UNIVERSIDAD NACIONAL AUTÓNOMA

DE MÉXICO

FACULTAD DE CIENCIAS

LOS NÚMEROS PRIMOS Y SUS PUENTES INESPERADOS

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

M A T E M Á T I C O

P R E S E N T A:

JORGE ALBERTO JARQUIN JACOBO

DIRECTOR DE TESIS:

MAT. JULIO CÉSAR GUEVARA BRAVO

2014

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

1. Datos del alumno.
   Jarquin
   Jacobo
   Jorge Alberto
   Universidad Nacional Autónoma de México
   Facultad de Ciencias
   Matemáticas
   408064882

2. Datos del tutor.
   Mat.
   Julio César
   Guevara
   Bravo

3. Datos del sinodal 1
   M en C. José Rafael
   Martínez
   Enríquez

4. Datos del sinodal 2
   Dr. Alejandro
   Ricardo
   Garciadiego
   Dantán

5. Datos del sinodal 3
   M. en C. Francisco de Jesús
   Struck
   Chávez

6. Datos del sinodal 4
   Mat. Anayanzi Delia
   Martínez
   Hernández

7. Datos del trabajo escrito
   Los números primos y sus puentes inesperados
   P 62
   2014

Índice general.

Introducción.

La teoría de los números en su extensa y permanente evolución se ha mostrado colmada de imprevistos, indefiniciones y de —aparentes— imposibilidades, como sucedió con la aparición de los inconmensurables o con la duplicación del cubo entre los griegos. En lo general, la matemática —para algunos— sería una ciencia más placentera si se pudiera colocar en un ámbito más determinista, a la manera de la física clásica de Newton, en donde el conocimiento de un sistema en un instante dado permite determinar el estado general del sistema en cualquier momento. Aunque esto es un efecto o consecuencia de la matemática misma, dado que las soluciones de la ecuación de momento son únicas. Eso es el determinismo.

Pero la matemática parece que no es tan moldeable, ésta posee una forma de ser que la hace única. Parte de su grandeza radica en su capacidad de llevarnos a situaciones desafiantes que nos hacen sentir que aún somos incapaces de encontrar algunos de sus secretos, y ahí es cuando aparece una duda: ¿la imposibilidad para encontrar algunas soluciones será un principio propio de determinados problemas o es solo nuestra incapacidad para encontrar o llegar a resultados?

La pregunta anterior la canalizaremos en este trabajo de tesis a una situación explícita dentro de la teoría de los números, y para ello nos remitimos a ciertas cuestiones acerca de los números primos.

Desde la antigüedad los números primos han dado espacio a la investigación, la incertidumbre, y a la fascinación. Los primos, por su presencia impredecible, irregular y escasa —en intervalos de naturales muy grandes— sembraron desde épocas tempranas del desarrollo de la matemática la inquietud por establecer certeza acerca de su cardinalidad. Afortunadamente, a lo largo de los siglos, personajes como Euclides, Kummer o Pólya, entre otros, demostraron en forma elegante que el conjunto de los primos sí es infinito. En esta tesis exhibiremos situaciones donde esta certidumbre acerca de su infinitud a la vez dará lugar a que la intuición que se puede tener respecto a cierto comportamiento de los primos puede ser totalmente errónea.

Un ejemplo de que nuestra intuición puede ser sorprendida es cuando se quiere conocer la distribución de los primos. Y es en este contexto que se puede mencionar que después de escudriñar entre los primos se ve que entre más grande es la secuencia de los naturales bajo estudio, la densidad de primos es menor. Por ejemplo: en el rango de 1 a

10^3 el porcentaje de primos es de 16.80%, pero en el rango de 1 a 10^{1000} es de 0.0434%, y así sucesivamente. El porcentaje continúa disminuyendo y tiende a cero cuando los rangos son mayores —aunque ya sabemos que no es cero porque el conjunto es infinito—. También podemos crear cadenas de dimensiones inimaginables de enteros positivos y que además sean compuestos consecutivos a través de la secuencia $(n+1)!+2$, $(n+1)!+3, \ldots, (n+1)!+(n+1)$. Este tipo de cadenas podrían llevar dirigir nuestra intuición a que al estar situados a grandes distancias entre ellos en la sucesión de los naturales, la distancia entre un primo y otro siempre sería enorme, pero resulta que ¡no es así!, y aquí es donde nuestra intuición sobre la aparición de los primos es errónea. Resulta que aún en distancias muy grandes pueden aparecen números impares consecutivos que también son primos. A los primos de esta clase se les conoce como *gemelos,* y su entrada en escena no es frecuente; por ejemplo, en el año 2000 La Barbera y Jobling encontraron la pareja de primos

$$(1693965)2^{66443} \pm 1,$$

que tienen 20,008 dígitos. Encontrar primos gemelos requiere muchas horas de cálculo y actualmente no sabemos si forman un conjunto infinito.

Lo anterior es un ejemplo de lo que se expone en la tesis, es decir, que se dan situaciones con los primos que le pueden dar un revés a nuestra intuición. Y en este sentido es importante mencionar que este trabajo puede ser de utilidad para quienes se están iniciando en la teoría de los números y en particular en la de los números primos.

En el primer capítulo comenzamos con una pregunta que para muchos quizás sea filosófica, pero que bien vale la pena discutir ya que a los matemáticos de diferentes épocas les causó problemas. La pregunta es ¿el número uno es primo? Para responder tal pregunta nos remitimos a Euclides y a otros matemáticos cuyas respuestas no eran del todo coincidentes.

En los capítulos posteriores de este trabajo exponemos propiedades que llamamos puentes inesperados dentro de los números primos y que dan lugar a rupturas de la intuición. Los puntos a tratar son: las demostraciones de Euler y Niven sobre la infinitud de los primos, primos de las formas $4k \pm 1$, primos como suma de cuadrados, teorema de Scherk, intervalos de Bertrand, primos en el intervalo $[2n, 3n]$, generalización del teorema de Bertrand-Chebyshev y primos gemelos.

Capítulo I

La unidad como generadora de todo.

Durante muchos siglos no hemos dejado de estudiar a los números, y lo hacemos dentro de clasificaciones que establecemos para tratar de entender de la mejor manera posible cómo están constituidos. Actualmente los podemos considerar a partir de las propiedades de un campo o de un anillo, algunos los hemos definido como algebraicos para entender las soluciones de ciertas ecuaciones, o los contemplamos bajo la categoría de lo que llamamos complejos para abordar situaciones no contempladas en los reales. Los agrupamos por las características que identificamos en ellos, ya sea como naturales, enteros, pares, impares, racionales, perfectos o de otras formas.

La capacidad de crear canales de clasificación para los números nos ha brindado los elementos necesarios para poder satisfacer algunas de nuestras inquietudes más añejas, que iniciaron con contar y medir. Desde épocas antiguas hemos contado de todo, las horas, los días, los años, nuestras posesiones, etc. De la misma manera medimos todo lo que está en nuestro entorno tangible o al alcance de nuestra vista. En ambos casos –contar o medir- tenemos un elemento que es fundamental para poder ejecutar esta práctica, y éste es la unidad. Este elemento aunado a una métrica previamente definida nos brinda las posibilidades de medir y posteriormente describir todo aquello que nuestros sentidos nos permiten percibir. Por otro lado con la unidad podemos generar a los números[1] y con éstos podemos contar lo que sea necesario, pero dentro de esta correspondencia nos centraremos en el hecho de que la unidad genera a los números enteros,[2] pero estos últimos a la vez pueden ser concebidos como generados por otros números de gran importancia, los primos.

[1] Estos es $2 = 1 + 1, 3 = 1 + 1 + 1, 4 = 1 + 1 + 1 + 1$, etc.

[2] La idea de construir a los enteros a partir de sumas reiteradas de unos se puede extender a crear un conjunto de cardinalidad infinita, y aquí no pensamos en mostrar un conjunto que tenga una cantidad infinita de elementos, lo que nos interesa es la existencia del proceso aditivo de unidades que nos lleva a generar una cantidad infinita de enteros. En este tenor Andrés Puig $[1672, 3]$comenta esto: *"la cantidad discreta o el número tiene disminución finita, pero su aumentación es infinita porque no se dará o hallará número tan grande, que no se pueda hallar otro mayor añadiéndole la unidad"*. Puig describió con palabras precisas a los naturales quienes prácticamente son los primeros números que aprendemos, y matemáticamente, resultan ser la base de lo que Gauss llamaba aritmética superior o teoría de números, que es como hoy la conocemos.

Por lo tanto tenemos dos formas de generar a los números, una aditiva donde agregamos tantas unidades como sea necesario hasta llegar al número requerido; la otra manera es como un producto de primos que también nos lleva a poder construir el mismo número.[3] Empero, como en este trabajo nos centraremos en los primos, entonces la primera pregunta que se nos presenta es ¿la unidad es un primo? actualmente sabemos que no es considerada así, pero si revisamos la definición de número primo resulta que la unidad sí cumple con ésta. Así, por lo antes mencionado ahondaremos en esta pregunta para tratar de entender desde su origen y en forma más intrínseca a los primos, y para esto primero haremos una revisión histórica sobre qué es la unidad.

¿La unidad es un número?

Actualmente no se discute si la unidad es un número. Se sabe o se acepta que lo es, tal y como lo requiere la lógica que rige a las matemáticas. No obstante, determinar su naturaleza no fue una tarea que se resolvió en poco tiempo, tuvieron que pasar siglos antes de que se disiparan las dudas respecto de si era un número o no.

Si nos remitimos a los trabajos de los antiguos griegos tenemos a Euclides [1994, 111] y sus *Elementos*, cuyo libro VII contiene la definición de unidad y número. En la definición uno enuncia que una unidad es *"aquello en virtud de lo cual cada una de las cosas que hay es llamada una"*. Y respecto a la idea de números la definición dos dice: *"un número es una pluralidad compuesta de unidades"*. Aquí tenemos elementos que nos indican que la percepción de Euclides respecto a su idea de número y unidad no son lo mismo, es decir, que la unidad no es un número, y esto se puede extraer de su definición de número ya que éste tiene que ser una pluralidad de unidades, pero no contempla que puede ser sólo una. Pero el que no deja dudas es Aristóteles, en su

[3] Pero aquí tenemos el primer freno a nuestro proceso intuitivo sobre cómo se pueden formar los enteros usando solo primos, pues resulta que parece que son escasos, y como no sabemos en donde van apareciendo dentro del orden de los enteros, entonces ¿qué no es dudoso pensar que solo con productos de primos se puede generar a cualquier entero? La intuición nos dirá que es poco probable que podamos generar a loa enteros solo con productos de primos, pero Euclides nos da un revés desde hace más de 2000 años, pues en la proposición 31 del libro VII de sus *Elementos* nos deja ver que sí es posible esta forma de representación solo con productos de primos. No hay duda que nuestra intuición nos puede generar una conclusión errónea.

definición de número primo[4] señala que un número primo no es medido por ningún número (*Analíticos Segundos* II 13, 16a36), pues la unidad no es un número (*Metafísica* 1088a6), sino solo el principio del número.

Con esto tenemos un panorama que nos lo proporcionan dos autoridades de la antigüedad, pero finalmente ellos son el reflejo más acabado de dos visiones de la matemática, y nos referimos a que existen otros perfiles que pensamos que es importante mencionar. Así, bajo este esquema recordemos a Jámblico en su *Comentario a la Introducción a la Aritmética de Nicómaco* [II, 5]. Dicho autor señala que la definición euclidiana de unidad proviene de autores recientes, y nos recuerda lo que otros señalaron:

- Timaridas, un pitagórico antiguo, define la unidad como una *"cantidad limitada"*.
- Teón de Esmirna sugiere que la unidad es *"aquello que, cuando la cantidad disminuye mediante sustracción continua, se ve privado de todo número y toma una posición y un resto permanentes"*.
- Aristóteles [*Metafísica* 1089b35] la definió como *"lo indivisible en lo que se refiere a la cantidad"*, y hace una comparación con la definición euclidiana de punto al mencionar que la unidad es como *"un punto sin posición"* [*Metafísica* 1084b26].

Hasta aquí los comentarios de Jámblico no han cruzado la frontera respecto a comentar sobre la definición de número, sólo hemos seleccionado los que se enfocan en la unidad. Se puede ver que en ninguna parte se menciona que la unidad sea a la vez un número; de hecho podemos decir que para los antiguos la unidad no es un número. Pero entonces ¿qué es la unidad?

Sin duda para los matemáticos de siglos pasados era algo especial, y las palabras de Andrés Puig [1672, 3] nos lo pueden ejemplificar: *"la unidad dicen es más perfecta que todos los números juntos, porque potencialmente contiene en sí todas la propiedades y excelencias de todos ellos"*. Entonces, lo que tenemos, en pocas palabras,

[4] Euclides en la definición doce enuncia: *"Un número primo es el medido por la sola unidad"*. Nótese que el término medido es lo que hoy entendemos como 'divide', además en la aritmética euclidiana un número no es parte de si mismo, por eso es que en la definición de primo sólo se contempla a la unidad como el único divisor.

es que para los antiguos la unidad es la generadora de los números, y como la unidad no es número, entonces los números inician a partir del dos.

Pero regresemos a las autoridades de la antigüedad para extraer el concepto de número; éste servirá de complemento a la definición euclidiana en los *Elementos*. Para esto haremos acopio de citas sólo de Aristóteles, y lo hacemos así porque consideramos que en este rubro él logra mostrar los diferentes perfiles del concepto de número que dominaron en la época. Así, en la *Metafísica* [libro X, 1053a30] señala que *"el número es un agregado de mónadas"*, y en este contexto consideraremos que para Aristóteles la mónada es la unidad carente de extensión y posición; ésta es el principio y medida de todo número, es decir, de toda pluralidad. Entonces número significa para Aristóteles "pluralidad" [libro X, 1088a4-10], por lo tanto el uno no es número, es solo el principio de ellos. Así, lo que se tiene es que el primer número es el dos.

La inquietud sobre la naturaleza de la unidad de ninguna manera llegó a su fin después de los trabajos de Euclides, Aristóteles, Diofanto o Nicómaco. Una muestra de esto la podemos ver cuando los temas matemáticos regresaron provocando el interés de los científicos europeos del siglo XVI. En este contexto los italianos en el siglo XVI se plantearon diversos temas, y entre ellos encontramos el de la solución de ecuaciones de tercer grado. Y aquí regresamos a que la reflexión sobre la naturaleza de la unidad estaba vigente, y la podemos localizar en la famosa controversia entre Nicolo Tartaglia y Girolamo Cardano por la autoría de la solución general de la ecuación cúbica. En el año 1547 Cardano y Tartaglia se encontraban inmersos en un debate que se generó por la cuestión de la prioridad acerca de la ecuación de tercer grado; el enfrentamiento llegó a niveles públicos en la ciudad de Milán, y una parte de los testimonios acerca de este debate -que es de nuestro interés- se encuentra en la pregunta treinta de la carta que le envíó Cardano –a través de Ludovico Ferrari- a Tartaglia [Tartaglia y Ferrari 1974, 68]. La pregunta dice lo siguiente:

"Te pregunto si la unidad es un número o no"

La respuesta de Tartaglia se centró en decir que éste no era un problema de carácter matemático, que estaba principalmente dirigido hacia una reflexión de tipo metafísico. Pero finalmente sí expresa una posición y dice que la unidad es un número en potencia, pero no en acto, pero que sí puede ser parte de cualquier tipo de número, es decir, que puede ser principio y final de cada una de las clases.

Ferrari le responde sin descalificarlo, pero su extensa respuesta fue para mostrar que conocía muy bien los trabajos de Aristóteles y Euclides donde se argumenta –como ya lo hicimos- que la unidad no es un número, y que éstos son una multitud de unidades. Respecto a la respuesta de Tartaglia, él tenía razón dentro del contexto de los clásicos griegos, pero no lo fundamentó de la manera que satisficiera a Ferrari. Por otro lado Tartaglia no tiene problemas en reconocer a la unidad como un número, y se puede ver explícitamente en la traducción que hizo de los *Elementos* de Euclides[1994].

Ya pudimos ver que la vieja discusión entre qué es la unidad y qué el número no estaba perdida en pleno periodo del Renacimiento europeo, lo podemos constatar con estos dos italianos precursores de lo que hoy conocemos como álgebra. Y por otro lado Tartaglia tenía razón cuando menciona que el problema de la unidad ya no es un problema que genere inquietud a los matemáticos. Para esta época los que estaban empezando a crear las bases de lo que fue la matemática de los siglos XVII al XIX no se cuestionaban estos asuntos de fundamentos, solo usaban a los enteros sin que esto les provocara inquietud alguna.

Números primos.

Ya sabemos qué es un número para los griegos, pero aún tenemos un asunto pendiente que da lugar a otra gran fuente de estudio, nos referimos a esa estructura interna que sostiene a aquellos números que son diferentes de la unidad, y sus elementos estructurales son los números primos.

Desde épocas tempranas los griegos ya tenían una clasificación de los naturales. Ésta la podemos encontrar en las definiciones del libro VII de los *Elementos*. Por ejemplo, hay diversas formas de caracterizar a los pares e impares, a los parmente pares, parmente impares, imparmente impares, entre otros[5]. Además, con base en su definición de divisibilidad[6] se pueden establecer dos conjuntos, uno que está conformado por números que tienen tres o más divisores, y el otro que contiene a los números que sólo poseen exactamente dos divisores, y este segundo conjunto es el de los números primos.

[5]Ver las definiciones del libro VII[1994]

[6] Euclides nunca usó el término divisibilidad. Cuando se refirió a lo que hoy conocemos como un número divide a otro, él lo definió pensando en segmentos, y por lo tanto menciona que un número es parte de otro [ver Euclides 1994, 113].

Según Euclides [1994, 116] *"un número primo es el medido por la sola unidad"*, y de acuerdo con Nicómaco *"sólo se puede llegar a ellos juntando unidades y la unidad es el principio del número"* [Euclides 1994, 116]. Por otro lado Nicómaco, Teón y Jámblico [Euclides 1994, 116] añadieron el término *"no compuesto"*, para ratificar la caracterización del número primo.

Entonces, con la definición euclidiana de número primo se puede inferir que el primero de ellos es el dos. Pero pese a esta definición tan precisa, entre otros pensadores griegos se presentan aún problemas para poder terminar de dilucidar cual es el primer número primo. Según Nicómaco [1994, 116], los primos no eran un subconjunto de los enteros, éstos solamente lo eran de los impares, y por esta razón él no consideraba al 2 como primo, pero también se da el contraste con Aristóteles ya que él sí contemplaba al 2 como parte de los primos.

Este tipo de problemas se suscitaron no sólo con el 2. De igual manera se dio una disyuntiva en cuanto al número uno y ésta perduró aproximadamente dos mil años. Empecemos por recordar que la definición moderna de primo nos indica que éstos son aquéllos que solamente son divididos por el uno y por sí mismo. Por siglos se dio el encuentro de opiniones entre los que afirmaban que el uno tiene dos divisores y que en particular es el mismo número; otros son los que solo aceptaban a un divisor y nada más. Y en este contexto regresamos a los tiempos de Euclides, donde el uno definitivamente no era primo, porque ni siquiera era un número. Aunado a esto podemos mencionar a personajes como Tartaglia [1586], Puig [1672], Commandino y Paccioli, y poner atención en sus obras para entender que ellos no consideraban al uno como número primo, y una de las razones está centrada en el hecho de que estaban apegados a las definiciones Euclidianas.

Por otro lado tenemos a personajes de la segunda mitad del siglo XVIII, como Christian Goldbach y Leonhard Euler, que propusieron lo que hoy conocemos como "Conjetura de Goldbach", y para esto consideraban que el uno era primo. En épocas más recientes podemos mencionar a P. A. Clement [1949, 24], que en 1949 nuevamente lo consideró como primo. Pese a todas las diferencias, por razones relacionadas con los fundamentos de la matemática hoy día no consideramos al uno como primo.

Pero ¿qué sucede si aceptamos que el uno es primo? Lo primero que tendríamos que plantearnos es ver cómo va funcionar el método más antiguo que conocemos para

generar primos, y nos referimos a la tabla conocida como la *criba de Eratóstenes*. En dicha tabla se colocan los primeros 100 números naturales, y se eliminan aquellos que son múltiplos de un primo. Por ejemplo, consideremos al 2, y acto seguido se eliminan a todos sus múltiplos, es decir, a todos los pares y sólo queda en la tabla el dos. Después tomamos al número 3, y actuamos como en el caso anterior pero ahora eliminamos a los múltiplos de tres y en la tabla sólo queda el tres. Si seguimos de esta manera los únicos números que no quedarán eliminados son los primos. Ahora regresemos a nuestra pregunta ¿qué pasa si el 1 es primo? Si esto sucede debemos de considerarlo en el mismo proceso de la criba, y entonces eliminar a todos sus múltiplos. Y aquí está el gran problema, pues sucede que sus múltiplos son todos los números después del uno, por lo tanto el conjunto de los primos se reduce sólo a un único elemento, a saber, el 1. Afortunadamente para los griegos y para nosotros no se considera primo a este número, y con esto nos evitamos un conflicto.

Hoy se dice que los primos comienzan con el 2 y que es el único número par que es primo, como lo enunció Aristóteles. Pero veamos otro argumento, que es de carácter más actual, por lo que el uno no puede ser primo. La respuesta radica en el hecho de que mientras el uno no sea primo se sostiene la validez de un teorema de suma importancia, y nos referimos al *Teorema Fundamental de la Aritmética*. Este teorema establece que todos los números naturales se pueden expresar como productos de potencias de primos de manera única salvo el orden de los factores. Entonces, si aceptamos al uno como primo estaríamos contradiciendo este teorema, ya que la unicidad del producto no se cumpliría, por ejemplo $8 = 2^3$, pero si el uno es primo entonces tendríamos $8 = 1 * 2^3$, $8 = 1 * 1 * 2^3$, $8 = 1 * 1 * 1 * 2^3$, …, etc., es decir, habría una infinidad de representaciones para 8 y algo análogo sucedería para todos los enteros cuando son escritos como productos de primos.

Y no es difícil corroborar, lo mencionado en el párrafo anterior, que el producto propuesto en el teorema fundamental es único. Supongamos que existe un número $m = p_1 * p_2 * \ldots * p_n = q_1 * q_2 * \ldots * q_n$, que tiene dos representaciones distintas, entonces p_1 debe dividir a $q_1 * q_2 * \ldots * q_n$, pero por ser primo divide a alguna q_j que también tiene que ser primo, por lo tanto, se llega a que $p_1 = q_j$. De manera análoga se llega a que cada p_r es igual a una q_s, por lo que ambas representaciones de m como producto de primos son iguales.

Una manera de evitar conflictos con el uno puede ser a través de realizar una modificación a la definición de número primo, y así salvar al *Teorema Fundamental de la Aritmética*. Y en este sentido una definición alternativa de números primos seria: *"un número primo es aquel que sólo admite a un entero mayor que uno en su descomposición"*. En este caso el uno no representa un obstáculo.

Después de comentar por qué al uno no lo consideraremos primo, pasemos a una primera auscultación respecto a su importancia. El primer punto está nuevamente en el teorema fundamental, que es mencionado de alguna manera por Euclides en la proposición 30 del libro VII de los *Elementos*. Pero antes, en la proposición 29 enuncia "*todo número primo es primo con respecto a todo número al que no mide*". Después en la proposición 31 afirmó que "*todo número primo es medido por algún primo*" y la proposición 32 establece que "*todo número es primo o es medido por algún primo*". Con estas proposiciones percibimos que Euclides tenía muy claro que, por un lado, con la unidad se pueden generar de manera aditiva a los números enteros; y por el otro, que con los primos podemos saber cuáles son los factores que los conforman, y asimismo también podemos generar a los enteros pero ahora como un producto de enteros irreducibles.

Pero inmediatamente se nos presentará una gran interrogante en el sentido de que ya sabemos que podemos generar una infinidad de enteros diferentes sumando unidades, pero a la vez como estos enteros pueden ser también representados como producto de primos diferentes, entonces esto nos lleva a que necesitamos una infinidad de primos. Y para esto Euclides aún nos sigue sorprendiendo con la proposición 20 del libro IX, que establece "*hay más números primos que cualquier cantidad propuesta de números primos*", es decir, la cantidad de números primos es infinita. Esto sin duda es una sorpresa para la intuición, puesto que si empezamos a listar a los primos, no es difícil darse cuenta de que poco a poco se van alejando unos de otros[7], lo cual podría hacer suponer que no hay muchos primos.

[7] Aunque llegan a aparecer parejas de impares consecutivos que son primos, los conocidos como primos gemelos.

Sobre el *Teorema Fundamental.*

Sabemos que los primos para los griegos fueron como la semilla primigenia de todos los números enteros, de hecho Euclides mismo lo visualizó así, por ello estableció dos proposiciones que son la base del *Teorema Fundamental de la Aritmética*. En la proposición 30 del libro VII $[1994, 152]$, se afirma que "*si dos números, al multiplicarse entre sí, hacen algún número, y algún número primo mide a su producto, también medirá a uno de los iniciales"*. Desde una perspectiva actual. Si $p|ab$ entonces $p|a$ o $p|b$.[8] Si suponemos que $p|a$ por lo tanto la proposición queda demostrada. Si $p \nmid a$ sucede que $(p, a) = 1$, por lo que existe la combinación lineal $1 = pt + az$ de donde $b = ptb + abz$, y como $p|ab$ entonces existe una w en los enteros tal que $ab = pw$. Entonces $b = p(tb + wz)$ y en consecuencia $p|b$.

Por otro lado, en la proposición 31 del libro VII [1994, 153], Euclides enunció que "*todo número compuesto es medido por algún número primo*". Para demostrar este resultado tomemos algún número *m* compuesto. Por la definición 14 sabemos que todo compuesto es dividido por algún número *k*. Ahora, si *k* es primo la proposición queda demostrada, pero si no lo es entonces *k* es compuesto y algún número *r* lo debe medir, si *r* es primo y mide a *k*, y como *k* mide a *m*, en consecuencia *r* mide a *m*, por lo tanto se demuestra la proposición. Pero si *r* es compuesto entonces existe un número que lo mide. Así, bajo este proceso se debe de encontrar algún número primo que mide a m, pues si esto no fuera así, hallaríamos una serie infinita de números compuestos positivos que miden a m, todos menores que los anteriores, lo cual no sucede en los naturales. Por lo tanto existe un número primo menor que *k* tal que mide a *m*, es decir, todo número es medido por algún primo.

Pero Euclides tuvo una visión extraordinaria y fusiona sus ideas sobre este punto y concluye en la proposición 32 que: "*todo número o es primo o es medido por algún número primo*". Estas proposiciones son fundamentales ya que establecen que los naturales están bien definidos tanto en su construcción como en su composición por un conjunto de números que, aunque no conocemos del todo, son capaces de generar una infinidad de números. Sin embargo la intuición respecto a los primos es manipulada de una manera muy directa, por un lado tenemos al conjunto infinito de los naturales que

[8] La notación p|ab indica que p divide al producto ab.

estaba bien definido, y por otro lado la base que le da sustento a los naturales está soportada sobre un conjunto aparentemente muy inestable, impredecible y tan escaso que corre el riesgo de ser finito y con ello quebrar la estructura de los naturales. Entonces, Euclides estableció la justificación de que los primos sí son un conjunto infinito, a pesar de lo poco que se podía ver en ellos de manera directa. Así, Euclides nos proporcionó una de las más bellas demostraciones de la matemática, ésta se encuentra en la proposición XX del libro IX.

Proposición 20 del libro IX [1994, 226]

"Hay más números primos que cualquier cantidad propuesta de números primos"

Demostración.

Supongamos que los primos son finitos, es decir, existen sólo $p_1, p_2, p_3, \dots, p_k$ primos. Sea $M = p_1.p_2.p_3 \dots p_k + 1$. Si M es primo entonces éste no puede ser uno de los conocidos p_i ya que es más grande que cualquiera de ellos, por lo tanto tendríamos un primo más que los propuestos, lo que es una contradicción con suponer que los p_i son un conjunto finito. Ahora, supongamos que M no es primo, en consecuencia, existe un primo que lo divide, supongamos que p_j es ese primo, pero si p_j divide a M entonces debe dividir al 1, lo cual es una contradicción. Por tanto existe otro primo diferente al conjunto de los conocidos $p_1, p_2, p_3, \dots, p_k$, y si se repite el proceso se llega a que la cantidad de primos es infinita.

Con este resultado podemos ver el nivel alcanzado por la matemática griega al demostrar que el conjunto de los primos, que no sabemos cómo se comportan, en efecto tienen cardinalidad infinita y sus elementos están en capacidad de generar a los naturales sin dificultad. Es importante mencionar que la demostración euclidiana es la misma que se sigue enseñando en los cursos actuales de álgebra.

Ahora que sabemos que son infinitos y que cada entero positivo es producto de primos, resulta importante ver cómo pueden sacudir nuestra intuición. Por un lado Euclides nos dice que los enteros son producto de primos, y por otro lado podemos ver que en determinada escala de los naturales ya son muy escasos, es decir, sabemos que son un conjunto infinito pero no qué tan frecuente es su presencia, Veamos a lo que nos referimos: Sea la secuencia $(3+1)!+2, (3+1)!+3, (3+1)!+4$, estos números son $26, 27, 28$ o visto como intervalo [26, 28], en donde no hay ningún primo. Supongamos

ahora que tenemos la secuencia (4+1)!+2, (4+1)!+3, (4+1)!+4, (4+1)!+5, el intervalo es [122, 125], donde tampoco hay primos, estos son cuatro números compuestos. Avancemos un poco más, sea la secuencia: (10+1)!+2, (10+1)!+3, (10+1)!+4, (10+1)!+5, (10+1)!+6, (10+1)!+7, (10+1)!+8, (10+1)!+9, (10+1)!+10, (10+1)!+11, entonces el intervalo es [39916800, 31916809]. Estos son 10 enteros consecutivos compuestos, es decir, en este intervalo no existe un solo primo. Supongamos ahora que nuestra secuencia es (n+1)!+2, (n+1)!+3… (n+1)!+(n+1), donde tenemos n números consecutivos que son compuestos. Lo interesante aquí es que nada detiene estas construcciones, esto es, podemos construir una cantidad infinita de intervalos donde en cada uno sólo hay números compuestos y esos intervalos son del tamaño que queramos que n lo sea, así podemos hacer intervalos con 100, 1000, 10000,… números compuestos consecutivos. Ese es el primer golpe a la intuición que nos muestran los primos: son infinitos pero al parecer muy escasos. Pero la respuesta a las dudas es que no hay problema, por muy escasos que sean los primos, éstos tienen la capacidad de representar a cualquier entero como producto de ellos, es más, podemos decir que tal escasez optimiza la representación como producto de potencias de ellos, ya que a partir de un subconjunto se forman todos los elementos de los naturales.

Después de lo visto anteriormente parecería que la relación entre los primos y los naturales quedaría confinada solo los *Elementos*, y que ésta concluía ahí con las proposiciones y definiciones hechas sobre los primos, pero aproximadamente 2000 años después apareció Leonhard Euler para darle nueva vida a esta historia, y llevó así a la teoría de números a una nueva dimensión donde los matemáticos no se imaginaron que llegarían.

Euler y los números primos.

De manera reiterada, cuando deseamos saber si un número es primo, nos enfrentamos a un camino tortuoso y con obstáculos que podrían parecer insalvables, y ésta es una de las razones por la que también es adecuado acercarse a los caminos utilizados por la teoría de la probabilidad. Sabemos que las posibilidades de que un número entero sea dividido por el 2 es de $\frac{1}{2}$, y la posibilidad de que no sea dividido es de $\left(1-\frac{1}{2}\right)$; de la

misma forma la posibilidad de que no lo divida el 3 es de $\left(1-\frac{1}{3}\right)=\frac{2}{3}$. Por otro lado, la posibilidad de que se den los dos eventos simultáneamente, es decir, que a un entero no lo divida ni el 2 ni el 3 es $\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)=\frac{1}{3}$, o que no lo divida ni ninguno de estos 3 es $\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=\frac{4}{15}$.

De lo anterior podemos decir que una aproximación de la probabilidad de que un entero *x* sea primo es

$$p(x)=\prod_{\substack{p\ primo\\ p<x}}\left(1-\frac{1}{p}\right)=\ \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right).....\left(1-\frac{1}{p}\right).$$

Si a esta igualdad la evaluamos en el logaritmo natural, entonces se tiene

$$Ln(p(x))=Ln\prod_{\substack{p\ primo\\ p<x}}\left(1-\frac{1}{p}\right)$$

$$Ln(p(x))=\sum_{\substack{p\ primo\\ p<x}}Ln\left(1-\frac{1}{p}\right).$$

Aquí podemos trabajar la expresión $Ln\left(1-\frac{1}{p}\right)$ como $Ln(1-t)$, donde $t=\frac{1}{p}$. Por otro lado, como[9] $Ln(1-t) = -t + O(t^2)$, entonces

$$Ln(p(x))=\sum_{\substack{p\ primo\\ p<x}}\left(-\frac{1}{p}+o(\frac{1}{p^2})\right).$$

Aquí tenemos que el error $O\left(\frac{1}{p^2}\right)$ que se genera en cada sumando es muy pequeño, es más, la suma de ellos $\sum_{\substack{p\ primo\\ p<x}} O\left(\frac{1}{p^2}\right)$ es menor que $\sum_{k=1}^{\infty}\frac{1}{k^2}=\frac{\pi^2}{6}$ y como este número es pequeño entonces podemos descartar los errores y adoptar la aproximación

$$Ln(p(x))\approx\sum_{\substack{p\ primo\\ p<x}}-\frac{1}{p}.$$

Además, $p(x)$ es mayor que cero y menor que uno, pero más aún, como

[9] Esta igualdad se puede generar a partir del desarrollo en serie de Taylor de f(x)=ln(1-t) donde f'(0)(t-0)=-t en el primer sumando y $O(t^2)$ es una aproximación de la serie de Taylor.

$$p(x) = \prod_{\substack{p\ primo \\ p<x}} \left(1-\frac{1}{p}\right) = \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\ldots\left(1-\frac{1}{p}\right) = \frac{\prod_{p<x}(p-1)}{\prod_{p<x} p}$$

tiende a acercarse a cero, entonces $Ln(p(x))$ es negativo y por tanto podemos considerar a la aproximación de $p(x)$ en términos positivos, esto es

$$Ln(p(x)) \approx \sum_{\substack{p\ primo \\ p<x}} \frac{1}{p}.$$

Finalmente, como $Ln(p(x))$ tiende a infinito cuando x tiende a infinito, entonces resulta que la suma $\sum_{\substack{p\ primo \\ p<x}} \frac{1}{p}$ diverge. Este razonamiento para enunciar la divergencia de esta serie es un tanto informal, pero el objetivo intrínseco era llegar a la propuesta de divergencia a través de un camino un tanto heurístico pero estimulante para la intuición, pues esto nos lleva a digerir la idea de que los primos es un conjunto más denso (dentro de los enteros) de lo que esperaríamos después de haber navegado por esos grandes agujeros que mencionamos en la página 10. El primer impacto después de percibir que no existen primos en ciertos intervalos, es pensar que los primos son un conjunto infinito pero a la vez escaso, pero después de la primera incursión en la divergencia de la suma del recíproco de los primos las ideas cambian. Ahora resulta que como la suma diverge entonces no podemos pensar que es suficiente con que el conjunto sea infinito, requerimos que además sea numeroso, porque de lo contrario puede pasar lo mismo que con los cuadrados, que son un conjunto infinito pero escaso, ya que la suma de sus recíprocos converge a $\frac{\pi^2}{6}$. Ahora daremos lugar a dos formas de convencernos de manera más estructurada de que la suma de los recíprocos de los primos diverge: una será la de Euler[10] y la segunda de Iván Niven.

[10] Cabe señalar que una de las pasiones de Euler dentro del cálculo era trabajar con series infinitas, y para ello se basó en los logaritmos que habían sido desarrollados el siglo anterior. Su contribución a esta disciplina demostrando que la serie armónica ($\sum_{k=1}^{\infty}\frac{1}{k}$) diverge. Otro de sus logros fue demostrar el llamado problema de Basilea, el cual consistía en ver a que número convergía exactamente la serie $\sum_{k=1}^{\infty}\frac{1}{k^2}$, y su conclusión fue que $\sum_{k=1}^{\infty}\frac{1}{k^2}=\frac{\pi^2}{6}$.

Demostración de Euler y Niven.

Antes de exponer el proceso de Euler para demostrar que la suma de los recíprocos de los primos diverge, sería importante conocer otro resultado que es fundamental para entender la divergencia de la suma mencionada. Por otro lado, este resultado previo será la base para lo que hoy se conoce como la función zeta de Euler –y de ésta se derivará la función zeta de Riemann-. Ahora pasamos a exponer este resultado.

La serie armónica y el producto de primos[11].

Euler consideró que a la serie armónica se le podían sustraer subconjuntos infinitos de sumandos de esta manera: Sea $x = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \cdots$, luego ésta se multiplica por $\frac{1}{2}$ y la nueva suma se resta de la original, es decir,

$$x - \frac{1}{2}x = \left(1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \cdots\right) - \left(\frac{1}{2} + \frac{1}{4} + \frac{1}{6} + \frac{1}{8} + \frac{1}{10} + \cdots\right) =$$

$$= \frac{1}{2}x = 1 + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{9} + \cdots (1)$$

Esta serie sólo contiene a los impares en sus denominadores. Posteriormente multiplicó a esta última por $\frac{1}{3}$ y la restó a (1), es decir,

$$\frac{1}{2}x - \left(\frac{1}{3}\right)\frac{1}{2}x = \left(1 + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{9} + \cdots\right) - \left(\frac{1}{3} + \frac{1}{9} + \frac{1}{15} + \frac{1}{21} + \frac{1}{27} + \cdots\right) =$$

$$= \frac{1 \cdot 2}{2 \cdot 3}x = 1 + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \cdots .$$

Después se hace lo mismo con $\frac{1}{5}$ para llegar a que

$$\frac{1 \cdot 2 \cdot 4}{2 \cdot 3 \cdot 5}x = 1 + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} + \cdots +,$$

y entonces el patrón parece claro; multiplicando por los inversos de los primos y restando ese resultado a la serie anterior obtuvo que

$$\frac{1 \cdot 2 \cdot 4 \cdot 6 \cdot 10 \cdot 12 \cdot 16 \ldots}{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13.17 \ldots}x = 1,$$

y despejando[12] x llegó a que

[11]Enseguida exponemos la forma que Euler usó para demostrar la relación entre recíprocos de primos y naturales. Es importante señalar que dejamos la demostración tal como la expuso Euler y esto incluye algunos pasos que no están plenamente justificados, y en su momento lo señalaremos.

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\cdots=\frac{2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13.17\ldots}{1\cdot 2\cdot 4\cdot 6\cdot 10\cdot 12\cdot 16\ldots}.$$

Para dejar las cosas más claras, esta demostración puede verse de otra manera:

Sea $S=1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{6}+\frac{1}{8}+\frac{1}{9}+\frac{1}{12}+\cdots$; esta serie es la de los inversos de los enteros positivos que tiene por denominador a números de la forma 2^m3^n, por tanto S se puede expresar como:

$$S=\left[1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots+\frac{1}{2^m}+\cdots\right]\left[1+\frac{1}{3}+\frac{1}{9}+\frac{1}{27}+\cdots\frac{1}{3^n}+\cdots\right],$$

pero notemos que cada una de las expresiones que se encuentran entre los corchetes, corresponde a una progresión geométrica, por lo que se deduce que

$$S=\left[\frac{1\left(1-\left(\frac{1}{2}\right)^{m+1}\right)}{1-\frac{1}{2}}\right]\left[\frac{1\left(1-\left(\frac{1}{3}\right)^{m+1}\right)}{1-\frac{1}{3}}\right]=\left[\frac{1}{1-\frac{1}{2}}\right]\left[\frac{1}{1-\frac{1}{3}}\right],$$

y simplificando el lado derecho se tiene que $S=\frac{2*3}{1*2}$. Este procedimiento lo podemos generalizar con todos los primos, es decir, como todo entero se puede escribir como un producto de potencia de primos, entonces tomamos los denominadores cuya expresión sea de la forma $2^m3^n5^s\cdots p^r$ y entonces tenemos

$$\sum_{k=1}^{\infty}\frac{1}{k}=\frac{2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13.17\ldots}{1\cdot 2\cdot 4\cdot 6\cdot 10\cdot 12\cdot 16\ldots},$$

o lo que es lo mismo

$$\sum_{k=1}^{\infty}\frac{1}{k}=\frac{\prod p}{\prod(p-1)}.$$

Así llegamos a una relación entre la serie armónica y los números primos.

Con este resultado ya podemos abordar la demostración de que la suma de los recíprocos de los primos diverge.

Euler consideró que $M=\sum_{k=1}^{\infty}\frac{1}{k}$, pero con base en lo anterior propuso que

$$M=\frac{2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13.17\ldots}{1\cdot 2\cdot 4\cdot 6\cdot 10\cdot 12\cdot 16\ldots}=\frac{1}{\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5}\cdot\frac{6}{7}\ldots\frac{10}{11}\ldots},$$

[12] Aquí se tiene que señalar que Euler no justificó que en el lado derecho de la igualdad los términos que restan después de 1 tienden a cero, pero en el párrafo siguiente se demuestra de otra manera.

y después aplicó logaritmo, lo cual no es sorpresa, ya que las series infinitas y los logaritmos eran sus armas preferidas dentro del ámbito de las matemáticas[13]. La expresión quedó de la siguiente manera

$$\ln(M) = \ln(1) - \ln\left(\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5}\cdots\frac{10}{11}\cdots\right) = -\ln\left(\frac{1}{2}\right) - \ln\left(\frac{2}{3}\right) - \ln\left(\frac{4}{5}\right) - \cdots$$

$$= -\ln\left(1-\frac{1}{2}\right) - \ln\left(1-\frac{1}{3}\right) - \ln\left(1-\frac{1}{5}\right) - \cdots - \ln\left(1-\frac{1}{11}\right) - \cdots,$$

y posteriormente uso un resultado ya conocido para su época

$$\ln(1-x) = -x - \frac{x^2}{2} - \frac{x^3}{3} - \frac{x^4}{4} - \cdots,$$

con esto, y considerando que $x = \frac{1}{p}$, p primo, y |x|≤ 1,

$$\ln(M) = \tfrac{1}{2} + \tfrac{1}{2}\left(\tfrac{1}{2}\right)^2 + \tfrac{1}{3}\left(\tfrac{1}{2}\right)^3 + \tfrac{1}{4}\left(\tfrac{1}{2}\right)^4 + \cdots + \tfrac{1}{3} + \tfrac{1}{2}\left(\tfrac{1}{3}\right)^2 + \tfrac{1}{3}\left(\tfrac{1}{3}\right)^3 + \tfrac{1}{4}\left(\tfrac{1}{3}\right)^4 + \cdots +$$

$$+ \cdots + \tfrac{1}{5} + \tfrac{1}{2}\left(\tfrac{1}{5}\right)^2 + \tfrac{1}{3}\left(\tfrac{1}{5}\right)^3 + \tfrac{1}{4}\left(\tfrac{1}{5}\right)^4 + \cdots + \cdots$$

Después agrupó términos semejantes

$$\ln(M) = \left[\frac{1}{2} + \frac{1}{3} + \frac{1}{7} + \frac{1}{11} + \cdots\right] + \frac{1}{2}\left[\left(\frac{1}{2}\right)^2 + \left(\frac{1}{3}\right)^2 + \left(\frac{1}{5}\right)^2 + \cdots\right] +$$

$$+ \tfrac{1}{3}\left[\left(\tfrac{1}{2}\right)^3 + \left(\tfrac{1}{3}\right)^3 + \left(\tfrac{1}{5}\right)^3 + \cdots\right] + \tfrac{1}{4}\left[\left(\tfrac{1}{2}\right)^4 + \left(\tfrac{1}{3}\right)^4 + \left(\tfrac{1}{5}\right)^4 + \cdots\right] + \cdots,$$

finalmente Euler renombró su ecuación y obtuvo $\ln(M) = A + \frac{1}{2}B + \frac{1}{3}C + \frac{1}{4}D + \cdots$, donde $A = \sum\frac{1}{P},\ B = \sum\frac{1}{P^2},\ C = \sum\frac{1}{P^3}$ ...

Con su gran capacidad para interpretar resultados Euler dedujo rápidamente que B, C, D,…tienen un valor finito y que la suma $\frac{1}{2}B + \frac{1}{3}C + \frac{1}{4}D + \cdots$ también tiene un valor finito, por lo cual la demostración casi estaba completa. Sin embargo, antes de seguir, veamos dos resultados importantes para comprender mejor lo que hizo Euler.

Teorema.

Para $n \geq 2$ tenemos la siguiente desigualdad:

$$\sum_{k=2}^{\infty}\frac{1}{k^n} \leq \frac{1}{n-1}.$$

[13] Véase Dunham[2000]

Demostración.

Consideremos $y = \frac{1}{x^n}$, entonces cada segmento de $\sum_{k=2}^{\infty} \frac{1}{k^n}$ queda acotado por $y = \frac{1}{x^n}$, es decir,

$$\sum_{k=2}^{\infty} \frac{1}{k^n} \leq \int_1^{\infty} \frac{1}{x^n} dx = \frac{1}{n-1},$$

por otro lado

$$\sum_{p} \frac{1}{p^n} \leq \sum_{p} \frac{1}{p^2} \leq \sum_{k=2}^{\infty} \frac{1}{k^2} \leq \frac{1}{n-1} \leq 1 < \infty.$$

Que es lo que se quería demostrar.

Teorema.

La suma $\frac{1}{2}B + \frac{1}{3}C + \frac{1}{4}D + \cdots$ es finita.

Demostración.

$$\frac{1}{2}B + \frac{1}{3}C + \frac{1}{4}D + \cdots = \frac{1}{2}\sum_{p} \frac{1}{p^2} + \frac{1}{3}\sum_{p} \frac{1}{p^3} + \frac{1}{4}\sum_{p} \frac{1}{p^4} + \cdots$$

$$\leq \frac{1}{2}\sum_{k=2}^{\infty} \frac{1}{k^2} + \frac{1}{3}\sum_{k=2}^{\infty} \frac{1}{k^3} + \frac{1}{4}\sum_{k=2}^{\infty} \frac{1}{k^4} + \cdots$$

Aplicando el teorema anterior a cada una de las sumas

$$\leq \frac{1}{2}(1) + \frac{1}{3}\left(\frac{1}{2}\right) + \frac{1}{4}\left(\frac{1}{3}\right) + \cdots$$

$$\leq 1 + \tfrac{1}{2}\left(\tfrac{1}{2}\right) + \tfrac{1}{3}\left(\tfrac{1}{3}\right) + \tfrac{1}{4}\left(\tfrac{1}{4}\right) + \cdots,$$

y esta es la suma de los recíprocos de los cuadrados y Euler fue el que demostró su convergencia que es:

$$= \sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{\pi}{6} < \infty,$$

entonces $\frac{1}{2}B + \frac{1}{3}C + \frac{1}{4}D + \cdots$ converge.

Después de estas demostraciones ahora sí damos paso a la demostración de corte euleriano.

Teorema.

La suma $\sum_{p} \frac{1}{p}$ diverge.

Demostración.

Euler ya había obtenido $\ln(M) = A + \frac{1}{2}B + \frac{1}{3}C + \frac{1}{4}D + \cdots$, por lo tanto

$$M = e^{A+\frac{1}{2}B+\frac{1}{3}C+\frac{1}{4}D+\cdots} = e^{A}e^{\frac{1}{2}B+\frac{1}{3}C+\frac{1}{4}D+\cdots},$$

por otro lado tenemos que

$$M = \sum_{k=1}^{\infty} \frac{1}{k} = \infty,$$

por lo tanto

$$e^{A}e^{\frac{1}{2}B+\frac{1}{3}C+\frac{1}{4}D+\cdots} = \infty,$$

pero $\frac{1}{2}B + \frac{1}{3}C + \frac{1}{4}D + \cdots$es finito, en consecuencia

$$e^{\frac{1}{2}B+\frac{1}{3}C+\frac{1}{4}D+\cdots},$$

es finito, entonces e^{A} es infinito, por tanto $A = \ln(e^{A}) = \infty$ y entonces

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{7} + \frac{1}{11} + \cdots = A = \infty.$$

Como consecuencia vemos que a pesar de que los primos van dando grandes saltos entre los enteros, su abundancia es mayor de la que nuestra intuición nos dice, esto es, no son tan inhabituales como los cuadrados y aunque ambos son infinitos, hay más primos que cuadrados.

Es importante hacer ver que Euler operaba con el infinito, pero con las reglas del álgebra que hoy conocemos puede parecernos que existen deficiencias lógicas en sus demostraciones. No obstante, también hay que recordar que el cálculo era una rama que estaba en pleno desarrollo, y que el rigor matemático no era como hoy lo conocemos, y hubo que esperar otro tiempo para que alguien más estableciera el rigor que hacía falta. Ante esta situación se han dado otras demostraciones de diversos teoremas de épocas anteriores entre las que está, por supuesto, este teorema de los recíprocos de los primos. En 1971 Iván Niven demostró también que $\sum_{p} \frac{1}{p}$ diverge.

Antes de dar paso a la demostración de Niven, hay que observar que cualquier número se puede escribir como el producto de dos factores, uno es un cuadrado perfecto y el otro no se puede escribir como producto de potencia, es decir, es producto de

primos diferentes. Entonces la factorización es de la forma ($n = j^2k$). Posteriormente Niven define

$$\sum_{k\leq n}{}' \frac{1}{k},$$

que representa la suma de los inversos de los números enteros sin potencia que sean menores o iguales que n (incluyendo al 1).

Lema.

$$\lim_{n\to\infty}\left(\sum_{k\leq n}{}' \frac{1}{k}\right) = \infty.$$

Demostración.

Tomemos una parte finita de la serie armónica

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\cdots+\frac{1}{n} \leq \left(\sum_{j\leq n}\frac{1}{j^2}\right)\left(\sum_{k\leq n}{}' \frac{1}{k}\right),$$

lo cual se puede deducir de la observación hecha anteriormente de que todo $r \leq n$ puede expresarse como $r = j^2k$ donde k no tiene exponentes, entonces $\frac{1}{r}$ aparece una sola vez en el lado derecho de la desigualdad, pero se tiene que notar que el producto de la derecha contiene más sumandos que los de la izquierda, así

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\cdots+\frac{1}{n} \leq \left(\sum_{j\leq n}\frac{1}{j^2}\right)\left(\sum_{k\leq n}{}' \frac{1}{k}\right) \leq \left(\sum_{j\leq n}^{\infty}\frac{1}{j^2}\right)\left(\sum_{k\leq n}{}' \frac{1}{k}\right) = \frac{\pi^2}{6}\left(\sum_{k\leq n}{}' \frac{1}{k}\right)$$

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\cdots+\frac{1}{n} \leq \frac{\pi^2}{6}\left(\sum_{k\leq n}{}' \frac{1}{k}\right),$$

en consecuencia

$$\frac{6}{\pi^2}\left(1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\cdots+\frac{1}{n}\right) \leq \left(\sum_{k\leq n}{}' \frac{1}{k}\right),$$

y si $n\to\infty$ entonces la serie armónica diverge y

$$\lim_{n\to\infty}\left(\sum_{k\leq n}{}' \frac{1}{k}\right) = \infty$$

Teorema.

La serie $\sum_p \frac{1}{p}$ diverge.

Demostración.

Supongamos que no diverge y que

$$\sum_p \frac{1}{p} = A \text{ (converge a A).}$$

Euler ya había obtenido el resultado que identifica a la función exponencial con una serie

$$e^x = 1 + x + \frac{x^2}{2!} + \cdots = \sum \frac{x^n}{n!},$$

para cualquier x. Para $x > 0$, $e^x \geq 1 + x$. Ahora, que sea $n \geq 2$ cualquier natural, y sea q el número primo más grande que es menor o igual que n, entonces

$$e^A > e^{\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\cdots\frac{1}{q}} = \prod_{p\leq n} e^{\frac{1}{p}}$$

$$\geq \prod_{p\leq n}\left(1+\frac{1}{p}\right) = \left(1+\frac{1}{2}\right)\left(1+\frac{1}{3}\right)\left(1+\frac{1}{5}\right)\left(1+\frac{1}{7}\right)\cdots\left(1+\frac{1}{q}\right),$$

recordemos que $e^{\frac{1}{p}} \geq 1 + \frac{1}{p}$ por lo tanto

$$\prod_{p\leq n}\left(1+\frac{1}{p}\right) = \left(1+\frac{1}{2}\right)\left(1+\frac{1}{3}\right)\left(1+\frac{1}{5}\right)\left(1+\frac{1}{7}\right)\cdots\left(1+\frac{1}{q}\right) \geq \sum_{k\leq n}{}' \frac{1}{k}$$

y veamos que del lado izquierdo se tienen los inversos de los enteros hasta n no elevados al cuadrado, junto con los inversos de otros números más grandes que tampoco están elevados al cuadrado, pero que son mayores que n. Por lo tanto

$$e^A > \sum_{k\leq n}{}' \frac{1}{k},$$

y también se cumple si $n \to \infty$ porque A contiene a todos los primos, y como e^A es finito, entonces $\sum_{k\leq n} \frac{1}{k}$, es divergente cuando $n \to \infty$. Entonces es una contradicción con que $\sum'_{k\leq n} \frac{1}{k}$ es finito, por lo tanto A no converge y

$$\sum_p \frac{1}{p} \text{ diverge.}$$

Con el resultado de Niven, obviamente apegado al rigor matemático que hoy conocemos, verificamos la autenticidad de las palabras de Euler. Y no es que se haya

dudado de él, sino más bien se trata de establecer de una manera más precisa y sin ambigüedades lógicas los teoremas por él demostrados. Así queda comprobado que a pesar de que la intuición dice una cosa, los hechos dicen otra.

Para terminar esta parte podemos, a partir de la serie armónica, ver que los primos son un conjunto infinito, y aunque ya lo sabíamos gracias a Euclides, esta forma de verlo es complementaria.

Corolario.

Los primos son un conjunto infinito.

Demostración.

Sabemos que $\sum_{k=1}^{\infty} \frac{1}{k}$ diverge, y también sabemos que

$$\sum_{k=1}^{\infty} \frac{1}{k} = \frac{\prod p}{\prod (p-1)}.$$

Pero para que $\frac{\prod p}{\prod (p-1)}$ sea infinita se necesita tener una infinidad de primos. Por tanto los primos son infinitos.

Como podemos apreciar, esta relación es interesante por el resultado tan trascendente que le sigue como consecuencia, pero todavía hay algo más detrás de todo esto. Euler, con su gran genio y su intuición matemática, llevo el análisis hasta donde era inimaginable, y construyó, a través de esta demostración, la base de lo que hoy llamamos teoría analítica de los números, o dicho con otras palabras, fusionó el análisis con la teoría de números, dando paso así a un desarrollo poderoso y novedoso que ya no volvería a ser abandonado por los matemáticos.

Capítulo II

Números primos en grupos.

En las secciones anteriores ahondamos en la reflexión sobre la existencia y la posición que tienen los primos dentro del conjunto de los naturales, y nos referimos a características globales como son la infinitud o su densidad respecto al conjunto total de los enteros. Ya vimos que los primos son inexistentes en grandes intervalos de enteros consecutivos donde sólo existen compuestos, pero a pesar de esto sabemos que siempre existirá un primo más adelante. Pero bajo esta incertidumbre respecto a la posible existencia ordenada de los primos resulta que sí podemos extraer de ellos una primera clasificación que nos lleva a enterarnos que ellos se localizan en dos grandes conjuntos ajenos entre ellos.

Clasificación de los primos.

Si nos ubicamos en una clasificación general de los enteros módulo cuatro, sabemos que los primos impares se tienen que repartir entre los números de la forma 4k + 1 o 4k – 1. Un ejemplo de primos en estos conjuntos es:

$$\{4k+1\} = \{5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 93, 97, \dots\},$$

y

$$\{4k-1\} = \{3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83 \dots\}.$$

Como los primos son un conjunto infinito entonces sabemos que los conjuntos mencionados bajo la unión también son un conjunto infinito, pero la pregunta es ¿por separado cada uno es infinito? o ¿uno es infinito y el otro finito? Estas preguntas inquietaron a Euler en el siglo XVIII, y para responder a éstas lo haremos por la vía de dos teoremas.

Teorema.

Existe una infinidad de primos de la forma $4k-1$.

Demostración.

La demostración tendrá semejanzas con la prueba euclidiana de la infinitud de los primos, pero primero necesitamos señalar que el producto de números de la forma $4k+1$ tiene esa misma forma, es decir,

$(4k+1)(4k'+1) = 16kk' + 4k + 4k' + 1 = 4(4kk' + k + k') + 1 = 4r + 1.$

Ahora, a la manera euclidiana, supongamos que sólo hay una cantidad finita de primos de la forma $4k-1$, es decir, $p_1 = 4k_1 - 1,\ p_2 = 4k_2 - 1, \dots, p_n = 4k_n - 1$ y con ellos formamos al número $M = 4(p_1 \cdot p_2 \cdot p_3 \cdots p_n) - 1$. Para analizar a M sigamos dos rutas, que éste sea primo o que no lo sea. Veamos las dos posibilidades.

Caso 1.

Si M es primo ya terminamos, porque M tiene que ser mayor que cualquiera de los p_i, y por lo tanto él es un primo más que no está en el conjunto que supusimos que era el que contenía a todos.

Caso 2.

Si M es compuesto, entonces tiene al menos un divisor primo, y como M es impar, entonces éste tiene que ser de la forma $4k+1$ ó $4k-1$. Ahora, si suponemos que es de la forma $4k_i - 1$, entonces tiene que ser uno entre p_1 y p_n, porque estos son el total de esos primos, y recordemos que son una cantidad finita. Pero si es uno de ellos entonces éste tiene que dividir también al uno ya que $4k_i - 1$ divide a M, y esto no es posible, ya que $p_i \geq 3$ por ser primo. Entonces nos queda que los divisores de M son sólo de la forma $4k+1$, pero esto no puede ser, ya que de acuerdo con la observación al principio, como el producto de primos de la forma $4k+1$ es de la misma forma, entonces para que M, que tiene la forma $4(p_1 \cdot p_2 \cdot p_3 \cdots p_n) - 1$, se pueda expresar como producto de primos, se necesitará que por lo menos uno de sus factores sea de la forma $4k-1$. Pero éste resultaría ser diferente de los que ya existen. Entonces tiene que existir otro primo más de la forma $4k-1$. En resumen, de los casos 1 y 2 tenemos que los primos de la forma $4k-1$ son un conjunto infinito.

El conjunto de los primos $4k+1$.

Ahora ya sabemos que por lo menos uno de los conjuntos es infinito, pero ¿qué sucede con el otro? Supongamos que el conjunto de primos de la forma $4k+1$ es finito y sigamos la idea de la demostración anterior. Sean

$$p_1 = 4k_1 + 1, p_2 = 4k_2 + 1, \dots, p_n = 4k_n + 1,$$

todos los primos de la forma $4k + 1$, y sea $M = 4(p_1 \cdot p_2 \cdot p_3 \cdots p_n) + 1$.

Caso 1.

Si M es primo ya terminamos, puesto que encontramos un primo de la forma $4k + 1$ que es diferente y mayor a los propuestos.

Caso 2.

Si M es compuesto, el problema comienza con el caso en el que se tenga que M está formado sólo con una cantidad par de factores de la forma $4k - 1$, pues sucede que sólo con números de la forma $4k' - 1$ sí se puede llegar a M, y nunca recurrimos a un factor de la forma $4k' + 1$ que nos pudiera llevar después a una contradicción. Entonces, este razonamiento no puede ser aplicado para demostrar que los primos de la forma $M = 4k + 1$ son infinitos.

De acuerdo con lo anterior cualquiera supondría que el único conjunto infinito es el de los primos de la forma $4k - 1$. No obstante, Euler vuelve a sorprendernos y realiza una demostración utilizando de nueva cuenta las series que tanto le apasionaron.

En un artículo de 1795 Euler vuelve a discutir acerca de la abundancia de los primos de la forma $4k + 1$ y considera la serie infinita $\frac{1}{3} - \frac{1}{5} + \frac{1}{7} + \frac{1}{11} - \frac{1}{13} - \frac{1}{17} + \frac{1}{19} + \frac{1}{23} - \frac{1}{29} + \cdots$, donde los primos de la forma $4k - 1$ vienen precedidos de un signo positivo y los primos de la forma $4k + 1$ tienen un signo negativo. Acto seguido Euler presenta una aproximación de esta suma que es 0.3349816, y con estos elementos construye la demostración de que los primos de la forma $4k + 1$ son infinitos. Veamos lo que hace: toma S y T tales que

$$S = \frac{1}{5} + \frac{1}{13} + \frac{1}{17} + \frac{1}{29} + \frac{1}{37} + \frac{1}{41} + \cdots \text{ y } T = \frac{1}{3} + \frac{1}{7} + \frac{1}{11} + \frac{1}{19} + \frac{1}{23} + \frac{1}{31} + \cdots,$$

por lo tanto, con las dos igualdades obtiene $T = S + (T - S)$ y por lo tanto

$$T = S + \left(\frac{1}{3} - \frac{1}{5} + \frac{1}{7} + \frac{1}{11} - \frac{1}{13} - \frac{1}{17} + \frac{1}{19} + \frac{1}{23} - \frac{1}{29} + \cdots\right) \approx S + 0.3349816,$$

entonces, retomando la suma de los recíprocos de los primos llega a la igualdad

$$\sum_p \frac{1}{p} = \frac{1}{2} + T + S \approx \frac{1}{2} + 2S + 0.3349816,$$

y como el miembro de la izquierda es divergente, entonces

$$S = \frac{1}{5} + \frac{1}{13} + \frac{1}{17} + \frac{1}{29} + \frac{1}{37} + \frac{1}{41} + \cdots,$$

debe ser divergente, lo cual sucederá sólo si existe un número infinito de primos de la forma $4k + 1$.

Ahora ya sabemos que ambos conjuntos son infinitos. Sin embargo, aún está la cuestión de saber cuál de los dos grupos de primos es más abundante. Si nos remitimos a los primeros 100 primos, veremos que hay más de la forma $4k-1$ que $4k+1$, e incluso si tomamos más de cien números, la tendencia seguirá siendo la misma, y de esta manera nos aventuraríamos a afirmar que hay más primos de la forma $4k-1$. En la siguiente tabla podemos ver datos que apoyan esta afirmación.

X	*Números primos de la forma 4k-1*	*Números primos de la forma 4k+1*
100	*13*	*11*
200	*24*	*21*
300	*32*	*29*
400	*40*	*37*
500	*50*	*44*
600	*57*	*51*
700	*65*	*59*
800	*71*	*67*
900	*79*	*74*
1000	*87*	*80*
2000	*155*	*147*
3000	*218*	*211*
4000	*280*	*269*
5000	*339*	*329*
6000	*399*	*383*
7000	*457*	*442*
8000	*507*	*449*
9000	*562*	*554*
10000	*619*	*609*
20000	*1136*	*1125*
50000	*2583*	*2549*

Pero la intuición falla de nuevo, ya que esta afirmación es incorrecta. De hecho, en algún momento los primos de la forma $4k + 1$sí superan a los de la forma $4k - 1$, y posteriormente la tendencia vuelve a cambiar. Pero quien nos puede quitar la duda de lo que sucede es J. L.Littlewood, quien en 1914 demostró el siguiente teorema:

Teorema de J.E. Littlewood, 1914

Existen valores arbitrariamente grandes de x para los cuales hay más primos de la forma 4n + 1 hasta x, que números primos de la forma 4n -1. Dicho de otra forma, hay arbitrariamente grandes valores de x para los que

$$\#\{primos\ 4n + 1 \leq x\} - \#\{primos\ 4n - 1 \leq x\} \geq \frac{1\sqrt{x}}{2lnx}\, lnlnlnx.$$

Con este teorema podemos confirmar que sí hay intervalos donde los (*4k+1*) superan a los otros, y por lo tanto pensar en la abundancia de unos u otros ya no tiene sentido. Así, en primera instancia pareciera que ya no hay nada que decir a partir del teorema de Littlewood, sin embargo, después de ver la poca frecuencia de que el conjunto de los (*4n+1*) sí es mayor que el conjunto de los (*4n-1*), no se debe de dar por un hecho la imposibilidad de la sospecha de que los (*4n-1*) casi siempre son un conjunto mayor "la mayor parte del tiempo". En 1962, Knapowski y Turán fundamentaron una conjetura que es consistente con el resultado de Littlewood, pero que nos lleva a pensar que los primos de la forma *4n-1* son más abundantes que los de la forma *4n+1*.

Parece que la clasificación *grosso modo* de los primos en los *4n-1* y *4n+1* nos proporciona elementos adicionales a los elementos de cardinalidad antes mencionados, y una de las características que se nos presenta es que algunos primos se pueden escribir como suma de cuadrados y otros no.

Primos como suma de cuadrados.

Ahora pasamos a ver cuáles son aquéllos en los que sí es posible expresar los primos como suma de cuadrados y cuales no.

Teorema.

Los números de la forma $4k - 1$ no se pueden representar como la suma de dos cuadrados. Dicho de otra forma, si $n \equiv -1 \pmod 4$ entonces no se puede representar como suma de dos cuadrados.

Demostración.

Sea n un número de la forma $4k-1$ y supongamos que se puede escribir como suma de dos cuadrados, es decir, $n=x^2+y^2$. En primer lugar se observa que módulo 4 los números son de la forma $4k, 4k+1, 4k+2$, o $4k+3$. Entonces, para los cuadrados se tiene que

$$4k(4k)=4s$$

$$(4k+1)(4k+1)=16k^2+8k+1=4r+1$$

$$(4k+2)(4k+2)=16k^2+16k+4=4m$$

$$(4k+3)(4k+3)=16k^2+24k+9=4(4k^2+6k)+(8+1)=4n+1,$$

y se puede notar que todos los cuadrados son de la forma $4k$ ó $4k+1$. En otras palabras el cuadrado de cualquier entero es congruente a cero o a uno módulo cuatro, pero la suma de dos cuadrados es congruente a 0, 1 ó 2 módulo 4, es decir,

$$n=x^2+y^2 \equiv 0,1 \text{ ó } 2(\text{mod}4)$$

y esto es una contradicción con el hecho de que $n \equiv -1\,(\text{mod}4)$. Por lo tanto ningún entero de la forma $n \equiv -1\ (\text{mod}\ 4)$ se puede representar como suma de dos cuadrados, y en particular los primos, que es lo que finalmente nos interesa en este trabajo.

¿Y qué pasará con los otros primos?, es decir, los de la forma $4k+1$. Veamos el siguiente resultado preliminar:

Teorema.

Sea p primo, si $p \equiv 1(mod\ 4)$, entonces existen $x, y \in \mathbb{Z}^+$ tales que $x^2+y^2=kp$ para algún $k \in \mathbb{Z}^+$ y $k<p$.

Demostración.

Como $p \equiv 1(\text{mod}\ 4)$, entonces[14] $\left(\frac{-1}{p}\right)=1$, es decir, -1 es residuo cuadrático $(\text{mod}\ p)$; esto significa que existe $a \in \mathbb{Z}^+$ tal que $a^2 \equiv -1(\text{mod}\ p)$ y además $a<p$.[15] Como $a^2 \equiv -1(\text{mod}\ p)$ entonces $a^2+1=kp$ por lo que $x=a$, $y=1$. Por lo tanto

[14] Sea p un primo impar y a cualquier entero tal que p no divide a a. El símbolo de Legendre $\left(\frac{a}{p}\right)$ se define como $\left(\frac{a}{p}\right)=\begin{cases} 1 \text{ si a es residuo cuadrático de p} \\ -1 \text{ en otro caso} \end{cases}$

[15] Si $a>p$ entonces $a^2 \equiv \lambda(mod p)$ donde $\lambda \epsilon \{0,1,2,\dots,(p-1)\}$ entonces $a^2 \equiv \lambda^2(mod p)$, y $\lambda^2 \equiv -1(mod p)$.

$x^2+y^2 = kp$. Sólo falta demostrar que $k < p$; para esto retomemos que $a < p$. Por lo tanto $a \leq p-1$ y $kp = a^2+1 < (p-1)^2-1 \leq (p-1)^2 < p^2$, entonces $kp < p^2$ y por lo tanto $k < p$.

Hasta este momento se tiene un gran avance, pues ya se sabe que para cualquier primo de la forma $4k+1$ existen $x, y \in \mathbb{Z}^+$ tal que $x^2+y^2 = kp$. Pero si la k que está multiplicando a p fuera la unidad entonces esos primos sí se podrían representar como suma de dos cuadrados. Para llegar a $k = 1$ se necesita del resultado anterior y del principio del buen orden, que nos permite tomar entre el conjunto de las k a la más pequeña. Demos paso al teorema.

Teorema.

Todo primo p tal que $p \equiv 1(\mathrm{mod}4)$ puede ser escrito como suma de 2 cuadrados.

Demostración.

Por el teorema anterior y por el principio del buen orden existe m (la más pequeña) tal que $mp = x^2+y^2$ para $x, y \in \mathbb{Z}^+$. Demostraremos que $m = 1$.

Supongamos que $m > 1$ y tomemos un sistema completo de residuos (SCR)[16] módulo m entre $-\frac{m}{2}$ y $\frac{m}{2}$, entonces existen r y s entre $\pm\frac{m}{2}$, es decir, $-\frac{m}{2} \leq r, s < \frac{m}{2}$, tal que $r \equiv x(mod m)$ y $s \equiv y(mod m)$ por lo que $x^2+y^2 \equiv r^2+s^2(mod m)$, pero como $x^2+y^2 = mp$ y $m|mp$, entonces $x^2+y^2 \equiv 0(mod m)$ por lo que $r^2+s^2 = mn$ para algún $n \in \mathbb{Z}$. Por un teorema anterior sabemos que $(x^2+y^2)(r^2+s^2) = m^2np$ y por lo tanto

$$(x^2+y^2)(r^2+s^2) = (rx+sy)^2 + (ry-sx)^2 = m^2np.$$

Regresando al SCR, se concluye que $rx \equiv x^2(mod m)$, y $sy \equiv y^2(mod m)$ y como $mp = x^2+y^2$, por lo tanto $rx+sy \equiv x^2+y^2 \equiv 0(mod m)$ y por otro lado se tiene que $ry \equiv xy(mod m)$ y $sx \equiv xy(mod m)$, por lo tanto $ry-xs \equiv xy-xy \equiv 0(mod m)$ en consecuencia $m|ry-sx$ y $m|rx+sy$, de donde se obtiene que

$$np = \left(\frac{rx+sy}{m}\right)^2 + \left(\frac{ry-sx}{m}\right)^2.$$

Como antes se consideró que $r, s < \frac{m}{2}$ entonces

$$r^2 \leq \frac{m^2}{2^2} \text{ y } s^2 \leq \frac{m^2}{2^2},$$

[16]Un conjunto es un sistema completo de residuos módulo m si cada entero es congruente exactamente con alguno de los residuos del conjunto, y además entre ellos son incongruentes módulo m.

además $r^2+s^2 = mn$, por lo tanto $mn \leq \frac{m^2}{2}$ y $n \leq \frac{m}{2}$ y entonces $n \leq m$. Pero como m es la más pequeña y $m > 1$, entonces n no puede ser cero, ya que si lo fuera pasaría que $r^2+s^2 = 0$, entonces se obtendría que $r = 0\, y\, s = 0$, y como $r \equiv x(modm)$ y $s \equiv y(modm)$ entonces

$$r \equiv 0(modm), s \equiv 0(modm) \Rightarrow m|x, m|y, \Rightarrow m^2|x^2+y^2,$$

y como $mp = x^2+y^2$ de donde $m^2|mp$ por lo tanto $m|p$. Pero del lema anterior $m < p$, y por ser p primo, entonces $m = 1$, lo cual es una contradicción. Entonces $n \neq 0$, y $n \in \mathbb{Z}^+\, y\, n < m$ tal que np =suma de dos cuadrados, pero *m* es la más pequeña y *m* no es mayor que 1, por lo tanto *m* =1, y como consecuencia $p = x^2+y^2$.

Con base en los resultados anteriores observamos que los primos de las formas 4k±1 son muy distintos en sus elementos intrínsecos, es decir, mientras que unos sí se pueden representar como suma de cuadrados, otros no, además surge una duda respecto a la densidad que presenta cada grupo si se les compara entre sí. A pesar de que no se conoce exactamente una fórmula general para expresar a los primos, sí se presentan nuevos elementos que los caracterizan y que permite establecer una diferencia entre estos inquietantes números.

Los primos se autogeneran.

Las representaciones aditivas de los primos no necesariamente requieren de cuadrados, cubos u otras potencias de enteros. Los primos pueden autogenerarse hablando desde la idea de lo aditivo, y nos referimos a que un primo p_i se puede generar en términos de sumas y restas de los primos anteriores a él (se incluye al uno).

La propuesta de la autogeneración de los primos se debe a H. F. Scherk, quien en 1830[17] estableció que para cada natural $n \geq 3$, y eligiendo adecuadamente los signos + ó -, se tiene que según el orden de los primos, estos se pueden representar de la forma

$$p_{2n} = 1 \pm p_1 \pm p_2 \pm p_3 \pm \cdots \pm p_{2n-1}$$

y

$$p_{2n+1} = 1 \pm p_1 \pm p_2 \pm p_3 \pm \cdots \pm p_{2n-1} + 2p_{2n},$$

donde los subíndices establecen el orden de aparición de los primos, y lo sobresaliente es que ***todo primo se puede representar como una combinación lineal de todos los***

[17] Véase Sierpinski [1964]

primos anteriores a él, y en el caso de los primos de orden p_{2n+1} el último sumando será multiplicado por dos. Por ejemplo, supongamos que $p_1 = 2$ y $p_2 = 3$, y para $n \geq 3$ se tiene que

$$p_3 = 1- 2 + 2(3) = 5$$
$$p_4 = 1 - 2 + 3 + 5 = 7$$
$$p_5 = 1 - 2 + 3 - 5 + 2(7) = 11$$
$$p_6 = 1 + 2 - 3 - 5 + 7 +11 = 13$$

La prueba de este teorema fue publicada por S. S. Pillai en 1928 y la demostración que veremos a continuación se debe a Sierpinsky.[18] Antes de dar paso a la demostración de las fórmulas veamos un lema que será de gran utilidad para esto.

Lema.

Existen $q_1, q_2, \ldots$ una sucesión infinita de enteros, tal que para $n \geq 3$ cada entero positivo impar menor que el elemento de la sucesión q_{2n+1}, es de la forma

$$\pm q_1 \pm q_2 \pm q_3 \pm \cdots \pm q_{2n-1} + q_{2n},$$

eligiendo adecuadamente los signos correspondientes.

Demostración.

La sucesión infinita que consideramos será la de los primos. Sea ésta

$$q_1 = 2, q_2 = 3, q_3 = 5, q_4 = 7, q_5 = 11, q_6 = 13, q_7 = 17$$

y esta sucesión tiene la particularidad de que[19] $q_{n+1} < 2q_n \ldots.$ (1), para $n = 1, 2, \ldots$. Con base en esta sucesión se demostrará que existe una forma aditiva para representar a los impares usando sólo a los primos. El proceso de demostración será a través de inducción.

Veamos que para $n = 3$ en q_{2n+1}, se tiene que $q_{2(3)+1}$ = 17, y que es posible expresar a todos los impares menores a 17 como suma de los 2(3) primos menores a él. Antes recordemos que $q_1 = 2, q_2 = 3, q_3 = 5, q_4 = 7, q_5 = 11, q_6 = 13, q_7 = 17$, por lo que:

$$1 = -q_1 + q_2 + q_3 - q_4 - q_5 + q_6 \quad = -2 + 3 + 5 - 7 - 11 + 13$$
$$3 = q_1 - q_2 - q_3 + q_4 - q_5 + q_6 \quad = 2 - 3 - 5 + 7 - 11 + 13$$
$$5 = q_1 + q_2 + q_3 - q_4 - q_5 + q_6 \quad = 2 + 3 + 5 - 7 - 11 + 13$$

[18] Véase Sierpinski [1964]

[19] Este hecho se debe al postulado de Joseph Louis Bertrand, el cual establece que para todo natural mayor que 1, entre *n* y *2n* existe por lo menos un primo. De esta manera entre q_n y $2q_n$ existe por lo menos un primo; si existieran más se puede elegir al más pequeño, que en este caso sería q_{n+1}. El postulado se abordará más adelante.

$$7 = -q_1 - q_2 - q_3 - q_4 + q_5 + q_6 \quad = -2 - 3 - 5 - 7 + 11 + 13$$
$$9 = q_1 + q_2 - q_3 + q_4 - q_5 + q_6 \quad = 2 + 3 - 5 + 7 - 11 + 13$$
$$11 = q_1 - q_2 - q_3 - q_4 + q_5 + q_6 \quad = 2 - 3 - 5 - 7 + 11 + 13$$
$$13 = q_1 - q_2 + q_3 + q_4 - q_5 + q_6 \quad = 2 - 3 + 5 + 7 - 11 + 13$$
$$15 = -q_1 + q_2 + q_3 + q_4 - q_5 + q_6 \quad = -2 + 3 + 5 + 7 - 11 + 13$$
$$17 = q_1 + q_2 - q_3 - q_4 + q_5 + q_6 \quad = 2 + 3 - 5 - 7 + 11 + 13$$

Como parte del proceso de inducción supongamos ahora que el lema es verdadero para $n \geq 3$, y acto seguido consideremos a $2k - 1$ un impar menor o igual que q_{2n+3}. Recordando que de $q_{n+1} < 2q_n$ se obtiene la desigualdad $q_{2n+3} < 2q_{2n+2}$, y en consecuencia[20] $-q_{2n+2} < 2k - 1 - q_{2n+2} < q_{2n+2}$, y eligiendo de manera adecuada los signos se puede llegar a que

$$0 \leq \pm 2k \pm 1 \pm q_{2n+2} < q_{2n+2}. \qquad (2)$$

Hagamos una pausa en la demostración y puntualicemos que el objetivo final es mostrar que si ya es posible escribir al impar $2k - 1$ con sumas y restas de los primeros $2n$ primos (por el paso anterior de la inducción), es decir, $\pm q_1 \pm q_2 \pm q_3 \pm \cdots \pm q_{2n}$, entonces será posible hacerlo de la misma manera pero con los primeros 2(n + 1) primos.

Siguiendo con la demostración, (1) se usa nuevamente de manera semejante para mostrar que $q_{2n+2} < 2q_{2n+1}$ y retomando (2) se le resta q_{2n+1} para obtener

$$-q_{2n+1} \leq \pm 2k \pm 1 \pm q_{2n+2} - q_{2n+1} < q_{2n+2} - q_{2n+1}, \qquad (3)$$

y de la desigualdad anterior se tiene que

$$q_{2n+2} - q_{2n+1} < 2q_{2n+1} - q_{2n+1} < q_{2n+1}.$$

De estas dos relaciones de desigualdades se concluye que

$$-q_{2n+1} \leq \pm 2k \pm 1 \pm q_{2n+2} - q_{2n+1} < q_{2n+1},$$

y nuevamente eligiendo adecuadamente los signos tenemos

$$0 \leq \pm 2k \pm 1 \pm q_{2n+2} \pm q_{2n+1} \leq q_{2n+1}.$$

Nótese que como cada uno de los primos es impar, entonces la suma

$$\pm 2k \pm 1 \pm q_{2n+2} \pm q_{2n+1},$$

[20] Por el postulado de Bertrand tenemos que $q_{2(n+1)+1} < 2q_{2(n+1)}$, luego por hipótesis suponemos que $2k - 1$ es un impar menor o igual que $q_{2(n+1)+1}$, y por lo tanto $0 < 2k - 1 < 2q_{2(n+1)}$, y además $-q_{2(n+1)} < 2k - 1 - q_{2(n+1)} < q_{2(n+1)}$.

es impar y menor que q_{2n+1}. Por hipótesis de inducción ya sabemos que todos los impares menores que q_{2n+1} se pueden escribir en términos de sumas y restas de los primeros $2n$ primos, es decir, $\pm q_1 \pm q_2 \pm q_3 \pm \cdots \pm q_{2n}$. Con esto tenemos que en particular $\pm 2k \pm 1 \pm q_{2n+2} \pm q_{2n+1}$ se puede escribir de esta forma, y así damos lugar a que con una elección adecuada de los signos se tiene que

$$\pm 2k \pm 1 \pm q_{2n+2} \pm q_{2n+1} = \pm q_1 \pm q_2 \pm q_3 \pm \cdots \pm q_{2n-1} + q_{2n}.$$

Por lo tanto, eligiendo el signo adecuado podemos concluir que

$$2k - 1 = \pm q_1 \pm q_2 \pm q_3 \pm \cdots \pm q_{2n} + q_{2n+1} + q_{2(n+1)}.$$

De esta manera todo impar se puede escribir como suma de primos, y con excepción del 2, como los primos son impares, entonces se tiene una forma de representarlos utilizando los primos anteriores a ellos. Sin embargo esta clasificación es muy general, por lo cual el teorema de H. F. Scherk brinda la oportunidad de establecer una diferencia entre unos primos y otros, de acuerdo con su orden de aparición, es decir, si aparecen en orden par o impar.

Demostración del teorema de Scherk.

Para $n \geq 3$ el número $q_{2n+1} - q_{2n} - 1$ es un impar menor que q_{2n+1}, por lo tanto, aplicando el lema anterior y eligiendo el signo adecuado se concluye que

$$q_{2n+1} - q_{2n} - 1 = \pm q_1 \pm q_2 \pm q_3 \pm \cdots \pm q_{2n-1} + q_{2n},$$

de donde

$$q_{2n+1} = 1 \pm q_1 \pm q_2 \pm q_3 \pm \cdots \pm q_{2n} + q_{2n+1} + 2q_{2n}$$

Para $n = 1$ y $n = 2$ podemos realizar la operación y ver que $q_3 = 1 - q_1 + 2q_2$ y $q_5 = 1 - q_1 + q_2 - q_3 + 2q_4$, con lo cual la fórmula queda demostrada para estos números.

Por otro lado, como $q_{2n+2} < 2q_{2n+1}$ y además $q_{2n+2} - q_{2n+1} < q_{2n+1}$, entonces se tiene que $q_{2n+2} - q_{2n+1} - 1$ es un impar menor que q_{2n+1}. De esta manera, usando el lema anterior para $n \geq 3$, y eligiendo correctamente los signos se tiene

$$q_{2n+2} - q_{2n+1} - 1 = \pm q_1 \pm q_2 \pm q_3 \pm \cdots \pm q_{2n} + q_{2n+1} + q_{2n},$$

de donde

$$q_{2n+2} = 1 \pm q_1 \pm q_2 \pm q_3 \pm \cdots \pm q_{2n} + q_{2n-1} + q_{2n} + q_{2n+1}.$$

Por lo tanto todos los números primos se pueden escribir de las formas

$$p_{2n} = 1 \pm p_1 \pm p_2 \pm p_3 \pm \cdots \pm p_{2n-1} \quad \text{y}$$

$$p_{2n+1} = 1 \pm p_1 \pm p_2 \pm p_3 \pm \cdots \pm p_{2n-1} + 2p_{2n}$$

respectivamente.

En conclusión, encontramos algunas maneras de diferenciar entre los primos de las formas $4k-1$ y $4k+1$, y de representarlos de manera aditiva a partir de ellos mismos. Sin embargo, aún tenemos la incógnita acerca de cómo y dónde localizamos de manera más precisa a los primos. Para aclarar algunas cuestiones sobre estos puntos en la siguiente sección analizaremos algunos intervalos y se establecerán propiedades para poder determinar si es que hay primos en ciertos intervalos.

Capítulo III

Primos en intervalos definidos.

Anteriormente se analizó un conjunto determinado de huecos –formados por enteros consecutivos compuestos- que existen entre los primos, y esto nos llevó a reflexionar sobre la posibilidad de que ellos –los primos- no fueran tan numerosos dentro de los enteros, pero se vio que esto es falso. Pero si resulta que no son tan escasos ¿entonces por qué se dificulta tanto encontrarlos? Esa es una tarea que ha atraído a muchos matemáticos de diferentes épocas. Mentes muy brillantes se aventuraron a intentar resolver este problema y quisieron hallar una fórmula que generara a todos los primos sin excepción alguna, lamentablemente ninguna de esas mentes privilegiadas tuvo éxito. Sin embargo, sí se ha avanzado mucho en conocer con muy buenas aproximaciones la cantidad de primos en intervalos definidos. En las secciones que siguen se va a intentar exhibir a los primos contenidos en intervalos previamente establecidos.

Función $\pi(x)$.

Para poder encontrar primos en ciertos intervalos primero tenemos que construir las herramientas que serán requeridas. Usaremos la notación universalmente conocida $\pi(x)$ para referirnos a la cantidad aproximada de primos menores que x.[21] Entonces nuestro objetivo será el de tratar de aproximarnos a $\pi(x)$. Esta búsqueda empezó formalmente con Euler y lo siguieron Legendre, Chevyshev, Gauss y Riemann, entre otros. Para no perdernos en el camino de la búsqueda, desde ahora anunciamos que construiremos la cota de Chevyshev para $\pi(x)$, y es la siguiente:

$$\frac{\log 2}{4} \cdot \frac{x}{\log x} < \pi(x) < 30(\log 2)\frac{x}{\log x}.$$

Es importante señalar que en la medida que crezca x la cota propuesta para $\pi(x)$ será mejor.

[21] Como ejemplo del funcionamiento de $\pi(x)$, sea $x = 10$, entonces $\pi(10) = 4$ porque los primos menores a 10 son; 2, 3, 5 y 7. Ahora sea $x = 25$, por lo tanto $\pi(x) = 9$, ya que los primos menores a 25 son; 2, 3, 5, 7, 11, 13, 17, 19 y 23.

Para obtener las desigualdades de Chevyshev tenemos que construir cierto andamiaje, y esto se hará paso a paso. Para nuestro trabajo el primer escalón será probar que $\frac{\pi(x)}{x} \leq \frac{\phi(k)}{k} + \frac{2k}{x}$, y de aquí se desprenderá la interrogante sobre qué pasa con $\frac{\pi(x)}{x}$ cuando *x* tiende a infinito. Otro elemento importante que se requiere es el de conocer cómo son las potencias de los primos en la factorización de *n*! de esto se ocupa el teorema de Legendre.

Para demostrar $\frac{\pi(x)}{x} \leq \frac{\phi(k)}{k} + \frac{2k}{x}$ suponemos que $[x] = kl + r$, donde $0 \leq r < k$, $[x]$ es el mayor entero que es menor o igual que x. Por otro lado $\phi(k)$ es la función que proporciona la cantidad de primos relativos positivos menores que k.[22] Posteriormente se toma el intervalo $[1, x]$ y se divide en l conjuntos de k enteros consecutivos, además de un conjunto de r enteros $kl + 1, kl + 2, \dots, kl + r$. Por otro lado, entre los enteros $1, 2, \dots, k$ hay a lo más k primos. Posteriormente entre $k + 1, k + 2 \ \dots, 2k$, hay a lo más $\phi(k)$ primos. De manera similar en los conjuntos restantes de k enteros hay a lo más $\phi(k)$ primos. Finalmente en el conjunto de r enteros existen a lo más r primos. Como consecuencia de todo lo anterior se concluye que $\pi(x) \leq k + (l-1)\phi(k) + r$. Por otro lado, se sabe que $(l-1)k \leq x$, por lo tanto $(l-1)\phi(k) \leq \frac{x}{k}\phi(k)$ y como $r < k$ entonces $\pi(x) \leq k + (l-1)\phi(k) + r \leq \frac{x}{k}\phi(k) + 2k$, de donde $\pi(x) \leq \frac{x}{k}\phi(k) + 2k$, por lo anterior $\frac{\pi(x)}{x} \leq \frac{\phi(k)}{k} + \frac{2k}{x}$. De esta manera se ha mostrado una cota superior para $\frac{\pi(x)}{x}$, pero ¿qué sucede si se considera el $\lim_{x\to\infty} \frac{\pi(x)}{x}$?

Antes de ver qué pasa con $\lim_{x\to\infty} \frac{\pi(x)}{x}$, veamos algunos casos particulares. Sea $x = 20$, entonces $\frac{\pi(20)}{20} = \frac{8}{20} = 0.4$. Sea $x = 100$, por tanto $\frac{\pi(100)}{100} = \frac{25}{100} = 0.25$. Ahora, si $x = 1000$, entonces $\frac{\pi(1000)}{1000} = \frac{168}{1000} = 0.168$. Y si $x = 1000000000$, entonces $\frac{\pi(1000000000)}{1000000000} = \frac{50847534}{1000000000} = 0.050847534$. Hasta este punto todo parece indicar que mientras más grande es x, menor va a ser el cociente, es decir, parece que $\lim_{x\to\infty} \frac{\pi(x)}{x} = 0$. Con este razonamiento podemos pensar nuevamente que los primos en ese intervalo son escasos. Sin embargo sabemos que el conjunto de los primos es

[22] Para ejemplificar cómo funciona $\phi(k)$, sea $k = 10$, entonces $\phi(10) = 4$, pues los primos relativos menores a 10 son 1, 3, 7, 9.

infinito, y ya se comentó antes que son más abundantes de lo que parece[23]. Ahora sigamos construyendo las herramientas que permitirán encontrar primos en un intervalo.

Pasemos ahora a observar la relación que existe entre el factorial y los números primos que son factores de éste. Por ejemplo, consideremos $n = 5$, entonces $n! = 5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$, y notemos que los factores primos de 5! son 2, 3 y 5. Para saber cuántas veces aparecen estos factores, consideremos al entero que es menor o igual que $\frac{n}{p}, \frac{n}{p^2}, \frac{n}{p^3}, \ldots$ para cada uno de los primos en 5! Ahora tomemos primero al 2, entonces $\left[\frac{5}{2}\right] = 2$. Por otro lado$\left[\frac{5}{2^2}\right] = 1$, y como $2^3 > 5$, entonces $\left[\frac{5}{2^3}\right] = 0$, y esto sucede para toda $j \in \{1, 2, 3, \ldots\}$. Lo interesante aquí es ver que ya tenemos tres factores dos, es decir, el exponente del 2 en 5! es $\left[\frac{5}{2}\right] + \left[\frac{5}{2^2}\right] = 2 + 1 = 3$, es decir, el 2 en la descomposición de los primos aparece como 2^3. De manera análoga podemos ver la potencia de los otros primos en la descomposición de 5! Después de haber observado este ejemplo, podemos pasar al respectivo teorema de Lagrange.

Teorema (Lagrange).

Si p es un primo, entonces

$$\sum_{j=1}^{\infty} \left[\frac{n}{p^j}\right],$$

es el exponente de p en la factorización de $n!$

Demostración.

Si $p > n$, entonces p no aparece en la factorización de $n!$, y en consecuencia cada suma

$$\sum_{j=1}^{\infty} \left[\frac{n}{p^j}\right] \text{ es cero.}$$

Si $p \leq n$ entonces existen $\left[\frac{n}{p}\right]$ enteros entre los números $\{1, 2, \ldots, n\}$ que son divisibles por p, a saber $p, 2p, 3p, \ldots, \left[\frac{n}{p}\right]p$. De esos enteros existen $\left[\frac{n}{p^2}\right]$ que son divisibles por p^2, a saber $p^2, 2p^2, \ldots, \left[\frac{n}{p^2}\right]p^2$. De manera similar hay $\left[\frac{n}{p^3}\right]$ enteros que son divisibles por p^3, y estos son $p^3, 2p^3, \ldots, \left[\frac{n}{p^3}\right]p^3$. Después de un número finito de pasos similares encontramos que el número de veces que p divide a los enteros $\{1, 2, \ldots, n\}$ es

[23] La demostración de que $\lim_{x\to\infty} \frac{\pi(x)}{x} = 0$ se realizará en el apéndice A al final del capítulo.

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\cdots=\sum_{j=1}^{\infty}\left[\frac{n}{p^j}\right],$$

en consecuencia esta suma es el exponente de p en la factorización de $n!$

El teorema anterior será fundamental para poder determinar si existen primos dentro de un intervalo de la forma $(n, 2n)$, pero antes requerimos usar algunas propiedades de la función $f(x)=\frac{x}{\log x}$. Enseguida las enunciaremos, pero las demostraciones se pueden ver en el apéndice B al final del capítulo:

1] $f(x)$ es decreciente para $x > e$.

2] $f(x-2) > \frac{1}{2}f(x)$ para $x \geq 4$.

3] $f\left(\frac{x+2}{2}\right) < \frac{15}{16}f(x)$, para $x \geq 8$.

Estas tres propiedades junto con las que a continuación se expondrán sobre coeficiente binomial serán centrales para la aproximación que construiremos de $\pi(x)$. Así, sea el coeficiente binomial

$$\binom{2n}{n}=\frac{(2n!)}{(n!)(n!)}=\frac{2n(2n-1)\cdots(n+1)}{n(n-1)\cdots 1},$$

y consideramos p un primo que se encuentre en el intervalo $(n, 2n]$, entonces p debe aparecer en el numerador del coeficiente, pero si $p > n$ éste no aparece en el denominador. De esta manera vemos que p divide a $\binom{2n}{n}$. Ahora multipliquemos a todos los primos que aparecen en el coeficiente binomial, por lo tanto p_n divide a $\binom{2n}{n}$, donde p_n es el producto de todos los primos tales que $n < p < 2n$. Por otro lado, entre 1 y $2n$ hay $\pi(2n)$ primos; análogamente entre 1 y n existen $\pi(n)$ primos, por lo que en $\binom{2n}{n}$ hay $\pi(2n)-\pi(n)$ primos, que son los factores de p_n. Además, como $n < p$ para todo p primo que es factor de $\binom{2n}{n}$, entonces

$$n^{\pi(2n)-\pi(n)} < p_n < \binom{2n}{n}.$$

Ahora establezcamos una correspondencia con cada primo, y definamos $r_p \geq 1$ para la desigualdad $p^{r_p} \leq 2n \leq p^{r_p+1}$. Ahora es necesario conocer cuál es la potencia de cada uno de estos primos p en la factorización de $\binom{2n}{n}$. Sabemos por el teorema de Lagrange, que

$$\sum_{j=1}^{r_p}\left(\left[\frac{2n}{p^j}\right]-2\left[\frac{n}{p^j}\right]\right),$$

es el exponente buscado.

Ahora, si $[x]$ denota el entero inmediato menor o igual que x, entonces

$$0 \leq [2x]-2[x] \leq 1$$

y en consecuencia

$$0 \leq \sum_{j=1}^{r_p}\left(\left[\frac{2n}{p^j}\right]-2\left[\frac{n}{p^j}\right]\right) \leq \sum_{j=1}^{r_p} 1 = r_p\,.^{24}$$

De los últimos resultados tenemos que $\binom{2n}{n}$ divide a Q_n, donde $Q_n$es el producto de todos los primos p^{r_p}. Así, cada $p^{r_p} \leq 2n$ y Q_n tiene $\pi(2n)$ factores de la forma p^{r_p}; por lo tanto

$$\binom{2n}{n} \leq Q_n \leq (2n)^{\pi(2n)}. \qquad 1)$$

Pero recordemos que teníamos la desigualdad

$$n^{\pi(2n)-\pi(n)} < p_n < \binom{2n}{n}, \qquad 2)$$

y tanto 1) como 2) son fundamentales para llegar a las cotas de $\pi(n)$ que enuncia Chevyshev en su teorema.[25]

Del teorema del binomio tenemos que

$$(1+x)^{2n} = 1+\binom{2n}{1}x+\binom{2n}{2}x^2+\cdots+\binom{2n}{n}x^n \ldots + x^{2n},$$

y para $x = 1$

$$2^{2n} = 1+\binom{2n}{1}+\binom{2n}{2}+\cdots+\binom{2n}{n}\ldots+1 > \binom{2n}{n} > 2^n, \qquad 3)$$

en consecuencia de 1) y 3) se llega a

$$2^n \leq (2n)^{\pi(2n)}, \qquad 4)$$

y aplicando logaritmo en ambos lados de 4) se concluye que $n\log 2 \leq \pi(2n)\log 2n$. Ahora, si usamos 4) y las propiedades 1] y 2] de $f(x) = \frac{x}{\log x}$ con$x \geq 5$, entonces $\pi(x) \geq \pi\left(2\left[\frac{x}{2}\right]\right)$, y con $n = 2\left[\frac{x}{2}\right]$ y utilizando los resultado indicados arriba tenemos que

[24] Esto se deduce de las siguientes desigualdades $2x-1 \leq [2x] \leq 2x$, $2x-2 \leq 2[x] \leq 2x$.

[25]Para no perder el camino de la demostración recordemos que las cotas que propone Chevyshev para $\pi(x)$ son: $\frac{\log 2}{4}\cdot\frac{x}{\log x} < \pi(x) < 30(\log 2)\frac{x}{\log x}$.

$$\left[\frac{x}{2}\right]\log 2 \leq \pi\left(2\left[\frac{x}{2}\right]\right)\log 2\left[\frac{x}{2}\right],$$

de donde

$$\frac{\log 2}{2}\cdot\frac{2\left[\frac{x}{2}\right]}{\log 2\left[\frac{x}{2}\right]} \leq \pi\left(2\left[\frac{x}{2}\right]\right) \leq \pi(x),$$

pero

$$\frac{\log 2}{2}\cdot\frac{2\left[\frac{x}{2}\right]}{\log 2\left[\frac{x}{2}\right]} = \frac{\log 2}{2} f\left(2\left[\frac{x}{2}\right]\right) > \frac{\log 2}{2} f(x-2) > \frac{\log 2}{4} f(x),$$

en consecuencia $\pi(x) \geq \pi\left(2\left[\frac{x}{2}\right]\right) > \frac{\log 2}{4} f(x)$, por lo que $\frac{\log 2}{4}\cdot\frac{x}{\log x} < \pi(x)$. En conclusión, hemos acotado por abajo a la función $\pi(x)$, lo cual resulta muy gratificante. Sin embargo, falta acotarla por arriba para demostrar completamente el teorema de Chevyshev.

Para determinar la cota superior de $\pi(x)$ es necesario retomar 2) y 3) para obtener $n^{\pi(2n)-\pi(n)} < 2^{2n}$, y después de aplicar logaritmo en ambos lados se obtiene

$$(\pi(2n) - \pi(n))\log n < 2n \log 2,$$

de donde

$$\pi(2n) < (2\log 2)\frac{n}{\log n} + \pi(n). \qquad 5).$$

Acto seguido usamos inducción matemática para determinar que

$$\pi(2n) < 32(\log 2)\frac{n}{\log n}, \qquad \text{para } n > 1. \qquad 6).$$

La justificación de esta desigualdad la exponemos en el apéndice C al final del capítulo. Y para cada real $x \geq 8$, tenemos que

$$\pi(x) < \pi\left(2\left[\frac{x}{2}\right] + 2\right) < 32(\log 2) f\left(\left[\frac{x}{2}\right] + 1\right),$$

pero por 3] obtenemos

$$\leq 32(\log 2) f\left(\frac{x+2}{2}\right)$$

y también que

$$< 32(\log 2)\frac{15}{16} f(x) = 30\,(\log 2) f(x) = 30(\log 2)\frac{x}{\log x}.$$

Así, finalmente, hemos conseguido acotar la función $\pi(x)$, es decir, hemos llegado al siguiente resultado

$$\frac{\log 2}{4} \cdot \frac{x}{\log x} < \pi(x) < 30(\log 2)\frac{x}{\log x},$$

lo cual resulta ser el teorema de Chebyshev.

Con lo anterior ya tenemos una aproximación de cuántos primos existen en el intervalo $(1, x)$, pero también hay que recordar que existen grandes vacíos donde no hay un solo primo. Ante esta situación lo que podemos hacer es explorar dentro del intervalo, es decir, explorar en intervalos más pequeños para saber si dentro de ellos existen primos y cuándo y cómo es que se da este suceso. Lo que haremos es demostrar que, efectivamente existe por lo menos un primo en el intervalo $(n, 2n)$.

Intervalos de Bertrand y coeficientes binomiales.

En 1845 Joseph Louis Bertrand conjeturó que para toda $n \geq 2$ existe un *p* primo tal que $n \leq p \leq 2n$. El primero en demostrar este resultado fue Chebyshev en 1850 y en 1931 el húngaro Paul Erdös presentó otra demostración. La prueba de Erdös se apoya en los coeficientes binomiales, y además generalizó la conjetura para los números reales. De esta forma la conjetura establece que para todo x real tal que $x \geq 2$ existe p primo tal que $x \leq p \leq 2x$. Este resultado fue fundamental para conocer más sobre los números primos, ya que nos permite garantizar la existencia de por lo menos un primo en determinados intervalos. Pasemos a ver cuáles fueron las ideas seguidas por Erdös para demostrar el postulado de Bertrand.[26]

De manera ingeniosa Erdös tomó el coeficiente binomial $\binom{2n}{n}$ y lo acotó por ambos lados de esta manera

$$\frac{1}{2n}(2^{2n}) < \binom{2n}{n} < \frac{1}{4}(2^{2n}). \qquad 1)$$

Por otro lado, consideró un intervalo de la forma $(10, b]$ y lo cubrió con pequeños intervalos $a_m < \gamma \leq 2a_m$, tales que $a_1 = \left\lceil \frac{b}{2} \right\rceil, a_2 = \left\lceil \frac{b}{2^2} \right\rceil, \ldots, a_k = \left\lceil \frac{b}{2^k} \right\rceil$. Después expresó el producto de los primos en el intervalo $(10, b]$ en términos de los intervalos más pequeños, es decir,

$$\prod_{10<p\leq b} p \leq \prod_{a_1<p\leq 2a_1} p \prod_{a_2<p\leq 2a_2} p \ldots \prod_{a_m<p\leq 2a_m} p .$$

[26]La demostración de este hecho se puede ver de manera completa en [Maldonado, 2012]. Aquí sólo se presenta un esbozo sobre la misma, ya que estaremos más enfocados en ver la generalización del postulado de Bertrand.

Cada factor del lado derecho está acotado por el coeficiente binomial

$$\prod_{n<p\leq 2n} p < \binom{2n}{n} < 2^{2(n-1)},$$

y por lo tanto

$$\prod_{10<p\leq b} p \leq 2^{2(a_1-1+a_2-1+\cdots+a_m-1)} < 2^{2b}. \qquad 2)$$

Estos resultados nos permiten ahora analizar la desigualdad

$$\binom{2n}{n} \leq \prod_{p\leq\sqrt{2n}} p \prod_{\sqrt{2n}<p\leq\frac{2}{3}n} p \prod_{n<p\leq 2n} p,$$

y si ahora suponemos que entre n y $2n$ no existen primos, y considerando los resultados de 1) y 2), se llega a la desigualdad

$$2^{2n} < 2n^{\sqrt{2n}+1} 2^{\frac{4}{3}n}.$$

Pero esta desigualdad tiene el gran problema que para n grande no se cumple, lo cual resulta ser una contradicción. La conclusión es que existe por lo menos un primo en dicho intervalo.

Otros intervalos.

Con el conocimiento de la existencia de un primo en el intervalo $[x, 2x]$, resulta interesante saber en qué otro tipo de intervalos podemos tener certeza de que existen primos.

Hagamos un pequeño análisis. Veamos qué sucede con el intervalo del postulado de Bertrand y un intervalo de la forma $[2n, 3n]$. Sea $n \in \{1, 12\}$

(n, 2n)	**(2n, 3n)**
(2, 4)	(2, 3)
(3, 6)	(4, 6)
(4, 8)	(6, 9)
(5, 10)	(8, 12)
(6, 12)	(10, 15)
(7, 14)	(12, 18)
(8, 16)	(14, 21)
(9, 18)	(16, 24)
(10, 20)	(18, 27)
(11, 22)	(20, 30)
(12, 24)	(22, 33)

Notemos que los intervalos de la forma $[2n, 3n]$(con la n adecuada según el caso) se pueden anidar dentro de los intervalos $[n, 2n]$, por ejemplo $[4, 6] \in [4, 8]$ ó $[6, 9] \in [5, 10]$; etc. Además existen algunos intervalos $[2n, 3n]$ que caben perfectamente en dos de la forma $[n, 2n]$; sin embargo, no se puede afirmar con ello que en $[2n, 3n]$ se encuentre un primo.

Primos en el intervalo $[2n, 3n]$.

Después del breve ejemplo de los intervalos $[2n, 3n]$ y $[n, 2n]$, no resulta difícil ver que al menos para $n \in \{1, 12\}$ sí hay por lo menos un primo en $[2n, 3n]$. Lo que probaremos es que sí existe por lo menos un primo en todos estos intervalos. Pero antes de realizar tal demostración se requieren dos lemas que a continuación enunciamos. Para la demostración ver [Barchraoui, 2006].

Lema 1.

- Si n es par entonces $\binom{\frac{3n}{2}}{n} < \sqrt{6.75}^n$.
- Si n es par tal que $n > 152$ entonces $\binom{\frac{3n}{2}}{n} < \sqrt{6.5}^n$.
- Si n es impar y $n > 7$ entonces $\binom{\frac{3n+1}{2}}{n} < \sqrt{6.75}^{n-1}$.
- Si $n > 945$ entonces $\left(\frac{6.5}{\sqrt{27}}\right)^n > (3n)^{\frac{\sqrt{3n}}{2}}$.

Lema 2.

a. Si n es par, entonces

$$\prod_{\frac{n}{2}<p<\frac{3n}{4}} p \cdot \prod_{n<p<\frac{3n}{2}} p < \binom{\frac{3n}{2}}{n}.$$

b. Si n es impar entonces

$$\prod_{\frac{n+1}{2}<p<\frac{3n}{4}} p \cdot \prod_{n<p<\frac{3n+1}{2}} p < \binom{\frac{3n+1}{2}}{n}.$$

Teorema.

Para cualquier entero positivo $n > 1$ existe un número primo entre $2n$ y $3n$.

Demostración.

Sea $n > 945$. Tenemos entonces que $\binom{3n}{2n} = \frac{(2n+1)(2n+2)\cdots 3n}{1\cdot 2\cdot 3\cdots n}$; en consecuencia el producto de los primos entre $2n$ y $3n$ divide a $\binom{3n}{2n}$. Por lo tanto usaremos la siguiente notación

$$T_1 = \prod_{P\leq\sqrt{3n}} P^{\beta(P)}, \qquad T_2 = \prod_{\sqrt{3n}<P\leq 2n} P^{\beta(P)}, \qquad T_3 = \prod_{2n+1\leq P\leq 3n} P^{\beta(P)},$$

por lo que

$$\binom{3n}{2n} = T_1T_2T_3 \qquad \text{(a).}$$

Tenemos ahora que por la descomposición en primos de $\binom{3n}{2n}$ los exponentes en T_2 son menores que 2 por la descomposición en primos de $\binom{n}{j}$. Además si p satisface

$$\frac{3n}{4} < p \leq n,$$

entonces el exponente es cero. Claramente, bajo esta condición, p aparece en el denominador de $\binom{3n}{2n}$; sin embargo, no aparece $2p$, y $3p$ aparece en el numerador, mientras que $4p$ no lo hace. Por otro lado, si $\frac{3n}{2} < p \leq 2n$, entonces los exponentes en T_2 son cero porque esos primos no aparecen en el numerador ni el denominador del coeficiente binomial, esto porque $2p > 3n$. Después, por el lema 2 y por el hecho de que $\prod_{p\leq x} P < 4^x$, tenemos lo siguiente:

- Si n es par entonces

$$T_2 < \prod_{\sqrt{3n}P\leq\frac{n}{2}} P \cdot \prod_{\frac{n}{2}<P\leq\frac{3n}{4}} P \cdot \prod_{n\leq P\leq\frac{3n}{2}} P$$

$$< 4^{\frac{n}{2}}\binom{\frac{3n}{2}}{n} < 4^{\frac{n}{2}}(6.75)^{\frac{n}{2}} = \sqrt{27}^n.$$

- Si n es impar entonces

$$T_2 < \prod_{\sqrt{3n}P\leq\frac{n+1}{2}} P \cdot \prod_{\frac{n+1}{2}<P\leq\frac{3n}{4}} P \cdot \prod_{n\leq P\leq\frac{3n+1}{2}} P$$

$$< 4^{\frac{n+1}{2}}\binom{\frac{3n+1}{2}}{n} < 4^{\frac{n+1}{2}}(6.75)^{\frac{n-1}{2}} = 4\cdot\sqrt{27}^{n-1} < \sqrt{27}^n.$$

Por ambos resultados concluimos que $T_2 < \sqrt{27}^n$. Por otro lado la descomposición en primos de $\binom{3n}{2n}$ proporciona la cota para $T_1 < (3n)^{\pi(\sqrt{3n})}$. Ahora, por el lema 2, la igualdad (a) y las desigualdades anteriores, encontramos que

$$(6.5)^n < T_1 T_2 T_3 < (3n)^{\pi(\sqrt{3n})} \sqrt{27}^n T_3,$$

lo cual implica que

$$T_3 > \left(\frac{6.5}{\sqrt{27}}\right)^n \frac{1}{(3n)^{\pi(\sqrt{3n})}},$$

pero tenemos que $\pi(\sqrt{3n}) \leq \frac{\sqrt{3n}}{2}$, y en consecuencia

$$T_3 > \left(\frac{6.5}{\sqrt{27}}\right)^n \frac{1}{(3n)^{\frac{\sqrt{3n}}{2}}} > 1.$$

De esto concluimos que el producto T_3 de primos entre $2n$ y $3n$ es mayor que 1, por lo tanto existe por lo menos un primo en dicho intervalo.

Después de haber demostrado que en dos tipos distintos de intervalos se encuentra por lo menos un primo, resultaría importante saber si existen otros tipos de intervalos que contengan por lo menos un primo, y si es que existen ¿cómo o qué condiciones deben satisfacer para que se cumpla tal característica?

Generalización del teorema de Bertrand-Chebyshev.

En matemáticas siempre se busca generalizar las ideas, de tal manera que éstas abarquen el mayor número, sino es que el total, de todos los casos posibles para un suceso, y el teorema de Bertrand-Chebyshev no fue la excepción. La generalización establece que para cada entero $n > 1$ y un entero fijo $k \leq n$ existe un numero primo entre kn y $(k+1)n$. Esta afirmación fue probada por Bachraoui para $k = 2$, quien se dio cuenta que si $k = n$ la respuesta podría servir para probar la existencia de un primo entre n^2 y $(n+1)^2$, que resulta ser la conjetura de Legendre. La prueba de esta generalización fue realizada por Shiva Kintali, quien determinó explícitamente el número N_k tal que para todo $n \geq N_k$ existe al menos un primo entre kn y $(k+1)n$; pero además de determinar tal número, ofrece también la generalización de la prueba de Erdös del teorema de Bertrand-Chebyshev, la cual también recurre a la combinatoria para poder determinar

ese hecho. Antes de llegar a la demostración del teorema veamos algunos lemas que nos servirán para ello.

Lema 1.

1. Si $k|n$ entonces

$$\binom{\frac{(k+1)n}{k}}{n} < \left(\frac{(k+1)^{(k+1)}}{k^k}\right)^{\frac{n}{k}}.$$

2. Si $k|(n+l), 0 < l < k$ y $n > (k+1)^k$ entonces

$$\binom{\frac{(k+1)n+l}{k}}{n} < \left(\frac{(k+1)^{(k+1)}}{k^k}\right)^{\frac{n+l}{k}}.$$

Demostración.

Sea $l = 0$ y usemos inducción sobre n. Supongamos que se cumple para $n = k$, entonces $\binom{k+1}{k} < \frac{(k+1)^{(k+1)}}{k^k}$.

P. d. Para $k+1$

Sea la desigualdad válida para $\binom{(k+1)n}{kn}$.

En consecuencia $\binom{(k+1)n+(k+1)}{kn+k} = \binom{(k+1)n}{kn} \frac{(k+1)((k+1)n+1)\cdots((k+1)n+k)}{(kn+1)\cdots(kn+k)}$, y comparando los coeficientes de n^k y n^{k-1} en el numerador y denominador, tenemos que para toda $n > k$

$$\frac{(k+1)((k+1)n+1)\cdots((k+1)n+k)}{(kn+1)\cdots(kn+k)} < \frac{(k+1)^{(k+1)}}{k^k}$$

Lema 2.

Si $k|n$ y $n \geq k(k+1)^{(k+1)}$ entonces $\binom{\frac{(k+1)n}{k}}{n} > \left(\frac{(k+1)^{(k+1)}-1}{k^k}\right)^{\frac{n}{k}}$.

Demostración.

Sea $n = k(k+1)^{(k+1)}$. Sea

$$S_k = \sum_{i=1}^{k} i.$$

Llevando a cabo un proceso similar a la demostración anterior y comparando los coeficientes de n^k y n^{k-1} en el denominador y numerador, tenemos que para toda n tal que

$$nk^k > S_k(k^{k-1}((k+1)^{k+1}-1) - k^k(k+1)^k,$$

resulta que

$$\frac{(k+1)((k+1)n+1)\cdots((k+1)n+k)}{(kn+1)\cdots(kn+k)} > \frac{(k+1)^{(k+1)}-1}{k^k}$$

Lema 3.

1. Sea $N_k = k(k+1)^{2k+2}$.

2. Si $n > N_k$ y $k > 1$ entonces $\left(\frac{(k+1)^{(k+1)}-1}{k^k}\right)^n \left(\frac{1}{(k+1)^{(k+1)}}\right)^{\frac{n}{k}} > ((k+1)n)^{\frac{\sqrt{(k+1)n}}{k}}$.

Demostración.

Como la función $\frac{\ln((k+1)x)}{\sqrt{x}}$ es decreciente, y tomando como válida la desigualdad para $n = N_k$, tenemos que $\frac{k}{\sqrt{(k+1)}} ln\left(\left(\frac{(k+1)^{(k+1)}-1}{k^k}\right)\left(\frac{1}{(k+1)^{(k+1)}}\right)^{\frac{1}{k}}\right) > \frac{\ln((k+1)n)}{\sqrt{n}}$, de donde finalmente se concluye que $\left(\frac{(k+1)^{(k+1)}-1}{k^k}\right)^n \left(\frac{1}{(k+1)^{(k+1)}}\right)^{\frac{n}{k}} > ((k+1)n)^{\frac{\sqrt{(k+1)n}}{k}}$.

Lema 4.

Sea la función:

$$\phi(a,b) = \prod_{a<p\leq b} p$$

1. Si $k|n$ entonces

$$\phi\left(\frac{n}{k}, \frac{(k+1)n}{(k+2)}\right)\phi\left(n, \frac{(k+1)n}{k}\right) < \binom{(k+1)n}{n}.$$

2. Si $k|(n+l), 0 < l < k$ entonces

$$\phi\left(\frac{n+l}{k}, \frac{(k+1)n}{(k+2)}\right)\phi\left(n, \frac{(k+1)n+l}{k}\right) < \binom{(k+1)n+l}{n}.$$

Demostración.

La demostración se realizará para $l = 0$.

Tenemos que $\binom{(k+1)n}{n} = \frac{(n+1)\cdots\frac{(k+1)n}{k}}{\frac{n}{k}!}$... (1) Entonces sabemos que $\phi\left(n, \frac{(k+1)n}{k}\right)$ divide a $\binom{(k+1)n}{n}$. Si $\frac{n}{k} < p \leq \frac{(k+1)n}{(k+2)}$ notemos que kp aparece en el numerador de (1), pero no en el denominador. Después de simplificar kp con algún número de la forma αk del denominador, podemos tomar el factor primo p en $\binom{(k+1)n}{n}$. Por lo tanto $\phi\left(\frac{n}{k}, \frac{(k+1)n}{(k+2)}\right)$ divide a $\binom{(k+1)n}{n}$.

Teorema.

Para cada entero $1 < k < n$ existe un número N_k tal que para todo $n \geq N_k$ existe al menos un primo entre kn y $(k+1)n$.

Demostración.

El producto de primos entre kn y $(k+1)n$ divide a $\binom{(k+1)n}{kn}$. Ahora fijemos un primo y sea $\beta(p)$ el número x más grande tal que p^x divide a $\binom{(k+1)n}{kn}$. Sea $\binom{(k+1)n}{kn} = P_1 P_2 P_3$, con

$$P_1 = \prod_{p \leq \sqrt{(k+1)n}} p^{\beta(p)},$$

$$P_2 = \prod_{\sqrt{(k+1)n} < p \leq kn} p^{\beta(p)},$$

$$P_3 = \prod_{kn+1 < p \leq (k+1)n} p^{\beta(p)}.$$

Tenemos que $p_1 < \left((k+1)n\right)^{\pi\left(\sqrt{(k+1)n}\right)}$. Posteriormente, por el lema 1, tenemos $P_2 < ((k+1)^{(k+1)})^{\frac{n}{k}}$, y por los lemas anteriores resulta que:

$$\left(\frac{(k+1)^{(k+1)}-1}{k^k}\right)^n < P_1 P_2 P_3 < \left((k+1)n\right)^{\pi\left(\sqrt{(k+1)n}\right)} ((k+1)^{(k+1)})^{\frac{n}{k}} P_3.$$

Y usando el lema y el hecho de que $\pi\left(\sqrt{(k+1)n}\right) \leq \frac{\sqrt{(k+1)n}}{2}$ entonces llegamos a

$$P_3 > \left(\frac{(k+1)^{(k+1)}-1}{k^k}\right)^n \left(\frac{1}{(k+1)^{(k+1)}}\right)^{\frac{n}{k}} \frac{1}{((k+1)n)^{\pi\left(\sqrt{(k+1)n}\right)}} > 1$$

por lo tanto $P_3 > 1$ y en consecuencia existe por lo menos un primo en P_3.

Apéndice A.

Teorema.

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

Demostración.

Sea *M* un entero "grande", y sea $k = p_1 p_2 \dots p_s$, donde $\{p_1, p_2, \dots p_s\}$ es el conjunto de todos los primos que no exceden a *M*. Entonces

$$\frac{\phi(k)}{k} = \frac{k\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_s}\right)}{k} =$$

$$\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_s}\right) < \left(\sum_{n=1}^{M}\frac{1}{n}\right)^{-1},$$

por lo tanto

$$\frac{\pi(x)}{x} \leq \left(\sum_{n=1}^{M}\frac{1}{n}\right)^{-1} + \frac{2p_1 p_2 \dots p_s}{x},$$

además, como la serie

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

es divergente podemos elegir *M*, suficientemente grande, tal que

$$\sum_{n=1}^{M}\frac{1}{n} > \frac{2}{\epsilon},$$

donde $\epsilon > 0$. De esta manera tenemos que para $x > \frac{4p_2 \dots p_s}{\epsilon}$, entonces

$$\frac{\pi(x)}{x} < \frac{\epsilon}{2} + \frac{2p_1 p_2 \dots p_s \epsilon}{2p_1 p_2 \dots p_s} = \epsilon.$$

Por lo tanto $\lim_{x\to\infty} \frac{\pi(x)}{x} = 0$.

Apéndice B.

Sobre la función $f(x) = \frac{x}{\log x}$.

1) Se trabaja con la derivada de $f(x)$, es decir $f'(x) = \frac{logx-1}{(logx)^2} > 0$, para $x > e$.
2) Para poder ver esto con claridad es importante notar que si $x \geq 4$, entonces $x - 2 \geq \frac{x}{2}$, de donde

$$\frac{x-2}{\log(x-2)} \geq \frac{x}{2\log(x-2)}.$$

Por otra parte tenemos que $x > x - 2$, y tomando logaritmo en ambos lados $logx > log(x-2)$, posteriormente

$$\frac{1}{logx} < \frac{1}{log(x-2)},$$

por lo tanto concluimos que

$$f(x-2) = \frac{x-2}{\log(x-2)} \geq \frac{x}{2\log(x-2)} > \frac{x}{2logx} = \frac{1}{2}f(x)$$

en consecuencia $f(x-2) > \frac{1}{2}f(x)$.

3) Como $x \geq 8$, entonces $\frac{x}{2} \geq x^{2/3}$ y $x + 2 \leq \frac{5x}{4}$. Tomando la primer desigualdad y aplicando logaritmo concluimos que

$$\frac{1}{log\frac{x}{2}} \leq \frac{1}{logx^{2/3}}$$

Posteriormente tenemos que

$$f\left(\frac{x+2}{2}\right) < \frac{x+2}{2\log\left(\frac{x}{2}\right)} \leq \frac{x+2}{2logx^{2/3}} \leq \frac{5x/4}{\frac{4logx}{3}} = \frac{15}{16}f(x),$$

por lo tanto

$$f\left(\frac{x+2}{2}\right) < \frac{15}{16}f(x).$$

Apéndice C.

Para demostrar que $\pi(2n) < 32(\log 2)\frac{n}{\log n}$ para toda $n > 1$, la demostración se lleva a cabo por inducción.

Demostración.

Notemos primeramente que $\pi(2n) < 32(\log 2)\frac{n}{\log n}$ …. (1) es válida para $2 \leq n \leq 8$, ya que

$$\pi(4) = 2 < \pi(6) = 3 < \pi(8) = 4 = \pi(10) = 4$$

$$< \pi(12) = 5 < \pi(14) = 6 = \pi(16) = 6 < 64 = 32(\log 2)\frac{2}{\log 2}.$$

Ahora supongamos que (1) se cumple para todo $n \leq k$ donde $k \geq 8$, entonces de 5) y ya que con $f(x) = \frac{x}{\log x}$, por lo tanto tenemos que

$$\pi(2k+2) < 2(\log 2)f(k+1) + \pi(k+1)$$

$$\leq 2\,(\log 2)f(k+1) + \pi\left(2\left[\frac{k+2}{2}\right]\right).$$

Por el apéndice B se tiene

$$2\,(\log 2)f(k+1) + \pi\left(2\left[\frac{k+2}{2}\right]\right) < 2\,(\log 2)f(k+1) + 32\,(\log 2)f\left(\left[\frac{k+2}{2}\right]\right).$$

Y quitando la parte entera

$$2\,(\log 2)f(k+1) + 32\,(\log 2)f\left(\left[\frac{k+2}{2}\right]\right) \leq 2\,(\log 2)f(k+1) + 32\,(\log 2)f\left(\frac{k+2}{2}\right)$$

y por el apéndice B

$$2\,(\log 2)f(k+1) + 32\,(\log 2)f\left(\frac{k+2}{2}\right) <$$

$$< 2\,(\log 2)f(k+1) + 32(\log 2)\frac{15}{16}f(k+1)$$

$$= 32(\log 2)f(k+1) = 32(\log 2)\frac{k+1}{\log(k+1)}.$$

Por tanto

$$\pi(2n) < 32(\log 2)\frac{n}{\log n}\ \forall\, n > 1.$$

Capitulo IV

Gemelos, trillizos y más…

No dejamos de sorprendernos al ver que los primos siguen apareciendo de manera controlada en ciertos intervalos, y aunque podemos pensar que cada vez están más distantes entre ellos -a pesar de que no son tan escasos-, resulta que nuevamente nos tienen reservado un resultado que no podemos dejar de lado, y nos referimos a los primos gemelos.

En este contexto tenemos una conjetura interesante y que ha dado lugar a múltiples resultados. Estos números deben su nombre a Paul Gustav Samuel Stäckel (1862-1919), aunque antes de llamarse así, eran conocidos como primos pares, dado que su diferencia es 2. Matemáticamente los primos gemelos son parejas de primos de la forma $p, p+2$; los primeros pares de estos primos son:

(3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73), (101, 103), etc.

Con el estudio de los primos gemelos se han obtenido diversos resultados de gran importancia. Primeramente recordemos que todos los primos con excepción del 2 y del 3 se pueden escribir en la forma $6k-1$ y $6k+1$, por ejemplo $5 = 6(1)-1$, $7 = 6(1)+1$, etc.

Es interesante el que ambos conjuntos de primos sean infinitos y que además los primos gemelos, excluyendo a $(3,5)$, se pueden escribir de las formas $6k-1$ y $6k+1$, y sumado a este hecho $(6k+1)-(6k-1) = 2$. Dado este resultado se podría llegar a pensar que los primos gemelos son infinitos. Sin embargo, en 1919 Viggo Brun en su artículo: *La série* $\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{29}+\frac{1}{31}+\frac{1}{41}+\frac{1}{43}+\frac{1}{59}+\frac{1}{61}+\cdots$ *où les dénominateurs sont « nombres premiers jumeaux est convergente ou finie*, demostró que la serie $\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{29}+\frac{1}{31}+\frac{1}{41}+\frac{1}{43}+\frac{1}{59}+\frac{1}{61}+\cdots$ es convergente, con lo cual genera la incertidumbre de que tales números sean infinitos, es decir, como la serie converge entonces tenemos elementos que nos hacen pensar que las parejas de primos gemelos son escasos. El número al cual converge es conocido como la constante de Brun. Thomas Nicely estimó dicha constante como $1{,}902160578$; sin embargo, la mejor estimación fue realizada en 2002 por Pascal Sebah en $1{,}902160583104$. Tal ha

sido el impacto que estos números causaron que en 1849 Alphonse de Polignac expresó la conjetura general sobre la diferencia de dos números primos consecutivos, y que afirma: "existe una cantidad infinita de números tales que todo número par se puede expresar como la diferencia de dos números primos." Desafortunadamente, esta conjetura tampoco ha sido demostrada. No obstante, en 1949, Clement publicó un artículo con el título *Congruences for sets of primes*, donde con ayuda de congruencias demostró cuándo dos números n y $n+2$ son primos. Veamos el teorema.

Teorema.

Sea $n > 1$ un entero. Los enteros n y $n+2$ son primos si y sólo si

$$4[(n-1)!+1]+n \equiv 0 \; mod \; n(n+2).$$

Demostración.

Sean n y $n+2$ primos. Por el teorema de Wilson[27] tenemos

$$(n-1)!+1 \equiv 0 \; mod \; (n) \qquad \text{(a)}$$

$$(n+1)!+1 \equiv 0 \; mod \; (n+2). \qquad \text{(b)}$$

Por otro lado $4[(n-1)!+1]+n \equiv 4 \cdot 0 + n \equiv 0(mod\; n)$. Posteriormente reduciendo el factorial de (b) $mod\; (n+2)$, tenemos $2[(n-1)!]+1 \equiv 0 \; mod \; (n+2)$ y por lo tanto

$$4[(n-1)!+1]+n \equiv 2\big[2\big((n-1)!\big)+2\big]+n$$

$$\equiv 2\big[2\big((n-1)!\big)+1+1\big]+n \equiv 2(1)+n \equiv 0 \; mod \; (n+2)$$

Finalmente, por el teorema chino[28] del residuo, obtenemos la congruencia deseada.

Supongamos ahora que $4[(n-1)!+1]+n \equiv 0 \; mod \; n(n+2)$ y demostremos que n y $n+2$ son primos. Si n no es primo entonces $(n-1)! \equiv 0 \; mod \; n$, por lo tanto

$$4[(n-1)!+1]+n \equiv 4+n \equiv 4 \; mod \; n,$$

y en consecuencia $n|4$, por lo que $n \leq 4$, lo cual es una contradicción y por lo tanto n debe ser primo. Por otro lado, si $n+2$ no es primo, tenemos que

$$(n+1)! \equiv 0 \; mod \; (n+2),$$

y por ende

$$4[(n-1)!+1]+n \equiv 2[(n+1)!+2]+n \; \equiv n+4 \equiv 2 \; mod \; (n+2)$$

[27] Si p es primo entonces $(p-1)! \equiv -1(modp)$

[28] El sistema lineal de congruencias $x \equiv a_i(modm_i)$, donde los módulos son primos relativos dos a dos y $1 \leq i \leq k$ tienen una única solución modulo $m_1 m_2 \ldots m_k$

de donde $(n+2)$ divide a 2, es decir $n \leq 0$ lo cual es una contradicción, por lo que $n+2$ es primo.

Por lo menos con esta demostración ya sabemos cuándo dos números son primos gemelos, pero ¿sólo habrá parejas?, es decir, ¿habrá tercias o cuartetas de características similares a los primos gemelos? En el mismo artículo de 1949, Clement demostró las condiciones necesarias y suficientes para tercias y cuartetas de primos. La idea es análoga a la de los primos gemelos, es decir, se basa en la congruencia de números. De esta manera tres enteros $n, n+2$ y $n+6$ son una tripleta de primos si y sólo si $4320\big[4\big((n-1)!+1\big)+n\big]+361n(n+2) \equiv 0\ mod\ n(n+2)(n+6)$.

La demostración es análoga a la de los primos gemelos. Para las cuartetas, Clement definió las funciones $P_2(n) = 4P_1(n) + n$, donde

$$P_1 \equiv (n-1)!+1$$

y

$$P_3(n) = 4320P_2(n) + 361n(n+2).$$

De esta manera los enteros $n, n+2, n+6$ y $n+8$ son una cuarteta de primos que consiste de dos conjuntos de primos gemelos, si y sólo si

$$P_4 \equiv 0\ mod\ n(n+2)(n+6)(n+8)$$

y

$$P_4 = 224P_3(n) + 111n(n+2)(n+6)$$

Es interesante hacer notar que para las tercias de números primos consecutivos existe otra clase que está dada por $n, n+4$ y $n+6$. Además se puede formar una 6-tupla, 8-tupla y k-tupla, es decir, 6, 8 y k números primos consecutivos. Además de esto existe la generalización del teorema de Clement, el cual establece que dados $n, k > 1$, los enteros n y $n+2k$ son parejas de primos si y sólo si n no tienen divisores primos propios menores que $2k$ y $2k(2k)!\,[(n-1)!+1]+[(2k)!-1]n \equiv 0\ mod\ n(n+2k)$ donde si $k = 1$ entonces tenemos el teorema de Clement.

Ya conocemos qué características deben tener dos números para que sean primos gemelos, pero esto no es todo en el estudio de estos números. Recordemos que anteriormente con los primos se utilizó la función $\pi(x)$. Pero también se tiene la analogía con una función $\pi_2(x)$ cuyo resultado es el número de primos gemelos

menores que x. Brun demostró que $\pi_2(x) = O\left(\frac{x}{log^2 x}\right)$, y posteriormente Hardy y Littlewood probaron que $\pi_2(x) \sim C\left(\frac{x}{log^2 x}\right)$ donde $C = 2\prod_{p>2}\left(1 - \frac{1}{(p-1)^2}\right) = 1.32032\ldots$

Conclusión.

Una de las conclusiones es que los números primos pueden llegar a confundir a nuestra imaginación: por un lado nuestra intuición nos indica que los primos se apegan a cierto comportamiento, pero después de hacer el trabajo formal apoyado en las demostraciones, nos percatamos que no estamos en lo correcto, y es cuando identificamos que se tienden puentes inesperados donde los primos –que aparentemente son impredecibles- son la estructura principal.

Por otro lado, parecía que no podíamos decir nada respecto a cómo se distribuyen los primos pero, finalmente, concluimos que sí podemos tener intervalos controlados donde existe por lo menos un primo. Por ejemplo, el postulado de Bertrand y sus derivados nos proporcionan esta información. También podemos identificar grupos de enteros que incluyen conjuntos infinitos de primos, y entonces resulta que sí conocemos bastante sobre el comportamiento de estos números.

A pesar de que los primos han sido estudiados por siglos, éstos tienen todavía muchas sorpresas que ofrecer, siendo un tema que aún no se agota ya que existen muchos posibles resultados que no han sido demostrados. Todo parece indicar que falta mucho para que llegue tal día.

Bibliografía.

Andrews, George. 1971. *Number Theory*. USA. Sanders company.

Aristóteles. 2000. *Metafísica*. Barcelona: Ed. Gredos.

Brun,V. "Le cribe d' Eratosthene et le theorem de Goldbach" *Videskapsselskapets Skrifter Matematisk Naturvidenskabeling Klase*, 1920, no. 3. 77-110.

Clement, P. A. "Congruences for Sets of Primes". *The American Mathematical Monthly*, Vol. 56, No. 1, 1949, pp. 23-25.

Dunham Williams. 2000. *Euler. El maestro de todos los matemáticos.* Madrid: Nivola.

Euclides. 1994. *Elementos*. Libros V-IX. Traducción y notas: M. Luisa Puerta. No. de colección: 191. Madrid: Gredos.

Golomb, Solomon W. "The Twin Prime Constant Source". *The American Mathematical Monthly*, Vol. 67, No. 8, 1960 pp. 767-769.

Koshy, Thomas. 2007. *Elementary number theory with applications*. USA. Academic Press Publication.

M. El Bachraoui. "Primes in the interval [2n,3n]". *J. Contemp. Math. Sciences*, Vol. 1, 2006, no. 13, 617-621.

Maldonado, Cortez Perla. 2012. Primos en intervalos definidos. El caso Bertrand Chebyshev. Tesis UNAM.

Niven, Ivan. "A Proof of the Divergence of σ 1/p Source". *The American Mathematical Monthly*, Vol. 78, No. 3, 1971, pp. 272-273.

Puig, Andrés. 1672. *Aritmética especulativa y practica y arte de algebra.* Barcelona.

Reid, Constance. 2008. "Del cero al infinito. Porque son interesantes los números". México. Consejo nacional para la cultura y las artes.

Shiva Kintali, *A Generalization of Erdos's Proof of Bertrand-Chebyshev Theorem*. http://www.cs.princeton.edu/ kintali, 2008.

Sierpinski, W. 1964. *Elementary theory of numbers*. Polonia. Elsevier Science Publishers B.V.

Tartaglia, Nicolo. , 1543. *Euclide Megarense Philosophosolo introduttore delle Scientie Mathematice diligentemente reassettato, et alla integrita rodotto per il degno Professore di tal Scientiae Nicolo Tartalea*, Brisciano, Venezia.

Tartaglia, Niccolo y Ferrari, Ludovico. 1974. *Cartelli di sfidamatematica*. Bresia, Italia. Ateneo di Bresia.

Tattersal, James J. 2005. *Elementary Number Theory in Nine Chapters*. USA. Cambridge University Press.