La Función de Euler y el Teorema de Fermat

Alan Reyes-Figueroa

Teoría de Números (Aula 11) 18.agosto.2022

Definición

Diremos que los números enteros $b_1, b_2, \ldots, b_k$ forman un ***sistema completo de invertibles*** *módulo n si*

$$\{\bar{b}_1, \bar{b}_2, \ldots, \bar{b}_k\} = (\mathbb{Z}/n\mathbb{Z})^* = U(n).$$

En otras palabras, $b_1, b_2, \ldots, b_k$ forman un sistema completo de invertibles, si todas las clases de congruencia invertibles, módulo n, están representadas en los b_i. Equivalente, eso ocurre si y sólo si los b_i satisfacen $(b_i, n) = 1$, $\forall i$, y $b_i \equiv b_j \pmod{n} \;\Rightarrow i = j$.

El conjunto $\{k \in \mathbb{Z} : \; 1 \leq k \leq n, \; (k, n) = 1\}$ se llama el sistema de invertibles **canónico** módulo n.

Estamos interesados en saber la cardinalidad de $U(n)$.

Definición

La función $\varphi : \mathbb{Z}^+ \to \mathbb{Z}$, dada por $\varphi(n) = |U(n)|$, se llama ***función φ de Euler***.

La Función de Euler

Alternativamente, podemos definir a la función de Euler como

$$\varphi(n) = \#\{k :\ 1 \leq k \leq n :\ (k, n) = 1\}.$$

Algunas observaciones:

- $\varphi(1) = \varphi(2) = 1$.
- Para $n > 2$, se tiene que $1 < \varphi(n) < n$ (1 y $n - 1$ son primos relativos con n).
- Si p es primo, entonces $\varphi(p) = p - 1$.
- Si p es primo, entonces $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p - 1)$.

  Prueba: Para mostrar esta afirmación, basta ver que si $1 \leq a \leq p^k$, $(a, p^k) = 1$ si y sólo si, a no es múltiplo de p; y hay precisamente p^{k-1} múltiplos de p en el intervalo $1 \leq a \leq p^k$.
- Para calcular la función φ en el caso general, vamos a mostrar antes una propiedad útil de esta función.

Proposición

Sean $m, n \in \mathbb{Z}^+$ tales que $(m, n) = 1$. Entonces $\varphi(mn) = \varphi(m)\varphi(n)$.
Esto es, φ es una función multiplicativa.

Prueba: Consideramos los números $1, 2, \ldots, mn$, con $(m, n) = 1$ y los colocamos en forma matricial como sigue:

$$\begin{array}{ccccc} 1 & 2 & 3 & \ldots & n \\ n+1 & n+2 & n+3 & \ldots & 2n \\ 2n+1 & 2n+2 & 2n+3 & \ldots & 3n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (m-1)n+1 & (m-1)n+2 & (m-1)n+3 & \ldots & mn \end{array}$$

Como $(m + j, n) = (j, n)$, si un número en esta table es primo relativo con n, entonces todos los números en esa columna son primos relativos con n. De ahí, existen $\varphi(n)$ columnas con elementos primos relativos con n.

La Función de Euler

Por otro lado, toda columna posee un sistema completo de residuos módulo m: si dos entradas i_1, i_2 son tales que $ni_1 + j \equiv ni_2 + j \pmod{m}$, entonces $i_1 \equiv i_2 \pmod{m}$. (Aquí se usa el hecho que n es invertible módulo m)

Así, en cada columna existen $\varphi(m)$ números que son primos relativos con m, y portanto la cantidad de números que son simultáneamente primos relativos con n y con m es $\varphi(mn) = \varphi(m)\varphi(n)$. $\square$

Obs! La propiedad anterior se generaliza: $\varphi(n_1 n_2 \cdots n_r) = \varphi(n_1)\varphi(n_2)\cdots\varphi(n_r)$, si los n_i son coprimos a pares. Basta aplicar inducción.

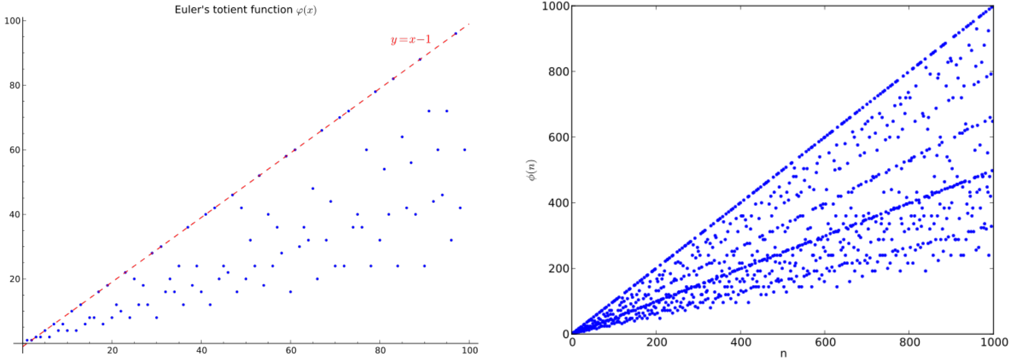
La conclusión de la proposición anterior es que tenemos un método sistemático para hallar $\varphi(n)$ para cualquier $n \in \mathbb{N}$. Si $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ es la factoración en primos de n. Como $(p_i^{k_i}, p_j^{k_j}) = 1$ para $i \neq j$, entonces

$$\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{k_i}) = \prod_{i=1}^{r} p_i^{k_i - 1}(p_i - 1) = \prod_{i=1}^{r} (p_i^{k_i} - p_i^{k_i - 1}) = n \prod_{i=1}^{r} \Big(1 - \frac{1}{p_i}\Big).$$

La Función de Euler

Ejemplo: Hallar $\varphi(372)$. Como $372 = 2^2 \cdot 3 \cdot 31$, entonces

$$\varphi(372) = \varphi(2^2) \cdot \varphi(3) \cdot \varphi(31) = 2(1) \cdot 2 \cdot 30 = 120.$$



Valores para la función φ de Euler.

Teorema (Teorema de Euler-Fermat)

Sean $a, n \in \mathbb{Z}$, $n > 1$ dos enteros tales que $(a, n) = 1$. Entonces

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Prueba: Observe que si $r_1, r_2, \ldots, r_{\varphi(n)}$ es un sistema completo de invertibles módulo n, y si $(a, n) = 1$, entonces también $ar_1, ar_2, \ldots, ar_{\varphi(n)}$ es un sistema completo de invertibles módulo n. De hecho, tenemos que $(ar_i, n) = 1$, y si $ar_i \equiv ar_j \pmod{n}$, entonces podemos cancelar a para obtener $r_i \equiv r_j \pmod{n}$. Luego $r_i = r_j$, y portanto $i = j$.

En consecuencia, cada ar_i debe ser congruente con algún r_j, y

$$\prod_{i=1}^{\varphi(n)} ar_i \equiv \prod_{i=1}^{\varphi(n)} r_i \pmod{n} \quad \Longrightarrow \quad a^{\varphi(n)} \prod_{i=1}^{\varphi(n)} r_i \equiv \prod_{i=1}^{\varphi(n)} r_i \pmod{n}.$$

Como los r_i son invertibles módulo n, también el producto $\prod_i r_i$ es invertible. Simplificanto este factor, resulta $a^{\varphi(n)} \equiv 1 \pmod{n}$. $\square$

Teorema (Pequeño Teorema de Fermat)

Sean $a \in \mathbb{Z}$, y p un número primo. Entonces

$$a^p \equiv a \pmod{p}.$$

Prueba: Si $p \mid a$, el resultado es inmediato, pues $a^p \equiv 0^p \equiv 0 \equiv a \pmod{p}$.
En el caso $p \nmid a$, entonces $(a, p) = 1$. Como $\varphi(p) = p - 1$, del Teorema de Euler-Fermat, tenemos que $a^{p-1} \equiv 1 \pmod{p} \Rightarrow a^p \equiv a \pmod{p}$. $\square$

Obs! El Teorema de Euler-Fermat también puede probarse utilizando el Teorema de Lagrange para grupos: si G es un grupo finito, y $g \in G$, entonces $g^{|G|} = 1$.
Aplicando esto en el caso $G = U(n)$, con $|G| = \varphi(n)$, se tiene que para $a \in U(n)$

$$a^{\varphi(n)} \equiv a^{|U(n)|} \equiv 1 \pmod{n}.$$

Dado un entero n, con factoración en primos de la forma $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, consideramos el número

$$M = [\varphi(p_1^{k_1}), \varphi(p_2^{k_2}), \ldots, \varphi(p_r^{k_r})] = mmc[\varphi(p_1^{k_1}), \varphi(p_2^{k_2}), \ldots, \varphi(p_r^{k_r})].$$

La Función de Euler

El Teorema de Euler puede ser optimizado de la siguiente forma

Proposición

Sean $a, n \in \mathbb{Z}$, $n > 1$ dos enteros tales que $(a, n) = 1$, y n se factora de la forma $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. Entonces

$$a^M \equiv 1 \pmod{n}. \qquad \textit{donde} \quad M = [\varphi(p_1^{k_1}), \varphi(p_2^{k_2}), \dots, \varphi(p_r^{k_r})].$$

Prueba: Por el Teorema de Euler-Fermat, sabemos que $a^{\varphi(p_i^{k_i})} \equiv 1 \pmod{p_i^{k_i}}$, para todo $i = 1, 2, \dots, r$. Elevando la congruencia anterior al exponente $M/\varphi(p_i^{k_i})$, obtenemos

$$a^M \equiv 1 \pmod{p_i^{k_i}}, \qquad \text{para } i = 1, 2, \dots, r.$$

Así, $a^M - 1$ es múltiplo de $p_i^{k_i}$, para todo $i = 1, 2, \dots, r$, y como estos números son coprimos dos a dos, se tiene que $n \mid a^M - 1 \;\Rightarrow\; a^M \equiv 1 \pmod{n}$. $\square$