Los números primos

Hernán Alberto Escobar

INTRODUCCION

La teoría de los números es la disciplina matemática que se ocupa de las propiedades de los números enteros positivos o también denominados números naturales.

En este artículo nos pronemos abordar muy sucintamente un aspecto estudiado por la teoría de los números en lo concerniente a los números primos. En realidad este tema es bastante amplio y denso y es prácticamente imposible describir en este artículo todo lo que se ha descubierto y la extensa literatura que sobre este tópico existe hoy en día. El interés radica en mostrar algunas curiosidades, propiedades muy particulares y además problemas planteados por ilustres matemáticos a lo largo de la historia.

DEFINICIONES

1) Si a y b son números enteros y $a \neq 0$, se dice que a divide a b ó a es divisor de b y se denota $a|b$ en caso de que exista un entero c, de modo que $b = a \cdot c$. De este modo es claro que $3|12$ puesto que $3 \cdot \boxed{4} = 12$, es decir $c = 4$. Del mismo modo $3|-18$ ya que $3 \cdot \boxed{-6} = -18$ o sea $c = -6$

2) Se dice que un entero $p > 1$ es primo, en caso de que los únicos divisores

positivos de p sean p y 1 Así por ejemplo los números 2, 3, 5, 7, 11, 13, 19, son primos; en tanto que los números -2, -1, 0, 4, 6, 8, 9, no lo son.

3) Si $n > 1$ es un entero positivo, el cual no es primo, entonces diremos que "n" es un número compuesto.

Las siguientes preguntas son obvias y se desprenden de las anteriores definiciones:

i) ¿ Existe algún mecanismo o fórmula para obtener **todos** los números primos, partiendo del hecho de que 2 es el primero, 3 el segundo ?

ii) ¿ Cuántos números primos hay ?

iii) ¿ Existe algún mecanismo para determinar si un número dado es primo o compuesto ?

iv) ¿ Dado un entero positivo x, cuántos primos existen tales que $p \leq x$?

Estas son apenas algunas preguntas, diríamos inciales, acerca de los números primos. Al finalizar este artículo mencionaremos algunos problemas, no resueltos, hasta hoy, concernientes a los números primos.

Es necesario, antes de intentar responder a estas preguntas, establecer unos resultados (sin demostración) muy importantes.

TEOREMA 1. Cada número $n \in Z^+$, $n > 1$ es primo o producto de primos (compuesto).

TEOREMA 2. (Teorema fundamental de la aritmética). Si $n > 1$ es entero, entonces o n es primo o se puede expresar como producto de primos de una única manera.

TEOREMA 3 Existe un número infinito de primos

La prueba de este último teorema se la puede realizar por reducción al absurdo, es decir suponer en principio que existe un número finito de primos.

El teorema 3 dá respuesta a la pregunta ii). Pero ¿ cómo se puede determinar si un número dado es primo o no, y además, cuáles son los números primos ?. Hasta la fecha nadie ha podido resolver estas preguntas adecuadamente. Con la ayuda de computadores se ha investigado la primacidad de un número entero. Hasta 1971, el primo más grande era $2^{19937}-1$. Sin embargo David Slowinski en enero de 1983 descubrió que $2^{86243}-1$ es primo, cuya expansión decimal contiene 25962 cifras !.

A pesar del trabajo arduo de brillantes matemáticos durante varios siglos de trabajo, nadie ha encontrado soluciones a la primera y cuarta preguntas. Para números pequeños, la <u>criba de Eratóstenes</u> es útil para determinar los primos menores que un número dado, por ejemplo 150.

CRIBA DE ERATOSTENES

$\boxed{2}$	$\boxed{3}$	4	$\boxed{5}$	6	$\boxed{7}$	8	9	10	$\boxed{11}$	12	$\boxed{13}$	14	15	16
$\boxed{17}$	18	$\boxed{19}$	20	21	22	$\boxed{23}$	24	25	26	27	28	$\boxed{29}$	30	$\boxed{31}$
32	33	34	35	36	$\boxed{37}$	38	39	40	$\boxed{41}$	42	$\boxed{43}$	44	45	46
$\boxed{47}$	48	49	50	51	52	$\boxed{53}$	54	55	56	57	58	$\boxed{59}$	60	$\boxed{61}$
62	63	64	65	66	$\boxed{67}$	68	69	70	$\boxed{71}$	72	$\boxed{73}$	74	75	76
77	78	$\boxed{79}$	80	81	82	$\boxed{83}$	84	85	86	87	88	$\boxed{89}$	90	91
92	93	94	95	96	$\boxed{97}$	98	99	100	$\boxed{101}$	102	$\boxed{103}$	104	105	106
$\boxed{107}$	108	$\boxed{109}$	110	111	112	$\boxed{113}$	114	115	116	117	118	$\boxed{119}$	120	121
122	123	124	125	126	$\boxed{127}$	128	129	130	$\boxed{131}$	132	133	134	135	136
$\boxed{137}$	138	$\boxed{139}$	140	141	142	143	144	145	146	147	148	$\boxed{149}$	150	

Antes de 150 existen 35 números primos.

La elaboración de la tabla es así: El entero 2 es primo, y los múltiplos de 2 no lo son, por lo tanto tachamos 4, 6, 8, ... etc. También 3 es primo y los múltiplos de 3 no lo son, de modo que estos últimos son descartados. Continuamos el proceso con los primos 5, 7 y 11 y no tomamos el 13 por cuanto su cuadrado 169 es evidentemente compuesto y se sale del límite de 150 previamente impuesto. De este modo los números que quedan sin tachar son primos (Los hemos encerrado en un rectángulo).

Naturalmente que la elaboración de una tabla de primos menores que un número más grande, digamos 3821911, empleando la metodología de la elaboración de la criba de Eratóstenes resulta poco práctica.

Ahora bien, resulta curioso observar que cuando se estudia una lista de primos "parece" que ocurriera que estos se vuelven cada vez más "escasos". Examinemos unos ejemplos:

Número de primos entre:

1 y 1000 → 168

1000 y 2000 → 135

2000 y 3000 → 127

3000 y 4000 → 120

4000 y 5000 → 119

Una tabla que daba la lista de todos los números primos menores que 10 millones (10'000.000) fue publicada en 1914 por el matemático americano D. N. Lehmer. Existen exactamente 664579 primos menores que 10 millones, o sea aproximadamente el 6.5%. Más recientemente, D. H. Lehmer (hijo de D. N. Lehmer) al finalizar los años cincuenta calculó el total de primos menores que 10 mil millones; hay exactamente 455052512 números primos o seal el 4.5% aproximadamente.

Un examen detallado de una table de primos pone de manifiesto que se hallan distribuidos de una manera muy irregular. Por ejemplo el primo 370261 va seguido de 111 compuestos. No existe primo alguno entre 20831323 y 20831533.

Antes de terminar este aparte, es curioso hacer notar que las tablas muestran reiteradamente primos consecutivos tales como 3 y 5; 101 y 103 que como puede notarse difieren tan solo en dos unidades. Tales primos se los conoce como primos gemelos. Hay exactamente 1000 pares de estos números por debajo de 100000 y unos 8000 por debajo de 1'000.000. El par más grande conocido hasta 1980 es $76 \cdot 3^{139} - 1$ y $76 \cdot 3^{139} + 1$ descubiertos por Williams y Zarnke.

NUMEROS PERFECTOS Y PRIMOS DE MERSENNE

Los griegos de la escuela de Pitágoras definieron los **números perfectos** como aquellos que tienen la propiedad de que la suma de sus divisores positivos propios reproduce el mismo número (excluyéndose así mismo). Por ejemplo $6 = 1 + 2 + 3$ y $28 = 1 + 2 + 4 + 7 + 14$ son perfectos. Los cinco primeros perfectos pares son 6, 28, 496, 8128 y 33550336.

En el libro IX, Euclides demuestra que todo número par es perfecto si tiene la forma

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

en donde p y $2^p - 1$ son primos.

En 1757 Leonard Euler (1707 – 1783) demostró el recíproco parcial del teorema de Euclides: si un número par es perfecto, entonces tiene la forma $2^{p-1}(2^p - 1)$ donde 2^{p-1} es primo. Nadie sabe hasta hoy si existen números perfectos impares. Si los hay de hecho deben ser muy grandes, pues en 1967 se demostró que si un número perfecto impar existe, debe ser mayor que 10^{36}.

Los números de la forma $2^p - 1$ en donde p es primo se llaman **números de Mersenne** en honor al fraile fransciscano Marín Mersenne quien inició la búsqueda de primos con esta ley de formación. Con cada número primo de Mersenne hay asociado un número perfecto, de ahí la importancia de su estudio. Mersenne afirmó que para valores de p iguales a 2, 3, 5, 7, 13, 17, 31, 67, 127 y 257 los enteros $2^p - 1$ son primos. En 1750 Euler demostró que Mersenne se había equivocado en $p = 67$ y $p = 257$ y que debía haber incluido en su lista valores de p iguales a 19, 61, 89, 107.

A pesar del error de Mersenne, estos primos todavía llevan su nombre y la búsqueda de tales primos aún continúa. Si hay infinitos primos de Mersenne habrán infinitos números perfectos; pero este es un problema que aún no tiene solución.

El mayor primo de Mersenne conocido hasta 1983 es $2^{86243} - 1$ que como ya lo mencionamos anteriormente fue descubierto por Slowinski en ese año. Con este número está asociado el 28° número perfecto par:

$$(2^{86243} - 1) \cdot 2^{86243}$$

GENERACION DE NUMEROS PRIMOS

Pierre de Fermat (1601 – 1665) gran matemático francés que incursionó en teoría de números primos, creyó haber descubierto una función o fórmula que generaba sólo números primos. La función definida como

$$f(n) = 2^{2^n} + 1 \; ; \quad n = 0, 1, 2, 3, \ldots$$

genera primos para $n = 0, 1, 2, 3$ y 4. Ante la evidencia de los primeros casos, Fermat murió convencido de que $f(n)$ es siempre primo. Sin embargo Euler demostró en 1732 que $f(5)$ es compuesto puesto que $2^{32} + 1$ es divisible por 641. En efecto

$$2^{32} + 1 = 6494967297 = (641)(6700417)$$

Más allá de $f(5)$ no se han hallado otros primos de Fermat. Se ha probado que para $5 \leq n \leq 16$ cada número de Fermat $f(n)$ es compuesto

Otra expresión que genera números primos fue propuesta por Euler en 1742. La función

$$f(x) = x^2 - x + 41$$

da valores primos para $x = 0, 1, 2, \ldots, 40$, pero para cuando $x = 41$ el resultado es un número compuesto.

El polinomio $x^2 - 79x + 1601$ proporciona números primos para $x = 0, 1, 2, \ldots, 79$. Para $x=80$ el resultado es un número compuesto.

Ninguna de tales fórmulas simples puede dar un número primo para cada valor de x, aunque se utilicen potencias superiores. De hecho, **Christian Goldbach** ($1690 - 1764$), en 1572 probó que ningún polinomio en x con coeficientes enteros puede dar primo para todo x, e incluso para x suficientemente grande.

Los resultados anteriores ilustran la irregularidad de la distribución de los números primos. Tal como lo mencionamos anteriormente, dá la impresión de que a medida que se avanza en una tabla de primos, estos se presentan cada vez más espaciados.

Dos de los maemáticos más conocidos a través de la historia como son **Carl F. Gauss** ($1777 - 1855$) y **Adrien Marie Legendre** ($1752 - 1833$), trataron en el siglo XIX de encontrar una función $f(x)$, que aún si no fuera igual a $\pi(x)$ para cada x, por lo menos aproximara a $\pi(x)$ cuando $x \to \infty$, en donde $\pi(x)$ es la cantidad de números primos p tales que $2 \leq p \leq x$. Legendre conjeturó que

$$f(x) = \frac{x}{\ell n\, x - 1.08336}$$

tendría esta propiedad, es decir que

$$\lim_{x \to \infty} \frac{\pi(x)}{f(x)} = 1$$

Gauss propuso la función

$$f(x) = \int_2^x \frac{dt}{\ell n\, t}$$

y ambos, Gauss y Legendre independientemente conjeturaron que

$$f(x) = \frac{x}{\ell n\, x}$$

resultaría la función deseada. La siguiente tabla nos proporciona una idea de lo razonable de los anteriores planteamientos.

x	$\pi(x)$	$\frac{x}{\ell n\, x}$	$\frac{x}{\ell n x - 1.08336}$	$\int_2^x \frac{dt}{\ell t}$	$\frac{\pi(x)}{x/\ell n\, x}$
1000	168	145	172	178	1.16
10000	1229	1086	1231	1246	1.13
100000	9592	8686	9588	9630	1.10
1000000	78498	7238	78543	78628	1.08
10000000	664579	620421	665138	664918	1.07

Examinando la tabla para $x \leq 10^6$, Gauss y Legendre propusieron independientemente que el cociente

$$\frac{\pi(x)}{x/\ell n\, x}$$

era próximo a 1 cuando $x \to \infty$. Aunque intentaron demostrar esta afirmación, no tuvieron éxito. El primer resultado importante en esa dirección se debe al matemático ruso **Chevyschev** quien demostró en 1850 que para valores grandes de x, la siguiente expresión es válida

$$\frac{x}{0.921\, \ell nx} < \pi(x) < 1.106\, \frac{x}{\ell nx}$$

Sin embargo no fue capaz de demostrar que el límite era 1.

Después de los fracasos de varios matemáticos, incluyendo a **Riemann**, finalmente en 1896 **J. Hadamard** y **C.J. de la Vallée Poussin** probaron independientemente uno de los problemas más notables de la historia de las matemáticas: ***el teorema de los números primos***, el cual, evidentemente, reivindicó a Gauss y a Legendre.

TEOREMA DE LOS NUMEROS PRIMOS

$$\boxed{\lim_{x\to\infty} \frac{\pi(x)}{f(x)} = 1, \quad \text{donde} \quad f(x) = \frac{x}{\ell n x}}$$

OTRAS CONJETURAS Y CURIOSIDADDES DE LOS NÚMEROS PRIMOS

No todas las conjeturas referentes a números primos han sido resueltas tan exitosamente.

Considérense las siguientes igualdades:

$$10 = 7 + 3 \qquad 60 = 37 + 13 \qquad 12 = 5 + 7$$

$$24 = 17 + 7 \qquad 148 = 17 + 131$$

Goldbach conjeturó en 1742 que todo entero par $n \geq 4$ se podría escribir como la suma de dos primos. Le pidió a Euler que la probara o la negara. Sin embargo Euler fracasó y así todos los matemáticos desde entonces, hasta nuestros días.

Esta conjetura está sin decidir hasta hoy, aunque en los últimos años se han efectuado algunos progresos que indican que la conjetura es probablemente verdadera, aunque no se ha encontrado una prueba con rigor matemático que determine la validez de la misma. No obstante, la conjetura de Goldbach ha sido comprobada utilizando el computador para todo número menor que 33×10^6. Es más, se ha establecido que cada número par n tal que $6 < n < 33 \times 10^6$ no solo se puede escribir como la suma de dos números primos sino como la suma de dos primos impares distintos.

Los esfuerzos realizados por ilustres matemáticos tendientes a demostrar la conjetura de Goldbach han permitido el descubrimiento de otras propiedades y curiosidades propias de los números primos. En este sentido, el matemático soviético I. **Vinográdov** estableció que cada entero mayor que $e^{e^{16.038}}$ se puede escribir como la suma de no más de cuatro primos y en 1937 mostró que a partir de un lugar, todo número impar es la suma de tres primos, siempre que n sea suficientemente grande. Este último resultado es verdadero para todo número impar $n > 3^{3^{15}}$, hecho que constituye hoy por hoy la evidencia de que efectivamente la conjetura de Goldbach es verdadera. Sin embargo nadie ha podido demostrar la afirmación de Goldbach a partir de la de Vinogradov.

Para terminar, mencionaremos algunos problemas no resueltos hasta hoy que involucran números primos:

1) ¿ Existe un número par $n > 2$ que no sea la suma de dos primos ?.
2) ¿ Existe una infinidad de primos gemelos ?.
3) ¿ Existe una infinidad de primos de Mersenne ?.
4) ¿ Existe una infinidad de números de Mersenne compuestos ?.
5) ¿ Existe una infinidad de primos cuyos digitos en base 10 sean todos uno ?

   (Existen ejemplos: 11 y 11111111111111111111111).

BIBLIOGRAFIA

[1] APOSTOL, Tom. Introducción a la Teoria Analítica de Números. Editorial Reverté S.A., Madrid, 1980.

[2] BOYER, C. A History of Mathemathics. John Wiley and Sons. New York, (USA), 1960.

[3] COLLETTE, Jean Paul. Historia de las Matemáticas. Edit. Siglo XXI, Madrid, 1986.

[4] PAREJA, Diego. Euler y la Teoria de Números. Matemática, Enseñanza Universitaria, No 34, 1985.

[5] VINOGRADOV, Iván. Fundamentos de la Teoría de los Números. Edit. Mir, Moscú, 1977.

DEPARTAMENTO DE MATEMATICAS Y ESTADISTICA
UNIVERSIDAD DE NARIÑO
PASTO(N)