La nueva criba de Eratóstenes

Efraín Soto Apolinar [1]
F.I.M.E. U.A.N.L. San Nicolás, N.L. México.
efrain@yalma.fime.uanl.mx

Resumen

Se dan algunas definiciones básicas relacionadas con la divisibilidad y las clases de congruencia en el conjunto de los números naturales. Se muestra una forma más eficiente de enlistar los números primos, lo que se denomina *la nueva criba de Eratóstenes*.

Palabras clave: *Congruencias – divisibilidad – módulos – números primos – primos gemelos – teoría de números.*

1. DEFINICIONES

Definición. 1.1. Cerradura *Sea $\mathbb{A}$ un conjunto no vacío, y sea $\circ$ una operación binaria definida para cualesquiera dos elementos $a, b \in \mathbb{A}$. Si $a \circ b \in \mathbb{A}$ para cualesquiera $a, b \in \mathbb{A}$, entonces, decimos que el conjunto $\mathbb{A}$ es cerrado bajo la operación $\circ$.*

Definición. 1.2. Número primo. *Un número natural es primo si tiene exactamente dos divisores (naturales).*

Definición. 1.3. Número compuesto. *Un número natural es compuesto si tiene 3 o más divisores.*

Definición. 1.4. Números primos gemelos. *Dos números primos son primos gemelos si la diferencia entre ellos es 2.*

Definición. 1.5. Divisibilidad. *Sean a, b, m números naturales. Decimos que el número b divide al número a, o de forma equivalente, que el número a es divisible por el número b, si existe un número natural m tal que $a = b \cdot m$, y se denota por $b|a$.*

Teorema 1.1 *Sean a, b, c, m, n números naturales. La divisibilidad tiene las siguientes propiedades:*

I. *Si $b|a$, entonces $b|(a \cdot c)$.*
II. *Si $b|a$, y $a|c$, entonces $b|c$.*
III. *Si $b|a$, y $b|c$, entonces $b|(a + c)$.*
IV. *Si $b|a$, y $b|c$, entonces $b|(a - c)$.*
V. *Si $b|a$, y $b|c$, entonces $b|(a \cdot m + c \cdot n)$.*
VI. *Si $b|a$ entonces $b \leq a$.*
VII. *Si $a \neq 0$, entonces $a|a$.*
VIII. *Si $a|b$, y $b|a$, entonces $a = b$.*
IX. $1|a$.

[1] Estudiante del programa de posgrado en Ingeniería de Sistemas de la Facultad de Ingeniería Mecánica – Eléctrica de la U.A.N.L.

La siguiente definición es una notación inventanda por Carl F. Gauss que nos ayudará a simplificar cálculos y nos facilitará la construcción de la nueva criba de Eratóstenes.

Definición. 1.6. **Congruencias.** *Si $a = b \cdot m + r$, se entiende que $b|(a - r)$, y escribimos: $a \equiv r$* mód *b para indicarlo y se lee "a es congruente con r módulo b".*

Teorema 1.2 *Sean a, b, c, r, s números naturales. Las congruencias tienen las siguientes propiedades:*

I. *Si $a \equiv r$ mód b, y $0 \leq r \leq b$, entonces r es el residuo de dividir a entre b*

II. $a \equiv r \mod b \quad \Leftrightarrow \quad b|(a - r) \quad \Leftrightarrow \quad a = b \cdot m + r$

III. $a \equiv a \mod b$

IV. *Si* $a \equiv r \mod b$, *entonces* $r \equiv a \mod b$

V. *Si* $a \equiv r \mod b$, *y* $r \equiv s \mod b$, *entonces* $a \equiv s \mod b$

VI. *Si* $a \equiv r \mod b$, *y* $c \equiv s \mod b$, *entonces* $a + c \equiv (r + s) \mod b$

VII. *Si* $a \equiv r \mod b$, *y* $c \equiv s \mod b$, *entonces* $a - c \equiv (r - s) \mod b$

VIII. *Si* $a \equiv r \mod b$, *y* $c \equiv s \mod b$, *entonces* $a \cdot c \equiv (r \cdot s) \mod b$

IX. *Si* $a \equiv r \mod b$, *entonces* $a^s \equiv r^s \mod b$

Teorema 1.3 *Sea $p \geq 5$ un número primo. Entonces, bien* $p \equiv 1 \mod 6$, *bien* $p \equiv 5 \mod 6$.

Demostración.
Un número natural a cualquiera puede estar en alguna de las siguientes clases de congruencia:

- $a \equiv 0 \mod 6$, con lo que sería divisible por 6.
- $a \equiv 1 \mod 6$, con lo que podría ser primo.
- $a \equiv 2 \mod 6$, con lo que resultaría ser divisible por 2.
- $a \equiv 3 \mod 6$, con lo que resultaría ser divisible por 3.
- $a \equiv 4 \mod 6$, con lo que resultaría ser divisible por 2.
- $a \equiv 5 \mod 6$, con lo que podría ser primo.

□

NOTA: *No todos los números naturales p que cumplen con* $p \equiv 1 \mod 6$, *o bien,* $p \equiv 5 \mod 6$ *son primos, pero todos los primos mayores o iguales a 5, tienen esa forma.* ✓

Teorema 1.4 *Sea $\mathbb{P}$ el conjunto de todos los números naturales $p \geq 5$ (no necesariamente primos) de la forma:* $p \equiv 1 \mod 6$, *ó* $p \equiv 5 \mod 6$; *o bien* $\mathbb{P} = \{p \mid p \equiv 1 \mod 6, \text{ ó } p \equiv 5 \mod 6; p \in \mathbb{N}, p \geq 5\}$. *Entonces, el conjunto $\mathbb{P}$ es cerrado bajo la multiplicación.*

Demostración.
Sea $a \equiv 1 \mod 6$, y $b \equiv 5 \mod 6$. Por definición, $a, b \in \mathbb{P}$. Por las propiedades I, IV y VIII de las congruencias de módulos tenemos:

- $a \cdot a \equiv 1 \mod 6$
- $a \cdot b \equiv 5 \mod 6$
- $b \cdot b \equiv 25 \mod 6 \equiv 1 \mod 6$

con lo que queda establecido el teorema. □

2. NUEVA CRIBA DE ERATÓSTENES

En los estudios de nivel elemental a medio superior se enseña la criba de Eratóstenes como un método para encontrar todos los números primos hasta un número natural finito. Con los teoremas enlistados tenemos una segunda forma (más eficiente) de encontrar la lista de los números primos.

Para este fin empezamos enlistando a los únicos dos números primos que no pertenecen al conjunto $\mathbb{P} = \{p \mid p \equiv 1 \mod 6, \text{ ó } p \equiv 5 \mod 6; p \in \mathbb{N}, p \geq 5\}$; esos dos números primos son 2 y 3.

Inmediatamente después podemos hacer una tabla donde enlistemos los números en columnas, de acuerdo a la clase de congruencia a la que pertenezcan:

$5 \mod 6$	$0 \mod 6$	$1 \mod 6$
5	6	7
11	12	13
17	18	19
23	24	25
29	30	31
35	36	37
41	42	43
47	48	49
53	54	55
59	60	61
⋮	⋮	⋮

Cuadro 1: Clases 5, 0 y 1 de módulo 6.

En la tabla 1 tenemos 3 columnas. La columna del centro contiene números que son divisibles por 6, solamente para que nos sirva de guía para encontrar las otras dos columnas. Las columnas de la izquierda y de la derecha son las que tienen a los elementos del conjunto $\mathbb{P}$.

En la lista podemos ver algunos números que no son primos, e.g., 25. El teorema 1.4 explica por qué tenemos números compuestos en $\mathbb{P}$.

La siguiente cuestión consiste en eliminar los números que son compuestos. Para lograr esta meta haremos uso del teorema 1.4 y de la definición de número compuesto.

Es obvio que todo número natural n (a excepción del número 1) tiene al menos dos divisores: el número 1 y el número n (i.e., él mismo). Entonces, si aparece un divisor más, se entiende que ya es compuesto.

Por el teorema 1.4 sabemos que algunos de los elementos de $\mathbb{P}$ tienen más de dos divisores, por lo que no son números primos, sino compuestos.

3. CONSTRUYENDO LA NUEVA CRIBA

La tarea ahora parece muy sencilla: tomamos el menor de todos los elementos del conjunto $\mathbb{P}$ (esto es posible gracias al principio del buen ordenamiento, que dice que un conjunto no vacío de números naturales tiene un elemento que es menor o igual a cualquier otro elemento del conjunto considerado) y lo multiplicamos por todos los elementos del conjunto $\mathbb{P}$. Así encontraremos los números $p \in \mathbb{P}$ que no son primos.

Después de haber multiplicado el primer número primo $5 \in \mathbb{P}$ por todos los elementos del conjunto $\mathbb{P}$ (incluido el 5 mismo), debemos continuar con el siguiente primo, en este caso el número 7. Ahora debemos multiplicar a este número primo por todos los demás elementos del conjunto $\mathbb{P}$ que todavía no han sido eliminados (en caso de no ser primos).

Es claro que no se requiere multiplicar 7×5, dado que esta multiplicación se realizó cuando empezamos multiplicando el número 5 por todos los elementos del conjunto $\mathbb{P}$. Entonces, debemos empezar desde 7×7.

Y así sucesivamente, hasta que hayamos terminado con la lista que deseamos obtener.

Enseguida se muestra el proceso elaborado hasta el número primo 61.

$5 \mod 6$	$1 \mod 6$
5	7
11	13
17	19
23	~~25~~
29	31
~~35~~	37
41	43
47	~~49~~
53	~~55~~
59	61
⋮	⋮

Cuadro 2: Nueva criba de Eratóstenes.

5×5 eliminó al número 25, 5×7 eliminó al número 35, 5×11 eliminó al número 55, etc., 7×7 eliminó al número 49, 7×11 elimina al número 77, etc., 11×11 elimina al número 121, etc., y así sucesivamente.

4. CONCLUSIONES

Este mismo procedimiento puede usarse para generar un algoritmo muy eficiente para verificar si un número natural dado n es o no un número primo. En este caso se debe iniciar comparando el número dado n con los dos únicos números primos que no están en $\mathbb{P}$. En caso de que no sea así, se debe encontrar el residuo de dividir el número n entre 6. Si este residuo es distinto a 1 ó 5, entonces, con certeza sabemos que el número es compuesto. Por otra parte, si el residuo de dividir n entre 6 es, bien 1, bien 5, entonces debemos verificar si se divide por alguno de los números $p \in \mathbb{P}$. No requerimos checar todos los números $p \in \mathbb{P}$ hasta uno antes de n, como es bien sabido, basta verificar hasta el número natural mayor o igual a $\sqrt{n}$.

El algoritmo creado con la criba de Eratóstenes verifica si el número n es divisible por los números impares. Es claro que hay 3 números impares de cada 6 números naturales. El algoritmo de la nueva criba de Eratóstenes solamente verifica 2 de cada seis números naturales: los que pertenecen al conjunto $\mathbb{P} = \{p \mid p \equiv 1 \mod 6, \text{ ó } p \equiv 5 \mod 6; p \in \mathbb{N}, p \geq 5\}$.

Más aún, algunos de los elementos del conjunto $\mathbb{P}$ son compuestos y es muy obvio verificarlo: cuando en la cifra de las unidades tiene un 5, por ejemplo: 25 (5×5), 55 (5×11), 125 (5×25), etc.

Se debe recordar que esta nueva criba no considera a los primeros dos números naturales primos: el 2 y el 3. Por tanto, cuando se haga la lista de los números primos utilizando la nueva criba de Eratóstenes deben incluirse estos dos números primos.

Durante mucho tiempo ha existido la pregunta (sin responder hasta el día de hoy) si existe un número infinito de parejas de números primos gemelos. El teorema 1.3 muestra por qué aparecen los números primos gemelos.

En el primer intento por demostrar esta conjetura[2] (la infinitud de los números primos gemelos) se encontraron los resultados que aquí se muestran. El reto que queda por resolver es la cuestión de si hay un número infinito de números primos gemelos, para lo cual habrá que estudiar la distribución de los productos de los elementos de $\mathbb{P}$.

[2]En este artículo se incluyen ideas compartidas por el físico Abel Chávez Morales.