Minerva Journal
ISSN-e: 2697-3650 Vol.4, Núm. 10, (pp. 122-134)
https://doi.org/10.47460/minerva.v4i10.111

Conteo de los números primos en sucesiones aritméticas

Pedro R. Suárez Surí
https://orcid.org/0000-0002-5237-7606
pedro1951rivero@gmail.com
Investigador independiente
Quito, Ecuador

Recibido (13/07/2022), Aceptado (09/01/2023)

Resumen. - En el presente trabajo se presentan los elementos teóricos que fundamentan el cálculo de la función contadora de números primos, $\pi(x)$, basados en propiedades de las sucesiones (6n-1) y (6n+1), $n \geq 1$. Como resultado se exponen criterios suficientes de primalidad para los términos de ambas sucesiones que sustentan un algoritmo computacional determinístico que reduce la cantidad de operaciones en el cálculo de la función $\pi(x)$ al exonerar del análisis a todos los múltiplos de 3; y en el proceso de análisis de primalidad de un término particular, se excluyen las divisiones por el factor 3. Tal algoritmo es posible aplicarlo en la búsqueda de números primos en cada sucesión por separado, posibilidad que permite reducir aproximadamente a la mitad el tiempo de búsqueda de números en aplicaciones prácticas.

Palabras clave: Función contadora de números primos, criterio de primalidad, algoritmo determinístico, términos puros en sucesiones aritméticas, términos mezclados en sucesiones aritméticas.

Counting prime numbers in arithmetic sequences

Abstract. - This paper presents the theoretical elements that support the calculation of the prime number counting function, $\pi(x)$, based on properties of the sequences (6n-1) and (6n+1), $n \geq 1$. As a result, Sufficient primality criteria are exposed for the terms of both sequences that support a deterministic computational algorithm that reduces the number of operations in calculating the function $\pi(x)$ by exonerating all multiples of 3 from the analysis. In analyzing the primality of a particular term, the divisions by factor 3 are excluded. Such an algorithm can be applied to the search for prime numbers in each sequence separately, a possibility that allows approximately half the time of number search in practical applications.

Keywords: Counting function of prime numbers, primality criterion, deterministic algorithm, pure terms in arithmetic sequences, mixed terms in arithmetic sequences.

CC BY

I. INTRODUCCIÓN

La función $\pi(x)$ que cuenta la cantidad de números primos hasta el número real x, ha motivado a muchos investigadores a buscar una solución que permita calcular este número con exactitud. Este empeño ha impulsado el desarrollo de la teoría de los números abordando el problema por distintos enfoques y se han establecido algoritmos determinísticos o probabilísticos, entre los cuales se encuentran los siguientes:

a) El algoritmo de AKS (Manindra Agrawal, Neeraj Kayal y Nitin Saxena) establecido en el 2002 [1], es un algoritmo de primalidad determinista en tiempo polinomial. Es el primer criterio de primalidad con estas características, a pesar de lo cual no es lo suficientemente eficiente para ser utilizado ampliamente en aplicaciones prácticas.
b) El test de primalidad probabilístico de Miller-Rabin [2], por su naturaleza probabilística, tiene la insuficiencia que puede proporcionar resultados erróneos con una probabilidad pequeña, a pesar de lo cual es el test que más se ha utilizado en aplicaciones criptográficas.
c) El test de primalidad determinista de Goldwasser-Killian basado en curvas elípticas [3], es una solución con otro enfoque para el problema de primalidad. Según el autor, se considera uno de los métodos más rápidos para probar primalidad de números naturales.
d) El test de primalidad determinista de secuencia de raíz digital tesla Zollner es otro intento para resolver el problema de primalidad parte de las sucesiones (6n-1) y (6n+1) y está basado en la teoría de la raíz digital de Tesla Zollner. En este sentido, "el Algoritmo de Primalidad desarrollado, tiene un comportamiento funcional de orden cuatro, O (n4), el cual puede ser optimizado, mejorando las condiciones iniciales de la estructura secuencial del algoritmo, ya que los procedimientos de cálculos son sencillos, con simples operaciones aritméticas básicas" [4].

Además de estas pruebas de primalidad existen otros algoritmos y variantes de algunos de los mencionados que aportan avances en este campo, sin embargo, hasta la fecha no se ha encontrado una solución satisfactoria a tal problema.

En el presente artículo se presenta el resultado de otro intento de solución a esta problemática, basado en propiedades elementales de las sucesiones aritméticas $(6n-1)$ y $(6n+1)$. En base a propiedades de estas sucesiones, se han establecidos criterios suficientes para la primalidad de cualquiera de sus términos y establecido algoritmos computacionales determinísticos para calcular con exactitud la cantidad de números primos en cada una de estas sucesiones hasta cualquier número x, en consecuencia, para la función contadora de primos $\pi(x)$. Sin pretender comparar en eficiencia esta solución con los algoritmos existentes, se presenta como otro camino en que se puede trabajar en la búsqueda de la solución al problema.

En la exposición de los resultados de esta investigación se presentan las secciones: conceptos básicos y propiedades, criterios de primalidad, fórmulas computacionales para el cálculo de la función $\pi(h)$, algoritmos computacionales, resultados y conclusiones.

II. DESARROLLO

A. Conceptos básicos y propiedades

En este epígrafe se presentan algunas propiedades de las sucesiones enunciadas que permiten justificar los criterios de primalidad que se exponen posteriormente.

Proposición 1.

Todo número primo mayor que 3 es un término de la sucesión $(a_n) = (6n-1)$; o de la sucesión $(b_n) = (6n+1); n \in N\,; n \geq 1$.

Demostración

Sea p>3 un número primo cualesquiera, entonces solo tiene los factores 1 y p, luego como p es impar y el factor tres no está en p, entonces el factor 3 estará en $p-1$ o en $p+1$ y como $p-1$ y $p+1$ son números pares entonces resulta:

Si $p-1$ es múltiplo de tres entonces es múltiplo de 6 (par y divisible por 3) entonces $p-1 = 6n\,; n \in N$; luego $p = 6n+1$.

Si $p+1$ es múltiplo de 3 entonces es múltiplo de 6 (par y divisible por 3) entonces $p+1 = 6n\,; n \in N$; luego $p = 6n-1$.

En lo que sigue, los términos de las sucesiones $(a_n) = (6n-1)$ y $(b_n) = (6n+1)$ con n ≥ 1 se denominan candidatos a primo de tipo A y tipo B respectivamente.

Algunas notaciones que se utilizan en este trabajo son:

La cantidad de candidatos a primos menores o iguales a un número real x se denota por los símbolos Cp(x) o $Cp_a(x)$ o $Cp_b(x)$, para referirse respectivamente al total de términos en ambas sucesiones hasta el número x, a los términos de la sucesión (a_n) hasta x, términos tipo A, o a los términos de la sucesión (b_n), tipo B, hasta x.

La cantidad de candidatos a primos que son menores o iguales a un número real x se calculan por las fórmulas:

$$Cp_a(h) = \left[\frac{x+1}{6}\right]\,,\;\; Cp_b(h) = \left[\frac{x-1}{6}\right] \text{ y } \;\; Cp(x) = \; Cp_a(x) + Cp_b(x) = \left[\frac{x+1}{6}\right] + \left[\frac{x-1}{6}\right] \quad (1)$$

Estas fórmulas se obtienen directamente de las inecuaciones $6n-1 \leq x$ y $6n+1 \leq x$, teniendo en cuenta que los términos de estas sucesiones son números naturales.

La expresión [x] indica parte entera del número x o función piso de x.

De la proposición 1 se deriva que el conjunto de los candidatos a primos está constituido por los números impares mayores o iguales a 5, que no son múltiplos de 3.

Otras notaciones:

$Co(x)$ indica la cantidad de candidatos a primos compuestos menores o iguales a x.

$Co_a(x)$ indica la cantidad de candidatos a primo del tipo **A** menores o iguales a **x,** que son compuestos; de igual forma $Co_b(x)$ indica la cantidad de compuestos de tipo **B** menores o iguales a x.

$\pi^*(x)$ es la cantidad de números primos de tipo **A** y tipo **B,** menores o iguales a **x** excluyendo a 2 y 3. Y $\pi^*{}_a(x)\;\; y \;\; \pi^*{}_b(x)$ indican la cantidad de primos en x, de tipo **A** o tipo **B** respectivamente.

De lo visto hasta aquí podemos afirmar que un candidato primo es un número primo o un número compuesto que no es par ni múltiplo de tres, luego si se puede calcular la cantidad de candidatos a primos hasta un número real x que son compuestos, por diferencia con Cp(x) podemos determinar la cantidad de primos hasta ese número x mediante las ecuaciones siguientes:

$$Cp(x) = \pi^*(x) + \; Co(x),\; Cp_a(x) = \pi^*{}_a(x) + \; Co_a(x) \;\; y \; Cp_b(x) = \pi^*{}_b(x) + \; Co_b(x) \quad (2)$$

Veamos algunas propiedades de las sucesiones $(a_n)\ y\ (b_n)$.

B. Propiedades de los términos de las sucesiones $(a_n) = (6n-1)$ *y* $(b_n) = (6n+1)$ *con n ≥ 1.*

Proposición 2

El producto de dos términos de la sucesión (a_n) es un término de la sucesión (b_n).

Demostración

Sean n y m números naturales cualesquiera, luego $6n-1$ y $6m-1$ son dos términos cualesquiera de la sucesión (a_n).

$(6n-1)(\,6m-1\,) = 36nm-6n-6m+1 = 6(6nm-n-m)+1\ \epsilon\,(b_n)$ (3)

Las proposiciones que siguen se demuestran de forma semejante o aplicando reiteradamente las proposiciones planteadas con anterioridad.

Proposición 3

El producto de un término de la sucesión (a_n) y un término de la sucesión (b_n) es un término de la sucesión (a_n)

Proposición 4

El producto de dos términos de la sucesión (b_n) es un término de la sucesión (b_n).

Proposición 5

El producto de cualquier cantidad de términos de la sucesión (b_n) es un término de la sucesión (b_n).

Proposición 6

El producto de una cantidad impar de términos de la sucesión (a_n) ,tipo A, es un término tipo A.

Proposición 7

El producto de una cantidad par de términos tipo A es un término tipo B.

Proposición 8

Todo término compuesto de la sucesión (a_n) puede ser representado como el producto de una cantidad impar de factores primos tipo A y de cualquier cantidad de factores primos tipo B, pudiendo ser cero la cantidad de factores tipo B.

Propiedad 9

Un término h de la sucesión (a_n) es compuesto si y solo si se puede expresar como producto de un término tipo A y un término tipo B.

C. Clasificación de los términos de las sucesiones $(a_n)\ y\ (b_n)$ *según el tipo de sus factores primos*

Los términos de las sucesiones $(a_n)\ y\ (b_n)$ se pueden agrupar en conjuntos disjuntos según el tipo de factores que contienen:

Definición: Un término de las sucesiones $(a_n)\ o\ (b_n)$ se denomina puro cuando solo contiene factores primos tipo A o tipo B respectivamente.

Ejemplo:17, 125 =5^3 y 5^2.11=275 son términos puros tipo A y 7, 49=7.7 y 91=7.13 son términos puros tipo B.

Los términos compuestos de estas sucesiones que no son puros le denominamos mezclados.

Ejemplo: 35=5.7 es un término mezclado de (a_n) y 175=25. 7 es un término mezclado de (b_n).

Los términos de la sucesión (b_n) que solo contienen factores primos tipo A, se denominan bpuroa.

Ejemplos: $25 = 5^2\ ,\ 55 = 5 \cdot 11$

Al conjunto de términos de la sucesión (b_n) que no son puros tipo B se denominan términos mezclados tipo B.

Proposición 10

Todo término compuesto de la sucesión (b_n) se puede expresar como producto de dos términos tipo A o como producto de dos términos puros tipo B.

D. Criterios para determinar si un término de las sucesiones (A_n) o (b_n) es un número primo

La forma más simple para determinar si un término h de estas sucesiones es compuesto es dividirlo por todos los números primos menores o iguales a su raíz cuadrada; pero esto tiene el inconveniente del costo computacional que genera el espacio necesario para guardar los números primos conocidos y luego recuperar la información sobre la primalidad de los términos necesarios de estas sucesiones para utilizarlos en las operaciones requeridas; por tal motivo en este trabajo se presenta una solución que no necesita de la condición de primalidad de los términos de estas sucesiones; pero bastaría guardar los primos encontrados hasta $\sqrt{h}$ y llamarlos en el algoritmo cuando se necesiten, es decir, los criterios son válidos si se divide solo por los números primos, cuestión que será conveniente cuando se trabaje con números grandes.

Al menos para números pequeños (menores a 32 401) resulta más ventajoso trabajar con todos los términos de las sucesiones $(a_n)\ o\ (b_n)$ que son menores que $\sqrt{h}$, que recuperar la información de los primos encontrados para dividir solo por ellos; comportamiento que pudiera cambiar con números grandes.

Presentamos continuación algunos criterios que permiten determinar con exactitud si un término de las sucesiones anteriores es primo o compuesto.

E. Primos en la sucesión $(a_n) = (6n - 1);\ n \in \mathbb{N}$

En base a las propiedades de los términos de las sucesiones (a_n) y (b_n), se pueden establecer los criterios siguientes:

Criterio 1

Criterio suficiente para la condición de compuesto de un término de la sucesión (a_n) en base a los candidatos a primo de tipo B.

Sea $h = 6k - 1; k \in \mathbb{N}$. Si $\exists\ a_i\, \epsilon (a_n)\ con\ a_i \leq \frac{h}{5}\ :\ C_{pb}\left(\frac{h}{a_i}\right) - C_{pb}\left(\frac{h-6}{a_i}\right) = 1$ entonces h es compuesto de tipo A.

Demostración

Supongamos que $\exists\ a_i\, \epsilon (a_n)\ con\ a_i \leq \frac{h}{5}\ : C_{pb}\left(\frac{h}{a_i}\right) - C_{pb}\left(\frac{h-6}{a_i}\right) = 1$, esto significa que en $\frac{h}{a_i}$ los candidatos a primo tipo B se incrementan en una unidad, es decir, entre $\left(\frac{h-6}{a_i}\right)$ y $\left(\frac{h}{a_i}\right)$ existe un candidato primo b_j , tipo B, tal que

$\frac{h-6}{a_i} < b_j \leq \frac{h}{a_i}$, multiplicando por a_i se obtiene $h-6 < a_i\, b_j \leq h$, como los términos consecutivos de la sucesión (a_n) se diferencian en 6 unidades y h es un término de (a_n) y por la propiedad 2, $a_i\, b_j$ también es un término de (a_n) entonces $h = a_i\, b_j$ es un compuesto de la sucesión (a_n).

La suma de las diferencias $T = \sum_{i=5}^{a_i \leq \frac{h}{5}} \left(C_{pb}\left(\frac{h}{a_i}\right) - C_{pb}\left(\frac{h-6}{a_i}\right)\right)$ (4) del criterio anterior indica la cantidad de factores primos tipo A distintos que existen en la descomposición en factores del número h, lo cual determina cuántos productos distintos de dos factores originan al mismo número h, es decir, si queremos contar cuántos compuestos existe en la sucesión (a_n) hasta h, se contaría T-1 compuestos de más; sin embargo si se suma el signo(T) para todos los términos de la sucesión (a_n) hasta h, se obtendría la cantidad exacta de compuestos hasta H. Pero esta solución tiene un costo computacional mucho mayor que los criterios que se presentan a continuación.

El contrarrecíproco del criterio 1 es una condición suficiente de primalidad para los términos de (a_n) :

Criterio 2

Criterio de primalidad

Sea $h = 6k-1; k \in \mathbb{N}$. Si $\forall\, a_i \epsilon (a_n)$ con $a_i \leq \frac{h}{5}$ se cumple $C_{pb}\left(\frac{h}{a_i}\right) - C_{pb}\left(\frac{h-6}{a_i}\right) = 0$ entonces h es un número primo.

El Criterio 1 para la condición de compuesto de un término de la sucesión (a_n), se ha planteado utilizando los Cpb, un criterio semejante también se puede plantear en función de los Cpa.

Criterio 3

Sea $h = 6k-1; k \in \mathbb{N}$. Si $\exists\, b_i \epsilon (b_n) con\, b_i \leq \frac{h}{7}:\ C_{pa}\left(\frac{h}{b_i}\right) - C_{pa}\left(\frac{h-6}{b_i}\right) = 1$ entonces h es compuesto de tipo A.

Demostración

Supongamos que $\exists\, b_i \epsilon (b_n)\, con\, b_i \leq \frac{h}{7}\ : C_{pa}\left(\frac{h}{b_i}\right) - C_{pa}\left(\frac{h-6}{b_i}\right) = 1$, esto significa que en $\frac{h}{b_i}$ los candidatos a primo tipo A se incrementan en una unidad, es decir, entre $\left(\frac{h-6}{b_i}\right)$ y $\left(\frac{h}{b_i}\right)$ existe un candidato primo a_j , tipo A, tal que

$\frac{h-6}{b_i} < a_j \leq \frac{h}{b_i}$, multiplicando por b_i se obtiene $h-6 < a_j\, b_i \leq h$, como los términos consecutivos de la sucesión (a_n) se diferencian en 6 unidades y h es un término de (a_n) y por la propiedad 2, $a_j\, b_i$ también es un término de (a_n) entonces $h = a_j\, b_i$ es un compuesto de la sucesión (a_n).

Mediante la aplicación de estos criterios se puede elaborar un algoritmo para determinar la condición de compuesto o primo de un término h de la sucesión (a_n) .

Para el caso de los términos de la sucesión (a_n), la diferencia

$d = C_{pb}\left(\frac{h}{a_i}\right) - C_{pb}\left(\frac{h-6}{a_i}\right)$ se puede transformar aplicando las fórmulas para el cálculo de los candidatos a primo; permitiendo de este modo operar con números más pequeños para reducir la complejidad de los cálculos en el algoritmo correspondiente.

$$d = C_{pb}\left(\frac{h}{a_i}\right) - C_{pb}\left(\frac{h-6}{a_i}\right) = \left[(\frac{h}{a_i} - 1)/6\right] - \left[\frac{\frac{h-6}{a_i} - 1}{6}\right] = \left[\frac{h-a_i}{6a_i}\right] - \left[\frac{h-6-a_i}{6a_i}\right]$$

$$= \left[\frac{6k-1-6i+1}{6a_i}\right] - \left[\frac{6k-1-6-6i+1}{6a_i}\right] = \left[\frac{k-i}{a_i}\right] - \left[\frac{k-i-1}{a_i}\right] = \left[\frac{k-i}{a_i}\right] - \left[\frac{k-i}{a_i} - \frac{1}{a_i}\right] \quad (5)$$

Propiedad 11

Si el cociente $\frac{k-i}{a_i} \in \mathbb{N}$ entonces la diferencia $d = \left[\frac{k-i}{a_i}\right] - \left[\frac{k-i-1}{a_i}\right] = 1.$

Demostración

Para cada $a_i \in (a_n)$ se tiene una sucesión aritmética (a_k) donde $\frac{k-i-1}{a_i}$ y $\frac{k-i}{a_i}$ son términos consecutivos con una diferencia $\frac{1}{a_i}$ tal que $0 < \frac{1}{a_i} < 1$

Supongamos que $\frac{k-i}{a_i} \in \mathbb{N}$. En este caso $\left[\frac{k-i}{a_i}\right] - \left[\frac{k-i}{a_i} - \frac{1}{a_i}\right] = E - \left[E - \frac{1}{a_i}\right]$; pero $\left[E - \frac{1}{a_i}\right] = E - 1$ luego $\left[\frac{k-i}{a_i}\right] - \left[\frac{k-i}{a_i} - \frac{1}{a_i}\right] = E - E + 1 = 1$

De forma semejante se cumple:

Propiedad 12

Si el cociente $\frac{k+j}{b_j} \in \mathbb{N}$ entonces la diferencia $d = \left[\frac{k+i}{b_i}\right] - \left[\frac{k+i-1}{b_i}\right] = 1.$

La demostración sigue la misma vía que en la propiedad 11

De acuerdo con este resultado las diferencias $d = \left[\frac{k-i}{a_i}\right] - \left[\frac{k-i-1}{a_i}\right] = 1$ se puede sustituir en los criterios enunciados anteriormente por $d = \frac{k-i}{a_i} - \left\lfloor\frac{k-i}{a_i}\right\rfloor = 0$ (En este caso si $d = 0$ el término h es compuesto y si para todos los a_i se cumple que $d \neq 0$ entonces h es primo.) También se puede sustituir por la expresión equivalente $d = (k-i)\ Mod\ a_i = 0$ o $d = (k+i)\ Mod\ b_i = 0$ que son expresiones respectivamente equivalen tes a $\frac{k-i}{a_i} \in \mathbb{N}$ y $\frac{k+j}{b_j} \in \mathbb{N}$.

Si se aplica la propiedad 9, que plantea que todo término compuesto h de (a_n) se puede expresar como $h = a_i b_j$, se puede reducir la cantidad de operaciones. En lugar de calcular todas las divisiones por los a_i con $i \leq \left[\frac{k+1}{7}\right]$ o por los b_i con $i \leq \left[\frac{k-1}{5}\right]$, es posible calcular los cocientes solo para $a_i \leq \sqrt{h}$ y los $b_j \leq \sqrt{h}$ debido a que si $a_i \leq \sqrt{h}$ entonces $b_j \geq \sqrt{h}$, y viceversa, si $b_j \leq \sqrt{h}$ entonces $a_i \geq \sqrt{h}$, de acuerdo con esto y la transformación realizada a la diferencia d, el criterio para la condición de compuesto de un término de la sucesión (a_n), se puede expresar de la forma siguiente:

Criterio 4

Un término h de la sucesión (a_n) es compuesto si $\exists\ a_i\ \epsilon(a_n)$ con $a_i \leq \sqrt{h}$ tal que $\frac{k-i}{a_i} - \left[\frac{k-i}{a_i}\right] = 0$ o $\exists b_j\ \epsilon(b_n)$ con $b_j \leq \sqrt{h}$ se cumple $\frac{k+j}{b_j} - \left[\frac{k+j}{b_j}\right] = 0.$

Este criterio se puede expresar utilizando las expresiones equivalentes $(k-i)Mod\ a_i = 0$ y $(k+j)Mod\ b_j = 0$ respectivamente.

Criterio 4.1

Un término h de la sucesión (a_n) es compuesto si $\exists\ a_i\ \epsilon(a_n)$ con $a_i \leq \sqrt{h}$ tal que $(k-i)Mod\ a_i = 0$ o $\exists b_j\ \epsilon(b_n)$ con $b_j \leq \sqrt{h}\ tal\ que\ (k+j)Mod\ b_j = 0$.

Criterio 5

Un término h de la sucesión (a_n) es primo si y solo si $\forall\ a_i\ \epsilon(a_n)$ con $a_i \leq \sqrt{h}$ se cumple $\frac{k-i}{a_i} - \left[\frac{k-i}{a_i}\right] \neq 0$ y $\forall\ b_j\ \epsilon(b_n)$ con $b_j \leq \sqrt{h}$ se cumple $\frac{k+j}{b_j} - \left[\frac{k+j}{b_j}\right] \neq 0$.

F. Primos en la sucesión $(b_n) = (6n+1);\ n \in \mathbb{N}$

Para determinar si un término de la sucesión (b_n) es compuesto se tiene en cuenta que todo término compuesto de esta sucesión es un término mezclado o es un término puro tipo B.

Criterio para los términos de la sucesión (b_n)

Todo término mezclado h de (b_n) se obtiene como el producto cada término a_i de (a_n) por todos los Cpa $\leq \frac{h}{a_i}$. Estos generan los términos mezclados de (b_n), que pueden ser términos Bapuros, que son aquellos que solo contienen factores primos tipo A o términos tipo B mezclados que contienen factores primos tipo A y factores primos tipo B.

Criterio 6

Sea $h = 6k+1; k \in \mathbb{N}$. Si $\exists\ a_i\,\epsilon(a_n)\ con\ a_i \leq \frac{h}{5}:\ C_{pa}\left(\frac{h}{a_i}\right) - C_{pa}\left(\frac{h-6}{a_i}\right) = 1$ o $\exists\ b_i\,\epsilon(b_n)\ con\ b_i \leq \frac{h}{7}:$ $C_{pb}\left(\frac{h}{b_i}\right) - C_{pb}\left(\frac{h-6}{b_i}\right) = 1$ entonces h es compuesto.

Demostración

Caso 1

Sea h un término de la sucesión (b_n).

Supongamos que $\exists\ a_i\,\epsilon(a_n)\ con\ a_i \leq \frac{h}{5}: C_{pa}\left(\frac{h}{a_i}\right) - C_{pa}\left(\frac{h-6}{a_i}\right) = 1$, esto significa que entre $\left(\frac{h-6}{a_i}\right)$ y $\left(\frac{h}{a_i}\right)$ existe un candidato primo a_j tipo A, tal que

$\frac{h-6}{a_i} < a_j \leq \frac{h}{a_i}$, multiplicando por a_i se obtiene $h-6 < a_i\,a_j \leq h$, como los términos consecutivos de la sucesión (b_n) se diferencian en 6 unidades y h es un término de (b_n) y $a_i\,a_j$ también es un término de (b_n) entonces $a_i\,a_j = h$ es un compuesto mezclado de la sucesión (b_n). ($\frac{h-6}{a_i} \neq a_j$ porque la diferencia $\frac{h}{a_i} - \frac{h-6}{a_i} = \frac{6}{a_i} \leq 1{,}2\ \forall\ a_i$ luego si $\frac{h-6}{a_i} \leq a_j$ resulta que $C_{pa}\left(\frac{h}{a_i}\right) - C_{pa}\left(\frac{h-6}{a_i}\right) = 0$)

Caso 2

Supongamos que $\exists\ b_i\,\epsilon(b_n)\ con\ b_i \leq \frac{h}{7}: C_{pb}\left(\frac{h}{b_i}\right) - C_{pb}\left(\frac{h-6}{b_i}\right) = 1$, esto significa que entre $\left(\frac{h-6}{b_i}\right)$ y $\left(\frac{h}{b_i}\right)$ existe un candidato primo b_j tipo B, tal que

$\frac{h-6}{b_i} < b_j \leq \frac{h}{b_i}$, multiplicando por b_i se obtiene $h-6 < b_i\, b_j \leq h$, como los términos consecutivos de la sucesión (b_n) se diferencian en 6 unidades y h es un término de (b_n) y $b_i\, b_j$ también es un término de (b_n) entonces $b_i\, b_j = h$ es un compuesto de la sucesión (b_n).

El contrarrecíproco del criterio anterior es el criterio de primalidad para un término de la sucesión (b_n).

Criterio 7

Sea $h = 6k+1; k \in \mathbb{N}$. Si $\forall\, a_i\, \epsilon(a_n)\ con\ con\ a_i \leq \frac{h}{5} :\ C_{pa}\left(\frac{h}{a_i}\right) - C_{pa}\left(\frac{h-6}{a_i}\right) = 0$ y $\forall\, b_i\, \epsilon(b_n)\ con\ b_i \leq \frac{h}{7} :\ C_{pb}\left(\frac{h}{b_i}\right) - C_{pb}\left(\frac{h-6}{b_i}\right) = 0$ entonces h es un número primo.

Para el caso de los términos de la sucesión (b_n) la primera proposición del criterio 6 se transforma en:

$d = C_{pa}\left(\frac{h}{a_i}\right) - C_{pa}\left(\frac{h-6}{a_i}\right) = \left[(\frac{h}{a_i}+1)/6\right] - \left[(\frac{h-6}{a_i}+1)/6\right] = \left[\frac{h+a_i}{6a_i}\right] - \left[\frac{h-6+a_i}{6a_i}\right] = \left[\frac{6k-1+6i+1}{6a_i}\right] - \left[\frac{6k-1-6+6i+1}{6a_i}\right] = \left[\frac{(k+i)}{a_i}\right] - \left[\frac{(k+i-1)}{a_i}\right]$ (6)

La segunda condición del criterio 6 se transforma en:

$d = C_{pb}\left(\frac{h}{b_j}\right) - C_{pb}\left(\frac{h-6}{b_j}\right) = \left[(\frac{h}{b_j}-1)/6\right] - \left[(\frac{h-6}{b_j}-1)/6\right] = \left[\frac{h-b_j}{6b_j}\right] - \left[\frac{h-6-b_j}{6b_j}\right] = \left[\frac{6k+1-6j-1}{6b_j}\right] - \left[\frac{6k+1-6-6j-1}{6b_j}\right] = \left[\frac{(k-j)}{b_j}\right] - \left[\frac{(k-j-1)}{b_j}\right]$ (7)

La primera condición del criterio 7 es equivalente a la propiedad 12.

Propiedad 12

Si el cociente $\frac{k+i}{a_i} \in \mathbb{N}$ entonces la diferencia $d = \left[\frac{k+i}{a_i}\right] - \left[\frac{k+i-1}{a_i}\right] = 1$.

(La demostración es semejante a la realizada en el criterio 11.)

La segunda condición del criterio 7 es equivalente a la propiedad 13.

Propiedad 13

Si el cociente $\frac{k-i}{b_i} \in \mathbb{N}$ entonces la diferencia $d = \left[\frac{k-i}{b_i}\right] - \left[\frac{k-i-1}{b_i}\right] = 1$.

(La demostración es semejante a la realizada en el criterio 11.)

El criterio de primalidad de un término de la sucesión (b_n) resulta de la negación del criterio 4 y el empleo de las siguientes equivalencias:

La expresión $\frac{k+i}{a_i} \in \mathbb{N}$ es equivalente a $\frac{k+i}{a_i} - \left[\frac{k+i}{a_i}\right] = 0$ o $(k+i)Mod\ a_i = 0$

La expresión $\frac{k-j}{b_j} \in \mathbb{N}$ es equivalente a $\frac{k-j}{b_j} - \left[\frac{k-j}{b_j}\right] = 0$ o $(k-j)Mod\ b_j = 0$

Criterio de primalidad de los términos de la sucesión (b_n)

Criterio 5

Un término h de la sucesión (b_n) es primo si $\forall\, a_i\ \epsilon(a_n)$ con $a_i \leq \sqrt{h}$ resulta $(k+i)Mod\ a_i = 0$ y $\forall\ b_j\ \epsilon(b_n)$ con $b_j \leq \sqrt{h}$ resulta $(k-j)Mod\ b_j = 0$.

III. METODOLOGÍA

La metodología empleada ha consistido en el análisis de las sucesiones (a_n) y (b_n) en cuanto a sus propiedades y su relación con los números compuestos hasta encontrar la regularidad de la formación de los números compuestos a partir de los términos de estas sucesiones y establecer criterios suficientes de primalidad sustentados en propiedades elementales. Posteriormente se procede a la implementación computacional de los criterios y análisis de los resultados.

IV. RESULTADOS

A. Fórmulas computacionales para el cálculo de la función $\pi(h)$

Según estos resultados se puede definir la función $\pi(h)$ mediante una fórmula computacional exacta; antes se definen las funciones $\pi_a(h)$ y $\pi_b(h)$ que determinan la cantidad de primos acumulados las sucesiones (a_n) y (b_n) respectivamente hasta el número h.

Sea $h = 6k - 1$

$$\pi_a(h) = k - 1 - \sum_{j=8}^{k}\left(sgn \sum_{i=1}^{\left[\frac{\sqrt{h}-1}{6}\right]} \left(\left[\frac{(j-i)}{a_i}\right] - \left[\frac{(j-i-1)}{a_i}\right]\right) + \; sgn \sum_{i=1}^{\left[\frac{\sqrt{h}+1}{6}\right]} \left(\left[\frac{(j+i)}{b_i}\right] - \left[\frac{(j+i-1)}{b_i}\right]\right)\right) \quad (8)$$

Donde $k = \left[\frac{h+1}{6}\right]$; $a_i = 6i - 1 \;\; b_i = 6i + 1$

Sea $h = 6k + 1$

$$\pi_b(h) = k - 1 - \sum_{j=8}^{k}\left(sgn \sum_{i=1}^{\left[\frac{\sqrt{h}+1}{6}\right]} \left(\left[\frac{(j+i)}{a_i}\right] - \left[\frac{(j+i-1)}{a_i}\right]\right) + sgn \sum_{i=1}^{\left[\frac{\sqrt{h}-1}{6}\right]} \left(\left[\frac{(j-i)}{b_i}\right] - \left[\frac{(j-i-1)}{b_i}\right]\right)\right) \quad (9)$$

Donde $k = \left[\frac{h-1}{6}\right]$; $a_i = 6i - 1$; $b_i = 6i + 1$

El 1 que se resta de K corresponde al compuesto que existe en cada sucesión hasta 43.

La sumatoria indica la cantidad de compuestos acumulados desde 47 hasta h.

Función $\pi(h)$

$$\pi(h) = 2 + \pi_a(h) + \pi_b(h) \quad (10)$$

El sumando 2 se refiere a los primos 2 y 3 que no se calculan en las fórmulas anteriores.

Las diferencias de las partes enteras que aparecen en estas fórmulas solo pueden tomar valores 1 o 0, lo que permite, en su implementación computacional, abandonar el ciclo correspondiente cuando aparece el primer 1; en tal caso no es necesario utilizar la función signo.

B. Implementación de los criterios expuestos en el cálculo de la función $\pi(h)$

La implementación de los criterios presentados anteriormente para calcular la función $\pi(h)$ se ha realizado mediante programación en VBA de Excel y se ha repetido el algoritmo para todos los términos de las sucesiones (a_n) y (b_n) desde 47 hasta 32401.

Para la implementación del procedimiento para cualquier número real $x \geq 37$ basta entrar el valor de x y calcular k mediante las ecuaciones $k = \left[\frac{x+1}{6}\right]$ o $k = \left[\frac{x-1}{6}\right]$ según se busque los valores de $\pi_a(h)$ o $\pi_b(h)$ respectivamente.

Algoritmo de primalidad para los términos de la sucesión (a_n)

H,l,k,m,n,a,b (enteros); d (double)

1-Entrar el valor de k y calcular $h = 6k - 1$.

2-Calcular $a = 6i - 1\ y\ d = (k - i)Mod\ a$ en un ciclo desde $i = 1$ hasta $m = int((Sqr(h) + 1)/6)$. Si $d = 0$ salir del ciclo y se pasa a 3.

3-Si $d = 0$ se concluye: h es compuesto; Si $d \neq 0$ se pasa a 4.

4-Calcular $b = 6i + 1\ y\ d = (k + i)Mod\ b$ en un ciclo desde $i = 1$ hasta $n = int((Sqr(h) - 1)/6)$. Si $d = 0$ salir del ciclo y se pasa a 5.

5- Si $d = 0$ se concluye: h es compuesto; Si $d \neq 0$ se concluye: h es primo.

Algoritmo de primalidad para los términos de la sucesión (b_n)

H,l,k,m,n,a,b (enteros); d (double)

1-Entrar el valor de k y calcular $h = 6k + 1$.

2-Calcular $a = 6i - 1\ y\ d = (k + i)Mod\ a$ en un ciclo desde $i = 1$ hasta $m = int((Sqr(h) + 1)/6)$. Si $d = 0$ salir del ciclo y se pasa a 3.

3-Si $d = 0$ se concluye: h es compuesto; Si $d \neq 0$ se pasa a 4.

4-Calcular $b = 6i + 1\ y\ d = (k - i)Mod\ b$ en un ciclo desde $i = 1$ hasta $n = int((Sqr(h) - 1)/6)$. Si $d = 0$ salir del ciclo y se pasa a 5.

5- Si $d = 0$ se concluye: h es compuesto; Si $d \neq 0$ se concluye: h es primo.

La implementación práctica de los algoritmos se realizó en una computadora Intel i3 4ta generación CPU 1.70 GHz 1.70 GHz con memoria RAM 12gb y HDD ssd sata 3.0.

Sin pretender considerar los resultados siguientes como un análisis de la complejidad computacional, sí pueden servir para valorar el comportamiento del tiempo del algoritmo analizado.

En el caso del algoritmo para los primos de la sucesión $(a_k = 6k - 1)$ se midió el tiempo para los valores de K desde 8 hasta 5400 a intervalos de 166 términos (términos desde 47 hasta 32399). A partir de la medición de los tiempos acumulados se establecieron modelos de regresión, resultando un modelo lineal ($Tiempo = (0{,}00007708K + 0{,}009,$ estadísticamente significativo (p=0,000; R^2=0,998) y un modelo potencial ($Tiempo = K^{0{,}927}$, estadísticamente significativo (p=0,000; R^2=0,998. Un modelo logarítmico resultó significativo con R^2=0,84. La estimación del tiempo del modelo potencial, para valores de K aproximadamente superiores a 4000 tienden a ser menores que en el modelo lineal. Considerando lo planteado en [5], pág. 210 sobre la comprobación del análisis de un algoritmo se observó que los cocientes Tiempo/K y Tiempo/(kln(k)) resultaron decrecientes por lo que se considera que ambos modelos sobreestiman el tiempo real, mientras

que el cociente Tiempo/(k ^0,927) es creciente, lo que indica que el modelo potencial subestima el tiempo real.

CONCLUSIONES

El algoritmo anterior tiene la ventaja que para determinar el valor de $\pi(x)$ solo hay que considerar los números impares $h \geq 5$ no divisibles por 3, que reducen, aproximadamente en 1/6 la cantidad de repeticiones del algoritmo y en cada h se excluye la división por 3 y sus múltiplos.

Los criterios presentados conducen a un algoritmo que calcula de forma exacta las funciones $\pi_a(h)$, $\pi_b(h)$ y $\pi(h) = 2 + \pi_a(h) + \pi_b(h)$.

Al realizar las divisiones utilizando el valor de k se disminuye el tamaño de los números objeto de análisis y con ello se reduce el tiempo de cálculo, cuestión probada empíricamente para números pequeños (menores a 32401). El algoritmo en su implementación, además de realizarse calculando los cocientes de todos los términos de ambas sucesiones menores o iguales a $\sqrt{h}$, se puede implementar utilizando solo los números primos menores o iguales a $\sqrt{h}$ encontrados en el proceso de análisis de ambas sucesiones.

Para el uso práctico de estos algoritmos en la búsqueda de números primos, se puede trabajar con algoritmos separados de búsqueda para primos tipo A y tipo B, disminuyendo aproximadamente a la mitad el tiempo de análisis de primalidad.

El algoritmo no se ha implementado para números grandes.

No se ha analizado la complejidad computacional de los algoritmos asociados a los criterios enunciados; pero con independencia de la eficiencia que pueda tener el algoritmo, el enfoque presentado puede representar otro sendero a explorar en la búsqueda de la solución al cálculo de la función $\pi(x)$ de forma exacta y eficiente.

La combinación del análisis de primalidad sobre estas sucesiones con otros criterios de primalidad pudiera incrementar la eficiencia de los algoritmos en aplicaciones prácticas.

Referencias

[1] V. Arroyo, «Estudio sobre primalidad con el algoritmo AKS,» Madrid, 2020.

[2] R. Martínez Zocón, L. Ortiz Céspedes, J. Horna Mercedes y A. Zavaleta Quipuscoa, «Algoritmos para pruebas de primalidad,» *Selecciones Matemáticas,* vol. 1, nº 02, p. 8, agosto-diciembre 2014.

[3] S. A. Ramírez Gajardo, Y. F. Vasquez Cea y C. Zenteno Acuña, «Curvas elípticas y test de primalidad,» Chillan, 2019.

[4] Z. Castellanos y Á. SandoVal, «Test de primalidad de secuencia de raíz digital Tesla Zollner,» *ResearchGate,* p. 8, septiembre 2022.

[5] M. Allen Weiss, Estructuras de datos en Java, cuarta edición ed., Pearson Educación, S.A., 2013, 2013, p. 945.

Pedro Suárez es de nacionalidad cubana, residente en Ecuador es licenciado en educación en la especialidad de Matemática y es Magister en Matemática aplicada, ha sido docente durante 53 años.