

Presentación Seminario 1: Números de Carmichael

Rodrigo Sebastián Ajmac Aroche

29 de septiembre de 2025

Recordando...

Definición de número primo

Un número primo es un número natural mayor que 1 que solo tiene dos divisores: él mismo y el 1.

Propiedades de los números primos

- Para un primo p , $\varphi(p) = p - 1$.
- El grupo $U(p)$ es de orden $p - 1$.

Otras características de los números primos

Teorema de Euler-Fermat

Si $\gcd(a, n) = 1$, entonces:

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

Pequeño Teorema de Fermat

Si p es primo y $\gcd(a, p) = 1$, entonces:

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

Ejemplos de pseudoprimos de Fermat

- 341 es pseudoprimo de Fermat en base 2, pero no en base 3.
- 9 es pseudoprimo de Fermat en base 8, pero no en otras bases.

¿Existirán números compuestos que pareciesen cumplir el pequeño teorema de Fermat?

Números de Carmichael

Definición número de Carmichael

Un número de Carmichael es un número compuesto n tal que:

$$a^{n-1} \equiv 1 \pmod{n} \quad \text{para todo } a \text{ con } \gcd(a, n) = 1.$$

(Carmichael Numbers - OeisWiki, s.f.)

Václav Šimerka (1885)



Descubrió en 1885 los primeros 7 números de Carmichael:

561, 1105, 1729, 2465, 2821, 6601, 8911

(Wikipedia-Autores, 2006)

Imagen tomada con fines educativos



En 1899 probó un resultado relacionado con los números de Carmichael, aunque no sabía aún la conexión con ellos. (Korselt's Theorem - ProofWiki, s.f.)

Robert Daniel Carmichael (1910)



Imagen tomada con fines educativos

Redescubrió el número de Carmichael más pequeño: 561. (Wikipedia contributors, 2025)

¿Por qué 561 es número de Carmichael?

- $a = 2$. $\gcd(2, 561) = 1$ y $2^{560} \equiv 1 \pmod{561}$.
- $a = 10$. $\gcd(10, 561) = 1$ y $10^{560} \equiv 1 \pmod{561}$.
- $a = 50$. $\gcd(50, 561) = 1$ y $50^{560} \equiv 1 \pmod{561}$.

(Estos son ejemplos concretos: $561 = 3 \cdot 11 \cdot 17$, y como 561 es número de Carmichael, cualquier a coprimo con 561 cumple la congruencia anterior.)

Teoremas relacionados con los números de Carmichael

Un número compuesto n es un número de Carmichael si y solo si:

- n es impar.
- n es libre de cuadrados.
- Para todo primo $p \mid n$, se cumple $p - 1 \mid n - 1$.

(Conrad. K, s.f.; Korselt's Theorem - ProofWiki, s.f.)

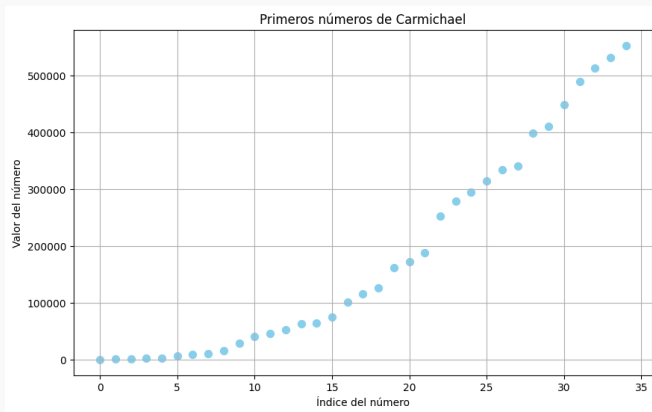
No existen números de Carmichael con solo dos factores primos.
(Carmichael Numbers - OeisWiki, s.f.)

Números de Carmichael conocidos actualmente

Conjunto conocido

Actualmente se conocen números de Carmichael como:

561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, . . .



(Carmichael Numbers - OeisWiki, s.f.)

¿Cómo construir números de Carmichael?

Fórmula de Chernick

Para $k = 3$ factores:

$$n = (6m + 1)(12m + 1)(18m + 1)$$

Formúla generalizada:

$$M_k(m) = (6m + 1)(12m + 1) \prod_{i=1}^{k-2} (9 \cdot 2^i m + 1), k \geq 3$$

(Carmichael Numbers - OeisWiki, s.f.)

¿Hay infinitos números de Carmichael?

Alford, Granville y Pomerance (1994)

Hay infinitos números de Carmichael.



William "Red" Alford
(1937 – 2003)



Andrew James
Granville (1962)



Carl Pomerance
(1944)

Otras sucesiones de números de Carmichael

- **Cantidad de números de Carmichael menores a 10^n con $n \geq 1$ (A055553):** $\{0, 0, 1, 7, 16, 43, 105, 255, \dots\}$
- **Número de Carmichael más pequeño con n factores primos, con $n \geq 3$ (A006931):** $\{561, 41041, 825265, 321197185, \dots\}$
- **Números de Chernick-Carmichael (A033502):** $\{1729, 294409, 56052361, 118901521, \dots\}$
- **Números de Chernick-Carmichael forma extendida (A317126):** $\{1729, 63973, 294409, 56052361, \dots\}$

(Carmichael Numbers - OeisWiki, s.f.)

Pseudoprimos

Otras formas de encontrar pseudoprimos

- Test de Euler-Jacobi
- Test de Miller-Rabin

- Alford, W. R., Granville, A., & Pomerance, C. (1994). There are infinitely many Carmichael numbers. *Annals of Mathematics*, 140(3), 703–722. <https://doi.org/10.2307/2118576>
- Carmichael numbers - OeisWiki. (s.f.). https://oeis.org/wiki/Carmichael_numbers
- Conditions for Integer to have Primitive Root - ProofWiki. (s.f.). https://proofwiki.org/wiki/Conditions_for_Integer_to_have_Primitive_Root
- Conrad, K. (s.f.) *CARMICHAEL NUMBERS AND KORSELT'S CRITERION* [PDF] <https://kconrad.math.uconn.edu/blurbs/ugradnumthy/carmichaelkorselt.pdf>
- Definition:Primitive root (Number Theory) - ProofWiki. (s.f.). [https://proofwiki.org/wiki/Definition:Primitive_Root_\(Number_Theory\)](https://proofwiki.org/wiki/Definition:Primitive_Root_(Number_Theory))

- Korselt's theorem - ProofWiki. (s.f.). https://proofwiki.org/wiki/Korselt%27s_Theorem#Historical_Note
- Wikipedia contributors. (2025, 11 julio). Carmichael number. Wikipedia. https://en.wikipedia.org/wiki/Carmichael_number
- Wikipedia contributors. (2025, abril 28). Fermat pseudoprime. Wikipedia. https://en.wikipedia.org/wiki/Fermat_pseudoprime
- Wikipedia contributors. (2025, septiembre 28). Fermat primality test. Wikipedia. https://en.wikipedia.org/wiki/Fermat_primality_test
- Wikipedia-Autoren. (2006, 4 marzo). Václav Šimerka. https://de.wikipedia.org/wiki/V%C3%A1clav_%C5%A0imerka