Revista Integración
ISSN: 0120-419X
integracion@matematicas.uis.edu.co
Universidad Industrial de Santander
Colombia

Castillo, John H.; García-Pulgarín, Gilberto; Velásquez-Soto, Juan Miguel
De los números de Midy a la primalidad
Revista Integración, vol. 33, núm. 1, 2015, pp. 1-10
Universidad Industrial de Santander
Bucaramanga, Colombia

Revista Integración
Escuela de Matemáticas
Universidad Industrial de Santander
Vol. 33, No. 1, 2015, pág. 1–10

De los números de Midy a la primalidad

John H. Castillo[a*], Gilberto García-Pulgarín[b], Juan Miguel Velásquez-Soto[c]

[a] Universidad de Nariño, Departamento de Matemáticas y Estadística, Pasto, Colombia.

[b] Universidad de Antioquia, Instituto de Matemáticas, Medellín, Colombia.

[c] Universidad del Valle, Departamento de Matemáticas, Cali, Colombia.

Resumen. Utilizando propiedades de los números de Midy se define el concepto de q-seudoprimo base b, el cual extiende la idea de seudoprimo fuerte base b, y a partir de dicho concepto se establece un nuevo criterio de primalidad que refina el Teorema de Pocklington.
Palabras clave: Números primos, seudoprimalidad fuerte, números de Midy, Teorema de Pocklington.
MSC2010: 11A51, 11Y11, 11Y55, 11B83.

From Midy numbers to primality

Abstract. We define the concept of q-pseudoprime to base b, which extends the idea of strong pseudoprime to base b. We stablish a new test of primality that refines the Pocklinton's Theorem using some properties of the Midy numbers.
Keywords: Prime numbers, strong pseudoprimality, Midy's numbers, Pocklington's Theorem.

1. Introducción

En el artículo 329 de sus *Disquisitiones Aritmethicae* [9] Gauss destaca la importancia de distinguir los números primos de los números compuestos y de factorizar estos últimos. Con la llegada de los computadores han surgido innumerables tentativas de obtener un algoritmo eficiente para determinar la primalidad de un número. Actualmente el problema tiene gran interés, dada la utilidad de los números primos en algoritmos criptográficos, entre los que se destacan los algoritmos RSA y ElGamal. Desde este punto de vista los tests de primalidad tienen gran importancia en ciencias como la computación teórica y la criptografía.

* E-mail: jhcastillo@gmail.com
Recibido: 23 de mayo de 2014, Aceptado: 02 de enero de 2015.
Para citar este artículo: J.H. Castillo, G. García-Pulgarín, J.M. Velásquez-Soto, De los números de Midy a la primalidad, *Rev. Integr. Temas Mat.* 33 (2015), no. 1, 1-10.

El método de división-ensayo, en el que se va verificando uno a uno si los primos menores a la raíz cuadrada de un número dado son divisores de dicho número o no, permite factorizar un entero, y si eso no ocurre se puede concluir que el número es primo. Si bien no hay mucha dificultad en verificar la divisibilidad entre un número y otro, el método resulta ineficiente cuando el número no tiene factores primos pequeños, hecho este que no se puede determinar a priori.

El de división-ensayo es sin duda uno de los métodos más simples que se podría imaginar para determinar primalidad.

Algunos teoremas de la Teoría de Números se pueden usar para determinar la primalidad de un número. Por ejemplo los teoremas de Wilson-Lagrange y Lucas, permiten saber si un número N es primo.

Teorema 1.1 (Teorema de Wilson-Lagrange, 1771). *Un entero N mayor que 1 es primo si y sólo si $(N-1)! \equiv -1 \mod N$.*

De esta forma, para determinar si N es primo se debe calcular $(N-1)!$ mód N, aunque si N es grande esta cuenta es quizá tanto o más difícil de hacer que aplicar el método de división-ensayo.

Teorema 1.2 (Teorema de Lucas, 1876). *Sean b y N enteros primos relativos, con $N > 1$. Si*

$$b^{N-1} \equiv 1 \mod N$$

y, para todo primo $q|N-1$,

$$b^{(N-1)/q} \not\equiv 1 \mod N,$$

entonces N es primo.

La factorización de $N-1$ puede ser difícil para muchos números N, pero no para todos. Por ejemplo, si se consideran los números de la forma $F_k = 2^{2^k} + 1$, conocidos como números de Fermat, la factorización de $N-1$ es directa. A la fecha los únicos números de Fermat que son primos son F_k con $0 \leq k \leq 4$.

La dificultad al aplicar el Teorema de Lucas no solamente recae en encontrar un b que cumpla las condiciones establecidas, esto es, ser una raíz primitiva módulo N, sino también en encontrar la factorización de $N-1$. Hay por tanto dos posibles formas de mejorar dicho Teorema: relajar las condiciones exigidas a b, o tener una factorización parcial de $N-1$.

El siguiente teorema mejora el de Lucas en la primera de las formas descritas arriba.

Teorema 1.3 (Teorema 2 de [4]). *Sea N un entero. Si para cada primo q divisor de $N-1$ existe un entero $b = b(q)$ tal que*

$$b^{N-1} \equiv 1 \mod N \qquad y \qquad b^{(N-1)/q} \not\equiv 1 \mod N,$$

entonces N es primo.

Un resultado de Pocklington exige sólo una factorización parcial de $N-1 = FR$, donde F está completamente factorizado. Si $F > R$ se puede garantizar la primalidad de N; en otro caso se dice qué forma tienen los divisores de N.

Teorema 1.4 (Teorema de Pocklington, 1914)**.** *Supóngase que $N-1=FR$, donde se conoce la factorización prima de F, y b es tal que*

$$b^{N-1}\equiv 1 \text{ mód } N$$

y, para todo primo $q|F$[1]*,*

$$\text{mcd}(b^{(N-1)/q}-1,\ N)=1.$$

Entonces todo factor primo de N es congruente con 1 módulo F. Además si $F\geq\sqrt{N}$, N es primo.

El Pequeño Teorema de Fermat da condiciones necesarias para la primalidad de un entero, y aunque no da condiciones suficientes, sí permite en ciertos casos determinar que el entero es compuesto.

Teorema 1.5 (Pequeño Teorema de Fermat)**.** *Si p es un número primo y b es un entero primo relativo con p, entonces*

$$b^{p-1}\equiv 1 \text{ mód } p.$$

En consecuencia, dado un entero N mayor que 1, se escoge $1<b<N$ y $\text{mcd}\,(b,N)=1$ y se calcula b^{N-1} mód N. Si N es primo b^{N-1}, debe ser congruente con 1 módulo N; cualquier otro resultado permite concluir que N es compuesto, caso en el cual se dice que b es un testigo de composición de N, garantizándose que N es compuesto aunque no se conozca ninguno de sus factores.

Por otro lado, si $b^{N-1}\equiv 1$ mód N, esto no demuestra que N sea primo, como se evidencia con $N=341=11\cdot 31$, al tomar $b=2$. Si N es un número compuesto impar tal que $b^{N-1}\equiv 1$ mód N, se dice que N es un *seudoprimos base b*, o seudoprimo de Fermat base b, y cuando no se sabe de la compositez[2] de N se le denomina *probable primo base b*. Pese a que los seudoprimos base b son escasos, se sabe que hay infinitos de ellos para cada base [7, Teorema 3.4.4].

Un procedimiento para determinar la compositez de un número puede ser escoger al azar números b menores que N, e ir calculando el $\text{mcd}(b,N)$. Si tal máximo común divisor es mayor que 1, N es compuesto. Si no, se procede a calcular b^{N-1} mód N; si este valor es distinto de 1, se concluye que N es compuesto y b es un testigo de su compositez. Si b^{N-1} mód N es 1, no se puede decidir acerca de la primalidad o compositez de N, él es un probable primo base b.

Aunque este procedimiento es más refinado que el Pequeño Teorema de Fermat, existen enteros compuestos que con esta idea no pueden detectarse como tales, si se restringe b al conjunto de los primos relativos con N. Es el caso de $N=561$, si b es primo relativo con N puede verificarse que $b^{N-1}\equiv 1$ mód N. A estos números se los conoce como *números de Carmichael*, o seudoprimos absolutos [7, Sección 3.4.2].

El concepto de probable primo se puede refinar un poco más y definir *probable primo fuerte base b*. Sabemos que si N es primo y escribimos $N-1=2^s t$ con t impar, existe un j mínimo con $0\leq j\leq s$, tal que $(b^t)^{2^j}\equiv 1$ mód N; si $j=0$, esto significa que $b^t\equiv 1$ mód N; si no, necesariamente $b^{2^{j-1}t}\equiv -1$ mód N. Así, decimos que el entero

[1] Como es usual con $\text{mcd}(m,n)$ se denota el máximo común divisor de los enteros m y n.
[2] Calidad de ser compuesto.

$N = 2^s t + 1$ con t impar es *probable primo fuerte base* b, si $b^t \equiv 1 \bmod N$ ó existe $1 \leq j \leq s$ tal que $b^{2^{j-1}t} \equiv -1 \bmod N$. Un probable primo fuerte base b que sea compuesto se llama *seudoprimo fuerte base* b.

En 1983, Leonard M. Adleman, Carl Pomerance y Robert S. Rumely [1] presentaron un test de primalidad determinista que decide sobre la primalidad del entero N, en un tiempo de ejecución $(\log N)^{O(\log\log\log N)}$.

Más recientemente, en 2002, M. Agrawal, N. Kayal y N. Saxena [2] mostraron que determinar la primalidad de un número se puede lograr con un algoritmo que corre en tiempo polinomial, obteniendo así el primer algoritmo determinista de este tipo. Desde entonces se han hecho muchos esfuerzos para implementar dicho algoritmo de forma eficiente, lo cual ha contribuido al surgimiento de diversas variantes, que ahora se conocen como algoritmos de clase AKS. Entre estas variantes se destacan las de Berrizbeitia [3], Cheng [6] y Lenstra & Pomerance [10].

Estudiando la propiedad de Midy o propiedad de los nueves [8], [5], [13], definimos una clase especial de enteros, que hemos llamado *números de Midy base* b. En la Sección 2 recogemos parte de ese trabajo.

Demostramos que si N es un número de Midy base b, él es un probable primo fuerte base b, lo cual permite establecer una estrecha relación entre números de Midy y primalidad.

En particular mostramos que desde los números de Midy hay una extensión natural del concepto de probable primo fuerte base b, lo que nos lleva a definir, en este trabajo, el concepto de *q-probable primo fuerte base* b, siendo q un divisor primo de $N-1$ con ciertas características. En la Sección 3 estudiamos tal concepto y establecemos, en el Teorema 3.10, un criterio de primalidad que refina el Teorema de Pocklington.

2. Generalidades

Sean N y b enteros positivos primos relativos, $b > 1$ la base de numeración, $|b|_N$ el orden de b en el grupo multiplicativo $\mathbb{U}_N$ de enteros positivos menores que N y primos relativos con N, y $x \in \mathbb{U}_N$. Se sabe que al escribir la fracción $\frac{x}{N}$ en base b, esta es periódica. El período denota la secuencia de dígitos en base b que se repite en tal expresión, y se puede probar que $|b|_N$ es la longitud del período de la fracción $\frac{x}{N}$. Sean d y k enteros positivos con $|b|_N = dk$, $d > 1$ y $\frac{x}{N} = 0.\overline{a_1 a_2 \cdots a_{|b|_N}}$, donde la barra indica el período y los a_i son dígitos en base b. A continuación se separa el período $a_1 a_2 \cdots a_{|b|_N}$ en d bloques de longitud k cada uno. De esta forma, sea

$$A_j = [a_{(j-1)k+1} a_{(j-1)k+2} \cdots a_{jk}]_b$$

el número representado en base b por el j-ésimo bloque y $S_d(x) = \sum_{j=1}^{d} A_j$. Si para todo $x \in \mathbb{U}_N$, la suma $S_d(x)$ es múltiplo de $b^k - 1$, decimos que N tiene la propiedad de Midy para b y d.

Dados b y N, se denota con $\mathcal{M}_b(N)$ el conjunto de todos los d tales que N tiene la propiedad de Midy para b y d, y se llamará conjunto de Midy de N para la base b. Con $\nu_p(N)$ se indica el mayor exponente del primo p en la factorización prima de N.

En [8, Theorem 3], se presenta la siguiente caracterización de la propiedad de Midy.

Teorema 2.1. *Si N es un entero positivo y $|b|_N = kd$, entonces $d \in \mathcal{M}_b(N)$ si y sólo si $\nu_p(N) \leq \nu_p(d)$, para todo divisor primo p de* $\operatorname{mcd}(b^k - 1,\ N)$.

El siguiente resultado es una forma de reescribir el Teorema 2.1.

Teorema 2.2. *Sean N un entero positivo y d un divisor de $|b|_N$. Las siguientes afirmaciones son equivalentes.*

1. $d \in \mathcal{M}_b(N)$.
2. *Para cada primo p divisor de N tal que $\nu_p(N) > \nu_p(d)$, existe un primo q divisor de $|b|_N$ que satisface $\nu_q\left(|b|_p\right) > \nu_q(|b|_N) - \nu_q(d)$.*

En [5, Cor. 1] se demuestra el siguiente teorema.

Teorema 2.3. *Sean d_1, d_2 divisores de $|b|_N$ y suponga que $d_1 \mid d_2$ y $d_1 \in \mathcal{M}_b(N)$; entonces $d_2 \in \mathcal{M}_b(N)$.*

A continuación se dan condiciones suficientes y necesarias para que una potencia de un número primo pertenezca al conjunto de Midy de un entero positivo en una base de numeración dada.

Teorema 2.4. *Sean b, N, q y v enteros positivos con q primo. Entonces $q^v \in \mathcal{M}_b(N)$ si y solo si $N = q^n p_1^{h_1} p_2^{h_2} \cdots p_l^{h_l}$, donde n es un entero no negativo, los p_i son primos diferentes tales que q es divisor de $|b|_{p_i}$ para todo i, los h_i son enteros no negativos no todos nulos y, además, $0 \leq n \leq v$ y*

$$0 \leq \nu_q(|b|_N) - v < \min_{1 \leq i \leq l} \left\{ \nu_q(|b|_{p_i}) \right\}.$$

Para la prueba de este teorema se utiliza el siguiente resultado [12, Teorema 3.6].

Teorema 2.5. *Sean q un primo impar que no divide a b, $m = \nu_q(b^{|b|_q} - 1)$ y n un entero positivo; entonces,*

$$|b|_{q^n} = \begin{cases} |b|_q & \text{si } n \leq m, \\ q^{n-m} |b|_q & \text{si } \ n > m. \end{cases}$$

Demostración del Teorema 2.4. Supóngase que $q^v \in \mathcal{M}_b(N)$, por tanto $|b|_N = q^t k$ con $\operatorname{mcd}(q, k) = 1$ y $t \geq v$. Sea $g = \operatorname{mcd}\left(b^{kq^{t-v}} - 1, N\right)$. Por el Teorema 2.1 se sabe que g no es divisible por un divisor primo de N que sea diferente de q, y además que $\nu_q(N) \leq v$; esto lleva a que N no puede ser potencia de q, pues de serlo q^v no sería divisor de $|b|_N$. Sea $p \neq q$ un divisor primo de N; como p no divide a g, se obtiene $|b|_p \nmid kq^{t-v}$, y como $|b|_p \mid |b|_N$, resulta ser $\nu_q(|b|_p) > t - v \geq 0$, y por ello N tiene la forma $N = q^n p_1^{h_1} p_2^{h_2} \cdots p_l^{h_l}$, con las condiciones sobre los p_i y los h_i dadas en el enunciado. Teniendo presente el Teorema 2.5, se encuentra que $t = \max_{1 \leq i \leq l} \left\{ n - m, \nu_q(|b|_{p_i}) \right\}$. De esta forma para todo

divisor primo p de N se tiene que $\nu_q(|b|_p) > \max\limits_{1\leq i\leq l}\left\{n-m,\, \nu_q(|b|_{p_i})\right\} - v \geq 0$, y por ello el resto del teorema.

Recíprocamente, a partir de la hipótesis el único divisor primo de N que podría ser divisor de g es q; así el Teorema 2.1 implica que $q^v \in \mathcal{M}_b(N)$. ☑

Si en el teorema anterior se toma $v = 1$, dado que para cualquier primo p divisor de N se tiene que $\nu_q\left(|b|_N\right) \geq \nu_q\left(|b|_p\right) > 0$, resulta el siguiente corolario.

Corolario 2.6. *Sean N un entero positivo y q un divisor primo de $|b|_N$; entonces $q \in \mathcal{M}_b(N)$ si, y solo si*

1. *Si $\operatorname{mcd}(N,\ q) = 1$, entonces $\nu_q(|b|_p) = \nu_q\left(|b|_N\right)$ para todo primo p divisor de N.*
2. *Si $\operatorname{mcd}(N,\ q) > 1$, entonces q^2 no divide a N y $\nu_q(|b|_p) = \nu_q\left(|b|_N\right)$ para todo divisor primo p de N diferente de q.*

Obsérvese que, del Teorema 2.4, el menor número N tal que $q^v \in \mathcal{M}_b(N)$ debe ser un número primo P tal que $q^v|\ |b|_P$. Recordando que $|b|_P$ divide a $P-1$, se obtiene el siguiente corolario.

Corolario 2.7. *Si q es primo y v es un entero positivo, entonces el menor entero N tal que $q^v \in \mathcal{M}_b(N)$ es un primo congruente con 1 módulo q^v.*

Este último resultado permite probar un caso particular del Teorema de Dirichlet acerca de primos en progresión aritmética.

Corolario 2.8. *Si q es un primo y v es un entero positivo, existen infinitos números primos congruentes con 1 módulo q^v.*

Demostración. Del Corolario 2.7 existe un primo P_1 congruente con 1 módulo q^v, tal que $q^v \in \mathcal{M}_b(P_1)$. Tómese un entero t_1 tal que $q^{t_1 v} > P_1$. Nuevamente, se puede encontrar un primo P_2 congruente con 1 módulo $q^{t_1 v}$ tal que $q^{t_1 v} \in \mathcal{M}_b(P_2)$. Dado que se puede continuar este proceso indefinidamente, se prueba que existen infinitos números primos congruentes con 1 módulo q^v. ☑

Es fácil ver que si N es un número primo, entonces cualquier divisor de $|b|_N$ mayor que 1 pertenece a $\mathcal{M}_b(N)$. En este sentido, el conjunto de Midy de N para la base b tiene el mayor número de elementos posible. Existen números compuestos N que gozan de esta propiedad para una determinada base, como es el caso de $N = 121$ y $b = 3$. Esto motiva la siguiente definición.

Definición 2.9. Se dice que un número impar N es un número de Midy para la base b, si N es primo relativo con b y con $|b|_N$, y para todo divisor $d > 1$, de $|b|_N$ se tiene que $d \in \mathcal{M}_b(N)$.

De esta forma, N es un número de Midy base b si, y solo si $q \in \mathcal{M}_b(N)$ para todo divisor primo q de $|b|_N$. El Corolario 2.6 permite la siguiente caracterización de los números de Midy.

Teorema 2.10. *Sean N y b enteros con N impar y* $\mathrm{mcd}(N,b) = 1$*; entonces N es de Midy base b si, y sólo si $|b|_N = |b|_p$ para todo divisor primo p de N.*

De esta forma, si q es un divisor primo de $|b|_N$ y N es un número de Midy base b, entonces $\nu_q(|b|_N) = \nu_q(|b|_p)$ para cualquier divisor primo p de N. Además, se puede probar que N es un seudoprimo fuerte base b [13, Theorem 16].

3. q-probable primalidad

En lo sucesivo N y b serán enteros positivos primos relativos. Con p y q denotaremos un divisor primo de N y $N-1$, respectivamente. Además escribiremos $N-1 = q^s t$ con t y q primos relativos.

Se puede probar que N es probable primo fuerte base b si y solo si N es probable primo base b y el exponente con el que aparece 2 en el orden de $|b|_p$ es constante para todo primo p divisor de N. Este hecho y el comentario posterior al Teorema 2.10 sugieren la siguiente definición.

Definición 3.1. Sean N y b enteros con $\mathrm{mcd}\,(b,N) = 1$ y $b^{N-1} \equiv 1 \mod N$, y sea q un primo tal que para todo p divisor primo de N, q divide a $p-1$. Se dice que N es un q-probable primo base b si existe un entero no negativo k tal que para todo primo p divisor de N se tiene $\nu_q\left(|b|_p\right) = k$. Adicionalmente, si N es compuesto se dice que es un q-seudoprimo base b.

En otras palabras, N es q-probable primo base b si es probable primo base b y el exponente con el que aparece q en $|b|_p$ es constante, para todo primo p divisor de N.

Es claro que si N es primo entonces N es q-probable primo para todo divisor primo q de $N-1$.

Ejemplo 3.2. Como $1891 = 31 \times 61$ y $1890 = 2 \times 3^3 \times 5 \times 7$ y $|3|_{31} = 30$ y $|3|_{61} = 10$, se tiene que 1891 es 2 y 5-seudoprimo para la base 3, pero no es 3-seudoprimo para esta base.

Ejemplo 3.3. Si $N = 1303 \times 16927 \times 157543 = 3\,474\,749\,660\,383$ y dado que $|3|_{1303} = 434 = 2{\times}7{\times}31$ y $|3|_{16927} = 2418 = 2{\times}3{\times}13{\times}31$ y $|3|_{157543} = 157\,542 = 2{\times}3{\times}7{\times}11^2{\times}31$ se sigue que N es 2 y 31-seudoprimo para la base 3 pero no es q-seudoprimo base 3 ni para $q = 3$ ni para $q = 7$ para tal base 3.

El siguiente resultado es el Teorema 2.3 de [11], donde $\Phi_n(x)$ denota el n-ésimo polinomio ciclotómico en la variable x.

Teorema 3.4. *Sean m, $b \geq 2$, $n \geq 3$ enteros y p el mayor primo divisor de n. El entero m es divisor de $\Phi_n(b)$ si y sólo si $b^n \equiv 1 \mod m$ y para todo primo q divisor de m y distinto de p se tiene $|b|_q = n$. Es más, si p divide a m, entonces $n = p^e\,|b|_p$ con $e \geq 1$.*

Como consecuencia del Teorema anterior se tiene el siguiente corolario.

Corolario 3.5. *Sean N, $b \geq 2$ enteros y q un primo; entonces N es divisor de $\Phi_q(b)$ si y solo si para todo primo p divisor de N, se tiene $|b|_p = q$.*

Este corolario permite caracterizar la q-probable primalidad.

Teorema 3.6. *Sean N un entero impar, b un entero positivo, primo relativo con N, y q un primo divisor de $N-1$. Sea $N-1=q^s t$, con q no divisor de t. Entonces N es q-probable primo base b si y sólo si se cumple una de las siguientes dos condiciones:*

1. *Todo divisor primo de N es congruente con 1 módulo q y $b^t \equiv 1 \pmod{N}$.*
2. *Existe un i con $0 \leq i < s$ tal que N divide a $\Phi_q\left(b^{q^i t}\right)$.*

Más aún, si se cumple la condición 2, entonces todo divisor primo de N es congruente con 1 módulo q^{i+1}.

Demostración. Es claro que si $b^t \equiv 1 \pmod{N}$, entonces $\nu_q(|b|_p) = 0$ para todo primo p divisor de N, y así N es q-probable primo base b.

Ahora, si existe i con $0 \leq i < s$ tal que N divide a $\Phi_q\left(b^{q^i t}\right)$, entonces, del Corolario 3.5, $\left|b^{q^i t}\right|_p = q$, cualquiera sea el primo p divisor de N. Por lo tanto, si p es primo divisor de N se tiene $\nu_q\left(|b|_p\right) = i+1$, y en consecuencia N es q-probable primo base b.

Supongamos ahora que N es q-probable primo base b. Si $\nu_q(|b|_p) = 0$, entonces $|b|_p$ es divisor de t, y por tanto $b^t \equiv 1 \pmod{N}$. Si $\nu_q(|b|_p) = i+1 > 0$, se tiene que $|b|_N = q^{i+1} t_1$ para cierto entero t_1 divisor de t, y por tanto $b^{q^{i+1} t} \equiv 1 \pmod{N}$ y $b^{q^i t} \not\equiv 1 \pmod{p}$ para todo primo p divisor de N, y en consecuencia $\left|b^{q^i t}\right|_p = q$; del Corolario 3.5 resulta que N divide a $\Phi_q\left(b^{q^i t}\right)$, lo que concluye la prueba. ☑

No basta que b^t sea congruente con 1 módulo N para garantizar q-seudoprimalidad, como lo muestran los siguientes ejemplos.

Ejemplo 3.7. Sea $N = 133141 = 211 \times 631$, $b = 5$ y $q = 3$. Aquí $b^t \equiv 1 \pmod{N}$, y como q divide a $p-1$ para todo p divisor primo de N, entonces N es 3-seudoprimo base 5.

Sean $N = 6601 = 7 \times 23 \times 41$, $b = 3$ y $q = 5$. Como $N - 1 = 5^2 \times 264 = q^s t$, entonces b^t es congruente con 1 módulo N, y además q divide a algunos de los $p-1$, pero no todos; por tanto, N no es 5-seudoprimo base 3.

El siguiente ejemplo ha sido tomado de [14]. Sea $N = 1592075340241 = 23 \times 89 \times 12959 \times 60017$, $N - 1 = 2^4 \times 3 \times 5 \times 7 \times 11^2 \times 19 \times 31 \times 13297$; si tomamos $q = 7, b = 3$, se verifica que $b^t \equiv 1 \pmod{N}$, pero N no es 7-seudoprimo base 3, ya que 7 no divide a $p-1$ para ningún divisor primo p de N.

En esta dirección se tienen los siguientes dos resultados, análogos al Lema 4.1 del ya referido trabajo [14].

Proposición 3.8. *Sea N un seudoprimo base b, y sea q un divisor primo de $N-1$ tal que q no divide a $p-1$ para algún divisor primo p de N. Entonces $b^t \equiv 1 \pmod{N}$.*

Demostración. Sea $N-1=q^st$ con q no divisor de t, como $(b^t)^{q^s}\equiv 1$ mód N por la hipótesis sobre q se sigue que $b^t\equiv 1$ mód N. ☑

Como consecuencia se tiene:

Teorema 3.9. *Sean N un número de Carmichael y q un primo divisor de $N-1$ para el cual existe un primo p divisor de N tal que q no divide a $p-1$. Entonces, para todo b primo relativo con N, $b^t\equiv 1$ mód N.*

En consecuencia, si se levanta la condición de que todo factor primo de N sea de la forma $hq+1$ en la definición de q-probable primo, se tendrían números análogos a los números de Carmichael entre los q-probables primos.

Estamos ahora en condiciones de presentar el resultado principal de nuestro artículo, el cual establece una versión mejorada del Teorema de Pocklington, Teorema 1.4.

Teorema 3.10. *Sean N un entero impar, b un entero positivo, primo relativo con N, y q un primo divisor de $N-1$ tal que $N-1=q^st$ con q no divisor de t. Si existe un i con $0\leq i<s$ tal que N divide a $\Phi_q\left(b^{q^it}\right)$, entonces todo factor de N es congruente con 1 módulo q^{i+1}. Además, si $2(i+1)>s+\log_q t$, entonces N es primo.*

Demostración. Sólo queda por probar lo referente a la primalidad de N. Supongamos N compuesto, y sea p un divisor primo de N menor que $\sqrt{N}$; como $p\equiv 1$ mód q^{i+1}, entonces $q^{i+1}\leq p-1<\sqrt{N}$; luego $q^{2(i+1)}<N=q^st+1$, lo cual contradice la desigualdad $2\,(i+1)>s+\log_q t$. ☑

El Teorema anterior efectivamente refina el Teorema de Pocklington, tal como se muestra en los ejemplos siguientes.

Ejemplo 3.11. Sea $N=703=19\times 37$, $N-1=2\times 3^3\times 13$, $b=q=3$. Como N divide a $\Phi_q(b^{qt})$, entonces del Teorema 3.10 se sigue que q^2 divide a $p-1$ para todo primo p divisor de N. Dado que $\mathrm{mcd}(3^{(N-1)/3}-1,N)\neq 1$, el Teorema de Pocklington no puede aplicarse, con $b=3$, para ningún F que sea divisible por q.

Algo similar ocurre con $N=221761=211\times 1051$, $N-1=2^6\times 3^2\times 5\times 7\times 11$, tomando nuevamente $b=q=3$, como N divide a $\Phi_q(b^t)$ entonces el Teorema 3.10 implica que q divide a $p-1$ para todo primo p divisor primo de N, pero nuevamente no se puede aplicar el Teorema de Pocklington ya que $\mathrm{mcd}(3^{(N-1)/3}-1,N)\neq 1$.

Ejemplo 3.12. Para el entero $N=1459$ se tiene $N-1=3^6\times 2$, así que al hacer $b=2$ y $q=3$, se verifican las condiciones del Teorema 3.10 con $i=4$. Puesto que $\mathrm{mcd}(2^{(N-1)/q}-1,N)=N$, no se puede utilizar el Teorema de Pocklington con ningún factor F de $N-1$ y $b=2$. Se presenta igual deficiencia del Teorema de Pocklington si se trabaja con $b=5$ y $q=3$.

Agradecimientos. Los autores son miembros del grupo de investigación: Álgebra, Teoría de Números y Aplicaciones, ERM. Los resultados presentados en este artículo hacen parte del proyecto de investigación "*La propiedad de Midy: una herramienta para distinguir números primos de compuestos*", financiado por la Vicerrectoría de Investigaciones, Postgrados y Relaciones Internacionales de la Universidad de Nariño. Los autores agradecen a los evaluadores del artículo por sus sugerencias y recomendaciones las cuales ayudaron a mejorar la presentación final del mismo.

Referencias

[1] Adleman L.M., Pomerance C. and Rumely R.S., "On distinguishing prime numbers from composite numbers", *Ann. of Math.* (2) 117 (1983), no. 1, 173–206.

[2] Agrawal M., Kayal N. and Saxena N., "PRIMES is in P", *Ann. of Math.* (2) 160 (2004), no. 2, 781–793.

[3] Berrizbeitia P., "Sharpening PRIMES is in P for a large family of numbers", *Math. Comp.* 74 (2005), no. 252, 2043–2059.

[4] Brillhart J. and Selfridge J.L., "Some factorizations of $2^n \pm 1$ and related results", *Math. Comp.* 21 (1967), 87-96; corrigendum, ibid. 21 (1967), 751.

[5] Castillo J.H., García-Pulgarín G. and Velásquez-Soto J.M., "Structure of associated sets to Midy's Property", *Mat. Enseñ. Univ.* 20 (2012), no. 1, 21–28.

[6] Cheng Q., "Primality proving via one round in ECPP and one iteration in AKS", *J. Cryptology.* 20 (2007), no. 3, 375–387.

[7] Crandall R. and Pomerance C., *Prime numbers. A computational perspective*, Springer, New York, 2005.

[8] García-Pulgarín G. and Giraldo H., "Characterizations of Midy's property", *Integers* 9 (2009), 191–197.

[9] Gauss C.F., "Disquisitiones arithmeticae", in *Colección Enrique Pérez Arbeláez* , Academia Colombiana de Ciencias Exactas, Físicas y Naturales, Translated from the Latin by Hugo Barrantes Campos, Michael Josephy and Ángel Ruiz Zúñiga, with a preface by Ruiz Zúñiga, 10 (1995).

[10] Lenstra H.W. Jr. and Pomerance C., "Primality testing with gaussian periods", https://www.math.dartmouth.edu/ carlp/aks041411.pdf, consultado el día 22 de abril de 2014, unpublished.

[11] Motose K., "On values of cyclotomic polynomials. II", *Math. J. Okayama Univ.* 37 (1995), 27–36.

[12] Nathanson M.B., *Elementary methods in number theory*, Springer-Verlag, New York, 2000.

[13] Shevelev V., Castillo J.H., García-Pulgarín G. and Velásquez-Soto J.M., "Overpseudoprimes, and Mersenne and Fermat Numbers as Primover Numbers", *J. Integer Seq.* 15 (2012), no. 7, 1-10.

[14] Zhang Z., "Notes on some new kinds of pseudoprimes", *Math. Comp.* 75 (2006), no. 253, 451–460.