El diablo de los números

Sección a cargo de

Javier Cilleruelo Mateo

Pruebas determinísticas de primalidad

por

Pedro Berrizbeitia

La búsqueda de primos grandes, y en particular de primos de la forma $2^n \pm 1$, es una historia muy antigua. En este artículo contaremos una pequeña parte de esa historia y explicaremos de qué manera la búsqueda de primos de esta familia ha contribuido al desarrollo de resultados más generales.

Los primos del tipo $2^n - 1$ se conocen como primos de Mersenne y los de la forma $2^n + 1$ son llamados primos de Fermat. Nos referiremos a las propiedades de los primeros como **PM** y a las de los segundos como **PF**. Con **PG** nos referiremos a propiedades generales que son aplicables a todo entero positivo.

La primera propiedad de los números de la forma $2^n - 1$ es una observación bien conocida.

PM1: *Si n es compuesto entonces $2^n - 1$ también lo es.*

En efecto, esto se deduce de la identidad algebraica $x^m - 1 = (x-1)(x^{m-1} + ... + x + 1)$, con $x = 2^d$, donde d es un divisor no trivial de $n = md$.

Por lo tanto, la búsqueda de primos de la forma $2^n - 1$ se restringe a los valores primos de n. Para los primeros primos $p = 2, 3, 5, 7$, el número $2^p - 1$ también es primo. Sin embargo, $2^{11} - 1 = 2047$ es un número compuesto, $2047 = 23 \times 89$. Ya en el año 1603, Pietro Cataldi había verificado que $2^{13} - 1, 2^{17} - 1$ y $2^{19} - 1$ son primos, y aventuró que lo mismo ocurría para $p = 23, 29$ y 31. Se equivocó con 23 y 29, como verificó en 1640, Pierre de Fermat.

Para determinar la primalidad de un número se contaba con una sencilla herramienta, conocida ya por Eratóstenes, que llamaremos PG1.

PG1: *Si n es un número compuesto, entonces n tiene un divisor primo que es menor o igual a $\sqrt{n}$.*

Fermat introdujo el famoso resultado conocido como "Pequeño teorema de Fermat", añadiendo una poderosa herramienta al estudio de la primalidad, pues permite, de una forma bastante eficiente, determinar que un número es

compuesto, sin necesidad de conocer ninguno de sus divisores. Lo enunciamos a continuación.

PG2 (Pequeño Teorema de Fermat): *Si p es un número primo, y a es un entero, entonces* $a^p \equiv a \pmod{p}$.

Este resultado es muy conocido, y su demostración se enseña en los primeros cursos de álgebra. Para los propósitos de este artículo, conviene presentar la siguiente demostración: El resultado es trivial si a es múltiplo de p. Si no lo es, entonces el orden de a módulo p es el orden de la clase de a en el grupo multiplicativo $(\mathbb{Z}/p\mathbb{Z})^*$ del cuerpo finito $\mathbb{Z}/p\mathbb{Z}$. Este orden divide al orden del grupo multiplicativo, que es $p-1$, por lo que $a^{p-1} \equiv 1 \pmod{p}$, de donde se obtiene el resultado deseado.

A primera vista el pequeño teorema de Fermat puede no parecer muy útil, pues si n es grande, entonces a^n es inmenso. Sin embargo, lo que se necesita calcular es $a^n \pmod{n}$ y para efectuar ese cálculo, escribiendo el exponente n en base dos, puede deducirse fácilmente que basta efectuar a lo sumo $2\log_2 n$ multiplicaciones módulo n, lo que es laborioso pero posible, aún para valores relativamente grandes de n. La limitación principal de este resultado, si quiere decirse así, es que nunca nos permite concluir que n es primo, sólo sirve para mostrar que es compuesto.

En 1644, en el prólogo de su libro "Cogitata Physica-Matematica", el monje francés Marin Mersenne afirmó que si $p \leq 257$ entonces $2^p - 1$ es primo si, y sólo si, $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ ó 257. A pesar de que la lista de Mersenne también resultó ser incorrecta (ni están todos los que son, ni son todos los que están), los números de la forma $M_p = 2^p - 1$, con p primo, reciben el nombre de números de Mersenne. La lista correcta para $p \leq 257$ no se obtuvo sino hasta 1947, en la era de la computadora.

Desviemos brevemente nuestra atención hacia los números de la forma $2^n + 1$.

PF1: *Si n no es una potencia de 2, entonces $2^n + 1$ es compuesto.*

Esto se deduce de la identidad algebraica $x^{2k+1} + 1 = (x+1)(x^{2k} - ... + x^2 - x + 1)$, con $x = 2^{n/(2k+1)}$, donde $2k+1$ es un divisor impar de n.

Los números de la forma $F_m = 2^{2^m} + 1$, $m \geq 0$, son llamados números de Fermat. Si $m = 0, 1, 2, 3$ ó 4, el número F_m es primo. Fermat conjeturó que F_m es primo para todo m. Estaba equivocado. De los muchos resultados matemáticos que se sabe Fermat anunció, éste es el único que no es correcto. Euler mostró que F_5 es compuesto, y hasta el día de hoy no se ha encontrado ningún otro primo de Fermat aparte de los ya mencionados.

Euler también mostró que M_{31} es primo. Para ello, Euler tuvo que comprobar que M_{31} no tiene divisores primos menores que $\sqrt{M_{31}}$. Sin embargo, encontró propiedades de los números de Mersenne que le permitió restringir la búsqueda de divisores primos a ciertas progresiones aritméticas. Lo que Euler mostró fueron las siguientes dos propiedades.

PM2: *Todo divisor primo q de M_p satisface* $q \equiv 1 \pmod{p}$.

Para ver esto obsérvese que si q es un divisor primo de M_p, entonces se cumple que $2^p \equiv 1 \pmod{q}$. Como $q \neq 2$, resulta que 2 tiene orden p módulo q, por lo que p divide al orden del grupo $(\mathbb{Z}/q\mathbb{Z})^*$, que es $q-1$.

PM3: *Todo divisor primo q de M_p, p primo impar, satisface* $q \equiv \pm 1 \pmod{8}$.

Presentaremos una demostración al final de la siguiente sección.

De las propiedades PM2 y PM3, Euler concluyó que los posibles divisores primos q de M_{31} debían satisfacer $q \equiv 1 \pmod{248}$ o $q \equiv 63 \pmod{248}$. Lo demás fue un cálculo para finalmente verificar que M_{31} es, en efecto, primo.

Euler encontró y demostró propiedades análogas para los números de Fermat, que le permitió luego encontrar un factor primo de F_5 . Estas propiedades, que demostraremos más adelante, se resumen en la siguiente:

PF2: *Todo divisor primo q de F_m, $m \geq 2$, satisface* $q \equiv 1 \pmod{2^{m+2}}$.

El trabajo de Euler fue realizado hacia 1770, más de 100 años después de que Mersenne y Fermat hubieran hecho sus respectivas afirmaciones. Se necesitaba una idea nueva para estudiar la primalidad de los siguientes números de la lista original de Mersenne.

Otros 100 años pasaron, hasta que Eduardo Lucas, en 1876, verificó que M_{127} es primo (el número anterior de la lista de Mersenne, M_{67} resultó ser compuesto). Lucas no hubiera podido realizar esto con la metodología empleada por Euler, pues $\sqrt{M_{127}}$ es demasiado grande. De hecho, la metodología de Euler no puede utilizarse, ni siquiera haciendo uso de las computadoras más modernas. En efecto, Lucas había descubierto una magnífica propiedad de los números de Mersenne, que permitía determinar la primalidad de esos números, sin necesidad de tener que dividir por todos los números primos menores que $\sqrt{M_p}$.

PM4 (Teorema de Lucas): *Sea $S_0 = 4$ y definamos la sucesión S_k, para $k \geq 0$, de la siguiente manera: $S_{k+1} = S_k^2 - 2$. Si $S_{p-2} \equiv 0 \pmod{M_p}$ entonces M_p es primo.*

Con este resultado, y un cálculo que no deja de ser monumental para haber sido hecho a mano, Lucas demostró que M_{127} es primo. Posteriormente, ya en el siglo XX, D. H. Lehmer demostró que la condición de Lucas para determinar la primalidad de M_p también es necesaria. Por ello, el teorema, que da una condición necesaria y suficiente para determinar la primalidad de M_p, se conoce hoy como la Prueba de Lucas-Lehmer. La demostración original que Lucas dio de su teorema se basa en el estudio de las propiedades de las hoy conocidas como sucesiones de Lucas. Varios libros modernos, como [R], [B], [W], presentan ese esquema de demostración. En este artículo daremos una demostración diferente, creemos que más sencilla y clara. Pero antes sigamos con un poco de historia. En 1883, Pervouchine mostró que M_{61}, que no estaba

Eduardo Lucas

en la lista de Mersenne, también es primo. En el siglo XX, Powers mostró que también M_{89} y M_{107} son primos. También estos primos se le habían escapado a Mersenne. Por el contrario, M_{257}, que aparecía en la lista original de Mersenne ha resultado ser un número compuesto. La lista completa de los primos de Mersenne con $p \leq 257$ es la siguiente: $p = 2, 3, 5, 6, 13, 17, 19, 31, 61, 89, 107, 127$. El interés en la búsqueda de primos grandes, y en particular de primos de Mersenne, se ha mantenido hasta nuestros días. Los progresos después de Lucas han consistido principalmente en mejoras en los algoritmos de multiplicación modular, en ingeniosas formas de organizar la búsqueda, y el hallazgo de nuevos primos ha sido posible también gracias al incremento en el poder computacional de las máquinas. El algoritmo de Lucas sigue siendo la clave, presente en todas las búsquedas. Hoy se conocen 38 primos de Mersenne, los 37 primeros son los 37 más pequeños. El último, el primo más grande conocido hasta ahora es $M_{6972593}$, encontrado por Hajratwala, Woltman, Kurowsky *et al,* con el llamado GIMPS (the Great Internet Mersenne Prime Search) en 1999. No se sabe aún si existe algún otro primo de Mersenne entre este primo y el número 37 de la lista.

En 1877, Teófilo Pepin descubrió un resultado análogo a la Prueba de Lucas-Lehmer para los números de Fermat:

PF3 (Prueba de Pepin): *Sea* $m \geq 1$*, sea* $S_0 = 3$ *y definamos la sucesión* S_k*, para* $k \geq 0$*, de la siguiente manera:* $S_{k+1} = S_k^2$*. Entonces* F_m *es primo si, y sólo si,* $S_{2^m-1} \equiv -1 \pmod{F_m}$.

Este algoritmo, a pesar de ser tan eficiente como el de Lucas-Lehmer, no ha servido para encontrar nuevos primos de Fermat. De hecho, se tienen pocas esperanzas de encontrar más. La demostración de este teorema es bastante sencilla. Se requiere sin embargo el manejo de las propiedades básicas del símbolo de Legendre, y de la Ley de Reciprocidad Cuadrática, que enunciaremos a continuación.

La ley de reciprocidad cuadrática

La Ley de Reciprocidad Cuadrática fue enunciada por Euler y demostrada por primera vez por Gauss, hacia finales del siglo XVIII. Éste es uno de los resultados centrales de la Teoría de Números, y se han publicado hasta ahora más de 150 demostraciones del mismo, las primeras de las cuales se encuentran en el libro de *Disquisitiones Arithmeticae,* del propio Gauss.

Sea p un número primo impar. Sea a un entero no divisible por p. Se dice que a es un residuo cuadrático módulo p si la ecuación $x^2 \equiv a \pmod{p}$ tiene solución. En caso contrario se dice que a es un residuo no cuadrático módulo p. Legendre introdujo el hoy llamado símbolo de Legendre de la siguiente manera: $\left(\frac{a}{p}\right) = 1$ si a es un residuo cuadrático módulo p y $\left(\frac{a}{p}\right) = -1$ si a es un residuo no cuadrático módulo p. El símbolo de Legendre tiene las siguientes propiedades elementales:

1) Si $a \equiv b \pmod{p}$ entonces $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

2) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

3) Si p no divide a ab entonces $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Con esta notación enunciamos la famosa Ley de Reciprocidad Cuadrática.

Ley de Reciprocidad Cuadrática (LRC): *Sean p y q primos impares.*

1) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

2) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{2}}$.

3) $\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)$

Esta ley provee un eficiente algoritmo para determinar si un primo q es o no, un residuo cuadrático módulo p, pero si p y q son grandes, el cálculo de $\left(\frac{q}{p}\right)$ puede requerir de sucesivas aplicaciones de la LRC y la factorización de los números compuestos que van apareciendo complicaría el cálculo.

Esta dificultad se evita con una extensión de la LRC obtenida por Jacobi. Extendió la noción de símbolo de Legendre a todos los números impares: Sea n un número impar y sea $n = p_1 \cdots p_s$ su descomposición en factores primos. Sea a un entero, coprimo con n. Se define el símbolo de Jacobi $\left(\frac{a}{n}\right)$ por la

fórmula

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_s}\right).$$

El símbolo de Jacobi, que coincide con el de Legendre si n es primo, satisface las propiedades 1) y 3) del símbolo de Legendre. Más aún, Jacobi demostró que el símbolo satisface la misma Ley de Reciprocidad Cuadrática, reemplazando los primos p y q por cualquier par de números impares n y m, coprimos entre sí.

Terminaremos esta sección demostrando las propiedades PM3 y PF2.

DEMOSTRACIÓN DE PM3: Sea q un divisor primo de M_p. Por la parte 2) de la LRC basta mostrar que $\left(\frac{2}{q}\right) = 1$. En la demostración de PM2 veíamos que, de la ecuación $2^p \equiv 1 \pmod{q}$, se deduce que p divide a $q-1$. Más aún, como p es impar, entonces p divide a $(q-1)/2$, por lo que $2^{\frac{q-1}{2}} \equiv 1 \pmod{q}$. Usando la propiedad 2) del símbolo de Legendre obtenemos $\left(\frac{2}{q}\right) = 1$.

DEMOSTRACIÓN DE PF2: Sea q un divisor de F_m. Entonces $2^{2^m} \equiv -1 \pmod{q}$, de donde se deduce que 2 tiene orden 2^{m+1} módulo q. Sigue que 2^{m+1} divide a $q-1$ y como $m \geq 2$, entonces resulta que $q \equiv 1 \pmod{8}$. Por la LRC, se concluye que $\left(\frac{2}{q}\right) = 1$, por lo que existe un entero a tal que $a^2 \equiv 2 \pmod{q}$. Como 2 tiene orden $2^{m+1} \pmod{q}$, entonces a tiene orden $2^{m+2} \pmod{q}$, de donde se obtiene el resultado deseado.

LAS PRUEBAS DE PEPIN Y DE LUCAS-LEHMER. EXTENSIONES

Contrariamente a lo ocurrido históricamente, en esta sección demostraremos primero la prueba de Pepin y una extensión suya conocida como el teorema de Proth. De la demostración de estos resultados extraeremos los elementos que nos permitirán diseñar una estrategia que nos conducirá a una demostración de la Prueba de Lucas-Lehmer.

Obsérvese que la Prueba de Pepin puede enunciarse de la siguiente forma:

Prueba de Pepin: *Sea $m \geq 1$, $F_m = 2^{2^m} + 1$. El número F_m es primo si, y sólo si, se satisface*

$$3^{\frac{F_m-1}{2}} \equiv -1 \pmod{F_m}. \qquad (*)$$

DEMOSTRACIÓN: Supongamos que F_m es primo. Usando la LRC obtenemos $\left(\frac{3}{F_m}\right) = \left(\frac{F_m}{3}\right) = \left(\frac{-1}{3}\right) = -1$. De la propiedad 2) del símbolo de Legendre se deduce $(*)$. Recíprocamente, supongamos que $(*)$ se satisface. Sea q un divisor primo de F_m. Por PG1, bastaría demostrar que $q > \sqrt{F_m}$ para concluir que F_m es primo. Obtenemos más que eso. En efecto, la hipótesis implica que $3^{\frac{F_m-1}{2}} = 3^{2^{2^m-1}} \equiv -1 \pmod{q}$, por lo que la clase del 3 tiene orden

$2^{2^m} = F_m - 1$ en el grupo $(\mathbb{Z}/q\mathbb{Z})^*$, de donde se deduce que $F_m - 1$ divide a $q-1$, lo que implica que $F_m \leq q$.

En 1878 Proth publicó la siguiente extensión del teorema de Pepin.

Teorema de Proth: *Sea $n = A \cdot 2^m + 1$, $0 < A < 2^m$. Sea a un entero tal que $\left(\frac{a}{n}\right) = -1$, donde el símbolo es el de Jacobi. Entonces n es primo si, y sólo si,*

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n} \qquad (**).$$

Demostración: Si n es primo, $(**)$ se deduce de la propiedad 2) del símbolo de Legendre. Recíprocamente, supongamos que se satisface $(**)$. Obsérvese que $A < 2^m$ implica que $2^m > \sqrt{n}$. Sea q un divisor primo de n. De $(**)$ sigue que

$$a^{\frac{n-1}{2}} = (a^A)^{2^{m-1}} \equiv -1 \pmod{q},$$

de donde se deduce que la clase de a^A tiene orden 2^m en el grupo $(\mathbb{Z}/q\mathbb{Z})^*$. Entonces 2^m divide a $q-1$. En particular, $q > 2^m > \sqrt{n}$, por lo que n es primo.

Analizaremos brevemente la estrategia empleada en la demostración de ambos teoremas. Al número n, cuya primalidad queremos estudiar, se le asocia una ecuación en el grupo $(\mathbb{Z}/n\mathbb{Z})^*$. Las propiedades del símbolo de Legendre (incluyendo LRC en el caso de la prueba de Pepin) permiten deducir que la ecuación se satisface si n es primo. Para el recíproco, el hecho fundamental es que $n-1$ es divisible por una potencia de 2 mayor que $\sqrt{n}$, de donde se deduce eventualmente, que cualquier divisor primo q de n también lo sería, lo cual sólo es posible si n es primo.

La misma metodología no puede aplicarse a los números de Mersenne M_p, porque $M_p - 1 = 2^p - 2$ no es divisible por potencias grandes de 2. Pero si asociamos a M_p una ecuación en un grupo multiplicativo de orden $M_p + 1 = 2^p$, o múltiplo de él, podemos tener éxito.

Si M_p es primo y $\mathcal{R}$ es el anillo de enteros algebraicos de una extensión cuadrática $\mathbb{Q}(\sqrt{d})$ de $\mathbb{Q}$, es un hecho básico de la teoría de estos anillos que la condición $\left(\frac{d}{M_p}\right) = -1$ implica que $\mathcal{R}/M_p\mathcal{R}$ es un cuerpo finito de M_p^2 elementos. El grupo multiplicativo $(\mathcal{R}/M_p\mathcal{R})^*$ es cíclico de orden $M_p^2 - 1 = (M_p+1)(M_p-1)$. Veremos ahora que $d = 3$ sirve nuestro propósito para los números M_p, con p primo impar. Aún nos faltaría encontrar la ecuación que debe satisfacerse en el grupo. Usaremos el siguiente lema.

Lema 1: *Sea $M_p = 2^p - 1$, p primo impar. Entonces*

$$\left(\frac{3}{M_p}\right) = \left(\frac{-2}{M_p}\right) = -1, \text{ donde } \left(\frac{\cdot}{M_p}\right) \text{ es el símbolo de Jacobi.}$$

Demostración: Es una consecuencia de LCR para el símbolo de Jacobi.

Sea $R = \mathbb{Z}[\sqrt{3}]$. Sea $\alpha = 1 + \sqrt{3}$, $\overline{\alpha} = 1 - \sqrt{3}$. Obsérvese que $\alpha\overline{\alpha} = -2$, $\frac{\overline{\alpha}}{\alpha} = -2 + \sqrt{3}$. Obsérvese también que si M_p es primo, entonces

$$\alpha^{M_p} \equiv (1+\sqrt{3})^{M_p} \equiv 1 + \left(3^{\frac{M_p-1}{2}}\right)\sqrt{3} \equiv 1 + \left(\frac{3}{M_p}\right)\sqrt{3} \equiv \overline{\alpha} \pmod{M_p},$$

donde la congruencia ocurre en el anillo $\mathcal{R}$.

Estamos ahora en posición de demostrar el siguiente teorema, que incluye la Prueba de Lucas-Lehmer.

Teorema: *Sea p un primo impar. Las siguientes proposiciones son equivalentes:*

i) M_p es primo

ii) $\left(2-\sqrt{3}\right)^{2^{p-1}} \equiv -1 \pmod{M_p}$

iii) La ecuación definida por $S_0 = 4$, $S_{k+1} = S_k^2 - 2$, $k \geq 0$ satisface $S_{p-2} \equiv 0 \pmod{M_p}$.

DEMOSTRACIÓN: i) $\Rightarrow$ ii)

$$(-1) = \left(\frac{-2}{M_p}\right) \equiv (-2)^{\frac{M_p-1}{2}} \equiv (\alpha\overline{\alpha})^{\frac{M_p-1}{2}}$$

$$\equiv \left(\alpha^{M_p+1}\right)^{\frac{M_p-1}{2}} \equiv \left(\alpha^{M_p-1}\right)^{\frac{M_p+1}{2}} \equiv (\overline{\alpha}/\alpha)^{\frac{M_p+1}{2}}$$

$$\equiv (-2+\sqrt{3})^{2^{p-1}} \equiv (2-\sqrt{3})^{2^{p-1}} \pmod{M_p}$$

ii) $\Rightarrow$ i). Sea q un divisor primo de M_p. Sea $\mathcal{Q}$ un ideal primo de $\mathcal{R}$ que yace sobre q. La ecuación $(2-\sqrt{3})^{2^{p-1}} \equiv -1 \pmod{\mathcal{Q}}$ implica que la clase de $2-\sqrt{3}$ tiene orden 2^p en el grupo multiplicativo $(\mathcal{R}/\mathcal{Q}\mathcal{R})^*$, cuyo orden divide a q^2-1. Sigue que 2^p divide a $(q+1)(q-1)$, de donde resulta $q \geq 2^{p-1} - 1 > \sqrt{M_p}$.

La equivalencia entre iii) y ii) proviene de las siguientes observaciones:

• Los términos de la sucesión de iii) vienen dados por $S_k = (2-\sqrt{3})^{2^k} + (2+\sqrt{3})^{2^k} = (2-\sqrt{3})^{2^k} + (2-\sqrt{3})^{-2^k}$.

• $(2-\sqrt{3})^{2^{p-2}} + (2-\sqrt{3})^{-2^{p-2}} \equiv 0 \pmod{M_p}$ si, y sólo si, $(2-\sqrt{3})^{2^{p-1}} \equiv -1 \pmod{M_p}$.

Terminaremos esta sección enunciando una extensión de este resultado, análogo al teorema de Proth.

Teorema: *Sea $n = A \cdot 2^m - 1$, $A < 2^m$. Sea d un entero tal que $\left(\frac{d}{n}\right) = -1$. Sea $\mathcal{R}$ el anillo de enteros algebraicos de $\mathbb{Q}(\sqrt{d})$. Supongamos que $\alpha \in \mathcal{R}$ y denotamos por $\overline{\alpha}$ al conjugado de α en $\mathbb{Q}(\sqrt{d})$. Supongamos que $\left(\frac{\alpha\overline{\alpha}}{n}\right) = -1$. Las siguientes afirmaciones son equivalentes:*

i) n es primo.

ii) $(\overline{\alpha}/\alpha)^{\frac{n+1}{2}} \equiv -1 \pmod{n}$.

iii) La sucesión definida por $S_0 = (\overline{\alpha}/\alpha)^A + (\alpha/\overline{\alpha})^A$, $S_{k+1} = S_k^2 - 2$ *para* $k \geq 0$, *satisface* $S_{m-2} \equiv 0 \pmod{n}$.

La demostración, que sigue los pasos del teorema anterior, queda como ejercicio para el lector.

Desarrollos posteriores: primalidad determinística en tiempos modernos

Lucas extendió sus métodos para estudiar la primalidad de números de la forma $n = A \cdot 3^m - 1$, $A < 3^m$. Más recientemente, desde la década de 1970, Hugh Williams desarrolló exhaustivamente la metodología de Lucas para determinar la primalidad de números de la forma $n = A \cdot r^m \pm 1$, $A < r^m$, r primo. La metodología empleada, y la mayor parte de sus resultados pueden encontrarse en su reciente libro [W].

Más recientemente, varios autores, entre los cuales me incluyo, han estudiado el problema con una metodología diferente, que consiste en extender la presentada en este artículo, generalizando el teorema de Proth y usando las leyes de reciprocidad de Eisenstein. Ambos métodos involucran aritmética en el anillo ciclotómico $\mathbb{Z}[\xi_r]$, donde ξ_r es una raiz primitiva r-ésima de la unidad. Unas ventajas que presentan los algoritmos basados en las generalizaciones del teorema de Proth sobre los anteriores es que son conceptualmente más sencillos y se aplican a una familia de números más grande.

A principios de la década de los 80, Adleman, Pomerance y Rumely, desarrollaron un algoritmo, que probaron tiene complejidad subexponencial, que permite determinar la primalidad de cualquier número n. Sus métodos consisten en asociar a n un conjunto de ecuaciones en un conjunto de grupos multiplicativos, cuidadosamente seleccionados y extraer de éstas información sobre los posibles divisores de n, suficiente como para determinar su primalidad. Las ecuaciones se deducen a partir de propiedades de las sumas de Gauss y de Jacobi, elementos de anillos ciclotómicos. La validez del algoritmo se obtiene a partir de una ingeniosa aplicación del principio de dualidad en grupos de caracteres. Cohen y Lenstra mejoraron e implementaron el algoritmo en 1981, que hoy se conoce como el APRCL.

Métodos determinísticos de primalidad usando la teoría de curvas elípticas, han sido desarrollados en los últimos 20 años. De hecho, los resultados teóricos más interesantes se han obtenido sobre las bases de esta teoría. Ver [A-H]. El libro de Henry Cohen [C] contiene una descripción detallada, tanto de APRCL, como de los métodos con curvas elípticas.

Para buscar primos muy grandes, se siguen utilizando algoritmos que se restringen a familias más específicas, pues son algoritmos más eficientes. Para estas familias no sólo es importante la complejidad del algoritmo, sino una estimación más precisa del número de operaciones modulares que debe efectuarse.

Varios problemas, importantes desde el punto de vista de la implementación de estos algoritmos, siguen ocupando el tiempo de investigadores en el tema.

Bibliografía

[A-H] Adleman, L., Huang, M., *Recognizing primes in random polynomial time,* LN in Math 1512, Springer-Verlag, Berlin, Heidelberg, 1992.

[A-P-R] Adleman, L., Pomerance, C., Ramely, R., *On distinghishing prime numbers from composite numbers,* Ann. of Math 117 (1983), 173-206

[B] Bressound, D., *Factorization and Primality Testing,* Springer-Verlag, New York 1989.

[B-B] Berrizbeitia, P., Berry, T., *Cubic Reciprocity and generalized Lucas-Lehmer Test for primality of* $A3^n \pm 1$*,* Proc. AMS 127 (1998), 1923-1925.

[B-O-T] Berrizbeitia, P., Odreman, M.,Tena, J., *Primality Test for numbers* M *with a large power of* 5 *dividing* $M^4 - 1$*,* 1776 LNCS, Springer 2000, 269-279.

[C] Cohen, H., *A course in Computational Algebraic Number Theory,* Springer-Verlag, Berlin, Heidelberg (1993)

[G] Guthmann, A., *Effective Primality Test for Integers as the forms* $N = k3^n + 1$ *and* $N = k2^m3^n + 1$*,* BIT 32 (1992), 529-534.

[L] Lucas, E., *Sur la recherche des grand nombre premiers,* Assoc. Francaise p. l'Avanc. des Sciences, 5, (1876), 61-68.

[P] Pepin, T. *Sur la formule* $2^{2^n} + 1$*,* C.R. Acad. Sci. Paris, 85, (1877), 329-331.

[Pr] Proth, F., *Thèoréms sur les nombre premiers ,* C.R. Acad. Sci. Paris, 85, (1878)

[R] Ribenboim, P., *The Little Book of Big Primes,* Springer-Verlag, New York (1991)

[W] Williams, H., *Edouard Lucas and primality testing ,* Canadian Mathematical Society Series of Monographs and Advanced Texts, 22. AWiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1998.

Pedro Berrizbeitia
Departamento de Matemáticas
Universidad Simón Bolivar
Caracas, Venezuela
correo electrónico: pedrob@usb.ve