TEORÍA ELEMENTAL DE NÚMEROS

DAVID M. BURTON, TRADUCIDO POR PAUL A. LOOMIS

3.1 El Teorema Fundamental de Aritmética

Esencial para todo lo discutido aquí - y, en realidad, a cada aspecto de la teoría de números - es la noción de número primo. Hemos observado anteriormente que cualquier entero $a > 1$ es divisible por ± 1 y $\pm a$; si estos agotan los divisores de a, se dice que es un número primo. En la Definición 3.1, decimos esto de manera algo diferente.

Definición 3.1. Se dice que un entero $p > 1$ es un *número primo*, o simplemente un *primo*, si sus únicos divisores positivos son 1 y p. Un entero mayor que 1 que no es primo es denotado *compuesto*.

Entre los primeros 10 enteros positivos, $2, 3, 5, 7$ son primos y $4, 6, 8, 9, 10$ son números compuestos. Nota que el entero 2 es el único primo par, y según nuestra definición el entero 1 juega un papel especial, siendo ni primo ni compuesto.

En el resto de este libro, se reservan las letras p y q, en la medida de lo posible, para primos.

La Proposición 14 del Libro IX de los *Elementos* de Euclides encarna el resultado que después fue conocido como el Teorema Fundamental de Aritmética; es decir, que cada entero mayor que 1 se puede representar como producto de primos en una y solo una manera. Para citar la proposición misma, "Si un número sea el menor que se mide por números primos, entonces no se medirá por ningún otro primo excepto aquellos que originalmente lo midieron." Como cada número $a > 1$ es o primo o, por el Teorema Fundamental, se puede descomponer en factores primos únicos y no más, los primos sirven como bloques de construcción de los cuales se pueden construir todos los demás números. En consecuencia, los números primos han intrigado a los matemáticos a través de los siglos, y aunque se han demostrado una serie de teoremas notables relacionados con su distribución en la sucesión de enteros positivos, aún más notable es lo que queda no demostrado. Las preguntas abiertas se pueden contar entre los problemas no resueltos sobresalientes en todas las matemáticas.

Para empezar en una manera más simple, observamos que el primo 3 divide al entero 36, en donde se puede escribir 36 como cualquier de los productos

$$6 \cdot 6 = 9 \cdot 4 = 12 \cdot 3 = 18 \cdot 2$$

En cada instancia, 3 divide a por lo menos uno de los factores involucrado en el producto. Es típico de la situación general, el resultado preciso siendo el Teorema 3.1.

Teorema 3.1. Si p es primo y $p|ab$, entonces $p|a$ o $p|b$.

Demostración: Si $p|a$, entonces no es necesario ir más lejos, así que supongamos $p \nmid a$. Como los únicos divisores positivos de p son 1 y el propio p, esto implica que $\text{mcd}(p, a) = 1$. (En general, $\text{mcd}(p, a) = p$ o $\text{mcd}(p, a) = 1$, según si $p|a$ o $p \nmid a$.) Entonces, citando el Lema de Euclides, obtenemos $p|b$.

Este teorema se extiende fácilmente a los productos de más que dos términos.

Corolario 1. Si p es un primo y $p|a_1a_2 \cdots a_n$, entonces $p|a_k$ por algún k, en donde $1 \leq k \leq n$.

Demostración: Procedemos por inducción en n, el número de factores. Cuando $n = 1$, la conclusión expresada obviamente es válida; mientras cuando $n = 2$, el resultado es el contenido del Teorema 3.1. Supongamos, como la hipótesis de inducción, que $n > 2$ y que siempre que p divide a un producto de menos que n factores, entonces n divide a unos de los factores. Ahora $p|a_1a_2 \cdots a_n$. Del Teorema 3.1, o $p|a_n$ o $p|a_1a_2 \cdots a_{n-1}$. Si $p|a_n$, entonces hemos terminado. En lo que respecta al caso en donde $p|a_1a_2 \cdots a_{n-1}$, la hipótesis de inducción asegura que $p|a_k$ por algún elección de k, en donde $1 \leq k \leq n - 1$. En cualquier caso, p divide a unos de los enteros $a_1, a_2, \ldots, a_n$.

Corolario 2. Si $p, q_1, q_2, \ldots, q_n$ todos son primos y $p|q_1q_2 \cdots q_n$, entonces $p = q_k$ por algún k, en donde $1 \leq k \leq n$.

Demostración: Por el Corolario 1, sabemos que $p|q_k$ por algún k, con $1 \leq k \leq n$. Como es primo, q_k no es divisible por ningún entero positivo excepto que 1 y q_k sí mismo. Como $p > 1$, nos vemos obligado a concluir que $p = q_k$.

Con esta preparación fuera del camino, llegamos a unos de las piedras angulares de nuestro desarrollo, el Teorema Fundamental de Aritmética. Como indicamos antes, este teorema afirma que cada entero mayor que 1 se puede factorizar en primos en esencialmente solo una manera; la ambigüedad lingüística *esencialmente* significa que $2 \cdot 3 \cdot 2$ no se considera como factorización distinta de 12 de la de $2 \cdot 2 \cdot 3$. Declaramos esto precisamente en el Teorema 3.2

Teorema 3.2. Teorema Fundamental de Aritmética. Cada entero positivo $n > 1$ es o un primo o un producto de primos; esta representación es única, aparte del orden en que ocurren los factores.

Demostración: O n es primo o n es compuesto; en el primer caso, no hay nada más que demostrar. Si n es compuesta, entonces existe un entero d que satisface $d|n$ y $1 < d < n$. Entre todos tales enteros d, elegir p_1 para ser el más pequeño (esto es posible por el Principio de Buen Orden). Entonces p_1 debe ser un número primo. Si no, también tendría un divisor q con $1 < q < p_1$; pero luego $q|p_1$ y $p_1|n$ implican que $q|n$, lo que contradice la elección de p_1 como el divisor mínimo positivo, no 1, de n.

Entonces podemos escribir $n = p_1n_1$, en donde p_1 es primo y $1 < n_1 < n$. Si sucede que n_1 es primo, tenemos nuestra representación. En el caso contrario, se repite el argumento para producer un segundo número primo p_2 tal que $n_1 = p_2n_2$; es decir,

$$n = p_1p_2n_2 \qquad 1 < n_2 < n_1$$

Si n_2 es primo, no es necesario ir más lejos. En otro caso, escribimos $n_2 = p_3n_3$, con p_3 primo:

$$n = p_1p_2p_3n_2 \qquad 1 < n_3 < n_2$$

La sucesión decreciente

$$n > n_1 > n_2 > \cdots 1$$

no puede continuar indefinidamente, de modo que después de un número finito de pasos n_{k-1} es un primo, digamos, p_k. Esto conduce a la factorización prima

$$n = p_1p_2 \cdots p_k$$

Para establecer la segunda parte de la demostración - la unicidad de la factorización prima - supongamos que se puede representar el entero n en dos maneras; digamos,

$$n = p_1p_2 \cdots p_r = q_1q_2 \cdots q_s \qquad r \leq s$$

en donde p_i y q_j todos son primos, escrito en magnitud creciente de modo que

$$p_1 \leq p_2 \leq \cdots \leq p_r \qquad q_1 \leq q_2 \leq \cdots \leq q_s$$

Como $p_1|q_1q_2 \cdots q_s$, el Corolario 2 de la Teorema 3.1 nos dice que $p_1 = q_k$ por algún k; pero entonces $p_1 \geq q_1$. Razonamiento similar da $q_1 \geq p_1$; entonces $p_1 = q_1$. Podemos cancelar este factor común y obtener

$$p_2p_3 \cdots p_r = q_2q_3 \cdots q_s$$

Ahora repetir el proceso para obtener $p_2 = q_2$ y, en su turno,

$$p_3p_4 \cdots p_r = q_3q_4 \cdots q_s$$

Continuar de esta manera. Si se mantuviera la desigualdad $r < s$, entonces eventualmente llegaríamos a

$$1 = q_{r+1}q_{r+2} \cdots q_s$$

lo que es absurdo, como cada $q_j > 1$. Entonces, $r = s$ y

$$p_1 = q_1 \qquad p_2 = q_2, \ldots, p_r = q_r$$

lo que hace las dos factorizaciones iguales. Ahora la demostración está completa.

Por supuesto, varios primos que aparecen en la factorización de un entero positivo dado pueden repetirse, como es el caso con $360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$.

Al coleccionar primos iguales y reemplazarlos por un solo factor, podemos reformular el Teorema 3.2 como un corolario.

Corolario. Todo entero positivo $n > 1$ puede ser escrito de manera única en la *forma canonica*

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

en donde, para $i = 1, 2, \cdot, r$, cada k_i es entero positivo y cada p_i es primo, con $p_1 < p_2 < \cdots p_r$.

Para ilustrar, la forma canonica del entero 360 es $360 = 2^3 \cdot 3^2 \cdot 5$. Como ejemplos adicionales citamos

$$4725 = 3^3 \cdot 5^2 \cdot 7 \qquad \text{y} \qquad 17460 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2$$

Las factorizaciones primas proveen otro modo de calcular los máximos comunes divisores. Suponer que $p_1, p_2, \ldots, p_n$ son los primos distintos que dividen o a o b. Permitiendo exponentes de cero, podemos escribir

$$a = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}, \qquad b = p_1^{j_1} p_2^{j_2} \cdots p_n^{j_n}$$

Entonces

$$\text{mcd}(a, b) = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$$

en donde $r_i = \min(k_i, j_i)$, el mínimo de los dos exponentes asociados con p_i en las dos representaciones. En el caso $a = 4725$ y $b = 17460$, tendríamos

$$4725 = 2^0 \cdot 3^3 \cdot 5^2 \cdot 7, \qquad 17460 = 2^2 \cdot 3^2 \cdot 5 \cdot 7^2$$

y entonces

$$\text{mcd}(4735, 17460) = 2^0 \cdot 3^2 \cdot 5 \cdot 7 = 315$$

Este es un momento oportuno para insertar un resultado famoso de Pitágoras. Las matemáticas como ciencia empezó con Pitágoras (569-500 a.C.) y mucho del contenido de los *Elementos* de Euclides se debe a Pitágoras y su escuela. Los pitagóricos merecen el credito por ser los primeros en clasificar los números en pares y impares, primos y compuestos.

Teorema 3.3. Pitágoras. El número $\sqrt{2}$ es irracional.

Demostración: Supongamos, al contrario, que $\sqrt{2}$ es un número racional, digamos $\sqrt{2} = a/b$, en donde a y b son enteros con $\text{mcd}(a, b) = 1$. Elevando ambos al cuadrado, obtenemos $a^2 = 2b^2$, de modo que $b|a^2$. Si $b > 1$, entonces el Teorema Fundamental de Aritmética garantiza la existencia de un primo p tal que $p|b$. Resulta que $p|a^2$ y, por el Teorema 3.1, que $p|a$; entonces $\text{mcd}(a, b) \geq p$. Por lo tanto, llegamos a una contradicción, salvo que $b = 1$. Pero si esto sucede, entonces $a^2 = 2$, lo que es imposible (suponemos que el lector está dispuesto a conceder

que no hay entero que se puede multiplicar por si mismo para obtener 2). Nuestra suposición que $\sqrt{2}$ es un número racional es insostenible, y entonces $\sqrt{2}$ debe ser irracional.

Hay una variación interesante de la demostración del Teorema 3.3 Si $\sqrt{2} = a/b$ con $\text{mcd}(a, b) = 1$, deben existir enteros r y s que satisfacen $ar + bs = 1$. Como resultado,

$$\sqrt{2} = \sqrt{2}(ar + bs) = (\sqrt{2}a)r + (\sqrt{2}b)s = 2br + as$$

Esta representación de $\sqrt{2}$ nos conduce a concluir que $\sqrt{2}$ es un entero, una imposibilidad obvia.

PROBLEMAS 3.1

1. Se han conjeturado que hay infinitos primos de la forma $n^2 - 2$. Exhibir cinco de estos primos

2. Dar un ejemplo para mostrar que la siguiente conjetura no es cierta: Cada entero positivo puede ser escrito en la forma $p + a^2$, en donde o p es un primo o 1, y $a \geq 0$.

3. Demostrar cada una de las siguientes afirmaciones:
a) Cualquier primo de la forma $3n + 1$ también es de la forma $6m + 1$.
b) Cada entero de la forma $3n + 2$ tiene un factor primo de esta forma.
c) El único primo de la forma $n^3 - 1$ es 7.
[Consejo: Escribir $n^3 - 1$ como $(n - 1)(n^2 + n + 1)$.]
d) El único primo para que $3p + 1$ es un cuadrado perfecto es $p = 5$.
e) El único primo de la forma $n^2 - 4$ es 5.

4. Si $p \geq 5$ es un número primo, demostrar que $p^2 + 2$ es compuesto.
[Consejo: p toma una de las formas $6k + 1$ o $6k + 5$.]

5. a) Dado que p es primo y $p|a^n$, demostrar que $p^n|a^n$.
b) Si $\text{mcd}(a, b) = p$, un primo, ¿cuáles son los valores posibles de $\text{mcd}(a^2, b^2)$, $\text{mcd}(a^2, b)$, y $\text{mcd}(a^3, b^2)$?

6. Establecer cada uno de las siguientes declaraciones:
a) Todo entero de la forma $n^4 + 4$, con $n > 1$, es compuesto.
[Consejo: Escribir $n^4 + 4$ como producto de dos factores cuadráticas.
b) Si $n > 4$ es compuesto, entonces n divide a $(n - 1)!$.
c) Cualquier entero de la forma $8^n + 1$ en donde $n \geq 1$, es compuesto.
[Consejo: $2^n + 1|2^{3n} + 1$.]
d) Cada entero $n > 11$ puede ser escrito como la suma de dos números compuestos.
[Consejo: Si n es par, digamos $n = 2k$, entonces $n - 6 = 2(k - 3)$; para n impar,

considerar el entero $n - 9$.]

7. Hallar todos los números primos que dividen a 50!.

8. Si $p \geq q \geq 5$ y p y q ambos son primos, demostrar que $24|p^2 - q^2$.

9. a) Una pregunta sin respuesta es si hay infinitos primos que son 1 más con una potencia de 2, como $5 = 2^2 + 1$. Hallar dos más de estos primos.
b) Una conjetura más general es que existen infinitos primos de la forma $n^2 + 1$, por ejemplo, $257 = 16^2 + 1$. Exhibir cinco primos más de este tipo.

10. Si $p \neq 5$ es un primo impar, demostrar que o $p^2 - 1$ o $p^2 + 1$ es divisible por 10.

11. Otra conjetura no demostrada es que hay infinitos primos que son 1 menos que una potencia de 2, como $3 = 2^2 - 1$.
a) Hallar cuatro más de estos primos.
b) Si $p = 2^k - 1$ es primo, demostrar que k es un entero impar, excepto cuando $k = 2$.
[Consejo: $3|4^n - 1$ para todo $n \geq 1$.]

12. Hallar la factorización prima de los enteros 1234, 10140, y 36000.

13. Si $n > 1$ es un entero no de la forma $6k + 3$, demostrar que $n^2 + 2^n$ es compuesto.
[Consejo: Mostrar que o 2 o 3 divide a $n^2 + 2^n$.]

14. Se he conjeturado que cada entero par puede ser escrito como la diferencia de dos primos consecutivos de infinitas maneras. Por ejemplo,

$$6 = 29 - 23 = 137 - 131 = 599 - 593 = 1019 - 1013 = \ldots$$

Expresar el entero 10 como la diferencia de dos primos consecutivos de 15 maneras.

15. Demostrar que un entero positivo $a > 1$ es un cuadrado si y solo si todos los exponentes de los primos en la forma canonica de a son enteros pares.

16. Un entero se dice que es *libre de cuadrados* si no es divisible por el cuadrado de ningún entero mayor que 1. Demostrar lo siguiente:
a) Un entero $n > 1$ es libre de cuadrados si y solo si se puede factorizar n como producto de primos distintos.
b) Todo entero $n > 1$ es el producto de un entero libre de cuadrados y un cuadrado perfecto.
[Consejo: Si $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ es la factorización canónica de n, entonces escribir $k_i = 2q_i + r_i$ en donde $r_i = 0$ o 1 según k_i sea par o impar.]

17. Verificar que todo entero n se puede expresar como $n = 2^k m$, en donde $k \geq 0$ y m es un entero impar.

18. La evidencia numérica hace que sea plausible que hay infinitos primos p tales que $p + 50$ también es primo. Listar 15 de estos primos.

19. Un entero positivo se llama *lleno de cuadrados*, o *poderoso* si $p^2|n$ para cada factor primo p de n (hay 992 números llenos de cuadrados menor que 250.000). Si n es lleno de cuadrados, demostrar que se puede escribirlo en la forma $n = a^2b^3$, con a y b enteros positivos.