primo de la forma $4n+1$ es suma de dos cuadrados. También estudió los números de la forma $F_n = 2^{2^n} + 1$ con $n \in \mathbb{N}_0$, llamados *números de Fermat*. Para $n \leqslant 4$ la fórmula da un número primo, y él creía que esto siempre era así. Sin embargo, en 1732 Euler halló que F_5 es compuesto. Estos números son de interés también en Geometría Plana. Gauss demostró que, si F_n es un primo, entonces se puede construir un polígono regular de F_n lados con regla y compás.

Poco tiempo después de Fermat, los nombres de Euler (1707-1783), Lagrange (1763-1813), Legendre (1752-1833), Gauss (1777-1855) y Dirichlet (1805-1859) resultaron prominentes en el posterior desarrollo de la teoría. El primer libro de Teoría de Números fue publicado por Legendre en 1798. Tres años más tarde Gauss publicó *Disquisitiones Arithmeticae* [14], un libro que transformaba la materia en una ciencia sistemática y bella. Sin embargo utilizaba gran cantidad de contribuciones de otras ramas de la Matemática, así como de otras ciencias. El mismo Gauss consideraba este libro sobre Teoría de Números su mejor obra.

Desde los tiempos de Gauss, ha existido un desarrollo intenso, vasto y profundo de la materia en muchas direcciones.

En el siglo XVIII suena el tema de la distribución de los números primos. Un examen detallado de una tabla de primos pone de manifiesto que se hallan distribuidos de forma muy irregular. Es fácil demostrar que entre números primos se pueden presentar eventualmente espacios arbitrariamente grandes. Por otro lado, se presentan reiterados primos consecutivos tales como 3 y 5, 5 y 7, o 11 y 13. Los pares de primos que, como éstos, difieren sólo en dos unidades se conocen como *primos gemelos*, y no se sabe si existen infinitos.

Una de las razones de la irregularidad en la distribución de primos es que no existe ninguna fórmula simple que produzca todos estos. Algunas fórmulas proporcionan muchos primos. Por ejemplo, la expresión

$$x^2 - x + 41$$

da un primo para $x = 0, 1, 2, \ldots, 40$. Sin embargo, en 1752 Goldbach probó que ningún polinomio en x con coeficientes enteros puede ser primo para todo x, incluso para x suficientemente grande. Goldbach también es popularmente conocido en la comunidad matemática por la conjetura que lleva su nombre; en una carta que envió a Euler en 1742, sugería que todo número par mayor a dos es suma de dos números primos. Aunque se han efectuado progresos, esta conjetura aún está sin decidirse.

Algunos polinomios representan infinidad de primos. Por ejemplo, cuando x, recorre los enteros, el polinomio lineal

$$2x + 1$$

da todos los números impares. En un trabajo famoso [11] publicado en 1837, Dirichlet demostró que, si d y a son enteros positivos carentes de factores comunes, el polinomio

$$dx + a$$

da una infinidad de primos cuando x recorre todos los enteros positivos. Este resultado se conoce como *Teorema de Dirichlet sobre progresiones aritméticas*. Para demostrar el teorema, Dirichlet salió fuera del reino de los enteros e introdujo instrumentos de Análisis tales como los límites y la continuidad. Por este motivo puso los fundamentos de una nueva rama de la Matemática llamada *Teoría Analítica de Números*, en la cual se utilizan ideas y métodos del Análisis real y complejo para resolver problemas sobre enteros.

A pesar de la irregularidad de esta distribución, si se examinan grandes bloques de primos se encuentra que su distribución media parece bastante regular. Si bien no se terminan los números primos, se presentan cada vez más espaciados, en media, a medida que se avanza en la tabla. La cuestión del enrarecimiento en la distribución fue motivo de muchas especulaciones en el siglo XIX. Para estudiar esta distribución, consideramos una función, designada por $\pi(x)$, que cuenta el número de primos $\leqslant x$. A fines del siglo XVIII, Gauss y Legendre conjeturaron independientemente que

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

los que significa que el cociente de ambas funciones tiende a 1 cuando $x \to \infty$. Pero aunque el problema atrajo la atención de distintos matemáticos eminentes, las herramientas analíticas necesarias para demostrar este resultado, conocido como *Teorema de los Números Primos*, se hicieron esperar casi un siglo. En la década de 1850, Chebyshev y Riemann hicieron aportes al problema. La demostración completa llegó en 1896 y de forma independiente por J. Hadamard y C. J. de la Vallée Poussin, concretando uno de los éxitos mas completos de la Teoría analítica de números.

En lo que sigue de este escrito, nos dedicamos en específico al tema que nos ocupa, que está bajo el paradigma de entender la distribución de los números primos.

1.2. Historia del Teorema de Dirichlet

Comenzamos nuestra historia con Leonhard Euler (Suiza, 1707 - Rusia, 1783). Desde el siglo XVII, el problema de calcular la serie

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

para N un natural mayor a 1, atrajo la atención de varios matemáticos. El caso especial correspondiente a $N = 2$ se conoce como *Problema de Basilea*, debido a la ciudad de origen

de la familia Bernoulli que, por cierto, tenia relación con la de Euler. En el siglo XVIII matemáticos como Jacob Bernoulli, Daniel Bernoulli y Christian Goldbach, obtuvieron algunos resultados preliminares sobre la suma de la serie en este caso. Finalmente, en 1735, Euler trata considerando funciones trigonométricas en serie de potencias y anuncia un resultado sorprendente:

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

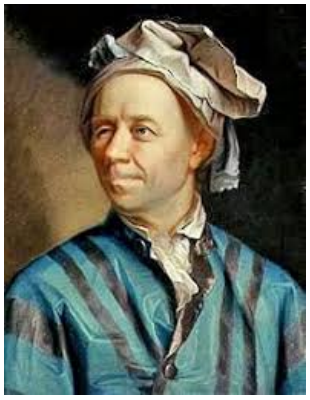

Figura 2: Euler.

Poco después, Euler estudia la serie para los N pares. En relación a estas series encontramos en [6, p. 172-176] uno de sus aportes a la Teoría de Números, el *producto de Euler*, un resultado de 1737 que relaciona los números primos con el conjunto de todos los números naturales. Mas precisamente, se tiene el siguiente resultado que en el fondo guarda la información del *Teorema Fundamental de la Aritmética* y que relaciona el crecimiento de los números con una expresión que no hace referencia a los mismos:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ primo}} \sum_{n=0}^{\infty} \frac{1}{p^s} = \prod_{p \text{ primo}} \frac{1}{1-p^{-s}} \qquad \forall\, s > 1$$

Primero lo piensa informalmente, para $s = 1$, y luego extiende la expresión a los s naturales, pero la misma prueba es válida para todo $s > 1$ real (y en realidad, es válida para todo complejo con parte real mayor a 1). De aquí, también deduce una prueba alternativa del *Teorema de Euclides*, pues al ser la serie de la izquierda divergente cuando $s = 1$, debe haber infinitos primos. Usando el resultado anterior, junto con métodos analíticos elementales, al final de [6, p. 187-188] Euler ve que

$$\sum_{p \text{ primo}} \frac{1}{p} = \infty$$

lo que quizás sea el primer resultado sobre la frecuencia de los primos, y nos permite decir, por ejemplo, que los números primos son mas frecuentes que los cuadrados. Estos hechos constituyen la semilla de la *Teoría Analítica de Números*, que se establecerá definitivamente con el Teorema de Dirichlet, exactamente un siglo después, en 1837. Euler también entendía la velocidad en que divergía esta serie, diciendo informalmente que su valor era $\ln(\ln \infty)$. Si traducimos sus palabras al lenguaje moderno y formal, sería

$$\sum_{p \leqslant x \text{ primo}} \frac{1}{p} \sim \ln(\ln x)$$

pero como otras pruebas suyas, era débil en cuanto a rigurosidad, y a menudo experimenta con sus ideas, además de visitar recurrentemente los temas sin completarlos. En 1874 Franz Mertens (quien se interese puede ver [9, § 3.2]) probaría que la aserción de Euler se cumplía incluso en un sentido mucho mas fuerte. Desde el punto de vista didáctico y relacionado con la última parte del prefacio de esta monografía, un aspecto positivo sobre la forma en que Euler escribía matemática, es que es mas fácil de entender su manera de pensar, sus intentos y descuidos hacen mas transparentes sus ideas, mientras que otros matemáticos fieles a los modos actuales, como Gauss, están dotados de un

claro, completo y satisfactorio rigor pero se muestran impenetrables al mostrar solo su producto final, sin manifestar diferentes estados. Esta forma de proceder, que limitaba la rigurosidad, también debe ser una de la razones de su abundante obra. En contraposición a esta filosofía, se cuenta que cuando cuestionaron a Gauss por sus formas, él respondió *"Un buen arquitecto no muestra sus andámios"*.

En el mismo artículo, Euler también estudia otras series similares, cita unos cálculos de Gottfried Wilhelm Leibniz debido a la serie $\sum \frac{(-1)^n}{2n+1}$, y construyó variantes de los argumentos anteriores que nos dejan a las puertas de tratar al problema de los primos en las progresiones aritméticas $4k+1$ y $4k+3$.

Tiempo después, en 1775, Euler conjetura que toda progresión aritmética de la forma $\mu k + 1$ contiene infinitos primos. Quizás debido a sus trabajos estaba mas familiarizado con este caso.

Figura 3: Legendre.

Podríamos decir que la conjetura sobre los primos en progresiones aritméticas tiene su origen en 1798 en los trabajos de Adrien-Marie Legendre (Francia, 1752 - Francia, 1833). De hecho el propio Dirichlet [12, p. 1-2] afirma en las páginas introductorias a su trabajo, que Legendre [10] es el único matemático que conoce que ha intentado una justificación de tal hecho. Según las propias palabras de Dirichlet, este resultado cuenta con numerosas aplicaciones, y Legendre no solo debería haber estado interesado en investigarlo porque la dificultad del tema le atraía, sino también porque lo utilizó como lema en algunos trabajos anteriores.

Concretamente, Legendre quería probar un teorema notable la *Ley de reciprocidad cuadrática*, que de forma compacta se enuncia: *Si p y q son primos impares distintos, entonces*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

donde

$$\left(\frac{p_1}{p_2}\right)$$

es el *Símbolo de Legendre*, que vale 1 si p_1 es un cuadrado módulo p_2, o -1 en caso contrario. Al ver el exponente de (-1) es evidente que este resultado relaciona los Símbolos de Legendre con las congruencias de p y q módulo 4; esta es la forma en la que se lo presentó originalmente, y fue Legendre quien luego lo expresa en una única formula simétrica. La ley, establecida primeramente de forma complicada por Euler en el período 1744-1746, fue redescubierta en 1785 por Legendre, que dio una demostración parcial. Gauss, por su cuenta, la descubrió a la edad de dieciocho años y un año más tarde, en 1796, dio la primera demostración completa. Respecto al Teorema de Dirichlet, Legendre afirmó erróneamente haberlo demostrado para el caso k par.

En [10] observó que el teorema se seguiría del siguiente lema: Dados dos enteros primos entre sí A, C, y cualquier conjunto de κ primos impares $\theta, \lambda, \ldots, \omega$ que no dividan a A y denotando el z-ésimo primo impar por $\pi^{(z)}$, entonces entre $\pi^{(\kappa-1)}$ términos consecutivos de la progresión $A-C$, $2A-C$, $3A-C$, ... hay al menos uno no divisible por ninguno de los primos $\theta, \lambda, \ldots, \omega$. Aunque Legendre supuso que había demostrado este lema, resulta ser falso.

En [4, p. 415-417] se pueden encontrar abundantes referencias para quien lo desee.

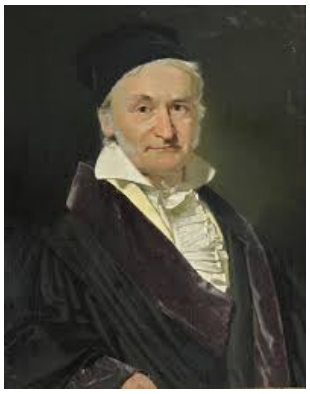

Figura 4: Gauss.

Todos sabemos que Johann Carl Friedrich Gauss (Alemania, 1777 - Alemania, 1855) ha poblado su nombre en toda disciplina matemática en la que ha incursionado, y el tema que nos ocupa no es la excepción. Sus aportes fueron indirectos, pero cruciales, de hecho el propio Dirichlet [12, § 7, p. 14] cita la notable obra *Disquisitiones arithmeticae* [14] que escribe en su juventud, en cuya sección III se encuentran los resultados profundos de la teoría de residuos que necesita Dirichlet. Por cierto, existe una traducción al castellano [15] del libro de Gauss, cuyo interés se eleva al considerar el contexto histórico que ofrece. Básicamente, en lenguaje moderno, Dirichlet usa que el grupo de unidades módulo k se puede factorizar como producto directo de grupos cíclicos correspondientes a la factorización prima de k, un resultado sorprendente que hasta el día de hoy no escatima en sutilezas. Para quien no entienda este lenguaje, cuando estudiemos exhaustivamente el artículo original de Dirichlet volveremos sobre esto en § 3.4. Revisando [15] y comparándolo con [12] podemos sacar nuestras propias conclusiones sobre la influencia de Gauss sobre Dirichlet en el manejo de distintos conceptos que además incluyen, por ejemplo, raíces de la unidad, residuos cuadráticos, suma de los elementos de grupos cíclicos, productos de raíces primitivas etc.

Otro aporte indirecto de Gauss tuvo lugar al estudiar los ya mencionados trabajos de Legendre. En [14, sect. 4] encontramos los trabajos de Gauss sobre la Ley de Reciprocidad Cuadrática. La teoría de formas cuadráticas, además de haber expuesto el enunciado del hoy Teorema de Dirichlet, constituye la parte más sustancial y técnica de la prueba original de Dirichlet [12, § 4] (aunque como veremos en § 4, después se logró sortear este tema). Volveremos sobre esto en § 3.3.

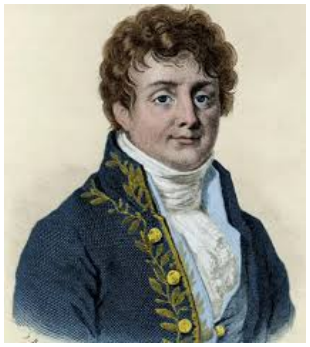

Figura 5: Fourier.

Jean-Baptiste Joseph Fourier (1768-1830), también francés, publica en 1807 sus resultados iniciales sobre las series que llevan su nombre, basado en descomposición de funciones periódicas en términos de funciones trigonométricas, con el objetivo de resolver la *Ecuación del Calor*. Increíblemente, su aporte iría mas allá de sus objetivos, llegando remotamente a la Teoría de Números, lo que nos muestras cómo a veces se pueden tocar disciplinas aparentemente distantes. La conexión aquí es la periodicidad de las funciones. Dirichlet, años antes de atacar el problema de las progresiones aritméticas, logra resultados relevantes dentro de la teoría de Fourier, y al meterse luego en el problema de las progresiones, considera funciones aritméticas periódicas módulo k que hoy conocemos como *Carácteres de Dirichlet*, y naturalmente aparecen otras funciones periódicas como la exponencial compleja y funciones trigonométricas. Si bien la influencia de Fourier en la prueba de Dirichlet puede ser debatible e directa, parece evidente su manejo natural de conceptos claves relacionados; de hecho posteriormente se desarrolló una teoría de *Análisis de Fourier en Grupos* con la cual se pueden estudiar los objetos definidos por Dirichlet [17]. Si buscamos "Dirichlet" en Wikipedia encontramos una cita ideal de Jacobi, cuya autenticidad no pude verificar en las recopilaciones de las cartas de Humboldt, pero nos da una idea del consenso que hay en esta influencia.

"... Dirichlet creó una parte nueva en las matemáticas, la aplicación de las series infinitas que Fourier ha introducido en la teoría del calor en la exploración de las propiedades de los números primos. Él ha descubierto una variedad de teoremas que ... son los pilares de las nuevas teorías".

C. G. J. Jacobi, 21 de diciembre de 1846, en una carta a Alexander von Humboldt

Figura 6: Dirichlet.

Recién ahora llega el momento de presentar a quien paradójicamente ya conocemos bien, el sucesor de Gauss en Gotinga. Johann Peter Gustav Lejeune Dirichlet (Alemania, 1805 - Alemania, 1859) desarrolló desde temprana edad una profunda pasión por las matemáticas. Con 16 años, decidió viajar a París para realizar sus estudios universitarios, debido al nivel insuficiente de las universidades alemanas de la época, lo que le permitió estar en contacto con grandes matemáticos como Fourier, Laplace, Poisson o Legendre. Ya durante este periodo, mostró interés por la Teoría de Números, y en particular, una ferviente admiración por el Disquitisiones Arithmeticae [14] de Gauss. De hecho, su primera publicación (1825) fue el estudio de un caso particular del Último Teorema de Fermat, lo que le reportaría fama instantánea. A finales de ese mismo año, se vio obligado a volver a Alemania, donde se le exigía una habilitación para enseñar en la universidad. Sin embargo, Dirichlet no podía optar a realizar una tesis de habilitación pues ni poseía un doctorado, ni era capaz de hablar latín, requisito de la época. Afortunadamente, le fue concedido un doctorado honorífico en la Universidad de Colonia, y se le permitió hacer su tesis de habilitación en la Universidad de Breslau. Más tarde, en 1828, publicaría su trabajo sobre Series de Fourier, y conseguiría trasladarse a Berlín, donde contrajo matrimonio con Rebeca Mendelssohn, hermana del compositor, y realizaría importantes aportaciones a las matemáticas en la definición el concepto moderno de FUNCIÓN, y posteriormente la demostración de la infinitud de números primos en progresiones aritméticas [17, p. 47].

Al encarar el teorema que lleva su nombre, afirma [12, p. 1] primero haber intentado el método propuesto por Legendre. Sin embargo, al no concretar resultados, abandona ese camino para tomar el propio, que lo llevará a probar de forma "euleriana" y nutriéndose de los tópicos ya mencionados, que la serie $\sum \frac{1}{p}$ sobre los inversos de los primos en una progresión aritmética fija, diverge. En su prueba, Dirichlet evitó siempre que pudo las variables complejas, tan solo tomó raíces de la unidad y logaritmo complejo de expresiones simples.

Años después de probar el teorema, Dirichlet publica sus investigaciones sobre números complejos [11, *Werke* 1:509-532].

Posteriormente, Mertens y otros pudieron simplificar la prueba. Concretamente, Mertens evita usar el Teorema de Reciprocidad, y el número de clases de formas cuadráticas binarias primitivas. También se desarrollaron pruebas que intentan evitar ciertos temas como el Análisis Complejo, pero son muy intrincadas. También hay pruebas más rápidas (para esto, [19] cita a [20]), pero no muy esclarecedoras. Hay algunas un poco mas algebraicas, como las de Selberg y Zassenhaus. Sin embargo, no se conoce una demostración esencialmente distinta a la original, y a pesar de estas discrepancias, a la comunidad no le parece descabellado que estas pruebas compartan la misma esencia y estructura

subyacente.

La prueba que daremos en § 4 es de las más populares. Es una modificación de la prueba original mediante el uso de la teoría caracteres y Análisis Complejo posteriormente desarrolladas, que cuenta a Landau como posible primer contribuyente de esta adaptación [19, p. 9].

El artículo [13] ya mencionado, será de interés para quien quiera extender este apartado histórico debido a la prueba de Dirichlet y el después.

1.3. La Teoría Analítica de Números

Definición 1.1. *La Función Zeta* $\zeta : (1, \infty) \to \mathbb{R}$ *se define por*

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

Para quien cursó Análisis Complejo, en una memoria de 1859 Riemann da una extensión meromorfa de ζ primero a $\{\operatorname{Re} s > 0\}$ y luego a todo $\mathbb{C}$ por medio de una ecuación funcional. Esta tiene exactamente un polo de orden 1 precisamente en $s = 1$ con residuo 1 [21, p. 13]. Luego conjetura su famosa *Hipótesis de Riemann* sobre los ceros de (la extensión de) ζ. Este es uno de los *Problemas del Milenio*, para el cual ya hay suficiente divulgación y nos evitamos la explicación técnica.

En este contexto también encontramos al *Teorema de los números primos*, conjeturado por Gauss (y Legendre) en su adolescencia, y afirma

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

Es decir, las funciones $\pi(x)$ y $\frac{x}{\ln x}$ son asintóticas (el cociente entre ellas tiende a 1 en el infinito). Riemann también dio unas directrices para demostrar este teorema, si bien los detalles de su argumento no fueron precisados hasta 1896, cuando aparecieron dos pruebas independientes, una de Jacques Hadamard y otra de Charles Jean de la Vallée-Poussin. Posteriormente se encontraron varias pruebas algo más simples, aunque todas ellas bastante sofisticadas. Selberg y Erdős dieron en 1949 una prueba elemental, en el sentido de que no requería resultados de la teoría de funciones de variable compleja, o análisis funcional en general [5, p. xiii], pero es demasiado intrincada [21, p. 20]. La prueba original, siguiendo las ideas de Riemann se basaban en una estrecha conexión que existe entre la función ζ y la distribución de los números primos [5, p. xvi].

Similar al Teorema de Dirichlet, el enunciado del Teorema del Número Primo se traduce a afirmaciones equivalentes y resulta como corolario de que $\zeta(s) \neq 0$ en la recta $\{\operatorname{Re} s = 1\}$ [21, p. 20].

1.4. Dos cerezas en el postre

Con el Teorema de Dirichlet probado y con una Teoría de Números afianzada y en auge, esta historia aún no termina. En § 1.4.1 le daremos un bello cierre a la versión analítica del problema. En § 1.4.2 veremos la historia paralela y autocontenida de las pruebas puramente algebraicas y qué límites teóricos presentan los procedimientos intentados.

1.4.1. Teoremas de densidad

La generalización del Teorema del Número Primo a progresiones aritméticas es llamado el *Teorema del Número Primo para Progresiones Aritméticas*, y se interesa en indicar cómo crece la cantidad de primos congruentes a un cierto a m módulo k (con m y k coprimos), sabiendo que hay infinitos (por el Teorema de Dirichlet) [21, p. 20]. Si llamamos $\pi_{m,k}$ a la cantidad de primos $\leqslant x$ en tal progresión aritmética, entonces

$$\lim_{x\to\infty} \frac{\pi_{m,k}(x)}{x/\ln x} = \frac{1}{\varphi(k)}$$

lo que equivalentemente se puede escribir

$$\pi_{m,k} \sim \frac{1}{\varphi(k)} \frac{x}{\ln x} \sim \frac{\pi}{\varphi(k)}$$

Esto se traduce a que, fijado k, en cada progresión aritmética (variando m) hay la "misma" cantidad de primos, es decir, hay $\frac{1}{\varphi(k)}$ del total [21, p. 21]. Para demostrar esto, Ch. de la Vallee-Poussin obtuvo sin cálculos, mediante el uso de la teoría de funciones de variable compleja, una prueba del punto difícil de la prueba de Dirichlet; probó que la suma de los logaritmos de los primos $\leqslant x$ en la progresión aritmética es asintótica a $\frac{x}{\varphi(k)}$ [4, 416].

Para no excedernos de los límites físicos de una monografía, no nos extendemos sobre esto más allá de la breve explicación. En los libros referenciados se puede encontrar material.

Para quien esté interesado en una abstracción de esta "densidad" al contexto de la *Teoría Algebraica de Números*, puede investigar sobre el *Teorema de Densidad de Chebotarev*, un resultado de 1922 publicado pocos años después, que le pone un broche realmente espectacular al tema.

1.4.2. Demostraciones euclidianas

Después de la demostración de Dirichlet, comenzaron a aparecer pruebas puramente algebraicas para algunos casos particulares. La idea clave es suponer que existen finitos primos en la progresión para luego tomar el producto de ellos y con él conseguir fabricar un número que forzosamente debe ser divisible por un nuevo primo de la progresión. Estas ideas tienen como punto de partida la prueba de Euclides sobre la infinitud de los números primos, los cuales trivialmente se corresponden con las progresiones aritmética $\mu + 1$ y $2\mu + 1$.

En 1843 V. A. Lebesgue prueba el caso $m = 1$, $k = 2p$ con p primo, quien mostró el hecho de que $x^{p-1} - x^{p-2}y + \ldots + y^{p-1}$ tiene además del posible factor p, solo factores primos de la forma $2\mu p + 1$. utilizando un método bastante similar, en 1853 F. Landry consideró divisores primos de $\frac{n^p+1}{n+1}$ para tratar las mismas progresiones. Por otro método bastante similar, se puede obtener el mismo resultado utilizando el hecho de que para cualquier primo p, cada divisor primo q de $\frac{n^p-1}{n-1}$ coprimo con p satisface $q \equiv 1 \pmod{p}$. El método análogo también es aplicado por Lebesgue en 1862 para la progresión $k = 2p$, $m = -1$. Usando las partes racionales e irracionales de $(a+\sqrt{b})^n$, en 1868/9 A. Genocchi vuelve a dar una demostración para estas dos progresiones. Además, en las lecciones de 1875/6 L. Kronecker dio otra prueba para el caso $k = 2p$, $m = 1$. Recientemente, en un trabajo de Romeo Meštrović se da una prueba simple del mismo resultado basada en

la función totiente de Euler y el pequeño teorema de Fermat. Tambien se desarrollaron adaptaciones de estas ideas para tratar potencias el caso en donde k es potencia de un primo y $m = 1$.

En 1886 A.S. Bang, y Sylvester en 1888 obtuvieron pruebas para el caso $m = 1$ y $k \geqslant 2$ arbitrarios. Ambas pruebas se basan en el hecho de que si p es un primo que no divide a k, entonces p divide a la evaluación del polinomio ciclotómico $\Phi_k(a)$ si y solo si el orden de a módulo p (es decir, el mínimo exponente n tal que $a^n \equiv 1 \pmod{p}$) es k. Este caso lo veremos con detalle en § 5.2.

Utilizando las propiedades de divisibilidad de los polinomios ciclotómicos, en 1888 J.J. Sylvester probó el caso $k = p^n$, $m = -1$. En 1896 R.D. von Sterneck trabaja esta caso utilizando produtos que involucran a la función de Möbius. En 1913 por R.D. Carmichael obtiene el mismo resultado para otros casos.

En 1911, H. C. Pocklington demuestra que para cualquier $k > 2$ fijo, hay infinitos primos que no son congruentes a 1 módulo k.

Como observó K. Conrad [26], una prueba euclidiana del teorema de Dirichlet para $m(moda)$ implica, como mínimo, la construcción de un polinomio no constante $h \in \mathbb{Z}[X]$ para el cual cualquier factor primo p de cualquier entero $h(n)$ satisface, con un número finito de excepciones, $p \equiv 1 \pmod{k}$ o $p \equiv m \pmod{k}$, y existen un número infinito de primos del último tipo. En 1912/13, Schur [23] demostro que si $m^2 \equiv 1 (\text{mod } k)$ entonces existe una prueba euclidiana para la progresión aritmética $\mu k + m$. En particular, Schur extendió el enfoque de Serret basado en la Ley de Reciprocidad Cuadrática para establecer pruebas de ciertos casos. Recién en 1988, cuando ya ha pasado demasiada agua debajo del puente, Murty [24] da una respuesta definitiva y precisa a nuestra inquietud, probando la recíproca del Teorema de Schur usando *Teoría de Galois*.

Sabemos entonces, por ejemplo, que no existe prueba para la progresión $5\mu + 2$ que imite la idea de Euclides, y que en cambio toda progresión con $24\mu + m$ con m arbitrario sí la tiene.

El Teorema de Murty le da un espectacular cierre a esa historia. Tenemos la demostración de Dirichlet, y un teorema que nos induce a pensar que era inevitable recurrir al reino del análisis. Sin embargo, como no podía ser de otra manera, en [25] también buscan generalizar estos resultados a otros contextos mas abstractos, dándole continuidad al tema.

2. Variae Observationes Circa Series Infinitas

Aquí tratamos de encontrar un equilibrio entre la notación de Euler [6] y la moderna así como la rigurosidad empleada en las pruebas, con el objetivo de representar el lenguaje de Euler pero sin estorbarnos. Cualquiera puede consultar a Euler para más detalles.

2.1. Producto de Euler

El resultado [6, Theorema 8] de 1737 se generaliza y formaliza fácilmente:

Proposición 2.1 (Producto de Euler)**.** $\forall\ s > 1$,

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ primo}} \frac{p^s}{p^s - 1}$$

Demostración. Siguiendo a Euler denotamos $x = \sum_{n=1}^{\infty} \frac{1}{n^s}$ y continuamos

$$\frac{1}{2^s} x = \sum_{n=1}^{\infty} \frac{1}{(2n)^s} = \sum_{2|n} \frac{1}{n^s}$$

$$\frac{2^s - 1}{2^s} x = \left(1 - \frac{1}{2^s}\right) x = \sum_{2\nmid n} \frac{1}{n^s}$$

$$\frac{3^s - 1}{3^s} \frac{2^s - 1}{2^s} x = \sum_{2\nmid n,\, 3\nmid n} \frac{1}{n^s}$$

En general, sean $N \in \mathbb{N}$, $P_N = \{\text{primos} \leqslant N\}$ y $\mathbf{N}_N = \{n \in \mathbb{N} \mid p \nmid n \ \forall p \in P_N\}$, entonces

$$x \prod_{p \in P_N} \frac{p^s - 1}{p^s} = \sum_{n \in \mathbf{N}_N} \frac{1}{n^s}$$

$$\lim_{N\to\infty} x \prod_{p \in P_N} \frac{p^s - 1}{p^s} = \lim_{N\to\infty} \sum_{n \in \mathbf{N}_N} \frac{1}{n^s}$$

$$x \lim_{N\to\infty} \prod_{p \in P_N} \frac{p^s - 1}{p^s} = \frac{1}{1^s}$$

$$x \prod_{p \text{ primo}} \frac{p^s - 1}{p^s} = 1$$

Luego,

$$x = \left(\prod_{p \text{ primo}} \frac{p^s - 1}{p^s} \right)^{-1} = \prod_{p \text{ primo}} \left(\frac{p^s - 1}{p^s} \right)^{-1} = \prod_{p \text{ primo}} \frac{p^s}{p^s - 1}$$

□

De Aquí, Euler también observa que de

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

se deduce que hay infinitos primos, pues la productoria no puede tener finitos términos. Esta aparentemente innecesaria observación, en realidad da la forma de encarar problemas que a simple vista parecen intratables.

En [6, Theo. 11] Euler cita de la siguiente forma un resultado que se debe a Leibniz:

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \frac{1}{13} \text{ etc.}$$

y con métodos similares a los anteriores, observa que

$$\frac{\text{etc.} \ \ 24 \cdot 20 \cdot 16 \cdot 12 \cdot 12 \cdot 8 \cdot 4 \cdot 4}{\text{etc.} \ \ 23 \cdot 19 \cdot 17 \cdot 13 \cdot 11 \cdot 7 \cdot 5 \cdot 3} \frac{\pi}{4} = 1$$

$$\frac{\pi}{4} = \frac{3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \ \text{etc.}}{4 \cdot 4 \cdot 8 \cdot 12 \cdot 12 \cdot 16 \cdot 20 \cdot 24 \ \text{etc.}}$$

aclarando en latín que los numeradores en esta última expresión son los números primos y los denominadores vienen de restar o sumarle 1 (lo cual dependerá de la congruencia módulo 4) a los correspondientes primos.

Dicho de otra forma, Euler cita el siguiente resultado:

$$\frac{\pi}{4} = \sum_{n>0 \text{ impar}} \frac{\pm 1}{n}$$

donde el numerador es tal que $n \equiv \pm 1 \pmod 4$. Así, si por ejemplo $n = 15 \equiv -1 \pmod 4$, entonces $4 \mid n+1$, y por lo tanto el término correspondiente en la serie es $\frac{-1}{n} = \frac{-1}{15}$. Análogamente, si $n = 5 \equiv 1 \pmod 4$, el término correspondiente es $\frac{1}{n} = \frac{1}{5}$.

La anterior, se denomina *serie de Gregory-Leibniz*, reconociendo también James Gregory, contemporáneo de Leibniz.

Proposición 2.2.

$$\frac{\pi}{4} = \prod_{p \text{ primo impar}} \frac{p}{p \mp 1}$$

donde $4 \mid p \mp 1$.

Nota: ∓ 1 *significa* $-(\pm 1)$. *Por ejemplo para* $p = 3$, *se tiene* $p \equiv -1 \pmod 4$, *y por ende el factor correspondiente en la productoria es* $\frac{1}{p+1} = \frac{1}{4}$. *Para* $p = 5 \equiv 1 \pmod 4$, *se tiene* $\frac{1}{p-1} = \frac{1}{4}$.

Demostración.

$$\frac{1}{3}\frac{\pi}{4} = \frac{1}{3}\sum_{n>0 \text{ impar}} \frac{\mp 1}{n} = \frac{1}{3} - \frac{1}{9} + \frac{1}{15} - \frac{1}{21} + \ldots = -\sum_{\substack{3 \mid n \\ n \text{ impar}}} \frac{\mp 1}{n}$$

Una forma de pensar esto, es que multiplicar por 3 "invierte" la congruencia módulo 4 porque $3 \equiv -1 \pmod 4$. Es decir, si $4 \mid n \pm 1$, entonces $4 \mid 3n \mp 1$. Luego,

$$\frac{4}{3}\frac{\pi}{4} = \left(1 + \frac{1}{3}\right)\frac{\pi}{4} = \sum_{n \text{ impar}} \frac{\mp 1}{n} - \sum_{3 \mid n} \frac{\mp 1}{n} = \sum_{\substack{3 \nmid n \\ n \text{ impar}}} \frac{\mp 1}{n}$$

Como $5 \equiv 1 \pmod 4$, multiplicar por 5 no cambia la congruencia módulo 4, así que

$$\frac{1}{5}\frac{4}{3}\frac{\pi}{4} = \sum_{\substack{3 \nmid n \\ n \text{ impar}}} \frac{\mp 1}{5n} = \sum_{\substack{5 \mid n,\ 3 \nmid n \\ n \text{ impar}}} \frac{\mp 1}{n}$$

$$\frac{4}{5}\frac{4}{3}\frac{\pi}{4} = \left(1 - \frac{1}{5}\right)\frac{4}{3}\frac{\pi}{4} = \sum_{\substack{5 \nmid n,\ 3 \nmid n \\ n \text{ impar}}} \frac{\mp 1}{n}$$

En gral., si $N \in \mathbb{N}$, $P_N = \{\text{primos impares} \leqslant N\}$ y $\mathbf{N}_N = \{n \text{ impar} \mid p \nmid n \ \forall p \in P_N\}$, entonces

$$\frac{\pi}{4}\prod_{p \in P_N} \frac{p \pm 1}{p} = \sum_{n \in \mathbf{N}_N} \frac{\mp 1}{n}$$

$$\frac{\pi}{4}\lim_{N\to\infty} \prod_{p \in P_N} \frac{p \pm 1}{p} = \lim_{N\to\infty} \sum_{n \in \mathbf{N}_N} \frac{\mp 1}{n}$$

$$\frac{\pi}{4}\prod_{p \text{ primo impar}} \frac{p \pm 1}{p} = 1$$

Luego,

$$\frac{\pi}{4} = \left(\prod_{p \text{ primo impar}} \frac{p \pm 1}{p} \right)^{-1} = \prod_{p \text{ primo impar}} \left(\frac{p \pm 1}{p} \right)^{-1} = \prod_{p \text{ primo impar}} \frac{p}{p \pm 1}$$

□

Luego, Euler continua dando resultados del estilo conectados con series intrínsecamente relacionadas con la congruencia módulo 4. Sin embargo, no dice encontré que diga explícitamente que hay infinitos primos con cierta congruencia módulo 4, posiblemente porque el problema de las progresiones aritméticas no se había planteado, y porque sus objetivos eran otros, como calcular series y obtener relaciones con otras expresiones, como productorias. Aparentemente, hasta aquí los vínculos con el teorema de Dirichlet pasaron desapercibidos. Por otro lado, quizás el lenguaje de la época de Euler no era propicio para enfatizar y explicitar patrones en las fórmulas, y esto no le permitió generalizar su fórmula del producto a funciones más generales, llamados *caracteres de Dirichlet*, que veremos en § 4.1.

2.2. Serie de inversos de los primos

En el último resultado [6, Theo. 19] de su artículo, haciendo uso de su fórmula del producto, da la primer prueba de que la suma de los inversos de los primos diverge. Para no extendernos mas de lo necesario con el lenguaje de Euler que ya hemos comprendido bien, usemos su idea pero adaptada a nuestro lenguaje moderno y riguroso, y de paso lo contrastamos.

Corolario 2.3.

$$\sum_{p \text{ primo}} \frac{1}{p} = \infty$$

Demostración. El producto de Euler nos da una relación que involucra todos los primos, y en el enunciado de este corolario aparece una sumatoria. Por lo tanto, tiene sentido aplicar el logaritmo, ya que transforma productos en sumas. Como ln es continua, podemos tranformar la productoria en una sumatoria, puesto que estos se definen como límites.

$$\ln \zeta(s) \;=\; \ln \prod_{p \text{ primo}} \frac{1}{1 - p^{-s}} \;=\; \sum_{p \text{ primo}} \ln \frac{1}{1 - p^{-s}}$$

Usando la serie de Taylor $\ln\left(\frac{1}{1-x}\right) = \sum_{n \in \mathbb{N}} \frac{x^n}{n} = x + R(x)$, donde

$$|R(x)| = \left| x^2 \sum_{n=0}^{\infty} \frac{x^n}{n+2} \right| \leqslant x^2 \qquad \forall\ |x| \leqslant \frac{1}{2}$$

tenemos

$$\ln \zeta(s) = \sum_{p \text{ primo}} \left(p^{-s} + R(p^{-s}) \right) \leqslant \sum_{p \text{ primo}} \frac{1}{p^s} + \sum_{p \text{ primo}} \frac{1}{p^{2s}} \leqslant \sum_{p \text{ primo}} \frac{1}{p^s} + \zeta(2)$$

Como $\ln \zeta(s)$ diverge cuando $s \to 1^+$, $\sum \frac{1}{p^s}$ tambien. □

3. La idea y el lenguaje de Dirichlet

Comenzamos fijando lo necesario del lenguaje que necesitamos para hablar con fluidez de algunos razonamientos. Mediante apreciaciones personales, en § 3.2 intento introducir la idea de la prueba exponiendo la conexión natural con el artículo de Euler [6]. También trato de naturalizar el punto de partida de la prueba de Dirichlet, procurando dar versiones aproximadas de los razonamientos que pudo tener Dirichlet antes de dar el primer paso concreto y acertado en su demostración. Esta subsección primero la escribí antes de leer la prueba de Dirichlet, de hecho aún creía que me sería imposible encontrar la versión original, así puedo pensar que la motivación es realmente "natural".

En § 3.3 comenzamos a analizar exhaustivamente la prueba original de Dirichlet [12], que arranca con el caso particular en donde k es un primo impar.

Para no ensuciarnos excesívamente con la notación densa, no vamos a entrar en los detalles finos de los cálculos que realizó Dirichlet para llegar a cada resultado que expongamos. De todos modos, muchos resultados sí que los completaremos, y en general quedará claro el procedimiento. Tampoco vamos a explicar de donde salen ciertas fórmulas o funciones que Dirichlet ya asume y las usa, como la *Función Gamma*. De todos modos, la prueba moderna que veremos de forma completa es lo suficientemente fiel a la original, por lo que allí se guarda la esencia de dichos cálculos.

En esencia, la idea se encuentra en el caso k primo impar, y la notación en el caso general se torna mas abrumadora, así que en § 3.4 solo nos dedicaremos a dar las principales expresiones generalizadas que dio Dirichlet para su propósito. Si bien seguiremos mostrando las expresiones idénticamente a como lo hizo Dirichlet, algunas explicaciones ahora las daremos con nuestro lenguaje moderno, ya que éstas son mas técnicas y además quedó clara la forma en que él redactaba. En esta parte, además de seguir consultando al propio Dirichlet [12], el artículo [13] fue de utilidad.

3.1. Preliminares: definiciones de cosas de grupos

Definición 3.1 (Grupo)**.** *Un grupo es un conjunto $G \neq \emptyset$ con una operación binaria (producto)*

$$\bullet : G \times G \to G$$

que es asociativa, cuenta con un elemento neutro e (es decir $eg = ge = g$ para todo $g \in G$), y todo elemento tiene inverso (para todo g, existe un g^{-1} tal que $gg^{-1} = g^{-1}g = e$).

El conjunto de clases módulo k es un grupo. Es decir, multiplicar dos números coprimos con k vuelve a dar un número coprimo, y su residuo módulo k se obtiene multiplicando los respectivos residuos. Además, todo numero coprimo se puede multiplicar por otro de forma que obtengamos uno congruente a 1 módulo k. A este grupo lo denotamos C_k^*. El supraíndice $*$ simboliza que estamos tomando el *grupo de unidades* del Anillo C_k, que es el que en las primeras clases de Álgebra solemos denotar $\mathbb{Z}_k$. Si bien existe esta típica notación $\mathbb{Z}_k$ o la otra $\mathbb{Z}/k\mathbb{Z}$, la segunda me parece fea y la primera en *Teoría Algebraica de Números* se usa para denotar a los llamados *números p-ádicos* por lo que me acostumbré a discriminarla.

Otro grupo que usaremos es $\mathbb{G}_n$, que es el subconjunto de $\mathbb{C}$ compuesto por todas las n-ésimas raíces de la unidad, y que usa el producto en $\mathbb{C}$ como operación binaria. Se denota $\mathbb{G}_\infty = \cup_{n=1}^{\infty} \mathbb{G}_n$.

La noción de *isomorfismo* de grupos también la usaremos. Dados dos grupos G y H, un isomorfismo $f : G \to H$ es una biyección que preserva la operación, es decir

$f(g_1 g_2) = f(g_1)f(g_2)$ para todo par $g_1, g_2 \in G$. Si no pedimos la condición de biyección, tenemos la definición de *homomorfismo* de grupos. Cuando dos grupos son isomorfos, son "esencialmente iguales", y toda propiedad que tenga uno se la heredará al otro.

El producto cartesiano $G \times H$ de dos grupos es un un grupo con la operación coordenada a coordenada.

Para más detalles, quien quiera puede consultar [28].

3.2. Motivación

Ya hemos mencionado que [6] da relaciones interesantes vinculadas a la congruencia módulo 4. De las proposiciones 2.1 y 2.2 podemos deducir que hay infinitos primos congruentes a -1 módulo 4. En efecto, si hubiera finitos, todos menores a un N, entonces todos los primos mayores o iguales a N son congruentes a 1 módulo 4, por ende escribimos informalmente

$$\frac{\pi}{4} = \prod_{p \text{ primo}} \frac{p}{p \mp 1} = \prod_{\substack{p \text{ primo} \\ p < N}} \frac{p}{p \mp 1} \underbrace{\prod_{\substack{p \text{ primo} \\ p \geqslant N}} \frac{p}{p-1}}_{\infty, \text{ por Prop 2.1}} = \infty$$

lo cual es absurdo.

Para escribir esto mas formal, podemos generalizar la Proposición 2.2 de la forma análoga a la Proposición 2.1:

$$L(s) := \sum_{n > 0 \text{ impar}} \frac{\pm 1}{n^s} = \prod_{p \text{ primo impar}} \frac{p^s}{p^s \mp 1}$$

donde $L(1)$ converge absolutamente por ser una serie alternada con término general tendiendo a cero, y $L(s)$ converge absolutamente para $s > 1$. Además, adaptando un poco la idea de nuestra prueba informal, podemos obtener una relación que nos permite continuar implementando el espíritu de Euler. Concretamente, tomamos

$$\lim_{s \to 1^+} \frac{\zeta(s)}{L(s)}$$

lo cual nos permite deshacernos de los primos $p \equiv 1 \pmod 4$. Veamos con detalle a que nos referimos, pero aprovecharemos para verlo para los primos congruentes a 1, que es el caso que nos falta. En este caso, en vez de $\frac{\zeta(s)}{L(s)}$ debemos tomar $\zeta(s)L(s)$ para deshacernos de los primos $p \equiv -1 \pmod 4$, de la siguiente manera:

$$\begin{aligned}
\zeta(s)L(s) &= \prod_{p \text{ primo}} \frac{p^s}{p^s - 1} \prod_{p \text{ primo impar}} \frac{p^s}{p^s \mp 1} \\
\zeta(s)L(s) &= \frac{2^s}{2^s - 1} \prod_{\substack{p \text{ primo} \\ p \equiv 1 \pmod 4}} \left(\frac{p^s}{p^s - 1}\right)^2 \prod_{\substack{p \text{ primo} \\ p \equiv -1 \pmod 4}} \left(\frac{p^s}{p^s - 1} \frac{p^s}{p^s + 1}\right) \\
\frac{2^s - 1}{2^s}\zeta(s)L(s) &= \prod_{\substack{p \text{ primo} \\ p \equiv 1 \pmod 4}} \left(\frac{p^s}{p^s - 1}\right)^2 \prod_{\substack{p \text{ primo} \\ p \equiv -1 \pmod 4}} \frac{p^{2s}}{p^{2s} - 1}
\end{aligned}$$

$$\frac{2^s-1}{2^s}\zeta(s)L(s) < \prod_{\substack{p \text{ primo} \\ p\equiv 1 \,(\mathrm{mod}\ 4)}} \left(\frac{p^s}{p^s-1}\right)^2 \underbrace{\prod_{p \text{ primo}} \frac{p^{2s}}{p^{2s}-1}}_{\zeta(2s)}$$

$$\frac{2^s-1}{2^s\,\zeta(2s)}\zeta(s)L(s) < \prod_{\substack{p \text{ primo} \\ p\equiv 1 \,(\mathrm{mod}\ 4)}} \left(\frac{p^s}{p^s-1}\right)^2$$

$$\infty = \frac{1}{2\,\zeta(2)}\,\frac{\pi}{4}\lim_{s\to 1^+}\zeta(s) \leqslant \lim_{s\to 1^+} \prod_{\substack{p \text{ primo} \\ p\equiv 1 \,(\mathrm{mod}\ 4)}} \left(\frac{p^s}{p^s-1}\right)^2$$

por lo tanto la productoria tiene infinitos términos. Una clave para tener ∞ del lado derecho fue que $L(1) \neq 0$. Veremos que probar esto en general es la parte más difícil de la prueba de Dirichlet. Él en realidad aplica logaritmo a ambos miembros y convierte los productos en sumas para luego buscar una combinación lineal adecuada, de esta forma la condición $L(1) \neq$ se traduce en que $\log L(1) \neq -\infty$.

La otra idea clave fue encontrar una expresión que "filtre" los primos de la forma $4\mu + 1$ de entre todos los demás primos [18, p. 2]. De esta tarea se encargan lo que hoy conocemos como carácteres de Dirichlet.

El trabajo de Dirichlet, y sus simplificaciones posteriores tratan de integrar la idea anterior en un conjunto de herramientas que sinteticen y tengan en cuenta los aporte de las distintas series vinculadas a congruencias arbitrarias. Para esto, parece natural ir en busca de nuevas series y generalizar las proposiciones 2.1 y 2.2. Observar que en estas, se consideran series

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

donde $\chi : \mathbb{N} \to \mathbb{Z}$. En el primer caso $\chi \equiv 1$ y en el otro $\chi(n) = \begin{cases} 1 & si \quad n \equiv 1 \,(\mathrm{mod}\ 4) \\ 0 & si \quad n \text{ es par} \\ -1 & si \quad n \equiv -1 \,(\mathrm{mod}\ 4) \end{cases}$

Si en el caso general queremos encontrar una relación entre $L(s,\chi)$ y un producto que involucre primos, análogo al de los dos casos anteriores, entonces el primer paso sería escribir

$$\frac{1}{2^s}L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{(2n)^s}$$

y multiplicarlo por algún k_2 que me devuelva la suma de los términos en los naturales pares. Mas concretamente, queremos que

$$\frac{k_2}{2^s}L(s,\chi) = \sum_{n=1}^{\infty} \frac{k_2\,\chi(n)}{(2n)^s} = \sum_{n=1}^{\infty} \frac{\chi(2n)}{(2n)^s}$$

es decir $k_2\,\chi(n) = \chi(2n)\ \forall\ n \in \mathbb{N}$. En particular, tomando $n = 1$ tenemos $k_2\,\chi(1) = \chi(2)$. Así, $\chi(2)\chi(n) = \chi(1)\chi(2n)\ \forall\ n \in \mathbb{N}$. Esto ya nos da una idea de que esperamos que χ sea multiplicativa, es decir que preserve el producto:

$$\chi(nr) = \chi(n)\chi(r) \quad \forall\ n, r \in \mathbb{N}$$

y en particular, $\chi(1) = 1$. De esta forma,

$$\left(1 - \frac{k_2}{2^s}\right) L(s,\chi) = \left(1 - \frac{\chi(2)}{2^s}\right) L(s,\chi) = \sum_{2\nmid n} \frac{\chi(n)}{n^s}$$

y continuando el procedimiento obtenemos

$$L(s,\chi) \prod_{p \text{ primo}} \left(1 - \frac{\chi(p)}{p^s}\right) = 1$$

$$L(s,\chi) = \prod_{p \text{ primo}} \frac{p^s}{p^s - \chi(p)}$$

Nota curiosa pero sin importancia: Se puede ver que con los χ mas generales posibles con la condición de que $\chi(p)\chi(n) = \chi(1)\chi(pn)$ para todo n tal que p es el menor primo que divide a n (esta condición sale al continuar con las iteraciones en la demostración del producto de Euler), están determinadas a partir de su valor en 1 (valor que debe ser distinto de cero si queremos evitar $\chi \equiv 0$) y en los números primos, y se llega a que

$$\chi(n) = \frac{1}{\chi(1)^{r-1}} \prod_{i=1}^{r} \chi(p_i)$$

donde p_i son los factores primos de n contando multiplicidad (es decir, pueden estar repetidos). Para esto, tenemos que ir dividiendo a n por sus factores primos de menor a mayor. La productoria que se logra es

$$L(s,\chi) = \chi(1) \prod_{p \text{ primo}} \frac{p^s}{p^s - \frac{\chi(p)}{\chi(1)}}$$

Por otro lado, cuando analizamos la progresiones módulo 4 nos fue muy útil el hecho de que ambas series implicadas ($\zeta(s)$ y la que denotamos $L(s)$) discriminen a los primos $p \equiv 1 \pmod 4$ de los $p \equiv -1 \pmod 4$. Observado esto, parece buena idea pedir que χ solo dependa de la congruencia módulo k si estamos mirando una progresión aritmética $\mu k + m$. Como en la productoria hay a lo sumo una cantidad finita de primos que no son coprimos con k (los primos que dividen a k), quizás no interesa el valor de χ en los números no coprimos con k, así que podemos asumir que allí vale cero. De esta manera, a χ la podemos pensar como una función multiplicativa $C_k^* \to \mathbb{Z}$ que se extiende a $\mathbb{N}$, y en realidad a todo $\mathbb{Z}$.

El hecho de que χ preserve el producto y que solo dependa de la congruencia módulo k implica que la imagen de χ es un subconjunto multiplicativo (cerrado por el producto) finito de $\mathbb{Z}$, y por ende está contenido en $\{-1, 0, 1\}$. Este es también el subconjunto multiplicativo finito mas grande de $\mathbb{R}$. En general, no hay suficientes funciones multiplicativas $\chi : C_k^* \to \{-1, 0, 1\}$, así que quizás nos falte información para cubrir todas las progresiones aritméticas. Por ejemplo, si $k = p \geqslant 5$ es primo, tenemos que analizar $\varphi(p) = p - 1 \geqslant 4$ progresiones aritméticas distintas, pero solo tenemos 2 posibles χ no nulas, ya que como C_p^* es cíclico, para determinar χ basta ver si manda al generador a 1 o -1. Esto nos obliga a considerar los complejos. Como la imagen debe ser un conjunto finito multiplicativo de $\mathbb{C}$, debe estar contenida en $S^1 \cup \{0\}$, donde $S^1 := \{z \in \mathbb{C} : |z| = 1\}$. Es decir $\chi : C_k^* \to S^1 \cup \{0\}$.

Dirichlet considera primero el caso $k = p$ primo, siendo muy sabido en el siglo XIX que C_p^* era cíclico y que es isomorfo a $\mathbb{G}_{p-1} \subset S^1$ (aunque nada de esto lo decían así, por supuesto), lo que por razones ya mencionadas lo hacía evidentemente el caso mas fácil.

3.3. Caso $k = p$ primo impar

Vamos a usar la separación en secciones como lo hizo Dirichlet, resumiendo cada una.

§ 1

Como mencionamos, considera primero el caso $k = p$ primo. Él toma un elemento primitivo módulo p, al cual denota c y dice que para cada n natural, existe un número γ_n tal que $c^{\gamma_n} \equiv n \,(\text{mod. } p)$.

Escribe simplemente ω^{γ_n}, donde ω es una raíz arbitraria de la ecuación $\omega^{p-1} - 1$, para referirse a la función $\chi(n)$, determinada a partir de $\chi(c) = \omega$. La notación de Dirichlet presupone que se ha fijado una elección del elemento primitivo c, aunque cualquiera funcionará igualmente bien.

Para un primo q distinto de p y s un real positivo mayor a 1, se tiene la serie geométrica

$$\frac{1}{1 - \omega^{\gamma}\frac{1}{q^s}} = 1 + \omega^{\gamma}\frac{1}{q^s} + \omega^{2\gamma}\frac{1}{q^{2s}} + \omega^{3\gamma}\frac{1}{q^{3s}} + \dots$$

donde aclara que γ está indexado por q (se refiere a γ_q). Esto lo hace para aliviar notación. Al avanzar las páginas y al considerar casos mas complicados, el omite el subíndice de γ nos hace requerir cierta memoria; aquí comienza a quedar en evidencia la ventaja del lenguaje moderno.

Ahora es donde define la serie. Dado un número factorizado en primos $n = q'^{m'} q''^{m''} \dots$, considera el término

$$\omega^{m'\gamma_{q'} + m''\gamma_{q''} + \dots}\frac{1}{n^s}$$

y observa que

$$m'\gamma_{q'} + m''\gamma_{q''} + \dots \equiv \gamma_n \,(\text{mod. } p-1)$$

entonces

$$\omega^{m'\gamma_{q'} + m''\gamma_{q''} + \dots} = \omega^{\gamma_n}$$

Por lo tanto tenemos la ecuación

$$\prod \frac{1}{1 - \omega^{\gamma}\frac{1}{q^s}} = \sum \omega^{\gamma}\frac{1}{n^s} = L \tag{1}$$

donde el producto es sobre todos los primos diferentes de p y la suma va de 1 a ∞ sobre los naturales no divisibles por p.

Dirichlet expresa que esta ecuación representa $p - 1$ ecuaciones diferentes (una para cada ω). Los posibles ω lo podemos obtener como potencia de un Ω (una raíz primitiva) elegido adecuadamente, de modo que los valores sean

$$\Omega^0,\ \Omega^1,\ \Omega^2,\ \dots,\ \Omega^{p-2}$$

Según esta notación escribe los diferentes valores L de la serie o producto como

$$L_0,\ L_1,\ L_2,\ \dots,\ L_{p-2}$$

Dirichlet piensa en $p - 1$ ecuaciones diferentes, en lugar de considerarla una única ecuación parametrizada por ω, como hoy haríamos.

§ 2

Posteriormente escribe $s = 1 + \rho$ y estudia el comportamiento de L para diferentes valores de ω cuando ρ se vuelve infinitamente pequeño. Comienza con L_0, fijándose en la suma

$$S = \frac{1}{k^{1+\rho}} + \frac{1}{(k+1)^{1+\rho}} + \frac{1}{(k+2)^{1+\rho}} + \dots$$

donde k es una constante positiva. Sustituyendo en la fórmula conocida

$$\int_0^1 x^{k-1} \log^\rho \left(\frac{1}{x}\right) dx = \frac{\Gamma(1+\rho)}{k^{1+\rho}} \tag{2}$$

para k, $k+1$, $k+2$, …, obtenemos

$$S = \frac{1}{\Gamma(1+\rho)} \int_0^1 \log^\rho \left(\frac{1}{x}\right) \frac{x^{k-1}}{1-x} dx = \frac{\Gamma(1+\rho)}{k^{1+\rho}}$$

Usando

$$\frac{1}{\rho} = \frac{\Gamma(\rho)}{\Gamma(1+\rho)} = \frac{1}{\Gamma(1+\rho)} \int_0^1 \log^{\rho-1} \left(\frac{1}{x}\right) dx$$

la ecuación se transforma en

$$S = \frac{1}{\rho} + \int_0^1 \left(\frac{x^{k-1}}{1-x} - \frac{1}{\log\left(\frac{1}{x}\right)} \right) \log^\rho \left(\frac{1}{x}\right) dx$$

donde el segundo término, para ρ infinitamente pequeño, se aproxima al límite finito

$$\int_0^1 \left(\frac{x^{k-1}}{1-x} - \frac{1}{\log\left(\frac{1}{x}\right)} \right) dx$$

Sacando un factor común, relaciona S con las sumas en donde en el denominador hay una progresión aritmética módulo p. Y observando que L_0 es suma de $p-1$ de estas series, concluye

$$L_0 \;=\; \frac{p-1}{p} \cdot \frac{1}{\rho} + \varphi(\rho) \tag{3}$$

donde $\varphi(\rho)$ se aproxima a un límite finito cuando ρ se hace infinitamente pequeño. En torno a esto, Dirichlet también argumenta en sus palabras, que al ser $s > 1$, la serie L converge absolutamente y por ende no depende del orden de los términos. Con arguentos elementales, afirma que el producto infinito de (1) tampoco no depende del orden.

§ 3

Para extender el estudio a la series correspondientes a los demás valores de ω, prueba que L es una función continua de $s > 0$, aunque no usa la notación $L(s)$, y su valor en 1 lo denota

$$\sum \omega^\gamma \frac{1}{n}$$

Para probarlo, toma un natural h y considera los primeros $h(p-1)$ términos de L usando la fórmula (2), válida para cualquier $1 + \rho > 0$ positivo, evaluada en $1 + \rho = s$ y $k = n$. La suma de los $h(p-1)$ términos queda

$$\frac{1}{\Gamma(s)} \int_0^1 \frac{\frac{1}{x} f(x)}{1-x^p} \log^{s-1} \left(\frac{1}{x}\right) dx - \frac{1}{\Gamma(s)} \int_0^1 \frac{\frac{1}{x} f(x)}{1-x^p} x^{hp} \log^{s-1} \left(\frac{1}{x}\right) dx \tag{4}$$

donde usa la abreviación

$$f(x) = \omega^{\gamma_1} x + \omega^{\gamma_2} x^2 + \ldots + \omega^{\gamma_{p-1}} x^{p-1}$$

Si ω no es 1, el polinomio $\frac{1}{x} f(x)$ es divisible por $1 - x$ porque

$$f(1) = \omega^{\gamma_1} + \omega^{\gamma_2} + \ldots + \omega^{\gamma_{p-1}} = 1 + \omega + \ldots + \omega^{p-2} = 0$$

Una forma de visualizar geométricamente la anulación de esta última suma es notar que el conjunto de sus sumandos es simétrico respecto del origen.

Dividiendo por $1 - x$ el numerador y denominador en el integrando de (4) y luego acotando la parte real e imaginaria de lo que nos queda en el término que aparece restando, esta desaparece cuando $h = \infty$. Por lo tanto

$$\sum \omega^{\gamma} \frac{1}{n^s} \;=\; \frac{1}{\Gamma(s)} \int_0^1 \frac{\frac{1}{x} f(x)}{1 - x^p} \log^{s-1}\left(\frac{1}{x}\right) dx$$

es es finita y derivable para $s > 0$. Luego, da dos ecuaciones funcionales para la parte real e imaginaria de esta última expresión, que relaciona su valor s con su valor en 1 y el valor de la derivada en otro punto.

§ 4

Para ω distinto de 1, el siguiente paso es probar que

$$\sum \omega^{\gamma} \frac{1}{n} \;=\; -\int_0^1 \frac{\frac{1}{x} f(x)}{x^p - 1} \, dx \tag{5}$$

no es cero. Primero simplifica la expresión de arriba, y posteriormente hace la prueba para el caso $\omega = -1$, que le lleva dos páginas. Comienza descomponiendo fácilmente el integrando como suma de fracciones simples, usando la factorización del denominador. De esta manera, obtiene

$$\sum \omega^{\gamma} \frac{1}{n} \;=\; -\frac{1}{p} \sum f\left(e^{\frac{2m\pi}{p}\sqrt{-1}}\right) \int_0^1 \frac{dx}{1 - e^{\frac{2m\pi}{p}\sqrt{-1}}}$$

donde la suma de la derecha va de $m = 1$ a $m = p - 1$. Argumentando fórmulas conocidas de la "ciclotomía", obtiene sin problemas la igualdad

$$f\left(e^{\frac{2m\pi}{p}\sqrt{-1}}\right) = \omega^{-\gamma_m} f\left(e^{\frac{2\pi}{p}\sqrt{-1}}\right)$$

Y usando que para cualquier fracción positiva α, se tiene

$$\int_0^1 \frac{dx}{1 - e^{2\alpha\pi\sqrt{-1}}} \;=\; \log(2 \sin \alpha\pi) + \frac{\pi}{2}(1 - 2\alpha)\sqrt{-1}$$

resulta

$$\sum \omega^{\gamma} \frac{1}{n} \;=\; -\frac{1}{p} f\left(e^{\frac{2\pi}{p}\sqrt{-1}}\right) \sum \omega^{\gamma_m} \left(\log\left(2 \sin \frac{m\pi}{p}\right) + \frac{\pi}{2}\left(1 - \frac{m\pi}{p}\right)\sqrt{-1}\right)$$

En este punto, me parece muy tentador ver que la parte imaginaria es distinta de cero, que sería ver que

$$\sum_{m=1}^{p-1} \omega^{\gamma_m} \;\neq\; \frac{\pi}{p} \sum_{m=1}^{p-1} m \omega^{\gamma_m}$$

Vimos que la suma de los primeros $p-2$ términos del miembro izquierdo es cero, así que nos queda

$$\frac{\pi}{p}\sum_{m=1}^{p-1} m\omega^{\gamma_m} \neq \omega^{\gamma_{p-1}}$$

Ya sabemos que esto no debería cumplirse para $\omega = -1$, y no me detuve a pensar los demás casos. Sin embargo, Dirichlet no parece señalar esto, y escribe:

> Aunque esta expresión es muy simple, en general no podemos concluir que $\sum \omega^{\gamma}\frac{1}{n}$ tiene un valor distinto de cero. Lo que falta son principios adecuados para la declaración de condiciones bajo las cuales los compuestos trascendentes que contienen enteros no definidos pueden desaparecer. Pero nuestra prueba deseada tiene éxito en el caso específico en el que $\omega = -1$. Para valores imaginarios de ω, daremos otro método en la sección siguiente que, sin embargo, no puede aplicarse al caso específico mencionado. [12, p. 9]

El caso $\omega = -1$ es el mas difícil. Dirichlet utilizó técnicas profundas de formas cuadradas, a partir de observar que como $(-1)^{\gamma_n} = \left(\frac{n}{p}\right)$, el valor de $L_{\frac{1}{2}(p-1)}$ cuando ρ es infinitamente pequeño, tiende a

$$\sum (-1)^{\gamma_n}\frac{1}{n} = \sum \left(\frac{n}{p}\right)\frac{1}{n}$$

Al final de la sección, hace dos comentarios adicionales. El primero es que a partir de la igualdad (1), viendo que en este caso todos los factores del producto son positivos cuando ρ es infinitamente pequeño. El segundo se refiere a la deducción como corolario de dos teoremas importantes (no los enunciamos porque requerimos notación que omitimos) sobre los primos de la forma $p = 4\mu + 3$, que según él, probablemente no podrían ser demostrados de otra manera.

En los años se encontraron formas alternativas y mas simples de manejar este caso, pero aún seguía siendo el paso mas sustancial y técnicamente complicado de la prueba.

§ 5

Para probar que L_m, si m no es 0 ni $\frac{1}{2}(p-1)$, no se aproxima a cero cuando ρ es infinitamente pequeño, aplicamos logaritmo en el producto de (1), y desarrolla en serie de potencias el logaritmo de cada factor. Le queda

$$\sum \omega^{\gamma}\frac{1}{q^{1+\rho}} + \frac{1}{2}\sum \omega^{2\gamma}\frac{1}{(q^2)^{1+\rho}} + \frac{1}{3}\sum \omega^{3\gamma}\frac{1}{(q^3)^{1+\rho}} + \ldots = \log L$$

Si sustituimos ω por la correspondiente potencia de Ω, recordamos que la suma

$$1 + \Omega^{h\gamma} + \Omega^{2h\gamma} + \ldots + \Omega^{(p-2)h\gamma}$$

se anula excepto cuando $h\gamma$ es divisible por $p-1$ (en cuyo caso la suma da $p-1$), condición que se identifica con los $q^h \equiv 1 \,(\text{mod. } p)$, y recordamos que log transforma productos en sumas, obtenemos

$$(p-1)\left(\sum \frac{1}{q^{1+\rho}} + \frac{1}{2}\sum \frac{1}{q^{2+2\rho}} + \frac{1}{3}\sum \frac{1}{q^{3+3\rho}} + \ldots\right) = \log(L_0 L_1 \cdots L_{p-2})$$

donde la primera, segunda, ... suma se relaciona con aquellos valores de q, cuyas primeras, segundas, ... potencias son de la forma $\mu p + 1$, respectivamente. El miembro izquierdo es siempre un real positivo. Veamos que si asumimos que L_m se aproxima a cero, entonces el miembro derecho sería $-\infty$ cuando ρ se anula. El lado derecho se puede escribir como

$$\log L_0 + \log L_{\frac{1}{2}(p-1)} + \log L_1 L_{p-2} + \log L_2 L_{p-3} + \dots$$

A partir de la igualdad (3) sabemos que $\log L_0$ se aproxima a $\log\left(\frac{1}{\rho}\right)$. Por § 4 sabemos que $\log L_{\frac{1}{2}(p-1)}$ tiene límite finito. Suponiendo que L_m tiene límite nulo y usando las ecuaciones funcionales que mencionamos (y no dimos) al final de § 3, ve mediante argumentos breves que $\log L_m L_{p-1-m}$ se aproxima al menos a $-2\log\left(\frac{1}{\rho}\right)$. Luego, $\log L_0 + \log L_m L_{p-1-m}$ se aproxima a algo menor o igual que $-\log\left(\frac{1}{\rho}\right)$, y es claro que este valor negativo infinitamente grande no puede ser cancelado por los otros términos (porque probamos que L_m tiene límite finito para $m > 0$).

Ya vimos que L_m tiene un límite finito distinto de cero, si $m > 0$. Luego, le dedica una página a comentar sobre el problema de calcular el límite explícito, lo cual no es necesario para probar el teorema en sí.

§ 6

Esta sección la dedica a termina de probar que si $m = 1, \dots, p-1$, entonces hay infinitos primos en la progresión aritmética $\mu p + m$. Para esto, dice él, multiplicamos las ecuaciones contenidas en (1), que corresponden consecutivamente a las raíces

$$1, \Omega, \Omega^2, \dots, \Omega^{p-2}$$

con

$$1, \Omega^{-\gamma_m}, \Omega^{-2\gamma_m}, \dots, \Omega^{-(p-2)\gamma_m}$$

respectivamente, y sumamos (es decir, está tomando una combinación lineal), obtenemos en el lado izquierdo

$$\begin{aligned}
&\sum \left(1 + \Omega^{\gamma-\gamma_m} + \Omega^{2(\gamma-\gamma_m)} + \dots + \Omega^{(p-2)(\gamma-\gamma_m)}\right) \frac{1}{q^{1+\rho}} \\
+ &\sum \left(1 + \Omega^{2\gamma-\gamma_m} + \Omega^{2(2\gamma-\gamma_m)} + \dots + \Omega^{(p-2)(2\gamma-\gamma_m)}\right) \frac{1}{q^{2+2\rho}} \\
+ &\sum \left(1 + \Omega^{3\gamma-\gamma_m} + \Omega^{2(3\gamma-\gamma_m)} + \dots + \Omega^{(p-2)(3\gamma-\gamma_m)}\right) \frac{1}{q^{3+3\rho}} \\
+ &\dots
\end{aligned}$$

donde debemos recordar que γ está indexada por q. Ahora, del hecho de que

$$1 + \Omega^{h\gamma-\gamma_m} + \Omega^{2(h\gamma-\gamma_m)} + \dots + \Omega^{(p-2)(h\gamma-\gamma_m)} = 0$$

excepto cuando $h\gamma - \gamma_m \equiv 0 \,(\text{mod. } p-1)$, en cuyo caso la suma es igual a $p-1$. Esta congruencia equivale a tener $q^h \equiv m \,(\text{mod. } m)$. Por lo tanto, tenemos la ecuación

$$\sum \frac{1}{q^{1+\rho}} + \frac{1}{2}\sum \frac{1}{q^{2+2\rho}} + \frac{1}{3}\sum \frac{1}{q^{3+3\rho}} + \dots$$

$$= \frac{1}{p-1}\left(\log L_0 + \Omega^{-\gamma_m}\log L_1 + \Omega^{-2\gamma_m}\log L_2 + \ldots + \Omega^{-(p-2)\gamma_m}\log L_{p-2}\right)$$

donde la primera sumatoria es sobre todos los primos q de la forma $\mu p + m$, la segunda sobre todos los primos q con cuadrados de esa forma, la tercera sobre todos los primos q con cubos de esa forma, etc. Si asumimos ahora que ρ se vuelve infinitamente pequeño, el lado derecho se volverá infinitamente grande a través del término $\log L_0$. Por lo tanto, el lado izquierdo también tiene que volverse infinito. Pero en este lado, la suma de todos los términos, excepto el primero, permanece finita porque, como es bien conocido, la suma

$$\frac{1}{2}\sum\frac{1}{q^2} + \frac{1}{3}\sum\frac{1}{q^3} + \ldots$$

sobre todos los enteros n mayores que 1, es finita. Así, la serie

$$\sum\frac{1}{q^{1+\rho}}$$

debe crecer mas allá de cualquier límite positivo, por lo que tiene infinitos términos, que son los primos q de la forma $\mu p + m$, q.e.d.

3.4. Caso general

Posteriormente a lo visto recién, Dirichlet generaliza estas ideas al caso en donde k es compuesto, y da comentarios interesantes sobre las ideas que tuvo y sobre otros problemas. Seguimos separando las secciones según lo hizo Dirichlet.

§ 7

Dirichlet comienza factorizando en primos

$$k = 2^\lambda p^\pi p'^{\pi'} \cdots$$

donde $\pi, \pi', \ldots$ son mayores o iguales a 1. Hoy, nos sería mas cómoda la notación $p_i^{\pi_i}$ para los factores. El grupo de unidades módulo k es igual al es isomorfo al producto de los grupos de unidades módulo cada uno de los factores $p_i^{\pi_i}$. Dirichlet cita a Gauss [14, *sect. III*], quien había demostrado que si p es un primo impar y $\pi \in \mathbb{N}$, entonces se puede encontrar un elemento primitivo c módulo p^π. Es decir, la clase de residuos de c genera el grupo cíclico $C^*_{p^\pi}$, o de manera equivalente, para cada n coprimo con p, existe un γ_n tal que $c^{\gamma_n} \equiv n \pmod{p^\pi}$. Así, podemos elegir elementos primitivos $c, c' \ldots$ correspondientes a $p^\pi, p'^{\pi'}, \ldots$ Sin embargo, si $\lambda \geqslant 3$, no existe un elemento primitivo módulo 2^λ. En su lugar, el grupo de unidades módulo 2^λ es producto de dos grupos cíclicos, y para cada n coprimo con 2, existen α_n y β_n tal que $(-1)^{\alpha_n}5^{\beta_n} \equiv n \pmod{2^\lambda}$. Así, para cualquier n coprimo con k podemos escribir

$$n \equiv (-1)^{\alpha_n}5^{\beta_n}c^{\gamma_n}c'^{\gamma'_n}\cdots \pmod{k}$$

Como antes, si elegimos raíces de la unidad apropiadas $\theta, \varphi, \omega, \omega', \ldots$, obtenemos una función

$$\chi(n) = \theta^{\alpha_n}\varphi^{\beta_n}\omega^{\gamma_n}\omega'^{\gamma'_n}\cdots$$

(como mencionamos antes, él no usa la notación $\chi(n)$). Luego suprime el subíndice n, dejándonos como tarea recordar esta dependencia. Un contraste con ciertas pruebas modernas (como la que daremos en CITAR), es que estas últimas tienen poco que decir

sobre ciertos χ en particular, a excepción del que Dirichlet había denotado L_0 y que tiene un comportamiento distintivo.

§ 8

La función χ es multiplicativa y depende solo de la congruencia módulo k, así que obtenemos un "producto de Euler" que luce

$$\prod \frac{1}{1 - \theta^\alpha \varphi^\beta \omega^\gamma \omega'^{\gamma'} \cdots \frac{1}{q^s}} = \sum \theta^\alpha \varphi^\beta \omega^\gamma \omega'^{\gamma'} \cdots \frac{1}{n^s} = L$$

donde el producto es sobre los primos q distintos de $2, p, p', \ldots$ y la suma sobre todos los naturales n coprimos con $2pp' \cdots$

Dirichlet denota por K a la cardinalidad del grupo de unidades módulo k, que es lo que nosotros estamos acostumbrados a denotar $\varphi(k)$, e insiste en que la ecuación general anterior contiene K ecuaciones particulares. Dirichlet continuó observando que podemos elegir raíces primitivas de la unidad $\Theta, \Phi, \Omega, \Omega', \ldots$ de manera que todas las elecciones de $\theta, \phi, \omega, \omega', \ldots$ puedan expresarse como potencias de estas:

$$\theta = \Theta^{\mathfrak{a}}, \qquad \varphi = \Phi^{\mathfrak{b}}, \qquad \omega = \Omega^{\mathfrak{c}}, \qquad \omega' = \Omega'^{\mathfrak{c}'}, \ldots$$

denotando a la correspondiente L, por

$$L_{\mathfrak{a},\mathfrak{b},\mathfrak{c},\mathfrak{c}',\ldots}$$

de forma análoga a la notación en el caso mas simple $k = p$ primo.

§ 9

Aquí, separa el conjunto de las funciones L en tres clases disjuntas, de forma análoga a lo hecho en el caso $k = p$ primo. La primera contiene solo a la serie $L_{0,0,0,0,\ldots}$, la segunda esta formada por todas las demás que se corresponden con los χ que tomen solo valores reales, o sea las que combinan los signos

$$\theta = \pm 1, \qquad \varphi = \pm 1, \qquad \omega = \pm 1, \qquad \omega' = \pm 1, \ldots$$

sin que todas sean 1. La tercera clase esta formada por las que alguna de las raíces $\varphi, \omega, \omega', \ldots$ es imaginaria (no incluimos a θ porque podemos asumir siempre que es ± 1). Es evidente que las series de esta última clase vienen de a pares conjugados.

Primero trabaja con la primera clase, descomponiendo la serie como K series correspondientes a cada progresión aritmética módulo k, y concluyendo rápidamente que la suma de estas contribuciones resultan en

$$\frac{K}{k} \cdot \frac{1}{\rho} + \varphi(\rho)$$

donde $\varphi(\rho)$ tiene un valor finito cuando ρ tiende a cero.

Al analizar las otras dos clases, llega sin inconvenientes a una fórmula análoga a (5).

§ 10

Salvo algunas modificaciones, la estructura que se sigue al probar la no anulación de las series de la segunda y tercera clase, es análoga a la del caso $k = p$ primo. Primero,

a partir de suponer que las de segunda clase no se anulan, lo prueba para las de tercera clase. En el transcurso, llega a una expresión análoga a la de la sección § 6, que luce así:

$$\sum \frac{1}{q^{1+\rho}} + \frac{1}{2}\sum \frac{1}{q^{2+2\rho}} + \frac{1}{3}\sum \frac{1}{q^{3+3\rho}} + \dots$$
$$= \frac{1}{K}\sum \Theta^{-\alpha_m \mathfrak{a}} \Phi^{-\beta_m \mathfrak{b}} \Omega^{-\gamma_m \mathfrak{c}} \Omega'^{-\gamma'_m \mathfrak{c}'} \cdots \log L_{\mathfrak{a},\mathfrak{b},\mathfrak{c},\mathfrak{c}',\dots}$$

donde la suma en el lado izquierdo es sobre todos los primos q cuyas primeras, segundas y terceras potencias están son de la forma $\mu k + m$, mientras que la suma de la derecha es sobre todas las series $L_{\mathfrak{a},\mathfrak{b},\mathfrak{c},\mathfrak{c}',\dots}$

Concluye la sección con el hecho de que si m es coprimo con k, la serie

$$\sum \frac{1}{q^{1+\rho}}$$

sobre los primos q de la forma $\mu k + m$ tiende a infinito cuando ρ tiende a cero, q.e.d.

§ 11

En esta sección, Dirichlet concluye su trabajo con comentarios sobre formas cuadráticas y el caso de las series de segunda clase.

4. Prueba moderna

Hay al menos dos pruebas modernas con diferentes variaciones. Quizás la parte discrepante se concentre mas que nada en como ver la no anulación de las series de segunda y tercera clase. Apostol [1] y otros libros exponen pruebas que, al igual que Dirichlet, discriminan la segunda clase de la tercera, aunque considerando la serie $\sum \frac{\ln p}{p}$ mediante una maquinaria algebraica que excede este escrito. Aquí presentaremos una demostración que utiliza fuertemente análisis complejo elemental, y que no discrimina a la segunda clase de la tercera, sino que concentra las dificultades de ambas en un mismo paso mas limpio. Elegimos esta para no ser repetitivos con el capítulo anterior y para exponer parte de la teoría general motivada a partir del teorema que nos ocupa. Para este propósito propósito, citamos los artículos [18], [19] y en menor medida [13]. Del muy breve análisis histórico que ofrecen estos, podemos apreciar que la prueba que daremos es fiel a la original, con modificaciones que cuenta a Edmund Landau como posible primer contribuyente.

El libro [5], de donde hemos tomado la cita de Erdős que está en nuestra portada, está poblado de ilustraciones interesantes, así como de resultados de interés para quien quiera profundizar en la teoría.

4.1. Series de Dirichlet y carácteres de grupos

Definición 4.1 (Series de Dirichlet)**.** *Una Serie de Dirichlet es una de la forma*

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

donde s y los a_n son complejos.

Retomando los preliminares § 3.1, definimos un grupo abeliano G como un grupo conmutativo, es decir que satisface $g_1 g_2 = g_2 g_1$ para todo par $g_1, p_2 \in G$.

Definición 4.2 (Carácteres de grupos)**.** *Un carácter de un grupo abeliano G es un homomorfismo de grupos $\chi : G \to \mathbb{C}^*$. El carácter trivial $\chi \equiv 1$ se denota $\chi = 1$. Al conjunto de carácteres de G se lo denota $\widehat{G}$.*

Como sabemos, estos carácteres tienen a $\mathbb{G}_\infty$ como conjunto de llegada, ya que $\forall\ g \in G$, $\exists\ k \in \mathbb{N}$ tal que $g^k = 1$, y por ende $\chi(g)^k = \chi(g^k) = \chi(1) = 1$.

Los carácteres que nos interesan en nuestra demostración son los siguientes:

Definición 4.3 (Carácteres de Dirichlet)**.** *Un $\chi \in \widehat{C_k^*}$ es un car. de Dirichlet mód. k.*

4.2. L-funciones

Como mencionamos en § 3.2, los carácteres de Dirichlet tienen a $\mathbb{G}_\infty$ como conjunto de llegada, y se pueden extender a todo $\mathbb{Z}$. De esta forma obtenemos las series de Dirichlet que nos interesan:

Definición 4.4 (L-funciones)**.** *Una L-función es una serie de Dirichlet donde $a_n = \chi(n)$, con $\chi : \mathbb{Z} \to \mathbb{G}_\infty \cup \{0\} \subset \mathbb{C}$ la extensión a $\mathbb{Z}$ de un carácter de Dirichlet. Se denota $L(s, \chi)$.*

A continuación escribimos formalmente un teorema que generaliza al de Euler (Prop. 2.1), y que ya hemos demostrado de forma comentada en medio de § 3.2. Aprovechamos para dejarlo presentado.

Teorema 4.1 (Producto de Euler)**.**

$$L(s, \chi) = \prod_{p \text{ primo}} \frac{1}{1 - \frac{\chi(p)}{p^s}}$$

Demostración.

$$\frac{\chi(2)}{2^s} L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(2)\chi(n)}{2^s n^s} = \sum_{n=1}^{\infty} \frac{\chi(2n)}{(2n)^s} = \sum_{2 \,|\, n} \frac{\chi(n)}{n^s}$$

$$\left(1 - \frac{\chi(2)}{2^s}\right) L(s, \chi) = \sum_{2 \nmid n} \frac{\chi(n)}{n^s}$$

$$\vdots$$

$$L(s, \chi) \prod_{p \text{ primo}} \frac{p^s - \chi(p)}{p^s} = 1$$

$$L(s, \chi) = \prod_{p \text{ primo}} \frac{p^s}{p^s - \chi(p)}$$

□

A simple vista, parece evidente que $L(1, 1)$ diverge porque $\zeta(1)$ lo hace. De hecho, esto se explicita con la siguiente fórmula válida $\forall\ \mathrm{Re}(s) > 1$.

Observación 4.2. *La L-función asociada al carácter trivial módulo d satisface*

$$L(s,1) = \prod_{\substack{p \text{ primo} \\ p \nmid d}} \frac{1}{1-p^{-s}} = \zeta(s) \prod_{\substack{p \text{ primo} \\ p \mid d}} (1-p^{-s})$$

Demostración. Es el producto de Euler (ver Teo. 4.7) aplicado a $\chi = 1$, y recordando que los carácteres módulo d (en este caso el trivial) anulan a los factores primos de d. □

Nota: Para visualizar mas fácil la igualdad anterior, se la puede pensar de forma análoga a lo hecho en la demostración del producto de Euler (Proposición 2.1). Solo que como la serie $L(s,1)$ solo contiene los términos correspondientes a los n coprimos con d, en la productoria deben aparecer solamente los primos que no dividen a d.

Proposición 4.3. *Las L-funciones satisfacen:*

1. $L(s,1)$ *diverge en* $s = 1$.
2. $L(s,\chi)$ *converge absolutamente solo en* $\{s \in \mathbb{C} \mid \mathrm{Re}(s) > 1\}$, $\forall\ \chi$.

Demostración. $\forall\ \chi$, se tiene

$$\left|\frac{\chi(n)}{p^{-s}}\right| = \frac{1(n)}{p^{-\mathrm{Re}(s)}}$$

Luego, $L(s,\chi)$ converge absolutamente si y solo si $L\big(\mathrm{Re}(s),1\big)$ converge, y por la Observación 4.2 esto ocurre si y solo si $\mathrm{Re}(s) > 1$, ya que ζ diverge en $s = 1$. □

La exponencial compleja es $e^{x+yi} = e^x\big(\cos y + i \sin y\big)$. Si al plano complejo le quitamos una semirecta que salga del cero hacia el infinito, allí existen infinitas funciones log tal que $\exp \circ \log = Id$, y toda ellas difieren en un múltiplo de 2π. Además, estas funciones son analíticas (versión compleja de diferenciable) en su dominio.

Antes de tomar log $L(s,\chi)$ tenemos que asegurarnos que $L(s,\chi)$ esté efectivamente en el dominio de una rama del logaritmo complejo, es decir hay que ver que no se anula para $\chi \neq 1$. La demostración de este hecho la veremos luego en § 4.5 para no perder el hilo de la idea general. Al probar esto, y por continuidad del log y de $L(s,\chi)$, podemos encontrar u entorno de $s_0 = 1 \in \mathbb{C}$ y una rama del log tal que $\log L(s,\chi)$ esta bien definido para todo χ y todo $s \neq s_0$ en dicho entorno.

Proposición 4.4. *Para* $\mathrm{Re}(s) > 1$ *se cumple*

$$\log L(s,\chi) = \sum_{p \text{ primo}} \frac{\chi(p)}{p^s} + O(1)$$

Demostración. Con un argumento análogo al del Corolario 2.3 tenemos

$$\log L(s,\chi) = \sum_{p \text{ primo}} \log \frac{1}{1-\chi(p)p^{-s}}$$

Como $\log\big(\frac{1}{1-z}\big)$ es analítica (por ser composición de analíticas) en el conjunto $\{z \in \mathbb{C} : |z| < 1\}$, allí es igual a su serie de Taylor. Dicha serie es como la que teníamos en variable real en la demostración del Corolario 2.3. Luego, si $|z| \leqslant \frac{1}{2}$, entonces tenemos

la cota $\left|\log\left(\frac{1}{1-z}\right) - z\right| \leqslant |z|^2$. Denotemos $z_p := \chi(p)p^{-s}$. Como $|z_p| = |p^{-s}| = p^{\mathrm{Re}(-s)} = p^{-\mathrm{Re}(s)} < p^{-1} \leqslant \frac{1}{2}\ \forall\ p$ primo,

$$\begin{aligned}\left|\log L(s,\chi) - \sum_{p \text{ primo}} \frac{\chi(p)}{p^s}\right| &= \left|\sum_{p \text{ primo}} \log\frac{1}{1-z_p} - \sum_{p \text{ primo}} z_p\right| \\ &\leqslant \sum_{p \text{ primo}} \left|\log\left(\frac{1}{1-z_p}\right) - z_p\right| \\ &\leqslant \sum_{p \text{ primo}} |z_p|^2 < \sum_{p \text{ primo}} \frac{1}{p^2} < \zeta(2)\end{aligned}$$

Es decir, la diferencia es una función acotada por la constante $\zeta(2) = \frac{\pi^2}{6}$. □

4.3. Isomorfismo natural y relaciones de ortogonalidad

Para dar el siguiente paso vamos a probar resultados de carácteres de grupos en general.

Proposición 4.5. *$G \simeq \widehat{G}$.*

Demostración. Si G es cíclico de orden m generado por c, $\chi \in \widehat{G}$ y $g \in G$ entonces $\chi^m(g) = \chi(g^m) = \chi(1) = 1$. Es decir, $\chi^m = 1$. Y como para cada $w \in \mathbb{G}_m$ podemos definir un único χ a partir de $\chi(c) = w$, concluimos que $\widehat{G} \simeq \mathbb{G}_m \simeq G$.

Para el caso general, por el Teorema de estructura tenemos $G \simeq \mathbb{G}_{m_1} \times \ldots \times \mathbb{G}_{m_r}$. Luego,

$$\widehat{G} \simeq \widehat{\mathbb{G}_{m_1}} \times \ldots \times \widehat{\mathbb{G}_{m_1}} \simeq \mathbb{G}_{m_1} \times \ldots \times \mathbb{G}_{m_r} \simeq G$$

□

También podemos pensar a $\widehat{G}$ como un grupo con la multiplicación de funciones, y preguntarnos lo que pasa con $\widehat{\widehat{G}}$. Por la proposición anterior aplicada dos veces, sabemos que es isomorfo a G. En realidad veremos que son más que isomorfos. No daremos la definición formal de "isomorfismo natural", concepto que aparece en el siguiente enunciado. Sin embargo, damos una intuición de su significado. La idea de estos isomorfismos es que se definen de forma "limplia" y genérica, sin ningún tipo de elección particular en cada caso. Por ejemplo, el isomorfismo de la proposición anterior lo construimos a mano, y depende de G y de una base del mismo, o sea sin deducirse de una formula general concisa.

Proposición 4.6. *La función*

$$\begin{aligned}\mathrm{ev} : G &\to \widehat{\widehat{G}} \\ g &\mapsto \mathrm{ev}_g \\ \mathrm{ev}_g(\chi) &:= \chi(g)\end{aligned}$$

es un isomorfismo natural.

Demostración. ev es claramente un homomorfismo de grupos con núcleo trivial. Al ser un monomorfismo entre dos grupos finitos del mismo orden, resulta un isomorfismo. □

La idea de los últimos dos resultados está presente en otros contextos, por ejemplo en Álgebra lineal, al ver que un espacio vectorial de dimensión finita es isomorfo a su dual, y naturalmente isomorfo a su doble dual.

Para motivar lo que sigue, consideremos el caso $k = p$ primo para simplificar. Una hecho clave en la prueba fue que

$$\sum_{\omega \in \mathbb{G}_{p-1}} \omega^k = \begin{cases} p-1 & si \quad k = 0 \\ 0 & si \quad 0 < k < p-1 \end{cases} \tag{6}$$

Una intuición geométrica respecto a eso es que $\mathbb{G}_{p-1}$ es un conjunto "simétrico" respecto del punto 0, por lo que la suma de sus elementos no debería indicar ninguna dirección privilegiada. Esta es una idea que puede tenerse al ver la demostración del próximo teorema. La última igualdad puede traducirse en

$$\sum_{\omega \in \mathbb{G}_{p-1}} \chi(\omega) = \begin{cases} p-1 & si \quad \chi = 1 \\ 0 & si \quad \chi \in \widehat{\mathbb{G}_{p-1}} \setminus \{1\} \end{cases}$$

cuya idea de prueba se puede generalizar de la siguiente forma:

Teorema 4.7. *Si G es un grupo abeliano finito, entonces*

$$\frac{1}{|G|} \sum_{g \in G} \chi(g) = \begin{cases} 1 & si \quad \chi = 1 \\ 0 & si \quad \chi \neq 1 \end{cases}$$

Demostración. Si $\chi = 1$, es claro, pues los $|G|$ términos de la sumatoria son iguales a 1. Si $\chi \neq 1$, entonces $\exists\, h \in G$ tal que $\chi(h) \neq 1$. Luego,

$$\chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(h)\chi(g) = \sum_{g \in G} \chi(hg) = \sum_{g \in hG} \chi(g) = \sum_{g \in G} \chi(g)$$

donde hemos usado que los conjuntos hG y G son iguales debido a que h es invertible por ser G un grupo. Por lo tanto,

$$\big(1 - \chi(h)\big) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(g) - \sum_{g \in G} \chi(g) = 0$$

Como $1 - \chi(h) \neq 0$, entonces la sumatoria debe ser anularse. □

Sea $a \in C_p^*$, tomando c un generador de C_p^* podemos escribir $a = c^k$ para algún $0 \leqslant k < p-1$. Usando en el fondo que $G \simeq \widehat{G}$, vemos

$$\sum_{\chi \in \widehat{C_p^*}} \chi(a) = \sum_{\chi \in \widehat{C_p^*}} \chi(c^k) = \sum_{\chi \in \widehat{C_p^*}} \chi(c)^k = \sum_{\omega \in \mathbb{G}_{p-1}} \omega^k$$

Es decir, de la ecuación (6) concluimos

$$\sum_{\chi \in \widehat{C_p^*}} \chi(a) = \begin{cases} p-1 & si \quad a = 1 \\ 0 & si \quad a \neq 1 \end{cases}$$

Otra forma de ver esto es directamente hacer la cuenta con χ variando y a fijo, y aplicar la idea análoga de recién en el Teorema 4.7 cuando era χ quien estaba fijo y g variaba. Una manera de pensar esto último conectando ideas y evitando repetir cuentas, es usar el isomorfismo de la Proposición 4.6, como hacemos a continuación.

Corolario 4.8. *Si G es un grupo abeliano finito, entonces*

$$\frac{1}{|G|}\sum_{\chi\in\widehat{G}}\chi(g) = \begin{cases} 1 & si \quad g = 1 \\ 0 & si \quad g \neq 1 \end{cases}$$

Demostración. Como $\widehat{G} \simeq G$, tenemos $|\widehat{G}| = |G|$. Y por la Proposición 4.6, como ev es un isomorfismo, tenemos que $\mathrm{ev}_g = \mathrm{ev}(g) \in \widehat{\widehat{G}}$ es igual a 1 si y solo si $g = 1$. Recurriendo también al Teorema 4.7, escribimos

$$\frac{1}{|G|}\sum_{\chi\in\widehat{G}}\chi(g) = \frac{1}{|\widehat{G}|}\sum_{\chi\in\widehat{G}}\mathrm{ev}_g(\chi) = \begin{cases} 1 & si \quad \mathrm{ev}(g) = 1 \\ 0 & si \quad \mathrm{ev}(g) \neq 1 \end{cases} = \begin{cases} 1 & si \quad g = 1 \\ 0 & si \quad g \neq 1 \end{cases}$$

□

Lo que necesitamos nosotros es el ítem 2 del siguiente corolario.

Corolario 4.9 (Relaciones de ortogonalidad de carácteres de Dirichlet)**.** *Sea $m \in \mathbb{N}$.*

1. *Sean χ y ψ dos (extensiones a $\mathbb{Z}$ de) caracteres de Dirichlet módulo m, entonces*

$$\frac{1}{\varphi(m)}\sum_{a=0}^{m-1}\overline{\psi(a)}\chi(a) = \begin{cases} 1 & si \quad \psi = \chi \\ 0 & si \quad \psi \neq \chi \end{cases}$$

2. *Sean $a, b \in \mathbb{N}$ coprimos con m, entonces*

$$\frac{1}{\varphi(m)}\sum_{\chi\in\widehat{C_m^*}}\overline{\chi(b)}\chi(a) = \begin{cases} 1 & si \quad a \equiv b \,(\mathrm{mod}\ m) \\ 0 & si \quad a \not\equiv b \,(\mathrm{mod}\ m) \end{cases}$$

Demostración. 1. Aplicamos el Teorema 4.7 a $\psi^{-1}\chi$. De $\overline{\psi(a)} = \psi(a)^{-1} = \psi^{-1}(a)$, sale

$$\sum_{a=0}^{m-1}\overline{\psi(a)}\chi(a) = \sum_{a=0}^{m-1}(\psi^{-1}\chi)(a) = \begin{cases} |C_m^*| & si \quad \psi^{-1}\chi = 1 \\ 0 & si \quad \psi^{-1}\chi \neq 1 \end{cases} = \begin{cases} \varphi(m) & si \quad \psi = \chi \\ 0 & si \quad \psi \neq \chi \end{cases}$$

2. Análogamente, ahora aplicando ahora el Corolario 4.8. Por $\overline{\chi(b)} = \chi(b)^{-1} = \chi(b^{-1})$,

$$\sum_{\chi\in\widehat{C_m^*}}\overline{\chi(b)}\chi(a) = \sum_{\chi\in\widehat{C_m^*}}\chi(b^{-1}a) = \begin{cases} |C_m^*| & si \quad b^{-1}a = 1 \\ 0 & si \quad b^{-1}a \neq 1 \end{cases} = \begin{cases} \varphi(m) & si \quad b = a \\ 0 & si \quad b \neq a \end{cases}$$

□

4.4. Cómo queda la demostración

Ya tenemos todos los ingredientes para nuestra demostración:

Teorema 4.10 (Dirichlet, 1837)**.** *Si d y a son naturales coprimos, entonces*

$$\sum_{\substack{p \text{ primo} \\ p\equiv a\,(\mathrm{mod}\ d)}}\frac{1}{p} = \infty$$

Demostración. De la Proposición 4.4 y el Corolario 4.8, sale

$$\begin{aligned}
\sum_{\chi \in \widehat{C_d^*}} \overline{\chi(a)} \log L(s,\chi) &= \sum_{\chi \in \widehat{C_d^*}} \overline{\chi(a)} \sum_{p \text{ primo}} \frac{\chi(p)}{p^s} + O(1) \\
&\shortparallel \qquad = \sum_{p \text{ primo}} \frac{1}{p^s} \sum_{\chi \in \widehat{C_d^*}} \overline{\chi(a)} \chi(p) + O(1) \\
&\shortparallel \qquad = \sum_{\substack{p \text{ primo} \\ p \equiv a \,(\mathrm{mod}\ d)}} \frac{\varphi(d)}{p^s} + O(1) \\
\varphi(d) \sum_{\substack{p \text{ primo} \\ p \equiv a \,(\mathrm{mod}\ d)}} \frac{1}{p^s} &= \sum_{\chi \in \widehat{C_d^*}} \overline{\chi(a)} \log L(s,\chi) + O(1) \\
\sum_{\substack{p \text{ primo} \\ p \equiv a \,(\mathrm{mod}\ d)}} \frac{1}{p^s} &= \frac{L(s,1)}{\varphi(d)} + \frac{1}{\varphi(d)} \sum_{\chi \neq 1} \overline{\chi(a)} \log L(s,\chi) + O(1)
\end{aligned}$$

Como $L(1,\chi) \neq 0$ para χ no principal, al tomar $\lim_{s \to 1^+}$ en el segundo miembro de la última igualdad, el primer término diverge y el segundo converge. Por ende el miembro derecho diverge. □

4.5. No anulación de $L(1,\chi)$

Como ya mencionamos, esta es sin duda la parte más difícil de la prueba.

La divergencia de $L(1,1)$ es muy lenta, tanto como la de la serie armónica. Es lo "más lenta posible", formalmente decimos que $L(s,1)$ (en realidad, su extensión analítica, que veremos en un rato) tiene un polo simple (o polo de primer orden) en $s = 1$. La idea entonces es que si $L(1,\chi) = 0$ para algún χ, tenemos que $\lim_{s \to 1} L(s,1)L(s,\chi)$ existe. Esto nos lleva a definir la *Función zeta de Dedekind*, como el producto de todas las L-funciones módulo d, y la denotamos ζ_k. Recordar que esta función fue usada por el propio Dirichlet al probar la no anulación de las series de tercera clase cuando vimos el caso $k = p$ primo impar. La ventaja de utilizar todos los caracteres radica en atacar todos los casos en simultaneo, favoreciendo a la manipulación de términos para llegar a fórmulas cerradas útiles.

Empezamos viendo los resultados finos sobre series de Dirichlet que necesitamos para aplicar a ζ_k. Luego vemos como estos confluyen en la conclusión de la prueba.

4.5.1. Preliminares: resultados básicos de Análisis complejo

Estos resultados forman parte de un curso básico de Análisis complejo, y los damos sin demostración. Un buen libro es el de Conway [16].

Teorema 4.11. *Toda función diferenciable en un abierto $D \subset \mathbb{C}$ es analítica. Es decir, satisface una representación en serie de Taylor en cada bola abierta contenida en D. A su vez, esto implica que las funciones diferenciables son infinitamente diferenciables.*

Nota: Lo anterior es una clara diferencia respecto del análisis real, y es el núcleo de la potencia del Análisis complejo, que presenta resultados sorprendentes.

Proposición 4.12. *El límite uniforme preserva la analiticidad. Es decir, si $f = \lim f_n$ es un límite uniforme en un abierto D donde las f_n son analíticas, entonces f también es analítica en D. Además, $f^{(r)} = \lim f_n^{(r)}$.*

Ya dijimos lo que es una función analítica. Un polo s_0 de una función f es un punto problemático en donde f es analítica en un entorno de z_0 salvo en ese punto, donde diverge. Básicamente, se tiene que f es de la forma $f = \frac{g}{(z-z_0)^n}$ donde algún $n \in \mathbb{N}$ y g es analítica. El mínimo n con esa propiedad se llama *orden del polo*. Por otro lado, tenemos la noción de *orden de un cero* c_0 de f, que es el mínimo n tal que f se escribe de la forma $f = (z - c_0)^n g$ donde g es analítica y no se anula en c_0. Observar que el producto de una función con un polo de orden n en z_0 con una que tiene un cero de orden $\geqslant n$ en z_0, resulta en una función analítica alrededor de dicho punto. En particular, esto ocurre si el polo es simple (de orden 1) y el cero es de cualquier orden. Este caso particular es el que nos aparece.

Una *Función meromorfa* en un dominio es una analítica salvo quizás en una cantidad finita de puntos, en donde presenta polos.

También nos viene bien saber qué son los *conjuntos compactos* de $\mathbb{C}$. Estos son los conjuntos cerrados (cualquier punto del complemento tiene todo un entorno contenido en el complemento) y acotados.

4.5.2. Resultados de analiticidad y extensiones

Para lo siguiente necesitamos usar una versión de la *Fórmula de sumación de Abel*: Sean $\{u_n\}, \{v_n\} \subset \mathbb{C}$ dos sucesiones complejas y $U_n := \sum_{i=1}^{n} u_i$, entonces

$$\sum_{n=1}^{N} U_n v_n = U_N v_N + \sum_{n=1}^{N-1} U_n (v_n - v_{n+1})$$

En particular, si $\lim\limits_{n\to\infty} U_n v_n = 0$, entonces

$$\sum_{n=1}^{\infty} u_n v_n = \sum_{n=1}^{\infty} U_n (v_n - v_{n+1})$$

y cualquiera de las series converge si y solo si converge la otra.

Teorema 4.13 (Cohen)**.** *Si una serie de Dirichlet converge en un determinado $s_0 \in \mathbb{C}$, entonces converge uniformemente sobre compactos en el semiplano abierto* $\operatorname{Re} s > \operatorname{Re} s_0$*, siendo analítica allí.*

Demostración. Sea $f(s) = \sum_n a_n n^{-s}$, aplicamos la Fórmula de sumación de Abel a

$$\frac{a_n}{n^s} = \underbrace{\frac{a_n}{n^{s_0}}}_{u_n} \underbrace{\frac{1}{n^{s-s_0}}}_{v_n(s)} = u_n v_n(s)$$

Por hipótesis, sabemos que $\{U_n\}$ es convergente, de hecho el límite es $f(s_0)$. Por otro lado, $v_n \to 0$ en el semiplano $\operatorname{Re} s > \operatorname{Re} s_0$. Luego, $U_n v_n(s) \to 0$ en el semiplano. Además,

$$\sum_{n=N}^{\infty} |U_n||v_n - v_{n+1}| \leqslant \sup_{n\in\mathbb{N}} |U_n| \sum_{n=N}^{\infty} |v_n - v_{n+1}|$$

Ya nos deshicimos de la sucesión $\{a_n\}$ y solo queda acotar uniformemente la cola de $\sum |v_n - v_{n+1}|$. Denotemos $\tilde{s} := s - s_0$. Por el *Teorema fundamental del cálculo*,

$$|v_n - v_{n+1}| = \left| \int_n^{n+1} \frac{d}{dt} t^{-\tilde{s}}\, dt \right| \leqslant \big((n+1) - n\big) \sup_{n \leqslant t \leqslant n+1} \left| \frac{-\tilde{s}}{t^{\tilde{s}+1}} \right| = \frac{|\tilde{s}|}{n^{1+\operatorname{Re}\tilde{s}}} \tag{7}$$

$$\sum_{n=N}^{\infty} |v_n - v_{n+1}| \leqslant |\tilde{s}| \sum_{n=N}^{\infty} \frac{1}{n^{1+\operatorname{Re}\tilde{s}}}$$

Y esta última serie sabemos que converge uniformemente sobre compactos en $\operatorname{Re}\tilde{s} > 0$.

La analiticidad sale de la Proposición 4.12. □

De la Prop. 4.12 también sale que la derivada se realiza término a término, resultando

$$f^{(k)}(s) = \sum \frac{a_n (-\log n)^k}{n^s}$$

Proposición 4.14 (Riemann, 1859)**.** *ζ admite una extensión meromorfa a $\{\operatorname{Re} s > 0\}$ con un único polo (simple) en $s = 1$.*

Demostración. Para $\operatorname{Re} s > 1$ tenemos

$$\zeta(s) - \frac{1}{s-1} = \sum_{n=1}^{\infty} \frac{1}{n^s} - \int_1^{\infty} \frac{1}{t^s} dt = \sum_{n=1}^{\infty} \left(\frac{1}{n^s} - \int_n^{n+1} \frac{1}{t^s} dt \right) = \sum_{n=1}^{\infty} \int_n^{n+1} \left(\frac{1}{n^s} - \frac{1}{t^s} \right) dt$$

Notar que $f_n := \int_n^{n+1} n^{-s} - t^{-s}$ son funciones analíticas en $\{\operatorname{Re} s > 0\}$. Queremos ver que $\sum f_n$ converge uniformemente sobre compactos para concluir que es analítica (Prop. 4.12). Esto lo logramos reciclando las cuentas hechas en (7):

$$|f_n| \leqslant \max_{n \leqslant t \leqslant n+1} |n^{-s} - t^{-s}| = |n^{-s} - (n+1)^{-s}| \leqslant \frac{|s|}{n^{1+\operatorname{Re} s}}$$

Luego, $\zeta = \frac{1}{s-1} + \sum f_n$ es suma de una función meromorfa en $\{\operatorname{Re} s > 0\}$ con un único polo (simple) en $s = 1$, y una función analítica en todo el semiplano abierto. □

Una intuición geométrica para entender lo que sigue es pensar el caso $k = p$. En este caso, las raíces de $\mathbb{G}_{p-1}$ vienen dadas de a pares ω, $-\omega$. De esta forma podemos partir la serie en $\frac{p-1}{2}$ series alternadas, cada una de las cuales debe converger. De hecho, hasta pensé que quizás podamos intuir la no anulación de $L(1, \chi)$ para ciertos caracteres particulares (cuando nos ayuda la simetría), partiendo 2 series en vez de en $\frac{p-1}{2}$, por ejemplo discriminando los ω según el signo de la parte imaginaria. Esta intuición se extiende al caso general a partir de la factorización de C_k^* como producto directo de grupos cíclicos.

Proposición 4.15. *Todo carácter de Dirichlet no principal se extiende analíticamente a $\{\operatorname{Re} s > 0\}$.*

Demostración. Extendemos el caractér χ a todo $\mathbb{Z}$ y aplicamos la Fórmula de sumación de Abel a $u_n = \chi(n)$ y $v_n = n^{-s}$. Por las relaciones de ortogonalidad (ver Teo. 4.7), U_n toma una cantidad finita de valores, por que podemos tomar $U = \max |U_n|$. Tenemos $U_n v_n \to 0$ y $\forall\ s > 0$ real se da la cota

$$\sum_{n=N}^{\infty} |U_n||v_n - v_{n+1}| \leqslant U \sum_{n=N}^{\infty} |v_n - v_{n+1}| = \frac{U}{N^s} \xrightarrow{N \to \infty} 0$$

O sea que la serie converge en todo s real positivo, y por ende en todo el semiplano abierto derecho siendo analítica allí (Teo. 4.13). □

En [5, p. 72], la demostración del siguiente teorema se acompaña de una pequeña ilustración sobre por qué podemos tomar una bola de radio mayor a 1.

Teorema 4.16 (Landau)**.** *Sea f una serie de Dirichlet con coeficientes $a_n \geqslant 0$ que converge en $\operatorname{Re} s > s_0 \in \mathbb{R}$ y admite una extensión analítica en un entorno de s_0. Entonces f converge en $\operatorname{Re} s > s_0 - \epsilon$ para algún $\epsilon > 0$.*

Demostración. Denotemos por $\tilde{f}$ a la extensión analítica de f. Por el Teorema de Cohen (4.13) y por hipótesis, $\tilde{f}$ es analítica en el semiplano $\operatorname{Re} s > s_0$ unido a una bola abierta centrada en s_0, y dicho conjunto contiene una bola de radio mayor a 1 centrada en $a := s_0 + 1$. O sea, existe un $\epsilon > 0$ tal que $\tilde{f}$ es analítica en $\{s \in \mathbb{C} : |s - a| < 1 + 2\epsilon\}$. Su serie de Taylor centrada en a es

$$\tilde{f}(s) = \sum_{k=0}^{\infty} \frac{f^{(k)}(a)}{k!}(s-a)^k = \sum_{k=0}^{\infty}\sum_{n=1}^{\infty} \frac{a_n(-\log n)^k}{k!\, n^a}(s-a)^k = \sum_{k=0}^{\infty}\sum_{n=1}^{\infty} \frac{a_n(\log n)^k}{k!\, n^a}(a-s)^k$$

Evaluando en $s = s_0 - \epsilon$, queda $a - s = 1 + \epsilon$ y

$$\tilde{f}(s_0 - \epsilon) = \sum_{k=0}^{\infty}\sum_{n=1}^{\infty} \frac{a_n(\log n)^k}{k!\, n^a}(1+\epsilon)^k$$

Como todos los términos de la serie son positivos, todas las convergencias son absolutas y por ende podemos reordenar los sumandos como queremos:

$$\tilde{f}(s_0 - \epsilon) = \sum_{n=1}^{\infty} \frac{a_n}{n^a} \sum_{k=0}^{\infty} \frac{\big((1+\epsilon)\log n\big)^k}{k!} = \sum_{n=1}^{\infty} \frac{a_n}{n^a} e^{(1+\epsilon)\log n} = \sum_{n=1}^{\infty} \frac{a_n}{n^a} n^{1+\epsilon} = \sum_{n=1}^{\infty} \frac{a_n}{n^{a-1-\epsilon}}$$

Esto último es la serie de Dirichlet evaluada en $a - 1 - \epsilon = s_0 - \epsilon$. Aplicando nuevamente el Teorema de Cohen, concluimos la prueba. □

4.5.3. Función zeta de Dedekind

Definición 4.5 (Función zeta de Dedekind módulo k)**.** $\forall\ \operatorname{Re} s > 1$,

$$\zeta_k(s) := \prod_{\chi \in \widehat{C_k^*}} L(s, \chi)$$

Observación 4.17. $\forall\ z \in \mathbb{C}$,

$$\prod_{w \in \mathbb{G}_k} (1 - wz) = 1 - z^k$$

Demostración. Los elementos de $\mathbb{G}_k$ vienen de a pares conjugados, salvo 1 y eventualmente -1 (si k es par). El producto de dos conjugados da $w\overline{w} = |w|^2 = 1$. Por otro lado, recorrer los inversos de $\mathbb{G}_k$ equivale a recorrerlos sin invertirlos. Luego,

$$\prod_w (1 - wz) = \left(\prod_w w\right) \prod_w \left(\frac{1}{w} - z\right) = (-1)^{k-1} \prod_w (w - z) = (-1)^{2k-1}(z^k - 1)$$

donde la última igualdad proviene de la factorización del polinomio $z^k - 1 \in \mathbb{C}[x]$. □

Dado p un primo que no divide a m, denotamos por $\overline{p}$ a su reducción de p módulo d, y por $|\overline{p}|$ al orden de $\overline{p} \in C_k^*$.

Observación 4.18. *Si $p \nmid d$ entonces*

$$\prod_{\chi \in \widehat{C_k^*}} \left(1 - \frac{\chi(p)}{p^s}\right) = \left(1 - \frac{1}{p^{|\overline{p}|s}}\right)^{\varphi(k)/|\overline{p}|}$$

Demostración. Denotemos $\alpha = \varphi(k)/|\overline{p}|$. Aplicar la Observación 4.17 a $z = p^{-s}$ y observar que cada $w = \chi(p) \in \mathbb{G}_{|\overline{p}|}$ se repite α veces. En efecto, si c es un generador de $\widehat{C_k^*}$, entonces $\overline{p} = c^\alpha$ y dado un tal w, el polinomio

$$z^\alpha - w = w\left(\left(\frac{z}{w^{1/\alpha}}\right)^\alpha - 1\right) \in \mathbb{C}[X]$$

tiene α raíces, cada una de las cuales es un posible $\chi(c)$. □

Observación 4.19. $\forall\ \operatorname{Re} s > 1$,

$$\zeta_k(s) \;=\; \prod_{p \nmid k} \left(\frac{1}{1 - p^{-|\overline{p}|s}}\right)^{\varphi(k)/|\overline{p}|} \;\geqslant\; L\big(\varphi(k)s, 1\big)$$

Demostración. Recordar el producto de Euler (Teorema 4.1) y que la productoria infinita es un límite. Como el producto finito (indexado por χ) de los límites es el límite del producto, y por la Observación 4.18, tenemos

$$\begin{aligned}\zeta_k(s) &= \prod_{\chi} \prod_{p \nmid k} \frac{1}{1 - \frac{\chi(p)}{p^s}} = \prod_{p \nmid k} \prod_{\chi} \frac{1}{1 - \frac{\chi(p)}{p^s}} = \prod_{p \nmid k} \left(\frac{1}{1 - p^{-|\overline{p}|s}}\right)^{\varphi(k)/|\overline{p}|} \\ &\geqslant \prod_{p \nmid k} \frac{1}{1 - p^{-|\overline{p}|s}} \geqslant \prod_{p \nmid k} \frac{1}{1 - p^{-\varphi(k)s}} = L\big(\varphi(k)s, 1\big)\end{aligned}$$

□

Como esta última diverge en $s = \frac{1}{\varphi(k)}$, esperamos que ζ_k no tenga una extensión analítica al semiplano $\{s \in \mathbb{C} : \operatorname{Re} s > 0\}$. Será útil lo siguiente.

Proposición 4.20. *ζ_k es una serie de Dirichlet con coeficientes reales no negativos.*

Demostración. ζ_k es producto de series de Dirichlet con coeficientes $\geqslant 0$ de la forma

$$\frac{1}{1 - p^{-|\overline{p}|s}} = \sum_{n=0}^{\infty} \left(p^{-|\overline{p}|s}\right)^n = \sum_{n=0}^{\infty} \frac{1}{\left(p^{n|\overline{p}|}\right)^s}$$

Solo queda argumentar que el producto de series de Dirichlet (con coeficientes no negativos) es una serie de Dirichlet (con coeficientes no negativos). Esto se puede ver con argumentos muy elementales y familiares, aunque densos de escribir, la idea sería ver que el producto de dos series d Dirichlet vuelve a ser una serie de Dirichlet, y pensar a la productoria infinita como un límite de productos finitos.

El procedimiento anterior garantiza que los coeficientes de ζ_k sean no negativos. Dado un punto s_0 en el interior de la intersección de los dominios de las series, veremos que localmente (en un entorno de s_0). □

Proposición 4.21. *ζ_k tiene una extensión meromorfa a $\{\operatorname{Re} s > 0\}$ con único polo (simple) en $s = 1$.*

Demostración. Todos los factores de la productoria que definen a ζ_k tienen una extensión analítica a $\{s \neq 1 : \operatorname{Re} s > 0\}$, por ende ζ_k también. Si ζ_k fuese analítica también en $s = 1$, lo sería en todo el semiplano $\{\operatorname{Re} s > 0\}$. Y como ζ_k es una serie de Dirichlet con coeficientes no negativos, debe converger en todo el semiplano (Teo. 4.16), contradiciendo que $\zeta_k \geqslant L\big(\varphi(k)s, 1\big)$. □

Corolario 4.22. *$L(1, \chi) \neq 0 \ \forall \ \chi \neq 1$.*

Demostración. $L(s, \chi)$ es analítica en $\{s \in \mathbb{C} : \operatorname{Re} s > 0\} \ \forall \ \chi \neq 1$ (Prop. 4.15). Por otro lado, $L(s, 1)$ tiene una extensión meromorfa a dicho semiplano con un polo simple en $s = 1$. De lo caso contrario ζ_k sería analítica en todo el semiplano, no teniendo un polo en $s = 1$. □

5. Demostraciones euclidianas

Un punto a favor de las pruebas que veremos es que son constructivas, nos dan una sucesión explícita (aunque probablemente demasiado creciente) de primos con la condición que queremos, y los podemos calcular.

5.1. Los primeros casos particulares

Para esto, fue útil [1, § 7.3] complementado con la Introducción del artículo [22].

Probablemente sin ser él consciente, el caso mas trivial ya lo sabía Euclides en el siglo III a.C., y es que tomando $m = k = 1$, el enunciado equivale a la infinitud de los números primos. Lo mismo ocurre para $k = 2, m = 1$.

Caso 5.1 (casos triviales: $m = 1$ y $k = 2$)**.** *Existen infinitos primos.*

Demostración. Primero tomamos un conjunto finito de primos y tomamos x igual al producto de todos ellos. Luego, $x + 1$ debe ser divisible por un primo distinto. Como esto vale para todo conjunto finito de primos, entonces estos números deben ser infinitos. □

Así, conectamos las progresiones aritméticas con las ideas de Euclides. Esta observación aparentemente ornamental, en realidad expone una forma de plantear el problema: adaptando la prueba de Euclides, podemos demostrar el Teorema de Dirichlet fácilmente para algunos casos particulares. Por ejemplo, si $\varphi(k) = 2$ (donde φ es la *Función phi de Euler*, que a cada número natural le asocia la cantidad de números coprimos menores que él), notar que m solo puede ser congruente a 1 o $k - 1$.

Caso 5.2 ($\varphi(k) = 2$, $m = k - 1$)**.** *Si $\varphi(k) = 2$, existen infinitos primos $p \equiv -1 \pmod{k}$.*

Demostración. Dado un conjunto finito P de primos congruentes a $m = k - 1$ módulo k, tomamos

$$N = m + k \prod_{p \in P} p$$

(si preocupa el caso $P = \emptyset$, usar la convención de productoria vacía igual a 1) y observamos que los primos que dividen a N son coprimos con k, no están en P, y no pueden ser todos

congruentes a 1 módulo k, pues de lo contrario $-1 \equiv m \equiv N \equiv 1 \,(\mathrm{mod}\, k)$, lo cual es absurdo porque $k > 2$. Por lo tanto existe un primo p que divide a N y tal que $P \not\ni p \equiv m \,(\mathrm{mod}\, k)$. □

Notas:

1. El número m que tomamos en la prueba, crece demasiado conforme crece el conjunto P, por lo que el nuevo primo que encontramos puede ser mucho mas grande que que el menor primo congruente a m módulo k que no está en P.

2. En lugar de tomar $N = \prod_{p \in P} p$ podríamos haber usado un número mas bruto, por ejemplo $N!$, donde N es una cota superior de P. Para simplificar la escritura, suele ser útil usar $N!$ sin siquiera nombrar el conjunto P (como haremos en el Caso 5.3). Podríamos pensar que este cambio puede hacer que el nuevo primo que encontremos sea aún mas grande, perdiendo noción sobre la frecuencia con la que estos aparecen, pero en realidad siempre podemos recordar que de hacer falta, podemos usar un conjunto P en la misma prueba.

Entonces tenemos resuelto el problema para $k \in \{1, 2\} = \varphi^{-1}(1)$, y parcialmente para $k \in \{3, 4, 6\} = \varphi^{-1}(2)$, de forma puramente algebraica. Al preguntarnos si por este camino podemos avanzar, rápidamente nos encontramos con un obstáculo: viendo el grupo de unidades de $\mathbb{Z}_k$ notamos que para cualquier otro par (k, m), los primos que dividen a N podrían no ser congruentes a m, ya que $m \in \mathbb{Z}_k^*$ puede escribirse como producto de unidades distintas a m. Por ejemplo, si $k = 4, m = 1$ y P es un conjunto finito de primos congruentes a m, entonces los números de la forma

$$\pm 1 + 4\,\mu \prod_{p \in P} p$$

en principio podrían tener a todos sus factores primos congruentes a -1, aunque eso parezca bastante sospechoso. Haciendo uso del *Pequeño Teorema de Fermat*, podemos superar esta dificultad en algunos casos.

Caso 5.3 ($k = 4$, $m = 1$)**.** *Existen infinitos primos* $p \equiv 1 \,(\mathrm{mod}\, 4)$.

Demostración. Dado N, queremos encontrar un primo p tal que $N < p \equiv 1 \,(\mathrm{mod}\, 4)$. Si $p > N$, entonces no divide a $N!$, y por lo tanto $(N!)^{p-1} \equiv 1 \,(\mathrm{mod}\ \mathrm{p})$. Por otro lado, como $\frac{p-1}{2}$ es par, tenemos $(-1)^{\frac{p-1}{2}} = 1$. En resumen,

$$(N!)^{2\frac{p-1}{2}} = (N!)^{p-1} \equiv 1 \equiv (-1)^{\frac{p-1}{2}} \,(\mathrm{mod}\ \mathrm{p})$$

lo cual nos hace pensar en que podemos buscar un p tal que $(N!)^2 \equiv -1 \,(\mathrm{mod}\ \mathrm{p})$, es decir un factor primo de $m = (N!)^2 + 1$. Eligiendo p de esta forma, si $N > 1$, tenemos que p es impar, y siguiendo las cuentas anteriores vemos que $(-1)^{\frac{p-1}{2}} \equiv 1 \,(\mathrm{mod}\, p)$, con lo cual $p \equiv 1 \,(\mathrm{mod}\, 4)$. □

Argumentos muy similares al del Caso 5.3 podemos usar para ver la infinitud de primos en otras progresiones aritméticas como $5\mu - 1$, $8\mu - 1$, $8\mu - 3$ o $8\mu + 3$ [1, p. 185]. Para avanzar un paso mas con estas ideas que vimos, hará falta añadir técnicas nuevas, aunque siguen siendo elementales.

5.2. Caso particular $m = 1$

Aquí probaremos el teorema de forma puramente algebraica y para una cantidad infinita de progresiones aritméticas: las de la forma $\mu k + 1$ con k arbitrario.

Los preliminares para este apartado se ven en un curso de *Estructuras Algebraicas*, pero afortunadamente son sencillos de explicar en palabras. Un libro estándar para seguir es *Algebra* de Thomas W. Hungerford [28]. Concretamente, necesitamos saber que $\mathbb{Q}[X]$ es un DFU. Esto significa que el anillo $\mathbb{Q}[X]$ satisface dos cosas:

1. Es un *dominio íntegro*. Es decir, el producto es conmutativo y no existe un par de elementos (en este caso son polinomios) tal que multiplicarlos me de cero.

2. Los elementos que no son cero ni una unidad (unidad significa que tiene inverso multiplicativo) admiten factorización en irreducibles (irreducible significa que no puede factorizarse como producto de dos elementos que nos son unidades) única salvo unidad. Es decir, dado $f \in \mathbb{Q}[X]$, si $f = p_1 \cdots p_r$ y $f = q_1 \cdots q_r$ son dos factorizaciones en irreducibles, entonces salvo el orden, se cumple que existen unidades $u_1, \ldots, u_r \in \mathbb{Q}[X]^*$ tal que $q_i = p_i u_i$ para todo $i = 1, \ldots, r$.

Para las definiciones anteriores siempre es útil hacer un paralelismo con $\mathbb{Z}$.

Para § 5.2.1 y § 5.2.2 fue muy útil el artículo [22].

Inspirados en el Caso 5.3 podemos ver una forma de encontrar primos como los que estamos buscando. En esta sección, $\mathbf{N}$ será un número natural. Usamos esta notación para recordarnos que en general será un número grande que depende de N, precisamente, nos interesará cuando sea un múltiplo de $N!$.

5.2.1. Nos socorren los polinomios ciclotómicos

Observación 5.1. *Si* $\mathbf{N}^k \equiv 1 \pmod{p}$*, entonces* $\mathbf{N}$ *y* p *son coprimos y* $\mathbf{N}^{p-1} \equiv 1 \pmod{p}$*. De esto nos gustaría concluir que* $k \mid p-1$*, o sea* $p \equiv 1 \pmod{k}$*. Si además,* $\mathbf{N}$ *es un múltiplo de* $N!$*, nos aseguramos que* $p > N$*.*

Lema 5.2. *Sean* k*,* $\mathbf{N}$ *y* p *tal que* $p \mid \mathbf{N}^k - 1$ *y* $p \nmid \mathbf{N}^d - 1$ $\forall$ d *divisor propio de* k*, entonces* $k \mid p-1$*.*

Demostración. Como $p \nmid \mathbf{N}$, tenemos $\mathbf{N}^{p-1} \equiv 1 \pmod{p}$. Sea $d = \operatorname{mcd}(k, p-1)$, veamos que $d = k$, y así $k \mid p-1$. Tomamos una combinación lineal entera $d = tk + s(p-1)$, y así $\mathbf{N}^d = (\mathbf{N}^k)^t (\mathbf{N}^{p-1})^s \equiv 1 \pmod{p}$. Por hipótesis del enunciado, d no puede ser menor a k, por ende $d = k$. □

Nota: Para el que sabe Teoría de grupos, una demostración alternativa sale observando que bajo esas hipótesis, el orden de $\overline{\mathbf{N}} \in \mathbb{Z}_p^*$ debe ser k, y por lo tanto $k \mid |\mathbb{Z}_p^*| = p-1$.

Al interesarnos $X^k - 1$ y $X^d - 1$ módulo p, parece buena idea estudiar dichos polinomios. Sean $\mathbb{G}_k \subset \mathbb{C}$ el conjunto de las raíces k-ésimas, y $\mathbb{G}_k^* \subset \mathbb{G}_k$ el conjunto de las primitivas, entonces hay una expresión como unión disjunta

$$\mathbb{G}_k = \bigsqcup_{1 \leqslant d \mid k} \mathbb{G}_d^*$$

Definición 5.1. *El k-ésimo polinomio ciclotómico se define como*

$$\Phi_k = \prod_{\xi \in \mathbb{G}_k^*} (X - \xi)$$

Con estos ingredientes, en $\mathbb{C}$ se tiene la factorización

$$X^k - 1 = \prod_{1 \leqslant d \,|\, k} \Phi_d$$

La siguiente propiedad se basa en que si $f, g \in \mathbb{Z}[X] \subset \mathbb{C}[X]$ con g mónico y $g \mid f$ en $\mathbb{C}[X]$, entonces $\frac{f}{g} \in \mathbb{Z}[X]$. Esto es evidente a partir del algoritmo recursivo clásico de la división de polinomios. Nos será útil denotar

$$\Gamma_k = \prod_{\substack{d \,|\, k \\ 1 \leqslant d < k}} \Phi_d = \frac{X^k - 1}{\Phi_k}$$

Lema 5.3. $\Phi_k \in \mathbb{Z}[X] \ \ \forall k$.

Demostración. Hacemos inducción fuerte en k. El caso base $k = 1$ es $\Phi_1 = X - 1$. Suponiendo que vale para todos los naturales menores a $k > 1$, entonces $\Gamma_k \in \mathbb{Z}[X]$ y es mónico por ser producto de mónicos, por lo tanto $\Phi_k = \frac{X^k - 1}{\Gamma_k} \in \mathbb{Z}[X]$. □

Observación 5.4. *$p \mid \mathbf{N}^d - 1$ para algún d divisor propio de k $\Leftrightarrow$ $p \mid \Phi_d(\mathbf{N})$ para algún d divisor propio de k $\Leftrightarrow$ $p \mid \Gamma_k(\mathbf{N})$.*

Debido a los resultados recopilados hasta ahora en la sección, nos interesa encontrar un $\mathbf{N}$ múltiplo de $N!$ y un primo que divida a $\mathbf{N}^k - 1$ sin dividir a $\Gamma_k(\mathbf{N})$, por lo que debe dividir a $\Phi_k(\mathbf{N})$. Si $\mathbf{N} > 2$, el siguiente resultado junto con el Lema 5.3 garantizan la existencia de un primo que divide a $\Phi_k(\mathbf{N})$, por ser este un natural mayor a 1.

Lema 5.5. *Φ_k es estrictamente creciente en $[1, \infty)$ $\forall\, k$. Además, $\Phi_k(1) \geqslant 0$.*

Demostración. Si k es 1 o 2, es claro porque $\Phi_1 = X - 1$ y $\Phi_2 = X + 1$. Supongamos entonces que $k > 2$. Como las únicas raíces reales de la unidad son 1 y -1, las raíces de Φ_k vienen de a pares conjugados. Es decir, Φ_k es producto de cosas de la forma $(X - \xi)(X - \overline{\xi})$. Si $X \in \mathbb{R}$, $(X - \xi)(X - \overline{\xi}) = (X - \xi)\overline{(X - \xi)} = |X - \xi|^2$ es estrictamente creciente en $[\mathrm{Re}(\xi), \infty) \subset [1, \infty)$. Por lo tanto Φ_k en $[1, \infty)$ es producto de funciones estrictamente crecientes y positivas. □

Como necesitamos que el primo divida a $\Phi_k(\mathbf{N})$ sin dividir a $\Gamma_k(\mathbf{N})$, sería útil dar alguna relación aritmética entre Φ_k y Γ_k. Como estos polinomios no comparten raíces en $\mathbb{C}$, deben ser coprimos en el DFU $\mathbb{Q}[X]$, así que existe una combinación lineal en $\mathbb{Q}[X]$

$$1 = f\Phi_k + g\Gamma_k$$

Tomando $n \in \mathbb{N}$ el mínimo común múltiplo entre todos los denominadores de f y g, resulta que $F := nf$ y $G := ng$ tienen coeficientes enteros, así que la igualdad

$$n = F\Phi_k + G\Gamma_k \tag{8}$$

se da en $\mathbb{Z}[X]$.

Observación 5.6. *Si* $p \mid \Phi_k(\mathbf{N})$ *entonces* $p \nmid \mathbf{N}$. *Si además* $p \nmid n$, *tenemos* $p \equiv 1 \pmod{k}$.

Demostración. La primera parte es obvia, pues $p \mid \Phi_k(\mathbf{N})\Gamma_k(\mathbf{N}) = \mathbf{N}^k - 1$, así que $p \nmid \mathbf{N}$.
Si además $p \nmid n$, evaluando en $\mathbf{N}$ la igualdad (8) obtenemos la igualdad en $\mathbb{Z}$

$$n = F(\mathbf{N})\Phi_k(\mathbf{N}) + G(\mathbf{N})\Gamma_k(\mathbf{N})$$

Luego, p no puede dividir a $\Gamma_k(\mathbf{N})$. Por la Obs. 5.4 y el Lema 5.2, $p \equiv 1 \pmod{k}$. □

Deducimos inmediatamente que si $p \mid \Phi_k(\mathbf{N})$ y $n \mid \mathbf{N}$, entonces $p \equiv 1 \pmod{k}$.

Caso 5.4 ($m = 1$)**.** $\forall\, k$, *existen infinitos primos* $p \equiv 1 \pmod{k}$.

Demostración. Si $N > 2$, tomamos $\mathbf{N} = nN! > 2$ y un primo p que divide a $\Phi_k(\mathbf{N})$. Así, $N < p \equiv 1 \pmod{k}$. □

5.2.2. Ejemplos y aplicaciones

El procedimiento anterior funciona para todo k, generando primos distintos. Al igual que en los casos 5.2 y 5.3, esto rápidamente arroja primos bastante grandes. Sin embargo, haciendo uso de la Observación 5.6, para algunos valores de k podemos obtener además otros primos mas pequeños.

Ejemplo 5.1 ($k = 12$, $m = 1$)**.** $p \equiv 1 \pmod{12}$ $\forall\ \mathbf{N} > 1$, $p \mid \Phi_{12}(\mathbf{N})$.

Demostración. Primero calculemos los polinomios involucrados:

$$\Phi_1 = X - 1, \qquad \Phi_2 = X + 1, \qquad \Phi_3 = \frac{X^3 - 1}{\Gamma_3} = X^2 + X + 1$$

$$\Phi_4 = \frac{X^4 - 1}{\Gamma_4} = X^2 + 1, \qquad \Phi_6 = \frac{X^6 - 1}{\Gamma_6} = X^2 - X + 1$$

$$\Gamma_{12} = X^8 + X^6 - X^2 - 1, \qquad \Phi_{12} = \frac{X^{12} - 1}{\Gamma_{12}} = X^4 - X^2 + 1$$

El algoritmo de Euclides para estos polinomios nos lleva a la igualdad (8) con

$$F = -X^6 + 3X^2 + 4, \qquad G = X^2 - 2, \qquad n = 6$$

Por la Observación 5.6, basta ver que ni 2 ni 3 (que son los factores primos de k) dividen a $\Phi_{12}(\mathbf{N})$, lo cual sale de que ambos dividen a $\mathbf{N}^2(\mathbf{N}^2 - 1) = \mathbf{N}^4 - \mathbf{N}^2 = \Phi_{12}(\mathbf{N}) - 1$. □

Si queríamos asegurarnos de obtener primos distintos, hacíamos lo siguiente:

1. *Evaluamos* $\Phi_{12}(n) = \Phi_{12}(6) = 20\,593$, *sabiendo que todos sus factores primos son congruentes a* 1 *módulo* 12. *Como él mismo es primo, tomamos* $p_1 = 20\,593$.

2. *Para obtener primos nuevos, evaluamos* $\Phi_{12}(np_1) = 3\,729\,095\,127\,575\,903\,994\,481$, *sabiendo que sus factores primos deben ser todos distintos de* p_1. *En este caso, dichos factores son* 341 *y* 10 685 086 325 432 389 669.

O sea que de esta forma, los primeros tres primos que encontramos son 20 593, 341 *y* 10 685 086 325 432 389 669. *Pero por lo que probamos recién, nos sirven todos los factores primos de* $\Phi_{12}(\mathbf{N})$ $\forall\ \mathbf{N} > 1$. *Es así como para* $1 < \mathbf{N} \leqslant 10$ *obtenemos los primos* 13, 73, 241, 601, 97, 181, 37, 109, 6481 *y* 9901.

Otra consecuencia de la Observación 5.6 tiene que ver con los *números de Mersenne*, que son los de la forma $M_n = 2^n - 1$ con $n \in \mathbb{N}$. Los factores primos de $M_4 = 15$ son congruentes a -1 y 1 módulo 4. Veamos una propiedad clásica: cuando n es primo, todos los factores primos de M_n son congruentes a 1 módulo n.

Aplicación 5.2 (Números de Mersenne)**.** *Si q es primo, $p \equiv 1 \pmod{q}$ $\forall$ $p \mid M_q$.*

Demostración. Si $q = 2$, $2^q - 1 = 3$ es un primo congruente a 1 módulo q. Supongamos ahora que $q > 2$. $\Gamma_q = X - 1$ y $\Phi_q = \frac{X^q - 1}{\Gamma_q} = \sum_{i=0}^{q-2} X^i$. La igualdad (8) se da con

$$F = 1, \qquad G = \sum_{i=0}^{q-1} (q - 1 - j)X^i, \qquad k = q$$

Por el *Pequeño Teorema de Fermat*, $2^q \equiv 2 \pmod{q}$, por ende

$$\Phi_q(2) = (2^q - 1)\Gamma_q(2) = 2^q - 1 \equiv 1 \pmod{q}$$

es coprimo con $k = q$. Por la Observación 5.6, todo primo que divide a $\Phi_q(2) = 2^q - 1 = M_q$ es congruente a 1 módulo q. □

En realidad, de forma elemental y sin este lenguaje, se puede ver que si $q > 2$, entonces todo diviso primo $p \mid M_q$ satisface $p \equiv 1 \pmod{2q}$.

La última aplicación que veremos en esta sección es sobre los *números de Fermat*, que son los de la forma $F_n = 2^{2^n} + 1$.

Aplicación 5.3 (Números de Fermat)**.** $p \equiv 1 \pmod{2^{n+1}}$ $\forall$ $p \mid F_n$.

Demostración. Para evitar solapar notación, aquí llamenos $\tilde{n}$ al miembro izquierdo de la igualdad (8). Es directo, por inducción en n, que

$$\Gamma_{2^{n+1}} = X^{2^n} - 1 \qquad \text{y} \qquad \Phi_{2^{n+1}} = X^{2^n} + 1$$

Así, es directo que la igualdad (8) se satisface con $F = 1$, $G = -1$ y $\tilde{n} = 2$. La Observación 5.6 dice que todo primo que divide a $\Phi_{2^{n+1}}(2) = F_n$ es congruente a 1 módulo 2^{n+1}. □

5.3. Comentando los teoremas de Schur y Murty

Con espíritu euclidiano hemos demostrado el *Teorema de Dirichlet* $\forall$ $k \in \{1, 2, 3, 4, 6\}$. Y para el resto de los $k \in \mathbb{N}$ lo tenemos de forma parcial (solo el caso $m = 1$).

Definición 5.2 (Demostración euclidiana)**.** *Una demostración euclidiana es una demostración de la infinitud de primos en una progresión aritmética $\mu k + m$ que procede de la siguiente manera:*

- *Se da un conjunto finito P de primos en la progresión aritmética $\mu k + m$.*
- *Se construye un entero M que es un polinomio en $x := \prod_{p \in P} p$*
- *M tiene que ser mayor a 1 y coprimo con x.*
- *M debe tener al menos un divisor primo en la progresión aritmética $\mu k + m$.*

Schur da el primer paso, y varias décadas después Murty remata nuestras preguntas.

Teorema 5.7 (Schur, 1912)**.** *Si* $m^2 \equiv 1 \pmod{k}$*, existe una demostración euclidiana.*

Teorema 5.8 (Murty, 1988)**.** *Solo existe una dem. euclidiana en los casos* $a^2 \equiv 1 \pmod{d}$*.*

Si ya el caso $m = 1$ costó algo de trabajo, podrán imaginarse que la prueba de Murty excede los limites de esta monografía, por muchas ganas que me guarde. Para quien esté interesado, en [25] Murty y Thain revisa [23] y [24], lo cual es muy útil porque estos últimos dos no parecen estar muy disponibles. El artículo [26] de K. Conrad es un excelente complemento.

Como mencionamos en la parte histórica, en [25] también buscan generalizar estos resultados a otros contextos mas abstractos.

6. Conclusiones

El Teorema de Dirichlet funda la Teoría Analítica de Números, además de impulsar diferentes áreas de la matemática.

Las similitudes en las pruebas de este Teorema de Dirichlet parecen compartir la misma esencia. Además, las pruebas puramente algebraicas que se intentaron tienen una limitación a casos particulares bien definidos, aunque tienen un buen contrapeso al ser constructivas y bellas. Esto me hace cuestionarme que, sorprendentemente, la historia parece haberse declinado en el único camino posible, como si las leyes matemáticas formaran un surco pedregoso que la líquida mente humana inevitablemente tiene que recorrer. O quizás haya varios surcos que se toquen, y en un futuro tengamos una nueva revelación.

"Las leyes de la naturaleza no son más que los pensamientos matemáticos de Dios."

Euclid (circa 300 b.C.)

Por otro lado, resultados como el Teorema de Números Primos en Progresiones Aritméticas muestra una dualidad entre desorden y regularidad de estos números. El Teorema de Densidad de Chebotarev muestra que esta regularidad se eleva a estructuras superiores.

Otra conclusión interesante es que el lenguaje de una época parece limitar sus capacidades. Como dije en su sección correspondiente, esta es la sensación que me dio al leer a Euler. En los siglos posteriores se vio una gran evolución en este sentido, el último cambio de paradigma que se me viene a la mente es el de la *Teoría de Categorías*. Es inevitable pensar ¿cuáles serán nuestras limitaciones?

Para terminar, la refinación y abstracción del teorema, así como el Teorema de Murty y su abstracción, llevaron el entendimiento de los primos en progresiones aritméticas a un estado posiblemente mayor de lo que pudieron haber especulado Dirichlet y sus antecesores.

7. Una miscelánea

Uno de las cuatro conjeturas "inabarcables en el estado actual de la ciencia" mencionados Edmund Landau en 1912: *Existen infinitos primos de la forma* $n^2 + 1$.

Referencias

[1] Apostol, Tom M. (1976). *Introduction to Analytic Number Theory*. Springer-Verlag. ISNB (New York): 0-387-90163-9. ISNB (Berlin-Heidelberg): 3-540-90163-9.

[2] Michael Sean Mahoney. *The Mathematical Career of Pierre de Fermat*.

[3] Ian Stewart (2008). *Historia de las Matemáticas en los últimos 10.000 años*. Crítica.

[4] Dickson, Leonard Eugene (1919). *History of the Theory of Numbers* (3 volumes). Washington, D. C.: Carnegie Institution of Washington. Reprinted by Chelsea Publishing Co., New York, 1966.

[5] Carlos Ivorra Castillo. *Teoría analítica de números*.

[6] Euler, Leonhard (1737). *Variae observationes circa series infinitas*. Commentarii Academiae Scientiarum lmperialis Petropolitane. 9 (1744), 1737, 160-188. [Opera Omnia I, 14; 216- 244]. E72 en la clasificación de Enestrom.

[7] Felipe Zaldívar (mayo 2008). *Productos de Euler*. Miscelánea Matemática. n°46 (2008) 49-72. ISSN-1665-5478.

[8] Fernando Chamizo Lorente (2007). *Euler y la Teoría de números*. Gaceta de la Real Sociedad Matemática Española. ISSN 1138-8927, Vol. 10, N°2, 2007, págs 407-426.

[9] Sergi Sanjuan Silvestre (2022). Trabajo fin de grado: *De los teoremas de Mertens a la Hipótesis de Riemann*

[10] Legendre, Adrien Marie. *Théorie des Nombres*. Paris, Didot, $3^{\text{ième}}$ ed. ? 1830, $4^{\text{ième}}$ Partie. §. IX.

[11] Dirichlet, P. G. Lejeune (1837) Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschlaftichen Factor sind, unendliche viele Primzahlen enthält. *Abhand. Ak. Wiss.*

[12] Johann Peter Gustav Lejeune Dirichlet Dirichlet. Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält. *Abhandlungen der königlich Preussischen Akademie der Wissenschaften*, pages 45–81, 1837. Reprinted in [25], pages 313– 342. Translated by Ralf Stefan as "There are infinitely many prime numbers in all arithmetic progressions with first term and difference coprime," arXiv:0808.1408

[13] Jeremy Avigad and Rebecca Morris (2014). *The concept of "character" in Dirichlet's theorem on primes in an arithmetic progression*.

[14] Gauss, Carl Friedrich. *Disquisitiones arithmeticae*. Lipsiae, Fleischer, 1801. art. 357.

[15] Carl F. Gauss. *Disquisitiones arithmeticae*. Traducción al castellano: Hugo Barrantes Campos, Michael Josephy y Angel Ruiz Zúñiga (1995). Santa Fé de Bogotá, D.C.

[16] John B. Conway (1978). *Funtions of One Complex Variable*. Springer-Verlag. Second Edition.

[17] Antonio Ismael Cano Mármol (2018). Trabajo Fin de Grado: *Análisis de Fourier en grupos*. Universidad de Murcia.

[18] Anthony Várilly. *Dirichlet's Theorem on Arithmetic Progressions*.

[19] Thai Pham (2012). *Dirichlet's Theorem on Arithmetic Progressions*.

[20] Garrett, Paul (2011). Primes in arithmetic progressions.

[21] Emilio Lauret. *Series de Dirichlet*.

[22] Sabia, J., & Tesauri, S. (2008). *Un caso particular del teorema de Dirichlet*. Revista De Educación Matemática, 23(2). URL: https://doi.org/10.33044/revem.10418.

[23] I. Schur, *Uber die Existenz unendlich vieler Primzahlen in einiger speziellen arithmetischen Progressionen*, S-B Berlin. Math. Ges., 11 (1912), 40–50.

[24] M.R. Murty, *Primes in Certain Arithmetic Progressions*, J. Madras Univ., Section B, 51 (1988), 161–169.

[25] M. R. Murty and N. Thain, *Primes in certain arithmetic progressions*, Funct. Approx. Comment. Math. 35 (2006), 249–259.
URL: https://projecteuclid.org/euclid.facm/1229442627.

[26] Keith Conrad (2010). *Euclidean proof of Dirichlet's theorem*.
URL: https://api.semanticscholar.org/CorpusID:9231577.

[27] Romeo Meštrović. *Euclid's theorem on the infinitude od primes: a historical survey of its 200 proofs (300 b.C.–2022)*. arXiv:1202.3670v4.

[28] Thomas W. Hungerford. *Algebra*. Graduate Texts in Mathematics. Springer. ISNB: 0387905189.

[29] Nieven, Ivan, & Zuckerman, Herbert S. (1966). *An Introduction to the Theory of Numbers*. John Wiley & Sons, Inc. ISNB 10: 0471641537. ISNB 13: 9780471641537.

[30] Le Veque, W. J. (1974). *Reviews in Number Theory* (6 volumes). Providence, RI: American Mathematical Society.