FACULTAD
DE
CIENCIAS

DEMOSTRANDO LA INFINITUD DE LOS NÚMEROS PRIMOS

(Proving the Infinitude of Primes)

Trabajo de fin de Grado
para acceder al

GRADO EN MATEMÁTICAS

Autor: Carlos Rodríguez San Emeterio

Director: Daniel Sadornil Renedo

Junio-2017

Índice general

Resumen:

Uno de los temas más estudiados a lo largo de la historia de las matemáticas ha sido la infinitud de los números primos, cuya primera demostración fue elaborada por Euclides en el siglo III a.C.. Desde esa fecha hasta nuestros días, han sido propuestas cientos de demostraciones, abordando el teorema desde diferentes áreas de las matemáticas. En este trabajo recogeremos algunas demostraciones, viendo las similitudes y diferencias que existen entre ellas.

Palabras clave: Primos, Demostración, Euclides.

Abstract:

One of the most studied subjects throughout the history of mathematics has been the infinitude of prime numbers, proof of which was first made by Euclid in the third century B.C.. From that date until today, hundreds of proofs have been proposed, approaching the theroem from different areas of the mathematics. In this work, we will analyse some of these proofs and we will compare their similarities and differences.

Key words: Primes, Proof, Euclid.

Capítulo 1

Introducción

Las matemáticas son una de las ciencias que ha acompañado al ser humano a lo largo de toda su historia. Una de las primeras inquietudes fue la numeración, es decir, el ser capaz de contar. Inicialmente sólo se consideraron los números 1, 2, 3,..., los que actualmente llamamos números naturales. Una vez definidos los números, se empezó a hacer operaciones sencillas con ellos: sumas, restas, multiplicaciones y divisiones (repartos). En la Antigua Grecia, aunque se desconoce si antes también, ya se dieron cuenta de que había números con propiedades especiales respecto a la divisibilidad. Estos números son los que actualmente llamamos números primos.

Definición. Llamamos números primos a aquellos enteros positivos que solamente son divisibles por sí mismos y por el 1.

Esta definición es la que todos aprendemos en la escuela, además, en ocasiones, a partir de ella, se incluye al número 1 como primo; pues es divisible por 1 y por sí mismo. En realidad, el 1 era considerado como primo hasta el siglo XIX, donde este hecho empezó a cuestionarse y dejó de aparecer en las listas de números primos. Para ver más información consultar [5].

Gracias a los primeros textos griegos, sabemos que en esa época ya se estudiaban y se trataban de demostrar, con mayor o menor fortuna, distintas hipótesis y enunciados, entre ellos algunos relativos a números primos. Uno de los matemáticos a resaltar en esta época fue Euclides, quien escribió una de las obras más importantes del mundo griego, *Los Elementos*, en el siglo III a.C.. Dicho tratado es una recopilación de los conocimientos matemáticos de la época. Consta de trece libros en los que encontramos tanto definiciones, como proposiciones y sus demostraciones. A nivel histórico, como muchos textos griegos, fue traducido primero en Oriente, y posteriormente al latín, sobre el siglo XII. Actualmente, es uno de los libros de texto más traducido y utilizado, ya que, a lo largo de la historia, era obligatorio su estudio en numerosas universidades de distintos países. Destacar que es el segundo libro más editado de la historia, sólo por detrás de la Biblia. En su interior encontramos tanto el enunciado como una demostración del tema que vamos a tratar en este trabajo, la infinitud de los números primos.

Teorema: Existen infinitos números primos.

Euclides no enunció el teorema con estas palabras, ya que en esa época el concepto de infinito no estaba definido, de modo que el teorema que encontramos en su libro es: *Hay más números primos que cualquier cantidad propuesta de números primos.* A lo largo de la historia, los matemáticos han abordado y demostrado este teorema de formas diferentes.

Pero, ¿por qué nos puede interesar dar demostraciones distintas de un mismo resultado? En primer lugar, vamos a explicar qué es una demostración. Esto es una secuencia finita y ordenada de fórmulas o razonamientos ya probados, que finalmente llegan a la conclusión de la veracidad del resultado propuesto. En matemáticas son esenciales, ya que nos permiten utilizar los resultados demostrados.

La veracidad o falsedad de una proposición o de un teorema no dependen de la cantidad de demostraciones que haya del mismo, ya que será válido con que exista alguna demostración correcta. Entonces nos preguntamos, ¿qué necesidad hay de demostrar una cosa de diferentes maneras? Este hecho se ha dado a lo largo de la historia de las matemáticas y no solo con la infinitud de los números primos, sino con otros teoremas, como el de Pitágoras, y con otros resultados, como la irracionalidad de $\sqrt{2}$. Vamos a intentar dar una respuesta a esa pregunta.

Tener demostraciones alternativas de un mismo enunciado permite explorar el resultado desde diversas ramas de las matemáticas, dando la posibilidad de alcanzar un alto nivel de comprensión del enunciado demostrado, así como de su entorno asociado. Este enfoque desde distintos ángulos permite observar diferentes matices e incluso aplicaciones que podemos dar al enunciado demostrado. Además, la diversidad de demostraciones permite conectar ramas matemáticas cuyo campo de acción es muy diferente, pudiendo generar relaciones que no se hubiesen encontrado al no tener un nexo de unión. Cada nueva demostración debe hacernos reflexionar fundamentalmente sobre su alcance junto con el grado de interconexión y simplicidad que exhibe respecto de otras demostraciones.

Si hablamos de demostraciones, tenemos que mencionar a Paul Erdös y *El Libro*. Erdös fue un matemático húngaro del siglo XX que viajó por todo el mundo colaborando con cientos de matemáticos, pues pensaba que las matemáticas eran una ciencia que debía ser compartida y la forma óptima de estudiarlas era trabajar en colaboración con otros compañeros. Erdös solía decir que no necesitas creer en Dios, pero, como matemático, deberías creer en *El Libro*. Este libro no es uno que puedas comprar ni escribir por tu cuenta, ya que lo que contiene todavía no se ha desarrollado en ningún sitio. Esto es debido a que en su interior están escritas las demostraciones más elegantes de todos los teoremas matemáticos, incluso los que todavía no están demostrados. Por ello, Erdös pensaba en *El Libro* como algo escrito por una divinidad vanidosa que no quiere compartirlo con la humanidad. No obstante, cada vez que encontraba una demostración que le gustaba, decía que esa era para *El Libro*. En la década de los 90, le propusieron tratar de escribir una aproximación de dicho libro. Desgraciadamente murió antes de poder completarlo, aunque sus compañeros lo publicaron en su memoria,

lo podemos ver en [1]. Sin embargo, es complicado elegir que demostraciones estarían incluidas en *El Libro*, ya que a cada matemático nos gusta una demostración diferente. Mencionar que en el libro de Aigner y Ziegler encontramos algunas demostraciones de la infinitud de los números primos.

En este trabajo vemos exactamente 31 demostraciones (¡Un número primo!) de la infinitud de los números primos, siendo la primera la de Euclides y la última es una publicación de Mayo de 2017, recorriendo en este trabajo 23 siglos de matemáticas. Pero, la historia no acaba aquí, hay cientos de demostraciones del teorema que nos ocupa, pero no es posible incluirlas todas en este trabajo, principalmente por falta de espacio. Ahora bien, podemos saber más acerca de ellas consultando el artículo de Romeo Meštrović, *Euclid's Theorem on the Infinitude os Primes: a historical survey of its proofs* [21]. En dicho artículo se recoge una gran cantidad de demostraciones de la infinitud de los números primos, así como las referencias donde podemos consultarlas.

La información para la elaboración de este trabajo ha sido obtenida de diversas fuentes, las principales han sido: Dickson [10], Hardy-Wright [17], Ribenboim [25] y Yamada [32] . No obstante, también se han incluido las referencias originales donde precisamente aparece la demostración en cuestión por primera vez. Es cierto que la mayoría de las demostraciones no requieren un conocimiento profundo de las matemáticas, pero la posibilidad de ver la aplicación de casi todas las ramas estudiadas y establecer relaciones entre ellas requiere la comprensión de las mismas, haciendo de este trabajo una buena forma de demostrar lo aprendido durante los estudios.

El trabajo está estructurado en diferentes capítulos, en los que se incluyen varias demostraciones agrupadas por sus similitudes en la mayoría de los casos. El título de cada capítulo hace referencia a la demostración más conocida del mismo.

- En el Capítulo 2, vemos la demostración original de Euclides y algunas que siguen un proceso similar, el cual consiste en suponer que existe una cantidad finita de primos, trabajar con el producto de todos ellos y encontrar un número primo que no está en la lista inicial.

- En el Capítulo 3, aparecen la demostración de Goldbach y aquellas en las que, utilizando una lista de números que son primos entre sí, somos capaces de demostrar que hay infinitos primos.

- En el Capítulo 4, se explican la demostración de Euler y aquellas en las que se utilizan series o sumas finitas para llegar a una contradicción.

- En el Capítulo 5, se incluyen aquellas demostraciones en las que a partir de la posibilidad de escribir un número de forma única como su factorización en números primos, somos capaces de llegar a una contradicción.

- En el Capítulo 6, se presenta una demostración utilizando propiedades topológicas y algunas reinterpretaciones en las que se evitan los conceptos de topología.

- En el Capítulo 7, tenemos varias demostraciones que consideramos que no deben ser incluidas en ninguno de los otros capítulos, ya que merecen un comentario aparte.

Capítulo 2

Demostraciones basadas en la idea de Euclides

La idea central en las demostraciones de esta sección es suponer que hay una cantidad finita de números primos y construir otro número a partir de éstos. Con este nuevo número podremos obtener otro primo que no está en la lista original que habíamos supuesto, con lo que llegamos a un absurdo. Por tanto, la hipótesis inicial de que existe una cantidad finita de primos es falsa, luego hay infinitos. Cabe destacar que con esta idea se pueden encontrar, como veremos más adelante, números primos con determinadas características.

2.1. Demostración de Euclides

Como ya hemos mencionado, Euclides es el primer matemático, del que tengamos constancia, que proporcionó una demostración. Aunque no está escrita con la formalidad actual, puede adaptarse al lenguaje matemático que usamos en estos días. La podemos encontrar en su libro *Los Elementos* del siglo III a.C., como hemos comentado en la introducción, lo podemos ver en [12]. Cabe destacar que en aquella época Euclides no utilizó el término infinito, pues no estaba definido de forma precisa como en la actualidad. Por esta razón, Euclides enunció el teorema de otra manera:

Proposición 2.1 *(Proposición 20 del libro IX): Hay más números primos que en cualquier lista finita de ellos.*

Necesitamos además, algunas definiciones previas para entender su demostración:

- (Libro VII, Def. 1) Una unidad es aquello en virtud de la cual cada una de las cosas que hay es llamada una.
- (Libro VII, Def. 2) Un número es una pluralidad compuesta de unidades.
- (Libro VII, Def. 11) Un número primo es el que es medido por una sola unidad.

- (Libro VII, Def. 13) Un número compuesto es aquello que es medido por algún número.

Estas definiciones de unidad y número se entienden perfectamente si asumimos que en la época griega la aritmética estaba estrechamente ligada a la geometría (longitudes y áreas). En la definición de número primo, Euclides utiliza el concepto de medida de un número por otro. En términos de longitudes, un número mide a otro cuando tomado una, o muchas veces le iguala. En términos actuales, un número a mide a otro número b cuando a divide a b o b es múltiplo de a.

Hablando de múltiplos y divisores, nos viene a la cabeza uno de los resultados más importante en teoría de números, el Teorema Fundamental de la Aritmética.

Teorema 2.1 *Cada número entero mayor que 1 tiene una factorización en números primos que es única salvo el orden de sus factores.*

Es cierto que el Teorema Fundamental de la Aritmética no se demuestra exactamente como tal en *Los Elementos*, pues fue Gauss el primero en dar una demostración completa y formal, la podemos ver en [16]. Ahora bien, las proposiciones 30, 31 y 32 del Libro VII y la proposición 14 del Libro IX son esencialmente el enunciado y la prueba de dicho teorema. Para la demostración dada por Euclides de la infinitud de los números primos, no es necesario utilizar toda la información que proporciona el teorema. Es suficiente con otra proposición que encontramos en sus libros:

Proposición 2.2 *(Proposición 31 del libro VII): Cualquier número compuesto es medido por algún número primo.*

Pasemos ahora a ver cómo demostró Euclides la infinitud de los números primos. Recordemos que se va a demostrar que hay más números primos que cualquier lista finita.

Demostración 1 *Sean A, B, C nuestra lista finita de números primos, vamos a ver que hay más números primos que A, B, C.*

Sea DE el menor número medido por A, B, C. Sea DF la unidad y sea EF la suma de DE y DF. Luego, EF puede ser un número primo o no. Si es primo, entonces hemos encontrado un nuevo número primo pues no está en nuestra lista inicial.

En caso contrario, EF es compuesto, por tanto, es medido por algún número primo G (proposición 2.2). Este primo G no puede ser ni A, ni B, ni C. Si fuera uno de ellos, como A, B, C miden a DE, G también mediría a DE. Pero además, mide a EF. Por tanto G, siendo un número (ya que no es unidad), medirá a la resta, la unidad DF, que es absurdo. Por lo tanto, G no es ninguno de los números A, B, C y por hipótesis es primo. Luego, hemos encontrado un número primo que no está en nuestra lista. □

En la demostración anterior, la expresión "Sea DE el menor número medido por A, B, C", equivale matemáticamente a la expresión: DE es el mínimo común múltiplo de A, B, C. Reescribiendo en términos actuales se tiene:

Demostración 2 *Supongamos que existe una cantidad finita de números primos (distintos) y los ordenamos de forma creciente* $p_1 < p_2 < ... < p_r$. *Sea* $N = p_1p_2...p_r + 1$.

Ahora bien, este nuevo número N *así construido puede ser primo o no. Si* N *es primo,* N *es un primo que no está en nuestra lista, ya que es mayor que todos los demás, al ser el producto de todos más uno.*

Si N *no es primo, por la proposición 2.2, existirá un primo* p *que lo divide. Se tiene que, para cada primo* p_i, *podemos escribir* $N = c_ip_i + 1$ *con* $c_i \geq 1$. *Entonces, el resto de dividir* N *entre* p_i *es siempre 1. Por tanto, este primo* p *que divide a* N, *no puede ser ninguno de los primos iniciales* p_i.

Luego, en ambos casos, nuestra lista inicial es incompleta. □

Esta demostración es, en cierto modo, constructiva pues permite a partir de una lista de primos dada, obtener un nuevo número primo (asumiendo, aunque no tenga sentido, pues no conocemos todos los primos, que podemos factorizar completamente).

Es interesante resaltar que no es necesario que N sea el mínimo común múltiplo de los números primos más 1. Es decir, podríamos introducir un nuevo múltiplo K, pudiendo ser cualquier número natural. Este hecho no altera la demostración ni añade nada nuevo, por tanto, no se suele considerar. Ahora bien, si atendemos a la información que se obtiene sobre el nuevo número primo, sí que influye. Esto se debe a que a partir de la demostración, tenemos una cota superior para el primo p, que es $p \leq N = p_1p_2...p_r + 1$, que evidentemente es mejor que si introducimos el múltiplo K, ya que en ese caso obtendríamos $p \leq N = Kp_1p_2...p_r + 1$, donde K puede ser cualquier número natural.

Nota 1: Para que sean más sencillos y visuales, vamos a suponer en los ejemplos de todo el trabajo que somos capaces de factorizar, aunque no conozcamos los nuevos números primos obtenidos al aplicar las diferentes demostraciones. También suponemos que somos capaces de saber si un número es primo, utilizando algún test de primalidad.

Veamos algunos ejemplos eligiendo como lista inicial una colección de primos dada de antemano:

- Sea $\mathcal{P} = \{2, 3, 5, 7, 11\}$ nuestra lista finita de primos. En este caso, se tiene que $N = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$. Es fácil comprobar que no es divisible por ninguno de los primos de la lista inicial y por tanto, es primo o existirá otro primo que no está en $\mathcal{P}$ que lo divide. En este caso, N es un nuevo número primo.

- Ahora consideramos la lista $\mathcal{Q} = \{3, 5, 7, 11\}$ como todos los números primos. De esta forma, $N = 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 1156$. Este nuevo número no es primo pues se factoriza como $1156 = 2^2 \cdot 17^2$, de donde podemos obtener dos nuevos números primos que no están en nuestra lista $\mathcal{Q}$, el 2 y el 17.

2.2. Demostración de Kummer

Enrst Eduard Kummer fue un matemático alemán del siglo XIX, que trabajó en distintos temas de las matemáticas, como teoría de funciones, el último teorema de

Fermat y geometría. También escribió una demostración del teorema que nos ocupa muy parecida a la de Euclides, la cual la podemos encontrar en uno de sus artículos que fue escrito en 1878, podemos verlo en [19].

Demostración 3 *Supongamos que existe una cantidad finita de números primos distintos y la ordenamos de forma creciente $p_1 < p_2 < ... < p_r$, con r mayor que 1. Sea $N = p_1 p_2 ... p_r > 2$. Consideremos también el entero $N - 1$.*

Por la proposición 2.2, existe al menos un primo p que divide a $N - 1$. A partir de la hipótesis realizada de que existen únicamente los primos $p_1, ..., p_r$, el primo p debe ser uno de ellos. Entonces, tenemos que para algún i, $1 \leq i \leq r$, p_i divide tanto a N como a $N - 1$ y por tanto, divide a su resta, es decir p_i divide a 1. Luego, $p_i = 1$, que es absurdo. □

Cabe destacar, que esta demostración, necesita que nuestra lista inicial tenga, al menos dos primos, porque sino $N - 1$ podría ser 1, con lo que no existiría un primo p que lo divida, con lo cual la demostración no tendría sentido.

Al igual que en la demostración de Euclides, podemos introducir un nuevo múltiplo K en el cálculo del N, aunque obtenemos el mismo resultado ya que tampoco aporta nada a la demostración.

Veamos ahora, que sucede si tomamos las mismas listas de primos que hemos mencionado en la demostración original de Euclides.

- Sea $\mathcal{P} = \{2, 3, 5, 7, 11\}$ nuestra lista finita de primos. En este caso, $N - 1 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 - 1 = 2309$. Se comprueba de manera sencilla que $N - 1$ no es divisible por ninguno de los primos de la lista inicial y por tanto, es primo o existe otro primo que no está en $\mathcal{P}$ que lo divide. En este caso, $N - 1$ es un nuevo número primo y además es distinto al obtenido en el ejemplo de la sección de Euclides.

- Ahora consideramos la lista $\mathcal{Q} = \{3, 5, 7, 11\}$ como todos los números primos. $N - 1 = 3 \cdot 5 \cdot 7 \cdot 11 - 1 = 1154$. Este nuevo número no es primo y podemos factorizarlo $1154 = 2 \cdot 577$, de donde podemos obtener dos números primos que no están en nuestra lista $\mathcal{Q}$, el 2 y el 577. En este caso, al igual que en el ejemplo de la sección de Euclides, obtenemos al 2 como nuevo primo, pero el otro es diferente.

2.3. Demostración de Stieltjes

Thomas Joannes Stieltjes fue un matemático holandés del siglo XIX que estudió numerosos campos de las matemáticas, como la cuadratura de Gauss o la integral de Riemann-Stieljes. También trabajó en la infinitud de los números primos, obteniendo una demostración con una idea general muy parecida a la de Euclides. Podemos encontrarla en [28], que fue publicado en 1890.

Demostración 4 *Asumimos que $p_1, p_2, ..., p_r$ es nuestra lista finita de primos. Sea $N = p_1 \cdot p_2 \cdot ... \cdot p_r$, es decir, el producto de todos ellos.*

Claramente N no es primo, por tanto lo podemos escribir como producto de dos factores $N = m \cdot n$, con m y n mayores que 1 y primos entre sí. Como m y n son primos entre sí, cualquier p_i que divida a m no divide a n y, de la misma forma, cualquier p_j que divida a n no divide a m. Con lo que cada uno de los primos de nuestra lista divide a m o a n pero no a los dos. Por tanto, no divide a la suma $m+n$.

Por la proposición 2.2, $m + n$ tendrá un factor primo p, que puede ser el mismo $m+n$, si éste es primo, u otro número. Pero, este primo p no puede ser ningún primo de nuestra lista inicial ya que divide a $m+n$ y ningún p_i divide a $m+n$. Luego, nuestra lista original es incompleta. □

Evidentemente necesitamos que m y n sean mayores que 1 para que sean primos entre sí. Ahora bien, supongamos que $n = 1$, entonces $m = N$ y $m + n = N + 1$. Con esto, la demostración pasa a ser muy similar, por no decir igual, a la de Euclides ya que en ambos casos vamos a buscar factores primos comunes entre N y $N + 1$.

Para ver algunos ejemplos, lo que vamos a cambiar en cada uno de ellos es el modo de separar el producto de los primos en dos factores, es decir, vamos a elegir diferentes m y n. Sea $\mathcal{P} = \{2, 3, 5, 7, 11\}$ nuestra lista finita de primos. Luego, $N = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$.

- Tomemos $N = 30 \cdot 77$, con lo que $m = 30 = 2 \cdot 3 \cdot 5$ y $n = 77 = 7 \cdot 11$. Luego, $m + n = 107$, que es fácil comprobar que ninguno de los números de nuestra lista lo divide, por tanto, es primo o tiene un factor primo que no está en nuestra lista. En este caso, es un nuevo número primo.

- Ahora tomamos $N = 154 \cdot 15$, con lo que $m = 154 = 2 \cdot 7 \cdot 11$ y $n = 15 = 3 \cdot 5$. Luego, $m + n = 169 = 13^2$, por tanto en este caso obtenemos al 13 como nuevo número primo.

2.4. Demostración de Boije af Gennäs

Boije af Gennäs era un matemático sueco de Goteborg, del que sabemos muy poco. Sin embargo, la demostración que desarrolló la incluimos en este trabajo porque se puede entender como la generalización de las demostraciones de esta sección. En esta ocasión, en lugar de tomar una lista de primos conocidos como en las demostraciones anteriores, tomaremos todos los números primos menores que un número cualquiera (esto es factible usando, por ejemplo, la criba de Eratóstenes). Esta demostración originalmente se encuentra en [3], texto de 1893, pero también puede verse en el clásico libro de Dickson [10].

Demostración 5 *Sea $X > 2$ un número real aleatorio y $p_1, p_2, ..., p_r$ son todos los primos menores o iguales que X. Sea $N = p_1^{e_1} \cdot p_2^{e_2} \cdot ... \cdot p_r^{e_r}$ con $e_i \geq 1$ para todo i.*

Escribimos N como el producto de dos enteros positivos que sean primos entre sí, $N = \delta \cdot N/\delta$, cumpliendo que $M = N/\delta - \delta$ sea mayor que 1. Como δ y N/δ son primos entre sí, cada p_i o divide a δ o divide a N/δ pero no a ambos. Por tanto, cada primo no divide a la resta de N/δ y δ.

Luego, M no es divisible por ninguno de los p_i, es decir no es divisible por ningún primo menor que X. Por tanto, M debe ser producto de primos mayores que X. Luego, existen primos mayores que X para cualquier X y, en consecuencia, hay infinitos primos. □

Esta demostración requiere algunos detalles técnicos para que sea válida. Necesitamos imponer que X sea mayor que 2 para que existan primos menores que el mismo. También se requiere que M sea mayor que 1, ya que sino no tendría factores primos. Es interesante ver que si consideramos todos los exponentes iguales a 1 y elegimos $\delta = 1$ tenemos la misma demostración que propuso Kummer.

En este caso, los ejemplos pueden ser muy variados según consideremos distintos X, distintos N y distintos δ. Veamos algunos:

- Tomamos $X = 12$ con lo que nuestra lista de primos es $\{2, 3, 5, 7, 11\}$. Consideramos $N = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$, es decir que tomamos todos los exponentes como 1. Si tomamos $\delta = 1$, tendríamos $M = N - 1 = 2309$, que es primo. Este ejemplo es el mismo que el que aparece en la demostración de Kummer, como ya habíamos deducido.

- Elegimos otra vez $X = 12$ obteniendo como lista de primos a $\{2, 3, 5, 7, 11\}$. Como anteriormente $N = 2310$, es decir que tomamos todos los exponentes como 1. Si tomamos $\delta = 30 = 2 \cdot 3 \cdot 5$, tendríamos $M = 77 - 30 = 47$, que es primo.

- Consideramos de nuevo $X = 12$ luego nuestra lista de primos es $\{2, 3, 5, 7, 11\}$. Consideramos $N = 2^2 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 11^2 = 5336100$, con lo que tomamos los exponentes iguales a 2. Si $\delta = 2^2 \cdot 3^2 \cdot 5^2 = 900$, tendríamos $M = 5929 - 900 = 5029 = 47 \cdot 107$, de donde obtenemos dos primos mayores que X.

2.5. Demostraciones utilizando progresiones aritméticas

Peter Gustav Dirichlet fue un matemático alemán del siglo XIX, que tuvo la suerte de aprender de los matemáticos más famosos de su tiempo, como Fourier o Laplace. Sus aportaciones más relevantes fueron en la teoría de números, prestando especial atención a la teoría de las series de Fourier. En relación con la infinitud de los primos, no la demostró como tal, pero si se deduce trivialmente del siguiente teorema que sí demostró.

Teorema 2.2 *Si $MCD(a, b) = 1$ entonces la progresión aritmética $\{an + b\}$ contiene infinitos números primos.*

Evidentemente, para que haya infinitos números primos en una progresión, es necesario que la cantidad de dichos números sea infinita, por tanto, al demostrar este teorema, se prueba la infinitud de los números primos. La demostración aportada por

Dirichlet, que la podemos ver en [11], exige importantes herramientas del análisis matemático, que se van del objetivo de este trabajo. Sin embargo, si podemos ver algunos casos particulares más sencillos, por ejemplo cuando $a = 4$ y $b = 3$. Es decir, vamos a probar que existen infinitos números primos de la forma $4n + 3$, donde n es un entero no negativo, con lo que quedará demostrada la infinitud de los números primos.

Demostración 6 *Supongamos que solamente hay una cantidad finita de números primos de la forma $4n + 3$, donde n es un entero no negativo. La lista será $p_1, p_2, ..., p_r$. Sea*

$$N = 4p_1p_2...p_r - 1$$

$$N = 4(4n_1 + 3)(4n_2 + 3)...(4n_r + 3) - 1$$

$$N = 4[(4n_1 + 3)(4n_2 + 3)...(4n_r + 3) - 1] + 3$$

donde $n_1, n_2, ..., n_r$ son enteros no negativos. Notemos que N es de la forma $4n + 3$.

Ahora bien, este nuevo número N puede ser primo o no. Si N es primo, debería estar en la lista inicial $p_1, p_2, ..., p_r$, ya que es de la forma $4n+3$. Sin embargo, no está, ya que es mayor que todos los demás.

Si N es compuesto, por el Teorema Fundamental de la Aritmética, N tendrá una factorización en números primos, que será $N = q_1q_2...q_t$ donde cada q_i es un primo, no necesariamente distinto de los demás. Como N es de la forma $4n+3$ es un número impar. Por tanto, todos sus factores también, por lo que cada factor puede ser de la forma $4n + 1$ o $4n + 3$.

Primero, vamos a ver que al menos uno de los factores es de la forma $4n+3$. Para ello, supongamos lo contrario, es decir que todos los factores son de la forma $4n + 1$. Consideramos

$$(4n_1 + 1)(4n_2 + 1) = 4(4n_1n_2 + n_1 + n_2) + 1$$

donde n_1 y n_2 son dos enteros no negativos. Acabamos de ver que el producto de dos números de la forma $4n + 1$ es otro número de la forma $4n + 1$. Luego, si todos los factores de N son de la forma $4n + 1$, N también lo será. Sin embargo, N es de la forma $4n + 3$, entonces, al menos un factor de N, digamos q_1, es de la forma $4n + 3$. Como q_1 es primo y de la forma $4n + 3$, deberá ser uno de los primos de nuestra lista inicial, luego $q_1 = p_i$ para algún i de 1 a r. Como p_i es un factor primo de N, p_i divide a N. Notemos que $N + 1 = 4p_1p_2...p_r$. Luego, p_i también divide a $N + 1$, por lo que divide a la resta, es decir p_i divide a 1. Entonces, $p_i = 1$, que es absurdo. □

Esta demostración es muy similar a la de Euclides, ya que la construcción de N se realiza en ambos casos a partir de los primos conocidos. La diferencia está en que en este caso, trabajamos con números primos de una forma particular.

Otro ejemplo similar que nos permite ver la infinitud de los números primos sería viendo que existen infinitos números primos no congruentes con 1 mód n, donde n es un entero mayor que 2.

Demostración 7 *Fijamos n como un entero mayor que 2. Supongamos que existe una cantidad finita de números primos $p_1, p_2, ..., p_r$ no congruentes con* 1 mód n. *Esta*

lista no es vacía ya que $p_1 = 2$*, que no es congruente con* $1 \bmod n$*. En este caso, tomamos* $N = np_1p_2...p_r - 1$ *y se procede como en la demostración anterior. Si* N *es primo, llegamos a un absurdo. Si* N *es compuesto, lo factorizamos, luego* $N = q_1q_2...q_t$*. Teniendo en cuenta que* $q_i \cdot q_j = (nk_i + 1)(nk_j + 1) = n(nk_ik_j + k_i + k_j) + 1$*, de manera similar a lo anterior, deducimos que algún factor no es congruente con* $1 \bmod n$ *y al igual que la demostración anterior, llegamos a un absurdo.* □

Vamos a ver algunos ejemplos de números primos no congruentes con 1 mód n, ya que los anteriores, los de la forma $4n + 3$, son un caso particular de estos últimos.

- Sea $n = 3$, nuestra lista finita de primos es $\mathcal{P} = \{2, 5, 11, 17, 23\}$. En este caso, se tiene que $N = 3 \cdot 2 \cdot 5 \cdot 11 \cdot 17 \cdot 23 - 1 = 129029 = 19 \cdot 6791$. Hemos obtenido dos números primos, pero el 19 es congruente con 1 mód 3, con lo que no nos sirve. Sin embargo, el 6791 no es congruente con 1 mód 3, con lo que tenemos un nuevo primo de la forma buscada.

- Sea $n = 8$, nuestra lista finita de primos es $\mathcal{Q} = \{2, 3, 5, 7, 11, 13, 19\}$. En este caso, se tiene que $N = 8 \cdot 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 - 1 = 4564559$, que es un número primo no congruente con 1 mód 8 que no esta en la lista inicial.

Estas demostraciones de que existen infinitos números primos con una forma determinada pueden parecer menos interesantes que las demostraciones más generales, pero no es así, y esto se debe a la forma actual que tenemos para determinar si un número es primo o no, se puede consultar más sobre el asunto en [25]. Para decidir cuando un número es primo, existen diferentes test de primalidad, los cuales usan diferentes algoritmos. En general, debido a la estructura de dichos algoritmos, es más sencillo y eficiente en cuanto a complejidad, determinar si un número entero es primo si este puede escribirse de alguna forma determinada, como por ejemplo $A \cdot 2^n + 1$ (Test de Proth) o los primos de Mersenne $2^p - 1$ (Test de Lucas-Lehmer). Además, los números primos más grandes conocidos actualmente son primos de Mersenne.

2.6. Relación entre las demostraciones

Mencionar que en esta relación no se van a tener en cuenta las demostraciones vistas en la sección dedicada a Dirichlet. Esto se debe a que dichas demostraciones son muy similares a la de Euclides, por tanto, no merecen mayor consideración a la hora de compararlas.

Hasta aquí, simplemente tenemos una recopilación de demostraciones que tienen varias cosas en común. En todas se parte de una cantidad finita de números primos, luego se construye un número a partir del producto de los elementos de la lista y finalmente, se encuentra un número primo que no está en dicha lista. Lo que vamos a hacer en esta sección es comentar las similitudes y diferencias que existen entre estas demostraciones.

En las demostraciones de Euclides y de Kummer no separamos dicho producto, es decir, vamos a construir un nuevo número a partir del producto de todos los primos

de la lista inicial. Por otro lado, en la de Stieljes y en la de Boije af Gennäs escribimos ese producto, como el producto de dos factores primos entre sí y construimos el nuevo número a partir de estos dos números.

La diferencia entre la de Euclides y la de Kummer es que en la primera, se le suma 1 al producto y en la segunda, se le resta. Sin embargo, a partir de esta consideración, vuelven a ser prácticamente iguales, ya que en ambos casos se busca un factor primo del nuevo número y llegando a contradicción nos damos cuenta de que dicho número es un primo que no está en nuestra lista.

La diferencia entre la de Stieljes y la de Boije af Gennäs es que en la primera, se considera la suma de los dos factores primos del producto. Mientras que en la segunda, se considera su resta. De aquí en adelante ambas buscan un factor primo de este nuevo número, pero el que encuentran no está en nuestra lista inicial, con lo que se llega a contradicción.

Destacamos que si en la demostración de Stieljes consideramos uno de los factores en los que descomponemos el producto como 1, tenemos la misma demostración que Euclides. Por tanto, se puede pensar que la demostración de Stieljes es una generalización de la de Euclides, ya que, como hemos visto, da lugar a más ejemplos tomando como punto de partida la misma lista inicial de primos.

Ocurre algo similar entre la de Boije af Gennäs y la de Kummer, es decir, que si en la demostración de Boije af Gennäs tomamos todos los exponentes iguales a 1 y se considera uno de los factores en los que descomponemos el producto como 1, necesariamente el que resta, obtenemos la demostración de Kummer.

En todos los casos sabemos que existe un número primo que no está en nuestra lista inicial. No obstante, en ninguno de ellos podemos calcularlo de manera general. Esto se debe a que no sabemos factorizar completamente, debido, entre otras cosas, a que no conocemos todos los números primos, tal como habíamos mencionado en la Nota 1, al dar los ejemplos en la parte dedicada a Euclides.

Sin embargo, hay una demostración que nos aporta más información sobre el nuevo número primo que las demás, esta es la de Boije af Gennäs. Esto se debe a que en esta demostración se consideran los primos menores que un número dado, con lo que el primo encontrado tendrá que ser mayor que éste. Destacar que en las otras demostraciones los números primos de la lista inicial no son necesariamente consecutivos, pero si se lo imponemos desde el principio tendríamos la misma cota inferior.

También se puede apreciar otra diferencia entre la demostración de Boije af Gennäs y las otras, y es que en ésta a la hora de calcular el producto de los primos de la lista, se consideran exponentes en estos números, mientras que en las demás no. No obstante, dicha consideración no aporta más información, más bien al contrario, ya que puede llevar a confusión, es decir, funciona igual si consideramos como 1 todos los exponentes, con lo que estaríamos en el caso de las otras demostraciones.

Capítulo 3

Demostraciones basadas en la idea de Goldbach

En esta sección, la idea de las demostraciones está en construir o disponer de una sucesión de números infinita y ver que sus elementos son todos primos entre sí, por tanto, aplicando la Proposición 31 del libro VII de Euclides, cada elemento tendrá un factor primo distinto y como tenemos infinitos números en la sucesión, tendremos infinitos factores primos.

3.1. Desmostración de Goldbach

Todo matemático ha oído alguna vez la conjetura de Goldbach, que nos dice que todo número par mayor que 2 puede representarse como suma de dos números primos. Esta conjetura tiene el nombre de su autor, Chistian Goldbach que fue un matemático prusiano del siglo XVIII, que trabajó en diversos campos de las matemáticas y estuvo en contacto con numerosos matemáticos contemporáneos. Cabe destacar su relación con Leonhard Euler, con quien mantenía una correspondencia en la cual trataban distintos temas matemáticos. Gracias a esto surgió esta demostración, ya que fue encontrada en una de las cartas que envió Goldbach a Euler en 1730, la carta original donde se encuentra la demostración de Goldbach la podemos ver en [15], además de poder encontrarla en [25]. Para la demostración, Goldbach utilizó los números de Fermat.

Definición 3.1 *Sea n un número natural, se definen los números de Fermat como* $F_n = 2^{2^n} + 1$.

Fermat fue un matemático francés del siglo XVII, que desarrolló sus estudios en diferentes ramas de las matemáticas, pero donde realmente destacó fue en la teoría de números, donde sus aportaciones todavía son utilizadas a diario.

Una de ellas fue la definición arriba mencionada. Fermat pensaba que todos los números de la forma $F_n = 2^{2^n} + 1$ eran primos, pero Euler en 1732 probó que no es así al factorizar F_5.

Actualmente, sólo se conocen cinco números primos de Fermat, que son $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$, que ya se conocían en tiempos del propio Fermat, y, a fecha de enero de 2009 sólo se conoce la factorización completa de los doce primeros (desde n=0 hasta n=11). Destacar que el tamaño de estos números crece exponencialmente, por ejemplo el número $F_{10} = 2^{2^{10}} + 1 = 2^{1024} + 1$ tiene 309 cifras.

A continuación, vamos a demostrar una serie de propiedades básicas de los números de Fermat. La primera de ellas es una fórmula recurrente y la segunda trata los divisores de un número de Fermat y el producto de los anteriores.

Lema 3.1 *Si n es un número natural, entonces,*

$$F_{n+1} - 2 = F_n \cdot F_{n-1} \cdot ... \cdot F_1 \cdot F_0$$

Demostración: Vamos a aplicar inducción sobre n.

Si $n = 0$, entonces $F_0 = 3$ y se tiene que $F_{0+1} - 2 = 5 - 2 = 3 = F_0$

Asumimos ahora que el resultado es cierto para n, veamos que se cumple para $n+1$. Por hipótesis de inducción, se tiene $F_{n+1} \cdot F_n \cdot ... \cdot F_1 \cdot F_0 = F_{n+1} \cdot (F_{n+1} - 2)$.

Luego, $F_{n+1} \cdot F_n \cdot ... \cdot F_1 \cdot F_0 = (2^{2^{n+1}} + 1)(2^{2^{n+1}} - 1) = 2^{2^{n+2}} - 1 = (2^{2^{n+2}} + 1) - 2 = F_{n+2} - 2$, como queríamos demostrar. □

Con este lema hemos obtenido una fórmula recurrente para los números de Fermat. Ahora veamos los divisores que tienen en común.

Lema 3.2 *Para todo número natural n se tiene que*

$$MCD(F_{n+1}, F_n \cdot F_{n-1} \cdot ... \cdot F_1 \cdot F_0) = 1$$

Demostración: Sea $d = MCD(F_{n+1}, F_n \cdot F_{n-1} \cdot ... \cdot F_1 \cdot F_0)$. Claramente, d divide a F_{n+1} y al producto $F_n \cdot F_{n-1} \cdot ... \cdot F_1 \cdot F_0$.

Utilizando la igualdad del lema 3.1, se tiene que d divide a $(F_{n+1} - 2)$. Entonces, como d divide a F_{n+1} y a $(F_{n+1} - 2)$, d divide a su resta, luego d divide a 2. Por tanto, $d = 1$ o $d = 2$. Ahora bien, como los números de Fermat son impares por construcción y d divide a uno de ellos, concretamente a F_{n+1}, se tiene que d no puede ser 2, entonces $d = 1$. □

Usando estos lemas vamos a demostrar que hay infinitos números primos.

Demostración 8 *Vamos a ver que cada uno de los F_n será divisible por un primo p_n distinto.*

Por el lema 3.2, F_{n+1} y $F_n \cdot F_{n-1} \cdot ... \cdot F_1 \cdot F_0$ no tienen factores primos en común. Luego, $MCD(F_i, F_j) = 1$ para todo $i \neq j$, es decir que son coprimos dos a dos. Por la proposición 2.2, cada F_n tiene un factor primo p_n. Se sigue que p_n no divide a F_j para todo $j \neq n$. Por tanto, tenemos que cada número de Fermat es divisible por, al menos, un primo distinto y como existen infinitos números de Fermat, tenemos tantos como números naturales, se tiene que hay infinitos primos. □

Esta demostración nos garantiza la existencia de infinitos números primos a partir de los números de Fermat. Ahora bien, si quisiéramos calcular dichos primos, necesitaríamos factorizar los números de Fermat, algo que no es posible actualmente, ya que solamente se han factorizado los doce primeros.

Veamos algunos ejemplos de números de Fermat y sus factorizaciones.

- $F_2 = 2^4 + 1 = 17$, que es un número primo.
- $F_3 = 2^8 + 1 = 257$, que es un número primo.
- $F_4 = 2^{16} + 1 = 65537$, que es un número primo.
- $F_5 = 2^{32}+1 = 4294967297 = 641 \cdot 6700417$, tenemos dos factores primos distintos.
- $F_6 = 2^{64} + 1 = 18446744073709551617 = 274177 \cdot 67280421310721$, tenemos dos factores primos distintos.
- $F_7 = 2^{128}+1 = 340282366920938463463374607431768211457 = 59649589127497217 \cdot 5704689200685129054721$, tenemos dos factores primos distintos.

3.2. Desmostración de Wunderlich

Si estamos hablando de series famosas de números, ya hemos visto los números de Fermat, no podemos pasar por alto la sucesión de Fibonnaci, que si bien es cierto que sus elementos no son coprimos dos a dos, se puede trabajar con ellos para conseguir una demostración de la infinitud de los números primos. Esto mismo hizo M. Wunderlich en 1965, que podemos verla en [31]. Por aquel entonces, Wunderlich estaba en la Universidad de Colorado donde se doctoró un año antes con una tesis sobre cribas de números y sucesiones. Además de estudiar la sucesión de Fibonacci, ha trabajado en fracciones continuas, teoría de números, primalidad y criptografía.

Para ver la demostración, vamos a empezar viendo cómo se define la sucesión de Fibonacci.

Definición 3.2 *Se conoce como sucesión de Fibonacci a la dada, de forma recursiva, por los siguientes números:* $f_0 = 0$, $f_1 = 1$ *y* $f_n = f_{n-1} + f_{n-2}$ *para cualquier número entero* n *mayor que* 1. *Por tanto, es la sucesión que se genera sumando los dos números anteriores.*

Esta sucesión ha sido largamente estudiada por los matemáticos a lo largo de toda la historia, pero fue Fibonacci quien la presentó en su libro *Liber Abaci* publicado en 1202. Surgió como solución a un problema de cría de conejos.

Si consideramos unos pocos elementos de dicha sucesión, vemos que efectivamente sus elementos no son coprimos dos a dos, $f_0 = 0$, $f_1 = 1$, $f_2 = 1$, $f_3 = 2$, $f_4 = 5$, $f_5 = 8$, $f_6 = 13$, $f_7 = 21$.

Entonces, para poder demostrar que hay infinitos números primos vamos a ver primero cómo es el máximo común divisor entre los elementos de la sucesión de Fibonacci. Empezaremos con unos resultados previos.

Lema 3.3 *$MCD(f_n, f_{n-1}) = 1$, para todo n entero positivo.*

Demostración: Vamos a proceder por inducción en n.

Si $n = 1$, $f_1 = 1, f_0 = 1$, luego $MCD(f_1, f_0) = 1$. Asumimos ahora que el resultado es cierto para n, veamos que se cumple para $n + 1$.

Por definición, $f_{n+1} = f_n + f_{n-1}$, luego $MCD(f_{n+1}, f_n) = MCD((f_n + f_{n-1}), f_n) = MCD((f_n + f_{n-1} - f_n), f_n) = MCD(f_n, f_{n-1}) = 1$, por hipótesis de inducción. □

Con este lema hemos visto que todo elemento de la sucesión de Fibonacci es coprimo con el anterior a él. Ahora vamos a ver que tenemos otra fórmula recurrente para los números de Fibonacci.

Lema 3.4 *Dados m,n dos enteros positivos, se cumple*

$$f_{m+n} = f_m \cdot f_{n-1} + f_{m+1} \cdot f_n$$

Demostración: Vamos a proceder por inducción en n, para ello fijamos m como un número entero positivo.

Si $n = 1$, $f_{n-1} = f_0 = 0$ y $f_n = f_1 = 1$. Si calculamos $f_m \cdot f_{n-1} + f_{m+1} \cdot f_n = f_m \cdot 0 + f_{m+1} \cdot 1 = f_{m+1} = f_{m+n}$, como queríamos ver.

Asumimos ahora que el resultado es cierto hasta n, veamos que se cumple para $n + 1$, es decir queremos probar que $f_{m+n+1} = f_m \cdot f_n + f_{m+1} \cdot f_{n+1}$.

Por definición, $f_{m+n+1} = f_{m+n} + f_{m+n-1}$. Aplicando la hipótesis de inducción, $f_{m+n} = f_m \cdot f_{n-1} + f_{m+1} \cdot f_n$ y $f_{m+n-1} = f_m \cdot f_{n-2} + f_{m+1} \cdot f_{n-1}$. Por tanto, $f_{m+n+1} = (f_m \cdot f_{n-1} + f_{m+1} \cdot f_n) + (f_m \cdot f_{n-2} + f_{m+1} \cdot f_{n-1}) = f_m \cdot (f_{n-1} + f_{n-2}) + f_{m+1} \cdot (f_n + f_{n-1}) = f_m \cdot f_n + f_{m+1} \cdot f_{n+1}$, como queríamos demostrar. □

Ahora veamos otra relación entre los elementos de la sucesión de Fibonacci.

Lema 3.5 *Dado m un número natural, se tiene que f_m divide a f_{mk}, para todo k entero positivo.*

Demostración: Vamos a demostrarlo usando inducción en k. Para ello fijamos m como un entero positivo.

Si $k = 1$, $f_{mk} = f_m$, luego f_m divide a f_{mk}.

Suponemos que se cumple hasta cierto k entero, veamos que ocurre con $k + 1$.

Utilizando el lema 3.4, tenemos $f_{m(k+1)} = f_{mk+m} = f_{mk} \cdot f_{m-1} + f_{mk+1} \cdot f_m$. Utilizando la hipótesis de inducción, se tiene $f_{mk} = qf_m$ para cierto entero q. Por tanto, tenemos que $f_{m(k+1)} = qf_m \cdot f_{m-1} + f_{mk+1} \cdot f_m = f_m(qf_{m-1} + f_{mk+1})$, de donde deducimos que f_m divide a $f_{m(k+1)}$, como queríamos demostrar. □

A raíz de este lema, es evidente que si la sucesión de Fibonacci contiene algún número primo, necesariamente el índice correspondiente a dicho elemento, tiene que ser un número primo, pero el recíproco no es cierto, por ejemplo $f_{19} = 4181 = 37 \cdot 113$.

El siguiente resultado es importante ya que permite calcular el máximo común divisor de dos elementos cualesquiera de la sucesión.

Proposición 3.1 *El máximo común divisor de dos números de Fibonacci es otro número de Fibonacci. En particular, si m y n son dos enteros positivos,*

$$MCD(f_m, f_n) = f_d, \text{ donde } d = MCD(m, n)$$

Demostración: Suponemos n es mayor que m, además $n = mk + r$ con r mayor o igual que 0 y menor que m.

Como hemos visto en el lema 3.4, $f_n = f_{mk+r} = f_{mk} \cdot f_{r-1} + f_{mk+1} \cdot f_r$. Por tanto, $MCD(f_m, f_n) = MCD(f_m, f_{mk} \cdot f_{r-1} + f_{mk+1} \cdot f_r)$.

Aplicando el lema 3.5, se tiene que $MCD(f_m, f_n) = MCD(f_m, f_{mk+1} \cdot f_r)$.

Con el lema 3.3 vemos que $MCD(f_{mk}, f_{mk+1}) = 1$. Además, sabemos que f_m divide a f_{mk}, luego $MCD(f_m, f_{mk+1}) = 1$. Se puede deducir fácilmente que $MCD(f_m, f_n) = MCD(f_m, f_r)$.

Si seguimos usando el algoritmo de Euclides en los índices, finalmente llegaremos a $MCD(f_m, f_n) = MCD(f_d, 0) = f_d$ donde $d = MCD(m, n)$. □

Tras esta recopilación de propiedades de la sucesión de Fibonacci, vamos a utilizarlas para demostrar que hay infinitos números primos

Demostración 9 *Supongamos que sólo existe una cantidad finita de números primos $2, 3, ..., p_r$, con algún $p_i = 37$. Estamos suponiendo que lógicamente ya conocemos unos cuantos primos, por ejemplo los menores que 100.*

Consideramos los correspondientes números de Fibonacci $f_2, f_3, ..., f_{p_r}$. Por la proposición 3.1, sabemos que estos números de Fibonacci son primos entre sí, ya que sus índices son números primos. Excluimos $f_2 = 1$. Tenemos r primos y $r - 1$ números de Fibonacci. Por el principio del palomar, uno de ellos tiene que tener dos factores primos mientras que los otros sólo tienen uno. Sin embargo, $f_{37} = 73 \cdot 149 \cdot 2221$ son 3 factores primos, luego llegamos a contradicción. □

En esta demostración se parte de la suposición que existe una cantidad finita de números primos, al igual que la demostración de Euclides, con lo que podíamos pensar que estaría mejor incluirla en la sección correspondiente. Sin embargo, el hecho de trabajar con sucesiones y buscar los divisores comunes de los elementos de dicha sucesión, es similar al trabajo realizado en la demostración de Goldbach.

Para ver algunos ejemplos, tomaremos algunos números primos, los menores que 40 por ejemplo, y calcularemos el elemento de la sucesión de Fibonacci correspondiente.

- $f_3 = 2$, $f_5 = 5$, $f_7 = 13$, $f_{11} = 89$, $f_{13} = 233$, $f_{17} = 1597$, $f_{23} = 28657$, $f_{29} = 514229$, son números primos. Por otro lado, $f_{19} = 4181 = 37 \cdot 113$, $f_{31} = 1346269 = 557 \cdot 2417$ y $f_{37} = 24157817 = 73 \cdot 149 \cdot 2221$, son números compuestos, pero sus factores primos son distintos.

Destacar que no es necesario que los subíndices sean números primos para encontrar primos distintos, basta con que sean primos entre sí, por ejemplo:

- $f_{11} = 89$, $f_{13} = 233$, $f_{14} = 377 = 13 \cdot 29$, $f_{15} = 610 = 2 \cdot 5 \cdot 61$, $f_{17} = 1597$, $f_{19} = 4181 = 37 \cdot 113$, donde vemos que los subíndices son primos entre sí y a su vez los números de Fibonacci obtenidos no tienen factores primos en común.

3.3. Desmostración de Schorn

Otra demostración parecida fue propuesta por Peter Schorn en 1984, la podemos ver en [25]. Schorn es un informático alemán que ha trabajado en matemática discreta y geometría computacional, en el Instituto tecnológico de Zurich donde se doctoró en 1991. En esta demostración no disponemos de una lista con nombre propio, sino que vamos a usar una más conveniente, en la cual utilizamos el factorial de un número. Destacar que en este caso la lista utilizada no es infinita, pero cumple igualmente el objetivo de demostrar la infinitud de los números primos. Para ello, primero necesitamos unos resultados previos.

Lema 3.6 *El factor primo más pequeño de* $(n!)k + 1$ *es mayor que* n*, para cualquier* k*, cumpliendo* $1 \leq k \leq n$*.*

Demostración: Dado $1 \leq k \leq n$, sea d el factor primo más pequeño de $(n!)k + 1$. Supongamos que d es menor o igual que n. Por definición del factorial de un número, d divide a $n!$, luego también divide a $(n!)k$. Como d divide a $(n!)k+1$ y a $(n!)k$, d divide a su resta, es decir que d divide a 1, luego $d = 1$. Como d era un factor primo, llegamos a contradicción, por tanto, d es mayor que n. □

Veamos ahora que los elementos de la lista $(n!)k + 1$ son coprimos dos a dos.

Lema 3.7 *El* $MCD((n!)i + 1, (n!)j + 1) = 1$ *para cualquier pareja* i, j *cumpliendo* i *distinto de* j *y* $1 \leq i, j \leq n$*.*

Demostración: Consideramos dos enteros i, j tales que $1 \leq i < j \leq n$. Podemos escribir $j = i+d$ con $1 \leq d \leq i-1$. Entonces, $MCD((n!)i+1, (n!)j+1) = MCD((n!)i+1, (n!)(i+d)+1) = MCD((n!)i+1, (n!)i+1+(n!)d) = MCD((n!)i+1, (n!)d)$. Ahora bien, aplicando el lema 3.6, tenemos que todos los factores primos de $(n!)i+1$ son mayores que n, por tanto, no pueden dividir a $(n!)d$. Luego, $MCD((n!)i+1, (n!)j+1) = 1$. □

Vistos los resultados, vamos a demostrar la infinitud de los números primos.

Demostración 10 *Supongamos que existe una cantidad finita de números primos, por ejemplo* r*. Tomamos* $n = r + 1$*. Por el lema 3.7, los* n *enteros de la forma* $(n)!k + 1$ *con* $1 \leq k \leq n$ *son coprimos dos a dos, luego cada uno tiene un factor primo distinto. Como tengo* n *elementos , necesito* $n = r + 1$ *números primos, pero sólo existen* r*. Luego, existen más primos de los dados. Con lo que llegamos a contradicción.* □

En esta ocasión, se ha definido la lista de forma que cumpla el lema 3.7, gracias a esto, no necesitamos tantos resultados previos como en las anteriores demostraciones. Por ello, puede parecer que esta demostración es más simple. Sin embargo, en realidad requiere un esfuerzo similar.

No tenemos garantizado que al elegir un elemento de la sucesión sea primo (algo que tampoco necesitamos para ver la infinitud de los números primos), sólo sabemos que cada uno tiene un factor primo distinto. Para ver algún ejemplo, vamos a suponer que sólo hay $r = 6$ números primos.

- Como $r = 6$, tomaremos $n = 7$, tenemos los siguientes elementos en función de k, que puede valer de 1 a 7:

  $(7!) + 1 = 5041 = 71^2$, tenemos un factor primo.

  $(7!)2 + 1 = 10081 = 17 \cdot 593$, tenemos dos factores primos.

  $(7!)3 + 1 = 15121$, el número es primo.

  $(7!)4 + 1 = 20161$, el número es primo.

  $(7!)5 + 1 = 25201 = 11 \cdot 29 \cdot 79$, tenemos tres factores primos.

  $(7!)6 + 1 = 30241$, el número es primo.

  $(7!)7 + 1 = 35281$, el número es primo.

  Tal como hemos demostrado, tenemos, al menos, un factor primo distinto para cada elemento y como tenemos $n = 7$, existen al menos siete primos, aunque nuestra hipótesis inicial era que sólo había seis.

3.4. Demostración de Harris

Al igual que Goldbach, Harris construye una sucesión infinita de números enteros primos entre sí, con lo que cada uno tendrá un factor primo distinto y por tanto, llegaremos a la conclusión de que hay infinitos números primos. Esta demostración fue publicada en 1956 y la podemos ver en [18]. Empecemos definiendo nuestra sucesión, que se define de forma recursiva al igual que la de Fibonacci.

Definición 3.3 *Sean A_0, A_1, A_2 tres números enteros coprimos dos a dos. Para cada $n \geq 3$, $A_n = A_0A_1A_2...A_{n-3}A_{n-1} + A_{n-2}$, la sucesión se define de manera recursiva.*

Ahora que ya tenemos la sucesión definida, veamos que sus elementos son coprimos dos a dos.

Lema 3.8 *Los elementos de la sucesión A_n son coprimos dos a dos.*

Demostración: Vamos a proceder por inducción en n, mostrando que A_n es primo con todos los elementos anteriores.

Como tenemos por hipótesis que A_0, A_1, A_2 ya son primos entre sí, empezaremos con $n = 3$. Por definición $A_3 = A_0A_2 - A_1$ que evidentemente es coprimo con A_0, A_1, A_2, al ser una combinación de los mismos.

Asumimos la hipótesis de inducción cierta para $n-1$, veamos que se cumple para n. Dado i entero menor que n, veamos que A_n y A_i son coprimos, para ello vamos a separarlo en dos casos:

a) Si $i \neq n-2$. Por definición, $A_n = A_0A_1...A_{i-1}A_i...A_{n-3}A_{n-1} + A_{n-2}$, luego $MCD(A_n, A_i) = MCD(A_{n-2}, A_i)$. Ambos subíndices son menores o iguales que $n-1$ y son distintos, luego podemos aplicar la hipótesis de inducción, $MCD(A_{n-2}, A_i) = 1$. Entonces, A_n y A_i son coprimos como queríamos demostrar.

b) Si $i = n-2$. Por definición, $A_n = A_0A_1...A_{n-3}A_{n-1} + A_i$ y por hipótesis de inducción se tiene que A_i y $A_0A_1...A_{n-3}A_{n-1}$ son coprimos. Entonces, $MCD(A_n, A_i) = MCD(A_0A_1A_2...A_{n-3}A_{n-1}, A_i) = 1$. Entonces, A_n y A_i son primos entre sí. □

Ahora que ya tenemos nuestra sucesión con elementos primos entre sí, veamos la demostración de la infinitud de los números primos.

Demostración 11 *Hemos demostrado que los elementos de la sucesión A_n, son coprimos dos a dos, es decir cada uno tiene, al menos, un factor primo distinto. Como en la sucesión tenemos tantos términos como números naturales, tenemos infinitos términos, y sabemos que cada uno tiene un factor primo distinto. Por tanto, podemos deducir que hay infinitos primos.* □

En este caso sí disponemos de una sucesión infinita con elementos primos entre sí, con lo que se asemeja mucho a la demostración de Goldbach. Para ver algunos ejemplos, vamos a elegir los primeros elementos de la sucesión.

- Tomemos $A_0 = 2, A_1 = 3, A_2 = 5$, entonces,

  $A_3 = 2 \cdot 5 + 3 = 13$, que es un número primo.

  $A_4 = 2 \cdot 3 \cdot 13 + 5 = 83$, que es un número primo

  $A_5 = 2 \cdot 3 \cdot 5 \cdot 83 + 13 = 2503$, que es un número primo

  $A_6 = 2 \cdot 3 \cdot 5 \cdot 13 \cdot 2503 + 83 = 976253$, que es un número primo.

  $A_7 = 2 \cdot 3 \cdot 5 \cdot 13 \cdot 83 \cdot 976253 + 2503 = 31601312113 = 7^2 \cdot 71 \cdot 1171 \cdot 7757$, que tiene cuatro factores primos distintos.

3.5. Desmostración de Srinivasan

Disponemos de otra demostración con características similares de la mano de S. Srinivasan, quien publicó la demostración en [27] en 1984. En ella, seguimos con la idea de construir un sucesión infinita cuyos elementos sean coprimos dos a dos para demostrar la infinitud de los números primos.

Esta vez buscaremos una sucesión x_n que cumpla que x_n divida a x_{n+1} y $MCD(x_n, \frac{x_{n+1}}{x_n}) = 1$. Entonces, tendremos que los elementos de la sucesión $\dfrac{x_{n+1}}{x_n}$ son coprimos dos a dos.

Sea $f(x) = x^2 + x + 1$. Dado r un número natural, se tiene que $f(r) \cdot f(-r) = (r^2+r+1)(r^2-r+1) = r^4+r^2+1 = f(r^2)$. Esta función tiene la siguiente propiedad.

Lema 3.9 *Dado r cualquier número natural, se cumple que el $MCD(f(r), f(-r)) = 1$.*

Demostración: Sea r un número natural, $MCD(f(r), f(-r)) = MCD(r^2 + r + 1, r^2 - r + 1) = d$. Se tiene que d divide a la diferencia, es decir d divide a $2r$. Sin embargo, d es impar, ya que d divide a $r^2 + r + 1$ que siempre es impar, luego d divide a r. Entonces, d divide a $r^2 + r$, luego d también divide a la resta de $r^2 + r + 1$ y $r^2 + r$, con lo que d divide a 1, por lo tanto $d = 1$. □

Con las propiedades demostradas de la función, estamos en condiciones de demostrar la infinitud de los números primos.

Demostración 12 *Sea la sucesión $x_n = f(2^{2^n})$. Esta es una sucesión que cumple que x_n divide a x_{n+1}, ya que $x_{n+1} = f(2^{2^{n+1}}) = f((2^{2^n})^2) = f(2^{2^n}) \cdot f(-2^{2^n})$. Además, por el lema 3.9, se tiene que $MCD(x_n, \frac{x_{n+1}}{x_n}) = MCD(f(2^{2^n}), f(-2^{2^n})) = 1$. Por tanto, la sucesión $\dfrac{x_{n+1}}{x_n}$ es una sucesión infinita cuyos elementos son coprimos dos a dos. Como tenemos infinitos términos en la sucesión y cada uno tiene un factor primo distinto, tenemos infinitos números primos.* □

Esta demostración se puede hacer con más sucesiones como menciona Srinivasan. Cabe mencionar que se utiliza la sucesión $x_n = 2^{p^n} - 1$ donde p es un número primo, para demostrar que existen infinitos primos congruentes con 1 mód p.

En este caso para ver algunos ejemplos, veremos la factorización de los primeros elementos de la sucesión $\dfrac{x_{n+1}}{x_n}$, donde $x_n = f(2^{2^n}) = 2^{2^{n+1}} + 2^{2^n} + 1$.

- Primero veamos los valores de x_n desde 0 hasta 5: $x_0 = 7$, $x_1 = 21$, $x_2 = 273$, $x_3 = 65793$, $x_4 = 4295032833$ y $x_5 = 18446744078004518913$

  $\dfrac{x_1}{x_0} = \dfrac{21}{7} = 3$, que es primo.

  $\dfrac{x_2}{x_1} = \dfrac{273}{21} = 13$, que es un primo que no ha aparecido.

  $\dfrac{x_3}{x_2} = \dfrac{65793}{273} = 241$, que es un primo que no ha aparecido.

  $\dfrac{x_4}{x_3} = \dfrac{4295032833}{65793} = 65281 = 97 \cdot 673$, tenemos dos factores primos.

  $\dfrac{x_5}{x_4} = \dfrac{18446744078004518913}{4295032833} = 4294901761 = 193 \cdot 22253377$, tenemos dos factores primos que no han aparecido.

Si quisiéramos continuar, tendríamos un inconveniente y es que $x_6 = 2^{128}+2^{64}+1$ que es del orden de 10^{38}, que son demasiadas cifras para poder calcular todas. Aun así, podríamos calcular $\frac{x_6}{x_5}$. Sin embargo, no nos importa el valor exacto, ni siquiera si es primo o no, ya que lo importante es que tiene, al menos, un factor primo distinto a los ya calculados.

3.6. Relación entre las demostraciones

En las demostraciones de este capítulo hemos partido de un conjunto, infinito o no, y hemos calculado el máximo común divisor entre sus elementos. En cada una, se utiliza un conjunto distinto, con el cual es más o menos sencillo trabajar, ya que algunos están específicamente elegidos para la demostración, como es el caso de Schorn, Harris y Srinivasan. Por otro lado, Goldbach y Wunderlich utilizan sucesiones con nombre propio, que son los números de Fermat y la sucesión de Fibonacci.

La idea fundamental de Goldbach es encontrar una sucesión infinita de elementos primos entre sí, con lo que, utilizando la Proposición 31 del libro VII de Euclides, cada elemento tendrá un factor primo, y como tenemos infinitos elementos, necesariamente existirán infinitos primos. Exactamente este proceso, se ve en las demostraciones de Harris y de Srinivasan.

La demostración que puede parecer más diferente es la de Schorn, ya que utiliza una secuencia finita. Debido a esto, para demostrar que hay infinitos números primos, necesitamos suponer que hay una cantidad finita y encontramos, utilizando la secuencia, otro primo que no está en la lista. Este procedimiento es similar al que utiliza Euclides, sin embargo, como trabajamos con un conjunto y calculamos el máximo común divisor entre sus elementos, obteniendo que son primos entre sí, incluimos esta demostración en este capítulo y no en el anterior.

Otra demostración un poco distinta es la de Wunderlich. Esto se debe a que los elementos de la sucesión no son primos dos a dos. Sin embargo, si existe una subsucesión cuyos elementos son primos entre sí y es la que se obtiene considerando los elementos de la sucesión de Fibonacci cuyo índice sea un número primo. Sin embargo, esta subsucesión no la podemos considerar infinita, ya que lo que queremos es demostrar que hay infinitos primos, con lo que necesitamos suponer que hay una cantidad finita y encontramos alguno que no está en la lista. Es similar al procedimiento que utilizamos en Schorn, con lo que también se podría incluir en Euclides, pero al igual que antes encaja mejor aquí.

Comparando este capítulo con el anterior, se podrían incluir todas estas demostraciones en el anterior. Esto se debe a que dada una sucesión de elementos primos entre sí, si considero que hay finitos primos, utilizando la sucesión puedo encontrar alguno que no está en la lista.

Hay que tener en cuenta que para seguir este procedimiento nos sirve cualquier sucesión con elementos primos entre sí. Por tanto, podríamos tener muchas más demostraciones en este capítulo.

Capítulo 4

Demostraciones basadas en la idea de Euler

En este capítulo, vamos a trabajar con series y sumas finitas. Supondremos que existe una cantidad finita de primos, operaremos en la serie o en la suma y llegaremos a contradicción. Por tanto, existirán infinitos números primos.

4.1. Demostración de Euler

Leonhard Euler fue un matemático suizo del siglo XVIII, el cual es considerado como uno de los matemáticos más importantes de su época. De hecho, se dice que Euler formuló más teoremas en teoría de números que todos sus predecesores juntos. Como ya hemos mencionado antes, Euler y Goldbach mantenían una correspondencia donde trataban distintos temas, principalmente matemáticos. La demostración aquí propuesta fue escrita en 1737 y la podemos ver en [13]. Para entenderla mejor, vamos a ver un resultado previo.

Lema 4.1 *Sea $r \geq 2$ y dados $p_1, p_2, ..., p_r$ números primos distintos, se tiene*

$$\prod_{i=1}^{r}\left(\sum_{k=0}^{\infty}\left(\frac{1}{p_i}\right)^k\right) = \sum_{k_1,k_2,...,k_r=0}^{\infty}\left(\frac{1}{p_1^{k_1}\cdot p_2^{k_2}\cdot ... \cdot p_r^{k_r}}\right)$$

Demostración: Vamos a aplicar inducción en r. Empecemos con $r = 2$. Sean p, q los números primos distintos, entonces,

$$\sum_{k=0}^{\infty}\left(\frac{1}{p}\right)^k \cdot \sum_{k=0}^{\infty}\left(\frac{1}{q}\right)^k = \left(1+\frac{1}{p}+\frac{1}{p^2}+...\right)\cdot\left(1+\frac{1}{q}+\frac{1}{q^2}+...\right) =$$

Multiplicando término a término se obtiene

$$= \left(1+\frac{1}{p}+\frac{1}{q}+\frac{1}{p^2}+\frac{1}{q^2}+\frac{1}{p\cdot q}+...\right) = \sum_{k,h=0}^{\infty}\left(\frac{1}{p^k\cdot q^h}\right)$$

Asumimos cierta la hipótesis de inducción, veamos el caso general.

$$\prod_{i=1}^{r}\left(\sum_{k=0}^{\infty}\left(\frac{1}{p_i}\right)^k\right)=\prod_{i=1}^{r-1}\left(\sum_{k=0}^{\infty}\left(\frac{1}{p_i}\right)^k\right)\cdot\sum_{k=0}^{\infty}\left(\frac{1}{p_r}\right)^k=$$

Aplicando la hipótesis de inducción se tiene

$$=\sum_{k_1,k_2,...,k_{r-1}=0}^{\infty}\left(\frac{1}{p_1^{k_1}\cdot p_2^{k_2}\cdot ...\cdot p_{r-1}^{k_{r-1}}}\right)\cdot\sum_{k=0}^{\infty}\left(\frac{1}{p_r}\right)^k=$$

$$=\sum_{k_1,k_2,...,k_{r-1}=0}^{\infty}\left(\frac{1}{p_1^{k_1}\cdot p_2^{k_2}\cdot ...\cdot p_{r-1}^{k_{r-1}}}\right)\cdot\left(1+\frac{1}{p_r}+\frac{1}{p_r^2}+...\right)=$$

De donde si multiplicamos término a término se obtiene la igualdad que buscábamos

$$=\sum_{k_1,k_2,...,k_{r-1}=0}^{\infty}\left(\frac{1}{p_1^{k_1}\cdot p_2^{k_2}\cdot ...\cdot p_{r-1}^{k_{r-1}}\cdot p_r^0}\right)+\sum_{k_1,k_2,...,k_{r-1}=0}^{\infty}\left(\frac{1}{p_1^{k_1}\cdot p_2^{k_2}\cdot ...\cdot p_{r-1}^{k_{r-1}}\cdot p_r^1}\right)+...=$$

$$=\sum_{k_1,k_2,...,k_{r-1}=0}^{\infty}\left(\frac{1}{p_1^{k_1}\cdot p_2^{k_2}\cdot ...\cdot p_r^{k_r}}\right)$$

□

Para ver la infinitud de los números primos, vamos a proceder por contradicción.

Demostración 13 *Supongamos que tenemos una cantidad finita de números primos,* $p_1, p_2, ..., p_r$. *Consideramos el siguiente producto*

$$\prod_{i=1}^{r}\left(\sum_{k=0}^{\infty}\left(\frac{1}{p_i}\right)^k\right)$$

Por un lado, aplicando el lema 4.1, se tiene

$$\prod_{i=1}^{r}\left(\sum_{k=0}^{\infty}\left(\frac{1}{p_i}\right)^k\right)=\sum_{k_1,k_2,...,k_r=0}^{\infty}\left(\frac{1}{p_1^{k_1}\cdot p_2^{k_2}\cdot ...\cdot p_r^{k_r}}\right)$$

Teniendo en cuenta que sólo existen r primos y utilizando el Teorema Fundamental de la Aritmética, se deduce que cada número natural aparece una única vez en la parte derecha de la igualdad. Por tanto, se tiene

$$\prod_{i=1}^{r}\left(\sum_{k=0}^{\infty}\left(\frac{1}{p_i}\right)^k\right)=\sum_{k=1}^{\infty}\frac{1}{k}$$

Es claro que esta serie es divergente, con lo que el producto también.

Por otro lado, si consideramos la serie

$$1 + \frac{1}{p_i} + \frac{1}{p_i^2} + ... = \sum_{k=0}^{\infty} \left(\frac{1}{p_i}\right)^k$$

es una serie geométrica de razón $\frac{1}{p_i} < 1$*, luego es convergente. Entonces, podemos escribir*

$$\sum_{k=0}^{\infty} \left(\frac{1}{p_i}\right)^k = \frac{1}{1-p_i} = \frac{p_i}{p_i - 1}$$

Con lo que podemos reescribir el producto inicial como

$$\prod_{i=1}^{r} \left(\sum_{k=0}^{\infty} \left(\frac{1}{p_i}\right)^k \right) = \prod_{i=1}^{r} \left(\frac{p_i}{p_i - 1} \right)$$

que es un producto finito y por tanto convergente. Como conclusión hemos obtenido por un lado que el producto es divergente y por otro, que es convergente, luego llegamos a una contradicción. Por tanto, necesariamente existirán infinitos primos. □

Esta demostración no es constructiva, ya que no buscamos en ningún momento un nuevo primo o que sean infinitos. Por este motivo, esta demostración es novedosa respecto a las ya vistas y de hecho no podemos hacer ningún ejemplo, ya que no tendría sentido.

4.2. Demostración de Chebysheff

Chebysheff fue un matemático ruso del siglo XIX que dedicó la mayor parte de sus estudios al área de la probabilidad. No obstante también trabajó en teoría de números, utilizando la propiedad aritmética del factorial para demostrar el postulado de Bertrand. También dio una demostración de la infinitud de los números primos, que podemos ver en [32]. Para ello vamos a ver primero unos resultados previos.

Lema 4.2 *Dado N un número natural y p cualquier número primo, se define $a(p, N)$ como el mayor exponente del primo p dividiendo a $N!$. Si p es mayor que N, $a(p, N) = 0$. Por otro lado, si p es menor o igual que N, entonces se cumple*

$$a(p, N) < \frac{N}{p-1}$$

Demostración: Es claro que si p es mayor que N, p no divide a $N!$ y por tanto el mayor exponente que lo divide es 0. Luego, en este caso $a(p, N) = 0$.

Ahora suponemos que p es menor o igual que N. Para ver cuanto vale $a(p, N)$ vamos a calcular el número de veces que aparece p multiplicando en el factorial de N.

Podemos escribir $N = q_p \cdot p + r_p$. Por tanto, el número de veces que aparece p multiplicando en $N!$ es $q_p = \left\lfloor \frac{N}{p} \right\rfloor$. Si p^2 es menor o igual que N, existen enteros en el intervalo $(1, N)$ divisibles por p^2 y la aportación de estos enteros en $a(p, N)$ es dos, mientras que sólo habíamos tenido en cuenta uno. De nuevo, escribimos $N = q_{p^2} \cdot p^2 + r_{p^2}$ y hemos de añadir $\left\lfloor \frac{N}{p^2} \right\rfloor$ a $a(p, N)$. Repetimos este procedimiento mientras p^h sea menor o igual que N. Por lo tanto, finalmente llegamos a que

$$a(p,N) = \left\lfloor \frac{N}{p} \right\rfloor + \left\lfloor \frac{N}{p^2} \right\rfloor + \ldots + \left\lfloor \frac{N}{p^h} \right\rfloor < \frac{N}{p} + \frac{N}{p^2} + \ldots + \frac{N}{p^h} = N \frac{p^{h-1} + p^{h-2} + \ldots + p + 1}{p^h} =$$

$$= \frac{N}{p^h} \sum_{i=0}^{h-1} p^i = \frac{N}{p^h} \cdot \frac{p^{h-1} - 1}{p-1} = \frac{N}{p-1} \cdot \frac{p^{h-1} - 1}{p^h}$$

Como $p^{h-1} - 1$ es más pequeño que p^h, la fracción es más pequeña que 1 y por tanto llegamos a que

$$a(p,N) < \frac{N}{p-1}$$

□

Necesitamos también otro resultado relativo al logaritmo del factorial de un número.

Lema 4.3 *Sea N cualquier número natural, entonces,*

$$\frac{1}{N} \cdot \ln(N!) > ln(N) - 1$$

Demostración: Sea N un número natural, empecemos tomando la definición de la exponencial como serie de potencias, es decir $e^N = \sum_{k=0}^{\infty} \frac{N^k}{k!}$. Es claro que si cogemos cualquier término de la serie será menor que la exponencial, por tanto tenemos

$$e^N > \frac{N^N}{N!}, \text{ o lo que es lo mismo, } N! > \frac{N^N}{e^N}$$

tomando logaritmos y aplicando sus propiedades

$$\ln(N!) > \ln\left(\frac{N^N}{e^N}\right) = N \ln(N) - N$$

dividiendo a ambos lados por N llegamos a la desigualdad buscada

$$\frac{1}{N} \cdot \ln(N!) > \ln(N) - 1$$

□

Con estos resultados vamos a demostrar la infinitud de los números primos.

Demostración 14 *Consideramos la siguiente suma* $\sum_{p\leq N}\frac{\ln p}{p-1}$. *Operando y utilizando los lemas previos se tiene*

$$\sum_{p\leq N}\frac{\ln p}{p-1}=\sum_{p\leq N}\frac{N\ln p}{N(p-1)}>\sum_{p\leq N}\frac{a(p,N)\ln p}{N}=\frac{1}{N}\cdot\ln(N!)>\ln(N)-1$$

Como el lado derecho de la desigualdad tiende a infinito cuando N *tiende a infinito, el lado izquierdo también tiende a infinito, por tanto tiene que haber infinitos números primos, ya que si fuesen una cantidad finita la suma no tendería a infinito.* □

Al igual que en la demostración de Euler, nos ayudamos de una serie para demostrar la infinitud de los números primos. Tampoco es posible realizar ningún ejemplo.

Como hemos mencionado, Chebysheff fue el primero en demostrar el postulado de Bertrand, el cual nos dice lo siguiente:

Teorema 4.1 *Dado* n *un número natural mayor que 1, siempre existe un número primo* p *entre* n *y* $2n$.

Si bien es cierto que la demostración se sale de los límites del trabajo y no tiene cabida en él, el postulado si que es interesante, ya que podemos demostrar la infinitud de los números primos utilizándolo.

Demostración 15 *Fijamos* n *como un número entero mayor que 1 y consideramos los intervalos* $(n,2n),(2n,4n),(4n,8n),\ldots$. *Por el postulado de Bertrand, en cada intervalo hay un primo distinto y como tenemos infinitos intervalos, existirán infinitos números primos.*

4.3. Demostración de Perott

J. Perott fue un matemático del siglo XIX, que realizó la mayor parte de su trabajo en Fracia, donde se interesó por diversos temas matemáticos. Uno de ellos fue la infinitud de los números primos, la cual demostró en 1881, la podemos ver en [24] y en [25].

Para esta demostración, necesitamos trabajar con $\sum_{n=1}^{\infty}\frac{1}{n^2}$ que es una serie convergente, como probó Euler, obteniendo el valor exacto de la suma, que es $\frac{\pi^2}{6}$. En este caso nos basta con que sea convergente y de valor menor que 2. Vamos a verlo.

$$\sum_{n=1}^{\infty}\frac{1}{n^2}<\sum_{n=1}^{\infty}\frac{n^2+n+1}{n^2+n}=1+\sum_{n=1}^{\infty}\frac{1}{n(n+1)}=1+\sum_{n=1}^{\infty}\left(\frac{1}{n}-\frac{1}{n+1}\right)=1+1=2$$

Ahora vamos con la demostración de la infinitud de los números primos.

Demostración 16 *Supongamos que sólo existen r números primos, $p_1 < p_2 < ... < p_r$. Sea N un número entero tal que $p_1 \cdot p_2 \cdot ... \cdot p_r < N$. Definimos $\delta = 2 - \sum_{n=1}^{\infty} \frac{1}{n^2}$, que es mayor que 0.*

Como sólo tenemos r números primos, aplicando el Teorema Fundamental de la Aritmética, obtenemos que cada número natural se tiene que escribir como combinación de estos números primos. Por tanto, el número de enteros menores o iguales que N que no son divisibles por un cuadrado es 2^r, ya que es la cantidad de todos los posibles conjuntos que podemos hacer con r primos sin que se repita ninguno.

Por otro lado, el número de enteros menores o iguales que N que son divisibles por p_i^2, es como mucho $\frac{N}{p_i^2}$. Por lo tanto, el número de enteros menores o iguales que N divisibles por algún cuadrado (asumiendo que sólo existen los primos $p_1, \ldots, p_r$) es como mucho $\sum_{i=1}^{r} \frac{N}{p_i^2}$. Teniendo en cuenta que $\sum_{i=1}^{r} \frac{1}{p_i^2} < \sum_{n=1}^{\infty} \frac{1}{n^2} - 1$, ya que en la parte izquierda están los cuadrados de todos los primos y en la parte derecha están los cuadrados de todos los números menos el 1, que lo quitamos porque nos conviene, tenemos la siguiente desigualdad.

$$N \leq 2^r + \sum_{i=1}^{r} \frac{N}{p_i^2} < 2^r + N\left(\sum_{n=1}^{\infty} \frac{1}{n^2} - 1\right) = 2^r + N(1-\delta)$$

Por tanto

$$0 \leq 2^r - N\delta$$

Con lo que, si elegimos un N tal que $N\delta > 2^r$ llegamos a contracción. □

De forma similar a como vimos en la demostración de Euler, en este caso partimos de una serie y utilizamos sus características para llegar a una contradicción. También suponemos que hay una cantidad finita de primos, pero es necesario si queremos probar la infinitud por contradicción. No tiene sentido trabajar con ejemplos, ya que no vamos a generar nuevos primos.

4.4. Demostración de Braun

Además de con series, también se puede demostrar la infinitud de los números primos utilizando sumas finitas. J. Braun la propuso en 1899, la podemos ver en [4]. Esta demostración destaca por su sencillez, además de mezclar las ideas de Euclides y Euler, ya que utiliza sumas pero busca primos que no están en la lista inicial.

Demostración 17 *Supongamos que tenemos una cantidad finita de números primos, $p_1, p_2, ..., p_r$, con r mayor o igual que 2. Sea N el producto de todos ellos, es decir $N = p_1 p_2 ... p_r$. Consideramos*

$$\sum_{i=1}^{r} \frac{1}{p_i} = \frac{1}{p_1} + \frac{1}{p_2} + ... \frac{1}{p_r} = \frac{p_2 ... p_r + p_1 p_3 ... p_r + ... + p_1 p_2 ... p_{r-2} p_r + p_1 p_2 ... p_{r-1}}{N} = \frac{a}{N}$$

Es claro que a es mayor que 1, luego por la proposición 2.2, tendrá un factor primo. Si este factor primo p_k está en la lista inicial, como $a = \sum_{i=1}^{r} \frac{N}{p_i}$, p_k tiene que dividir a $\frac{N}{p_k}$, que es imposible. Por tanto, hemos encontrado un número primo que no está en nuestra lista inicial. Por tanto, llegamos a contradicción. □

Como podemos ver esta demostración es muy sencilla y sólo requiere trabajar un poco con la suma de los inversos de los números primos. Por un lado, supone que hay una cantidad finita de primos y, utilizando sumas finitas, llega a contradicción, por lo que bien podría encajar en este capítulo. Por otro lado, a partir de una lista finita de primos, encuentra otro que no está en la lista original, lo que recuerda a Euclides. La incluimos en este capítulo porque no utiliza exactamente el mismo procedimiento de las demostraciones del capítulo referente a Euclides.

En este caso, al ser parecida a la demostración de Euclides, podemos ver algún ejemplo, ya que buscamos números primos que no están en la lista inicial.

- Sea $\mathcal{P} = \{2, 3, 5, 7, 11\}$ nuestra lista finita de primos. Consideramos la suma de sus inversos

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} = \frac{1155 + 770 + 462 + 330 + 210}{2310} = \frac{2927}{2310}$$

  como 2927 es primo obtenemos un nuevo número primo que no está en nuestra lista inicial.

- Sea $\mathcal{Q} = \{3, 5, 7, 11\}$ nuestra lista finita de primos. Consideramos la suma de sus inversos

$$\frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} = \frac{385 + 231 + 165 + 105}{1155} = \frac{886}{1155}$$

  como $886 = 2 \cdot 443$ obtenemos dos factores primos que no están en nuestra lista inicial.

4.5. Relación entre las demostraciones

En este capítulo hemos trabajado con series, y sumas finitas para poder demostrar la infinitud de los números primos. El procedimiento que hemos seguido es suponer que hay una cantidad finita de números primos, salvo en la de Chebysheff, y, operando en la serie o en la suma finita, llegamos a contradicción, por lo que hay infinitos. Destacar que esta idea general es diferente a las ya vistas. Aunque suponemos que hay una cantidad finita de primos igual que en las demostraciones del capítulo de Euclides, no encontramos un número primo que no está en la lista inicial, salvo en la de Braun. Con respecto a las del capítulo de Goldbach, no trabajamos con sucesiones ni con elementos primos entre sí, por lo que son bastante diferentes.

Euler fue el primero en proponer este tipo de demostración en la cual supone que existe una cantidad finita de primos, opera en una serie y obtiene por un lado que

es convergente y por otro divergente, con lo que llegamos a contradicción. Por tanto, existirán infinitos primos. Este mismo procedimiento pero con otra serie lo realiza Perott. La única diferencia es que Perott alcanza una desigualdad que no se cumple.

La demostración de Chebysheff puede parecer diferente, ya que no supone que hay una cantidad finita de primos. Sin embargo, también trabaja con series, en este caso con una que depende de los números primos menores que un cierto número. Se demuestra que esta serie es divergente, por lo que la cantidad de números primos tiene que ser infinita, ya que sino la suma sería finita. No obstante, podemos hacer que sea similar a la de Euler, para ello si suponemos al principio que sólo hay una cantidad finita de primos, al final llegamos a que tenemos una serie convergente y divergente a la vez, al igual que en la demostración de Euler, llegando a contradicción.

La demostración de Braun comienza igual que la de Euler, suponiendo que hay una cantidad finita de números primos, sin embargo, en este caso trabajamos con una suma finita y encontramos un nuevo primo que no está en la lista inicial, con lo que llegamos a contradicción. Esta idea de encontrar un número primo que no esté en la lista inicial es del capítulo de Euclides.

Hay que tener en cuenta que podemos tener más demostraciones de este tipo, para ello necesitamos una serie en la que intervengan números primos y trabajando con ella llegar a una contradicción de algún tipo.

Capítulo 5

Demostraciones basadas en combinatoria

La combinatoria es la rama de las matemáticas que estudia las diferentes posibilidades en que se pueden agrupar los elementos de un conjunto. En estas demostraciones, vamos a calcular los números a partir de los exponentes dados en la descomposición en factores primos, dada por el Teorema Fundamental de la Aritmética. Como en otras demostraciones, supondremos que hay una cantidad finita de números primos y llegaremos a contradicción. Por lo tanto, existirán infinitos primos.

5.1. Demostración de Thue

Axel Thue fue un matemático noruego de finales del siglo XIX que trabajó principalmente en combinatoria y en aproximaciones diofánticas. En 1897 desarrolló una demostración de la infinitud de los números primos que utiliza el Teorema Fundamental de la Aritmética, la podemos ver en [29].

Demostración 18 *Sean n, k dos números enteros mayores o iguales que 1 que cumplen $(1+n)^k < 2^n$. Sean $p_1 = 2, p_2 = 3, \ldots, p_r$ todos los primos menores que 2^n. Supongamos que r es menor o igual que k.*

Por el Teorema Fundamental de la Aritmética, cada entero m menor o igual que 2^n se puede escribir de forma única como una combinación de los primos dados, es decir $m = 2^{e_1} \cdot 3^{e_2} \cdot \ldots \cdot p_r^{e_r}$. Se tiene que $0 \leq e_i \leq n$ para todo i, esto se debe a que si uno fuese mayor, por ejemplo $e_i = n+1$ se tendría $m = 2^{e_1} \cdot 3^{e_2} \cdot \ldots p_i^{e_i} \cdot \ldots \cdot p_r^{e_r} \geq p_i^{n+1} \geq 2^{n+1} > 2^n$, que es una contradicción.

El número de posibilidades para cada exponente es $n+1$, luego la cantidad de elecciones para todos los exponentes es menor o igual que $(n+1)^r$. Entonces, tenemos que $2^n \leq (n+1)^r \leq (n+1)^k < 2^n$, que es absurdo. Por tanto, r es mayor k.

Si fijamos $n = 2k^2$ para cada entero k mayor o igual que 1, tenemos que $1 + 2k^2 < 2^{2k}$ y, elevando a la k, $(1+2k^2)^k < 2^{2k^2} = 4^{k^2}$, que es la desigualdad inicial $(1+n)^k < 2^n$. Por tanto, para cada k mayor o igual que 1 existen al menos $k+1$

números primos menores que 4^{k^2}. Como podemos elegir cualquier k, deducimos que hay infinitos números primos. □

De la parte final de la demostración podemos deducir una cota para la cantidad de primos menores que 4^{k^2}; existen $k+1$ números primos. Como el número crece exponencialmente mientras que la cota crece de forma polinómica, deducimos que la cota no es buena. Podemos ver un ejemplo tomando $k=5$ y $k=6$. Se tiene que existen 6 números primos menores que $4^{25} \simeq 10^{15}$ y 7 números primos menores que $4^{36} \simeq 10^{21}$. Por tanto, solo hemos podido demostrar que existe un primo en el intervalo $(10^{15}, 10^{20})$.

Un punto a tener en cuenta en esta demostración, es la forma de obtener los enteros n y k que cumplan la desigualdad $(1+n)^k < 2^n$. En la demostración directamente elegimos un caso particular, $n = 2k^2$, pero podemos obtenerlos de forma sencilla. Para ello, tomamos logaritmos en base 2 a ambos lados la desigualdad y obtenemos $k \cdot \log_2(1+n) < n$ o equivalentemente $k < \dfrac{n}{\log_2(n+1)}$, por lo que a partir de cualquier n, podemos calcular el k.

Hacer ejemplos en este caso no tiene sentido, porque no estamos calculando nuevos primos, simplemente deducimos que hay infinitos.

5.2. Demostración de Auric

Otra demostración similar fue propuesta por Auric en 1915, podemos verla en [2]. Al igual que Thue, utiliza el Teorema Fundamental de la Aritmética para factorizar los números menores que otro dado y así llegar a contradicción.

Demostración 19 *Supongamos que sólo existe una cantidad finita de números primos, $p_1 < p_2 < \ldots < p_r$. Sea t cualquier número entero mayor o igual que 1 y sea $N = p_r^t$.*

Por el Teorema Fundamental de la Aritmética, cada entero positivo m menor o igual que N se escribe como $m = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$ donde la r-tupla $(e_1, e_2, \ldots, e_r)$ queda definida de forma única. Sea $E = \dfrac{\ln p_r}{\ln p_1}$, como $p_1^{e_i} \leq p_i^{e_i} \leq N = p_r^t$, tomando logaritmos, se tiene que cada $e_i \leq t \cdot E$. Por tanto, la cantidad de r-tuplas que podemos definir es como mucho $(1 + t \cdot E)^r$.

Como cada entero queda determinado de forma única por la r-tupla, N es como mucho el número de r-tuplas $(e_1, e_2, \ldots, e_r)$ y por lo tanto $p_r^t = N \leq (t \cdot E + 1)^r \leq t^r \cdot (E+1)^r$. Como la función exponencial crece más rápido que una función polinómica, para cierto t y valores mayores, la función exponencial será mayor que la polinómica. Entonces, llegamos a contradicción con la desigualdad. □

Esta demostración es más sencilla que la de Thue, ya que no requiere de números que cumplan ciertas características. Por contra, no da ninguna cota para los primos. Tampoco es posible realizar ejemplos.

5.3. Demostración de Chernoff

Una demostración más reciente, es de 1965, fue propuesta por el matemático estadounidense Paul R. Chernoff, la podemos ver en [8]. Es similar a las anteriores, pero necesitamos dar algún comentario breve sobre símplices (ver por ejmplo [30]).

Definición 5.1 *Se define símplice de dimensión d como la envolvente conexa de $d+1$ puntos afínmente independientes en $\mathbb{R}^d$.*

Teorema 5.1 *Dado S un símplice de dimensión d generado por los vértices $v_1, v_2, \ldots, v_d$, v_{d+1}, el volumen euclídeo de dicho símplice es*

$$Vol(S) = \frac{1}{d!} \det \begin{pmatrix} 1 & 1 & \ldots & 1 & 1 \\ v_1 & v_2 & \ldots & v_d & v_{d+1} \end{pmatrix}$$

donde las coordenadas de los vectores v_i van en columna

Demostración 20 *Supongamos que sólo existen r primos, $p_1, p_2, \ldots, p_r$. Sea N un número entero mayor que 1. Por el Teorema Fundamental de la Aritmética, para cada entero positivo m menor o igual que N, existe una descomposición de la forma $m = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$ donde cada exponente es un entero no negativo. Como cada entero está asociado a una r-tupla, tenemos N r-tuplas de enteros no negativos $(e_1, e_2, \ldots e_r)$ que satisfacen la siguiente desigualdad $p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r} \leq N$, si tomamos logaritmos y aplicamos sus propiedades tenemos*

$$e_1 \ln p_1 + e_2 \ln p_2 + \ldots e_r \ln p_r \leq \ln N$$

Si lo vemos desde el punto de vista de símplices, el número de r-tuplas será el número de puntos del retículo contenido en el símplice de dimensión r, definido por las siguientes $r+1$ ecuaciones.

$$x_1 \ln p_1 + x_2 \ln p_2 + \ldots x_r \ln p_r \leq \ln N,\ x_i \geq 0$$

Por tanto, el número de r-tuplas será como mucho el volumen de dicho símplice, cuyos vértices obtenemos de las ecuaciones anteriores y son $v_1 = (0, 0, \ldots, 0)$, $v_2 = (\frac{\ln N}{\ln p_1}, 0, 0, \ldots, 0)$, $v_3 = (0, \frac{\ln N}{\ln p_2}, 0, 0, \ldots, 0)$, $\ldots$, $v_r = (0, 0, \ldots, \frac{\ln N}{\ln p_{r-1}}, 0)$, $v_{r+1} = (0, 0, \ldots, \frac{\ln N}{\ln p_r})$. Aplicando el teorema 5.1, obtenemos que el volumen es

$$\frac{(\ln N)^r}{r! \cdot \ln p_1 \cdot \ln p_2 \cdot \ldots \cdot \ln p_r}$$

Por tanto, $N \leq c \cdot (\ln N)^r$ para cierta constante c independiente de N. Como una función logarítmica crece más despacio que una función polinómica, para un cierto N y valores superiores, la función logarítmica será menor que la polinómica. Esto es justo lo contrario que la desigualdad anterior, con lo que llegamos a contradicción. □

5.4. Demostraciones de Erdös

Paul Erdös, del que ya hablamos en la introducción, fue un matemático húngaro que vivió en el siglo XX, que estudió problemas sobre combinatoria, teoría de grafos, teoría de números, análisis, teoría de aproximación, teoría de conjuntos y probabilidad, es decir casi todos los campos de las matemáticas. Dichos estudios los realizaba en diferentes universidades y con distintos compañeros, pues no solía permanecer mucho tiempo en el mismo sitio. Muchos de estos trabajos no fueron publicados mientras el estaba con vida, por ello es uno de los matemáticos más prolíficos de todos los tiempos. Como homenaje a su carrera, se inventó el número de Erdös. Este número mide la distancia en colaboradores entre un individuo y Erdös. Para calcularlo hay que seguir la siguiente regla: Erdös tiene asignado el número 0, los que colaboraron directamente con él tienen el 1, alguien que haya trabajado con alguno de estos colaboradores tendrá el 2, y así sucesivamente.

Entre sus trabajos, encontramos una demostración nueva de la infinitud de los números primos de 1938, pero además también demostró que la suma de los inversos de los números primos es infinita, lo que también implica la infinitud de estos. Ambas demostraciones las podemos ver en [17].

Veamos primero un lema, que nos permite factorizar cualquier entero como un factor libre de cuadrados y un cuadrado perfecto.

Lema 5.1 *Cada número entero n mayor que 1 es el producto de un entero libre de cuadrados y un cuadrado perfecto.*

Demostración: Sea n un número entero mayor que 1. Del Teorema Fundamental de la Aritmética, se deduce que $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, donde los p_i son primos distintos y los e_1 son enteros positivos. Cada e_i es par o impar, por lo que podemos escribir $e_i = 2q_i + r_i$, donde $r_i = 1$ para los exponentes impares y $r_i = 0$ para los pares. Para los e_i impares tenemos $p_i^{e_i} = p_i^{2q_i+r_i} = p_i^{2q_i+1} = p_i^1 p_i^{2q_i}$.

Aplicando las propiedades de la multiplicación, podemos reordenar el producto inicial. Llamaremos a al producto de todos los factores primos de la forma p^1 y b al producto del resto de factores, que son de la forma p^{2q_i}. Como a es el producto de primos distintos, a es libre de cuadrados. Como b es el producto de primos con exponente par, b es un cuadrado perfecto. Luego, como n era un entero cualquiera, cada entero mayor que 1 es el producto de un entero libre de cuadrados y un cuadrado perfecto. □

Visto el resultado, veamos ahora cómo demuestra Erdös la infinitud de los números primos.

Demostración 21 *Supongamos que existe una cantidad finita de primos $p_1 = 2, p_2 = 3, \dots, p_r$ y sea n un entero mayor que 1. Por el lema 5.1, podemos escribir n como el producto de un entero libre de cuadrados y un cuadrado perfecto, es decir $n = a \cdot b^2$.*

Aplicando el Teorema Fundamental de la Aritmética, tenemos que $a = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ donde cada e_i es 0 o 1, ya que a es libre de cuadrados. Como para cada exponente

tenemos dos opciones, en total tenemos 2^r posibilidades para los exponentes y por lo tanto tenemos, como máximo, 2^r diferentes valores para a. Fijado a, tenemos $b \leq \sqrt{n}$, luego no existen más de $\sqrt{n}$ posibles valores de b para cada a.

Entonces, tenemos $n \leq 2^r\sqrt{n}$ o, elevando al cuadrado y operando, $n \leq 2^{2r}$. Como es cierto para todo n mayor que 1, tomando $n = 2^{2r} + 1$ llegamos a contradicción. □

Como hemos visto en la demostración, si n es cualquier número entero cuya factorización sea $n = p_1^{e_1}p_2^{e_2}\dots p_r^{e_r}$, siempre se cumple la desigualdad $n \leq 2^r\sqrt{n}$. Esta idea se puede utilizar para demostrar que la suma de los inversos de los primos es divergente, lo que prueba su infinitud.

Teorema 5.2 *La suma de los inversos de los números primos es infinita, es decir la serie*

$$\sum \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \dots$$

es divergente.

Demostración: Supongamos que la serie es convergente, entonces existirá un p_i tal que

$$\frac{1}{p_{i+1}} + \frac{1}{p_{i+2}} + \dots < \frac{1}{2}$$

Entonces, para cualquier entero n, se tiene

$$\sum_{p>p_i} \frac{n}{p} < \frac{n}{2}$$

Ahora dividimos los enteros menores que n en dos conjuntos. Sea n_1 el número de enteros positivos menores que n que son divisibles por algún primo mayor que p_i y n_2 el resto de enteros menores que n.

Entonces, tenemos $n_1 \leq \sum_{p>p_i} \left\lfloor \frac{n}{p} \right\rfloor \leq \sum_{p>p_i} \frac{n}{p} < \frac{n}{2}$. Para calcular n_2 vamos a aplicar un razonamiento similar al de la demostración anterior. Si k es un número entero menor que n que no es divisible por ningún primo mayor que p_i, por el teorema fundamental de la aritmética, $k = p_1^{e_1}p_2^{e_2}...p_i^{e_i}$. Ahora aplicando el lema 5.1, escribimos $k = a \cdot b^2$, donde a es libre de cuadrados, luego tenemos 2^i posibles valores y b es un cuadrado perfecto, luego $b \leq \sqrt{k} < \sqrt{n}$. Entonces, tenemos $n_2 < 2^i\sqrt{n}$. Por tanto, si tomamos un n suficientemente grande, $n = n_1 + n_2 < \frac{n}{2} + 2^{p_i}\sqrt{n} < n$, con lo que llegamos a contradicción. □

Una vez visto que la suma de los inversos de los números primos es infinita podemos demostrar de forma sencilla la infinitud de los mismos.

Demostración 22 *Supongamos que existe una cantidad finita de primos. Consideraremos la suma de los inversos de todos los primos $\sum \frac{1}{p}$. Hemos visto en el lema anterior que la serie es divergente, pero al ser una cantidad finita de elementos, la suma tiene que ser finita. Por lo tanto, llegamos a contradicción.*

Esta demostración es similar a las del capítulo dedicado a Euler, ya que, suponiendo que existe una cantidad finita de primos, tenemos una suma que es a la vez divergente y convergente, que es absurdo.

5.5. Relación entre las demostraciones

Como en la mayoría de las demostraciones vistas hasta ahora, las demostraciones de este capítulo suponen que existe una cantidad finita de números primos y llegan a contradicción. Sin embargo, lo que las hace diferentes es que utilizamos el Teorema Fundamental de la Aritmética para escribir cada número positivo como la tupla de los exponentes de su factorización en números primos, ya que esta es única.

En las demostraciones de Thue y de Auric, descomponemos cualquier número menor que una cierta cota, para obtener todas las posibles tuplas de exponentes. Con ello, llegamos a una desigualdad la cual no se cumple siempre.

Chernoff también utiliza la descomposición de un número en sus factores primos, pero también utiliza nociones de símplices, lo que complica un poco la demostración. No obstante, al utilizar otra rama de las matemáticas, también se enriquece la demostración.

Las dos demostraciones propuestas por Erdös utilizan la misma idea, separar los números en dos factores uno libre de cuadrados y un cuadrado perfecto y sobre el primero aplica el Teorema Fundamental de la Aritmética para obtener la tupla y llegar a contradicción. Es cierto que la segunda demostración podría incluirse en la sección de Euler, ya que demuestra que la suma de los inversos de los números primos es divergente, lo que encaja con las series de dicho capítulo. Sin embargo, lo incluimos aquí para no separar las demostraciones del mismo autor.

Las demostraciones de este capítulo siguen el mismo procedimiento que algunas de las ya vistas. Suponen que hay una cantidad finita de primos y llegan a contradicción. Sin embargo, la gran diferencia es que en este caso trabajamos con posibilidades, es decir con las diferentes formas en las que podemos escribir un número en función de su descomposición en factores primos. Para esto no nos sirve la Proposición 31 del libro VII de Euclides porque sólo nos garantiza la existencia de un único factor primo y para estas demostraciones necesitamos la factorización en todos sus factores primos. Además, no encontramos más primos que los dados como sucede en las demostraciones de dicho capítulo.

Capítulo 6

Una demostración topológica

Otra forma novedosa de demostrar la infinitud de los números primos es utilizando resultados y razonamientos topológicos. Para ello vamos a utilizar una topología específica y veremos que el conjunto de los números primos es infinito. También vamos a ver que es posible reescribir la demostración de tal forma que no utilicemos elementos topológicos, aunque si seguiremos la idea principal.

6.1. Demostración de Furstenberg

Harry Furstenberg es un matemático israelí que realizó, en 1955 la primera demostración de la infinitud de los números primos utilizando argumentos topológicos. Lo que vamos a demostrar es que el conjunto de los números primos es infinito. Esta demostración la podemos ver en [14].

Para ello recordemos la definición de topología.

Definición 6.1 *Sea X un conjunto y $P(X)$ el conjunto de sus subconjuntos, también llamado partes de X. Una topología sobre X es un conjunto $\tau \subseteq P(X)$ que cumple las siguientes propiedades.*

1.- El conjunto vacío, $\emptyset$, y el total, X, pertenecen a τ.

2.- Si $A, B \in \tau$, entonces $A \cap B \in \tau$.

3.- Si $A_i \in \tau$, entonces $\bigcup_i A_i \in \tau$.

Recordemos que los elementos de una topología τ se denominan abiertos y el complementario de un conjunto abierto se denomina cerrado.

Definición 6.2 *Sea $\mathbb{Z}$ el conjunto de los números enteros. Dados $a, b \in \mathbb{Z}$, definimos las progresiones aritméticas como $S(a,b) = \{an + b; n \in \mathbb{Z}\} = a\mathbb{Z} + b$. También definimos el siguiente conjunto $\tau = \{U \subseteq \mathbb{Z} / \ U = \emptyset \ o \ U = \bigcup S(a,b)\}$.*

Esta definición del conjunto τ es equivalente a decir que $U \in \tau$ si para todo x perteneciente a U existe algún entero a distinto de 0 tal que $S(a,b) \subseteq U$.

Veamos ahora que el conjunto τ así definido nos proporciona una topología sobre $\mathbb{Z}$.

Proposición 6.1 *El conjunto τ es una base para una topología sobre $\mathbb{Z}$.*

Demostración: Vamos a comprobar que τ es una topología sobre $\mathbb{Z}$:

1.- Por definición, $\emptyset \in \tau$. Por otro lado, $\mathbb{Z} = S(1,0)$, por lo que también es abierto.

2.- Sean $A, B \in \tau$ y sea $x \in A \cap B$, sabemos que existen a_1, a_2, tales que $S(a_1, x) \subseteq A$ y $S(a_2, x) \subseteq B$. Sea a el mínimo común múltiplo de a_1 y a_2. Entonces, $S(a, x) \subseteq S(a_1) \subseteq A$ y $S(a, x) \subseteq S(a_2) \subseteq B$, luego $S(a, x) \subseteq A \cap B$. Por tanto, $A \cap B \in \tau$.

3.- Si $A_i \in \tau$, como cada conjunto es vacío o unión de progresiones geométricas, al hacer la unión de todos ellos también obtenemos que el conjunto es vacío o unión de progresiones geométricas, por tanto, $\bigcup_i A_i \in \tau$. □

Esta topología cumple dos propiedades necesarias para la demostración.

Lema 6.1 *El complementario de un conjunto finito no puede ser un conjunto cerrado de la topología τ.*

Demostración: Como cada abierto de τ distinto del vacío contiene al menos una progresión, se tiene que ningún conjunto finito puede ser abierto, es decir todos los conjuntos abiertos son infinitos. Con ello, se ve que el complementario de un conjunto finito no puede ser un conjunto cerrado, ya que sino ese conjunto finito sería abierto y ya hemos visto que no puede ocurrir. □

Lema 6.2 *Los conjuntos $S(a, b)$ son abiertos y cerrados en τ.*

Demostración: Es claro que los conjuntos $S(a, b)$ son abiertos. Para ver que son cerrados vamos a ponerlos como el complementario de una unión de abiertos de la siguiente forma

$$S(a,b) = \mathbb{Z} \setminus \bigcup_{j=1}^{a-1} S(a, b+j)$$

Vamos a comprobar esta igualdad de conjuntos por doble contenido.

Sea $x \in S(a, b)$, luego $x = an + b$ para cierto entero n. Es claro que $x \in \mathbb{Z}$, ¿x pertenece a alguno de los conjuntos $S(a, b+j)$ para $1 \leq j \leq a-1$? Supongamos que x está en alguno de los $S(a, b+j)$. Los elementos de $S(a, b+j)$ son de la forma $am+b+j$ luego x tendrá esa forma. Tomemos primero $m = n$, entonces $x = an + b = an + b + j$ de donde $j = 0$, que no es válido. Tomemos ahora $m = n + 1$, entonces $x = an + b = a(n+1) + b + j = an + a + b + j$ de donde $j = a$, que tampoco es válido. Por tanto, x no pertenece a ninguno de los $S(a, b+j)$. Luego, $x \in \mathbb{Z} \setminus \bigcup_{j=1}^{a-1} S(a, b+j)$.

Sea $x \in \mathbb{Z} \setminus \bigcup_{j=1}^{a-1} S(a, b+j)$. Podemos escribir x de la siguiente forma, $x = an + r$ con $b \leq r < b + a$, para algún entero n. Como x no está en ninguno de los $S(a, b+j)$, r no pertenece al conjunto $\{b+1, b+2, \ldots, b+a-1\}$. Luego, sólo puede ser $r = b$ y por tanto $x \in S(a, b)$. □

Una vez vistos los resultados, vamos a demostrar que el conjunto de los números primos es infinito.

Demostración 23 *Veamos primero que*

$$\mathbb{Z} \setminus \{-1, 1\} = \bigcup_{p \text{ primo}} S(p, 0)$$

Sea $x \in \mathbb{Z} \setminus \{-1, 1\}$, por la proposición 2.2, x será múltiplo de algún primo p, luego $x \in S(p, 0)$ y por tanto, $x \in \bigcup_{p \text{ primo}} S(p, 0)$. Entonces, $\mathbb{Z} \setminus \{-1, 1\} \subseteq \bigcup_{p \text{ primo}} S(p, 0)$.

Sea $x \in \bigcup_{p \text{ primo}} S(p, 0)$, luego x es un número entero múltiplo de algún primo. Es claro que x no puede ser ni 1 ni -1, ya que no son múltiplos de ningún primo. Por tanto, $x \in \mathbb{Z} \setminus \{-1, 1\}$. Entonces, $\mathbb{Z} \setminus \{-1, 1\} \supseteq \bigcup_{p \text{ primo}} S(p, 0)$

Por el lema 5.1, $\mathbb{Z} \setminus \{-1, 1\}$ no puede ser cerrado, ya que es el complementario de un conjunto finito. Por el lema 5.2, cada $S(p, 0)$ es cerrado.

Supongamos ahora que existe una cantidad finita de números primos. Entonces, $\bigcup_{p \text{ primo}} S(p, 0)$ es una unión finita de conjuntos cerrados. De la definición de topología se deduce que la unión finita de cerrados es un cerrado, por lo que tendríamos que ese conjunto es cerrado. Luego, tendríamos que un conjunto no cerrado es igual a un cerrado, que es una contradicción. Por tanto, el conjunto de los números primos es infinito. □

Utilizar razonamientos topológicos fue algo novedoso a la hora de demostrar la infinitud de los números primos. Sin embargo, la idea de la demostración no lo es, ya que, partiendo de la suposición de que hay una cantidad finita de primos, llegamos a una contradicción. Es novedosa en el sentido de que dicha contradicción se debe a la topología, ya que encontramos una igualdad en la que el lado derecho es un conjunto cerrado, mientras que el izquierdo no lo es.

Con el paso de los años, esta demostración se ha reescrito de diferentes maneras para eliminar la parte topológica de la demostración. Vamos a ver alguna de ellas.

6.2. Demostración de Cass y Wildenberg

En esta primera reinterpetación, llevada a cabo por Cass y Wildenberg en 2003, la podemos ver en [7], vamos a utilizar periodicidad. Empecemos definiendo cuando un conjunto es periódico, para ello utilizaremos la función característica, que toma el valor uno si el elemento está en el conjunto o 0 en otro caso.

Definición 6.3 *Dado un conjunto A de números enteros, diremos que es periódico si su función característica es periódica.*

Notemos que si S y T son dos conjuntos periódicos cuyos periodos son s y t respectivamente, entonces $S \cup T$ es periódico con un periodo que divide al mínimo común múltiplo de s y t. Esto se puede extender a uniones finitas de forma sencilla. Además, si S es periódico, entonces su complementario también lo es.

Ahora veamos la demostración, usaremos la misma notación que en la demostración de Furstenberg.

Demostración 24 *Para cada primo p, es trivial ver que el conjunto $S(p,0)$ es periódico. Como hemos visto en la demostración anterior, se cumple la siguiente igualdad*

$$\mathbb{Z} \setminus \{-1,1\} = \bigcup_{p \ primo} S(p,0)$$

Supongamos que existe una cantidad finita de primos, entonces el lado derecho de la igualdad es la unión finita de conjuntos periódicos y por tanto periódica. Sin embargo, el lado derecho es claro que no es periódico, con lo que llegamos a contradicción. □

Esta demostración, cambia la topología por periodicidad, ya que utilizando la misma igualdad que antes llegamos a que el lado derecho es periódico, mientras que el izquierdo no lo es.

6.3. Demostración de Mercer

Otra reinterpretación de la demostración fue propuesta por Idris Mercer en 2009, la podemos ver en [20]. En este caso usaremos propiedades de conjuntos y de las progresiones aritméticas. Para ello, necesitamos unos resultados previos. Empecemos definiendo el conjunto de enteros que no es divisible por cierto número.

Definición 6.4 *Dado m un número entero mayor que 2, se define $NM(m)$ como el conjunto de todos los enteros que no son divisibles por m.*

Es fácil ver que

$$NM(m) = S(m,1) \cup S(m,2) \cup \ldots \cup S(m,m-1)$$

Para demostrar la infinitud de los números primos, necesitaremos los siguientes lemas, cuyas demostraciones son sencillas.

Lema 6.3 *Una intersección finita de progresiones aritméticas es vacía o infinita.*

Lema 6.4 *Si $\mathcal{S}$ es cualquier colección de conjuntos, entonces una intersección finita de uniones finitas de conjuntos de $\mathcal{S}$ es también una unión finita de de intersecciones finitas de conjuntos de $\mathcal{S}$.*

Demostración 25 *Supongamos que tenemos una cantidad finita de primos, $p_1, p_2, \ldots, p_r$. Por el Teorema Fundamental de la Aritmética, los únicos enteros que no son múltiplos de ningún primo son el -1 y el 1, luego tenemos la siguiente igualdad*

$$\{-1,1\} = NM(p_1) \cap NM(p_2) \cap \ldots \cap NM(p_r)$$

Como cada $NM(p_i)$ es una unión finita de progresiones aritméticas, en el lado derecho de la igualdad tenemos una intersección finita de uniones finitas de progresiones aritméticas. Entonces, por el lema 6.4, lo podemos ver como la unión finita de intersecciones finitas de progresiones aritméticas que, por el lema 6.3, es vacía o infinita. Luego, llegamos a contradicción. □

6.4. Demostración de Carlson

Por último, vamos a reescribir la demostración de Furstenberg de tal forma que recuerde a la de Euclides. Esto lo hizo Nathan Carlson en 2014, la podemos ver en [6]. Continuamos usando la notación anterior para progresiones aritméticas y para el conjunto de todos los enteros que no son divisibles por un número entero.

Demostración 26 *Supongamos que existe una cantidad finita de primos, $p_1, p_2, \ldots, p_r$ y llamemos $P = p_1 \cdot p_2 \cdot \ldots \cdot p_r$. Aplicando el Teorema Fundamental de la Aritmética como en la demostración anterior, tenemos*

$$\{-1, 1\} = NM(p_1) \cap NM(p_2) \cap \ldots \cap NM(p_r)$$

Sea m cualquier número entero, entonces $m \cdot P + 1$ no es múltiplo de ningún primo p_i, es decir $m \cdot P + 1 \in NM(p_)$ para todos los primos p_i. Luego, está en la intersección de todos. Ahora bien $m \cdot P + 1 > 1$, luego llegamos a contradicción. □

6.5. Relación entre las demostraciones

En este capítulo hemos visto una demostración utilizando argumentos topológicos y algunas reinterpretaciones de la misma en las que se evita el uso de la topología.

En todas las demostraciones suponemos que hay una cantidad finita de primos y se utiliza la siguiente igualdad que utilizó Furstenberg en su demostración

$$\mathbb{Z} \setminus \{-1, 1\} = \bigcup_{p \ primo} S(p, 0)$$

Furstenberg prueba, usando topología, que el lado derecho es cerrado y el izquierdo no lo es. Cass y Wildenberg reescriben la demostración de tal forma que, sin usar topología, ven que el lado derecho es periódico, mientras que el izquierdo no lo es.

Mercer y Carlson utilizan el conjunto de números que no son múltiplos de un número dado. Por ello, en vez de usar esa igualdad, utilizan la que se obtiene si consideramos los complementarios ambos lados

$$\{-1, 1\} = NM(p_1) \cap NM(p_2) \cap \ldots \cap NM(p_r)$$

Mercer demuestra que el lado derecho es infinito, llegando a contradicción. Por otro lado, Carlson construye un número distinto de -1 y 1 que está en el conjunto de la derecha, con lo que también llega a contradicción.

Mencionar que podemos relacionar la demostración de Euclides y la de Furstenberg. Para ello, tenemos que fijarnos en la de Carlson,ya que el número que construye utiliza el producto de todos los primos más 1, que es el mismo que utiliza Euclides.

Capítulo 7

Otras demostraciones

En este capítulo vamos a ver otras demostraciones las cuales o no encajan en ninguno de los capítulos anteriores, o requieren un comentario aparte. Destacar que hay cientos de demostraciones de dicho teorema, pero no podemos incluirlas todas en el trabajo, podemos ver más en [21].

7.1. Demostración de Saidak

Filip Saidak es un matemático estadounidense que ha proporcionado una de las demostraciones más recientes de la infinitud de los números primos, es de 2006 y la podemos ver en [26]. Además, esta demostración es concisa, en el sentido de que demuestra de forma directa la infinitud de los números primos utilizando que dos números consecutivos son primos entre sí.

Demostración 27 *Sea n un entero mayor que 1. Como n y $n+1$ son números consecutivos, tienen que ser primos entre sí. Sea $N_2 = n(n+1)$, como n y $n+1$ son coprimos no tienen factores primos en común, luego N_2 tiene, al menos dos factores primos distintos. Consideramos ahora el número $N_3 = N_2 \cdot (N_2+1)$, como N_2 y N_2+1 son números consecutivos, son coprimos, luego tienen factores primos distintos. Como sabemos que N_2 tiene dos factores primos diferentes, N_3 tiene tres factores primos distintos. Este procedimiento lo podemos repetir tantas veces como queramos, por tanto tienen que existir infinitos números primos.* □

Esta demostración utiliza el hecho de que dos números consecutivos son coprimos y, aunque no llegue a definirla, utiliza una sucesión, la cual sería $N_i = N_{i-1} \cdot (N_{i-1}+1)$. Este procedimiento nos puede recordar a la demostración de Goldbach, sin embargo, en la sucesión dada sus elementos no son todos primos entre sí. Lo que utiliza es que en cada iteración encontramos un nuevo factor primo.

7.2. Demostraciones utilizando el número π

Vamos a ver dos demostraciones en las cuales usaremos que π es irracional para demostrar la infinitud de los números primos. Ambas demostraciones usan resultados de Leibniz y de Euler. Pueden verse en [9] y [10], pero no podemos asegurar el autor y la fecha en que aparecieron. Las referencias utilizadas no lo muestran.

En la primera, vamos a usar la fórmula de Leibniz de π y lo veremos como un producto de Euler. No vamos a profundizar en ello ya que se escapa de los contenidos de este trabajo, pero la demostración es digna de ver.

Demostración 28 *Usando la fórmula de Leibniz para π y viéndolo como un producto de Euler, tenemos*

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \ldots = \sum_{i=1} \frac{(-1)^i}{2i+1} =$$

$$= \left(\prod_{p \equiv 1 \mod 4} \frac{p}{p-1} \right) \cdot \left(\prod_{p \equiv 3 \mod 4} \frac{p}{p+1} \right) = \frac{3}{4} \cdot \frac{5}{4} \cdot \frac{7}{8} \cdot \frac{11}{12} \cdot \ldots$$

Ahora bien, si suponemos que hay una cantidad finita de primos, la parte derecha de la igualdad es un producto finito de fracciones, por lo tanto es un número racional, mientras que la parte izquierda de la igualdad es un número irracional, con lo que llegamos a contradicción. □

En la segunda demostración, usaremos dos igualdades probadas por Euler y que π^2 es irracional. Estas dos igualdades son

$$\frac{\pi^2}{6} = \sum_{n=1} \frac{1}{n^2} = \prod \frac{1}{1 - p^{-2}}$$

Demostración 29 *Supongamos que sólo existe una cantidad finita de números primos, por tanto $\prod \frac{1}{1-p^{-2}}$ será siempre un número racional, al ser un producto finito de fracciones.*

Por otro lado, utilizando las igualdades probadas por Euler tenemos

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

Entonces, llegamos a que el lado izquierdo de la igualdad es un número irracional, mientras que el derecho es racional. Luego, llegamos a contradicción. □

7.3. Demostración de una línea

Sam Northshield es un profesor de matemáticas de la universidad de Nueva York en Plattsburgh, que ha desarrollado diferentes demostraciones de la infinitud de los números primos. Una de ellas, publicada en 2015, se puede escribir en una sola línea, pero nosotros vamos a explicarla en detalle, con lo que ocupará algo más. La podemos ver en [22].

Demostración 30 *Supongamos que sólo existe una cantidad finita de números primos, entonces*

$$0 < \prod_p \sin\left(\frac{\pi}{p}\right) = \prod_p \sin\left(\frac{\pi}{p} + (2\pi)\prod_{p'} p'\right) = \prod_p \sin\left(\frac{\pi(1+2p\prod_{p'} p')}{p}\right) = 0$$

La primera desigualdad se debe a que $\frac{\pi}{p}$ *es un ángulo mayor que 0 y menor o igual que* $\frac{\pi}{2}$ *para cualquier primo p, por tanto está en el primer cuadrante, luego su seno es mayor que 0.*

La última igualdad se debe a que, por la Proposición 2.2, $1+2p\prod_{p'} p'$ *tiene que ser divisible por algún primo p y por tanto* $\frac{1+2p\prod_{p'} p'}{p}$ *es un número entero.* □

Esta demostración tan sencilla, recuerda a la demostración de Euler, ya que suponemos que hay una cantidad finita de primos y llegamos a una contradicción utilizando productos, aunque en este caso sean finitos.

7.4. Demostración usando probabilidad

Sam Northshield también ha desarrollado una demostración de los números primos en la que se utilizan nociones básicas de probabilidad, la podemos ver en [23]. Mencionar que dicha demostración se publicó en 2017.

Demostración 31 *Supongamos que existe una cantidad finita de números primos,* $p_1, p_2, \ldots, p_r$. *Sea* $X = p_1^{T_1} p_2^{T_2} \ldots p_r^{T_r}$, *donde los* T_i *son independientes y con distribución* $P(T_i = a) = \frac{p_i - 1}{p_i^{a+1}}$. *Este X está bien definido, además cumple lógicamente* $P(X \text{ sea divisible por } n) = \frac{1}{n}$, *como debería ser. Por el Teorema Fundamental de la Aritmética,* $n = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$ *y si tenemos en cuenta la independencia de los* T_i, *entonces,*

$$P(X = n) = P(T_1 = e_1) \cdot P(T_2 = e_2) \cdot \ldots \cdot P(T_r = e_r) =$$

$$= \prod_{i=1}^{r} \frac{p_i - 1}{p_i^{e_i+1}} = \prod_{i=1}^{r} \frac{1}{p_i^{e_i}} \cdot \frac{p_i - 1}{p} = \frac{1}{n} \prod_{i=1}^{r} \frac{p_i - 1}{p_i}$$

Ahora bien, entonces tenemos

$$1 = \sum_{n} P(X = n) = \prod_{i=1}^{r} \left(\frac{p_i - 1}{p_i} \right) \cdot \sum_{n} \left(\frac{1}{n} \right) = \infty$$

Por tanto, llegamos a contradicción. □

Al igual que Euler, utilizando series llegamos a que una serie es divergente y convergente a la vez, pero en este caso necesitamos utilizar probabilidad.

Bibliografía

[1] Aigner, M. y Ziegler G.M. Proofs from THE BOOK, 4ª edición, Springer, 2010.

[2] Auric, A. Suite illimitée des nombres premiers, L'intermédiaire des Math. 22, p. 252, 1915.

[3] Boije af Gennäs, C.O. Trouver un nombre premier plus grand qu'un nombre premier donne, Öfversigt K. Sv. Vetenskaps-Akad. Förhand., Stockholm, 50, No. 7, p. 469–471, 1893.

[4] Braun, J. Das Fortschreitungsgesetz der Primzahlen durch eine transzendente Gleichung exakt dargestellt, JBer. Gymnasium Trier, Wiss. Beilage, p. 1–96, 1899.

[5] Caldwell, C.K. y Xiong, Y. What is the Smallest Prime?, Journal of Integer Sequences, vol. 15, article 12.9.7, 2012.

[6] Carlson, N.A. A connection between Furstenberg's and Euclid's proofs of the infinitude of primes. American Mathematical Monthly 121, no. 5, 444, 2014.

[7] Cass, D. y Wildenberg, G. Math Bite: A Novel Proof of the Infinitude of Primes, Revisited, Mathematics Magazine 76, p. 203, 2003.

[8] Chernoff, P.R. A "Lattice Point" Proof of the Infinitude of Primes, Math. Magazine 38, p. 208, 1965.

[9] Debnath, L. The Legacy of Leonhard Euler: A Tricentennial Tribute, World Scientific, p. 214, 2010.

[10] Dickson, L.E. History of the Theory of Numbers, Vol. I: Divisibility and Primality, Carnegie Institution of Washington, p. 413, 1919.

[11] Dirichlet, P.G.L. Beweis des Satzes, dass jede unbegrentze arithmetische progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält, Abh. der Königlichen Preuss. Akad. der Wiss. p. 45–81, 1837.

[12] Euclides, Los Elementos. Traducción y anotaciones de M. L. Puertas, Editorial Gredos, Madrid, 1994.

[13] Euler, L.Variae observationes circa series infinitas, Comment. Acad. Sci. Petropol. 9, p. 160–188, 1744.

[14] Furstenberg, H. On the Infinitude of Primes, American Mathematical Monthly 62, p. 353, 1955.

[15] Fuss, P.N. Correspondance mathématique et physique de quelques cèlébres géométres du XVIIIéme siécle, St. Pétersbourg, 1843, carta de Goldbach a Euler, 20 de Julio de 1730, disponible en http://eulerarchive.maa.org/correspondence/correspondents/Goldbach.html, recuperado el 7 de Junio de 2017.

[16] Gauss, C.F. Disquisitiones Arithmeticae, G. Fleischer, Leipzig, 1801.

[17] Hardy, G.H. y Wright, E.M. An Introduction to the Theory of Numbers, 6ª edición, Oxford University Press, Section 2.6. 2008.

[18] Harris, V.C. Another proof of the infinitude of primes, American Mathematical Monthly 63, p. 711, 1956.

[19] Kummer, E.E. Neuer elementarer Beweis des Satzes, dass die Anzahl aller Primzahlen eine unendliche ist, Monatsber. Akad. d. Wiss., Berlin, p. 777-778, 1978/9.

[20] Mercer, I.D. On Furstenberg's Proof of the Infinitude of Primes, Amererican Mathematical Monthly 116, p. 355-356, 2009.

[21] Meštrović R. Euclid's Theorem on the Infinitude of Primes: A Historical Survey of its Proofs, arXiv:1202.3670v2 [math.HO], 2012.

[22] Northshield, S. A one-line proof of the infinitude of primes, American Mathematical Monthly 122, no. 5, p. 466, 2015.

[23] Northshield, S. Two Short Proofs of the Infinitude of Primes, College Mathematical Journal 48, no. 3, p. 214–216, 2017.

[24] Perott, J. Sur l'infinité de la suite des nombres premiers, Bulletin de la Societé Mathématiques et Astronomiques de France (2) 5, p. 183–184, 1881.

[25] Ribenboim, P. The little book of bigger primes, Second edition, Springer- Verlag, New York, 2004.

[26] Saidak, F. A New Proof of Euclid's theorem, American Mathematical Monthly 113, p. 937–938, 2006.

[27] Srinivasan, S. On infinitude of primes, Hardy-Ramanujan Journal 7, p. 21-26, 1984.

[28] Stieltjes, T.J. Sur la théorie des nombres, Ann. Fac. Sci. Toulouse 4, p. 1–103, 1890.

[29] Thue, A. Mindre meddelelser, II; Et bevis for at primtalleness antal er uendeligt., Arch. for Math. og Natur., Kristiania, 19, No. 4, p. 1–5, 1897.

[30] Wikipedia, Simplex, https://en.wikipedia.org/wiki/Simplex, recuperado el 7 de Junio de 2017.

[31] Wunderlich, M. Another Proof of the Infinite Primes Theorem, American Mathematical Monthly 72, No. 3, p. 305, 1965.

[32] Yamada, T. Proofs of the infinitude of primes, disponible en http://tyamada1093.web.fc2.com/math, recuperado el 7 de Junio de 2017.