Miscelánea Matemática **58** (2014) 67-76 SMM

Primos distantes y parientes relativos

Pablo Castañeda

Instituto Tecnológico Autónomo de México
Río Hondo No. 1, Col. Progreso Tizapán
México D.F. 01080, México
pablo.castaneda@itam.mx

Resumen

En teoría de números, el estudio de los números primos tiene una relevancia central. Se sabe que Hilbert creía que esta teoría sería siempre la parte más pura de las matemáticas, el vuelco vino con la criptografía y a su vez la búsqueda por números primos cada vez más grandes.

Vemos, a lo largo de la historia desde 1952 hasta los días actuales, que 32 de los 33 números primos más grandes registrados son aquellos llamados primos de Mersenne; solamente de 1989 a 1992 el número $391581 \cdot 2^{216193} - 1$ salió de esta regla. Desde 1996 todos los resultados provienen del proyecto colectivo *GIMPS*.

Este trabajo propone una prueba simple para el teorema por el cual conocemos los primos de Mersenne, sin sofisticadas herramientas de teoría de números. La prueba es accesible y tan sencilla que nos permitirá ir un poco más allá y generalizar los primos de Mersenne al mostrar una gran parte de la familia que estaba escondida.

1. Introducción

Marin Mersenne fue un monje medieval y, como buen monje, parte de la élite que controlaba el conocimiento. Era un hombre del saber y se interesaba por el mundo y sus raíces. Las matemáticas no se encontraban fuera de sus terrenos del conocimiento. En 1644, a la edad de 56 años, afirmó que los números de la forma $2^p - 1$ eran primos para $p = 2$, 3, 5, 7, 13, 17, 19, 31, 67, 127 y 257, y sin embargo, compuestos para todos los otros valores de p menores que 257.

Este resultado no es solamente incorrecto (pues, para $p = 67, 257$, los números no son primos, así como, para valores $p = 61, 89, 107$ los números son primos), sino parece no ser el primero. Moreira y Saldanha resaltan en su libro [6] que Hudalricus Regius mostró en 1536 que $2^p - 1$ no necesita ser primo siempre que p lo sea, por ejemplo, $2^{11} - 1 = 2047 = 23 \cdot 89$. Además, en 1588, Pietro Cataldi había verificado la primalidad de $2^{17} - 1$ e $2^{19} - 1$.

Empero, el resultado por el cual conocemos los llamados primos de Mersenne es asombroso:

Teorema 1.1. *Si $a^n - 1$ es primo, entonces $a = 2$ y n es primo.*

Antes de ir más lejos, notemos que la condición $a = 2$ es necesaria, pues $a^n - 1$ es igual a $(a - 1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$. (Claramente tenemos un solo factor solamente cuando $a - 1 = 1$.)

Aunque parezca que tenemos un algoritmo maravilloso para encontrar todos los números primos que queramos, esto no es del todo correcto. Primero notemos que (como ya sabemos) si p es primo, $2^p - 1$ no es necesariamente un primo: por ejemplo $p = 11$.

De todas formas, sabemos por el teorema que solamente tenemos que buscar tales números cuando p es primo. Además, existen algoritmos muy eficaces para probar la primalidad de números de la forma $2^p - 1$, [7, 8]. La más eficiente de estas pruebas es la *prueba de primalidad de Lucas–Lehmer*: para $p > 2$ primo tenemos que $M_p := 2^p - 1$ es primo si, y solamente si, M_p divide a S_{p-2}, donde $S_0 = 4$ y para $k > 0$, $S_k = S_{k-1}^2 - 2$.

Mi intención hoy no es la de discutir tales pruebas o de entender porque ellas funcionan; en las referencias encontrarás detalles sobre estos temas. Yo te quiero llevar a una prueba muy simple del teorema... ¿Corta? Tal vez no, pues con las herramientas de teoría de números, la prueba puede ser escrita en apenas dos líneas. No entraré en detalles, pero transcribo aquí la prueba que se encuentra en [6]:

Demostración. Si $n = ab$ con $a, b \geq 2$ entonces $1 < 2^a - 1 < 2^n - 1$ y $2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 \equiv 1^b - 1 = 0 \pmod{2^a - 1}$ y $2^n - 1$ es compuesto. □

La parte más «complicada» de esta prueba es el módulo, el cual establece la sencilla relación $(2^a)^b \equiv 1 \pmod{2^a - 1}$, concluyendo entonces que $2^a - 1$ es un divisor de $2^p - 1$. (De modo análogo sabemos que $2^b - 1$ es divisor.)

La prueba que propongo es conceptualmente más simple. Sin embargo, tendremos que entender cómo hacer una división en una base diferente a la decimal. Entonces, ¿por qué no explicar mejor el concepto

de módulo? Porque la generalización de los números de Mersenne sería un poco obscura en teoría de números.

2. División en cualquier base no decimal

Como bien sabes, nuestro sistema númerico fue construido en base 10. Esto quiere decir que un número como 257 es simplemente la suma inteligente de $2\cdot 10^2+5\cdot 10^1+7\cdot 10^0$. Del mismo modo, el número $(101)_2$ representa un número en base 2 con valor decimal $1\cdot 2^2+0\cdot 2^1+1\cdot 2^0=5$.

En general, las cifras usadas en una base $b \geq 2$ son aquellas que toman valores tales como 0, 1, ..., $b-1$ y escribimos tales números como $(a_n a_{n-1}\ldots a_2 a_1 a_0)_b$, donde n es un número natural y cada cifra a_k para $k = 0, 1, \ldots, n$ es uno de esos valores entre 0 y $b-1$. Esta representación tiene el valor dado por la relación

$$(a_n a_{n-1}\ldots a_2 a_1 a_0)_b = a_n\cdot b^n + a_{n-1}\cdot b^{n-1} + \cdots + a_1\cdot b^1 + a_0\cdot b^0 = \sum_{k=0}^{n} a_k\cdot b^k.$$

Pero entonces, ¿cómo dividimos dos números en base b? De la misma forma que dividimos en base 10, solo recordando que al sumar uno a $(b-1)_b$ obtenemos $(10)_b$, pues

$$(b-1)_b + (1)_b = (b-1)\cdot b^0 + 1\cdot b^0 = b\cdot b^0 = 1\cdot b^1 + 0\cdot b^0 = (10)_b.$$

Sin embargo, para nuestros fines, no necesitamos ir muy lejos. Nota que al dividir $(1111)_b$ entre $(11)_b$ siempre nos dará como resultado $(101)_b$, sin importar la base pues

$$\begin{aligned}(11)_b\cdot(101)_b &= (1\cdot b^1+1\cdot b^0)(1\cdot b^2+0\cdot b^1+1\cdot b^0)\\ &= 1\cdot b^3+1\cdot b^2+1\cdot b^1+1\cdot b^0 = (1111)_b.\end{aligned}$$

Esta división tan simple es el camino para una prueba más sencilla para el teorema y su generalización. Tal vez quieras dibujar la «casita» tradicional de la división e intentar con algunas divisiones. Hazlo, puede ser muy revelador.

3. Los primos de Mersenne en base 2

La sección anterior ya nos dio el camino de la prueba que proponemos. La solución está ahí, solamente falta limpiar un poco el camino de vuelta.

Estamos interesados entonces en números de la forma 2^n-1 para n un número natural. Si $n = 1$, tenemos que $2^n - 1 = 1$, luego $2^n - 1 =$

$(1)_2$, si $n = 2$ tenemos $2^n - 1 = 3$ que también es fácil de ver que es $(11)_2$. En general, tenemos que $2^n - 1 = (11 \dots 11)_2$, donde la colección de números 1 tiene exactamente n elementos. De ahora en adelante, usaremos la notación $(1 \dots (n) \dots 1)_2$ para representar este número.

Una manera simple de ver esto es por inducción matemática. Veamos:

$$2^{n+1} - 1 = 2(2^n - 1) + 1 = (1 \dots (n) \dots 10)_2 + (1)_2 = (1 \dots (n+1) \dots 1)_2$$

dado que al multiplicar por 2 en binario es semejante a multiplicar por 10 en base decimal.

Con estos resultados podemos reescribir otra versión de demostración del teorema.

Demostración. Si $n = ab$, entonces $2^n - 1$ en base 2 puede ser escrito como $(1 \dots (n) \dots 1)_2$, con una colección de n elementos 1 o como $(\{1 \dots (b) \dots 1\} \dots (a) \dots \{1 \dots (b) \dots 1\})_2$, una colecćon de a elementos $\{1 \dots (b) \dots 1\}$ los cuales contienen cada uno b elementos 1, pues $n = ab$. (Las llaves $\{\ \}$ sirven solo como separadores.)

Ahora, con una división en base 2, tenemos que podemos factorizar $2^n - 1$ por

$$(2^b - 1) \cdot (\{0 \dots (b-1) \dots 01\} \dots (a) \dots \{0 \dots (b-1) \dots 01\})_2$$

o por

$$(2^a - 1) \cdot (\{0 \dots (a-1) \dots 01\} \dots (b) \dots \{0 \dots (a-1) \dots 01\})_2,$$

y por lo tanto $2^n - 1$ es compuesto. □

Nota entonces que si $n = ab$ tenemos que $2^n - 1 = (2^a - 1)(1 + 2^a + 2^{2a} + \cdots + 2^{(b-1)a}) = (2^b - 1)(1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b})$; o sea, tenemos cuatro divisores (si $a \neq b$). Observa que estas factorizaciones son en sí la prueba del teorema, sin embargo, estoy interesado en darte un ejemplo para la división en bases distintas a la decimal.

La prueba de arriba, aunque es corta, es mucho más larga que la demostración que dimos en la introducción. Sin embargo, guarda algunas ventajas. La primera es su simplicidad: ya en la preparatoria podríamos entender su significado. Además de eso, como segunda ventaja, la prueba nos brinda directamente con por lo menos un divisor de $2^n - 1$ que no sea un primo de Mersenne. (Por ejemplo, cuando n es un número cuadrado como 4, obtenemos $2^4 - 1 = (1111)_2 = 15$ y por la prueba los dos divisores, a saber, $(11)_2 = 3$ y $(101)_2 = 5$.)

Sería deseable entender los patrones de los divisores para números $2^p - 1$ compuestos con p primo. Implícito en la prueba vemos que tales divisores nunca tienen la forma $2^n - 1$. Se sabe que si p es primo impar y que q divide $2^p - 1$, entonces q es de la forma 1 más un múltiplo de

$2p$. De todos modos, los ejemplos no nos dicen mucho:

$$2^{11} - 1 = (10111)_2 \cdot (1011001)_2,$$
$$2^{23} - 1 = (101111)_2 \cdot (101011100100110001)_2,$$
$$2^{29} - 1 = (11101001)_2 \cdot (10001001111)_2 \cdot (100000101001)_2.$$

Algunos ejemplos aquí son los siguientes: $2{\cdot}11{+}1 = (10111)_2$, $2{\cdot}23{+}1 = (101111)_2$, $4(2{\cdot}11){+}1 = (1011001)_2$ y $4(2{\cdot}29){+}1 = (11101001)_2$. Intenta escribir a los otros.

Y todavía más interesante es el sendero que la prueba nos muestra, ese camino para buscar otro tipo de primos, lo que discutiremos en la próxima sección.

4. Generalización de los primos de Mersenne, el camino a otras bases

En la sección anterior dimos una prueba, estructurada en la división en base 2, de cuáles números no son primos de Mersenne. Entre otros hechos describimos los números $2^n - 1$ como números de la forma $(1 \dots (n) \dots 1)_2$ y mostramos que cuando n es compuesto un número de la forma $(1 \dots (a) \dots 1)_2$ es un divisor; si a divide a n. Pero, ¿por qué es importante estar en base 2? ¡No lo es! (Tal vez solo porque 2 es un número primo.)

Nota que la prueba anterior muestra que para un número natural $b \geq 2$ y un número compuesto n, tendremos que $(1 \dots (a) \dots 1)_b$ divide $(1 \dots (n) \dots 1)_b$ si a es divisor de n. Estos números son conocidos como números *repunit* en alusión al inglés ***rep****eated* ***unit***, unidad repetida. (La referencia [4] tiene resultados interesantes.)

Entonces busquemos una forma de escribir en base decimal los números $(1 \dots (n) \dots 1)_b$. Esto es fácil, pues

$$(1 \dots (n) \dots 1)_b \;=\; 1 \cdot b^{n-1} + 1 \cdot b^{n-2} + \cdots + 1 \cdot b^1 + 1 \cdot b^0,$$

luego, multiplicando arriba y abajo por $b - 1$ obtenemos una suma telescópica en el numerador y, por lo tanto,

$$(1 \dots (n) \dots 1)_b \;=\; \frac{b^n - 1}{b - 1}. \tag{1}$$

Con lo cual podemos reformular el teorema anterior generalizando los primos de Mersenne:

Teorema 4.1. *Si para un número natural $b \geq 2$ tenemos que $\dfrac{b^n - 1}{b - 1}$ es primo entonces n es primo.*

Substituyendo $b = 2$, notamos que el primer teorema esta incluido en el segundo. Nota también que si b es un primo mayor que 2, entonces para $n = 2$ el número $(b^n - 1)/(b - 1)$ nunca será primo, pues este es $b + 1$, que será un número par.

Denotamos de ahora en adelante al número en (1) por $M_{n,\,b}$ para n, b números naturales; nota que si $M_{p,\,2}$ es primo, entonces es uno de los primos de Mersenne (a veces usaremos la notación usual M_p para estos casos). Por eso siempre que $M_{p,\,b}$ sea primo lo llamaremos un *primo de Mersenne generalizado* o *primo de Mersenne en base b*. Algunas pruebas númericas muestran los siguientes primos:

b	p
2	2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 521, 607, 1279
3	3, 7, 13, 71, 103, 541, 1091, 1367, 1627
5	3, 7, 11, 13, 47, 127, 149, 181, 619, 929
7	5, 13, 131, 149, 1699
11	17, 19, 73, 139, 907, 1907
13	5, 7, 137, 283, 883, 991, 1021, 1193
17	3, 5, 7, 11, 47, 71, 419
19	19, 31, 47, 59, 61, 107, 337, 1061
23	5
29	5, 151
31	7, 17, 31
37	13, 71, 181, 251, 463, 521
41	3, 83, 269, 409, 1759
43	5, 13
47	127
53	11, 31, 41, 1571

Las pruebas de primalidad fueron hechas utilizando `Maple` para b corriendo en la lista de los 100 primeros primos y para todo p primo menor que 2000. La verdad, para números pequeños así, la rutina es muy rápida.

Aunque parece que para bases mayores la cantidad de primos $M_{p,\,b}$ que pueden existir es escasa, tenemos que para un primo «grande» como $b = 89$, los $M_{p,\,b}$ primos son para $p = 3$, 7, 43, 47, 71, ... y, tenemos además, que $M_{p,\,549}$ para $p = 31, 709, 1907, \ldots$ son números primos muy grandes. De hecho el mayor número primo que encontré con un día de máquina es

$$M_{1907,\,549} \approx 4{,}2235 \times 10^{5221}.$$

Después paré la máquina, pues para hacer eficiente la búsqueda de números mayores es preciso fijar la base específica en la que pretendemos trabajar, mira [5, 7], por ejemplo.

Me gustaría poder conjeturar que con los primos de Mersenne generalizados $M_{p,\,b}$ encontramos todos los primos, sin embargo, si observamos la lista arriba, vemos que los primos como: 5, 11, 17, 19, ... no aparecen. Tenemos: $M_{2,2} = 3$, $M_{3,2} = 7$, $M_{5,2} = 31$, ..., $M_{3,3} = 13$, $M_{7,3} = 1093$, ..., $M_{3,5} = 31$, etcétera. ¡Es imposible!

Empero, verificando la prueba vemos que nunca pedimos que la base b fuera un número primo, de hecho, tenemos primos de la forma $M_{p,\,b}$ con b no primo, ejemplos son $M_{2,4} = 5$, $M_{2,10} = 11$ o $M_{3,8} = 73$; podemos hacer también una tabla de estos números. Un caso interesante se da cuando $b = 10$, pues obtenemos secuencias de unos en la base decimal, casos de primos de esta forma existen para $p = 2$, 19, 23, 317, 1031, ... donde cada uno tiene longitud p.

Notando entonces que $M_{2,\,b} = b + 1$, vemos que podríamos construir todos los números primos, pues recorreríamos todos los números naturales. ¡Pero esto es absurdo! La idea sería tener un análogo a la *Criba de Eratóstenes* solo que más eficiente. Sin embargo, podemos retirar varios números como posibles bases:

Lemma 4.2. *Sea $b \geq 2$ un número natural y p un primo mayor que 2, entonces $M_{p,\,b^2}$ es siempre compuesto y $M_{p,\,b}$ uno de sus divisores.*

Demostración. Nota que la definición en (1) puede ser empleada para bases negativas, por ejemplo:

$$M_{p,\,-b} \;=\; \frac{(-b)^p - 1}{-b - 1} \;=\; \frac{b^p + 1}{b + 1} \;=\; b^{p-1} - b^{p-2} + \cdots + b^2 - b + 1,$$

pues $p > 2$ siendo primo es un número impar. Ahora, una simple multiplicación muestra que $M_{p,\,b^2} = M_{p,\,b} \cdot M_{p,\,-b}$, y así el lema. □

Notamos que el lema no sirve para $p = 2$. De hecho tenemos el caso $M_{2,b^2} = 5$ para $b = 2$ donde el número es primo.

5. Números perfectos y algunas otras curiosidades

Para hablar de *números perfectos*, nos hace falta decir lo que son los divisores propios de un número. Dado un natural n definimos un divisor propio como todo otro natural $d < n$ tal que la división de n entre d sea exacta. Luego, los divisores propios de 12, por ejemplo, son 1, 2, 3, 4 y 6; nota que 12 se divide a sí mismo exactamente, pero no es considerado *propio*.

La búsqueda de números perfectos es un juego que se remonta a la época de los griegos. La meta es encontrar números tales que la suma de sus divisores sea exactamente este número. Ahora conocemos varios de estos números y mucho más sobre ellos, pero vamos por pasos. El

primer caso es el número 6; sus divisores propios son 1, 2 y 3, tenemos que $1 + 2 + 3$ es justamente 6.

Se conocen muchos números perfectos, pero todos ellos (por ahora) son solamente pares: 6, 28, 496, 8128, 33550336, etcétera. Por increíble que parezca, estos números tienen una fuerte relación com los números de Mersenne.

Lemma 5.1. *Un número par es perfecto si, y solamente si, puede ser expresado en la forma $2^{p-1}M_p$, para M_p un primo de Mersenne.*

Veremos una prueba de solo una de las direcciones de este Lema; la dirección que era conocida desde la Grecia antigua y que aparece en los *Elementos IX* de Euclides. (Solo en el siglo XVII el matemático Leonhard Euler encontró el camino de vuelta, y por eso, a veces se conoce como el Teorema de Euclides–Euler.) Definamos la siguiente función $\sigma : \mathbb{N} \to \mathbb{N}$ de forma tal que sea la suma de todos los divisores de un número, quiero decir $\sigma(6) = 1 + 2 + 3 + 6 = 12$. Nota que incluimos al propio 6, además, vemos que cuando un número n es perfecto entonces $\sigma(n) = 2n$.

Una segunda curiosidad aparece cuando notamos que dados dos números a y b sin divisores en común (esto es que el MCD$(a, b) = 1$), ellos satisfacen la siguiente propiedad:

$$\sigma(ab) \;=\; \sigma(a)\,\sigma(b),$$

pues todos sus divisores son distintos, luego el producto de los divisores de los factores es divisor de ab. Este es el resultado básico que usaremos.

Sea M_p un primo de Mersenne, entonces $\sigma(M_p) = 1 + M_p$. Nota que 2^{p-1} es par y menor que M_p, que es primo, luego MCD$(2^{p-1}, M_p) = 1$. Así tenemos que $\sigma(2^{p-1}) = 1 + 2 + 2^2 + \cdots + 2^{p-1} = 2^p - 1 = M_p$, y por tanto

$$\begin{aligned}\sigma(2^{p-1}M_p) = \sigma(2^{p-1})\sigma(M_p) &= (2^p - 1)(M_p + 1)\\ &= 2^pM_p - M_p + (2^p - 1) = 2(2^{p-1}M_p),\end{aligned}$$

con lo cual $2^{p-1}M_p$ es un número perfecto y par.

Hay varias conjeturas sobre números perfectos impares; se dice que si existen, entonces estos números deben ser muy grandes y satisfacer ciertas propiedades. Supón que N es un número perfecto impar, entonces N debe ser mayor que 10^{300} (se estima que debe ser mayor que 10^{1500}; ésto todavía no es un hecho), formado con por lo menos 9 factores primos distintos, de los cuales uno de ellos debe ser mayor que 10^8, otro mayor que 10^4 y uno más mayor que 10^2; si N tiene al 3 como divisor, entonces N debe tener por lo menos 12 factores primos distintos.

Sin embargo, ahora tenemos una expresión semejante a los primos de Mersenne para muchos otros primos, ¿será que conseguimos decir algo al respecto sobre estas conjeturas?

Muy bien, notemos que el *paso de maestro* en el cálculo anterior es justamente que $\sigma(2^{p-1})$ es tanto M_p como $2 \cdot 2^{p-1} - 1$. De esta forma si buscamos un número A para un primo de Mersenne generalizado $M_{p,\,b}$ tal que $\sigma(A)$ sea justamente $M_{p,\,b}$, ¿será que tendríamos algún resultado para $AM_{p,\,b}$? Bien, $M_{p,\,b}$ es primo y podemos suponer que A es menor que él, luego

$$\sigma(AM_{p,\,b}) \;=\; \sigma(A)\sigma(M_{p,\,b}) \;=\; M_{p,\,b}(M_{p,\,b}+1).$$

Pero queremos que este resultado sea justamente $2AM_{p,\,b}$, así si $M_{p,\,b}$ es igual a $2A-1$, tendremos nuestro resultado. En efecto, si $A = (M_{p,\,b}+1)/2$ es tal que $\sigma(A) = M_{p,\,b}$, tendremos que $AM_{p,\,b}$ es un número perfecto, pues

$$\sigma(AM_{p,\,b}) \;=\; (2A{-}1)(M_{p,\,b}{+}1) = 2AM_{p,\,b}{-}M_{p,\,b}{+}(2A{-}1) \;=\; 2AM_{p,\,b}.$$

Por el Lema anterior, sabemos que los perfectos pares fueron encontrados, entonces si A es impar, el producto lo será también.

Esto no debe ser novedad. Empero, tenemos una forma para los primos de Mersenne generalizados y por lo tanto una forma para A. Si $M_{p,\,b}$ es primo, entonces queremos que A sea

$$A \;:=\; \frac{M_{p,\,b}+1}{2} \;=\; \frac{b^p+b-2}{2(b-1)}.$$

Para mostrar la validez de esta fórmula finalizamos con un caso curioso: nota que $M_{3,5} = 31$ es primo. Y vemos que

$$A = \frac{5^3+5-2}{2(5-1)} = \frac{128}{2\cdot 4} = 16,$$

además $\sigma(16) = 1+2+4+8+16 = M_{3,5}$. Luego tenemos que $16 \cdot M_{3,5}$ es perfecto; y sí, pero este resultado ya existía en el Lema, pues $M_{3,5}$ es exactamente el primo de Mersenne M_5 y «casualmente» A es 2^{5-1}.

He rodado sin suceso algunos días de máquina, pero espero que un día alguna de estas cuentas ayude a encontrar alguno de los inalcanzables perfectos impares o por lo menos que algún número primo muy grande sea encontrado como un Mersenne generalizado. Sobre todo, estaré muy feliz si has disfrutado de este texto.

Las referencias y la amplia bibliografía contenida en las mismas puede proporcionar mucha información valiosa a los interesados en el tema. En la página electrónica del proyecto GIMPS (*Great Internet Mersenne Prime Search*) puede encontrarse más información. Como el mayor primo conocido $M_{57885161}$ encontrado el 25 de Enero de 2013; de hecho tú puedes ayudar en la búsqueda de los primos de Mersenne.

Otros primos interesantes son los llamados primos de Fermat, puedes encontrar información al respecto en [1], así como proyectos análogos al GIMPS liderados por los profesores R.E. Crandall y L. Duman.

Bibliografía

[1] J. Alfaro Pastor y C. Bosch Giral, «La peor conjetura de Fermat sigue abierta», *Miscelanea Matemática*, vol. 34, 2001, 113–123.
[2] S. C. Coutinho, *Números inteiros e criptografia RSA*, IMPA, Brasil, 2001.
[3] ———, *Primalidade em tempo plinomial: uma introdução ao algoritmo AKS*, IMPA, Brasil, 2004.
[4] R. L. Francis, «Mathematical haystacks: another look at repunit numbers», *The College Mathematical Jornal*, vol. 19(3), 1988, 240–246.
[5] M. Lemos, *Criptografia, números primos e algoritmos*, IMPA, Brasil, 1989.
[6] C. G. Moreira y N. Saldanha, *Primos de Mersenne (e outros primos muito grandes)*, Publicações matemáticas, IMPA, Brasil, 2008.
[7] P. Ribenboim, *The little book of bigger primes*, Springer-Verlag, New York, 2004.
[8] G. Villa Salvador, «Postulado de Bertrand y distribución de los números primos», *Miscelánea Matemática*, vol. 50, 2009, 57–76.