Revista de Educación Matemática
Volumen 32, N° 3 (2017), páginas 29 – 36
Unión Matemática Argentina - Famaf (UNC)

NÚMEROS PRIMOS: UNA HISTORIA SIN FIN

Eugenia Bernaschini

Sutilmente escondidos en la infinitud de los números enteros se encuentran unos peculiares numerillos que han movilizado el desarrollo de la matemática por siglos. Su peculiaridad radica en la capacidad que tienen de generar todos y cada uno de los números enteros. Son como las "partículas elementales"de la matemática. Son los *números primos*.

§1. El comienzo de esta historia: Euclides y los Elementos

Euclides fue un célebre matemático griego que vivió durante los años 325 – 265 a.C. Se lo conoce como *El Padre de la Geometría*, y se le atribuye la autoría de una famosa obra, titulada *Elementos*, que recopila gran parte del saber matemático de la época.

Figura 1. Euclides, dibujo en grafito sobre papel de la autora del artículo

Dicha obra es un tratado que consta de trece volúmenes en los cuales se presentan y se desarrollan, de manera sistemática y formal, conceptos de geometría del plano, geometría de los objetos sólidos y algunos resultados de lo que hoy se conoce como Teoría de Números.

Después de la Biblia, los Elementos es el libro con mayor cantidad de ediciones publicadas en la historia [2]. Incluso hoy en día algunas universidades lo siguen utilizando como bibliografía para sus cursos de geometría. Sin lugar a duda, es uno de los tratados más importantes de la historia de la disciplina, y es en donde se aprecia por primera vez el surgimiento de una matemática deductiva y analítica, que busca las verdades universales.

En uno de los tantos tomos de los Elementos, Euclides introduce un tipo especial de números, los *números primos*:

> Un *número primo* es el medido por la sola unidad [1].

En términos modernos, un número primo es un número natural distinto de 1 que sólo es divisible por 1, -1, por sí mismo y por su opuesto. Por ejemplo, 5 es un número primo, pues sólo es divisible por 1, -1, 5 y -5; en cambio 6 no es un número primo, ya que además de ser divisible por 1, -1, 6 y -6, es divisible por 2 y -2. A los números que no son primos se los llama *números compuestos.*

Los números primos son los bloques constitutivos de los números enteros. Esto quiere decir que todo número entero distinto de 0, 1 y -1 se factoriza de forma única como producto de números primos, por ejemplo $440 = 2^3 \cdot 5 \cdot 11$, donde 2, 5 y 11 son números primos. Este hecho se conoce en matemática como *El Teorema fundamental de la Aritmética*, y fue Euclides quien lo demostró por primera vez.

Otra característica importante de los números primos es que existen infinitos de ellos. A estas alturas no creo sorprender al lector al decir que Euclides ya estaba al tanto de este fenómeno, y su demostración va más o menos como sigue:

> *Supongamos que hay una cantidad finita de números primos, y que todos ellos son* $p_1, p_2, \ldots, p_n$. *Sea*
>
> $$r = p_1 \cdot p_2 \cdots p_n + 1.$$
>
> *Como* r *es un número entero mayor que* 1, *el Teorema Fundamental de la Aritmética (mencionado más arriba) nos permite afirmar que existe un primo* p *que divide a* r. *Como* $p_1, p_2, \ldots, p_n$ *son los únicos primos que existen,* $p = p_j$ *para algún* j *entre* 1 *y* n, *luego* p *divide a* $p_1 \cdot p_2 \cdots p_n$. *Pero como* p *también divide a* r, *entonces* p *divide a* 1, *lo que es un absurdo.* □

§2. Primalidad

Determinar si un cierto número es primo o compuesto se denomina *problema de primalidad*. Y los métodos que dan con la solución son algoritmos conocidos como *test de primalidad*. Existen dos tipos de test, lo deterministas y los probabilísticos. Los test deterministas son capaces de afirmar con absoluta certeza la primalidad de un número dado. En cambio, los test probabilísticos sólo nos indican qué tan probable es que dicho número sea primo, sin ningún tipo de garantía matemática.

El primer test determinista surgió en el siglo II a. C. y se lo conoce como *la criba de Eratóstenes*, en honor a su creador, quien fue un matemático y astrónomo griego contemporáneo a Arquímedes.

La criba de Eratóstenes no sólo permite deducir la primalidad de un número dado n, sino que también encuentra todos los números primos menores que n. Funciona de la siguiente manera:

Se arma una tabla con todos los números comprendidos entre 2 y n. A continuación, se tachan todos los múltiplos de 2. El primer número que no ha sido tachado en la tabla (el 3) será número primo. Luego se tachan todos los múltiplos de ese número (los múltiplos de 3), y se repiten los pasos anteriores hasta el último número menor o igual a $\sqrt{n}$. Si al final del procedimiento el número n no ha sido tachado, entonces será un número primo. Por ejemplo, en la Figura 2, luego de haber tachado todos los múltiplos de los primos menores o iguales a $\sqrt{97}$, vemos que el 97 quedó sin tachar, por lo tanto 97 es un número primo.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97			

FIGURA 2. Criba de Eratóstenes para $n = 97$.

Si bien la criba de Eratóstenes es un método determinista para el análisis de primalidad, es ineficiente cuando se aplica a n grandes, pues requiere de tiempos de cómputo muy prolongados.

Un resultado teórico muy bello que podría ser utilizado como test de primalidad determinista es el llamado *Teorema de Wilson*:

> *Teorema de Wilson:* El número entero $n > 1$ es primo si y sólo si n divide a $(n-1)! + 1$.

Desafortunadamente, al igual que la criba de Eratóstenes, en la práctica, usar el Teorema de Wilson para determinar la primalidad de un número dado es muy costoso computacionalmente.

En el año 2002 un grupo de investigadores desarrolló un test de primalidad determinista con la característica de ser un algoritmo que se ejecuta en *tiempo polinomial*. Sin entrar en detalles técnicos, eso quiere decir que el tiempo que le lleva a una computadora completar el procedimiento es bastante "aceptable". El test se denomina *Test de primalidad AKS* [3], por las siglas de sus diseñadores. Y está basado en una generalización del *Pequeño Teorema de Fermat*:

> *Pequeño Teorema de Fermat:* Sea p un número primo y a un número natural, entonces p divide a $a^p - a$.

Una consecuencia directa del Pequeño Teorema de Fermat es la siguiente:

> *Corolario del PTF:* Si p es un número primo y a es un número natural no divisible por p, entonces p divide a $a^{p-1} - 1$.

Si bien la recíproca del corolario no vale, hay muchos valores de p para la cual sí se verifica. En ese hecho se basa un test probabilístico conocido como *Test de primalidad de Fermat* [4]. Los números en donde falla este test se llaman *Números de Carmichel*, por el matemático Robert Carmichel (1879 - 1967), quien se dedicó a estudiarlos. El número de Carmichael más pequeño es $n = 561 = 3 \times 11 \times 17$, que no es primo. Sin embargo, $a^{560} - 1$ es divisible por 561 para cualquier a coprimo con 561.

§3. Factorización

El *problema de factorización* consiste en escribir cualquier número n como producto de primos, y es aún más complicado que el problema de primalidad. Un algoritmo elemental que se enseña en la escuela primaria (Figura 3) permite factorizar, con papel, lápiz y calculadora, cualquier número n (no muy grande) en producto de primos. Pero, desventajosamente, ese algoritmo requiere conocer previamente todos los números primos menores o iguales a n; además de muuucha paciencia y tiempo.

68	2
34	2
17	17
1	

FIGURA 3. $68 = 2^2 17$.

A diferencia del problema de primalidad, aún no se sabe si el problema de factorización se puede resolver en *computación clásica* en tiempo polinomial. Sin embargo, existe un algoritmo de factorización en tiempo polinomial en lo que se conoce como *computación*

cuántica [5], que es otro enfoque a la computación, y que se encuentra en sus primeras etapas de desarrollo.

§4. Fábrica de números primos

No nos costó mucho entender que hay infinitos números primos, pero decir quiénes son es otra historia, y una muy difícil. Desde su descubrimiento, los matemáticos han trabajado arduamente en la búsqueda de nuevos números primos. El interés por encontrarlos no nace sólo del reto intelectual que implica, sino también de la utilidad práctica que tienen estos números para, por ejemplo, la criptografía. Los números primos son la base de los sistemas de seguridad informática que protegen las comunicaciones y los datos en Internet.

Una *fórmula de números primos* es una regla que genera estos números, como una especie de fábrica de primos. El desafío del matemático consiste en encontrar fórmulas de números primos que requieran tiempos de ejecución razonables.

Consideremos la siguiente fórmula

$$n^2 - n + 41.$$

Para $n = 1$ obtenemos 41, que es un número primo. Para $n = 2$ da 43, que también es primo. Para $n = 3$ sale 47, que nuevamente es un número primo. ¿Será cierto que para cualquier $n = 1, 2, 3, 4, \ldots$ número natural $n^2 - n + 41$ es un número primo? A pesar de que para los primeros números naturales la fórmula produce exitosamente números primos, para $n = 41$ falla, pues el número que se obtiene es 41^2, que es claramente un número compuesto.

En la primera mitad del siglo XVII el matemático francés Pierre de Fermat conjeturó que todos los números de la forma

$$F_n = 2^{2^n} + 1,$$

donde n es un número natural, son números primos. Por ejemplo $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ y $F_4 = 65537$ son ciertamente números primos. Sin embargo F_5 ya no es un número primo, pues es divisible por 641. Lo que prueba la falsedad de la conjetura.

Las dos fórmulas arriba presentadas no son fórmulas de números primos, ya que para ciertos valores de n (conocidos y desconocidos) el cálculo no da número primo. Pero entonces... ¿existen fórmulas de números primos? Actualmente sí se conocen algunas, un ejemplo deriva del ya mencionado Teorema de Wilson [6].

Por otra parte, no es difícil probar que no existe una fórmula polinómica

$$f(x) = a_n x^n + \cdots + a_1 x + a_0,$$

de grado $n \geq 1$, tal que $f(k)$ sea un número primo para todo entero k. Sin embargo, se conocen sistemas de *ecuaciones diofánticas* (ecuaciones algebraicas en una o más incógnitas con coeficientes enteros) en 26 variables que pueden ser usadas para obtener números primos [7].

Finalmente, cabe destacar que, a pesar de que existen fórmulas de números primos, las que se conocen hasta la fecha son demasiado complicadas como para ser aplicables computacionalmente. Para fortuna de los matemáticos, aún queda muchísimo por investigar y descubrir :)

§5. Primos con nombre propio

Si bien algunas fórmulas no generan siempre números primos, son muy útiles para encontrar conjuntos pequeños de estos números. Es por ello que se les han asignado nombre propio. Algunos ejemplos:

Primos de Fermat. Estos primos ya se han mencionado más arriba. Son de la forma

$$F_n = 2^{2^n} + 1,$$

para algún número entero n mayor o igual a cero. Curiosamente, los únicos primos de Fermat que se conocen son F_0, F_1, F_2, F_3 y F_4.

Primos de Mersenne. Un primo de Mersenne es de la forma

$$M_p = 2^p - 1,$$

donde p es un número primo. El 7 de enero de 2016 se anunció el descubrimiento del primo más grande que se conoce: es el primo de Mersenne $M_{74207281}$, ¡y tiene más de 22 millones de cifras! [8].

Primos de Sophie Germain. Un número primo p se dice que es de Sophie Germain si $2p+1$ también es un número primo. Estos primos recibieron el nombre de la matemática francesa Sophie Germain (1776 – 1831), quien obtuvo importantes resultados en el área de Teoría de Números.

§6. El Teorema de los Números Primos

Se sabe que hay infinitos números primos, pero... ¿se conoce su distribución entre los números naturales? Hacia el siglo XVIII el matemático alemán llamado Johann Carl Friedrich Gauss se planteó este interrogante. La idea intuitiva de la época era que los números primos se hacen cada vez menos frecuentes cuanto más grandes son. Gauss conjeturó que, si $\pi(n)$ es la cantidad de números primos menores o (iguales a n, entonces $\pi(n)$ es aproximadamente (de forma que precisaremos más adelante) igual a $n/\log n$.

Recién en el año 1896 J. Hadamard y C. de la Vallée Poussin demostraron, de manera independiente pero con técnicas similares, la conjetura de Gauss [9], convirtiéndola en uno de los teoremas más importantes y emblemáticos de la Teoría de Números.

Teorema de los Números Primos:

$$\pi(n) \sim \frac{n}{\log n}.$$

Aquí, el símbolo $\sim$ se define por $f(x) \sim g(x)$ si y sólo si $\lim \frac{f(x)}{g(x)} = 1$ cuando x tiende a infinito.

§7. ¿Cómo sigue esta historia?

¿Existen infinitos primos de Mersenne? ¿Hay sólo cinco primos de Fermat? ¿Todo número par es la diferencia de dos números primos? ¿Existe un número primo entre n^2 y $(n+1)^2$?... Conjeturas como éstas hay un montón. Una muy famosa, y que algunos matemáticos la califican como el problema abierto más difícil de la historia de la matemática, es la *conjetura de Goldbach*. Fue conjeturada por Christian Goldbach en el año 1742, y sorprendentemente tiene un enunciado muy muy sencillo:

> *Conjetura de Goldbach:* Todo número par mayor que 2 puede escribirse como suma de dos números primos.

Han pasado 275 años y muchas mentes brillantes y aún no se ha encontrado una demostración. Sin embargo, entre los año 2012 y 2013 el matemático peruano Harald Helfgott publicó dos trabajos ([10], [11]) en donde logra probar una versión débil de la conjetura:

> *Conjetura débil de Goldbach:* Todo número impar mayor que 5 puede expresarse como suma de tres números primos.

Notar que la Conjetura de Goldbach implica la Conjetura Débil de Goldbach.

Sobre números primos aún queda muchísimo por descubrir. Numerosas conjeturas y preguntas abiertas son temas de investigación actual. La curiosidad y la fascinación por estos números nos motivan a indagar cada vez más profundo sobre su naturaleza. Sin lugar a duda, esta historia sigue para adelante...

Referencias

[1] Euclides. *Elementos. Libros I-XIII. Vol. I, II y III. Trad. M.L. Puertas Castaños.* Notas: L. Vega Reñón. Madrid: Editorial Gredos. 1991.

[2] Boyer. Carl B. Boyer, Uta C. Merzbach. *A History of Mathematics*. New York: Wiley, 1991.

[3] Manindra Agrawal, Neeraj Kayal, Nitin Saxena. *PRIMES is in P*, Ann. Math. 160, no. 2, (781–793) 2004.

[4] https://es.wikipedia.org/wiki/Test_de_primalidad_de_Fermat.

[5] Peter Shor. *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*. SIAM Journal on Computing, Vol. 26,No. 5, (1484–1509), 1997.

[6] https://en.wikipedia.org/wiki/Formula_for_primes.

[7] James Jones, Daihachiro Sato, Hideo Wada, Douglas Wiens *Diophantine representation of the set of prime numbers*. American Mathematical Monthly 83, no. 6, (449–464) 1976.

[8] http://www.bbc.com/news/technology-35361090.

[9] Andrew Granville. *Harald Cramér and the distribution of prime numbers*, Scandinavian Actuarial Journal 1, (12–28) 1995

[10] Harald A. Helfgott *Major arcs for Goldbach's theorem*, 2013, arXiv:1305.2897.

[11] Harald A. Helfgott. *Minor arcs for Goldbach's problem*, 2012, arXiv:1205.5252.

Eugenia Bernanschini
Facultad de Matemática, Astronomía, Física y Computación (Famaf),
Universidad Nacional de Córdoba (UNC).
Av. Medina Allende s/n , Ciudad Universitaria (X5000HUA) Córdoba, Argentina.
(✉) bernasch@famaf.unc.edu.ar

Recibido: *4 de julio de 2017*.
Aceptado: *2 de setimebre de 2017*.
Publicado en línea: *1 de diciembre de 2017*.