TEORÍA ELEMENTAL DE NÚMEROS

DAVID M. BURTON, TRADUCIDO POR PAUL A. LOOMIS

7.2 La función ϕ de Euler

Este capítulo trata de esta parte de la teoría que surge del resultado conocido como la Generalización de Euler del Teorema de Fermat. En una palabra, Euler extendió el teorema de Fermat, que se refiere a las congruencias con módulos primos, a módulos arbitrarios. Mientras lo hacía, introdujo una función número-teorica importante, descrita en la Definición 7.1.

Definición 7.1. Para $n \geq 1$, sea $\phi(n)$ denotar el número de enteros positivos que no exceden n y que sean coprimos con n.

Como ilustración de la definición, encontramos que $\phi(30) = 8$; como, entre los enteros positivos que no exceden 30, hay ocho que son coprimos con 39; específicamente,

$$1, 7, 11, 13, 17, 19, 23, 29$$

De manera similar, para los primeros enteros positivos, el lector puede comprobar que

$$\phi(1) = 1, \phi(2) = 1, \phi(3) = 2, \phi(4) = 2, \phi(5) = 4,$$
$$\phi(6) = 2, \phi(7) = 6, \ldots$$

Nota que $\phi(1) = 1$, como $\text{mcd}(1, 1) = 1$. En el evento $n > 1$, entonces $\text{mcd}(n, n) = n \neq 1$, de modo que se puede caracterizar $\phi(n)$ como el número de enteros menor que n y coprimo a n. La función $\phi(n)$ generalmente se llama la *función phi de Euler* (a veces, el *indicador* o *tociente*) por su creador; sin embargo, la notación funcional $\phi(n)$ se atribuye a Gauss.

Si n es un número primo, entonces cada entero menor que n es coprimo con ello; de donde $\phi(n) = n - 1$. Por otro lado, si $n > 1$ es compuesto, entonces n tiene un divisor d tal que $1 < d < n$. Resulta que hay por lo menos dos enteros entre $1, 2, 3, \ldots, n$ que no son coprimos con n; a saber, d y n mismo. Como resultado, $\phi(n) \leq n - 2$. Esto demuestre que para $n > 1$,

$$\phi(n) = n - 1 \qquad \text{si y solo si } n \text{ es primo}$$

Theorem 7.1. Si p es un primo y $k > 0$, entonces

$$\phi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right)$$

Demostración. Claramente, $\text{mcd}(n, p^k) = 1$ si y solo si $p \nmid n$. Hay p^{k-1} enteros entre 1 y p^k divisibles por p; a saber,

$$p, 2p, 3p, \ldots, (p^{k-1})p$$

Entonces, el conjunto $\{1, 2, \ldots, p^k\}$ contiene exactamente $p^k - p^{k-1}$ enteros que son coprimos con p^k, de modo que por la definición de la función phi, $\phi(p^k) = p^k - p^{k-1}$.

Por ejemplo, tenemos

$$\phi(9) = \phi(3^2) = 3^2 - 3 = 6$$

los seis enteros menor de y coprimo con 9 siendo $1, 2, 4, 5, 7, 8$. Para dar una segunda ilustración, hay 8 enteros que son menor que 16 y coprimo con ello; son $1, 3, 5, 7, 9, 11, 13, 15$. El Teorema 7.1 produce el mismo conteo:

$$\phi(16) = \phi(2^4) = 2^4 - 2^3 = 16 - 8 = 8$$

Ahora sabemos como evaluar la función phi para potencias de primos, y nuestro es obtener una fórmula para $\phi(n)$ basada en la factorización de n como un producto de primos. El eslabón perdido en la cadena es obvio: demostrar que ϕ es una función multiplicativa. Allanamos el camino con un lema fácil.

Lema. Dado enteros a, b, c, $\text{mcd}(a, bc) = 1$ si y solo si $\text{mcd}(a, b) = 1$ y $\text{mcd}(a, c) = 1$.

Demostración. Primero supongamos que $\text{mcd}(a, bc) = 1$, y pongamos $d = \text{mcd}(a, b)$. Entonces $d|a$ y $d|b$, de donde $d|a$ y $d|bc$. Esto implica que $\text{mcd}(a, bc) \geq d$, lo que obliga $d = 1$. Un razonamiento similar da lugar a la afirmación $\text{mcd}(a, c) = 1$.

Para la otra dirección, tome $\text{mcd}(a, b) = 1 = \text{mcd}(a, c)$ y suponer que $\text{mcd}(a, bc) = d_1 > 1$. Entonces d_1 debe tener un divisor primo p. Como $d_1|bc$, resulta que $p|bc$; en consecuencia, $p|b$ o $p|c$. Si $p|b$, entonces (en virtud del hecho que $p|a$) tenemos $\text{mcd}(a, b) \geq p$, una contradicción. Del mismo modo, la condición $p|c$ lleva a la conclusión igualmente falsa que $\text{mcd}(a, c) = p$. Entonces, $d_1 = 1$ y el lema queda demostrado.

Teorema 7.2. La función ϕ es una función multiplicativa.

Demostración. Es requerido demostrar que $\phi(mn) = \phi(m)\phi(n)$, siempre que m y n no tienen factores en común. Como $\phi(1) = 1$, el resultado obviamente es cierto si o m o n es igual a 1. Ordena los números enteros del 1 al mn en m columnas

de n elementos cada una, de la siguiente manera:

$$\begin{array}{ccccccc} 1 & 2 & \dots & r & \dots & m \\ m+1 & m+2 & & m+r & & 2m \\ 2m+1 & 2m+2 & & 2m+r & & 3m \\ \vdots & \vdots & & \vdots & & \vdots \\ (n-1)m+1 & (n-1)m+2 & & (n-1)m+r & & nm \end{array}$$

Sabemos que $\phi(mn)$ es igual al número de entradas en esta matriz que son coprimos con mn; en virtud del lema, este es el mismo del número de enteros que son coprimos con ambos m y n.

Antes de entrar en los detalles, vale la pena comentar las tácticas a adoptar: como $\text{mcd}(qm + r, m) = \text{mcd}(r, m)$, los números en la columna r son coprimos con m si y solo si r mismo es coprimo con m. Por lo tanto, solo $\phi(m)$ columnas contienen enteros coprimos con m, y cada entrada en la columna será coprimo con m. El problema es mostrar que en cada una de estas $\phi(m)$ columnas hay exactamente $\phi(n)$ enteros que son coprimos con n; porque entonces por completo habría $\phi(m)\phi(n)$ números en la tabla que son coprimos con ambos m y n.

Ahora, las entradas en la columna r (en donde se supone que $\text{mcd}(r, m) = 1$) son

$$r, m + r, 2m + r, \dots, (n-1)m + r$$

Hay n enteros en esta sucesión y no hay dos que son congruentes módulo n. De hecho, si

$$km + r \equiv jm + r \pmod{n}$$

con $0 \leq k < j < n$, resultaría que $kn \equiv jm \pmod{n}$. Como $\text{mcd}(m, n) = 1$, podriamos cancelar m de ambos lados de la congruencia para llegar a la contradicción $k \equiv j \pmod{n}$. Entonces, los números en la columna r son congruentes módulo n a $0, 1, 2, \dots, n-1$ en algún orden. Pero si $s \equiv t \pmod{n}$, entonces $\text{mcd}(s, n) = 1$ si y solo si $\text{mcd}(t, n) = 1$. La implicación es que la columna r contiene tantos enteros coprimos con n como el conjunto $\{0, 1, 2, \dots, n-1\}$, a saber, $\phi(n)$ enteros. Por lo tanto, el número total de entradas en el matriz que son coprimos con ambos m y n es $\phi(m)\phi(n)$. Esto completa la demostración del teorema.

Con estos preliminares en la mano, ahora podemos demostrar el Teorema 7.3.

Teorema 7.3. Si el entero $n > 1$ tiene la factorización en primos $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, entonces

$$\begin{aligned} \phi(n) &= (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_r^{k_r} - p_r^{k_r-1}) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right) \end{aligned}$$

Demostración. Pretendemos utilizar la inducción en r, el número de factores primos distintos de n. Por el Teorema 7.1, el resultado es cierto para $r = 1$. Supongamos que es cierto para $r = i$. Como

$$\text{mcd}(p_1^{k_1} p_2^{k_2} \cdots p_i^{k_i}, p_{i+1}^{k_{i+1}}) = 1$$

la definición de una función multiplicativa da

$$\begin{aligned}\phi\left(\left(p_1^{k_1} p_2^{k_2} \cdots p_i^{k_i}\right) p_{i+1}^{k_{i+1}}\right) &= \phi\left(p_1^{k_1} \cdots p_i^{k_i}\right) \phi\left(p_{i+1}^{k_{i+1}}\right) \\ &= \phi\left(p_1^{k_1} \cdots p_i^{k_i}\right)\left(p_{i+1}^{k_{i+1}} - p_{i+1}^{k_{i+1}-1}\right)\end{aligned}$$

Invocando el hipótesis de inducción, el primer factor en el lado derecho se convierte en

$$\phi\left(p_1^{k_1} p_2^{k_2} \cdots p_i^{k_i}\right) = \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right) \cdots \left(p_i^{k_i} - p_i^{k_i-1}\right)$$

y esto sirve para completar el paso de inducción y con esto la demostración.

Ejemplo 7.1. Calculemos el valor $\phi(360)$, por ejemplo. La descomposición en potencias de primos de 360 es $2^3 \cdot 3^2 \cdot 5$, y el Teorema 7.3 nos dice que

$$\begin{aligned}\phi(360) &= 360\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) \\ &= 360 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 96\end{aligned}$$

El lector atento se habrá dado cuenta que, salvo $\phi(1)$ y $\phi(2)$, los valores de $\phi(n)$ en nuestros ejemplos siempre son pares. Esto no es un accidente, como muestra el siguiente teorema.

Teorema 7.4. Para $n > 2$, $\phi(n)$ es un entero par.

Demostración. Primero, supongamos que n es una potencia de 2, digamos $n = 2^k$, con $k \geq 2$. Por el Teorema 7.3,

$$\phi(n) = \phi(2^k) = 2^k\left(1 - \frac{1}{2}\right) = 2^{k-1}$$

un entero par. Si n no resulta ser una potencia de 2, entonces es divisible por un primo impar p; por lo tanto podemos escribir n como $n = p^k m$, en donde $k \geq 1$ y $\text{mcd}(p^k, m) = 1$. Explotando la naturaleza multiplicativa de la función ϕ, obtenemos

$$\phi(n) = \phi(p^k)\phi(m) = p^{k-1}(p-1)\phi(m)$$

lo cual nuevamente es par porque $2|p-1$.

Podemos establecer el teorema de Euclides sobre la infinitud de los primos en la siguiente manera nueva. Como antes, supongamos que solo hay un número finito de primos. Los llamamos $p_1, p_2, \ldots, p_r$ y consideramos el entero $n = p_1 p_2 \cdots p_r$. Arguamos que si $1 < a \leq n$, entonces $\text{mcd}(a, n) \neq 1$. El Teorema Fundamental

de Aritmética nos dice que a tiene un divisor primo q. Como $p_1, p_2, dots, p_r$ son los únicos primos, q debe ser uno de esos p_i, de donde $q|n$; en otras palabras, $\text{mcd}(a, n) \geq q$. La implicación de todo esto es que $\phi(n) = 1$, que claramente es imposible por el Teorema 7.4.

PROBLEMAS 7.2

1. Calcular $\phi(1001)$, $\phi(5040)$, y $\phi(36000)$.

2. Verificar que la igualdad $\phi(n) = \phi(n+1) = \phi(n+2)$ es cierto cuando $n = 5186$.

3. Demostrar que los enteros $m = 3^k \cdot 568$ y $n = 3^k \cdot 638$, en donde $k \geq 0$, satisfacen simultaneamente

$$\tau(m) = \tau(n), \qquad \sigma(m) = \sigma(n), \quad \text{y} \quad \phi(m) = \phi(n)$$

4. Establecer cada una de las siguientes afirmaciones:
(a) Si n es un entero impar, entonces $\phi(2n) = \phi(n)$.
(b) Si n es un entero par, entonces $\phi(2n) = 2\phi(n)$.
(c) $\phi(3n) = 3\phi(n)$ si y solo si $3|n$.
(d) $\phi(3n) = 2\phi(n)$ si y solo si $3 \nmid n$.
(e) $\phi(n) = n/2$ si y solo si $n = 2^k$ por algún $k \geq 1$.
[*Consejo:* Escribir $n = 2^k N$, en donde N es impar, y usar la condición $\phi(n) = n/2$ para demostrar que $N = 1$.]

5. Demostrar que la ecuación $\phi(n) = \phi(n + 2)$ es satisfecha por $n = 2(2p - 1)$ siempre cuando p y $2p - 1$ ambos son primos impares.

6. Demostrar que hay infinitos enteros n para que $\phi(n)$ es un cuadrado perfecto.
[*Consejo:* Considerar los enteros $n = 2^{2k+1}$ para $k = 1, 2, \ldots$.]

7. Verificar el siguiente:
(a) Para cualquier entero positivo n, $\frac{1}{2}\sqrt{n} \leq \phi(n) \leq n$.
[*Consejo:* Escribir $n = 2^{k_0} p_1^{k_1} \cdots p_r^{k_r}$, de modo que $\phi(n) = 2^{k_0-1} p_1^{k_1-1} \cdots p_r^{k_r-1}(p_1 - 1) \cdots (p_r - 1)$. Ahora usar las desigualdades $p - 1 > \sqrt{p}$ y $k - \frac{1}{2} \geq \frac{k}{2}$ para obtener $phi(n) \geq 2^{k_0-1} p_1^{k_1/2} \cdots p_r^{k_r/2}$.]
(b) Si el entero $n > 1$ tiene r factores primos distintos, entonces $\phi(n) \geq n/2^r$.
(c) Si $n > 1$ es un número compuesto, entonces $\phi(n) \leq n - \sqrt{n}$.
[*Consejo:* Sea p el divisor primo más pequeño de n, de modo que $p \leq \sqrt{n}$. Entonces $\phi(n) \leq n(1 - 1/p)$.

8. Demostrar que si el entero n tiene r factores primos distintos, entonces $2^r|\phi(n)$.

9. Demostrar el siguiente:
(a) Si n y $n + 2$ son un par de primos gemelos, entonces $\phi(n + 2) = \phi(n) + 2$;

esto también es cierto para $n = 12$, 14, y 20.
(b) Si p y $2p + 1$ ambos son primos impares, entonces $n = 4p$ satisface $\phi(n + 2) = \phi(n) + 2$.

10. Si cada primo que divide a n también divide a m, establecer que $\phi(nm) = n\phi(m)$; en particular, $\phi(n^2) = n\phi(n)$ para cada entero positivo n.

11. (a) Si $\phi(n)|n - 1$, demostrar que n es un entero libre de cuadrados.
[*Consejo:* Suponer que n tiene la factorización en primos $n = p_1^{k_1}p_2^{k_2} \cdots p_r^{k_r}$, en donde $k_1 \geq 2$. Entonces $p_1|\phi(n)$, de donde $p_1|n - 1$, que nos lleva a una contradicción.]
(b) Demostrar que si $n = 2^k$ o 2^k3^j, con k y j enteros positivos, entonces $\phi(n)|n$.

12. Si $n = p_1^{k_1}p_2^{k_2} \cdots p_r^{k_r}$, derivar las siguientes desigualdades:
(a) $\sigma(n)\phi(n) \geq n^2(1 - 1/p_1^2)(1 - 1/p_2^2) \cdots (1 - 1/p_r^2)$.
(b) $\tau(n)\phi(n) \geq n$.
[*Consejo:* Demostrar que $\tau(n)\phi(n) \geq 2^r \cdot n(1/2)^r$.]

13. Suponiendo que $d|n$, demostrar que $\phi(d)|\phi(n)$.
[*Consejo:* Trabajar con las factorizaciones en primos de d y n.]

14. Obtener las siguientes dos generalizaciones del Teorema 7.2:
(a) Para enteros positivos m y n, en donde $d = \text{mcd}(m, n)$,

$$\phi(m)\phi(n) = \phi(mn)\frac{\phi(d)}{d}$$

(b) Para enteros positivos m y n,

$$\phi(m)\phi(n) = \phi(\text{mcd}(m, n))\phi(\text{mcm}(m, n))$$

15. Demostrar lo siguiente:
(a) Hay infinitos enteros n para que $\phi(n) = n/3$.
[Consejo: Considerar $n = 2^k3^j$, en donde k y j son enteros positivos.]
(b) No hay enteros n para que $\phi(n) = n/4$.

16. Demostrar que la Conjectura de Goldbach implica que para cada entero par $2n$ existen enteros n_1 y n_2 con $\phi(n_1) + \phi(n_2) = 2n$.

17. Dado un entero positivo k, demostrar lo siguiente:
(a) Hay como máximo un número finito de enteros n para que $\phi(n) = k$.
(b) Si la ecuación $\phi(n) = k$ tiene una solución única, digamos $n = n_0$, entonces $4|n_0$.
Una conjetura famosa de R.D. Carmichael (1906) es que no hay un k para que la ecuación $\phi(n) = k$ tiene precisamente una solución; ha sido demostrado que cualquier contraejemplo debe exceder $10^{10000000}$.

18. Hallar todas las soluciones de $\phi(n) = 16$ y $\phi(n) = 24$.
[Consejo: Si $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ satisface $\phi(n) = k$, entonces $n = [k/\prod(p_i - 1)] \prod p_i$. Entonces se puede determinar los enteros $d_i = p_i = 1$ por las condiciones (1) $d_i | k$, (2) $d_i + 1$ es primo, y (3) $k/\prod d_i$ contiene ningún factor primo que no es en $\prod p_i$.]

19. (a) Demostrar que la ecuación $\phi(n) = 2p$, en donde p es un número primo y $2p + 1$ es compuesto, no es soluble.
(b) Demostrar que no hay solución a la ecuación $\phi(n) = 14$, y que 14 es el mínimo (positivo) entero par con esta propiedad.

20. Si p es un primo y $k \geq 2$, demostrar que $\phi(\phi(p^k)) = p^{k-2}\phi((p-1)^2)$.

21. Verificar que $\phi(n)\sigma(n)$ es un cuadrado perfecto cuando $n = 63457 = 23 \cdot 31 \cdot 89$.