

## **EL TEST DE PRIMALIDAD DE FERMAT**

ALAN REYES-FIGUEROA  
TEORÍA DE NÚMEROS

(AULA 14B) 18.AGOSTO.2023

# Aplicaciones

El teorema de Euler-Fermat tiene muchas aplicaciones y es fundamental para gran parte de lo que se hace en teoría de números.

**Cálculo de potencias:** Como mínimo, puede ser un dispositivo que ahorra trabajo en ciertos cálculos.

Ejemplo: Se pide hallar  $5^{38} \pmod{11}$ .

Como  $\varphi(11) = 10$ , y  $(5, 11) = 1$  entonces del Teorema de Euler-Fermat, sabemos que  $5^{10} \equiv 1 \pmod{11}$ . Así

$$5^{38} \equiv 5^{3(10)+8} \equiv (5^{10})^3 \cdot 5^8 \equiv (1)^3 \cdot 5^8 \equiv 5^8 \equiv (5^2)^4 \equiv 3^4 \equiv 81 \equiv 4 \pmod{11}.$$

Ejemplo: Calcular  $7^{91} \pmod{100}$ .

Sabemos que  $100 = 2^2 \cdot 5^2$ . Entonces  $\varphi(100) = \varphi(2^2) \cdot \varphi(5^2) = 2(1) \cdot 5(4) = 2 \cdot 20 = 40$ .

Como  $(7, 100) = 1$ , por el Teorema de Euler-Fermat tenemos que  $7^{40} \equiv 1 \pmod{100}$ .

Entonces

$$7^{91} \equiv 7^{2(40)+11} \equiv (7^{40})^2 \cdot 7^{11} \equiv 7^{11} \pmod{100}.$$

# Aplicaciones

Ahora calculamos  $7^{11} \pmod{100}$  usando el algoritmo de exponenciación binaria:  
Observe que  $11 = 2^3 + 2^1 + 2^0 = (1011)_2$ . Entonces

$$7^1 \equiv 7 \pmod{100},$$

$$7^2 \equiv 49 \pmod{100},$$

$$7^4 \equiv 49^2 \equiv 2401 \equiv 1 \pmod{100},$$

$$7^8 \equiv 1^2 \equiv 1 \pmod{100}.$$

De ahí que

$$7^{91} \equiv 7^{11} \equiv 7^8 \cdot 7^2 \cdot 7^1 \equiv 1 \cdot 49 \cdot 7 \equiv 343 \equiv 43 \pmod{100}.$$

**Ejemplo:** Existen infinitos números enteros de la forma  $2000 \dots 0009$ , que son múltiplos de 2009.

Observe primero que el problema es equivalente a encontrar infinitos valores de  $k \in \mathbb{N}$  tales que  $2 \cdot 10^k + 9 \equiv 0 \pmod{2009}$ .

Pero

$$\begin{aligned} 2 \cdot 10^k + 9 \equiv 0 \pmod{2009} &\iff 2 \cdot 10^k + 9 \equiv 2009 \pmod{2009} \\ &\iff 2 \cdot 10^k \equiv 2000 \pmod{2009} \\ &\iff 10^k \equiv 1000 \equiv 10^3 \pmod{2009} \\ &\iff 10^{k-3} \equiv 1 \pmod{2009}, \end{aligned}$$

ya que  $(2, 2009) = 1$  y  $(1000, 2009) = 1$ .

Como  $(10, 2009) = 1$ , por el Teorema de Euler-Fermat, tenemos que  $10^{\varphi(2009)} \equiv 1 \pmod{2009}$ , esto implica que  $10^{t\varphi(2009)} \equiv 1^t \equiv 1 \pmod{2009}$ , para todo  $t \in \mathbb{N}$ .

Basta entonces hacer  $k - 3 = t(2009)$ , de modo que cualquier número de la forma  $n = 2 \cdot 10^{3+t\varphi(2009)} + 9$ ,  $t \in \mathbb{N}$ , satisface la condición requerida.

**Ejemplo:** No existen soluciones enteras para la ecuación  $x^3 \equiv 2 \pmod{103}$ .

Observe que 103 es primo. Entonces  $\varphi(103) = 102$ .

Supongamos que existe una solución  $x \in \mathbb{Z}$  de  $x^3 \equiv 2 \pmod{103}$ . En particular,  $103 \nmid x$ .

Elevando ambos lados de la congruencia anterior a  $\varphi(103)/3 = \frac{102}{3} = 34$ , obtenemos

$$(x^3)^{34} \equiv x^{102} \equiv x^{\varphi(103)} \equiv 1 \pmod{103},$$

debido al Teorema de Euler-Fermat.

Por otro lado,

$$(x^3)^{34} \equiv 2^{34} \equiv (2^{14})^2 \cdot 2^6 \equiv (7)^2 \cdot 64 \equiv 49 \cdot 64 \equiv 3136 \equiv 46 \pmod{103},$$

lo que es una contradicción, pues  $1 \not\equiv 46 \pmod{103}$ .

Portanto, no existe tal solución.

# Test de Primalidad de Fermat

**Tests de primalidad:** Otro uso del teorema de Euler-Fermat es como herramienta para probar la primalidad de un determinado entero  $n$ .

En este caso aplicamos el Pequeño Teorema de Fermat. Si pudiera demostrarse que la congruencia  $a^n \equiv a \pmod{n}$  no se cumple para alguna elección de  $a$ , entonces  $n$  debe ser necesariamente compuesto.

Como ejemplo, veamos  $n = 117$ . El cálculo se mantiene bajo control si seleccionando un entero pequeño para  $a$ , digamos,  $a = 2$ .

Como  $2^7 \equiv 128 \equiv 11 \pmod{117}$ , resulta

$$2^{117} \equiv 2^{7(16)+5} \equiv (2^7)^{16} \cdot 2^5 \equiv 11^{16} \cdot 2^5 \equiv (121)^8 \cdot 2^5 \equiv 4^8 \cdot 2^5 \equiv 2^{21} \pmod{117}.$$

Pero  $2^{21} \equiv (2^7)^3 \equiv 11^3 \pmod{117}$ , lo que conduce a

$$2^{117} \equiv 2^{21} \equiv 11^3 \equiv (11)^2 \cdot 11 \equiv 4 \cdot 11 \equiv 44 \not\equiv 1 \pmod{117}.$$

Esto muestra que 117 no es primo. De hecho,  $117 = 3^2 \cdot 13$ .

# Test de Primalidad de Fermat

El Recíproco de Teorema de Fermat, no vale, esto es, si  $a^{n-1} \equiv 1 \pmod{n}$ , para algún entero  $a$ , no necesariamente  $n$  es primo.

Para ver esto, precisamos del siguiente lema:

## Lema

Si  $p$  y  $q$  son primos distintos, y  $a^p \equiv a \pmod{q}$ ,  $a^q \equiv a \pmod{p}$ , entonces  $a^{pq} \equiv a \pmod{pq}$ .

Prueba: Del Pequeño Teorema de Fermat, tenemos que  $(a^q)^p \equiv a^q \pmod{p}$ . Además, por hipótesis  $a^q \equiv a \pmod{p}$ . Combinando estas congruencias, se tiene  $a^{pq} \equiv a \pmod{p}$ . Análogamente, se muestra que  $a^{pq} \equiv a \pmod{q}$ .

Esto muestra que  $p \mid a^{pq} - a$  y  $q \mid a^{pq} - a$ . Como  $p$  y  $q$  son primos distintos, entonces  $pq \mid a^{pq} - a$ , de modo que  $a^{pq} \equiv a \pmod{pq}$ .  $\square$

# Test de Primalidad de Fermat

**Ejemplo:** Vamos a mostrar que  $2^{340} \equiv 1 \pmod{341}$ .

Observe que  $2^{10} \equiv 1024 \equiv 31 \cdot 33 + 1$ . Por lo tanto,

$$2^{11} \equiv 2 \cdot 2^{10} \equiv 2 \cdot 1 \equiv 2 \pmod{31},$$

y

$$2^{31} \equiv 2 \cdot (2^{10})^3 \equiv 2 \cdot (1)^3 \equiv 2 \pmod{11}.$$

Explotando el lema,  $2^{341} \equiv 2^{11 \cdot 31} \equiv 2 \pmod{341}$ , de modo que al cancelar un factor 2, obtenemos  $2^{340} \equiv 1 \pmod{341}$ , y el recíproco del Teorema de Fermat es falso.

Los matemáticos chinos hace 25 siglos afirmaban que  $n$  es primo si y sólo si  $n \mid 2^n - 2$  (de hecho, este criterio vale para  $n \leq 340$ ). Nuestro ejemplo de  $n = 341$  es el contraejemplo (descubierto en 1819).

La situación en la que  $n \mid 2^n - 2$ , sin  $n$  ser primo, ocurre con suficiente frecuencia. Un entero compuesto  $n$  se llama **pseudoprimo** siempre que  $n \mid 2^n - 2$ . Hay infinitos pseudoprimos, por ejemplo: 341, 561, 645 y 1105.

# Test de Primalidad de Fermat

## Definición

De manera más general, un entero compuesto  $n$  para el cual  $a^n \equiv a \pmod{n}$  se llama un **pseudoprimo** en la base  $a$ . (Cuando  $a = 2$ , simplemente se dice que  $n$  es un pseudoprimo).

**Ejemplo:** 91 es el menor pseudoprimo para la base 3, mientras que 217 es el menor pseudoprimo en la base 5.

Observaciones:

- Se ha demostrado (1903) que hay infinitos pseudoprimos para cualquier base dada.
- Estos “primos impostores” son mucho más raros que los verdaderos primos. De hecho, hay sólo 247 pseudoprimos menores de un millón, en comparación con 78,498 primos.
- El primer ejemplo de un pseudoprimo par, a saber, el número  $161,038 = 2 \cdot 73 \cdot 1103$  fue encontrado en 1950.

# Test de Primalidad de Fermat

El **test de primalidad de Fermat** es un algoritmo probabilístico que hace uso del Pequeño Teorema de Fermat.

Resulta que el recíproco de este teorema suele (con alta probabilidad) ser verdad: si  $p$  es compuesto, entonces  $a^{p-1}$  es poco probable que sea congruente con  $1 \pmod{p}$  para un valor arbitrario de  $a$ . Sin embargo, los pseudoprimos fallan este test.

Idea: Tome  $a \in \mathbb{Z}$ ,  $(a, n) = 1$  al azar. Si  $a^{n-1} \equiv 1 \pmod{n}$ , entonces  $n$  tiene alta probabilidad de ser primo.

Observe que si  $a = 1$ , la congruencia  $a^{n-1} \equiv a \pmod{n}$  es trivial. También la congruencia  $a^{n-1} \equiv a \pmod{n}$  se satisface de forma trivial si  $a = n - 1$ , y  $n$  es impar. Por esta razón, usualmente se elige un candidato  $1 < a < n - 1$ .

Cualquier  $a$  que satisface  $a^{n-1} \equiv a \pmod{n}$  cuando  $n$  es compuesto se llama un **mentiroso de Fermat** (*Fermat liar*). En este caso  $n$  es un pseudoprimo para la base  $a$ . Si elegimos  $a$  tal que  $a^{n-1} \not\equiv a \pmod{n}$ ,  $a$  se llama un **testigo de Fermat** (*Fermat witness*) para la no primalidad de  $n$ .

# Test de Primalidad de Fermat

**Algoritmo:** (Test de Primalidad de Fermat)

*Inputs:*  $n \in \mathbb{Z}^+$ ,  $n > 3$ , un entero a testar su primalidad,  $k$  número de réplicas del test.

*Output:* 0 si  $n$  es compuesto, en caso contrario responde, primo con alta probabilidad.

For  $i = 1, 2, \dots, k$ :

    Pick  $a$  randomly in the range  $[2, n - 2]$ .

    If  $a^{n-1} \not\equiv 1 \pmod{n}$ : then return 0.

return probably prime.

El Test de Fermat es muy simple, sin embargo tiene fallas.

Existen números compuestos  $n$  que son pseudoprimos para cada base  $a$ ; es decir,  $a^{n-1} \equiv 1 \pmod{n}$ , para todos los enteros  $a$  con  $(a, n) = 1$ .

Estos números se conocen como **números de CARMICHAEL** (descubiertos en 1910).

El menor de estos números excepcionales es  $561 = 3 \cdot 11 \cdot 17$ . Carmichael indicó otros tres:  $1105 = 5 \cdot 13 \cdot 17$ ,  $2821 = 7 \cdot 13 \cdot 31$  y  $15841 = 7 \cdot 31 \cdot 73$ . Dos años más tarde presentó 11 adicionales.

# Test de Primalidad de Fermat

Para ver que  $561 = 3 \cdot 11 \cdot 17$  es un número de Carmichael, un pseudoprimo absoluto, observe que  $(a, 561) = 1$  produce

$$(a, 3) = 1, \quad (a, 11) = 1, \quad (a, 17) = 1.$$

Aplicando el Teorema de Euler-Fermat, obtenemos las congruencias

$$a^2 \equiv 1 \pmod{3}, \quad a^{10} \equiv 1 \pmod{11}, \quad a^{16} \equiv 1 \pmod{17},$$

que a su vez producen

$$a^{560} \equiv (a^2)^{280} \equiv (1)^{280} \equiv 1 \pmod{3},$$

$$a^{560} \equiv (a^{10})^{56} \equiv (1)^{56} \equiv 1 \pmod{11},$$

$$a^{560} \equiv (a^{16})^{35} \equiv (1)^{35} \equiv 1 \pmod{17}.$$

Siendo 3, 11 y 17 primos, esto da lugar a la congruencia  $a^{560} \equiv 1 \pmod{561}$ , siempre que  $(a, 561) = 1$ . Así, 561 es un número de Carmichael.