UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

El Pequeño Teorema de Fermat

Alan Reyes-Figueroa

Teoría de Números

(Aula 14a) 17.agosto.2023

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

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

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

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

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