Teorema de Euler Fermat

Prof. Jhon Fredy Tavera Bucurú

2025

Definición (Grupo de Unidades)

Definimos el grupo de unidades $(\mathbb{Z}/n\mathbb{Z})^\times \subseteq \mathbb{Z}/n\mathbb{Z}$ *del anillo de enteros módulo* n *como el subconjunto formado por los elementos invertibles de* $\mathbb{Z}/n\mathbb{Z}$*:*

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{a \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{mcd}(a, n) = 1\}.$$

Lema

Si p es primo, entonces las únicas soluciones de $x^2 \equiv 1 \pmod{p}$ en $\mathbb{Z}/(p)$ son $\overline{1}$ y $\overline{-1}$. En particular, si $x \in (\mathbb{Z}/(p))^{\times} - \{1, -1\}$, entonces $x^{-1} \neq x$ en $\mathbb{Z}/(p)$.

Demostración: Tenemos:

$$x^2 \equiv 1 \pmod{p} \iff p \mid (x^2 - 1) \iff p \mid (x-1)(x+1).$$

Entonces:

$$p \mid x - 1 \text{ o } p \mid x + 1.$$

Lo cual implica:

$$x \equiv 1 \pmod{p} \text{ o } x \equiv -1 \pmod{p}.$$

$\square$

Definición (Sistema completo de restos)

Decimos que un conjunto de n números enteros $a_1, \ldots, a_n$ forma un sistema completo de restos módulo n (scr) si

$$\{\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n}\} = \mathbb{Z}/(n).$$

Definición (Sistena completo de invertibles)

De igual forma, decimos que los números enteros $b_1, b_2, \ldots, b_{\varphi(n)}$ *forman un sistema completo de invertibles módulo n (sci) si*

$$\{\overline{b_1}, \overline{b_2}, \ldots, \overline{b_{\varphi(n)}}\} = (\mathbb{Z}/(n))^{\times},$$

donde $\varphi(n)$ *representa el número de elementos de* $(\mathbb{Z}/(n))^{\times}$*.*
En otras palabras, $b_1, b_2, \ldots, b_{\varphi(n)}$ *forman un sci módulo n si, y sólo si, representan todas las clases de congruencia invertibles módulo n o, equivalentemente,*

$$\mathrm{mdc}(b_i, n) = 1 \quad \textit{para todo } i \quad \textit{y} \quad b_i \equiv b_j \pmod{n} \implies i = j.$$

El conjunto

$$\{k \in \mathbb{Z} \mid 1 \leq k \leq n \text{ } y \text{ } \mathrm{mdc}(n, k) = 1\}$$

es un ejemplo de sci módulo n.

Definición (Función Φ de Euler)

La función

$$\Phi(n) \stackrel{def}{=} |(\mathbb{Z}/n\mathbb{Z})^\times|$$

es llamada función phi de Euler.

Algunas propiedades basicas:

- $\varphi(1) = 1$ y, por lo tanto, también $\varphi(2) = 1$.
- Si p es primo,

  $$\varphi(p) = p - 1,$$

  ya que todos los enteros de 1 a p salvo uno son coprimos con p.
- Más generalmente, para $k \geq 1$,

  $$\varphi(p^k) = p^k - p^{k-1},$$

  pues en el intervalo $1 \leq a \leq p^k$ hay exactamente p^{k-1} múltiplos de p.

Teorema (φ de Euler multiplicativa)

Sea φ la función de Euler. Si $\gcd(m, n) = 1$, entonces

$$\varphi(mn) \ = \ \varphi(m)\,\varphi(n).$$

Demostración: Note que si $a, b, c \in \mathbb{Z}$. $(a, bc) = 1$ si y solamente si $(a, b) = 1$ y $(a, c) = 1$, luego hay tantos números que son primos relativos con nm como números que son primos relativos con n y m simultaneamente.

consideremos los enteros

$$1, 2, \ldots, nm$$

y organizemoslos en una matriz de m filas y n columnas:

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ n+1 & n+2 & n+3 & \ldots & 2n \\ \vdots & \vdots & \vdots & & \vdots \\ n(m-1)+1 & n(m-1)+2 & n(m-1)+3 & \ldots & nm \end{pmatrix},$$

donde la entrada en la fila i, columna j es

$$n(i-1)+j\,.$$

Note que $1 \leq j \leq n$ y que $0 \leq i-1 \leq m-1$

1. Observa que
$$(n(i-1)+j,\ n)\ =\ (j,n).$$
Por tanto, si $(j,n)=1$ toda la columna j es coprima con n. Hay exactamente $\varphi(n)$ columnas así.
2. Ahora probaremos que cada columna forma un sistema completo de residuos para $\mathbb{Z}_m$.
a) Note que cada columna tiene m elementos.
b) Supongamos que en la columna j tenemos que dos clases de equivalencia son iguales
$$\overline{n(i_1-1)+j}=\overline{n(i_2-1)+j}$$
Por tanto.
$$\begin{aligned} n(i_1-1)+j &\equiv n(i_2-1)+j \mod m \\ n(i_1-1) &\equiv n(i_2-1) \mod m \\ (i_1-1) &\equiv (i_2-1) \mod m/(n,m) \end{aligned}$$
por hipotesis $(n,m)=1$ entonces $m|i_1-i_2$ y como ambos son menores que m, entonces $i_1-i_2=0$. Es decir si $i_1\neq i_2$ entonces $\overline{n(i_1-1)+j}\neq\overline{n(i_2-1)+j}$

1. Concluimos entonces que hay $\varphi(n)$ columnas en donde cada número es primo relativo con n y además en cada una de esas columnas hay $\varphi(m)$ numeros que son primos relativos con m. Es decir, el número total de enteros en $\{1, \ldots, nm\}$ coprimos a la vez con n y con m es

$$\varphi(n)\,\varphi(m).$$

Por lo tanto, cuando $(n, m) = 1$ se cumple

$$\varphi(nm) = \varphi(n)\,\varphi(m),$$

como queríamos demostrar. $\square$

Teorema (de Euler Fermat)

Sean a y m dos enteros con $m > 0$ y $\mathrm{mdc}(a, m) = 1$. Entonces:

$$a^{\Phi(m)} \equiv 1 \pmod{m}.$$

Demostración: Observemos que si $r_1, r_2, \ldots, r_{\varphi(m)}$ es un sistema completo de invertibles módulo m y a es un número natural tal que $\mathrm{mdc}(a, m) = 1$, entonces $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ también es un sistema completo de invertibles módulo m. De hecho, tenemos que $\mathrm{mdc}(ar_i, m) = 1$ para todo i y, si $ar_i \equiv ar_j \pmod{m}$, entonces $r_i \equiv r_j \pmod{m}$, pues a es invertible módulo m, lo que implica $r_i = r_j$ y, por tanto, $i = j$.
Consecuentemente, cada ar_i debe ser congruente con algún r_j y, por tanto,

$$\prod_{1 \leq i \leq \varphi(m)} (ar_i) \equiv \prod_{1 \leq i \leq \varphi(m)} r_i \pmod{m}.$$

Esto implica:

$$a^{\varphi(m)} \prod_{1 \leq i \leq \varphi(m)} r_i \equiv \prod_{1 \leq i \leq \varphi(m)} r_i \pmod{m}.$$

Pero, como cada r_i es invertible módulo m, simplificando el factor $\prod_{1 \leq i \leq \varphi(m)} r_i$, obtenemos el resultado deseado:

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

Teorema (Pequeño Teorema de Fermat)

Sea a un entero positivo y p un primo, entonces:

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

Demostración: De hecho, observemos que si $p \mid a$, el resultado es evidente. Entonces, podemos suponer que $\mathrm{mdc}(a, p) = 1$. Como $\varphi(p) = p - 1$, por el Teorema de Euler tenemos:

$$a^{p-1} \equiv 1 \pmod{p}.$$

Multiplicando por a, obtenemos el resultado deseado:

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

$\square$

Ejemplo 1

Ejemplo 1

Calcule el resto de

$$2^{2^{2011}} \quad \text{al dividirlo por} \quad 39.$$

Solución

Como $\gcd(2,39) = 1$, por Teorema de Euler,

$$2^{\varphi(39)} \equiv 1 \pmod{39}, \quad \varphi(39) = \varphi(3)\,\varphi(13) = 2 \cdot 12 = 24.$$

Luego

$$2^{2^{2011}} \equiv 2^{\,2^{2011} \bmod 24} \pmod{39}.$$

- Observamos que para $k \geq 3$:

$$2^k \bmod 24 = \begin{cases} 8, & k \text{ impar}, \\ 16, & k \text{ par}. \end{cases}$$

Como 2011 es impar y mayor que 3,

$$2^{2011} \bmod 24 = 8.$$

- Por tanto

$$2^{2^{2011}} \equiv 2^8 \pmod{39}, \quad 2^8 = 256 \equiv 256 - 6 \cdot 39 = 22 \pmod{39}.$$

Por tanto $2^{2^{2011}} \bmod 39 = 22.$

Ejemplo 2

Ejemplo 2

Demostrar que, para todo $n \geq 0$,

$$13 \mid 7^{2n+1} + 6^{2n+1}.$$

Demostración

1. Observamos que

$$7 + 6 = 13 \quad \Longrightarrow \quad 7 \equiv -6 \pmod{13}.$$

2. Como $2n+1$ es impar, al elevar obtenemos

$$7^{2n+1} \equiv (-6)^{2n+1} = -6^{2n+1} \pmod{13}.$$

3. De aquí sigue inmediatamente

$$7^{2n+1} + 6^{2n+1} \equiv -6^{2n+1} + 6^{2n+1} = 0 \pmod{13},$$

Ejemplo 3

Ejemplo 3

Demuestra que existen infinitos múltiplos de 1991 que son de la forma

$$1\underbrace{99\cdots9}_{n}1.$$

Demostración

Definimos para cada $n \geq 0$

$$A_n \;=\; 1\underbrace{99\cdots9}_{n}1 \;=\; 2\cdot 10^{\,n+1} - 9.$$

Note que:

$$A_2 = 2\cdot 10^3 - 9 = 2000 - 9 = 1991 \equiv 0 \pmod{1991}.$$

Por otro lado, $1991 = 11 \times 181$. Por tanto $\gcd(10, 1991) = 1$, aplicando el Teorema de Euler-Fermat, tenemos

$$10^{\varphi(1991)} \equiv 1 \pmod{1991},$$

donde

$$\varphi(1991) = \varphi(11)\,\varphi(181) = 10 \times 180 = 1800.$$

Concluimos:

$$10^{1800} \equiv 1 \pmod{1991}.$$

Para cada $m \geq 0$, consideremos

$$A_{2+1800m} = 2 \cdot 10^{(2+1800m)+1} - 9 = 2 \cdot 10^{3} \left(10^{1800}\right)^{m} \; - \; 9.$$

Reduciendo módulo 1991:

$$A_{2+1800m} \equiv 2 \cdot 10^{3} \cdot 1^{m} - 9 = 2000 - 9 = 1991 \equiv 0 \pmod{1991}.$$

Como m es arbitrario, obtenemos *infinitos* $A_n \equiv 0 \pmod{1991}$.

Es decir $1991 | A_{2+1800m} \;\; \forall m \in \mathbb{N}$

Definición (congruencia lineal)

La congruencia $f(x) \equiv 0 \pmod{n}$ *se llama lineal cuando* $f(x)$ *es un polinomio de grado uno. Toda congruencia lineal se puede escribir en la forma:*

$$ax \equiv b \pmod{n}.$$

Teorema

La congruencia lineal $ax \equiv b \pmod{n}$ *tiene solución si y solo si* $d \mid b$, *donde* $d = (a, n)$.

Si la congruencia tiene solución, entonces tiene exactamente d *soluciones incongruentes.*

Teorema

Consideremos la congruencia lineal $ax \equiv b \pmod{n}$*. Si* y_0 *es una solución de la congruencia* $ny \equiv -b \pmod{a}$*, entonces el número:*

$$x_0 = \frac{ny_0 + b}{a}$$

es una solución de la congruencia original.

Definición (ecuación diofántica lineal 2 variables)

Una ecuación diofántica lineal en dos variables tiene la forma:

$$ax + by = c,$$

donde a, b *y* c *son enteros con* $ab \neq 0$.
Determinar las soluciones de esta ecuación diofántica es equivalente a determinar las soluciones de alguna de las congruencias lineales:

$$ax \equiv c \pmod{b} \quad o \quad by \equiv c \pmod{a}.$$

Teorema

La ecuación diofántica $ax + by = c$ *tiene solución si, y solo si,* $d \mid c$, *donde* $d = \gcd(a, b)$.
Además, si x_0 *y* y_0 *es una solución particular de la ecuación, entonces todas las soluciones están dadas por las ecuaciones:*

$$x = x_0 + k\frac{b}{d}, \quad y = y_0 - k\frac{a}{d},$$

donde k *es un entero arbitrario.*

Teorema (Teorema Chino del Residuo)

Sean $m_1, m_2, \ldots, m_r$ *enteros positivos primos relativos dos a dos, y sean* $a_1, a_2, \ldots, a_r$ *enteros arbitrarios.*
Entonces, el sistema de congruencias lineales:

$$
\begin{aligned}
x &\equiv a_1 \pmod{m_1},\\
x &\equiv a_2 \pmod{m_2},\\
&\vdots\\
x &\equiv a_r \pmod{m_r},
\end{aligned}
$$

tiene solución única módulo $m = \prod_{i=1}^{r} m_i$.