# APROXIMACIÓN A LOS NÚMEROS PRIMOS

*Pregunta de examen: El producto de dos números primos, ¿es primo?*

*Respuesta (un tanto airada) de un alumno: Pero, ¿primos de quién?*

**Francisco Bellot Rosado**

La lectura del primer capítulo de un libro realmente excelente, ***Le lezioni del supplente (Un tentativo di insegnare la matematica che non si insegna),*** del recientemente desaparecido **Italo D'Ignazio,** me da pie a tratar de escribir una primera aproximación a los números primos, para los alumnos de Olimpiadas y Seminarios de ampliación. La foto del Prof. D'Ignazio ha sido gentilmente cedida por el Prof. Ercole Suppa, de Teramo (Italia).

Para este artículo me he servido no solamente del libro mencionado, sino también de los que cito igualmente en la Bibliografía, y que, a mi entender, no deberían faltar en ninguna Biblioteca del Departamento de Matemáticas de los centros escolares de cualquier nivel educativo.

Se suponen conocidos los conceptos de divisibilidad, máximo común divisor, mínimo común múltiplo y de números primos entre si (cuando su máximo común divisor es 1).

**Paulo Ribenboim,** en el prólogo de su obra ***Nombres premiers: mystères et records,*** enumera las preguntas que de una manera natural, surgen en relación con los números primos:

a) ¿Cuántos números primos hay?

b) ¿Cómo reconocer si un número natural dado es primo?

c) ¿Hay fórmulas o algoritmos para generar los números primos?

d) ¿Cómo se distribuyen los números primos entre los naturales?

## 1. Números primos y compuestos

Algunos números naturales se pueden descomponer en producto de dos o más factores más pequeños; otros, como 7, 13, 17, no. Diremos que si el número natural c = a x b, siendo a y b números naturales, éstos se dicen factores o divisores de c. Todo número admite la *factorización trivial*

$$c = 1xc = cx1;$$

y en correspondencia con esto diremos que 1 y c son los *divisores triviales* de c. Cualquier número natural c > 1 que tiene alguna factorización no trivial, se llamará *compuesto.* Los que solamente admiten la factorización trivial se llaman *números primos.*

Entre los 100 primeros números naturales, los 25 de la tabla siguiente son primos:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,

43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

El número 1 no es ni primo, ni compuesto.

El primer resultado que probaremos es sencillo, pero importante:

***Todo entero c>1, o es primo, o admite un divisor primo.***

Si c no es primo, sea *p* el menor divisor no trivial de *c*. Entonces, *p* tiene que ser primo, porque si fuera compuesto, *c* tendría un divisor menor que *p.*■

La siguiente observación, igualmente sencilla e importante, es que no necesitamos dividir *c* por todos los números menores que *c* para saber si es primo o compuesto. Si *c = a x b,* los dos divisores *a* y *b* no pueden ser mayores que √c, porque si ese fuera el caso, se tendría

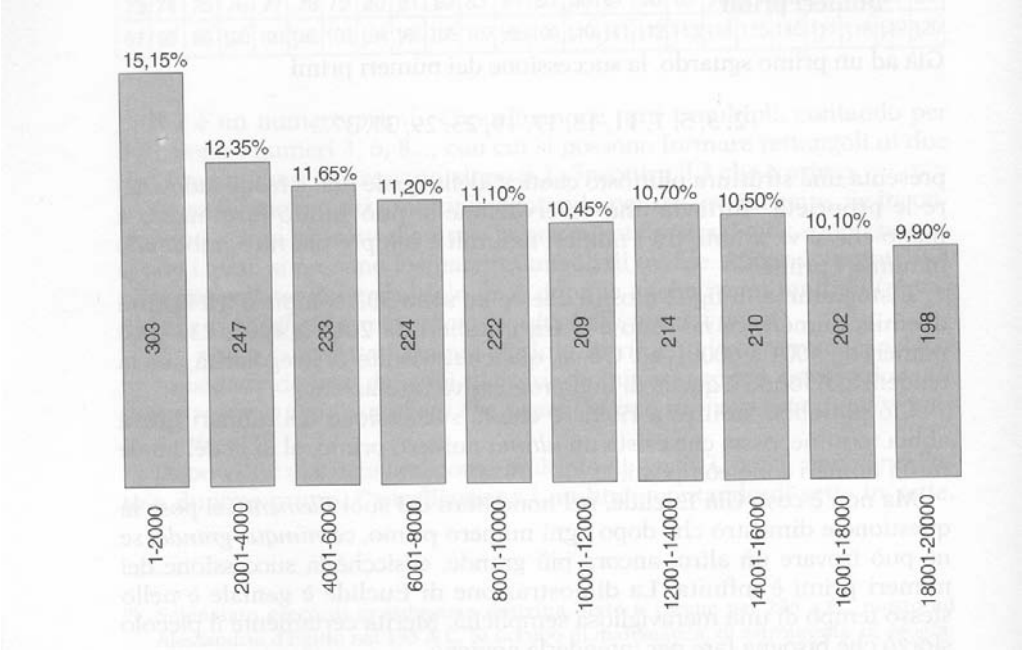
$$axb > \sqrt{c} \; x \; \sqrt{c} = c,$$

lo cual es imposible. Por lo tanto, es suficiente probar los números primos que son menores o iguales que √c.

Desde la escuela se conoce el procedimiento llamado *criba de Eratóstenes* para encontrar los números primos menores que un número natural dado: a partir del 2, se suprimen todos los múltiplos de 2; a continuación, dejando el 3, se suprimen todos los múltiplos de 3 que no hayan sido previamente borrados; se repite el proceso con el 5, etc.

## 2. El conjunto de los números primos es infinito

En el libro de D'Ignazio se muestra el siguiente histograma para ilustrar lo que llama *rarefacción de los números primos:*




El significado de las barras es claro: hay 303 primos entre los números 1 y 2000, etc.

Podría pensarse que, a la vista de esto, hay un número primo mayor que todos los demás. Pero ya Euclides demostró (en los *Elementos*) que no es así.

Observemos la tabla siguiente:

$$2 \times 3 + 1 = 7$$

$$2 \times 3 \times 5 + 1 = 31$$

$$2 \times 3 \times 5 \times 7 + 1 = 211$$

$$2 \times 3 \times 5 \times 7 \times 11 + 1 = 2311$$

$$2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031$$

Los números que aparecen en los segundos miembros no son divisibles (obviamente) por los números primos que se multiplican en los primeros miembros. Los cuatro primeros (7, 31, 211 y 2311) son primos, mayores que los que se van multiplicando. En cuanto al quinto, se tiene

$$30031 = 59 \times 509,$$

y estos dos primos son mayores que 13.

La generalización de estas observaciones constituye la famosa **demostración de Euclides de que la sucesión de números primos es infinita:**

Supongamos que la lista de números primos $p_1=2$, $p_2=3,\ldots p_r$ *sea finita.* Entonces formamos el número

$$P = p_1p_2p_3\ldots.p_r + 1.$$

Si P es primo, no hay nada que demostrar. En caso de no ser primo, sea *p* un número primo que divide a *P*. Este número *p* no puede ser ninguno de los primos $p_1,p_2,\ldots,p_r$, ya que en tal caso *p* dividiría a la diferencia $P - (p_1p_2p_3\ldots.p_r) = 1$, *lo que es absurdo.* Por lo tanto, *p* es un número primo mayor que $p_r$, y por lo tanto la lista de números primos no puede ser finita.■

La demostración de Euclides es simple, pero al mismo tiempo es brillante. Es uno de los primeros ejemplos de demostración por reducción al absurdo, que es algo que nuestros alumnos no dominan bien, sobre todo al principio.

**Ribenboim** en su libro incluye 9 demostraciones de este resultado.

La criba de Eratóstenes permite obtener otra demostración de este teorema

Supongamos que sólo hubiera k primos,

$$2,3,5,7,\ldots,p_k.$$

Entonces, en la criba no podrían quedar números después de $p_k$, puesto que vamos suprimiendo los múltiplos de los diferentes primos. Pero esto es imposible, porque si consideramos el número

$$P = 2x3x5x\ldots xp_k$$

éste habría sido suprimido k veces, una vez por cada uno de los primos, y el número P + 1 no habría sido suprimido por ninguno de ellos.■

Esta demostración aparece en el libro de **Oystein Ore** ***Invitation to Number Theory.***

### 3. El Teorema fundamental de la aritmética

***Todo entero positivo se puede descomponer en producto de números primos de manera única, salvo el orden de los factores.***

Este resultado es conocido desde la escuela primaria; sin embargo, podemos demostrarlo (una actividad común entre los matemáticos, que queremos demostrarlo casi todo; sorprendentemente en los primeros años de la enseñanza secundaria no se demuestra casi nada ( clases de Matemáticas incluidas!). Vamos a seguir la demostración de **D'Ignazio,** un prodigio de claridad y sencillez.

Sea N un número compuesto; si $p_1$ es el menor de sus divisores (distinto de 1), tiene que ser necesariamente primo (esto lo habíamos visto en el párrafo 1). Hagamos la división N:$p_1$ *y sea* $N_1$ *el cociente:*

$$N = p_1N_1 \qquad (1)$$

Si $N_1$ es primo, la (1) da ya la descomposición de N en producto de primos; en caso contrario repetimos el proceso con $N_1$*:* sea $p_2$ el menor divisor de $N_1$ que ha de ser necesariamente primo y mayor o igual que $p_1$; hacemos la división y obtenemos $N_1 = p_2N_2$ con lo cual

$$N = p_1p_2N_2;$$

Reiterando el procedimiento obtenemos $N > N_1 > N_2 >$ …y al cabo de un cierto número de operaciones llegaremos a un cociente $N_k$ primo. Entonces la (1) se convierte en

$$N = p_1p_2...p_k \quad (2)$$

donde hemos puesto, para unificar la notación, $N_k = p_k$. Hay que observar que algunos de los factores primos $p_i$ pueden ser iguales, y se podrán asociar en forma de potencias.

Vamos a demostrar que la factorización obtenida para el número N es única.

Supongamos que existiera otra:

$$N = q_1q_2...q_h$$

Entonces se tendrá

$$p_1p_2...p_k = q_1q_2...q_h \qquad (3)$$

Sin pérdida de la generalidad se puede suponer que los factores “p” y los factores “q” están en orden creciente:

$$p_1 \leq p_2 \leq ... \leq p_k \qquad \text{y} \qquad q_1 \leq q_2 \leq ... \leq q_h$$

Ahora bien, $p_1$ es el menor divisor primo de N; como $q_1$ también lo es, tiene que ser $p_1 = q_1$.

Dividiendo los dos miembros de (3) por $p_1 = q_1$ se obtiene

$$p_2p_3...p_k = q_2q_3...q_h$$

y la situación se repite, con lo cual resulta que todos los factores de la primera factorización son iguales a todos los de la segunda, y esa es única.■

Otras demostraciones de este resultado utilizan el método de reducción al absurdo (v. **Puig Adam, *Matemáticas Preuniversitario,*** Madrid 1967).

En el libro del gran matemático polaco **Waclaw Sierpinski**, ***Elementary theory of numbers*** se llama teorema fundamental de la aritmética al siguiente, también conocido en otras fuentes como *primer teorema de Euclides:*

***Si un número divide a un producto de dos factores y es primo con uno de ellos, entonces divide al otro.***

Veamos la demostración de **Sierpinski**:

Sean *a* y *b* dos números primos entre sí y *c* un número natural, tales que *b* divide al producto *ac.* El número *ac* es divisible tanto por *a* como por *b*, y por lo tanto, por su mínimo común múltiplo, que es *ab.* Entonces

$$ac = tab,$$

con *t* entero, luego $c=tb$ y por lo tanto *b* divide a *c.*■

A la pregunta b) de **Ribenboim** es fácil contestar cuando el número dado no es muy grande, pero si no, se convierte en un problema con aplicaciones prácticas inesperadas, como la criptografía. No entraremos aquí a tratar de los *tests de primalidad* y sus problemas asociados de velocidad en los cálculos hechos con los ordenadores más potentes.

### 4. Números primos de Fermat

**Fermat** (1601 – 1665) conjeturó que los números que son de la forma

$$F_n = 2^{2^n} + 1$$

eran todos primos. La notación utilizada para la potencia cuyo exponente es otra potencia significa que 2 lo elevamos a $2^n$, y no que $2^2$ lo elevamos al exponente n, ya que en ese caso hubiéramos escrito simplemente $4^n$.

Con las posibilidades de cálculo de la época, era una conjetura razonable, porque

$$F_0 = 2^{2^0} + 1 = 3,\ F_1 = 2^{2^1} + 1 = 5,\ F_2 = 2^{2^2} + 1 = 17,$$
$$F_3 = 2^{2^3} + 1 = 257, F_4 = 2^{2^4} + 1 = 65537$$

son primos.

Sin embargo, el matemático suizo **Leonhard Euler** demostró en 1732 que el siguiente número de Fermat,

$$F_5 = 2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417$$

no es primo. En 1958 se demostró que $F_{1945}$ era divisible por $5x2^{1947} + 1$.

Tal vez la historia de los números de Fermat hubiera terminado aquí, pero por una de esas *vueltas de tuerca* que da la historia en general y la de las matemáticas en particular, en 1801 el genial matemático alemán **C.F.Gauss** (1777-1855) demostró en sus *Disquisitiones Arithmeticae* que los polígonos regulares con un número n primo impar de lados son construibles con regla y compás si y solamente si $n = F_m$. En particular, el polígono de 17 lados es construible, y la lápida de la tumba de Gauss en Braunschweig representa este polígono regular, en su honor. Gauss descubrió este último resultado cuando tenía 19 años, si bien la publicación se produjo más tarde.

## 5. Los números de Mersenne

El monje francés **Marin Mersenne** (1588 – 1648) estudió los números de la forma siguiente:

$$M_p = 2^p - 1, \quad p \text{ primo.}$$

Los cuatro primeros números de **Mersenne**

$$M_2 = 2^2 - 1 = 3;\ M_3 = 2^3 - 1 = 7;\ M_5 = 2^5 - 1 = 31;\ M_7 = 2^7 - 1 = 127$$

son primos, pero $M_{11} = 2^{11} - 1 = 2047 = 23x89$. Sin embargo, hay otros primos de **Mersenne**: **Euler** probó en 1750 que $M_{31}$ es primo, y en 1876 el francés **Lucas** estableció que $M_{127}$ , un número de 39 cifras, es primo.

En el momento de redactar esta nota, el mayor número primo conocido, descubierto en agosto de 2008, es el número de Mersenne $M_{43112609}$ y tiene más de doce millones de cifras; para ser exactos, 12 978 189.

## 6. La búsqueda de fórmulas o algoritmos para generar números primos

Hay varios ejemplos de polinomios en *n* que dan valores primos hasta un cierto valor, a partir del cual pueden dar valores primos o compuestos. **Ribenboim** señala que una tal función *f(n)* debería cumplir al menos una de las condiciones siguientes:

a) $f(n) = p_n$ (el n-ésimo primo)

b) *f(n) siempre es primo, y si n es distinto de m, f(n) no es igual a f(m)*

c) *El conjunto de los números primos* es *igual al conjunto de valores de la función f.*

Es claro que a) es más restrictiva que b) ó c).

La mayor parte de las funciones f buscadas tienen expresiones muy complicadas. ¿Por qué no probar con los polinomios? Al fin y al cabo, Euler observó que $n^2 + n + 41$ toma valores primos desde n = 0 hasta 39. Para n = 40 el valor es 1681 = $41^2$. Con $n^2 - 79n + 1601$ se avanza algo más; da valores primos desde n = 0 hasta 79, pero para n = 80 obtenemos otra vez $41^2$ . La razón para no seguir esta vía la da el teorema negativo siguiente:

***Si f es un polinomio en n con coeficientes enteros, no constante, existen infinitos enteros n tales que el valor absoluto de f(n) no es un número primo.***

**Demostración** (**Ribenboim,** pg.129)

Como el polinomio no es constante, sería trivial si tomase todos sus valores compuestos. Por lo tanto, se puede suponer que existe un entero $n_0 \geq 0$ tal que $|f(n_0)| = p$ sea primo. Igualmente porque el polinomio no es constante, se tiene $\lim_{x\to\infty} f(x) = \infty$, luego existe $n_1 > n_0$ tal que si $n \geq n_1$, entonces $|f(n)| > p$ . Para todo entero *h* tal que $n_0 + ph \geq n_1$ se tiene

$$f(n_0 + ph) = f(n_0) + (\text{múltiplo de p}) = (\text{múltiplo de p}) .$$

Dado que $|f(n_0 + ph)| > p$ , $|f(n_0 + ph)|$ es compuesto.■

Siguiendo los pasos de **Euclides**, es posible construir un conjunto de números primos tan grande como se quiera. Empezando por 2 y 3, ponemos 2 x 3 + 1 =7 y ya tenemos el conjunto {2,3,7}. Poniendo 2x3x7+1 = 43, tenemos {2,3,7,43}. Ahora 2x3x7x43+1 = 1807 = 13x139 y eso conduce al conjunto {2,3,7,43,13,139}. Y así sucesivamente…

Pero, por otra parte, y eso ya está relacionado con la distribución de los números primos dentro de la serie natural, ***dado un número k arbitrario, se pueden encontrar k números consecutivos que no son primos.***

## 7. La distribución de los números primos dentro del conjunto de los números naturales

Vamos en primer lugar a justificar la afirmación que cierra el párrafo 6:

***Dado un número k arbitrario, se pueden encontrar k números consecutivos que no son primos.***

Consideramos los números

$$N_1 = (k+1)! + 2$$

$$N_2 = (k+1)! + 3$$

$$N_3 = (k+1)! + 4$$

……..

$$N_k = (k+1)! + k+1$$

Este conjunto de k números consecutivos responde a la cuestión; pues el primero es múltiplo de 2, el segundo de 3, etc. ■

Este apartado 7 de esta nota trata de la pregunta d) de las planteadas por **Ribenboim** en su obra. Necesitamos, entre otras cosas una notación para una de las funciones aritméticas importantes: la que cuenta los números primos *p* menores o iguales que un cierto número x>0, y que se representa por π(x). Lo formalizamos como

$$\pi(x) = \#\{p \in P \text{ tales que } p \le x\}$$

Un aspecto de la distribución de los números primos en el conjunto de los naturales lo dio la ***conjetura de Bertrand*** (1845), que afirma que **para todo** $n \ge 2$**, existe un número primo entre n y 2n .** Esta conjetura fue demostrada por **Chebyshev,** y desde entonces se conoce como teorema de **Bertrand-Chebyshev.**

**El teorema del número primo**

En 1792 **Gauss** conjeturó que $\pi(x) \sim \int_2^x \frac{dt}{\ln t}$ y dado que el logaritmo integral es asintóticamente equivalente a $\frac{x}{\ln x}$ (es decir que su cociente tiende a 1 cuando x tiende a infinito), el resultado

$$\pi(x) \sim \frac{x}{\ln x}$$

se conoce, desde su primera demostración en 1896 por **Hadamard** y **de la Vallée-Poussin** (independientemente uno del otro) como el **teorema del número primo.**

Esta incursión de las nociones de Análisis en la Teoría de números dio lugar a la **Teoría analítica de Números.** Se creía que solamente era posible este tipo de demostración para este teorema, pero en 1949, **Erdös** y **Selberg** dieron (por separado) demostraciones que utilizaban estimaciones elementales de ciertas funciones aritméticas (y que por eso se llaman *demostraciones elementales del teorema del número primo).*

## 8. La conjetura de Goldbach

Finalizaremos esta digresión sobre los números primos con uno de los problemas *abiertos* de la Teoría de Números. Es la conjetura de **Goldbach** quien en 1742 pidió a **Euler** que demostrase que ***todo número par,***

***mayor que 2, es suma de 2 números primos.*** La conjetura parece razonable, ya que, por ejemplo, 10 = 3 + 7 = 5 + 5; 24 = 11 + 13 = 7 + 17; 8 = 5 + 3; etc. Pero, hasta la fecha, no hay ninguna demostración general, si bien, como dice **D'Ignazio** en los últimos párrafos del capítulo sobre primos de su libro, el haberse probado que ***todo número natural, suficientemente grande, es suma de no más de cuatro números primos***, debería ser el preludio de una demostración de la conjetura.

### 9. Dos observaciones finales…pero no últimas

A punto de enviar al webmaster de la OEI el número 48 de la REOIM se han producido dos noticias que han revolucionado a los matemáticos.

Por una parte, el matemático peruano Harald Helfgott, investigador en el Centre Nationale de la Recherche Scientifique de París ha demostrado la llamada conjetura débil de Goldbach: ***Todo número impar mayor que 5 puede expresarse como suma de tres números primos.***

Casi simultáneamente, un investigador chino, Yitang Zhang, de la Universidad de New Hampshire, envió a la prestigiosa revista *Annals of Mathematics* un manuscrito (escrito con claridad cristalina y no dejando ni un detalle sin demostrar) en el que prueba un resultado clave en el estudio de la distribución de los números primos: ***Existe un número N menor que 70 millones tal que hay infinitos pares de primos que difieren en N.*** El 17 de mayo de 2013, mientras Zhang daba cuenta de su demostración en una conferencia en la Universidad de Harvard, "saltó" a las noticias el resultado de Helfgott.

## Algunos problemas para resolver

**i)** Demostrar que $n^4 + 4$ no es primo si $n > 1$ (Sophie Germain)

**ii)** Si a y n son enteros, $a \geq 0, n \geq 2$, demostrar que

$$N = \left(1 + a + a^2 + \cdots + a^n\right)^2 - a^n$$

es compuesto.

**iii)** Si a,b son números naturales mayores que 1 y primos entre sí, demostrar que $\log_a b$ es irracional.

**iv)** Un número $N = 2^x.3^y.5^z$ . Se suprimen 24 divisores al dividirlo por 2, 18 al hacerlo por 3 y 12 al hacerlo por 5. Calcular N.

**v)** ¿Es siempre posible convertir un número entero en primo, modificando una sola de sus cifras (Sierpinsky)

**vi)** Probar que n! es divisible por la suma 1 + 2+ 3+…+ n si y solamente si n+1 no es un primo impar (V. Thébault)

**vii)** Probar que no existen un primo p > 5 ni un natural m tales que (p – 1)! + 1 = $p^m$

**viii)** Si p es primo y $1 \leq k \leq p$, entonces $(k-1)!(p-k)!+(-1)^{k-1} \equiv 0(\mathrm{mod}\ p)$ y recíprocamente (H.Demir, Mathesis 1962)

**ix)** Demostrar que en cualquier progresión aritmética, cuyp primer término y la diferencia sean números naturales, se puede encontrar cualquier número prefijado de términos que no sean primos.

**x)** Se consideran los números primos 2, 3, 5, 7, …, p; demostrar que el número 2.3.5.7….p + 1 nunca es cuadrado perfecto (V. Thébault)

## 10. Bibliografía


**1) Cilleruelo, J. & Córdoba, A.** ***La teoría de los números.*** Mondadori, Madrid 1992.

**2) D'Ignazio, I.** ***Le lezioni del supplente.*** Interlinea Ed., Teramo, 1995.

**3) Ore, O.** ***Invitation to Number Theory.*** New Mathematical Library #20, M.A.A., 1967.

**4) Ribenboim, P.** ***Nombres premiers: mystères et records.*** P.U.F. Paris, 1994.

**5) Sautoy, M. de.** ***The music of the primes.*** Harper, New York 2004.

**6) Sierpinski, W.** ***Elementary Theory of Numbers.*** North-Holland & PWN, Amsterdam y Varsovia 1988.