# GRANDES NUMEROS PRIMOS

Por THÖGER BANG[1]

En las escuelas danesas la teoría de los números se ha ido restringiendo gradualmente hasta no incluír sino la demostración de la descomposición unívoca de los números enteros en números primos y la demostración del teorema clásico de EUCLIDES sobre la existencia de un número primo arbitrariamente grande.

Desde hace menos de un año el pénsum incluye también el teorema de FERMAT: *Si* p *es primo, entonces* p *divide a* $a^p - a$, *cualquiera que sea el valor de* a. Respecto de lo que sigue debo recordar una demostración de este teorema, frecuentemente empleada. Del desarrollo binomial se tiene

$$(a+1)^p - (a+1) = a^p - a + \\ + \left[ \binom{p}{1} a + \binom{p}{2} a^2 + \ldots + \binom{p}{p-1} a^{p-1} \right],$$

que muestra que si $p$ divide a $a^p - a$, también dividirá a $(a+1)^p - (a+1)$, pues para $0 < j < p$ todos los coeficientes binomiales

$$\binom{p}{j} = \frac{p\,(p-1)\ldots(p-j+1)}{j\,(j-1)\ldots 2.1}$$

evidentemente contienen a $p$ como factor primo. De allí se prueba el teorema por inducción, pues inmediatamente se ve que es válido para $a = 1$.

Aunque se sabe que existen infinitos números primos[2], no se puede dar concretamente una serie infinita de ellos. En toda época

---

[1] Conferencia llevada a cabo en marzo de 1953 en la Asociación de Profesores de Matemáticas de las Escuelas y Seminarios de Dinamarca. Traducido de Nordisk Matematisk Tidskrift, vol. 2 (1954), pp. 157-169, por OTTO DE GREIFF.

[2] Ver Vol. II., pp. 15-16 y pp. 21-22 de esta Revista. (N. del T.).

ha habido un número primo máximo conocido; dos famosos de tales "récords" entre los números primos son el número de EULER

$$2^{31} - 1 = 2147483647$$

y el de LUCAS

$$2^{127} - 1 = 1701\ 41183\ 46046\ 92317\ 31687\ 30371\ 58841\ 05727.$$

Diré algo más aquí sobre cómo se pueden determinar tales grandes números primos, y sobre el "récord" actual.

No tiene nada de casual el hecho de que ambos números mencionados sean de la forma $2^n - 1$, es decir una potencia de 2 disminuída de 1, pues los números de esta forma son, como vamos a verlo, particularmente fáciles de investigar. En el caso de que $2^n - 1$ sea primo, lo designaremos abreviadamente por $M_n$. Ya EUCLIDES se interesó por los números $M_n$, y mostró en el pasaje final de sus libros sobre teoría de los números (IX, 36) que si $2^n - 1$ es primo, entonces $2^{n-1}(2^n - 1)$ es un "número perfecto", es decir, un número que es igual a la suma de sus divisores propios. Por ejemplo, si se tiene $M_2 = 3$, esto nos da el número perfecto 6 (que tiene como divisores propios 1, 2 y 3, cuya suma es 6); otro número primo es $M_3 = 7$, que conduce al número perfecto 28 (cuyos divisores 1, 2, 4, 7 y 14 suman 28). Mucho tiempo después EULER mostró que no existe ningún otro número perfecto par que no sea del tipo dado por EUCLIDES. Que haya números perfectos impares es hasta hoy una cuestión no resuelta; si los hay, deben en todo caso ser bastante grandes y complicados de formar.

Antiguamente se conocían en todo caso los primeros números primos $M_n$, a saber

$$M_2 = 3, M_3 = 7, M_5 = 31, M_7 = 127.$$

Se tienen manuscritos de la Edad Media, en los que se ha continuado esta serie, en la creencia de que todos los valores impares de $n$ conducían a números primos $M_n$, así $2^9 - 1 = 511, 2^{11} - 1 = 2047$, $2^{13} - 1 = 8191, \ldots$ En el Renacimiento, entre tanto, se concluyó que esto es erróneo, pues $511 = 7 \times 73$ y $2047 = 23 \times 89$, mientras $M_{13}$ es realmente número primo, hallándose también los dos siguientes números primos $M_n$, a saber $M_{17}$ y $M_{19}$.

Estos son números de seis cifras, y por lo tanto es practicable su investigación por medio de división por todos los números primos hasta la raíz cuadrada. Pero para números grandes la labor por este

método es altamente dispendiosa; hay otros, que fueron creados cuando FERMAT (1601-1665) fundó la teoría de los números propiamente dicha.

En primer lugar debe advertirse que $2^n - 1$ sólo puede ser número primo cuando el exponente mismo $n$ es también número primo, pues si $n = pq$, entonces $2^n - 1 = (2^p)^q - 1$ será divisible por $2^p - 1$. Esto concuerda con lo dicho, pues $2^9 - 1 = 511$ es divisible por $2^3 - 1 = 7$ (y da también base para tener en cuenta solamente los valores impares de $n$, para $n > 2$). En todo lo que sigue, en consecuencia, supondremos que $n$ es un número impar primo. Pero el ejemplo $n = 11$ muestra que *la condición de que* n *sea un número impar primo no es suficiente para afirmar que* $2^n - 1$ *es primo*. Se ve cómo justamente trabajando con estos problemas llegó FERMAT al teorema mencionado al comienzo, y es seguro que por medio de él mostró que cuando $n$ es primo los divisores enventuales de $2^n - 1$ son de la forma $hn + 1$, donde $h$ designa un número entero; como los divisores son impares y $n$ es impar, se deduce que $h$ debe ser un número par. Se ve cómo esto está de acuerdo en el caso de los divisores de $2^{11} - 1$, que son $23 = 2 \times 11 + 1$ y $89 = 8 \times 11 + 1$. En la continuación de los trabajos de FERMAT varias condiciones fueron establecidas por EULER (1707-1783), que entre otras cosas muestran que estos divisores eventuales deben ser además de las formas $8h - 1$ u $8h + 1$ (siendo $h$ un número entero); el divisor 23 es del primer tipo, mientras 89 es del segundo.

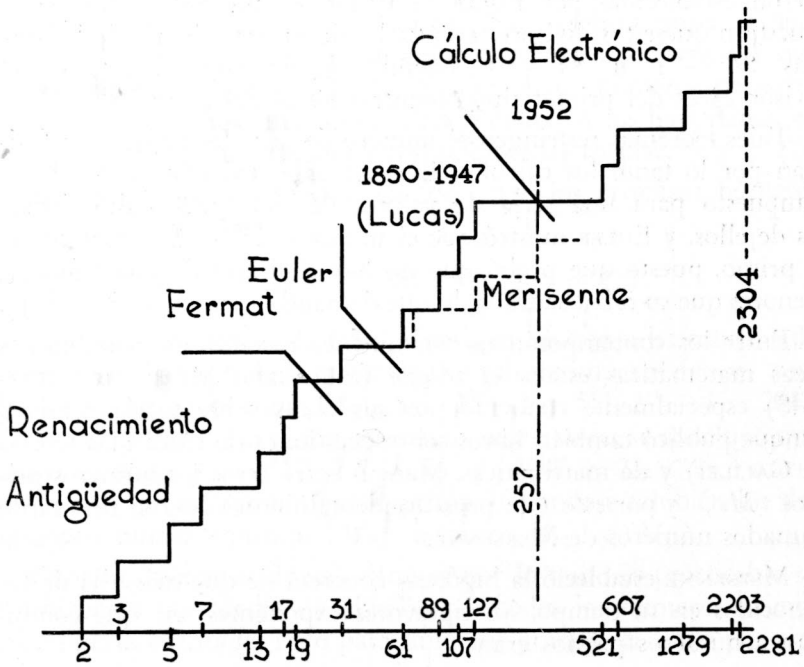
Tales teoremas restringen el número de posibles divisores y facilitan por lo tanto los cálculos. FERMAT encontró que $2^n - 1$ es compuesto para una serie de valores de $n$, pues halló divisores de ellos, y EULER mostró que el número $2^{31} - 1$ antes citado es primo, puesto que probó que no hay divisores de este número, menores que su raíz cuadrada, lo que demanda varios días de trabajo.

Entre los contemporáneos con quienes FERMAT intercambió sus ideas matemáticas estaba el monje franciscano MERSENNE (1588-1648) especialmente conocido por sus obras sobre teoría musical, aunque publicó también libros sobre cuestiones de física (las teorías de GALILEI) y de matemáticas. Manejó entre otros los números primos $M_n$, y por esto (un poco accidentalmente) fueron más tarde llamados números de MERSENNE.

MERSENNE estableció la hipótesis concreta de que más allá de los conocidos en su tiempo, los siguientes exponentes $n$ que conducían a números primos eran

y tenía la hipótesis general de que los valores convenientes estaban en las cercanías de potencias de 2. El valor 31 fue, como se dijo, corroborado por EULER más de cien años después, y en 1947, como se verá, se completó una investigación sobre todos los números hasta 257; muestran ellas que, de los otros tres propuestos hay uno correcto (127) y dos incorrectos. Por otra parte la hipótesis expresa una idea correcta, por cuanto los números rápidamente van haciéndose más escasos en la serie; en realidad, entre 31 y 257 (inclusive) no hay cuatro sino cinco valores convenientes entre los 45 números primos que se encuentran en este trecho.

Antes de seguir adelante construyamos una gráfica de los exponentes $n$. En la figura de esta página se toman las $n$ como abscisas y como ordenadas el número de los números de MERSENNE con exponentes menores que o iguales a $n$. Se obtiene por tanto como curva una línea en escalera, que salta en una magnitud 1 en los puntos que corresponden a los exponentes utilizables. Pero como éstos rápidamente llegan a distanciarse notablemente, hemos empleado en el eje de las abscisas una *escala logarítmica* con el fin de obtener una figura razonable.



En esta figura se aprecia qué pequeña fue la labor alcanzada en el período brillante de la teoría clásica de los números (1600-1800), que sólo logró el escaso avance de un peldaño frente a los siete previamente existentes; pero para apreciar la contribución precedente hay que considerar la escala logarítmica. Con esta base la adición de los últimos tiempos a la curva resulta sumamente imponente. Con trazo punteado se inicia la hipótesis de MERSENNE; y se ve que aunque sólo se da una parte de la curva, que en parte resulta correcta.

Con el número de EULER $M_{31}$ el resultado para el mayor número primo conocido fue conquistado entre los números de MERSENNE, y este resultado desde entonces, con excepción del corto período 1951-1952 (véase pág. 56), se ha mantenido. Pero primero debió transcurrir casi un siglo antes de que aquel resultado fuera mejorado.

Alrededor de 1800 hábiles calculistas hallaron factores del siguiente número $2^n - 1$, y en 1886 SEELHOFF probó que $M_{61} = 2^{61} - 1$ divide a $3^{M_{61}} - 3$, y concluyó aplicando el teorema de FERMAT que $M_{61}$ es número primo. Pasado algún tiempo se hicieron oír voces que advertían que el teorema de FERMAT sólo da una condición necesaria pero no suficiente para que un número fuera primo; desde entonces se han emprendido las investigaciones suplementarias para demostrar que $M_{61}$ es realmente un número primo. Otra falla en la hipótesis de MERSENNE fue mostrada por F. N. COLE quien hacia 1900, en una conferencia anunciada en la American Mathematical Society, nada dijo al respecto, pero en una clase adicional calculó con auxilio de tablas

$$1937\ 07721 \times 76\ 18382\ 57287 \quad \text{y} \quad 2^{67}.$$

El último número es mayor que el primero en una unidad, y por lo tanto $n = 67$ no corresponde a exponente de un número de MERSENNE; es característico en este cálculo el que desgraciadamente un control efectivo resulta tan prolongado como el cálculo aritmético mismo.

Pero anteriormente, en 1876, había ocurrido algo mucho más importante en la teoría de los números de MERSENNE. El nombre principal entonces es el de LUCAS (1842-1891), matemático francés, más conocido por otra parte por sus libros sobre matemáticas de los juegos y matemáticas recreativas.

También LUCAS se había sentido incomodado por el hecho de que el teorema de FERMAT sólo procurara un camino, e ideó en con-

secuencia un teorema que da una condición necesaria y suficiente para que $2^n - 1$ sea número primo. En el teorema de FERMAT (después de una obvia división por $a$) interviene la cantidad [3] $p - 1$, mientras que para un número $p$ de MERSENNE evidentemente es la cantidad $2^n = p + 1$ la cual debe entrar en un criterio sencillo y es ésta que usó LUCAS en su teorema. Vamos a demostrar éste, comenzando con algunas consideraciones generales.

Supongamos que existen dos sucesiones $C_m$ y $S_m$ de números enteros, $m = 1, 2, \ldots$, que satisfacen las fórmulas

$$S_{m\pm l} = S_m\, C_l \pm S_l\, C_m \tag{1}$$

y

$$C^2_m + aS^2_m = 1, \tag{2}$$

donde $a$ es un número entero $\neq 0$. Se tiene

TEOREMA I. *Todos los índices* r, *para los cuales* $S_r$ *es divisible por un cierto número primo impar* p, *son (en caso de que realmente se encuentre alguno) justamente todos los múltiplos del menor de dichos índices* $r_0$.

Puesto que poniendo $l = r_0$ en (1) y empleando signo positivo se ve que con $S_m$ también $S_{m+r_0}$ es divisible por $p$, y por lo tanto con $S_{r_0}$ también $S_{2r_0}$, $S_{3r_0}$, ... son divisibles por $p$. Y aceptando que además de estos índices se encuentre aún un índice $r$ tal que $hr_0 < r < (h+1)\, r_0$ ($h$ entero), que gozara de la propiedad, entonces en (1) se puede poner con signo negativo $m = r$ y $l = hr_0$, y se tendrá que $r - hr_0$ también goza de la propiedad, en oposición a que $r_0$ fuera el mínimo valor.

TEOREMA II. *Todos los índices* r *para los cuales* $C_r$ *es divisible por un número dado primo impar* p *son justamente todos los múltiplos impares de* $r_0/2$, *donde* $r_0$ *es el índice mencionado en el teorema* I (*ya que tales índices* r *ocurren sólo si existe un* $r_0$, *y que éste sea número par*).

Puesto que con $m = l = r$ en (1) se tiene $S_{2r} = 2S_r\, C_r$; por consiguiente si $p$ divide a $C_r$, $p$ en consecuencia divide a $S_{2r}$, y por lo tanto $2r$ es un múltiplo de $r_0$, y si viceversa $2r$ es un múltiplo de $r_0$, entonces $p$ divide a $C_r$ o a $S_r$. Pero

[3] Es decir el teorema de FERMAT se puede enunciar también en la forma siguiente: Si $p$ no divide a $a$, entonces divide $a^{p-1} - 1$. N. del T.).

(2) muestra que $p$ no puede dividir al mismo tiempo a $C_r$ y a $S_r$. Concordando estas aclaraciones se obtiene el teorema II.

Las fórmulas (1) y (2) recuerdan fórmulas trigonométricas conocidas; y podemos transformarlas poniendo

$$(3) \qquad C_m = \cos mt\,,\ S_m = \frac{\operatorname{sen} mt}{\operatorname{sen} t} \quad \text{y} \quad a = \operatorname{sen}^2 t = 1 - \cos^2 t\,.$$

Obtenemos así un ejemplo en que las dos sucesiones $C_m$ y $S_m$ satisfacen (1) y (2), con sólo elegir un valor para $t$ y así utilizar la definición (3). Si se pide que las sucesiones deben constar de números enteros, automáticamente se cumplirá esto cuando simplemente $C_1 = \cos t$ sea entero, pues es sabido (lo que se puede probar por inducción) que

$$(4) \qquad \cos mt = P(\cos t) \quad \text{y} \quad \frac{\operatorname{sen} mt}{\operatorname{sen} t} = Q(\cos t)\,,$$

donde $P(\cos t)$ y $Q(\cos t)$ son polinomios en $\cos t$ con coeficientes enteros.

Deseamos utilizar adelante un valor de $t$ para el cual

$$\cos t = 2\,.$$

Así abandonamos la trigonometría elemental, pero las funciones trigonométricas pueden prolongarse en funciones de variable compleja, y para determinados valores de esta variable puede el coseno tomar el valor 2. Lo esencial para nosotros es que también para variables complejas sea válido todo el formulario habitual, tal como (1), (4) y (2), donde ahora $a = -3$. Además, se encuentran fórmulas que dan relaciones entre las funciones exponenciales y las trigonométricas, a saber, por ejemplo

$$e^{iz} = \cos z + i \operatorname{sen} z \quad \text{y} \quad \cos z = \frac{1}{2}(e^{iz} + e^{-iz}).$$

Elegimos ahora $t$ tal que

$$(5) \qquad e^{it/2} = \sqrt{\frac{3}{2}} + \sqrt{\frac{1}{2}}$$

y por lo tanto

(6) $$e^{-it/2} = \sqrt{\frac{3}{2}} - \sqrt{\frac{1}{2}}\,.$$

De aquí se tiene

$$e^{it} = 2 + \sqrt{3} \quad \text{y} \quad e^{-it} = 2 - \sqrt{3}$$

tal que $\cos t = 2$, como arriba se menciona. Además se tendrá

$$\cos pt = \frac{1}{2}(e^{pit} + e^{-pit}) = \frac{1}{2}[(2+\sqrt{3})^p + (2-\sqrt{3})^p].$$

Si se desarrolla según la fórmula binomial, las potencias impares de $\sqrt{3}$ se eliminarán, lo que da

$$\cos pt = \sum_{j \text{ par}} \binom{p}{j} 2^{p-j} (\sqrt{3})^j.$$

Si ahora se supone, como antes, que $p$ es un número primo impar, entonces, (ver pág. 45) dividirá todos los coeficientes binomiales que ocurran, excepto $j = 0$, y por lo tanto $p$ dividirá a $\cos pt - 2^p$. Como por el teorema de FERMAT se ve que $p$ divide a $2^p - 2$, y como $2 = \cos t$, se obtiene el

TEOREMA III. *Si* p *es número impar, divide a* cos pt - cos t.

Por otra parte se ve casi inmediatamente que la demostración y el teorema son válidos cuando $\cos t$ es un número entero cualquiera. Este teorema general puede entenderse como la formulación trigonométrica del teorema de FERMAT.

Del teorema III se sigue que $p$ dividirá a

$$\cos pt - \cos t = -2 \operatorname{sen} \frac{p+1}{2} t \,.\, \operatorname{sen} \frac{p-1}{2} t = 6 S_{\frac{p+1}{2}} \,.\, S_{\frac{p-1}{2}},$$

y esto, en combinación con el teorema I, conduce al

TEOREMA IV. *Para todo número primo* $p > 3$ *existe un índice* $r_0$ *(de la forma mencionada en el teorema I), y éste divide a* $(p+1)/2$ *o a* $(p-1)/2$.

Después de estos preparativos podemos demostrar el teorema de Lucas.

Teorema Principal. *Sean:* $n > 1$ *un número impar y* $\cos t = 2$. *La condición suficiente y necesaria para que* $2^n - 1$ *sea número primo es que* $2^n - 1$ *divida a* $C_{2}^{n-2} = \cos(2^{n-2}t)$.

Que la condición es suficiente se ve así: sea $p$ un divisor primo de $2^n - 1$; no puede ser 2, ni, puesto que $n$ es impar, tampoco 3. En virtud del teorema IV a $p$ corresponderá un $r_0$, y en virtud del teorema II es $2^{n-2}$ igual a un múltiplo impar de $r_0/2$; aquí el factor impar debe ser 1, y $r_0$ en consecuencia igual a $2^{n-1}$. Se ve por el teorema IV que $r_0$ divide a $(p \pm 1)/2$ y $p \pm 1$ es por lo tanto un múltiplo de $2^n$. Puesto que $p \leqslant 2^n - 1$ queda la única posibilidad de que $p$ mismo sea igual a $2^n - 1$, que así es un número primo.

Se ve que esta prueba de que la condición es suficiente puede ser efectuada sin alteración, independientemente del número que se haya escogido como valor de $\cos t$, cuando simplemente $-a = (\cos t - 1)(\cos t + 1)$ es primo con $2^n - 1$. La prueba de que la condición es necesaria, la cual vamos a dar ahora, toca por otra parte con las propiedades del número 2 en la teoría de los números en cuanto a que aquel puede ser reemplazado por ciertos otros enteros, por ejemplo 26.

Sea $p$ un número primo impar. Utilizando (5) y (6) se tiene

$$2\cos\frac{p+1}{2}t = e^{(p+1)it/2} + e^{-(p+1)it/2} =$$

$$\left(\sqrt{\frac{3}{2}}+\sqrt{\frac{1}{2}}\right)^{p+1}+\left(\sqrt{\frac{3}{2}}-\sqrt{\frac{1}{2}}\right)^{p+1}.$$

Al desarrollar los términos por la fórmula binomial se eliminan entre sí las potencias impares de $\sqrt{1/2}$, dando

$$2^{(p+1)/2}\cos\frac{p+1}{2}t =$$

$$= 2^{(p+1)/2}\sum_{j\ \text{par}}\binom{p+1}{j}\left(\sqrt{\frac{3}{2}}\right)^{j}\left(\sqrt{\frac{1}{2}}\right)^{p+1-j} =$$

$$= \sum_{l=0}^{(p+1)/2}\binom{p+1}{2l}3^{l}.$$

Exactamente de la misma manera como se probó al demostrar el teorema de FERMAT, se ve que $p$ divide todos los coeficientes binomiales que aparecen, con excepción del primero y del último, que son ambos iguales a 1; y $p$ por lo tanto divide a

$$2^{(p+1)/2} \cos \frac{p+1}{2} t - 3^{(p+1)/2} - 1 =$$

(7)

$$= 2^{(p+1)/2} (\cos \frac{p+1}{2} t + 1) - [2^{(p+1)/2} + 3^{(p+1)/2} + 1].$$

Suponiendo ahora que $2^n - 1$ sea un número primo impar $p$, un cálculo sencillo demuestra que $p$ es de la forma $24h + 7$, donde $h$ es un entero. Para completar la demostración podemos ahora utilizar la teoría clásica de los residuos cuadráticos. Para la forma especial referida de $p$ es 2 residuo cuadrático, mientras que 3 no lo es, o sea

$$2^{(p-1)/2} \equiv 1 \ (mod p), \ 3^{(p-1)/2} \equiv -1 \ (mod p).$$

De aquí se deduce que $p$ divide el último paréntesis de (7), y que $p$ en consecuencia dividirá también a

$$\cos \frac{p+1}{2} t + 1 = 2 (\cos \frac{p+1}{4} t)^2$$

y por lo tanto a $\cos [(p+1)\, t/4] = \cos (2^{n-2} t)$, con lo cual queda demostrado el teorema.

Los trabajos de LUCAS en donde aparecen teoremas y cuestiones del mismo tipo son muy difíciles de entender (sobre que las condiciones del teorema sean o no necesarias, por ejemplo, nada dice), y entre los matemáticos el teorema durante mucho tiempo ha jugado un papel mal juzgado. Sólo durante la última generación han aparecido varias demostraciones exactas (entre otras una de D. H. LEHMER quien —lo mismo que antes su difunto padre D. N. LEHMER— ocupa una posición de comando en el terreno de los calculistas de la teoría de los números). El desarrollo aquí expuesto se basa poco en aquellas demostraciones, pero está construído sobre una idea mencionada en sólo un lugar en LUCAS.

En todo caso LUCAS y otros emplearon teoremas para hallar nuevos números de MERSENNE. Los valores $n = 89$, 107 y 127 dan números primos $M_n$. El último de éstos, cuyas 39 cifras están transcritas en la pág. 46 fue encontrado ya por LUCAS en 1876.

Cuando se ha presentado un resultado tal de un cálculo semejante, puede dudarse de su exactitud, pero aquí se considera como muy improbable que una falla de cálculo pueda dar un número que divida a otro de 39 cifras, por ejemplo. Es más dudoso afirmar con ayuda de teoremas, que un número no es primo porque las divisiones no dan resultado; además hay una notable situación por cuanto *hay números que por demostración se sabe que son compuestos, pero de los cuales no se conoce ningún divisor.*

Pero veamos un poco más por qué el teorema significa un progreso en los cálculos. Si se quiere probar con posibles divisores hasta la raíz cuadrada del número, para comprobar si $2^n - 1$ es primo, el trabajo crecerá exponencialmente con $n$, aunque se tome en consideración la facilidad arriba mencionada. Una investigación tal para el número $M_{127}$ daría trabajo completo durante algunos siglos a toda la humanidad, suponiéndola formada sólo por hábiles calculistas, y requeriría un recipiente de tinta de las dimensiones del Lago Negro (Sordedamssoen) en Copenhague[4].

El teorema de Lucas requiere por lo tanto solamente el conocimiento de las sucesiones de números $C_2, C_4, C_8 \ldots$. y éstas pueden con facilidad ser formadas sucesivamente, mediante $C_{2j} = 2C^2_j - 1$ (fórmula para el coseno del ángulo doble). Una inspección de $2^n - 1$ requiere en consecuencia esencialmente sólo $n$ elevaciones al cuadrado. Aquí se puede sin embargo observar que la sucesión $C_2, C_4, \ldots$ crece tan grandemente que apenas puede hablarse de escribir sus elementos más allá de los primeros diez o doce. En la práctica se puede, en consecuencia, en la investigación de un determinado $M_n = 2^n - 1$, tomar siempre el residuo $R$, obteniendo así por división con $M_n$ la forma $2R^2 - 1$, y no tomando residuos, etc. En total se ejecutarán por consiguiente $n - 3$ elevaciones al cuadrado de residuos de división (cada uno de los cuales puede ser de la misma magnitud que $M_n$) y además igualmente muchas divisiones de $M_n$. Este trabajo, considerándolo todo, es proporcional a $n^3$ y crece en consecuencia mucho más lentamente con $n$ que en el método anterior. Lucas pudo solo, y en el curso de algunos meses, emprender el cálculo de $M_{127}$.

La resolución por los residuos de división es la mitad del trabajo, pero esto condujo a emprender cálculos en el *sistema binario.*

---

[4] De acuerdo con informaciones del autor, este lago de Dinamarca tiene una capacidad de $10^6$ metros cúbicos, es decir, un millón de metros cúbicos, lo que equivale a un cubo que tuviera de base una hectárea, o sea un cuadrado de 100 metros de lado. (N. del T.).

En éste el número $2^n - 1$ se escribe $11 \ldots 11$ ($n$ unos); y por este mismo simple método se muestra en el sistema decimal que 376249 dividido por 999 da como residuo 376 + 249. Para algunos $M_n$ existen cálculos en el sistema binario impresos en forma de hojas cuadradas provistas de cruces que marcan los números unos, mientras que los ceros no son dados.

Ultimamente se emplearon las máquinas ordinarias de cálculo, y gradualmente se logró investigar (H. S. UHLER) todos los números $2^n - 1$ hasta el límite de MERSENNE, $n = 257$, que fue completado en 1947. Es este un largo y fatigoso trabajo. Por una parte no se puede confiar en los cálculos, y hay que someterlos a toda clase de control. Por otra parte, estas máquinas calculan en el sistema decimal, que es menos adecuado para este propósito. Y finalmente las máquinas no pueden trabajar directamente con los números de gran magnitud (hasta de 78 cifras) sin que giren hasta la posición inicial; con la multiplicación no es esto tan absurdo, pues simplemente se pueden repartir los números en menores grupos de cifras, que se multiplican conjuntamente, pero las divisiones dan algunas molestias. Se hallaron así pocos números primos.

Las máquinas electrónicas de cálculo han abierto nuevas posibilidades. En Inglaterra se hizo la prueba de ir más allá del límite de MERSENNE; se llegó hasta $n = 450$ aproximadamente pero sin encontrar ningún número primo. Como mientras tanto había interés en establecer un "récord", se utilizó en 1951 el número $M_{127}$ de LUCAS para hallar algunos números primos, ninguno de los cuales mayor que aquél, y ninguno de ellos número de MERSENNE (el conocimiento sobre un número primo se obtiene al relacionarlo con el "próximo", empleando el teorema de FERMAT para la condición necesaria y suficiente de que el número sea primo).

Un trabajo de cálculo aun más grandioso y también más fecundo en resultados ha sido llevado a cabo en el curso del año 1952 con una máquina llamada SWAC, en Los Angeles. Esta, como todas las máquinas electrónicas modernas de cálculo, trabaja en el sistema binario, y por la razón antes mencionada las investigaciones sobre los números de MERSENNE con el auxilio del criterio de LUCAS dan obviamente un trabajo sumamente adecuado para tal máquina. Se han controlado todos los resultados previos y se ha proseguido sistemáticamente con todos los posibles exponentes $n$ de MERSENNE. Por razones de control todos los cálculos se efectúan por lo menos dos veces con un intervalo mínimo de una semana, para no cometer un error opuesto, independientemente (sea por la máquina o por quienes la mane-

jan); además la máquina es revisada antes de rendir informe, y los cálculos son efectuados casi como "tiempo libre de trabajo" de la máquina.

La máquina calcula rápidamente; el número $M_{127}$ de LUCAS puede ser controlado en un par de segundos, y la duración del examen de un $M_n$ es del orden de magnitud de $10^{-6}.n^3$ segundos. Una comparación con la duración sin auxilio mecánico lleva a considerar la contribución de la máquina como equivalente al factor $10^{-6}$.

Se ha comprobado que hay una laguna sorprendentemente grande en la serie de los exponentes de MERSENNE después de 127, como que los dos siguientes, que fueron encontrados en enero de 1952, son 521 y 607. Más tarde en ese año se encontró el 1279, y finalmente en octubre los dos más grandes exponentes hasta entonces conocidos, 2203 y 2281. En consecuencia se conocen en total 17 números de MERSENNE; sus exponentes están dados en la figura de la página 48.

Se podría creer que sólo basta seguir calculando así pero la cosa no es tan sencilla. En realidad se llevó a cabo un programa que iba hasta el estudio de los posibles valores de $n$ hasta 2304, y fue sumamente interesante ver que hasta este límite sólo se hallaron dos exponentes más.

Cuando se establece un límite, naturalmente se tiene en cuenta que el trabajo va creciendo gradualmente; una única investigación del exponente 2281 dura así 66 minutos, que con la medida pecuniaria establecida para una máquina electrónica de cálculo no es ciertamente insignificante. Pero el límite mencionado fue también fijado de acuerdo con la construcción misma de la máquina. La máquina en cuestión es de un tipo de "memoria" muy rápida en la acción, pero por otra parte comparativamente pequeña; puede abarcar hasta 256 números de 36 cifras (en el sistema binario). La mitad de la memoria debe reservarse para fines de control y dirección en los cálculos, y en las circunstancias ordinarias del cálculo un residuo $R$ de división debe llenar a lo sumo una cuarta parte de la memoria, que para $n$ da el límite señalado $\frac{1}{4} \times 36 \times 256 = 2304$.

Se ha hecho por diversión el cálculo de $M_{2281}$ en el sistema decimal, y aunque pueda decirse que es esta una cuestión indiferente, voy sin embargo a mostrar cómo se ve este hasta ahora máximo número primo conocido. Tiene 687 cifras, como sigue:

$2^{2281} - 1 =$ 44 60875 57183 75842 95711 51706 40210 18098
86208 63241 28599 01111 99121 99634 04685 79282 04733 69112
54526 90039 89026 15324 59311 24316 70239 57587 05693 67936
47909 03497 46114 70710 65254 19335 39381 24978 22630 79473
12410 79887 48690 40070 27932 84288 10311 75484 41080 94878
25249 48667 60969 58699 81289 82645 87759 60289 79171 53696
25030 68429 61733 17021 84750 32458 30091 71832 10491 60501
57628 88660 63721 45501 70222 59251 25224 07682 96054 27173
57396 48129 95250 56941 24807 20738 47685 52936 81666 71284
48311 90877 62060 67866 63862 19024 01185 70736 83190 18864
79225 81041 47140 78935 38656 24979 68178 72912 76295 94924
41196 09613 86713 94627 98992 75006 95491 71397 58796 06122
38033 93537 38103 46664 94402 95105 20590 47968 69325 53886
47930 44092 51041 86817 00964 01717 64133 17241 81328 36351

Después de haberse calculado tantos exponentes de MERSENNE podría esperarse que el sistema para lograr el cálculo sería evidente. Pero parece que no es éste el caso. Una sola observación, que tiene que ver con la hipótesis antes mencionada de MERSENNE, puede ser ahora expuesta, o sea que los números primos 3, 7, 31 y 127, que son números de MERSENNE, también son exponentes de MERSENNE. Supuesto que esto fuera una ley general se podría concretamente dar una sucesión infinita de números primos, pero sería terriblemente larga su determinación. Calculando las probabilidades puede darse la razonable aunque distante afirmación de que el número de exponentes hasta un límite dado $N$ crece proporcionalmente con $log\ N$; esto significa que la línea escalonada de la figura crece linealmente, lo que parece ser cierto aproximadamente.

Junto con el número de MERSENNE se habla a menudo del "número de FERMAT" como una sucesión de números que contiene grandes números primos. Se entienden estos como números primos de la forma $2^n + 1$. Se conocen cinco números primos de este tipo, siendo el mayor $2^{16} + 1 = 65537$. Se ve fácilmente que $n$ debe ser una potencia de 2, y esto tiene como efecto que, aunque se puede construír una teoría sobre ellos, análoga a la de los números de MERSENNE, ella no tendría tan gran interés, pues la sucesión de números crece rápidamente más allá de lo que es accesible para el cálculo. Los menores números $2^{2^m} + 1$ cuyo carácter de primos es desconocido, provienen de $m = 10$ (éste, sin embargo, es accesible al cálculo electrónico) y de $m = 13$ (éste escasamente lo

es). Se ha probado que sus eventuales divisores tienen la forma $h \cdot 2^{m+2} + 1$, donde $h$ es un número entero, y con ayuda de esto se han obtenido divisores para una serie de valores $m$. Especialmente para $m = 73$ (MOREHEAD) se ha comenzado por encontrar que $5 \times 2^{75} + 1$ es divisor; este resultado puede considerarse como negativo para el problema propiamente dicho, pero por otra parte se ha probado que $5 \times 2^{75} + 1$ es un número primo.

De diversas maneras se han encontrado otros grandes números primos, aunque ninguno de ellos se puede comparar con los mencionados antes. Concluyo dando un ejemplo pintoresco (debido a KRAITCHK), o sea el número de 23 cifras (en el sistema decimal),

$$11111111111111111111111 .$$

*Adiciones y correcciones:*

Como consecuencia de un cálculo de R. M. ROBINSON, quien dirige las investigaciones mencionadas con la SWAC, se ha dado respuesta en 1953 a dos de las cuestiones de que se habló atrás. Con una máquina electrónica de cálculo de la Universidad de Illinois se ha emprendido una investigación de $2^{8191} - 1$ que demuestra (supuesto que no haya habido error de cálculo) que este número no es primo. Como 8191 es el número $M_{13}$ de MERSENNE, refuta esto la hipótesis de que todo número de MERSENNE sirve como exponente de MERSENNE. En la máquina SWAC se ha estudiado posteriormente el número primo eventual de FERMAT $2^{2^m} + 1$, donde $m = 10$, demostrando el cálculo que también este número es compuesto. El resultado será prontamente reafirmado, pues parece que se ha de encontrar un divisor de este número.

*Universidad de Copenhague*