## ¿Sabías que...

por Leandro Cagliero y Ricardo Podestá

*se pueden cribar los números primos con una parábola?*

Todos sabemos desde chicos que los números primos, es decir, aquellos que sólo son divisibles por 1 y por sí mismos, son infinitos. En efecto, ya lo sabían los antiguos griegos, pues en los *Elementos* de Euclides ya aparece una demostración de este hecho. Pero también sabemos que no hay una fórmula para hallar el $n$-ésimo número primo. De esta manera, se vuelve un problema básico dado un entero positivo $N$ saber cuántos primos menores a $N$ hay y cuáles son.

Para resolver ambos problemas tenemos el método de la criba (cribar quiere decir zarandear). La primer criba conocida es la del polímata griego Eratóstenes (276 a.C.–194 a.C.) quien fue matemático, astrónomo y geógrafo. De hecho, le debemos a Eratóstenes la ¡primer medición del radio de la tierra!

Seguramente casi todos conocen la mencionada criba de la escuela primaria o secundaria. Funciona así: se elije un número natural $N$, digamos el 100 y se hace una lista de todos los números del 1 al $N$. El 1 no es primo (podemos tacharlo) y el primer número primo es el 2. Marcamos el 2 con un círculo y tachamos todos los números pares mayores que 2 (múltiplos de 2), ya que no serán primos. Luego miramos el primer número no tachado, que es el 3. Como 3 es primo, lo circulamos y tachamos todos los múltiplos de 3, ya que no serán primos. Por una cuestión de eficiencia, si queremos no volvemos a tachar un número ya tachado (por ejemplo el 6 o cualquier múltiplo de 6 se tacha por ser par y por ser múltiplo de 3). Siguiendo este procedimiento, los números menores que 100 que no se encuentren tachados serán primos, como puede verse en la siguiente figura:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2 | 3 | ~~4~~ | 5 | ~~6~~ | 7 | ~~8~~ | ~~9~~ | ~~10~~ |
| 11 | ~~12~~ | 13 | ~~14~~ | ~~15~~ | ~~16~~ | 17 | ~~18~~ | 19 | ~~20~~ |
| ~~21~~ | ~~22~~ | 23 | ~~24~~ | ~~25~~ | ~~26~~ | ~~27~~ | ~~28~~ | 29 | ~~30~~ |
| 31 | ~~32~~ | ~~33~~ | ~~34~~ | ~~35~~ | ~~36~~ | 37 | ~~38~~ | ~~39~~ | ~~40~~ |
| 41 | ~~42~~ | 43 | ~~44~~ | ~~45~~ | ~~46~~ | 47 | ~~48~~ | ~~49~~ | ~~50~~ |
| ~~51~~ | ~~52~~ | 53 | ~~54~~ | ~~55~~ | ~~56~~ | ~~57~~ | ~~58~~ | 59 | ~~60~~ |
| 61 | ~~62~~ | ~~63~~ | ~~64~~ | ~~65~~ | ~~66~~ | 67 | ~~68~~ | ~~69~~ | ~~60~~ |
| 71 | ~~72~~ | 73 | ~~74~~ | ~~75~~ | ~~76~~ | ~~77~~ | ~~78~~ | 79 | ~~80~~ |
| ~~81~~ | ~~82~~ | 83 | ~~84~~ | ~~85~~ | ~~86~~ | ~~87~~ | ~~88~~ | 89 | ~~90~~ |
| ~~91~~ | ~~92~~ | ~~93~~ | ~~94~~ | ~~95~~ | ~~96~~ | 97 | ~~98~~ | ~~99~~ | ~~100~~ |

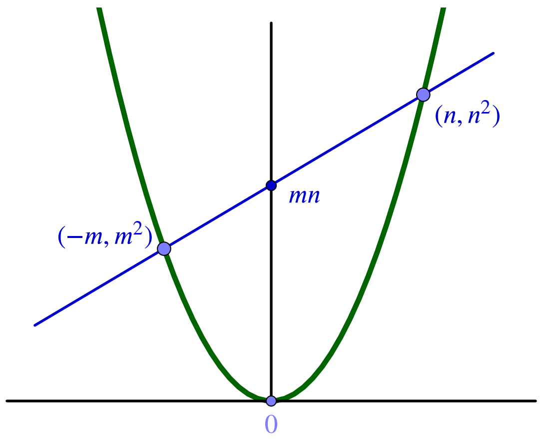
Por supuesto, existen otras cribas más modernas (de las cuales quizás nos ocupemos en otra ocasión), como la de Sundoran (1934), la de Atkin (2003) y las llamadas cribas de rueda. Sin embargo, hay una de ellas que lleva adelante la

Criba de Eratóstenes de una manera geométrica. Se trata de la criba parabólica que explicamos a continuación.

Consideremos la parábola de la forma

$$y = x^2.$$

Ya August Möbius observó en 1841 (*Geometrische Eigenschaften einer Factorentafel*, Journal für die reine und angewandte Mathematik, Vol. 22, pp. 276–284) que la recta que une dos puntos cualquiera de la parábola, uno en cada rama de ella, digamos $P = (-m, m^2)$ y $Q = (n, n^2)$, corta al eje $y$ en el punto $R = (0, mn)$.




En efecto, la recta

$$y = (n - m)x + mn.$$

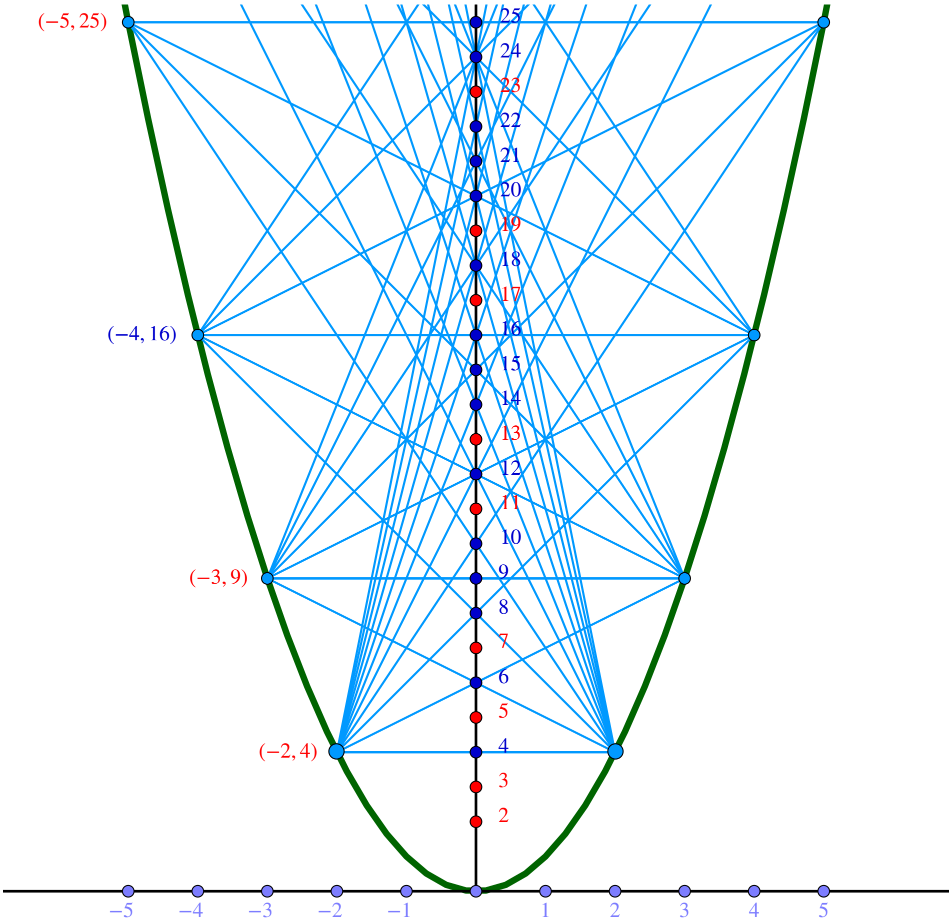
pasa por los puntos $P = (-m, m^2)$ y $Q = (n, n^2)$ y tiene ordenada al origen $mn$.

En 1999, los matemáticos rusos Yuri Matiyasévich y Boris Stechkin publicaron en la página personal de Yuri la mencionada criba parabólica (ver la página logic.pdmi.ras.ru/ yumat/personaljournal/sieve/sieve.html), que te contamos a continuación. Utilizando la observación de Möbius hecha más arriba (aunque no sabemos si Yuri la conocía o no), consideramos todos los puntos enteros de la parábola $y = x^2$, es decir todos los puntos de la forma

$$P = (-m, m^2) \qquad \text{y} \qquad Q = (n, n^2)$$

con $m, n \in \mathbb{N}$. Si unimos todos los puntos enteros $P$ de una rama con todos los puntos enteros $Q$ de la otra rama con rectas (digamos que para $n, m < N$), encontramos que cortan al eje $y$ en los puntos de la forma $nm$ con $n, m \in \mathbb{N}$. Esto quiere decir que estas rectas cruzan al eje $y$ exactamente en los números compuestos $nm$ y no corta a los números primos. Es decir, ¡estamos cribando a los números primos en un eje usando una parábola!

A continuación graficamos la parábola con las primeras rectas y los primeros primos, pues ya se sabe que una imagen vale más que mil palabras.




O sea, los puntos $(\pm 2, 4)$ tachan los múltiplos de 2 mayores que 2, los puntos $(\pm 3, 9)$ tachan todos los múltiplos de 3 mayores que 3, los puntos $(\pm 5, 25)$ tachan los múltiplos de 5 mayores que 5, etc.

Finalmente notamos que, tal como hacemos en la Criba de Eratóstenes, buscando evitar algunas "tachaduras" repetidas, basta trazar los segmentos que unen $(-p, p^2)$ –en rojo en la figura– y $(n, n^2)$ con $p$ recorriendo los primos que nos van apareciendo y $n \geq p$.

**August Ferdinand Möbius** (Schulpforta, 17/11/1790 – Leipzig, 26/9/1868) fue un matemático y astrónomo alemán. Es mas que nada conocido por su descubrimiento en 1858 de la superficie que hoy lleva su nombre, la cinta de Möbius. Además, fue el primero en introducir las coordenadas homogéneas en geometría proyectiva. Se interesó también por la teoría de números donde la función aritmética de Möbius $\mu(n)$ y la fórmula de inversión de Möbius se nombran así por él.

**Yuri Vladímirovich Matiyasévich** (Leningrado, 2/3/1947) es un matemático ruso. En 1964 obtuvo el primer premio de la 6º Olimpiada Internacional de Matemática que tuvo lugar en Moscú. Matiyasévich se graduó en el Departamento de Matemáticas y Mecánica de la Universidad Estatal de Leningrado en 1969. Es muy conocido por su solución negativa al décimo problema de Hilbert sobre soluciones a ecuaciones Diofánticas, presentada en su tesis doctoral en 1972 con 25 años, en el Departamento de Leningrado del Instituto de Matemáticas Steklov.