CARACTERIZACIÓN DE NÚMEROS PRIMOS

CHARACTERIZATION OF PRIME NUMBERS

Héctor Carlos Guimaray Huerta[1]

RESUMEN

Los números primos es motivo de investigación en la teoría de números; en la actualidad, no existe una fórmula que nos permita obtener dichos números, y que la distribución de los mismos se considera que es aleatoria. Lo que existe son métodos para averiguar si un número es primo o compuesto. En el presente artículo se presenta una caracterización de números primos que es el complemento de los números compuestos.

Palabras clave.- Divisor, Número primo, Número compuesto, Caracterización, Conjetura.

ABSTRACT

The prime numbers motivate the investigation in number theory; nowadays, does not exist a formula that allows get those numbers, and that the distribution thereof is considered random. There are methods to find whether a number is prime or composite. This article presents a characterization of prime numbers which is the complement of composite numbers.

Key words.- Divisor, Prime number, Composite number, Characterization, Conjecture.

INTRODUCCIÓN

En la teoría de números usando el concepto de divisor surgen los números primos, siendo su complemento de éstos los números compuestos. Existen teoremas que caracterizan los números primos; así, como métodos para averiguar si un determinado número es primo o compuesto. En el concepto de números primos existen muchas conjeturas, como por ejemplo la conjetura de los números primos gemelos que aún no está resuelta. En el presente artículo se da una caracterización de los números primos analizando como el complemento de los números compuestos; además, esbozando la función de distribución en un gráfico.

PRELIMINARES

Notación.- $\mathbb{N}$ es el conjunto de los números naturales.

Definición.- n $\in \mathbb{N}$ se llama número primo si sus únicos divisores son 1 y n [1, 5].

Notación.- $\mathbb{P} = \{ p \in \mathbb{N} \,/\, p$ es primo$\}$

Definición.- $n \in \mathbb{N}$ se llama número compuesto si n no es primo [3].

$\mathbb{N} \setminus \mathbb{P} = \{n \in \mathbb{N} /$ n es compuesto$\}$

Teorema fundamental de la aritmética.- Todo número natural n $\geq$ 2 puede ser expresado como el producto de números primos [4, 2].

Teorema de Eratóstenes.- Si n es compuesto entonces n tiene divisor primo p $\leq \sqrt{n}$. [7]

Números primos de Mersene.- Son los números primos del tipo $2^n - 1$.

Números primos de Fermat.- Son los números primos del tipo $2^n + 1$.

Pequeño teorema de Fermat.- Si $n \in \mathbb{N}$ no es divisible por p $\in \mathbb{N}$ entonces $n^p - 1$ es compuesto [6]. Este teorema apareció en 1636.

[1]Maestro, Docente de la Facultad de Ciencias de la Universidad Nacional de Ingeniería.

Teorema de Wilson.- p es primo si y solo si $(p - 1)! \equiv -1\ (p)$ [8].

Ejemplo:

n = 11
$\Longrightarrow$
(n -1)! = 3628800
$\Longrightarrow$
3628800 = 329891 x 11 – 1
$\Longrightarrow$
$(n-1)! \equiv -1\ (n)$
$\Longrightarrow$
11 es primo.

Definición.- Se dice que dos primos son gemelos si su diferencia es dos.

Primos gemelos.- 3 y 5, 5 y 7, 11 y 13, 17 y 19, …

Conjetura de primos gemelos.- $\exists$ infinitos primos p / p + 2 es también primo.

Conjetura de Goldbach.- Todo par mayor que 2, es la suma de dos primos.

4 = 2 + 2, 6 = 3 + 3, 8 = 3 + 5, 10 = 5 + 5, …

Conjetura de Legendre.- $\forall n \in \mathbb{N} \exists$ un primo entre n^2 y $(n+1)^2$.

Conjetura de Cramer. –

$$\lim_{n\to+\infty} sup \frac{p_{n+1} - p_n}{(logp_n)^2} = 1$$

Función π. – $\mathbb{N} \to \mathbb{N}$ donde π (n) es el número de primos $p \leq n$.

PROPUESTA DE INVESTIGACIÓN

Caracterización de números primos

Formulación de hipótesis.- La caracterización de números primos se obtiene analizando los números compuestos.

Proposición

$$\mathbb{N}\backslash\mathbb{P} = \bigcup_{n>2} \{nk/k \geq 2\}, n \in \mathbb{N}$$

Es decir, es la unión de dobles, triples, etc.

Prueba.-

$m \in \mathbb{N}\backslash\mathbb{P}$
$\Longleftrightarrow$
m es compuesto
$\Longleftrightarrow$
$m = n\,k \,/\, n \geq 2, k \geq 2$
$\Longleftrightarrow$
$$m \in \bigcup_{n>2} \{nk/k \geq 2\}$$

Proposición. –

$$\mathbb{N}\backslash\mathbb{P} = \bigcup_{n>2} \{nk/k \geq n\}, n \in \mathbb{N}$$

Es decir, los números compuestos se repiten para $2 \leq k \leq n-1$.

Prueba:

Se tiene que

$$\bigcup_{n>2} \{nk/k \geq n\} \subseteq \bigcup_{n>2} \{nk/k \geq 2\}$$

$\Rightarrow$

$$\bigcup_{n>2} \{nk/k \geq n\} \subseteq \mathbb{N}\backslash\mathbb{P}$$

Ahora, sea $m \in \mathbb{N}\backslash\mathbb{P}$
$\Rightarrow$
$m = n\,k \,/\, n \geq 2, k \geq 2$
i) $2 \leq k \leq n-1$
$\Rightarrow$
$m = k\,n \,/\, k \geq 2, n \geq k$
$\Rightarrow$
$$m \in \bigcup_{n>2} \{nk/n \geq k\}$$
$\Rightarrow$
$$m \in \bigcup_{n>2} \{nk/k > n\},$$

se vuelve a denotar las variables.
ii) $n \leq k$
$\Rightarrow$
$m = n\,k \,/\, n \geq 2, k \geq n$
$\Rightarrow$
$$m \in \bigcup_{n>2} \{nk/k \geq n\}$$

$$\text{Luego, } \mathbb{N}\backslash\mathbb{P} \subseteq \bigcup_{n>=2} \{nk/k \geq n\}$$

Proposición.

$$\mathbb{N}\backslash\mathbb{P} = \bigcup_{p\geq 2}\{pk \,/\, k \geq p\}, p \in \mathbb{P}$$

Es decir, los números compuestos se repiten.

Prueba.-

Se tiene que $\bigcup_{n>2}\{pk/k \geq p\} \subseteq \mathbb{N}\backslash\mathbb{P}$

Ahora, sea $m \in \mathbb{N}\backslash\mathbb{P}$

$\Rightarrow$

m = n k / k $\geq n \wedge$ n $\geq$ 2

Pero, n = p j / p $\in \mathbb{P} \wedge j \geq 1$

$\Rightarrow$

m = (p j) k / k $\geq n$

= p (j k) / k $\geq$ p; pues, n $\geq$ p

= p (j k) / j k $\geq$ j p

= p (j k) / j k $\geq$ p; pues, j p $\geq$ p

= p l / $l \geq$ p

$\Rightarrow$

$$m \in \bigcup_{p\geq 2}\{pk \,/k \geq p\}$$

$\Rightarrow$

$$\mathbb{N}\backslash\mathbb{P} = \bigcup_{p\geq 2}\{pk/k \geq p\}$$

Observación.-

$$\mathbb{P} = \mathbb{N}\backslash\bigcup_{p\geq 2}\{pk/k \geq p\}, p \in \mathbb{P}$$

Proposición.-

$\mathbb{N}\backslash\mathbb{P} = \{n \in \mathbb{N}/n = p^2 + pk$ donde $p \in \mathbb{P} \wedge k \in \mathbb{N} \cup \{0\}\}$.

Prueba:

n $\in \mathbb{N}\backslash\mathbb{P}$

$\Leftrightarrow$

n = p k / k $\geq p$, p $\subset \mathbb{P}$

$\Leftrightarrow$

n = p (p + j) / j $\geq$ 0 con j = k – p

= $p^2 + pj$ donde p $\in \mathbb{P} \wedge$ j $\in \mathbb{N} \cup \{0\}$

Observación.- i) $n \in \mathbb{N}\backslash\mathbb{P}$ si y solo si $\exists(p, k) \in \mathbb{P}x\mathbb{N} \cup \{0\}/ n = p^2 + pk$

ii) $n \in \mathbb{N}\backslash\mathbb{P}$ si y solo si $\exists$ solución de n $= p^2 + pk$ en $\mathbb{P}x\mathbb{N} \cup \{0\}$

iii) n$\in \mathbb{P}$ si y solo si n $\neq p^2$ + p k $\forall$(p, k) $\in \mathbb{P}x\mathbb{N} \cup \{0\}$

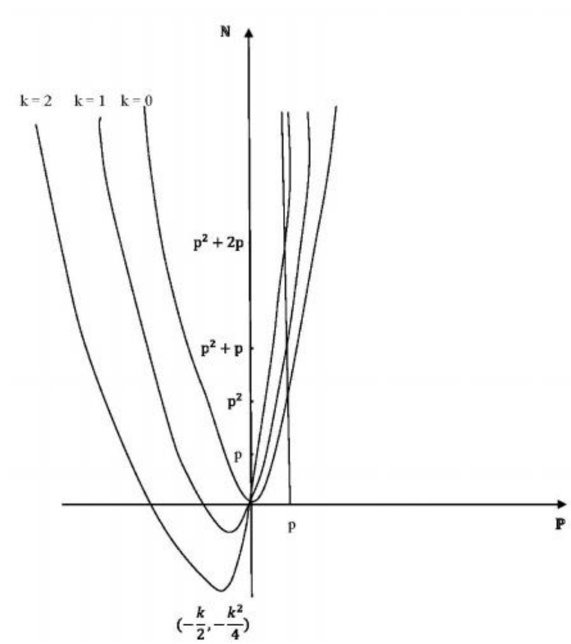
iv) n$\in \mathbb{P}$ si y solo si $\nexists$ solución de

n = $p^2 + k$ en $\mathbb{P}x\mathbb{N} \cup \{0\}$

Ahora, consideramos la siguiente función.-

f : $\mathbb{P} \to \mathbb{N}$ donde f (p) = $p^2 + kp$

$$f(p) = (p + \frac{k}{2})^2 - \frac{k^2}{4}$$



Se tiene que n es compuesto si y solo si $\exists$ (p,k)$\in \mathbb{P}$x$(\mathbb{N} \cup \{0\})/n = p^2 + kp$.

Luego:

i) n $\in \mathbb{N}$ es primo si y solo si

$\frac{n - p^2}{p} \notin (\mathbb{N} \cup \{0\}) \;\; \forall p \in \mathbb{P}$

ii) n $\in \mathbb{N}$ es primo si y solo si

$\frac{n - p^2}{p} \notin \mathbb{N} \cup \{0\} \forall p \in \mathbb{P} / \leq \sqrt{n}$

iii) n $\in \mathbb{N}$ es primo si y solo si

$\frac{n - p^2}{p} \not\subset (\mathbb{N} \cup \{0\}) \forall p \subset \mathbb{P}$ divisor de n / p $\leq \sqrt{n}$

iv) Sean n $\in \mathbb{N}$, p$\in \mathbb{P}$. Luego, p es divisor de n si y solo si p es divisor de n - p^2

Esta condición necesaria y suficiente permite dar una contribución en el artículo sobre caracterización de números primos; pues, de no haber divisores se tiene que n es primo.

Ejemplo: Determinar que 17 es primo.

Solución.-

Usaremos la caracterización de números primos dado por iv).
Los primos p $\leq \sqrt{17}$ son 2 y 3, por la parte ii)
$\Longrightarrow$
17 - 2^2 = 13
17 - 3^2 = 8
$\Longrightarrow$
2 y 3 no son divisores de 8 y de 13
$\Longrightarrow$
17 es primo.

<u>Condición necesaria de primo</u>.- Si
$p \subset \mathbb{P}$entonces
$p = \dfrac{\sqrt{k^2+4n}-k}{2}$ donde $n \in \mathbb{N}\backslash\mathbb{P}$,
$k \in (\mathbb{N} \cup \{0\})$
Prueba:
Sea $p \in \mathbb{P}$
$\Longrightarrow$
n = $p^2 + kp, \ \ k \in (\mathbb{N} \cup \{0\})$
$\Longrightarrow$
$p^2 + kp - n = 0$
$\Longrightarrow$
$p = \dfrac{-k \pm \sqrt{k^2+4n}}{2}$
$\Longrightarrow$
$p = \dfrac{\sqrt{k^2+4n}-k}{2}$ donde
$n \in \mathbb{N}\backslash\mathbb{P}, k \in (\mathbb{N} \cup \{0\})$

<u>Condición necesaria de primo</u> .- Si
$p \in \mathbb{P}$entonces $p = \sqrt{\dfrac{n}{2}}$ donde
$n \in \mathbb{N}\backslash\mathbb{P}$
Es decir, los primos se dan en números pares que tiene raíz cuadrada.

<u>Prueba</u>.-
Sea $p \in \mathbb{P}$
$\Longrightarrow$
n = $p^2 + kp, \ \ k \in (\mathbb{N} \cup \{0\})$
Ahora, sea k = p
$\Longrightarrow$
$n = p^2 + p^2$
$= 2\,p^2$
$\Longrightarrow$
$p - \sqrt{\dfrac{n}{2}}$

Intersección de Dobles $(p_1 = 2)$ y Triples $(p_2 = 3)$:
$p_1^2 + mp_1 = p_2^2 + np_2$
$\Longrightarrow$
4 + 2 m = 9 + 3 n
$\Longrightarrow$
2 m – 3 n = 5
$\Longrightarrow$
(m, n): (4, 1), (7, 3), (10, 5), (13, 7), (16, 9), (19, 11), …
m = 3 k + 1, n, n = 2 k – 1; $k \in \mathbb{N}$

Intersección de Dobles $(p_1 = 2)$ y Quintuples $(p_3 = 5)$:
$p_1^2 + mp_1 = p_3^2 + np_3$
$\Longrightarrow$
4 + 2 m = 25 + 5 n
$\Longrightarrow$
2 m – 5 n = 21
$\Longrightarrow$
(m, n): (13, 1), (18, 3), (23, 5), (28, 7), (33, 9), (38, 11), …
m = 5 k + 8, n = 2 k - 1; $k \in \mathbb{N}$

Intersección de Triples $(p_2 = 3)$ y Quintuples $(p_3 = 5)$:
$p_2^2 + mp_2 = p_3^2 + np_3$
$\Longrightarrow$
9 + 3 m = 25 + 5 n
$\Longrightarrow$
3 m – 5 n = 16
$\Longrightarrow$
(m, n): (7, 1), (12, 4), (17, 7), (22, 10), (27, 13), (32, 16),
m = 5 k + 2, n = 3 k - 2; $k \in \mathbb{N}$

CONCLUSIÓN

La caracterización de números primos nos permite analizar los divisores de números menores, expresados por n - p^2, que el número n que deseamos averiguar si es primo. Haciendo notar que si uno de estos números menores no tiene divisores, entonces el número por averiguar es primo.
Se debe indicar que esta caracterización tiene relevancia cuando se desea averiguar si un número grande es primo.

REFERENCIAS

1. **Herstein, I. N., "**Topics in Algebra", pp. 18, Blaisdell Publishing Company, New York, 1964.
2. **Lang, S., "**Linear Algebra, pp. 210, Addison-Wesley Publishing Company, Inc., U.S.A., 1966.
3. **Olmsted John, M. H**., "Real Variables, pp. 11, Appleton-Century-Crofts, Inc., New.York, 1959.
4. **Potápov, M**., "Álgebra y análisis de funciones elementales", pp. 15, Editorial MIR, Moscú, 1986.
5. **Zaring, W. M.**, "An Introduction to Analysis", pp. 96, the Macmillan Company, New York, 1967.
6. http://www.mat.ucm.es/~dazagrar/docencia/tn6.pdf, p.1
7. http://www2.uca.es/matematicas/Docencia/ESI/1711003/Apuntes/Leccion11.pdf, 11
8. http://w3.math.uminho.pt/site/files/historicooutros/1596_Capitulo3(EulerWilson).pdf, p.9

Correspondencia: hguimaray@hotmail.com

Recepción de originales: febrero 2013
Aceptación de originales: abril 2013