OTROS ARTÍCULOS

SOBRE LOS NÚMEROS PRIMOS

A

José Miguel Pacheco Castelao
Luis González Sánchez
Dpto. de Matemáticas.
Universidad de Las Palmas de Gran Canaria.

1. INTRODUCCIÓN

La rama de las matemáticas que estudia las propiedades de la sucesión de los números naturales (también llamados enteros positivos): 1,2,3,4,5,... se denomina Aritmética Superior o Teoría de Números. La moderna Teoría de Números nace como disciplina científica independiente con la obra "Disquisitiones Arithmeticae" escrita en 1801 por el matemático alemán Carl Friedrich Gauss. Fue el propio Gauss (quizás el mejor matemático de todos los tiempos) quien afirmó que *"La Matemática es la reina de las ciencias y la Teoría de Números es la reina de las Matemáticas"*.

Un número natural mayor que 1 se dice primo si sólo es divisible por él mismo y por la unidad. El resultado básico de la Teoría de Números (conocido como Teorema Fundamental de la Aritmética) afirma que cualquier número no primo (compuesto) puede escribirse de una única manera como producto de números primos. Por ejemplo:

$$12936 = 2^3 \cdot 3 \cdot 7^2 \cdot 11$$

Los números primos son, por tanto, los cimientos sobre los que se construye todo el edificio de la Aritmética, razón por la cual constituyen el objeto central de su estudio. Recurriendo a un símil químico, el Teorema Fundamental de la Aritmética afirma que los números primos son las partes indivisibles (átomos) de las que se componen los números naturales (moléculas).

Obviamente, todos los números primos, con la única excepción del 2, son impares y esta es la lista de los veinticinco primeros (los primos menores que 100):

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,
43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

Escribió el matemático alemán D. Zagier que *"Al contemplar los números primos se tiene la impresión de hallarse en presencia de secretos inexplicables"*. A lo largo de estas notas comprobaremos cuán cierta es esta afirmación. Quedan muchas cuestiones por aclarar sobre estos misteriosos números, pero en esto radica también gran parte de su atractivo.

2. CONJETURAS

Una de las características más conocidas de la Aritmética es el contraste entre la sencillez de muchos de sus enunciados y la dificultad que entraña el probarlos. No es de extrañar, por tanto, que la Teoría de Números y, particularmente la Teoría de Números Primos, esté plagada de conjeturas, muchas de ellas de enunciado muy simple. He aquí algunas conjeturas sobre primos:

1) Todo número par mayor que 2 es suma de dos primos (Conjetura fuerte de Goldbach).

2) Todo número impar mayor que 5 es suma de tres primos (Conjetura débil de Goldbach).

3) Existe una secuencia de primos de cualquier longitud prefijada en las que cada uno es el doble del anterior más uno. Estas secuencias se llaman cadenas de Cunningham y la siguiente es de longitud cinco: 2, 5, 11, 23, 47. A un primo impar p tal que $2 \cdot p + 1$ también es primo, se le llama primo de Sophie Germain.

4) En cada uno de los siguientes cuadrados:

$$\begin{matrix} 1 & 2 \\ 3 & 4 \end{matrix} \quad ; \quad \begin{matrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{matrix} \quad ; \quad \begin{matrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{matrix} \quad ; \quad \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 \\ 16 & 17 & 18 & 19 & 20 \\ 21 & 22 & 23 & 24 & 25 \end{matrix} \quad \ldots\ldots$$

cada fila contiene al menos un número primo (Conjetura P de Sierpinski).

5) Cada fila (salvo la primera) del siguiente "triángulo infinito"

$$\begin{matrix} 1 & & & & \\ 2 & 3 & & & \\ 4 & 5 & 6 & & \\ 7 & 8 & 9 & 10 & \\ 11 & 12 & 13 & 14 & 15 \\ \ldots & \ldots & \ldots & \ldots & \ldots \end{matrix}$$

contiene al menos un número primo (Conjetura de Schinzel).

6) Existen infinitos números primos de cada una de las siguientes formas:

$$n^2+1 \quad ; \quad n\cdot 2^n-1 \quad ; \quad n!\pm 1 \quad ; \quad n\#\pm 1 \quad ; \quad 2^{2^n}+1 \quad ; \quad 2^p-1 \ (p \text{ primo})$$

(donde $n!$ y $n\#$ denotan respectivamente el producto de los naturales o primos, hasta n).

7) Existen infinitos números primos de cada una de las siguientes formas:

$$10^n+1 = 10...01 \quad ; \quad \frac{10^n-1}{9} = 11...1 \quad ; \quad 1+2^1+...+2^n = 11...1_{(2}$$

Sabemos que para que el número 11...1 (escrito en base 10 o en base 2) sea primo es necesario que el número de sus dígitos sea primo (11 ó $127 = 1111111_{(2}$).

8) Por contra, se cree que todos los números 12^n+1 (n>1) son compuestos:

$$12^2+1 = 5\cdot 29 \quad , \quad 12^3+1 = 7\cdot 13\cdot 19 \quad , \quad 12^4+1 = 89\cdot 233 \quad , \quad ...$$

9) Si se disponen en filas las diferencias (absolutas) sucesivas de los números primos:

2 3 5 7 11 13 17 ...
1 2 2 4 2 4 ...
1 0 2 2 2 ...
1 2 0 0 ...
1 2 0 ...
1 2 ...
1 ...

todas las filas (salvo la primera) empiezan por 1 (Conjetura de Gilbreath).

10) Existen infinitos primos gemelos.

11) La sucesión de Fibonacci contiene infinitos números primos.

12) Si p es primo, entonces 2^p-1 no es nunca divisible por el cuadrado de un primo.

13) Dado un número primo p mayor que 7 ¿Cuál es la máxima distancia (*gap*) posible hasta el siguiente número primo? El cuadrado de su logaritmo natural: $(\log p)^2$.

Un ejemplo notable de conjetura (sobre primos) recientemente "vencida" es el Último Teorema de Fermat: "La ecuación $x^n + y^n = z^n$ no admite soluciones enteras positivas cuando n es mayor que 2". A pesar de la sencillez de su enunciado, su

prueba definitiva, una hazaña del matemático británico Andrew Wiles en 1994 ¡tres siglos y medio después de que Fermat lo enunciara!, se basa en una compleja relación entre curvas elípticas y funciones modulares, en el ámbito de la Geometría Algebraica.

3. EL N-ÉSIMO NÚMERO PRIMO

La primera cuestión que se nos plantea es si la lista de números primos: 2, 3, 5,... tiene fin o es ilimitada. La respuesta, dada por Euclides hace unos 2.300 años, es que: "existen infinitos números primos" y su demostración original es un ejemplo de brevedad y elegancia matemática, que reproducimos a continuación. "Sean $2,3,5,...,p_n$ los n primos números primos. Veamos que siempre existe un primo adicional (mayor que todos ellos). El número $N = 2\cdot3\cdot5\cdot...\cdot p_n + 1$ o bien es primo (en cuyo caso es el primo buscado), o bien es compuesto y entonces será divisible por algún primo necesariamente mayor que p_n".

No sabemos si hay infinitos primos de la forma $p_n\# + 1 = 2\cdot3\cdot5\cdot...\cdot p_n + 1$, pero, con estos números, R. Fortune diseñó un curioso y sencillo procedimiento para producir un número primo a partir de otros:

"Sea P el primer primo posterior a $p_n\# + 1$. Entonces, ¡$P-p_n$ # es un número primo!".

Por ejemplo:

$$7\# + 1 = 2\cdot3\cdot5\cdot7 + 1 = 211 \Rightarrow P = 223 \Rightarrow P - 7\# = 223 - 210 = 13 \text{ es primo}$$

¿En dónde se esconde el n-ésimo número primo p_n? Divídase cada uno de los 25 primeros primos por el primo precedente. Por otro lado, réstese a la raíz cuadrada de cada uno de ellos la raíz cuadrada del anterior. ¿Han hecho bien las cuentas? Para todo n:

$$\frac{p_n}{p_{n-1}} \leq 5/3 \text{ (Tma. de Sandor)} \quad ; \quad \sqrt{p_n} - \sqrt{p_{n-1}} < 1 \text{ (Conjetura de Andrica)}$$

Estas fórmulas relacionan cada primo p_n con el anterior p_{n-1}. Demos sólo una de las muchas que aproximan p_n en términos absolutos (válida para $n \geq 8602$).

$$n(\log n + \log\log n - 1.0073) < p_n < n\,(\log n + \log\log n - 0.9385)$$

Por ejemplo, "el primo un millón" es exactamente $P_{1.000.000} = 15485863$ y la fórmula da:

$$15434002 < p_{1.000.000} < 15502803$$

Un viejo sueño de los especialistas en Teoría de Números es obtener una fórmula que genere todos y sólo los números primos. El trinomio de Euler $n^2 - n + 41$ da

valores primos para $n = 1,2,...,40$, pero es compuesto para $n = 41$. El récord actual de polinomios cuadráticos con valores consecutivos de n primos lo ostenta el polinomio de Ruby: $36n^2 - 810n + 2753$ que da 45 primos para $n = 0,1,...,44$, pero es compuesto para $n = 45$. No es de extrañar, Goldbach probó en 1752 que ningún polinomio (y Legendre que ningún cociente de polinomios) en una variable y de coeficientes enteros es primo para todo x. En otras palabras, no existe ninguna "fórmula sencilla" que genere sólo números primos. En 1947, el matemático W.H. Mills probó que la fórmula (existen infinitas posibilidades de elección de las constantes A y c):

$$[A^{c^n}] = [(1.306377883863...)^{3^n}] \quad ; \quad n = 1,2,3,... \text{ y } [x] = \text{parte entera de } x$$

A

da exclusivamente números primos. Pero no los da todos. El lector puede comprobar que para $n = 1,2,3$ se obtienen, respectivamente, los primos 2, 11 y 1361; con lo que la expresión (creciente en n) "olvida" todos los primos intermedios. También el número:

$$\left[2^{2^{\cdot^{\cdot^{2^{w}}}}}\right] \quad ; \quad w \cong 1.92878$$

(n veces)

es primo para todo $n \geq 1$. En 1970, el matemático Yuri Matyasevich construyó un polinomio de 26 variables y grado 27, cuyos valores positivos, cuando las variables recorren el conjunto de los enteros, son ¡exactamente (todos y sólo) los números primos!

Como conclusión, la imposibilidad de construir una fórmula sencilla que genere la serie de los primos nos permite concluir que el n-ésimo número primo se encuentra en ... paradero desconocido.

4. UNA DISTRIBUCIÓN CAÓTICA

La inexistencia de fórmulas simples que den exactamente los números primos (o, al menos, que sólo tomen valores primos) se debe a la extraordinaria irregularidad de su distribución en la sucesión de los números naturales. Veamos cuatro datos que confirman este extraño comportamiento:

i) Es muy probable que existan infinitos pares $(p, p+2)$ de primos gemelos como:

$$3 \text{ y } 5 \quad ; \quad 5 \text{ y } 7 \quad ; \quad 11 \text{ y } 13 \quad ; \quad ... \quad ; \quad 361700055 \cdot 2^{39020} \pm 1$$

(los mayores conocidos hasta hoy)

En 1949, Clement caracterizó así estas parejas de números:

"*n y $n+2$ son primos gemelos si y sólo si* $4[(n-1)!+1] + n$ *es múltiplo de* $n(n+2)$"

condición más exigente (obviamente) que la del Test de Wilson:

"*n es primo si y sólo si* $(n-1)!+1$ *es múltiplo de n*"

En todo caso, aún cuando se confirmase la existencia de infinitos primos gemelos, hay que decir que los primos gemelos son "muy pocos" en relación con la totalidad de los primos. Esta afirmación puede interpretarse comparando la suma de los recíprocos de todos los primos con la suma de los recíprocos de sólo los primos gemelos:

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{23}+\frac{1}{29}+\frac{1}{31}+\ldots=\infty$$

$$\left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\left(\frac{1}{17}+\frac{1}{19}\right)+\left(\frac{1}{29}+\frac{1}{31}\right)+$$

$$+\ldots\cong 1.90216 \text{ (Cte. de Brun)}$$

ii) Quizás el número del D.N.I. del lector no sea primo, pero seguro que existe un primo que empieza por ese número. Dada una secuencia cualquiera de dígitos existe siempre un número primo cuyos primeros dígitos son los dados. Por ejemplo, 133 no es primo pero sí lo es 13327.

iii) Obsérvese que, cualquiera sea el número natural n, entre $n!+1$ y $n!+n+1$ no existe ningún número primo. La conclusión (tomando n tan grande como se quiera) es que pueden encontrarse cadenas ¡arbitrariamente largas! de números compuestos consecutivos separando dos primos sucesivos.

iv) Llamamos "campeón de salto" respecto a un número n a la distancia entre primos consecutivos menores o iguales que n, que se repite con más frecuencia. Por ejemplo, el campeón de salto respecto a 18 es 2 porque:

$$3-2=1\ ,\ 5-3=2\ ,\ 7-5=2\ ,\ 11-7=4\ ,\ 13-11=2\ ,\ 17-13=4$$

Se cree que los campeones de salto crecen indefinidamente y, ¡lo más espectacular!, los únicos campeones de salto conocidos son 1, 4 y los factoriales de primos:

$$2\ ,\ 2\cdot3=6\ ,\ 2\cdot3\cdot5=30\ ,\ 2\cdot3\cdot5\cdot7=210\ ,\ 2\cdot3\cdot5\cdot7\cdot11=2310,\ldots$$

Si se contrastan las afirmaciones (i) y (ii) (que indican cercanía o abundancia) con (iii) y (iv) (que expresan lejanía o escasez) en la serie de los números primos, la conclusión sólo puede ser esta: la distribución de los números primos es extraordinariamente caprichosa.

5. ORDEN EN EL CAOS

¿Cómo poner orden en este caos? Contemplando los números primos globalmente, se observa que la proporción de primos inferiores o iguales a x disminuye, cuando x aumenta. Por ejemplo (véase tabla adjunta), entre los 100 primeros números naturales hay 25 primos (el 25%), entre los 10.000 primeros hay 1.229 primos (el 12.29%). en el primer millón de números hay 78.498 primos (el 7.85%),... A la edad de 14 años, el alemán Carl Friedrich Gauss fue capaz de reconocer el patrón que rige estas proporciones. Denotando por $\Pi(x)$ al número de primos menores o iguales que x, Gauss formuló el siguiente Teorema del número primo (uno de los mejores ejemplos en Matemáticas de como encontrar orden en el caos).

$$\Pi(x) \approx \frac{x}{\log x} \quad (x \to \infty)$$

es decir, la proporción $\Pi(x)/x$ de primos son mayores que x es aproximadamente igual al inverso $1/\log x$ de su logaritmo natural (neperiano), y esta aproximación es tanto mejor cuanto mayor es x. El teorema explica que estos porcentajes (0.25, 0.1229, 0.0785,...) decrecen a cero, aunque no muy deprisa. El número e (la base de los logaritmos neperianos) aparece una vez más en los lugares más insospechados de la Matemática; esta vez marcando el son al que se mueven los números primos. La Tabla 1 ilustra el Teorema mediante comparación de sus dos últimas columnas:

TABLA 1

x	$\Pi(x)$	$\Pi(x)/x$	$1/\log x$
10^2	25	0.25	0.2171
10^4	1229	0.1229	0.1086
10^6	78498	0.0785	0.0724
10^8	5761455	0.0576	0.0543
10^{10}	455052511	0.0455	0.0434

6. LA HIPÓTESIS DE RIEMANN

Existen muchas estimaciones de $\Pi(x)$ mejores que la proporcionada por el cociente $x/\log x$. Por ejemplo, la siguiente aproximación (también atribuida a Gauss) constituye una formulación equivalente del Teorema del número primo, que merece un comentario especial:

$$\Pi(x) \approx Li(x) = \int_2^x \frac{dt}{\log t} \quad (x \to \infty)$$

donde $Li(x)$ es la llamada función logaritmo integral. La cuarta columna de la Tabla 2 (convergente a 1) ilustra esta nueva aproximación:

TABLA 2

x	$\Pi(x)$	$Li(x)$	$\Pi(x)/Li(x)$	$\lvert\Pi(x)-Li(x)\rvert$	$\sqrt{x}\log x$
10^2	25	29	.8621	4	46
10^4	1229	1246	.9863	17	921
10^6	78498	78628	.9983	130	13815
10^8	5761455	5762209	.9998	754	184207
10^{10}	455052511	455055614	.9999	3103	2302585

Pero, ¿qué calidad tiene esta segunda aproximación? Es decir, ¿cuál es la magnitud del error que se comete al aproximar $\Pi(x)$ por $Li(x)$? En respuesta a esta pregunta, hoy se piensa (aunque no se ha podido demostrar) que, para x lo bastante grande, se tiene la acotación:

$$\left| \Pi(x) - \int_2^x \frac{dt}{\log t} \right| \leq A\, x^{1/2} \log x$$

es decir: la función $|\Pi(x) - Li(x)|$ (5ª columna de la tabla 2), que mide la distancia entre el número exacto de primos no mayores que x y la estimación de Gauss, está mayorada (para x suficientemente grande) por el producto de una constante A adecuada por la raíz cuadrada de x y por su logaritmo neperiano (6ª columna de la tabla 2). Más brevemente, empleando la "O mayúscula" de Landau:

$$\Pi(x) - Li(x) \asymp O(x^{1/2} \log x) \ (x \to \infty)$$

Esta afirmación, que se refiere directamente a la distribución de los números primos, recibe el nombre de Hipótesis de Riemann (versión aritmética) y constituye ¡la conjetura no resuelta más importante de todas las matemáticas! Su confirmación definitiva nos daría mucha luz sobre esta misteriosa distribución. Además, en Teoría algebraica de números, se ha formulado una generalización de la Hipótesis de Riemann estrechamente vinculada con el problema de la existencia de un test determinista de primalidad (computacionalmente) eficiente. Más conocida es la versión clásica (analítica) de la Hipótesis de Riemann: Todos los ceros no triviales de (la prolongación analítica de) la función zeta de Riemann:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad (s \in C - \{1\})$$

tienen parte real 1/2.

Pasemos ahora a describir dos tipos específicos de números primos: los primos de Fermat y de Mersenne, dos especies muy codiciadas por los "cazadores de primos gigantes".

7. PRIMOS DE FERMAT

Es fácil probar que si un número de la forma $2^s + 1$ es primo, entonces s debe ser una potencia de 2. Pierre de Fermat, magistrado francés de la primera mitad del siglo XVII, pensaba que la afirmación recíproca también era cierta. Es decir, creía que todos los números de la forma $F_n = 2^{2^n} + 1$ (números de Fermat) eran primos. Estaba equivocado. Aunque los cinco primeros números de Fermat:

A

$$F_0 = 3\ ,\ F_1 = 5\ ,\ F_2 = 17\ ,\ F_3 = 257\ ,\ F_4 = 65537$$

son efectivamente primos (como él mismo comprobó), Euler descubrió en 1742 que el sexto es compuesto:

$$F^5 = 2^{32} + 1 = 641 \cdot 6700417$$

Hoy, 350 años después de que Fermat anunciase los cinco primos anteriores, no hemos sido capaces de encontrar ningún otro primo de Fermat. Y, lo que es mucho peor, no se sabe si tal primo existe. Tan sólo sabemos que, además de F_5, hay otros 169 números de Fermat compuestos (obtenidos mediante el Test de primalidad de Pepin). Es decir, sólo se conoce el carácter de 175 números de Fermat (5 primos, 170 compuestos).

La propiedad más curiosa de estos números (establecida por Gauss a la temprana edad de 19 años) es un aviso a los dibujantes: "Condición necesaria y suficiente para que la circunferencia pueda dividirse, con regla y compás, en n partes iguales es que los únicos primos que figuren en la factorización de n sean el 2 y/o primos de Fermat distintos entre sí". Así que (con regla y compás) podemos inscribir en la circunferencia el triángulo equilátero, el cuadrado, el decágono, el heptadecágono regular, ..., pero no el heptágono regular (pues 7 no es un primo de Fermat). Este era uno de los problemas.

Otros dos Teoremas básicos en el estudio de los números de Fermat son el que nos proporciona una condición necesaria (no suficiente) para los divisores de $F_n = 2^{2^n} + 1$, y el que establece una condición necesaria y suficiente para que F_n sea primo:

- Todo divisor mayor que 1 de F_n (n>2) es de la forma: $k2^{n+2} + 1$ ($k \in N$).
- *F_n es primo si y sólo si* $F_n | 3^{(F_n-1)/2} + 1$.

Por otro lado, los números de Fermat son, dos a dos, primos relativos, lo que puede deducirse de la identidad:

$$F_0F_1...F_{n-1} + 2 = F_n$$

Hoy conocemos tan sólo el carácter de 175 números de Fermat (los 5 primos citados y otros 170 compuestos) pero persiste la duda de si existe algún otro primo de Fermat mayor que F_4.

En todo caso, la infructuosa búsqueda de primos de Fermat mayores que los cinco conocidos por él (F_0, F_1, F_2, F_3, F_4) condujo a los matemáticos a un cambio de estrategia para la caza de primos gigantes. Se trataba de probar con otra especie numérica cuyos individuos primos se dejasen capturar más fácilmente: los números de Mersenne.

8. PRIMOS DE MERSENNE

Marin Mersenne, monje francés contemporáneo de Fermat, se interesó por los números de la forma 2^n–1. Para que estos números sean primos es necesario que n también lo sea. Pero no es suficiente:

$$2^{11} - 1 = 2047 = 23 \cdot 89$$

Los números de la forma $M_p = 2^p - 1$ (p primo) se llaman números (primos o compuestos) de Mersenne. Los cinco primeros primos de Mersenne son:

$$M_2 = 3 \ , \ M_3 = 7 \ , \ M_5 = 31 \ , \ M_7 = 127 \ , \ M_{13} = 8191$$

Es de destacar que un número de Mersenne cuyo exponente es un primo de Mersenne no siempre es primo. Por ejemplo: $M_{M_{13}} = M_{8191} = 2^{8191} - 1$ es compuesto. Sin embargo, se ignora si todos los números de Mersenne de la siguiente secuencia son primos:

$$M_2 \ , \ M_{M_2} \ , \ M_{M_{M_2}} \ , \ M_{M_{M_{M_2}}} \ , \ M_{M_{M_{M_{M_2}}}} \ , \ ...$$

esto es:

$$M_2 = 3 \ , \ M_3 = 7 \ , \ M_7 = 127 \ , \ M_{127} = 2^{127} - 1 \ , \ M_{2^{127}-1} = 2^{2^{127}-1} - 1 \ , \ ...$$

pues aunque los cuatro primeros lo son, persiste la duda sobre el "monstruoso" $2^{2^{127}-1} - 1$. Es obvio que si uno de ellos fuese compuesto, lo serían también todos los que le siguen.

En relación con los divisores de los números de Mersenne, se sabe que todo divisor primo q de $M_p = 2^p - 1$ es simultáneamente de las formas:

$$q = 8h \pm 1 \ (h \in N) \quad y \quad q = 2kp + 1 \ (k \in N)$$

Existe una curiosa relación entre los primos de Mersenne y los primos de Sophie-Germain, como consecuencia de la siguiente proposición establecida por Euler: Sea p primo tal que $p \equiv 3 \pmod 4$. Entonces:

$$2 \cdot p+1 \text{ es primo si y sólo si } 2 \cdot p+1 \text{ divide a } M_p$$

En particular: Si el número de Mersenne $M_p = 2^p-1$ es primo, entonces el primo p no es un primo de Sophie-Germain.

Hoy son conjeturas la existencia de infinitos números primos de Mersenne (sólo conocemos 38) y la existencia de infinitos números compuestos de Mersenne, y es una cuestión abierta la existencia de compuestos de Mersenne divisibles por el cuadrado de un primo.

A

9. NÚMEROS PERFECTOS

Los primos de Mersenne están ligados a los números perfectos. Un número se dice perfecto si es la suma de todos sus divisores positivos (salvo él mismo). Los cuatro primeros números pefectos son:

$$6 = 1+2+3 \quad , \quad 28 = 1+2+4+7+14 \quad , \quad 496 = 1+2+4+8+16+31+62+124+248$$

$$8128 = 1+2+4+8+16+32+64+127+254+508+1016+2032+4064$$

que pueden factorizarse como sigue:

$$6 = 2^{2-1}(2^2-1) \quad , \quad 28 = 2^{3-1}(2^3-1) \quad , \quad 496 = 2^{5-1}(2^5-1) \quad , \quad 8128 = 2^{7-1}(2^7-1)$$

donde el segundo factor es el primo de Mersenne $M_p = 2^p-1$ (p=2,3,5).

No es casualidad. Euclides y Euler demostraron que:

n (par) es perfecto si y sólo si $n = 2^{p-1}(2^p-1)$ y 2^p-1 es primo (de Mersenne)

Por tanto, hay tantos números pares perfectos como primos de Mersenne y se sospecha que hay infinitos (como se ha dicho, hoy sólo se conocen 38). He aquí algunas propiedades curiosas de estos números.

Sea $n=2^{p-1}(2^p-1)$ un número perfecto par mayor que 6. Entonces:

- n acaba en 6 (si $p-1 = 4$) o n acaba en 28 (si $p-1 \neq 4$).
- $n \equiv 0 \pmod 4$, $n \equiv 1 \pmod 9$, $n \equiv 4 \pmod{12}$.
- La suma de los inversos de los divisores de n es 2.
- n es triangular, esto es, de la forma $1+2+...+m$.
- n es de la forma $1^3+2^3+...+m^3$.
- $n = 11...\overset{p}{...}...100.\overset{p-1}{...}.0_{(2}$
- La suma reiterativa de las cifras de n, hasta llegar a un dígito, es la unidad.

Sabemos que de existir alguno algún número perfecto impar, éste tendría que ser muy grande (más de 300 dígitos) y de la forma:

$$n^2 \cdot p^{2m-1} \ (m \ , \ n \in N \ ; \ p \text{ primo})$$

pero lo cierto es que hoy no se conoce ningún número perfecto impar, y se ignora si existe. ¡¡¡Este es, probablemente, el problema irresuelto más antiguo de todas las Matemáticas!!!

10. EL MAYOR NÚMERO PRIMO CONOCIDO

Actualmente los primos de Mersenne constituyen la principal cantera para la obtención de primos gigantes. De hecho, el mayor número primo hoy conocido ("capturado" el 01-06-1999 por Nayan Hajratwala) es el primo de Mersenne:

$$¡¡¡¡¡¡¡ \ M_{6972593} = 2^{6972593} - 1 \ !!!!!!!$$

un número de:

¡¡¡ 2.098.960 dígitos !!!

Ni que decir tiene que el exponente $p = 6972593$ es un número primo (enano) y que el mayor número perfecto hoy conocido es:

$$2^{6972592} \ (2^{6972593}-1)$$

Pero, ¿cómo se obtuvo este primo gigante? No existe ningún algoritmo que permita decidir a un ordenador, con total certeza y en un tiempo "razonable", si un número dado es primo o compuesto. Sin embargo, la Teoría algebraica de números nos proporciona un test determinista de primalidad eficiente para los números de Mersenne:

Test de Lucas-Lehmer

"Sea p primo impar. Formemos la siguiente secuencia recurrente de restos módulo M_p:

$$S_1 \equiv 4 (M_p) \ , \ S_2 \equiv S_1^2 - 2 (M_p) \ , \ S_3 \equiv S_2^2 - 2 (M_p), \ ..., \ S_{p-1} \equiv S_{p-2}^2 - 2 \ (M_p)$$

Entonces:

$$M_p = 2^p - 1 \text{ es primo si y sólo si } S_{p-1} \equiv 0 \ (M_p)"$$

Como ejemplo, apliquemos el test de Lucas-Lhemer para comprobar que $M5 = 31$ es primo. En este caso $p = 5$ y obteniendo los restos de dividir por 31, se forma la secuencia:

$$S_1 \equiv 4 \ , \ S_2 \equiv 14 \ , \ S_3 \equiv 8 \ , \ S_{p-1} = S_4 \equiv 0$$

y, puesto que $S_4 \equiv 0$ (M_5), concluimos que ¡$M_5 = 31$ es un número primo! A esto se llama matar moscas con cañones.

Este test, que es ideal para los ordenadores porque las divisiones por $M_p = 2^p-1$ en sistema binario son muy rápidas, se ha refinado computacionalmente con técnicas tales como el uso de Transformadas rápidas de Fourier para multiplicar a gran velocidad. El soporte informático para los cálculos fue coordinado por el programa GIMPS (Great Internet Mersenne Prime Search) que, desde su fundación en 1996, ha ganado todos los años el "Oscar al mayor número primo". Así fue como se probó que el número $2^{6972593}-1$ es primo.

A

11. ALGUNAS NOTAS CURIOSAS

Finalicemos con algunas propiedades elegantes y otras notas curiosas, sobre estos curiosos y elegantes números:

1) El primer test de primalidad de la Historia fue la archifamosa Criba de Eratóstenes.

2) Veamos otra curiosa forma de averiguar si un número n es primo o compuesto. Formemos el triángulo de Pascal:

```
                1
              1   1
            1   2   1
          1   3   3   1
        1   4   6   4   1
      1   5   10  10  5   1
    1   6   15  20  15  6   1
```

Para ver que 7 (n) es primo, restemos y sumemos 1, alternativamente, a los números de la fila 7 (n). Obtenemos la secuencia: 0, 7, 14, 21, 14, 7, 0. Como todos éstos números son múltiplos de 7 (n), concluimos que 7 (n) es un número primo. Si al menos uno de ellos no fuese múltiplo de n, concluiríamos que n es compuesto.

3) Una lista de diez primos consecutivos y reversible (1193 y 3911 son ambos primos):

1193, 1201, 1213, 1217, 1223, 1229, 1231, 1237, 1249, 1259

4) Todos los números capicúas con un número para dígitos son múltiplos de 11. Luego, el único de estos números que es primo es el 11. Pero sí existen primos capicúas con un número impar de cifras. Por ejemplo: 10301 y 98689 son el menor y el mayor primo capicúa de cinco cifras (¡para jugarlos en la lotería!).

5) Ya comentamos que a un primo p tal que $2 \cdot p+1$ también es primo se le llama un primo de Sophie Germain. Y también se dijo que a una secuencia recursiva de primos de Sophie Germain (cada uno es el doble del anterior más uno) se le llama cadena de Cunningham. Aquí va la cadena de Cunningham más larga que se conoce (14 primos):

$$p_1 = 1437482924225328303 9 , \ldots , p_{14} = 1177586011525389009223679$$

6) El último "año primo" fue el año pasado 1999, el anterior fue su gemelo 1997. ¿Existen infinitas parejas de primos gemelo $(p,p+2)$?

7) El próximo "año primo" será el 2003. Así que tenemos (1997, 1999, 2003), una tripleta de números primos (tres primos consecutivos tales que la diferencia entre el mayor y el menor es de 6). ¿Existen infinitas tripletas de números primos de las formas $(p,p+2,p+6)$ o $(p,p+4,p+6)$?

8) Al dividir un primo p (impar) por 4 sólo podemos obtener resto 1 ó 3. Pues bien:

p es congruente con 1 (mod.4) si y sólo si p es suma de dos cuadrados perfectos

Por ejemplo:

$$5 = 1^2 + 2^2 \quad \text{y} \quad 1997 = 29^2 + 34^2$$

Recordemos que todo número natural es suma, a lo más, de 4 cuadrados perfectos.

9) Hay muchas fórmulas que ligan los números primos con el número π, como la identidad de Euler:

$$\prod_{p\,PRIMO} \frac{p^2}{p^2-1} = \frac{2^2}{2^2-1} \cdot \frac{3^2}{3^2-1} \cdot \frac{5^2}{5^2-1} \cdot \frac{7^2}{7^2-1} \cdot \frac{11^2}{11^2-1} \cdot \frac{13^2}{13^2-1} \cdots\cdots = \frac{\pi^2}{6}$$

10) De la anterior expresión se deduce que la probabilidad de que dos números naturales, elegidos al azar, sean coprimos es precisamente $6/\pi^2 \cong 60.79\%$.

11) Mientras que la sucesión de sumas parciales de la serie armónica es un infinito equivalente a log$n$, las sumas parciales de la serie de los recíprocos de los primos crecen a infinito como log(log n).

12) Además del Teorema del número primo, existen muchas otras relaciones que ligan los números primos con el logaritmo natural. Por su belleza y simplicidad citamos la siguiente fórmula de Moser. Denotemos por $f(n)$ el número de representaciones del natural n como suma de uno o más primos consecutivos. Por ejemplo $f(41) = 3$ porque:

$$41 = 11 + 13 + 17 = 2 + 3 + 5 + 7 + 11 + 13$$

A

Se verifica:

$$\lim_{N\to\infty} \frac{f(1) + f(2) + \ldots + f(N)}{N} = \log 2 = 0.6931471805\ldots$$

o sea: ¡el promedio del número de particiones en primos consecutivos tiende a log 2! El resultado de Moser expresa una elegante propiedad de la distribución de los números primos y confirma el Teorema de Euclides sobre la infinitud de éstos.

13) ¡¡¡El número de curiosidades sobre primos que hemos citado aquí es primo!!!

REFERENCIAS

APARICIO, E. (1993). *"Teoría de los Números"*. Ed. Universidad del País Vasco. Bilbao.

DAVIS, P.J. y HERSCH, R. (1988). *"Experiencia Matemática"*. Centro de Publicaciones del M.E.C. y Ed. Labor, S.A. Barcelona.

DUNHAM, W. (1995). *"El Universo de las Matemáticas"*. Ed. Pirámide, S.A. Madrid.

LÓPEZ, F. y TENA, J. (1990). *"Introducción a la Teoría de Números Primos (aspectos algebraicos y analíticos)"*. Instituto de Ciencias de la Educación. Universidad de Valladolid. Valladolid.

PETERSON, I. (1992). *"El turista matemático"*. Ed. Alianza Editorial, S.A. Madrid.

RIESEL, H. (1994). *"Prime Numbers and Computer Methods for Factorization"*. Ed. Birkhäuser. Boston.

SIERPINSKI, W. (1988). *"Elementary Theory of Numbers"*. Ed. North-Holland. Amsterdam.

STEWART, I. (1988). *"Conceptos de matemática moderna"*. Ed. Alianza Universidad. Madrid.