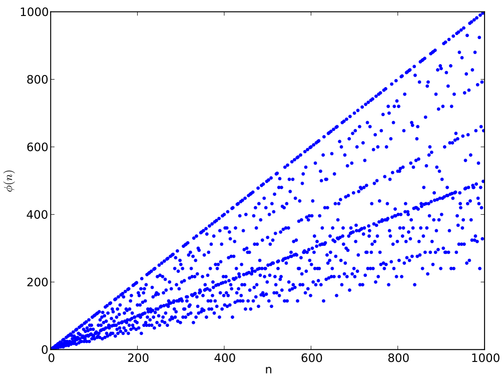
Función φ de Euler



Los primeros mil valores de $\varphi(n)$.

La **función φ de Euler** (también llamada **función indicatriz de Euler**) es una función importante en teoría de números. Si *n* es un número entero positivo, entonces φ(*n*) se define como el número de enteros positivos menores o iguales a *n* y coprimos con *n*, es decir, formalmente se puede definir como:

$$\varphi(m) = |\{n \in \mathbb{N} | n \leq m \wedge \operatorname{mcd}(m,n) = 1\}|$$

donde |·| significa la cantidad de números que cumplen la condición.

La función φ es importante principalmente porque proporciona el tamaño del grupo multiplicativo de enteros módulo n. Más precisamente, $\varphi(n)$ es el orden del grupo de unidades del anillo $\mathbb{Z}/n\mathbb{Z}$. En efecto, junto con el teorema de Lagrange de los posibles tamaños de subgrupos de un grupo, proporciona una demostración del teorema de Euler que dice que $a^{\varphi(n)} \equiv 1 \pmod{n}$ para todo *a* coprimo con *n*. La función φ juega también un papel clave en la definición del sistema de cifrado RSA.

1 Primeras propiedades y cálculo de la función

Se sigue de la definición que $\varphi(1) = 1$, pues el elemento (1) sólo puede ser coprimo consigo mismo. Para otros números se cumple que:

1. $\varphi(p) = p - 1$ si p es primo.
2. $\varphi(p^k) = (p-1)p^{k-1}$ si *p* es primo y *k* es un número natural. Se demuestra mediante inducción sobre *k*:
3. φ es una función multiplicativa: si *m* y *n* son primos entre sí, entonces $\varphi(mn) = \varphi(m)\varphi(n)$.

La primera propiedad se demuestra fácilmente, porque un número primo es coprimo con todos sus anteriores. Y, por tanto, existen *p*−1 elementos coprimos con *p*.

La segunda propiedad se demuestra por inducción, supongamos que *k* = 1. Entonces $\varphi(p^1) = \varphi(p) = p - 1$ por la propiedad 1, de manera que se puede escribir como $\varphi(p^1) = (p-1)p^{1-1}$. Se debe demostrar que se cumple para $\varphi(p^{k+1}) = (p-1)p^k$.

Reescribiendo la identidad, $(p-1)p^k = (p-1)p^{k-1}p$, luego $((p-1)p^{k-1})p = \varphi(p^k)p$. Como $\varphi(p^k)$ es la cantidad de números coprimos con p^k , si multiplicamos dicha cantidad por *p*, el número que es coprimo con los demás debe aumentar *p* veces, con lo que $\varphi(p^k)p = \varphi(p^{k+1}) = (p-1)p^k$.

Con esto, el valor de φ(*n*) puede calcularse empleando el teorema fundamental de la Aritmética: si

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

donde los *pj* son números primos distintos, entonces

$$\varphi(n) = (p_1 - 1)p_1^{k_1-1} \cdots (p_r - 1)p_r^{k_r-1}.$$

Esta última fórmula es un producto de Euler y a menudo se escribe como

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

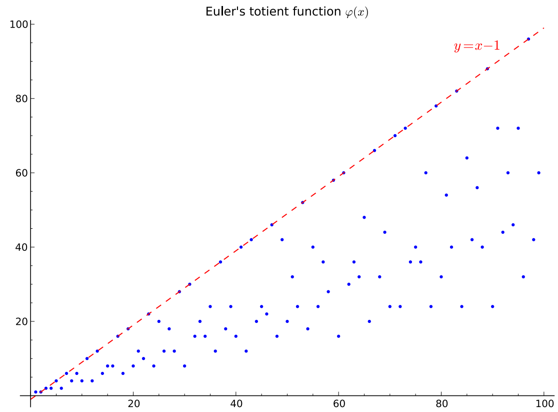
donde los *p* son los distintos primos que dividen a *n*.

1.1 Ejemplo de cálculo

$$\varphi(36) = \varphi\left(3^2 2^2\right) = 36\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{2}\right) = 36 \cdot \frac{2}{3} \cdot \frac{1}{2} = 12.$$

Se puede comprobar manualmente que los números coprimos con 36 (o sea, que no son divisibles por 2 ni por 3) son doce: 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, y 35.

2 Algunos valores



Representación gráfica de los 100 primeros valores. Nótese que el límite inferior marcado por la recta y = 4n/15 *no es el límite inferior de la función de manera global, sino para múltiplos de 30.*

Los 99 primeros valores de la función vienen escritos en la siguiente tabla, así como gráficamente.

3 Propiedades

- El valor de φ(*n*) es igual al orden del grupo de las unidades del anillo **Z**/*n***Z** (véase aritmética modular). Esto, junto con el teorema de Lagrange, proporciona una demostración del teorema de Euler.

- φ(*n*) también es igual al número de generadores del grupo cíclico *Cn* (y por ello también es igual al grado del polinomio ciclotómico Φ*n*). Como cada elemento de *Cn* genera un subgrupo cíclico y los subgrupos de *Cn* son de la forma *Cd* donde *d* divide a *n* (notación: *d*|*n*), se tiene que

$$\sum_{d|n} \varphi(d) = n$$

donde la suma es de todos los divisores positivos *d* de *n*.

De esta manera, se puede emplear la fórmula de inversión de Möbius para «invertir» esta suma y obtener otra fórmula para φ(*n*):

$$\varphi(n) = \sum_{d|n} d\mu(n/d)$$

donde μ es la usual función de Möbius definida sobre los enteros positivos.

- La siguiente fórmula es de una serie de Dirichlet que genera un grupo cíclico φ(*n*):

$$\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}$$

4 Véase también

- Teorema de Euler
- Función de Carmichael
- Función indicatriz de Jordan

5 Referencias

6 Enlaces externos

- Weisstein, Eric W. «Euler's Totient Function». En Weisstein, Eric W. *MathWorld* (en inglés). Wolfram Research.
- EulerPhifunction en PlanetMath

Wikilibros

- Wikilibros alberga un libro o manual sobre **Implementaciones de la función φ de Euler**.

7 Origen del texto y las imágenes, colaboradores y licencias

7.1 Texto

- **Función φ de Euler** *Fuente:* https://es.wikipedia.org/wiki/Funci%C3%B3n_%CF%86_de_Euler?oldid=90694660 *Colaboradores:* Sabbut, Pilaf, Julie, Head, DefLog, Sms, Toad32767, Huhsunqu, Renabot, LeonardoRob0t, Rembiapo pohyiete (bot), RobotQuistnix, Chobot, CSTAR, Yrbot, BOTijo, YurikBot, Wewe, LoquBot, KnightRider, Chlewbot, Folkvanger, Alexav8, Mister, Davius, Zenko corp, Thijs!bot, JAnDbot, TXiKiBoT, Rei-bot, Jorge C.Al, Technopat, AlleborgoBot, Muro Bot, BotMultichill, Gerakibot, Loveless, BOTarate, Toobaz, DragonBot, Farisori, Alejandrocaro35, Botito777, Alexbot, Juan Mayordomo, Raulshc, Mariols15, Pedrorupin, Lualalsa, DumZiBoT, Andreasmperu, MystBot, ArthurBot, Xqbot, Jkbw, Gusbelluwiki, RedBot, KamikazeBot, EmausBot, Antonsusi, Ruben.mg, Addbot, Juancarlosgonzalez1994, Juax 1994 y Anónimos: 30

7.2 Imágenes

- **Archivo:EulerPhi.svg** *Fuente:* https://upload.wikimedia.org/wikipedia/commons/9/9b/EulerPhi.svg *Licencia:* GFDL *Colaboradores:* Trabajo propio *Artista original:* Pietro Battiston (it:User:Toobaz)
- **Archivo:EulerPhi100.svg** *Fuente:* https://upload.wikimedia.org/wikipedia/commons/f/f3/EulerPhi100.svg *Licencia:* CC0 *Colaboradores:* Trabajo propio *Artista original:* User:Sverdrup
- **Archivo:Wikibooks-logo.svg** *Fuente:* https://upload.wikimedia.org/wikipedia/commons/f/fa/Wikibooks-logo.svg *Licencia:* CC BY-SA 3.0 *Colaboradores:* Trabajo propio *Artista original:* User:Bastique, User:Ramac et al.

7.3 Licencia del contenido