La Columna de Matemática Computacional

Sección a cargo de

Tomás Recio

El objetivo de esta columna es presentar de manera sucinta, en cada uno de los números de La Gaceta*, alguna cuestión matemática en la que los cálculos, en un sentido muy amplio, tengan un papel destacado. Para cumplir este objetivo el editor de la columna (sin otros méritos que su interés y sin otros recursos que su mejor voluntad) quisiera contar con la colaboración de los lectores, a los que anima a remitirle (a la dirección que se indica al pie de página*[1]*) los trabajos y sugerencias que consideren oportunos.*

En este número ...

... presentamos la primera parte de un extenso artículo del profesor Gómez Pardo, de la Universidad de Santiago de Compostela. Si el prof. Tena Ayuso se centraba en esta misma columna, hace un año (La Gaceta 3.3) en los test de primalidad y en su importancia para los sistemas criptográficos, el prof. Gómez Pardo aborda ahora otra cuestión no menos interesante: ¿Cuántos primos hay? El texto de su artículo conjuga, de un modo extraordinariamente ameno y asequible, las reflexiones matemáticas, las anécdotas históricas, los cálculos y experimentos (al alcance, en muchos casos, de cualquier lector que se anime a desarrollarlos por sí mismo) con el programa *Mathematica* ...

Aspectos computacionales de los números primos (I)

por

José Luis Gómez Pardo

La importancia de los números primos es conocida desde la antigüedad y arranca del llamado 'Teorema fundamental de la aritmética', según el cual todo entero (positivo) es producto de números primos en forma única (salvo el orden). Por eso se ha dicho que los números primos son como los bloques a partir de los cuales se construyen todos los números enteros y, en cierto sentido,

[1]Tomás Recio. Departamento de Matemáticas. Facultad de Ciencias. Universidad de Cantabria. 39071 Santander. recio@matesco.unican.es

el estudio de estos últimos se reduce al de los primos. El teorema fundamental de la aritmética está ya contenido en los 'Elementos' de Euclides, publicados hacia el año 300 a.C. En los *Elementos* también aparece otro resultado que es aun más básico: existen infinitos números primos.

Estos dos resultados, aun siendo muy importantes, están lejos de despejar todas las incógnitas sobre los números primos y, como ocurre a menudo en matemáticas, dan lugar a muchos problemas, algunos de ellos muy difíciles y que permanecen sin resolver hasta la fecha. En estas notas pasaremos revista a algunos de esos problemas, poniendo énfasis en sus aspectos computacionales y utilizando *Mathematica* como lenguaje para programar algoritmos y realizar experimentos. La versión de *Mathematica* utilizada es la 4.0 y algunas de las funciones que se manejan no funcionan en versiones anteriores. No es necesario tener acceso a *Mathematica* para poder leer estas notas, pero un conocimiento básico de su lenguaje de programación se puede adquirir, por ejemplo, en [6], o bien consultando *The Mathematica Book* de S. Wolfram, que viene incluído en el propio paquete. También en [3] hay un apéndice que puede servir para adquirir estos conocimientos básicos.

El problema genérico que vamos a abordar aquí es el de tratar de dar respuesta a la pregunta: ¿Cuántos primos hay? El interés de la respuesta no es puramente académico, pues la cuestión planteada tiene, también, una considerable importancia práctica que se hará patente al estudiar "primos grandes" en la segunda parte de este artículo, que se publicará próximamente.

Aparentemente, la demostración de Euclides de que el número de primos es infinito ya responde a esta pregunta. Incluso si consideramos el concepto de cardinal, que se usa en teoría de conjuntos para clasificar a éstos según su 'tamaño', vemos que el problema está, en este sentido, resuelto: todos los subconjuntos infinitos de $\mathbb{N}$ son numerables y por tanto el de los números primos lo es también.

Sin embargo, esta respuesta no es completamente satisfactoria si queremos saber 'como es de grande' el conjunto de los números primos en comparación con el conjunto de todos los números enteros. Para ilustrar lo que puede ocurrir, consideremos el conjunto de los cuadrados perfectos 1, 4, 9, 16 ... y preguntémonos si estos son más o menos abundantes que los primos. Una forma de valorarlo consiste en considerar la suma de sus inversos. Euler demostró que la serie

$$1/1 + 1/4 + 1/9 + 1/16 + 1/25 + \ldots$$

converge a $\pi^2/6$. El hecho de ser finita esta suma nos dice que el conjunto de los cuadrados perfectos es, en cierto sentido, 'pequeño' en comparación con el de todos los enteros positivos. En efecto, si se considera la suma los recíprocos de los enteros positivos, se obtiene la denominada *serie armónica*, que es divergente de modo que, como cabía esperar, el conjunto de todos los enteros positivos es 'grande' en este sentido. La pregunta natural es, pues, la siguiente: ¿La serie

$$\sum_{p \text{ primo}} 1/p$$

es convergente o divergente?

La respuesta la dio Euler en 1737, al demostrar (aunque de modo poco riguroso) que la suma de los recíprocos de los primos diverge (cf. [14], que usaremos como referencia general sobre números primos, junto con [5, 12, 17, 18]). Esto podemos interpretarlo en el sentido de que el conjunto de los primos es 'grande' y los primos son mucho más abundantes que, por ejemplo, los cuadrados perfectos.

Con *Mathematica* podemos observar que la suma de los recíprocos de los primos diverge muy lentamente, por ejemplo:

```
Sum[1./Prime[n], {n, 1, 1000000}]
3.06822
```

muestra que la suma de los recíprocos del primer millón de primos es poco mayor que 3. De hecho, se estima que la suma de los recíprocos de todos los primos calculados por todos los ordenadores existentes, es aproximadamente 4 y no va a aumentar sustancialmente en el futuro inmediato.

Lo anterior nos da la idea de que los primos son "relativamente abundantes" entre los enteros positivos, pero esto es demasiado vago y, naturalmente, los matemáticos intentaron obtener información más precisa sobre el tamaño del conjunto de los primos. Por eso, la pregunta natural, que fue planteada explícitamente en el libro famoso [11] de G.H. Hardy y E.M. Wright, publicado por primera vez en 1938, es la siguiente:

¿Existe una fórmula para el n-simo número primo?

Lo que se pedía era encontrar una expresión para el primo n-simo p_n, en términos de n, mediante funciones que sean "computables" en el sentido de que proporcionan un algoritmo eficiente para calcular p_n en la práctica. Aun interpretando el término "fórmula", en su sentido más amplio, como un "algoritmo", los existentes (como el implementado en *Mathematica* por la función `Prime`, que hemos utilizado antes) no cumplen las condiciones requeridas y su valor práctico es nulo cuando n es grande (no permiten calcular, por ejemplo, $p_{10^{50}}$).

El método más evidente de determinar p_n consiste en generar la lista de todos los primos $\leq$ que un entero conveniente x, de modo que x sea suficientemente grande como para que dicha lista contenga al menos n primos y, a continuación, contarlos para determinar cual es el que ocupa el lugar n. La lista de los primos $\leq x$ puede construirse usando un algoritmo que ya era conocido por Eratóstenes de Cyrene, un matemático griego que vivió entre el 276 y el 194 a.C. La *criba de Eratóstenes* comienza escribiendo la lista de todos los enteros positivos entre 2 y x. El primer número de la lista (el 2) es primo y, en el primer paso, marcamos todos los números de la lista que son múltiplos de 2 pero distintos de 2, lo cual se hace saltando las posiciones de dos en dos. El primer entero después del 2 que no ha sido marcado (el 3) tiene que ser primo y, a continuación, vamos saltando posiciones de tres en tres y marcando así todos los múltiplos de 3 que son mayores que 3. Continuando de esta forma, cada vez que se encuentra un nuevo primo, se marcan todos sus

múltiplos mayores que él y se pasa al siguiente entero que no ha sido marcado, el cual tiene que ser, de nuevo, primo. Cuando se llega a un primo mayor que $\sqrt{x}$, todos los enteros que quedan sin marcar tienen que ser primos, puesto que eso significa que ninguno de ellos tiene un factor menor o igual que su raíz cuadrada.

La criba de Eratóstenes es, todavía hoy, el algoritmo más eficiente conocido para generar la tabla de los primos $\leq$ que un x dado. Su eficiencia proviene de que al ir marcando múltiplos de los números que se van obteniendo, las únicas operaciones aritméticas que se usan son adiciones y, además, no es necesario alcanzar x sino que el proceso termina al sobrepasar $\sqrt{x}$. Pero si se quiere probar con ella que un entero dado x es primo, requiere aproximadamente $\sqrt{x}$ pasos, que son muchos cuando x es grande.

El principal inconveniente de la criba es que requiere mucha memoria y para paliar este problema se pueden hacer algunas modificaciones. La más evidente –y que también contribuye a aumentar la rapidez del proceso– consiste en descartar ya de entrada los números pares como se hace en la implementación de *Mathematica* que damos a continuación. Otra posibilidad que ahorra mucha memoria consiste en no almacenar los números impares menores que n sino "unos" (que requieren menos memoria) en su lugar; más adelante utilizaremos este método para cribar intervalos de números muy grandes.

```
Eratostenes[x_] := Module[{P = Range[1, x, 2], i = 3},
 While[i^2 <= x,
  If[P[[(i + 1)/2]] != 1,
   Do[P[[j]] = 1, {j, (i^2 + 1)/2, Length[P], i}]]; i = i + 2];
 Prepend[Rest[Union[P]], 2]] /; x > 1
```

Por ejemplo, se obtiene inmediatamente la lista de los primos ≤ 200:

```
Eratostenes[200]

 {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, 101, 103, 107, 109, 113,
 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181,
 191, 193, 197, 199}
```

Sin embargo, para generar, por ejemplo, la lista de los primos comprendidos entre $10^7 - 100$ y $10^7 + 100$, no tendría mucho sentido –aunque es posible hacerlo– usar la criba de Eratóstenes hasta $10^7 + 100$ y seleccionar los números mayores que $10^7 - 100$, pues este proceso requiere mucha memoria y es muy poco eficiente. Más adelante veremos como modificar la criba para esta situación, pero por el momento podemos utilizar para esto la función `PrimeQ` predefinida en *Mathematica*. Si esta función responde `False`, entonces el argumento es compuesto. Si responde `True` lo único que se puede decir es que es *extremadamente probable* que sea primo pues existe la posibilidad teórica de que el número pueda ser compuesto, aunque no se conoce ningún ejemplo concreto de este comportamiento. En la segunda parte de estas notas me referiré

con más detalle al funcionamiento de esta función (que se sabe que siempre proporciona la respuesta correcta cuando el argumento es menor que 10^{16}) y también a los métodos existentes para *demostrar* la primalidad de un entero grande. Para los experimentos sobre la distribución de los primos que vamos a hacer aquí, la función `PrimeQ` es perfectamente adecuada y, en los casos en que se hace mención explícita de primos concretos, estos lo son realmente, pues su primalidad se ha demostrado usando otros métodos. Se tiene:

```
Select[10^7 - 100 + Range[200], PrimeQ]

{9999901, 9999907, 9999929, 9999931, 9999937, 9999943,
9999971, 9999973, 9999991, 10000019, 10000079}
```

obteniendo el resultado de forma inmediata. Obsérvese la diferencia entre el número de primos existente en los dos intervalos de longitud 200 que hemos considerado, pues de 46 que había en el primero se ha pasado a sólo 11 en el segundo, lo cual, como veremos, no ocurre por casualidad.

Se puede usar la criba de Eratóstenes para obtener, por ejemplo, el primo "millonésimo": `Eratostenes[16*10^6][[10^6]] = 15485863`, pero este método es muy poco eficiente y, por eso, la criba de Eratóstenes no proporciona una respuesta satisfactoria a la pregunta de Hardy y Wright. De hecho, ellos ya aclararon que la fórmula buscada debería de ser menos laboriosa que dicha criba. Aunque se conocen métodos más eficientes que la criba para calcular el primo n-simo (por ejemplo, el implementado por la función `Prime` de *Mathematica*, cf. [3], que nos dice rápidamente que `Prime[1000000] = 15485863`), la pregunta de Hardy-Wright todavía carece de una respuesta afirmativa satisfactoria, y no parece probable que vaya a tenerla.

Para determinar el primo n-simo mediante la tabla de Eratóstenes es necesario primero conocer un valor de x tal que el número de primos $\leq x$ sea mayor que n (pero no mucho mayor, para que el proceso sea lo más eficiente posible desde el punto de vista computacional). Esto lleva a plantear la cuestión del tamaño del conjunto de los números primos de una forma ligeramente diferente, mediante la pregunta:

¿Cuántos primos hay menores que el número entero x?

Al número de primos $\leq x$ se le denota usualmente por $\pi(x)$ y el conocimiento preciso de $\pi(x)$ sugiere la posibilidad de calcular p_n pues, claramente, $p_n = \min\{x|\pi(x) = n\}$ (o bien, si x es primo y $\pi(x) = n$, entonces $x = p_n$). Por tanto, conocer el valor exacto de $\pi(x)$ sería prácticamente equivalente a responder afirmativamente la pregunta sobre el primo n-simo. Por eso, lo que se busca no es una respuesta exacta sino sólo aproximada, lo que es suficiente para conocer como va variando la densidad de los primos al crecer x.

Un problema que aparece al estudiar $\pi(x)$ es que la distribución de los primos es, en cierto sentido, muy aleatoria. En palabras del matemático Don Zagier, en una conferencia pronunciada en Bonn, en 1975 [21]: *... los números primos son uno de los más arbitrarios y pendencieros objetos estudiados por los matemáticos: crecen como semillas entre los números naturales sin que*

parezcan obedecer más ley que la del azar, y nadie puede predecir donde brotará el próximo.

Por ejemplo, hemos visto que entre los 100 enteros que preceden a 10^7 hay nueve primos, mientras que entre los cien siguientes a 10^7 sólo hay dos, es decir, la densidad de primos del primero de estos intervalos es más de cuatro veces superior a la del segundo. Por otra parte, consideremos el problema de determinar el *hueco (gap)* entre dos primos consecutivos p_n y p_{n+1}, que se define como $g(p_n) = p_{n+1} - p_n$. En *Mathematica*, el primo siguiente a un entero dado se puede calcular mediante la función `NextPrime`, perteneciente al paquete `NumberTheory`NumberTheoryFunctions`` que, para números menores que 10^{20}, es esencialmente equivalente a la función siguiente:

```
PrimoSiguiente[n_?IntegerQ] :=
NestWhile[# + 2 &, n + 1 + Mod[n,2], ! PrimeQ[#] &]/; n > 1
```

Utilizando `PrimoSiguiente`, podemos calcular los dos huecos entre tres primos consecutivos, mediante la función:

```
DosPrimosSiguientes[n_] := NestWhileList[PrimoSiguiente,n,True,3]
```

que, aplicada a primos convenientes, proporciona los siguientes huecos:

```
DosPrimosSiguientes[1129]

{1129, 1151, 1153}
```

y, análogamente, `DosPrimosSiguientes[1357201] = {1357201, 1357333, 1357337}` y `DosPrimosSiguientes[7177162611713] = {7177162611713, 7177162612387, 7177162612393}`, que nos muestran huecos de tamaño 22, 132 y 674 seguidos, respectivamente, por huecos de tamaño 2, 4 y 6. En el último caso vemos que el hueco precedente a 7177162612387 es más de 100 veces superior al siguiente. Aun más llamativo es el hecho de que existen huecos arbitrariamente grandes entre dos primos consecutivos, puesto que si $n > 1$, entonces $n! + 2$, $n! + 3$, $\ldots$, $n! + n$, son todos compuestos. En contraste, los huecos más pequeños posibles entre primos (impares) tienen valor 2 y se producen cuando $p_{n+1} - p_n = 2$ en cuyo caso se dice que p_n y p_{n+1} son *primos gemelos*. La conjetura según la cual existen infinitos primos gemelos recibe el nombre de *conjetura de los primos gemelos* y, por diversas razones, alguna de las cuales mencionaré más adelante, está extendida la creencia de que es cierta. De ser así, podemos apreciar claramente la enorme irregularidad existente en la distribución de primos en intervalos pequeños. El tamaño de los huecos crece arbitrariamente, *pero no de forma regular* pues, si existen infinitos primos gemelos, siempre es posible encontrar un hueco arbitrariamente grande y, después de él, uno del tamaño mínimo.

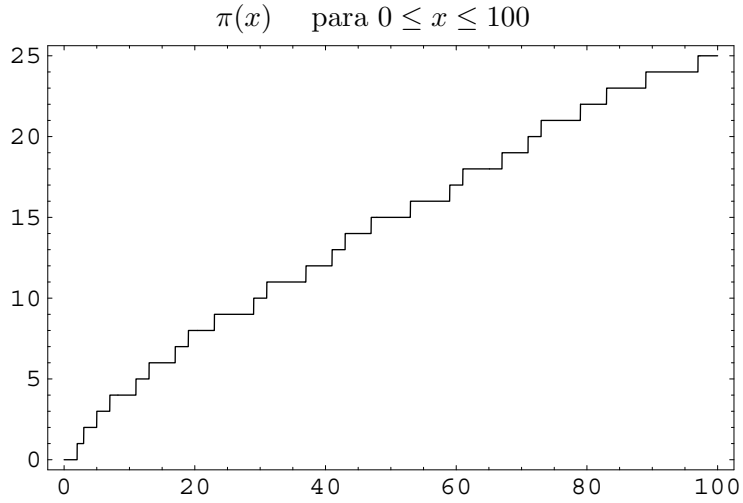
A pesar de todo esto, Zagier [21] dice lo siguiente: *"... los números primos muestran una impresionante regularidad, ... hay leyes que gobiernan su comportamiento, y obedecen esas leyes con precisión casi militar."*

La explicación de esta aparente contradicción reside en el hecho de que la irregularidad en la distribución de los primos se circunscribe a cuando se consideran solamente *intervalos pequeños*, mientras que, por el contrario, la distribución global de los mismos —es decir, la función $\pi(x)$—, muestra, como vamos a ver, una impresionante regularidad. Para hacerse una idea de como va variando $\pi(x)$ podemos empezar por calcularla para valores pequeños de x, siguiendo así los pasos de Gauss que se dice que calculó todos los primos hasta tres millones en intervalos de 1000 números. Podemos definir la función:

```
PrimosHasta[x_] := Length[Eratostenes[x]]
```

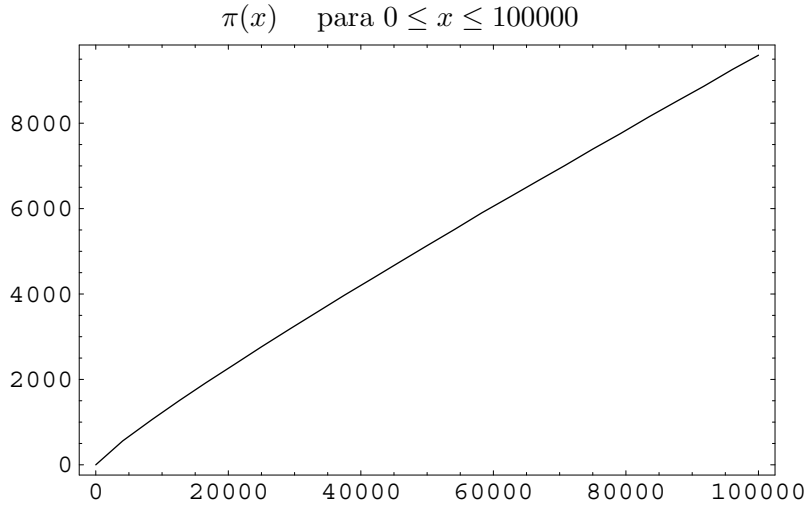
que nos da, por ejemplo, `PrimosHasta[1000000] = 78498`, de modo que $\pi(1000000) = 78498$. Pero es preferible usar la función `PrimePi`, incluída en *Mathematica*, que es mucho más rápida para valores grandes de x pues no necesita calcular, como había hecho Gauss, todos los primos menores que x. Ahora bien, incluso con los algoritmos más eficientes conocidos en la actualidad, el valor mayor de $\pi(x)$ que se ha podido calcular por el momento es $\pi(4 \cdot 10^{22}) = 783964159852157952242$ (en Marzo de 2001, por Xavier Gourdon y el "Proyecto $\pi(x)$", una computación distribuida en la que se puede colaborar a través de la página Web [9]) y no parece probable que en el futuro inmediato se pueda calcular para valores mucho mayores de x. Esto, aparentemente, deja sin responder nuestra pregunta anterior pero hay que darse cuenta que para obtener la respuesta no necesitamos conocer el valor exacto de $\pi(x)$, sino solamente su valor aproximado, y observar como crece éste al hacerse x grande. Con esta idea, podemos empezar por observar la representación gráfica de este función para valores pequeños de x. El grafo de $\pi(x)$ para $x \leq 100$ se puede obtener de la forma siguiente:

```
Plot[PrimePi[x], x, 0, 100, PlotPoints -> 100, Frame -> True,
PlotLabel -> "π(x) para 0≤x≤100"]
```



El grafo anterior es bastante irregular pero si nos "alejamos" un poco y consideramos los valores de x menores que 100000 podemos observar un fenómeno interesante:

```
Plot[PrimePi[x], {x, 0, 100000}, Frame -> True,
PlotLabel -> "π(x) para 0≤x≤100000"]
```



La irregularidad que se observaba en el primer grafo ha disminuido notablemente y se aprecia una forma que sugiere la predecibilidad de $\pi(x)$ para x grande. De hecho, el grafo aparece ya prácticamente liso: para Zagier, la suavidad con la que esta curva crece es uno de los hechos más asombrosos de todas las matemáticas. Podemos construir fácilmente un programa que muestra como crece, para x pequeño, el valor de $x/\pi(x)$:

```
g[x_] := List[x, PrimePi[x], x/PrimePi[x]];
Map[g, NestList[(#*10) &, 10.^4, 6]] // TableForm
```

con el resultado siguiente:

x	$\pi(x)$	$\frac{x}{\pi(x)}$
10000	1229	8,1367
100000	9592	10,4254
1000000	78498	12,7392
10000000	664579	15,0471
100000000	5761455	17,3567
1000000000	50847534	19,6666
10000000000	455052511	21,9755

Se observa que cada vez que x se multiplica por 10, el valor de $x/\pi(x)$ aumenta en $2,3$ que es, aproximadamente, el logaritmo natural de 10. Esto conduce a la conjetura razonable (que hicieron Gauss y Legendre a principios del siglo XIX) :

• *Para x grande, el valor de $\pi(x)$ es, aproximadamente, $x/\ln x$.*

donde $\ln x = \log_e x$ denota el logaritmo natural de x.

Esto se confirmó en 1.896, cuando Hadamard y de la Vallée Poussin demostraron, independientemente, y usando fundamentalmente los métodos desarrollados por Riemann, el llamado *Teorema del número primo*, que proporciona rigurosamente este valor. Para describir este teorema consideremos primero dos funciones f, g, que toman valores reales positivos. Se dice que $f(x)$ y $g(x)$ son *asintóticamente iguales* (o asintóticas) cuando $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$. En este caso se escribe $f(x) \sim g(x)$ y la idea es que, entonces, $g(x)$ es una buena aproximación de $f(x)$ para x grande. Se tiene:

Teorema del número primo (TNP). $\pi(x) \sim x/\ln x$.

El teorema del número primo confirma la idea de que el conjunto de los primos es un subconjunto "grande" del conjunto de todos los enteros positivos. Chris Caldwell cuenta, en su excelente página Web sobre números primos [4], la anécdota de que recientemente alguien le envió un e-mail pidiéndole una lista de todos los primos de no más de 300 dígitos decimales. Por TNP dicha lista habría de tener aproximadamente $1,4 \cdot 10^{297}$ términos y, en consecuencia, ¡no puede existir físicamente!

El teorema del número primo también da una respuesta aproximada a nuestra pregunta anterior sobre el primo n-simo. Si denotamos por $p(n)$ la función que al entero positivo n le hace corresponder el primo n-simo (de modo que $p(n) = p_n$), entonces se tiene que $p(n) \sim n \ln n$ (cf. [20, p. 84]). De hecho, esto es equivalente a TNP, aunque existen aproximaciones mejores), por ejemplo $p(n) \sim n(\ln n + \ln\ln n - 1)$, que es también consecuencia del teorema del número primo.

La aproximación de $\pi(x)$ dada por $x/\ln x$ es razonable (por ejemplo, $\pi(10^{22}) = 201467286689315906290$ y $10^{22}/\ln(10^{22}) \approx 197406582683296285296$, de modo que el error relativo para $n = 10^{22}$ es, aproximadamente, del 2%) pero no es, desde luego, la mejor posible. Gauss, basándose en las tablas de primos que iba construyendo en sus "ratos libres", conjeturó, en primer lugar, cual debería ser que la probabilidad de que un entero aleatorio grande x resulte ser primo. Usando *Mathematica* podemos hacer un experimento, siguiendo sus pasos, pero usando números mucho más grandes de los que el podía manejar a mano. Si hacemos

```
P = NestList[#^2 &, 10^10, 4];
Q = Length[Select[# - 50000 + Range[100000], PrimeQ]] & /@  P


{4276, 2166, 1080, 510, 276}
```

obtenemos el número de primos que hay en un intervalo de longitud 100000, centrado en los números $10^{10}, 10^{20}, 10^{40}, 10^{80}, 10^{160}$. Se puede observar que al elevar el número al cuadrado, es decir, al duplicar su tamaño (o, en otras palabras, su logaritmo), la densidad de primos se reduce, aproximadamente, a la mitad. Esto sugiere que la probabilidad de que el entero aleatorio x resulte ser primo es inversamente proporcional a su logaritmo. Más aun, si a continuación comparamos la frecuencia relativa de primos en la proximidad de x con el recíproco de su logaritmo, mediante

```
TableForm[Transpose[{N[P], Q/100000., 1./Log[P]}],
   TableHeadings ->
    {None, {"x", "Frecuencia relativa de primos", "1/ln x "}}]
```

se obtiene el resultado siguiente:

x	Frecuencia relativa de primos	$1/\ln x$
10^{10}	0.04276	0.0434294
10^{20}	0.02166	0.0217147
10^{40}	0.01080	0.0108574
10^{80}	0.00510	0.00542868
10^{160}	0.00276	0.00271434

Es fácil apreciar la gran coincidencia entre ambos valores y por eso no resulta nada sorprendente la conclusión a la que llegó Gauss: que la probabilidad de que x resulte ser primo debe de ser, aproximadamente, $1/\ln x$.

De aquí dedujo que $\pi(x)$ debía de ser aproximadamente la suma de probabilidades $\pi(x) = \sum_{2\le n\le x} \frac{1}{\ln n}$. Esto conduce a la aproximación $x/\ln x$, contando el número total de enteros desde 2 a x, que es aproximadamente x y multiplicando por la mayor de estas probabilidades que es $1/\ln x$. Pero parece claro que de esta forma se ha simplificado demasiado y se obtiene una aproximación peor que la suma anterior o que la *integral logarítmica*:

$$\mathrm{li}(x) = \int_2^x \frac{dt}{\ln t}$$

de la cual dicha suma es una "suma de Riemann". Por eso Gauss tomó como aproximación esta integral, que es asintótica a $x/\ln x$, de modo que la conjetura de Gauss es equivalente a TNP. *Mathematica* tiene la función `LogIntegral` que representa la integral impropia $\int_0^x \frac{dt}{\ln t}$, de modo que podemos definir:

```
li[x_?NumericQ] := LogIntegral[x]-LogIntegral[2]
```

Por supuesto, como `LogIntegral[2]` $\approx$ `1.04516`, la diferencia entre usar cualquiera de las dos versiones de $\mathrm{li}(x)$ es mínima y, desde luego, no afecta a las estimaciones asintóticas.

Para hacernos una idea de la calidad de la aproximación de $\pi(x)$ mediante $\mathrm{li}(x)$ podemos usar `PrimePi`. Dado que la versión actual de esta función sólo

calcula $\pi(x)$ para valores de x menores que $9 \cdot 10^{13}$, es conveniente completar esta función añadiéndole los valores de $\pi(x)$ computados más recientemente [9] para las potencias de 10 comprendidas entre 10^{13} y 10^{22}. Llamando, por ejemplo, `PiPrima`, a la nueva función así obtenida, la comparación de $\pi(x)$ con $\mathrm{li}(x)$ (redondeada al entero más próximo), nos la da:

```
L[n_] := {N[n],PiPrima[n],Round[li[n]],Round[li[n]-PiPrima[n]]};
Map[L, NestList[(#*10^2) &, 10^8, 7]] // TableForm
```

El resultado es el siguiente:

x	$\pi(x)$	$\mathrm{li}(x)$	$\mathrm{li}(x) - \pi(x)$
10^8	5761455	5762208	753
10^{10}	455052511	455055614	3103
10^{12}	37607912018	37607950280	38262
10^{14}	3204941750802	3204942065691	314889
10^{16}	279238341033925	279238344248556	3214631
10^{18}	24739954287740860	24739954309690414	21949554
10^{20}	2220819602560918840	2220819602783663483	222744643
10^{22}	201467286689315906290	201467286691248261497	1932355207

Se observa en la tabla que esta estimación de $\pi(x)$ es mucho mejor que la dada por $x/\ln x$ pues ahora, aproximadamente, la primera mitad de los dígitos de $\pi(x)$ es dada correctamente por $\mathrm{li}(x)$; es decir, el error en este rango no excede de $\sqrt{x}$ (y, en particular, el error relativo para $x = 10^{22}$ ha descendido al $9,59 \cdot 10^{-10}\%$). La conjetura según la cual este error crece en forma esencialmente proporcional a $\sqrt{x}$ es el problema abierto más famoso de todas las matemáticas: la *Hipótesis de Riemann* (HR). Para formularla de modo más preciso es conveniente introducir la llamada "notación O mayúscula". Si $f(n)$ y $g(n)$ son dos funciones sobre los enteros con valores reales, se dice que $f(n) = O(g(n))$ cuando existe un entero N y una constante $c > 0$ tal que $|f(n)| \leq c \cdot g(n)$ para todo $n \geq N$, donde $|\ |$ denota el valor absoluto. La idea es que, entonces, f es a lo sumo proporcional a g por lo que si g está bien elegida, su crecimiento asintótico es el mismo que el de f. La Hipótesis de Riemann fue originalmente formulada por éste en términos de la "función zeta", $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$, donde $s = \sigma + it$ es una variable compleja con parte real $\sigma = \Re(s) > 1$ y que puede ser definida por prolongación analítica sobre todo el plano complejo con una única singularidad, un "polo simple", en el punto $s = 1$, donde la función zeta se reduce a la serie armónica que es divergente. La función ζ está relacionada con los primos a través de la fórmula del producto de Euler $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$, donde p recorre los primos, y Riemann descubrió que la distribución de sus *ceros* (los $s \in \mathbb{C}$ tales que $\zeta(s) = 0$) está estrechamente relacionada con la distribución de los números primos. Los ceros de la función ζ son de dos tipos: los llamados "ceros triviales" (o ceros reales), que son los puntos $-2, -4, -6, -8, \ldots$, y los no triviales que, como

ya observó Riemann, están dentro de la "banda crítica" $0 \leq \Re(s) \leq 1$ y son simétricos con respecto al eje real (y también con respecto a la "recta crítica" $\Re(s) = \frac{1}{2}$). La Hipótesis de Riemann es que todos los ceros no triviales de $\zeta(s)$ se encuentran de hecho en la recta $\Re(s) = \frac{1}{2}$ (donde se sabe que hay infinitos). Para probar el teorema del número primo, Hadamard y de la Vallée Poussin ya mostraron que no hay ceros en la frontera de la banda crítica, puesto que no hay ceros s con $\Re(s) \geq 1$. El término de error en la estimación de $\pi(x)$ dada por $\mathrm{li}(x)$ está relacionado con la existencia de una región sin ceros en la banda crítica: cuanto mayor sea dicha región, es decir, cuanto más alejados estén los ceros de la frontera, más pequeño es este error. No se puede excluir la posibilidad de que haya ceros extremadamente próximos a la frontera pero el caso más favorable se produce si, como conjeturó Riemann, todos los ceros están en la recta crítica, lo que proporciona la siguiente estimación, que es equivalente a HR y expresa de forma precisa la observación realizada a partir de la tabla anterior, según la cual el término de error en la aproximación de $\pi(x)$ dada por $\mathrm{li}(x)$ es poco mayor que $\sqrt{x}$:

Hipótesis de Riemann. Para cualquier $\varepsilon > 0$, se verifica que $\pi(x) = \mathrm{li}(x) + O(x^{1/2+\varepsilon})$.

Dado que $\lim_{x\to\infty} \frac{\ln x}{x^{\varepsilon}} = 0$, se observa que $\ln x = O(x^{\varepsilon})$ para cada $\varepsilon > 0$, es decir, para x grande, la función logarítmica es menor que cualquier potencia de x por pequeña que sea. Por eso, el ε que aparece en la estimación anterior se puede sustituir por la función logarítmica y, de hecho, tal como demostró Von Koch en 1901 [14], la Hipótesis de Riemann es también equivalente a $\pi(x) = \mathrm{li}(x) + O(x^{1/2} \ln x)$. La influencia de HR para la calidad de la aproximación de $\pi(x)$ por $\mathrm{li}(x)$ se puede apreciar fácilmente si se observa que, por ejemplo,

```
N[Li[10^100], 47] =

4.36197198714070315909950911322916461153875721 17x10^97
```

lo cual nos da el valor de $\pi(10^{100})$ con todos los dígitos dados correctos si suponemos que HR se verifica pues, en ese caso, el error al aproximarla por $\mathrm{li}(10^{100})$ no excede de 10^{51}. Por el contrario, sin HR, sólo se sabe que dicho error es menor que $3 \cdot 10^{95}$ [19] de modo que el tercer dígito de la anterior expresión ya podría ser erróneo (aunque esta cota podría mejorarse si se tienen en cuenta los cálculos recientes de ceros de la función ζ).

La Hipótesis de Riemann ya figuraba en la famosa lista de problemas presentados por Hilbert en el Congreso Internacional de Matemáticas de Paris en el año 1900. En efecto, el Problema 8 incluía los problemas sobre números primos entre los que éste era el más importante. Cien años después, y a pesar de que los problemas de Hilbert tuvieron una importancia decisiva en el desarrollo de las matemáticas durante el siglo XX, HR sigue resistiendo todos los intentos de demostrarla. En el año 2000 un comité de matemáticos

de primerísima línea ha seleccionado, bajo los auspicios del "Clay Mathematics Institute", creado por el millonario norteamericano Landon T. Clay, los *Problemas del milenio* que incluyen aquellos problemas que, a su juicio, serán los más importantes para el desarrollo de las matemáticas durante el próximo siglo XXI (cf. `http://www.claymath.org`). El Instituto Clay ha instituido un premio de un millón de dólares por la resolución de cada uno de los siete problemas seleccionados que fueron anunciados en el "Millennium meeting" en París apenas 100 años después de la famosa conferencia de Hilbert. Por supuesto que uno de ellos es precisamente la Hipótesis de Riemann [2].

Un testimonio indirecto de la importancia y la dificultad de HR lo proporciona un curioso episodio que se cuenta que ocurrió cuando G.H. Hardy estaba haciendo una travesía en barco desde Escandinavia a Inglaterra. Dado que Hardy tenía mucho miedo a lo que pudiera ocurrir en dicho viaje, decidió contratar una póliza de seguros pero lo hizo de forma bastante inusual, escribiendo una postal a un amigo en la que decía: *"He conseguido demostrar la Hipótesis de Riemann"*. Su razonamiento era que Dios no iba a permitir que él pereciese en un naufragio y pasase falsamente a la Historia por haber resuelto el problema matemático más difícil. Ni que decir tiene que Hardy sobrevivió al viaje.

Existen muchas razones para creer que la Hipótesis de Riemann es cierta, comenzando por la existencia de muchos resultados profundos de teoría de números que son consecuencias de HR (o de alguna versión más general de la misma) y que también pueden ser probados sin hacer uso de ella. Otras razones a favor de HR incluyen argumentos heurísticos de tipo probabilista y también la evidencia empírica obtenida bien a través del cálculo directo de miles de millones de ceros de la función ζ o bien a través del estudio de la distribución de los números primos; un análisis detallado de todas estas razones se encuentra en [2]. Sin embargo, hay que señalar que es peligroso hacer conjeturas sobre los enteros tomando como base solamente datos experimentales. La tabla anterior puede servir como ejemplo, pues se observa que en ella el valor de $\mathrm{li}(x)$ es siempre mayor que el de $\pi(x)$, es decir, la diferencia $\mathrm{li}(x) - \pi(x)$ es positiva. De hecho, esto ocurre para todos los valores de x que han sido computados, hasta $x = 10^{23}$. Esto podría hacer pensar que $\mathrm{li}(x) - \pi(x)$ es positivo para todo x y así lo conjeturó Riemann, pero Littlewood demostró en 1914 que esta diferencia cambia de signo infinitas veces. Quizá ésta fuera una de las razones por las que, a pesar de la evidencia experimental que él no aceptaba como tal, Littlewood creía (en 1962, cf. [7]) que la Hipótesis de Riemann era falsa.

En un trabajo publicado en 1968, I.J. Good y R.F. Churchhouse [8] dieron, siguiendo una idea de Denjoy, un argumento heurístico de tipo probabilista en favor de la verificación de la hipótesis de Riemann, que se puede resumir como sigue. Consideremos la *función de Möbius* definida de la manera siguiente:

$$\mu(n) = \begin{cases} 0 & \text{si } n \text{ es divisible por un cuadrado} \neq 1 \\ (-1)^t & \text{si } n = p_1 \dots p_t \text{ es producto de } t \text{ primos distintos} \end{cases}$$

Sea entonces $M(x) = \sum_{n \leq x} \mu(n)$, la llamada *función de Mertens*. Si n es un entero grande libre de cuadrados (es decir, $\mu(n) \neq 0$) no existe ninguna razón especial para suponer que n deba tener un número par o impar de factores primos y así se podría considerar a $\mu(n)$ como una variable aleatoria acotada cuya distribución es simétrica en torno a 0. Si los valores de $\mu(n)$ fuesen independientes cabría esperar que $|M(x)|$ no creciese demasiado y, de hecho, se tendría por un resultado de teoría de la probabilidad llamado "desigualdad de Hausdorff" o "estimación de Hausdorff" que $M(x) = O(x^{1/2+\varepsilon})$ para todo $\varepsilon > 0$. Pero es conocido que esto equivale a la verificación de HR [5, Theorem 1.4.3]. Por tanto, si los valores de la función de Möbius que, por supuesto, es completamente determinista, satisfacen la hipótesis de independencia anterior, la Hipótesis de Riemann sería verdadera. Para dar fuerza a este argumento, Good y Churchhouse calcularon los valores de la suma de $\mu(n)$, con n recorriendo intervalos de longitud 1000, y comprobaron que los datos obtenidos proporcionaban evidencia de tipo estadístico en favor del modelo aleatorio propuesto (los valores de la función μ se obtienen de forma determinista pero, aparentan comportarse como si hubieran sido obtenidos aleatoriamente). Además, calcularon el número de ceros de $\mu(n)$ para n comprendido entre 1 y $33 \cdot 10^6$. La probabilidad de que un entero n tomado al azar no sea múltiplo de p^2 es $\frac{p^2-1}{p^2}$ y, si las condiciones de divisibilidad por los distintos p^2, con p primo, son independientes, se obtiene que la probabilidad de que $\mu(n) \neq 0$ es el producto infinito

$$\prod_p \frac{p^2-1}{p^2}$$

cuyo valor resulta ser $6/\pi^2$. Por lo tanto, el número de ceros esperado en el intervalo anterior es $33 \cdot 10^6 \cdot (1 - 6/\pi^2) = 12.938.405,6$. El número real de ceros que calcularon es 12.938.407, lo cual es una aproximación asombrosa o, en palabras de Good y Churchhouse *mejor de lo que merecíamos*. Usando *Mathematica*, podemos repetir, e incluso ampliar el experimento de Good y Churchhouse. En primer lugar, construimos una función que calcula el número de ceros de $\mu(n)$ en el intervalo $[1, n]$:

```
CerosdeMu[n_] := Module[{i = 1, j = 0},
     While[i <= n, If[MoebiusMu[i] == 0, j++]; i++]; j]
```

que nos permite calcular:

```
CerosdeMu[33*10^6] = 12938407
```

Se podría pensar que Good y Churchhouse tuvieron mucha suerte, pero si se calcula:

```
CerosdeMu[33*10^7] = 129384061
```

vemos que, como `33*10^7(1-6/π^2) = 129384056`, el error relativo es incluso menor, siendo en este caso inferior al $0,000004$ %. Si tabulamos el número de ceros de $\mu(n)$ en los intervalos $[1, 10^2], \ldots [1, 10^9]$, comparándolo con los valores redondeados de $10^2 \cdot (1 - \frac{6}{\pi^2}), \ldots 10^9 \cdot (1 - \frac{6}{\pi^2})$, obtenemos el resultado siguiente:

n	$\#\{x \in [1,n] \mid \mu(x) = 0\}$	$n(1 - \frac{6}{\pi^2})$
100	39	39
1000	392	392
10000	3917	3921
100000	39206	39207
1000000	392074	392073
10000000	3920709	3920729
100000000	39207306	39207290
1000000000	392072876	392072898

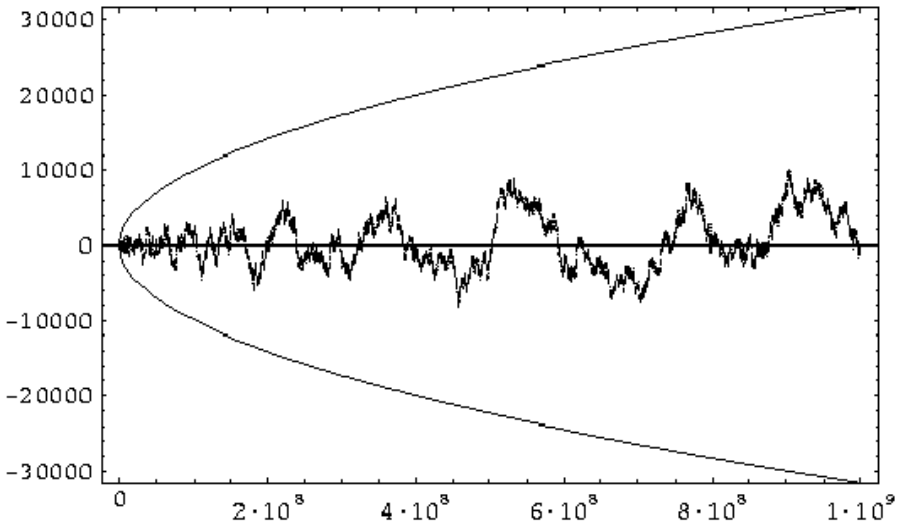
Vemos que la coincidencia entre los valores obtenidos y los esperados de acuerdo con el modelo aleatorio es asombrosa. Por otra parte, función:

```
M[r_,s_]:= Module[{L = { }},
L = Table[Sum[MoebiusMu[j], {j, (i-1)*r + 1, i*r}], {i, s}];
Do[L[[i]] = L[[i-1] + L[[i]], {i, 2, s}];
Transpose[{Range[r, r*s, r], L}]]
```

devuelve la lista de los valores de $M(x)$ en los puntos $\{r, 2r, \ldots, s \cdot r\}$. Tomando, por ejemplo, $r = 100000$ y $s = 10000$, podemos obtener los valores de $M(x)$ en los múltiplos de 100000 comprendidos entre 0 y 10^9. Si representamos gráficamente estos valores, junto con los de $\sqrt{x}$ y $-\sqrt{x}$, mediante:

```
M10e9 = ListPlot[M[100000, 10000], PlotStyle -> PointSize[.001]];
R1 = Plot[Sqrt[x], {x, 0, 10^9}];
R2 = Plot[-Sqrt[x], {x, 0, 10^9}];
Show[M10e9, R1, R2, PlotRange -> {-32622, 31622}]
```

obtenemos la siguiente figura:



Los valores de $M(x)$ en este intervalo parecen acordes con el modelo aleatorio antes expuesto y el grafo anterior muestra el aspecto característico de la función suma de un "paseo aleatorio". Además, se aprecia claramente que los valores de la función de Mertens permanecen dentro de la región acotada por $\sqrt{x}$, con un margen muy amplio.

Aunque el argumento heurístico es bastante persuasivo, hay que ser muy cautos con este tipo de razonamientos (de hecho, Hardy y Littlewood ya muestran en [10] una cierta desconfianza sobre el uso de argumentos heurísticos de tipo probabilístico en teoría de números, a pesar de que ellos mismos los utilizaron). Por otra parte, el experimento anterior también podría inducir a conjeturar que $|M(x)| < \sqrt{x}$. Esta desigualdad es la llamada *conjetura de Mertens*, que fue planteada por éste en 1897 sobre la base de sus cálculos de $M(x)$ para $x = 1, 2, \ldots, 10000$ y es, obviamente, más fuerte que HR. Sin embargo, la conjetura de Mertens es *falsa*, como mostraron Odlyzko y te Riele en 1985 [16]. Para ello computaron los 2000 primeros ceros de la función ζ con unos 100 dígitos decimales significativos, pero aun no se conoce un valor concreto de x para el cual esta desigualdad falla, aunque sí se sabe que existe uno menor que $e^{3,21\cdot 10^{64}}$. Además, se conjetura que el valor de $|M(x)|/\sqrt{x}$ no está acotado, contrariamente a lo afirmado por Stieltjes en 1885 (lo cual, de ser cierto, significaría que Stieltjes habría probado HR). El que HR pueda ser cierta, a pesar de esto, no debe sorprender demasiado pues, como ya hemos observado, $O(x^{1/2+\varepsilon})$ crece asintóticamente de forma más rápida que, por ejemplo, $\sqrt{x}\ln x$. Esto muestra la gran distancia existente entre decir que "$M(x)$ crece poco más que proporcionalmente a $\sqrt{x}$" (HR, cuya veracidad es creencia casi generalizada) y decir que "$M(x)$ está acotada por $\sqrt{x}$" (conjetura de Mertens).

Existe una generalización de la Hipótesis de Riemann que tiene, como veremos más adelante, consecuencias importantes en la teoría de los números primos. Para introducirla, hagamos primero un pequeño experimento, siguiendo los pasos de Legendre. Excepto el 2 y el 5, todos los primos terminan en 1, 3, 7 o 9. Preguntémonos, por ejemplo, cuántos hay de cada uno de estos tipos entre los primos menores que 3000000, que fueron los que llegó a calcular Gauss. Para ello, observemos que los números terminados en 1 son los del conjunto $\{10k + 1 | k \in \mathbb{N}\}$ y lo análogo se puede decir de los terminados en 3, 7 y 9. La función:

```
Legendre10[a_] :=
{a, Count[Map[PrimeQ[#] &, Range[a, 3*10^6, 10]], True]}
```

nos proporciona el número de primos $\leq$ 3.000.000 terminados en a y nos permite tabular, en pocos segundos, cuantos hay de cada una de las clases anteriores,

```
Map[Legendre10, {1, 3, 7, 9}] // TableForm
```

con el resultado siguiente:

a	# de primos $\leq 3 \cdot 10^6$ terminados en a
1	54175
3	54230
7	54249
9	54160

Es fácil darse cuenta de que los cuatro números están muy próximos entre sí y esto ya lo observó Legendre (usando menos primos y con bastante más trabajo). De hecho, Legendre observó algo bastante más general, y es que los primos parecen estar uniformemente distribuidos entre las varias clases residuales módulo n. Recordemos que si n es un entero ≥ 2, la clase residual de un entero a módulo n está formada por todos los enteros de la forma $kn + a$ con $k \in \mathbb{Z}$. Cada clase residual módulo n contiene un único entero r tal que $0 \leq r < n$ y por tanto existen exactamente n de estas clases. Si a es un entero perteneciente a la misma clase que r, entonces r es precisamente el resto obtenido al realizar la división entera de a por n, es decir, $a = qn + r$ para algún entero q y se dice que r es el menor residuo no negativo de a módulo n, simbólicamente $r = a \pmod{n}$. Si a y b están en la misma clase residual módulo n, es decir, si el menor residuo no negativo módulo n de ambos coincide, se dice que a es congruente con b módulo n, simbólicamente $a \equiv b \pmod{n}$. Las clases residuales módulo n forman una partición del conjunto $\mathbb{Z}$ de los números enteros, es decir, $\mathbb{Z}$ es la unión disjunta de todas ellas. Por eso lo que pensó Legendre resulta bastante natural si los primos están distribuidos en $\mathbb{Z}$ de forma homogénea. Al decir que los primos están uniformemente distribuidos entre las distintas clases residuales módulo n, hay que excluir todas las correspondientes a enteros a que tienen un factor no trivial común con n pues si $d = \mathrm{mcd}(a, n)$ es el máximo común divisor de a y n, entonces todos los elementos de la clase residual de $a \pmod{n}$ son múltiplos de d y, como máximo, esta clase sólo puede contener un primo en caso de serlo d. Esto nos deja exactamente $\phi(n)$ clases, donde $\phi(n)$ es la "función ϕ de Euler" que cuenta el número de enteros positivos $\leq n$ que son primos con n (pues las clases que nos interesan son las que corresponden precisamente a los $\phi(n)$ menores residuos no negativos que son primos con n). Por eso, en el ejemplo anterior, hemos considerado solamente las clases de 1, 3, 7 y 9 que son los cuatro residuos no negativos $\pmod{10}$ coprimos con 10. Obsérvese también que el número total de primos en estas cuatro clases suma 216814, pues faltan el 2 y el 5 para completar el número total $\pi(3 \cdot 10^6) = 216816$.

La función `Legendre10` antes definida, se puede generalizar fácilmente para obtener una función que calcula el número de primos $\leq x$ que son congruentes con $a \pmod{n}$, donde $a < n$ y $\mathrm{mcd}(a, n) = 1$:

```
NumerodePrimos[a_, n_, x_] :=
Count[Map[PrimeQ[#]&, Range[a,x,n]], True]/;a<n && GCD[a, n]==1;
Attributes[NumerodePrimos] = {Listable};
```

Por ejemplo, `NumerodePrimos[Range[10], 11, 3 10^6] = {21651, 21715, 21657, 21661, 21631, 21717, 21689, 21689, 21717, 21690}`, lo que nos

da el número de primos $\leq 3 \cdot 10^6$ que hay en cada clase no nula módulo 11 (con su orden natural) observándose, de nuevo, que la desviación de la media (21682) es muy pequeña en todos los casos.

Basándose en sus observaciones para primos pequeños, Legendre conjeturó el siguiente resultado, que fue demostrado por Dirichlet en 1837:

• *Si* $\mathrm{mcd}(a, n) = 1$*, entonces existen infinitos primos congruentes con* a *mod* n

Este teorema se conoce como el "Teorema sobre los primos en una progresión aritmética", pues una progresión aritmética con primer elemento a y razón n es lo mismo que la clase residual de a mod n (o que sus términos positivos). Por tanto, el teorema de Dirichlet dice que todas las progresiones aritméticas "interesantes" contienen un número infinito de primos. Se podría pensar que este resultado es una sencilla generalización del teorema de Euclides sobre la infinitud de los primos pero no es así. La demostración de Dirichlet utiliza métodos analíticos y fue un logro asombroso teniendo en cuenta los conocimientos de la época. De hecho, muchos la consideran como el auténtico nacimiento de la teoría de números analítica, pues los resultados obtenidos anteriormente por métodos analíticos eran mucho más sencillos y, a menudo, poco rigurosos.

Si los primos están equidistribuidos entre las $\phi(n)$ clases de congruencia "interesantes" módulo n, la conclusión lógica es que si $\pi(x, n, a)$ denota el número de primos $\leq n$ y congruentes con a mod n, entonces el valor de esta función para n grande debería de ser aproximadamente $x/(\phi(n) \ln x)$. Efectivamente es así y ambas funciones son asintóticas como demostró de la Vallée Poussin. Esto nos dice por ejemplo, teniendo en cuenta que $\phi(10) = 4$, que el número de primos $\leq x$ terminados en 9 es asintótico a $x/4 \ln x$ y también a $\mathrm{li}(x)/4$, y lo mismo vale para los primos terminados en 1, 3 o 7. De la misma manera que la función zeta de Riemann controla el término de error en el teorema del número primo, existen unas funciones complejas llamadas *L-funciones* o *L-series* de Dirichlet, que generalizan la función zeta y controlan el término de error para el teorema del número primo relativo a progresiones aritméticas. La *Hipótesis de Riemann extendida*, HRE, se enuncia usualmente en términos de los ceros de las L-funciones pero tiene una forma equivalente, similar a la antes vista para HR, que es la siguiente:

HRE. Si $\mathrm{mcd}(a, n) = 1$, entonces para cualquier $\varepsilon > 0$ se verifica

$$\pi(x, n, a) = \frac{\mathrm{li}(x)}{\phi(n)} + O(x^{1/2+\varepsilon})$$

Los argumentos heurísticos en favor de la HRE son similares a los que existen para la Hipótesis de Riemann.

Examinemos ahora el problema de la "densidad" de los primos gemelos. En 1919, el matemático noruego Viggo Brun, que fue uno de los primeros en usar los llamados "métodos de criba", tenía la esperanza de probar la conjetura de los primos gemelos mostrando que la serie formada por la suma de los

inversos de dichos primos divergía, aunque lentamente. Pero, en lugar de ello, probó que dicha serie converge, lo que solamente lleva a la conclusión de que la densidad de primos gemelos es mucho menor que la de primos cualesquiera. La suma de los recíprocos de los primos gemelos es la llamada *constante de Brun*, cuyo valor exacto no se conoce pero que ha sido estimado heurísticamente en 2000 por T.R. Nicely usando los primos gemelos menores que 3×10^{15}, como $1,9021605823 \pm 0,0000000008$.

Podemos determinar fácilmente los primos p tales que $p+2$ es primo y $p \leq n$:

```
Gemelos[n_] := Module[{E = Eratostenes[n], G = {}},
  G = Intersection[E, Map[# - 2 &, E]];
  If[Last[E]>n-2 && PrimeQ[Last[E]+2], Append[G,Last[E]],G]]/;n>1
```

y la constante de Brun puede ser aproximada por una suma parcial de la serie

$$(1/3 + 1/5) + (1/5 + 1/7) + (1/11 + 1/13) + \ldots \ldots$$

mediante la función de *Mathematica*:

```
SumaBrun[n_] :=
   Apply[Plus, Map[(1./#) &, Gemelos[n]]] +
     Apply[Plus, Map[(1./#) &, Gemelos[n] + 2]]/;n > 2
```

que tomando, por ejemplo, $n = 10^7$, nos da `SumaBrun[10^7] = 1.73836`, un valor que está todavía bastante alejado del valor real de esta constante puesto que la serie anterior converge muy lentamente. Para aproximar mejor su valor, existe una extrapolación basada en un argumento heurístico de Hardy y Littlewood y obtenida por Fröberg en 1961 [15], la cual consiste en aproximar la constante de Brun por

```
Brun[n_] := SumaBrun[n] + (4*0.6601618158)/Log[n]/;n > 2
```

donde 0.6601618158 es la llamada "constante de los primos gemelos" a la que me referiré más adelante, y el error estimado es $O(1/(\sqrt{n}\ln n))$. Esto nos permite calcular `Brun[10^7] = 1.90219`, con un error ya pequeño si se toma como referencia el valor de la constante computado por T.R. Nicely.

Es posible ver que uno de los hechos que dan plausibilidad a la conjetura de los primos gemelos es precisamente TNP. Si la primalidad de un entero aleatorio grande n y la del entero $n+2$ fuesen sucesos independientes, se deduciría de TNP que la probabilidad de que ambos sean primos es, aproximadamente, $1/(\ln n)^2$ y, en consecuencia, que hay unos $n/(\ln n)^2$ (pares de) primos gemelos $\leq n$. Pero es fácil darse cuenta de que esto no es así, pues, por ejemplo, si $n > 2$ es primo, entonces $n+2$ es impar, lo cual aumenta la probabilidad de que sea primo en comparación con la de un entero aleatorio del mismo tamaño. La cosa tampoco termina aquí pues, dado que exactamente uno de cada tres enteros consecutivos es múltiplo de 3, la probabilidad de que $n+2$ no sea múltiplo de 3 es $1/2$ y, por tanto, menor que la de un entero arbitrario. Se puede continuar así, pero antes hagamos un experimento para ver lo que puede ocurrir en la práctica. La función:

```
G[n_, r_] := Module[{P = {}, L = {}},
    P = Select[n + Range[r], PrimeQ];
    L = Intersection[P, Map[# - 2 &, P]];
      If[P == {}, 0,
        If[Last[P] > n + r - 2 && PrimeQ[Last[P] + 2],
          Length[Append[L, Last[P]]], Length[L]]]]
```

nos proporciona el número de primos p en el intervalo $[n+1, n+r]$ tales que $p+2$ es también primo y así la función:

```
GM[n_, r_] := G[n, r]*Log[n]^2/r
```

nos da la relación entre la frecuencia relativa de primos gemelos en el intervalo y $1/(\ln n)^2$ (este valor sólo es significativo cuando n es mucho mayor que r). Por ejemplo, se tiene que `GM[10^10, 10^6] // N = 1.30904`, lo que sugiere que la probabilidad de que n y $n+2$ sean primos está próxima, para n grande, a $1,31/(\ln n)^2$, algo que, como vamos a ver, concuerda grandemente con una conjetura a la que se puede llegar usando un argumento heurístico sencillo de tipo probabilista (cf. [1, p. 225], [5, p. 13]).

Supongamos que p es primo y m, m', n son enteros grandes de, aproximadamente, el mismo tamaño. Si suponemos que n no es divisible por p (donde $p > 2$), la probabilidad de que $n+2$ tampoco lo sea será $(p-2)/(p-1)$ pues, excluyendo la clase residual de $n \pmod p$ (que no puede ser 0), quedan $p-1$ posibles clases residuales módulo p que pueden contener a $n+2 \pmod p$, de las cuales $p-2$ son distintas de cero. Por tanto, denotando las probabilidades por P se tiene que $P[n, n+2 \not\equiv 0 \pmod p] = \frac{p-1}{p} \cdot \frac{p-2}{p-1} = \frac{p-2}{p}$. Por otra parte, $P[m, m' \not\equiv 0 \pmod p] = ((p-1)/p)^2$ y, en consecuencia:

$$\frac{P[n, n+2 \not\equiv 0 \pmod p]}{P[m, m' \not\equiv 0 \pmod p]} = \begin{cases} 2 & \text{si } p = 2 \\ p(p-2)/(p-1)^2 & \text{si } p \text{ es impar} \end{cases}$$

Suponiendo que las condiciones de divisibilidad para los distintos primos p sean independientes se tendrá:

$$P[n, n{+}2 \text{ ambos primos}] = \frac{P[n, n+2 \text{ ambos primos}]}{P[m, m' \text{ ambos primos}]} \cdot P[m, m' \text{ ambos primos}]$$

$$= 2 \prod_{p \geq 3} \frac{p(p-2)}{(p-1)^2} \cdot \frac{1}{(\ln n)^2}$$

Por eso, Hardy y Littlewood conjeturaron que el número $\pi_2(x)$ de primos gemelos menores que x (más precisamente, el número de primos p tales que $p+2$ es primo y $p \leq x$) debería de ser asintótico a (cf. [18, pp. 60-68]):

$$2 \prod_{p \geq 3} \frac{p(p-2)}{(p-1)^2} \int_2^x \frac{dt}{(\ln t)^2}$$

donde se ha introducido una integral cuyo valor es asintótico a $1/(\ln x)^2$ para mejorar la calidad de la estimación. El producto infinito que aparece en la expresión anterior es la llamada *"constante de los primos gemelos"*, C_2. Se puede obtener fácilmente un valor aproximado bastante preciso para C_2, utilizando, por ejemplo, el primer millón de primos:

```
NumberForm[Product[Prime[n]*(Prime[n] - 2.)/(Prime[n] - 1.)^2,
{n, 2, 1000000}], 9] = 0.660161818
```

El valor real estimado por Wrench, Nicely y otros es $0,6601618158\ldots$, de modo que se obtiene para la función $\pi_2(x)$ la estimación

$$\mathrm{li}_2(x) = 1,320323632 \int_2^x \frac{dt}{(\ln t)^2}$$

a la cual $\pi_2(x)$ debe de ser asintótica de ser correcto el argumento heurístico utilizado. Como el valor de $\mathrm{li}_2(x)$ tiende a ∞ al tender x a ∞, de ser esto cierto se deduciría que el número de primos gemelos es infinito. Por otra parte, vemos que el valor de $2C_2$ concuerda bien, como cabría esperar de ser cierta la conjetura de Hardy-Littlewood, con el valor `1.3094` obtenido en el experimento anterior con primos gemelos próximos a 10^{10}.

El valor exacto de $\pi_2(x)$ puede ser computado, para valores no muy grandes de x, mediante la función

```
pi2[n_] := Length[Gemelos[n]]/;n > 1
```

la cual, por ejemplo, nos da, `pi2[10^6] = 8169`.

La calidad de la estimación proporcionada por $\mathrm{li}_2(x)$ es muy alta si uno toma como referencia los cálculos numéricos que se han hecho hasta $x = 3,09 \cdot 10^{15}$ (cf. [15]) pues, por ejemplo, se tiene que para el valor de x mencionado, $\pi_2(3,09 \cdot 10^{15}) = 3404004348968$, mientras que

```
Round[2*0.660161815846869573927812110014555778432623*
     Integrate[1/Log[t]^2, {t, 2, 3.09*10^15}]]

3404003492820
```

(donde se ha usado el último valor computado por Nicely de la constante de los primos gemelos). Entonces el círculo se cierra y la conjetura de los primos gemelos que, de ser cierta, es muestra palpable de la irregularidad de la distribución de los primos en intervalos pequeños recibe su mayor apoyo del Teorema del número primo que es la plasmación de la disciplina casi militar con la que, según Zagier, se comportan. Es curioso que el anterior argumento en favor de la conjetura de los primos gemelos se deba precisamente a Hardy y Littlewood, teniendo en cuenta su desconfianza, ya mencionada, hacia los métodos heurísticos de tipo probabilístico.

Para ilustrar algunas de las ideas anteriores y, en particular, el teorema del número primo, consideraré, de nuevo, el problema de determinar el primo

siguiente a un entero n dado. Ya hemos visto como se puede hacer mediante la función `PrimoSiguiente`, pero ahora vamos a tratar de optimizar esta función para el caso en que se aplica a números muy grandes. Una posibilidad es hacer como en la función `NextPrime` incluida en *Mathematica*. Aunque en la documentación se menciona que usa una criba, lo que hace en realidad es ir descartando (mediante el cálculo del máximo común divisor con un producto de primos) los números que son divisibles por "primos pequeños" antes de aplicar `PrimeQ`. Otra posibilidad, que es la que voy a explorar a continuación, consiste en utilizar una criba (en sentido estricto) para este mismo fin. La siguiente función criba un intervalo de enteros positivos `[a,b]`, eliminando todos aquellos que sean divisibles por un primo $\leq p_m$. Dado que se puede utilizar para cribar números muy grandes, con la finalidad de ahorrar memoria se han sustituido los números (impares) de dicho intervalo por unos y sólo se recuperan dichos números una vez finalizado el proceso de cribar.

```
Criba[a_Integer, b_Integer, m_Integer] :=
  Module[{i = 2, r = a + Mod[a, 2, 1] - 1, k, T = {}},
   l = (b + Mod[b, 2] - 1 - r)/2 + 1;
   T = Table[1, {l}];
    While[i <= m, k = 1 +
     Mod[(Mod[Mod[r,Prime[i]],2,1]*Prime[i] - Mod[r,Prime[i]])/2,
     Prime[i]];
    Do[T[[j]] = 0, {j, k, l, Prime[i]}]; i++];
    T = Table[T[[v]]*(r + 2*(v - 1)), {v, 1, l}];
    Rest[Union[T]]];m > 1 && a > 1.7*m*Log[m] && b - a > 4
```

El inconveniente de utilizar una criba radica en el hecho de que uno nunca sabe –recordemos las palabras de Zagier– donde va a aparecer el próximo primo y la criba se ha de realizar sobre un intervalo de longitud fijada de antemano. Dado que, según TNP, aproximadamente uno de cada $\ln n$ enteros próximos a n es primo, parece natural que el intervalo a cribar varíe en forma proporcional a $\ln n$. En el programa siguiente hemos elegido como tamaño del intervalo de criba $t = 4 \cdot \ln n$, lo cual asegura que para la gran mayoría de los enteros n, el primo siguiente estará en este intervalo y no será necesario iterar la criba, mientras que, por otra parte, el intervalo no es demasiado grande y no se pierde mucho tiempo aunque el primo siguiente esté próximo. Otro problema es el de determinar el número de primos m a utilizar para cribar. Se podría pensar que el primo mayor que se utiliza para cribar debería crecer en forma proporcional a t. Para ello habría que tomar, usando de nuevo TNP, m proporcional a $t/\ln t$. Pero esto no tiene en cuenta el hecho de que el coste de la criba crece mucho menos que el coste de ejecutar `PrimeQ` sobre los números no eliminados y, por eso, es conveniente hacer crecer m incluso más que t. En la función siguiente, `SiguientePrimo` se toma m proporcional a $t \cdot (\ln t)^2$ porque, en la práctica, se ve que da buenos resultados. Aunque para valores relativamente pequeños de n (por ejemplo, los comprendidos entre 2^{128} y 2^{256}) es ligeramente más lenta que `NextPrime` (cuando el primo está muy próximo, la división es algo más eficiente), esto carece de importancia pues en este

rango el primo siguiente se obtiene en centésimas de segundo, y para valores más grandes como, por ejemplo, 2^{512} y números mayores, la criba muestra su eficacia y `SiguientePrimo` es, por término medio, apreciablemente más rápida que `NextPrime`.

```
SiguientePrimo[n_] :=
  Module[{i = n, t = Floor[4 Log[n]], P = {}, k = 1},
   If[i < 2^140, PrimoSiguiente[i],
   While[True, P = Criba[i + 1, i + t, Floor[t Log[t]^2/100]];
    While[k <= Length[P] && ! PrimeQ[P[[k]]], k++];
  If[k <= Length[P], Break[], k = 1; i = i + t]]; P[[k]]]]/;n > 1
```

Esta función puede trabajar con números muy grandes. Se llaman *primos titánicos* los primos que tienen mil dígitos decimales o más; el nombre proviene de un artículo de S. Yates (1985), titulado *"Sinkers of the Titanics"*, un juego de palabras que hace referencia al barco y a los buscadores de primos grandes. El programa:

```
Rest[NestList[SiguientePrimo[#] &, 10^999, 3]] - 10^999
{7, 663, 2121}
```

muestra que los tres primeros primos titánicos son $10^{999}+7$, $10^{999}+663$ y $10^{999}+2121$ (aunque aquí se han obtenido usando `PrimeQ`, estos son realmente primos y no sólo primos probables).

Si se quiere cribar intervalos muy grandes, es conveniente modificar la criba anterior, haciendo que los números que sobrevivan a la criba no se recuperen simultáneamente sino que se mantengan almacenados en forma de "unos" una vez finalizado el proceso. Aunque omitiré los detalles por ser, quizá, demasiado técnicos, mencionaré que, usando una criba de este tipo y `PrimeQ` he calculado todos los primos titánicos (probables) del intervalo $[10^{999}, 10^{999}+3\cdot 10^7]$, que son un total de 13112 y entre los cuales hay nueve pares de primos gemelos. La lista de los "huecos maximales relativos" de este intervalo, es decir, de los huecos que son mayores que cualquier hueco precedente en el intervalo, es la siguiente: 656, 1458, 3596, 3894, 6042, 7024, 16284, 19650, 21570, 21612. Los primos que limitan este último hueco, que es el mayor del intervalo, son $10^{999}+24196837$ y $10^{999}+24218449$.

El hueco que acabo de mencionar es bastante grande (más aun si se tiene en cuenta que el hueco más grande calculado en 1993 era, según [17, p. 251], de longitud 864), pero el "hueco record", es decir, el mayor hueco calculado explícitamente y limitado por dos números que se ha *demostrado* que son primos era, en julio de 2001, un hueco encontrado por Dubner próximo a 10^{1883} y que tiene longitud 50206. Para buscar un hueco más grande, cribé los primeros 20 millones de números de 2^{13} bits, usando para ello los 10^7 primeros primos, y eliminando así todos los compuestos que tienen un factor menor que 179424673, lo cual dejó algo menos del 3% de los números del intervalo. Después usé un programa optimizado para buscar huecos mayores que uno dado (50206 en este caso) entre los primos del intervalo y un hueco de

longitud 52478 apareció entre los números $2^{8191}+19506585$ y $2^{8191}+19559063$. En Septiembre de 2001 ambos números fueron certificados como primos por Nathan Russell y Greg Childers, respectivamente, usando el programa *Primo*, de Marcel Martin [13], que implementa el método ECPP (basado en curvas elípticas) para demostrar que un entero es primo. Por tanto, en el momento de escribir estas líneas, el hueco de 52478 es el mayor hueco conocido entre dos números que se ha demostrado que son primos. Sin embargo, en un cierto sentido, se puede decir que este hueco no es tan grande si se tiene en cuenta el tamaño de los primos manejados. Existe una conjetura de Shanks [18, p.82] según la cual un hueco de longitud g debe de aparecer antes de $e^{1,62\sqrt{g}}$ (o, incluso, antes de $e^{1,13\sqrt{g}}$ [15]). De ser así, un hueco de longitud mayor que 52478 debe de ocurrir antes de 10^{162} (y un hueco superior a dos millones antes de 10^{995}, es decir, antes de llegar a los primos titánicos) aunque, dada la escasez de huecos de este tamaño en el entorno de los números mencionados, sería extremadamente difícil (o, más bien, prácticamente imposible) encontrarlos.

En el intento de responder a la pregunta ¿Cuántos primos hay?, nos hemos metido de lleno, y de forma natural, a trabajar con primos grandes. Podemos entonces preguntarnos: ¿Por qué buscar primos grandes? En la segunda parte de estas notas trataré de dar respuesta a esta pregunta y a ella remito al lector interesado.

Bibliografía

[1] Bach, E., Shallit, J.: *Algorithmic Number Theory, Vol. 1*, The MIT Press, Cambridge (1996).

[2] Bombieri, E.: *Problems of the Millennium: The Riemann Hypothesis,* en `http://www.claymath.org`.

[3] Bressoud, D., Wagon, S.: *A course in computational number theory,* Key College Publishing, Emeryville (2000).

[4] Caldwell, C.: `http://www.utm.edu/research/primes`.

[5] Crandall, R., Pomerance, C.: *Prime numbers. A computational perspective,* Springer-Verlag, New York (2001).

[6] Gaylord, R. J., Kamin, S. N., Wellin, P. R.: *An introduction to programming with Mathematica, 2nd Ed.,* Springer-Verlag, New York (1996).

[7] Good, I. J.: *The scientist speculates,* Heinemann & Basic Books, New York (1962).

[8] Good, I. J., Churchhouse, R. F.: *The Riemann hypothesis and pseudorandom features of the Möbius sequence,* Math. Comp. 22 (1968), 857-864.

[9] Gourdon, X.: `http://numbers.computation.free.fr/Constants/constants.html`.

[10] Hardy, G. H., Littlewood, J. E.: *Some problems of 'partitio numerorum'; III: on the expression of a number as a sum of primes,* Acta Math. 44 (1922), 1-70.

[11] Hardy, G. H., Wright, E. M.: *An introduction to the theory of numbers,* Fifth Ed., Oxford Univ. Press, Oxford (1979).

[12] López, F., Tena, J.: *Introducción a la teoría de los números primos,* Publicaciones de la Universidad de Valladolid (1990).

[13] Martin, M.: `http://http://www.znz.freesurf.fr`.

[14] Narkiewicz, W.: *The development of prime number theory,* Springer-Verlag, Berlin (2000).

[15] Nicely, T. R.: `http://www.trnicely.net`.

[16] Odlyzko, A. M., te Riele, H. J.: *Disproof of the Mertens conjecture,* J. Reine Angew. Math., 357 (1985), 138-160.

[17] Ribenboim, P.: *The New Book of Prime Number Records,* Springer-Verlag, New York (1996).

[18] Riesel, H.: *Prime numbers and computer methods for factorization, 2nd Ed.,* Birkhäuser, Boston (1994).

[19] Wagon, S.: *Where are the zeros of zeta of s,* Mathematical Intelligencer, 8 (1986), 57-62.

[20] Yan, S. Y.: *Number theory for computing,* Springer-Verlag, Berlin (2000).

[21] Zagier, D.: *The first 50 million prime numbers,* Mathematical Intelligencer 0, (1977), 7-19.

José Luis Gómez Pardo
Departamento de Álxebra
Universidade de Santiago
15782 Santiago de Compostela
correo electrónico: `pardo@usc.es`