TEORÍA ELEMENTAL DE NÚMEROS

DAVID M. BURTON, TRADUCIDO POR PAUL A. LOOMIS

3.2 La Criba de Eratóstenes

Dado un entero particular, ¿cómo podemos determinar si es primo o compuesto?, y en el último caso, ¿cómo podemos realmente encontrar un divisor no trivial? El enfoque más obvio consiste en dividir sucesivamente el entero en cuestión por cada de los números que le preceden; si ninguno de ellos (excepto 1) sirve como divisor, entonces el número debe ser primo. Aunque este método es muy simple describir, no puede considerarse útil en la práctica. Incluso si uno no se deja intimidar por cálculos grandes, la cantidad de tiempo y esfuerzo requerido puede ser prohibitiva.

Hay una propiedad de los números compuestos que nos permite reducir materialmente los cálculos requeridos - pero todavía el proceso sigue siendo duro. Si un entero $a > 1$ es compuesto, entonces se puede escribirlo como $a = bc$, en donde $1 < b < a$ y $1 < c < a$. Suponiendo que $b \leq c$, obtenemos $b^2 \leq bc = a$, y entonces $b \leq \sqrt{a}$. Como $b > 1$, el Teorema 3.2 asegura que b tiene por lo menos un factor primo p. Entonces $p \leq b \leq \sqrt{a}$; además, como $p|b$ y $b|a$, resulta que $p|a$. El punto es simplemente este: un número compuesto siempre poseerá un divisor primo p que satisface $p \leq \sqrt{a}$.

Al probar la primalidad de un entero particular $a > 1$, entonces es suficiente dividir a por los primos que no exceda $\sqrt{a}$ (suponiendo, por supuesto, la disponibilidad de una lista de los primos hasta $\sqrt{a}$). Esto se puede clarificar al considerar el entero $a = 509$. Ya que $22 < \sqrt{509} < 23$, solo necesitamos probar los primos que no son mayor que 22 como divisores posibles; es decir, los primos $2, 3, 5, 7, 11, 13, 17, 19$. Al dividir 509 por cada uno de estos, en su turno, encontramos que ninguno sirve como divisor de 509. La conclusión es que 509 debe ser un número primo.

Ejemplo 3.1. La técnica precedente provee un medio práctico para determinar la forma canónica de un entero, digamos $a = 2093$. Como $45 < \sqrt{2093} < 46$, es suficiente examinar los primos $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43$. Por prueba, el primero de estos para dividir a 2093 es 7, y $2093 = 7 \cdot 299$. Con respecto al entero 299, los siete primos menor que 18 (nota que $17 < \sqrt{299} < 18$) son $2, 3, 5, 7, 11, 13, 17$. El primer divisor primo de 299 es 13, y realizando la división requerida, obtenemos $299 = 13 \cdot 23$. Pero el propio 23 es primo, y entonces 2093 tiene exactamente tres factores primos, 7, 13, y 23:

$$2093 = 7 \cdot 11 \cdot 23$$

Otro matemático griego cuyo trabajo en la teoría de números queda significante es Eratóstenes de Cirene (276-194 a.C). Aunque la posteridad lo recuerda principalmente como el director de la mundialmente famosa biblioteca de Alejandría, estaba dotado en todas las ramas de saber, si no en primer lugar en alguna; en su época, lo apodaron "Beta" porque, según se decía, ocupaba al menos el segundo puesto en todos los campos. Quizás la hazaña más impresionante de Eratóstenes fue su medición precisa de la circunferencia de la Tierra mediante una aplicación simple de la geometría euclídeana.

Hemos visto que si un entero $a > 1$ no es divisible por ningún primo $p \leq \sqrt{a}$, entonces a es necesariamente un primo. Eratóstenes utilizó este hecho como base de una técnica inteligente, llamada la *Criba de Eratóstenes*, para encontrar todos los primos menor que un entero dado n. El esquema requiere anotar los enteros del 2 al n en su orden natural y luego eliminar sistemáticamente todos los números compuestos por tachar todos los multiples $2p, 3p, 4p, 5p, \ldots$ de los primos $p \leq \sqrt{n}$. Los enteros que quedan en la lista - los que no caen por la "criba" - son primos.

Para ver un ejemplo de como este funciona, supongamos que queremos hallar todos los primos que no exceden 100. Consideramos la sucesión de enteros consecutivos $2, 3, 4, \ldots, 100$. Reconociendo que 2 es un primo, comenzamos tachando todos los enteros pares de nuestra lista, excepto el 2. El primero de los enteros restantes es 3, que debe ser un primo. Nos quedamos con el 3, pero tachamos todos los múltiplos superiores de 3, de modo que $9, 15, 21, \ldots$ ahora están eliminados (los múltiplos pares habiendo sido eliminado en el paso anterior). El mínimo entero después de 3 que aún no ha sido eliminado es 5. No es divisible por 2 o 3 - de lo contrario hubiera sido tachado - por eso, también es primo. Todos múltiplos adecuadas de 5 siendo números compuestos, a continuación eliminamos $10, 15, 20, \ldots$ (uno de estos, por supuesto, ya eliminados), mientras mantenemos 5 sí mismo. El primer entero sobreviviente 7 es primo, como no es divisible por 2, 3, o 5, los únicos primos que lo preceden. Después de eliminar los múltiplos adecuadas de 7, el primo más grande menor que $\sqrt{10}$, todos los números compuestos en la sucesión $2, 3, 4, \ldots, 100$ han caído por la criba. Los enteros positivos que quedan, esto es, $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$, son todos los primos menor que 100.

El table siguiente representa el resultado de la criba completa.

	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~~	~~70~~
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~~

En este punto, al lector se le debe haber ocurrido una pregunta obvia. ¿Hay un número primo más grande, o continuan los primos para siempre? Se encuentra la respuesta en una demostración notablemente simple por Euclides en el Libro IX de sus *Elementos*. El argumento de Euclides es universalmente considerado como un modelo de elegancia matemática. En términos generales, dice así: dado cualquier lista finita de números primos, siempre se puede hallar un primo que no es en la lista; entonces, el número de primos es infinito. Los detalles reales aparecen a continuación.

Teorema 3.4. Euclides. Hay un número infinito de primos.

Demostración: La demostración de Euclides es por contradicción. Sean $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7, \ldots$ los primos en orden creciente, y supone que hay un último primo, llamado p_n. Ahora consideramos el entero positivo

$$P = p_1 p_2 \cdots p_n + 1$$

Como $P > 1$, podemos poner el Teorema 3.2 a trabajar otra vez y concluir que P es divisible por algún primo p. Pero $p_1, p_2, \ldots p_n$ son los únicos números primos, de modo que p debe igualar a uno de los $p_1, p_2, \ldots, p_n$. Al combinar la relación de divisibilidad $p|p_1 p_2 \cdots p_n$ con $p|P$, llegamos a $p|P - p_1 p_2 \cdots p_n$ o, equivalentemente, $p|1$. El único divisor positivo del entero 1 es el 1 mismo y, como $p > 1$, surge una contradicción. Por lo tanto, ninguna lista finita de primos es completa, y entonces el número de primos es infinito.

Para un primo p, definimos $p^{\#}$ como el producto de todos los primos menor o igual que p. Números de la forma $p^{\#}+1$ podrían denominarse *números euclidianos*, como aparecen en el esquema de Euclides para demostrar la infinitud de los primos.

Es interesante notar que en formar estos enteros, los primeros cinco, a saber,

$$\begin{aligned} 2^{\#} + 1 &= 2 + 1 = 3 \\ 3^{\#} + 1 &= 2 \cdot 3 + 1 = 7 \\ 5^{\#} + 1 &= 2 \cdot 3 \cdot 5 + 1 = 31 \\ 7^{\#} + 1 &= 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211 \\ 11^{\#} + 1 &= 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311 \end{aligned}$$

todos son números primos. Sin embargo,

$$\begin{aligned} 13\# + 1 &= 59 \cdot 509 \\ 17^{\#} + 1 &= 19 \cdot 97 \cdot 277 \\ 19^{\#} + 1 &= 347 \cdot 27953 \end{aligned}$$

no son primos. Una pregunta sin respuesta es que si hay infinitos primos p tales que $p^{\#} + 1$ también es primo. De hecho, ¿hay infinitos compuestos $p^{\#} + 1$?

En la actualidad, se han identificado 22 primos de la forma $p^{\#} + 1$. Los primeros corresponden a los valores $p = 2, 3, 5, 7, 11, 31, 379, 1019, 1021, 2657, 3229$. El vigésimo segundo ocurre cuando $p = 392113$ y consiste en 169966 dígitos. Fue encontrado en 2001.

El teorema de Euclides es demasiado importante para que estemos contentos con una sola demostración. Aquí hay una variación en el razonamiento: Formar la sucesión infinita de enteros positivos

$$\begin{aligned} n_1 &= 2 \\ n_2 &= n_1 + 1 \\ n_3 &= n_1 n_2 + 1 \\ n_4 &= n_1 n_2 n_3 + 1 \\ &\vdots \\ n_k &= n_1 n_2 \cdots n_{k-1} + 1 \\ &\vdots \end{aligned}$$

Como cada $n_k > 1$, cada de estos enteros es divisible por un primo. Pero no dos n_k pueden tener el mismo divisor primo. Para verlo, sea $d = \text{mcd}(n_i, n_k)$ y supongamos que $i < k$. Entonces d divide a n_i y entonces debe dividir a $n_1 n_2 \cdots n_{k-1}$. Como $d | n_k$, el Teorema 2.2 nos dice que $d | n_k - n_1 n_2 \cdots n_{k-1}$. La implicación es que $d = 1$, de modo que los enteros n_k $(k = 1, 2, \dots)$ son coprimos en pares. El punto que deseamos dejar claro es que hay tantos primos distintos como enteros n_k, es decir, infinitos.

Sea p_n denotar el enésima de los números primos en su orden natural. La demostración de Euclides muestra que la expresión $p_1 p_2 \cdots p_n + 1$ es divisible

por por lo menos un primo, Si hay varios tales divisores primos, entonces p_{n+1} no puede exceder el más pequeño de estos, de modo que $p_{n+1} \leq p_1 p_2 \cdots p_n + 1$ para $n \geq 1$. Otra manera de decir la misma cosa es que

$$p_n \leq p_1 p_2 \cdots p_{n-1} + 1 \qquad n \geq 2$$

Con una ligera modificación del razonamiento de Euclides, se puede mejorar esta desigualdad para obtener

$$p_n \leq p_1 p_2 \cdots p_{n-1} - 1 \qquad n \geq 3$$

Por ejemplo, cuando $n = 5$, nos dice que

$$11 = p_5 \leq 2 \cdot 3 \cdot 5 \cdot 7 - 1 = 209$$

Podemos ver que la estimación es bastante extravagante. Una limitación más estricta en el tamaño de p_n esta dado por *la Desigualdad de Bonse*, que declara que

$$p_n^2 < p_1 p_2 \cdots p_{n-1} \qquad n \geq 5$$

Esta desigualdad produce $p_5^2 < 210$, o $p_5 \leq 14$. Una estimación de tamaño algo mejor para p_5 proviene de la desigualdad

$$p_{2n} \leq p_2 p_3 \cdots p_n - 2 \qquad n \geq 3$$

Aquí obtenemos

$$p_5 < p_6 \leq p_2 p_3 - 2 = 3 \cdot 5 - 2 = 13$$

Para aproximar el tamaño de p_n de estas fórmulas, es necesario saber los valores de $p_1, p_2, \ldots, p_{n-1}$. Para una cota en que no se entran los primos anteriores, tenemos el siguiente teorema.

Teorema 3.5. Si p_n es el enésimo número primo, entonces $p_n \leq 2^{2^{n-1}}$.

Demostración: Procederemos por inducción en n, como la desigualdad afirmada claramente es cierta cuando $n = 1$. Como hipótesis de inducción, suponemos que $n > 1$ y que el resultado es cierto para todos los enteros hasta n. Entonces

$$\begin{aligned} p_{n+1} &\leq p_1 p_2 \cdots p_n + 1 \\ &\leq 2 \cdot 2^2 \cdots 2^{2^{n-1}} + 1 = 2^{1+2+2^2+\cdots+2^{n-1}} + 1 \end{aligned}$$

Recordando la identidad $1 + 2 + 2^2 + \cdots + 2^{n-1} = 2^n - 1$, obtenemos

$$p_{n+1} \leq 2^{2^n - 1}$$

Sin embargo, $1 \leq 2^{2^n - 1}$ para todo n, y entonces

$$\begin{aligned} p_{n+1} &\leq 2^{2^n - 1} + 2^{2^n - 1} \\ &= 2 \cdot 2^{2^n - 1} = 2^{2^n} \end{aligned}$$

que completa el paso de inducción, y el argumento.

Hay un corolario al Teorema 3.5 que es de interés.

Corolario. Para $n \geq 1$, hay por lo menos $n+1$ primos menor que 2^{2^n}.

Demostración: Del teorema, sabemos que todos $p_1, p_2, \ldots, p_{n+1}$ son menor que 2^{2^n}.

Podemos hacer considerablemente mejor de lo que se indica el Teorema 3.5. En 1845, Joseph Bertrand conjeturó que los números primos son bien distribuidos en el sentido que siempre hay por lo menos un primo entre $n \geq 2$ y $2n$. No podía establecer su conjetura, pero lo verificó para todo $n \leq 3.000.000$. (Una manera de lograr esto es considerar una sucesión de primos 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 5003, 9973, 19937, 39869, 79699, 159839, ... cada uno de los cuales es menor que dos veces el anterior.) Como requiere un verdadero esfuerzo para fundamentar esta conjetura famosa, contentémonos con decir que la primer demostración fue realizado por el matemático ruso P. L. Tchebycheff en 1852. Concediendo el resultado, no es difícil mostrar que

$$p_n < 2^n \qquad n \geq 2$$

y como consecuencia directa, $p_{n+1} < 2p_n$ para $n \geq 2$. En particular,

$$11 < p_5 < 2 \cdot p_4 = 14$$

Para ver que $p_n < 2^n$, arguamos por inducción en n. Claramente, $p_2 = 3 < 2^2$, de modo que la desigualdad aquí está cierta. Ahora supongamos que la desigualdad mantiene para un entero n, de donde $p_n < 2^n$. Al invocar la conjetura de Bertrand, existe un número primo que satisface $2^n < p < 2^{n+1}$; es decir, $p_n < p$. Esto inmediatamente conduce a la conclusión que $p_{n+1} \leq p < 2^{n+1}$, que completa la inducción y la demostración.

Los primos de forma especial han sido de constante interés. Entre estos, los primos repunidades son sobresalientes por su simplicidad. Una *repituno* es en entero escrito (en notación decimal) como una cadena de 1s, como 11, 111, o 1111. Cada tal entero debe tener la forma $(10^n - 1)/9$. Utilizamos el símbolo R_n para denotar la repituno que consiste en n 1s consecutivos. Una característica peculiar de estos números es la aparente escasez de primos entre ellos. Hasta ahora, solo R_2, R_{19}, R_{23}, R_{317}, R_{1031}, R_{49081}, R_{86453}, R_{109297}, y R_{270343} han sido identificado como primos (el último en 2007). Se sabe que los únicos primos repitunos posibles R_n para todo $n \leq 49000$ son los nueve números indicados. No se han conjeturado sobre la existencia de otros. Para que una repituno R_n sea primo, el subíndice debe ser primo; que esto no es una condición suficiente está demostrado por

$$R_5 = 11111 = 41 \cdot 271 \qquad R_7 = 1111111 = 239 \cdot 4649$$

PROBLEMAS 3.2

1. Determinar si el entero 701 es primo probando todos los primos $p \leq \sqrt{701}$ como divisores posibles. Hacer lo mismo para el entero 1009.

2. Empleando la criba de Eratóstenes, obtener todos los primos entre 100 y 200.

3. Dado que $p \nmid n$ para todos los primos $p \leq \sqrt[3]{n}$, demostrar que $n > 1$ o es un primo o es producto de dos primos.
[Consejo: Suponer lo contrario que n contiene por lo menos tres factores primos.]

4. Establecer los siguientes hechos:
a) $\sqrt{p}$ es irracional para cualquier primo p.
b) Si a es un entero positivo y $\sqrt[n]{a}$ es racional, entonces $\sqrt[n]{a}$ debe ser un entero.
c) Para $n \geq 2$, $\sqrt[n]{n}$ es irracional.
[Consejo: Utilizar el hecho que $2^n > n$.]

5. Demostrar que cualquier entero compuesto de tres dígitos debe tener un factor primo menor o igual que 31.

6. Completar los detalles que faltan en esta boceta de una demostración de la infinitud de primos: Supongamos que hay solo finitos primos, digamos $p_1, p_2, \ldots, p_n$. Sea A el producto de cualquier r de estos primos y poner $B = p_1 p_2 \cdots p_n / A$. Entonces cada p_k divide a o A o B, pero no ambos. Como $A + B > 1$, $A + B$ tiene un divisor primo distinto de cualquier de los p_k, que es una contradicción.

7. Modificar la demostración de Euclides suponiendo la existencia de un primo más grande p y utilizando el entero $N = p! + 1$ para llegar a una contradicción.

8. Dar otra demostración de la infinitud de los primos suponiendo que solo hay finitos primos, digamos $p_1, p_2, \ldots, p_n$ y utilizando el siguiente entero para llegar a una contradicción:

$$N = p_2 p_3 \cdots p_n + p_1 p_3 \cdots p_n + \cdots + p_1 p_\cdot \cdot p_{n-1}$$

9. a) Demostrar que si $n > 2$, entonces existe un primo p que satisface $n < p < n!$.
[Consejo: Si $n! - 1$ no es primo, entonces se tiene un divisor primo p; y $p \leq n$ implica $p | n!$, que conduce a una contradicción.]
b) Para $n > 1$, demostrar que cada divisor primo de $n! + 1$ es un entero mayor que n.

10. Sea q_n el mínimo primo que es estrictamente mayor que $P_n = p_1 p_2 \cdots p_n + 1$. Se ha conjeturado que la diferencia $q_n - (p_1 p_2 \cdots p_n)$ siempre es primo. Confirmar esto para los primero cinco valores de n.

11. Si p_n denota el enésima número primo, poner $d_n = p_{n+1} - p_n$. Una pregunta abierta es si la ecuación tiene infinitas soluciones. Dar cinco soluciones.

12. Suponiendo que p_n es el enésima número primo, establecer cada uno de los siguientes declaraciones.

a) $p_n > 2n - 1$ para $n \geq 5$.
b) Ninguno de los enteros $P_n = p_1 p_2 \cdots p_n + 1$ es un cuadrado perfector.
[Consejo: Todo P_n es de la forma $4k + 3$ para $n > 1$.]
c) La suma

$$\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n}$$

nunca es entero.

13. Para los repitunos R_n, verificar los siguientes afirmaciones:
a) Si $n|m$, entonces $R_n|R_m$.
[Consejo: Si $m = kn$, considerar la identidad

$$x^m - 1 = (x^n - 1)(x^{(k-1)m} + x^{(k-2)m} + \cdots + x + 1.]$$

b) Si $d|R_n$ y $d|R_m$, entonces $d_R n + m$.
[Consejo: Demostrar que $R_{m+n} = R_n 10^m + R_m$.]
c) Si $\text{mcd}(n, m) = 1$, entonces $\text{mcd}(R_n, R_m) = 1$.

14. Utilizar el problema anterior para obtener los factors primos de la repituno R_{10}.