Universidad Nacional Autónoma de México
Facultad de Ciencias

Recreaciones en Teoría de Números

Traducción capítulo 12 "Phi-Fo-Fum"

Por: Lorenzo Antonio Alvarado Cabrera

Algunos problemas aparentemente inocentes, llenos de trampas para los incautos, surgen en relación con la función Φ de Euler -el número de enteros menores o iguales a un número primos relativos con él. Si se le pidiera a uno que expresara un número relativamente simple, digamos 72, como un "producto de potencias de números primos", no se experimentaría ninguna dificultad particular. Descomponemos el número como un compuesto químico podría descomponerse en sus elementos esenciales. Los números primos son los elementos de la aritmética. Dividiendo 72 entre 2 y 3 tantas veces como sea posible, finalmente obtenemos $72 = 2^3 \cdot 3^2$. De manera similar $120 = 2^3 \cdot 3 \cdot 5$; y 60840, que obviamente contiene dos, tres y cinco, se resuelve en $2^3 \cdot 3^2 \cdot 5 \cdot 13^2$. Ya hemos señalado que la expresión general para cualquier entero positivo, N, como producto de las potencias primos es

$$N = {p_1}^{a_1} {p_2}^{a_2} \cdots {p_n}^{a_n} \qquad \text{(Formula A)}$$

En los libros de texto se muestra que el número de enteros menores que N y primos relativos con él, es decir, que no tienen ningún factor, excepto la unidad, en común con él viene dado por la expresión:

$$\Phi(N) = {p_1}^{a_1 - 1}(p_1 - 1){p_2}^{a_2 - 1}(p_2 - 1)\cdots {p_n}^{a_n - 1}(p_n - 1) \qquad \text{(Formula B)}$$

Se escribe $\Phi(n)$ y se lee "Phi de N". Por lo que:

$$\Phi(72) = \Phi(2^3 \cdot 3^2) = 2^2(2-1)3^1(3-1) = 4 \cdot 1 \cdot 3 \cdot 2 = 24$$
$$\Phi(120) = \Phi(2^3 \cdot 3 \cdot 5) = 2^2(2-1)3^0(3-1)5^0(5-1) = 4 \cdot 1 \cdot 1 \cdot 2 \cdot 1 \cdot 4 = 32$$
$$\begin{aligned}\Phi(60840) &= \Phi(2^3 \cdot 3^2 \cdot 5 \cdot 13^2) = 2^2(2-1) \cdot 3^1(3-1) \cdot 5^0(5-1) \cdot 13^1(13-1) \\ &= 4 \cdot \cdot 1 \cdot 3 \cdot 2 \cdot 1 \cdot 4 \cdot 13 \cdot 12 = 14976\end{aligned}$$

Cabe señalar que siempre que un número primo aparece solo en la primera potencia en la Fórmula A, no aparece en la Fórmula B ya que $p^0 = 1$. Debido a esta ausencia y también por muchas otras razones, la función Φ, presenta muchos problemas interesantes:

I. Encontrar *todas* las formas, si las hay, de expresar un número dado $b = \Phi(N)$ en la forma de la Fórmula B, y formular un practico procedimiento para hacerlo.
II. Obtener todos los números, N, a partir de estos valores de $\Phi(N)$.
III. Encontrar los números, b, que no se puedan poner de esta forma.

Ni siquiera es necesario saber que $\Phi(N)$ significa el número de enteros menos a N y primos relativos con él para resolver estos problemas. La fórmula A define un número N, y la fórmula B es una función que involucra a N. Solamente a partir de estas dos relaciones, los problemas pueden resolverse, pero se debe ejercitar un ingenio considerable para obtener todas las soluciones N para un número dado b, y establecer un conjunto de reglas prácticas para hacerlo.

En I, si $b = 6$, entonces $3^1(3-1)$ es una forma de expresarlo en la forma de la Formula B. Para $b = 8$, una solución es $2^3(2-1)$. Pero por más que lo intentemos, $b = 14$ no se puede expresar de esta manera. A primera vista tampoco parece haber una solución para el número 10, pero $10^0(11-1)$ cumple los requisitos.

Si $N = 1$, entonces por la Formula B,

$$\Phi(1) = 1^{1-1}(1-1) = 1^0 \cdot 0 = 0\,;$$

pero arbitrariamente, la unidad es primo relativo para todo entero *incluido él mismo*, de modo que $\Phi(1) = 1$ a pesar de la Fórmula B.

Expresar un número entero, b, en forma de la Fórmula B implica un valor correspondiente de N dado por la Fórmula A; por lo tanto, habrá tantos números, N, que satisfagan $\Phi(N) = b$, como formas de escribir b en la forma de la fórmula B. (Ya se ha señalado la unidad como excepción; ambos $\Phi(2)$ y $\Phi(1)$ son iguales a 1, pero para $b = 1$ se puede escribir de la forma, $2^0(2-1)$, entonces $\Phi(1) = 1$ por definición, no por la formula.) Esto plantea una pregunta fascinante: ¿Existe un número entero, N, cuyo $\Phi(N) = b$ es único, es decir, puede haber una sola solución, N, para algún $b = \Phi(N)$? Se ha demostrado que no existe tal número entero N menor que 10^{400}, y parece muy improbable que existan tales números enteros. (El número de gotas de agua en esta tierra es menor que 10^{30}.) Por debajo de este límite, siempre es posible encontrar al menos dos soluciones, N, para un $b = \Phi(N)$ dado. Por tanto, si un número impar, N, es una solución, $2N$ también es una solución; si un número par, $N = 2(2x+1)$, es una solución, entonces el número impar, $2x+1$, también es una solución. Por tanto, si existe un número, N, cuya $\Phi(N)$ es única, N debe ser un múltiplo de 4.

Es fácil ver que el número b no puede ser impar, excepto para $b = 1$ que tiene solución $2^0(2-1)$: La fórmula B muestra que hay al menos un factor $(p_1 - 1)$ de b y este factor es par si el primo es mayor que 2. Si $p_1 = 2$, entonces $p_1^{a_1 - 1}$ es par. Si $a_1 = 1$ tenemos la única excepción de número impar mencionada anteriormente.

La solución $3^1(3-1)$ es solo una de las cuatro formas de escribir el número 6 en la forma de la Fórmula B. Las otras tres son:

$$7^0(7-1) = 6$$
$$2^0(2-1)\cdot 7^0(7-1) = 6$$
$$2^0(2-1)\cdot 3^1(3-1) = 6$$

Para mostrar que todos son distintos, podemos escribir los valores respectivos de N, para estos valores de $\Phi(N)$, con la ayuda de las fórmulas A y B. Estos se enumeran en la Tabla 43.

TABLA 43

Valores de N tal que $\Phi(N) = 6$

N	Enteros menores a N primos relativos con el	Números enteros tales que $b = \Phi(N)$
$7^1 = 7$	1; 2; 3; 4; 5; 6	$7^0(7-1) = 6$
$3^2 = 9$	1; 2; 4; 5; 7; 8	$3^1(3-1) = 6$
$2\cdot 7 = 14$	1; 3; 5; 9; 11; 13	$2^0(2-1)\cdot 7^0(7-1) = 6$
$2\cdot 3^2 = 18$	1; 5; 7; 11; 13; 17	$2^0(2-1)\cdot 3^1(3-1) = 6$

Se podría trabajar al revés y mostrar que si 9, 7, 14 y 18 están escritos cada uno en la forma de Fórmula A, entonces el valor de $\Phi(N)$ dado por la Fórmula B será 6 en cada caso.

El factor aparentemente trivial $2^0(2-1)$ produce soluciones distintas cuando se combina con otros números como en las soluciones $N = 14$ y 18.

Para $\Phi(N) = 12$, se tienen seis soluciones:

$$13^0(13-1);\ 2^0(2-1)\cdot 13^0(13-1);\ 3^0(3-1)\cdot 7^0(7-1);$$
$$2^0(2-1)\cdot 3^0(3-1)\cdot 7^0(7-1);\ 2^1(2-1)\cdot 3^1(3-1);$$
$$2^1(2-1)\cdot 7^0(7-1)$$

Los valores correspondientes de N son 13, 26, 21, 42, 36 y 28, y cada uno de estos enteros tiene exactamente 12 enteros (incluida la unidad) menores que él, tales que no tiene ningún factor en común con ellos excepto la unidad.

Se requiere cuidado al resolver III; los hechos esenciales a menudo se nos escapan antes de que puedan ser capturados. Se dijo anteriormente que un número como $b = 14 = 2 \cdot 7$ no se puede poner en la forma $p_1^{a_1}(p_1 - 1)$ o un producto repetido de varias $p's$. Algunos otros valores imposibles se muestran en la Tabla 44.

TABLA 44

Valores imposibles de $\Phi(N)$

14	62	90	122	152
26	28	94	124	154
34	74	98	134	158
38	76	114	142	170
50	86	117	146	174

Si un número dado b es: (1) dos veces la potencia de un primo, $2p^a$, y (2) si p es mayor que 3, y (3) si $2p^a + 1$ es compuesto, entonces b no se puede poner en la forma de la Fórmula B. Ésta es solo una de las muchas formas imposibles. La formulación de algunos de ellos se deja al lector.

Será interesante y un poco estresante trabajar en un conjunto de reglas estrictas como se requiere en I y II. Después de que el lector haya hecho esto, tal vez desee resolver los siguientes cinco problemas, donde $b = \Phi(N)$ es dado y N se encuentra: $b = 1$; 72; 144; 480; $6600 = 2^3 \cdot 3 \cdot 5^2 \cdot 11$.

R. D. Carmichael tabuló una vez todos los números, N, para valores dados de b de 1 a 1000, que son soluciones de $\Phi(N) = b$. Como era de esperar, esto implicó una considerable cantidad de trabajo; por ejemplo, hay 47 valores de N para los cuales $\Phi(N) = 960$. Para b que no exceda de 50, el mayor número de soluciones se obtiene de 48, que tiene 11. Solo hay 21 valores posibles de b por debajo de 50 que tienen soluciones, por lo que el cálculo de una tabla de tales soluciones para b que no exceda este límite no debería ser muy laborioso y el lector puede querer probarlo.

* * *

Los enteros menores que un número dado N que son primos relativos con él pueden, por supuesto, ser primos o compuestos. Pero en unos pocos casos estos números son todos primos, es decir, para $N = 2$, 3, 4, 6, 8, 12, 18, 24 y 30. Por ejemplo, $\Phi(18) = 6$ enteros menores que 18 y primos relativos con él, que son 1, 5, 7, 11, 13, 17. Esta relación es notable porque estos nueve números son los únicos para los que se cumple; ningún entero mayor que 30 puede poseer esta propiedad.

*　　　*　　　*

Hay muchas relaciones llamativas que involucran la función Φ, algunas de ellas de gran complejidad. Uno bastante sorprendente afirma que la suma de los enteros menores que n y primos relativos con el es igual a $(n/2)[\Phi(n)]$, siempre que n exceda la unidad. Para probar esto, observemos que si I es un entero primo relativo con n, entonces $n-I$ es otro entero primo relativo con n. Pero hay $[\Phi(n)]/2$ pares de estos números enteros, por lo que la suma de todos estos números debe ser $n[\Phi(n)]/2$ o $(n/2)[\Phi(n)]$.

*　　　*　　　*

Las ecuaciones $k \cdot \Phi(x) = x+1$ y $k \cdot \Phi(x) = x-1$ son interesantes. Considere la primera forma. Cuando $k=1$, tenemos $\Phi(x) = x+1$, y como $\Phi(x)$ nunca puede exceder x, esto es imposible. Cuando $k=2$, tenemos $2 \cdot \Phi(x) = x+1$, que tiene la solución $x=3$, además de otras como se muestra en la Tabla 45. Cuando $k=3$, hay una solución $x=2$. Pero si hay otra solución para este valor de k debe ser el producto de al menos 32 factores primos distintos.

TABLA 45

Soluciones de $k \cdot \Phi(x) = x+1$

k	x	$x+1$	$\Phi(x)$
1	No hay soluciones	---	---
2	3	2^2	2^1
2	$3 \cdot 5$	2^4	2^3
2	$3 \cdot 5 \cdot 17$	2^8	2^7
2	$3 \cdot 5 \cdot 17 \cdot 257$	2^{16}	2^{15}
2	$3 \cdot 5 \cdot 17 \cdot 353 \cdot 929$	$2^{16} \cdot 11 \cdot 29$	$2^{17} \cdot 11 \cdot 29$
2	$3 \cdot 5 \cdot 17 \cdot 257 \cdot 929 \cdot 65537$	2^{32}	2^{31}
2	$3 \cdot 5 \cdot 17 \cdot 353 \cdot 929 \cdot 83623937$	$2^{36} \cdot 11^2 \cdot 29^2$	$2^{35} \cdot 11^2 \cdot 29^2$
2	Producto de al menos 7 primos distintos	---	---
3	2	3	1
3	Producto de al menos 32 primos distintos	---	---

Actualmente esta tabla se queda igual, no se han encontrado los valores faltantes

Ahora considera $k \cdot \Phi(x) = x - 1$. Cuando $k = 1$, cualquier primo x, es una solución de la ecuación, dado que $\Phi(x)$ siempre es igual a $x - 1$.

La fórmula B hace claramente evidente que cuando x es compuesto, $\Phi(x)$ debe diferir de x en más de la unidad; por tanto, no puede haber un valor compuesto de x que satisfaga $\Phi(x) = x - 1$.

Cuando k es mayor que 1, x debe, por supuesto, ser compuesto ya que, para un primo, $\Phi(x)$ es exactamente igual a $x - 1$. Pero si x es compuesto, debe ser el producto de al menos siete primos distintos. Sin embargo, no se conoce ninguna solución. Se sospecha que una solución para un número compuesto x es imposible, pero una prueba de esto implica dificultades del mismo orden que las del hecho hasta ahora no demostrado de que no hay números perfectos impares.

Cuando $k = 3$, una solución x debe contener nuevamente al menos 32 factores primos distintos. Estos hechos se resumen en la Tabla 46.

TABLA 46

Soluciones de $k \cdot \Phi(x) = x - 1$

k	x	$x-1$	$\Phi(x)$
1	Cualquier primo	$x-1$	$x-1$
2	Un producto de al menos 7 primos distintos; no se conocen soluciones	---	---
3	Un producto de al menos 32 primos distintos; no se conocen soluciones	---	---

*Este problema se llama “Lehmer's totient problem” y es un problema aún sin resolver, En 1988, Hagis demostró que, si 3 divide cualquier solución x, entonces $x > 10^{1937042}$ *