Teoría de números

Números de Carmichael

Docente: Gabriel Chicas Reyes, MSc.
Alumno: Kevin López Aquino

Domingo 8 de diciembre de 2019

I. Introducción

El pequeño teorema de Fermat nos dice que si p es primo y a es un entero tal que $p \nmid a$, se tiene que

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

De forma equivalente, si n y a son enteros coprimos, y

$$a^{n-1} \not\equiv 1 \pmod{n},$$

podemos afirmar que n es un número compuesto.

Existen aplicaciones en las que se desea saber si un entero n, usualmente *grande*, es primo. Supongamos que n satisface (1) para varios enteros coprimos con n. Aunque no podamos afirmar con certeza que n sea primo, existen algoritmos probabilísticos que se basan, al menos inicialmente, en el hecho que esta condición se cumpla. Si esto sucede, n probablemente es primo. De lo contrario, sabemos que n es compuesto.

Sin embargo, existen enteros compuestos n que cumplirán (1) sin importar cuántos enteros a coprimos con n se elijan. V. Šimerka listó los primeros siete en 1885[1]:

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

Estos números tiene propiedades interesantes y se denominan **números de Carmichael** en honor a Robert Carmichael, quien escribió sobre ellos en sus artículos de 1910[2] y 1912[3]. En lo que sigue, estudiamos sus propiedades básicas.

[1] Václav Šimerka, *Zbytky z arithmetické posloupnosti,* Časopis pro pěstování mathematiky a fysiky **14** (1885), p. 224 . Disponible aquí.

[2] R. D. Carmichael, *Note on a new number theory function*, Bulletin Amer. Math. Soc. **16** (1910). Disponible aquí.

[3] R. D. Carmichael, *On composite P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \pmod{P}$* , Bulletin Amer. Math. Monthly **19** (1912). Disponible aquí.

II. Resultados

Definición 1. Un **número de Carmichael** es un entero compuesto n que cumple que

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

para todo a coprimo con n.

Nuestra primera observación es que todos los números en la lista de Šimerka son impares. Podemos usar la definición para demostrar que esto es cierto para todos los números de Carmichael. Supongamos que existe un número de Carmichael par y llamémoslo n. Notemos que 2 no es un número de Carmichael, puesto que es primo. Así, $n \geq 4$. En particular,

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

Sin embargo,

$$(n-1)^{n-1} \equiv (-1)^{n-1} \equiv -1 \pmod{n},$$

de forma que $1 \equiv -1 \pmod{n}$, lo cual es absurdo. Por tanto, n debe ser impar.

• **Ejemplo.** 561 es un número de Carmichael. Para demostrar esto, notamos la factorización $561 = 3 \cdot 11 \cdot 17$ y tomamos un entero arbitrario a coprimo con 561. Por el pequeño teorema de Fermat, tenemos que

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

Notando que $2, 10$ y 16 dividen a $n - 1 = 560$, se sigue que

$$a^{560} \equiv 1 \pmod{3}$$
$$a^{560} \equiv 1 \pmod{11}$$
$$a^{560} \equiv 1 \pmod{17}.$$

Además, $\text{mcm}(3, 11, 17) = 3 \cdot 11 \cdot 17 = 561$, de forma que $a^{560} \equiv 1 \pmod{561}$. ■

En el ejemplo anterior, teníamos un número de Carmichael n y notábamos que si p es un factor primo de n, se tiene que $p - 1 \mid n - 1$. Esto siempre se cumple y fue observado por A. Korselt en 1899 cuando demostró[4], sin dar ejemplos, que los enteros que cumplen con la **definición 1** se pueden caracterizar de la siguiente forma:

[4] A. R. Korselt, *Problème chinois*, L'intermédiaire des mathématiciens (1899).

Proposición 2 (criterio de Korselt). Un entero compuesto n es un número de Carmichael si y solo si
(i) n es libre de cuadrados y
(ii) $p-1 \mid n-1$ para todos los primos p que dividen a n.

Demostración. ($\Rightarrow$) Sea n es un número de Carmichael.

$\star$ Primero demostramos que n es libre de cuadrados. Procedemos por contradicción. Sea p un primo divisor de n, de forma que

$$n = p^k m$$

donde $k \geq 2$ y $\text{mcd}(p, m) = 1$. En particular, tenemos que $p^2 \mid n$. Sea g una raíz primitiva módulo p^2. Notamos que $\text{mcd}(p^2, m) = 1$, de forma que podemos usar el teorema chino del resto para garantizar la existencia de un entero b que cumple

$$b \equiv g \pmod{p^2}$$

$$\text{y} \quad b \equiv 1 \pmod{m}.$$

De lo anterior, notamos que b es una raíz primitiva módulo p^2, de forma que $\text{mcd}(b, p^2) = 1$ y $\text{mcd}(b, p^k) = 1$. Además, $\text{mcd}(b, m) = \text{mcd}(1, m) = 1$, de lo que se sigue que $\text{mcd}(b, n) = 1$. Puesto que n es un número de Carmichael, tenemos

$$b^{n-1} \equiv 1 \pmod{n},$$

de donde

$$b^{n-1} \equiv 1 \pmod{p^2}.$$

Puesto que b es una raíz primitiva módulo p^2, se sigue que

$$\text{ord}_{p^2}(b) = p(p-1) \mid n-1,$$

de lo que deducimos que $p \mid n-1$. Pero $p \mid n$, de lo que podemos concluir que $n-1$ y n tienen a p como divisor común, contradiciendo el hecho que son coprimos. La contradicción proviene de la asunción que n es un número de Carmichael y divisible por algún cuadrado. Por tanto, si n es un número de Carmichael, debe ser libre de cuadrados.

$\star$ Sea p un divisor primo de n. Ahora demostramos que $p-1 \mid n-1$. Por la parte anterior, podemos escribir $n = pm$, donde $\text{mcd}(p, m) = 1$. Sea g una raíz primitiva módulo p. Por el teorema chino del resto, existe un entero b tal que

$$b \equiv g \pmod{p}$$

$$\text{y} \quad b \equiv 1 \pmod{m}.$$

Notamos que b es coprimo con n, por lo que $b^{n-1} \equiv 1 \pmod{n}$ y que $b^{n-1} \equiv 1 \pmod{p}$. Por tanto, $p-1 \mid n-1$.

($\Leftarrow$) Ahora supongamos que $n = p_1 p_2 \dots p_r$ y que $p_j - 1 \mid n - 1$ para $1 \leq j \leq r$. Sea a coprimo con n. Por el pequeño teorema de Fermat, tenemos que

$$a^{p_j - 1} \equiv 1 \pmod{p_j},$$

de forma que

$$a^{n-1} \equiv 1 \pmod{p_j},$$

para $1 \leq j \leq r$. Notando que $\operatorname{mcm}(p_1, \dots, p_r) = p_1 \dots p_r = n$, se sigue que

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

□

Una forma alternativa de alcanzar una contradicción al demostrar que un número de Carmichael es libre de cuadrados, es notar que si

$$n = p^k m,$$

donde $k \geq 2$ y $\operatorname{mcd}(p, m) = 1$, se sigue, usando el teorema chino del resto, que existe un b tal que

$$b \equiv 1 + p \pmod{p^2}$$
$$\text{y} \quad b \equiv 1 \pmod{m}.$$

Entonces, $\operatorname{mcd}(b, n) = 1$, de forma que $b^{n-1} \equiv 1 \pmod{n}$. Debilitando la congruencia, obtenemos que

$$(1 + p)^{n-1} \equiv 1 \pmod{p^2}.$$

Pero

$$\begin{aligned}(1+p)^{n-1} = \sum_{k=0}^{n-1} \binom{n-1}{k} p^k &= 1 + (n-1)p + \ldots + (n-1)p^{n-2} + p^{n-1} \\ &\equiv 1 + (n-1)p \pmod{p^2} \\ &\equiv 1 - p \pmod{p^2}.\end{aligned}$$

Así, $1 \equiv 1 - p \pmod{p^2}$, lo cual es absurdo.

Corolario 3. Sea n impar y sean $p_1, \dots, p_r$ primos distintos. Un entero $n = p_1 \dots p_r$ es un número de Carmichael si y solo si

$$\lambda := \operatorname{mcm}(p_1 - 1, \dots, p_r - 1) \mid n - 1.$$

Demostración. Por hipótesis, n es libre de cuadrados. Entonces,

$$n \text{ es un número de Carmichael } \iff p_i - 1 \mid n - 1 \text{ para } 1 \leq i \leq r \iff \lambda \mid n - 1.$$

□

Proposición 4. Un entero n es un número de Carmichael si y solo si n es compuesto y $a^n \equiv a \pmod{n}$ para todo $a \in \mathbb{Z}$.

Demostración. ($\Rightarrow$) Sea $n = p_1 p_2 \dots p_r$ un número de Carmichael y a un entero arbitrario. Primero demostramos que

$$a^n \equiv a \pmod{p_i}$$

para $1 \leq i \leq r$. Por el pequeño teorema de Fermat, tenemos que

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

A partir de esto, consideramos dos casos.

Caso I. $p_i \mid a$. Entonces, se sigue que

$$a^n \equiv a \equiv 0 \pmod{p_i}.$$

Caso II. $p_i \nmid a$. Entonces,

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

Pero $p_i - 1 \mid n - 1$, de forma que

$$a^{n-1} \equiv 1 \pmod{p_i}.$$

Multiplicando por a ambos lados de la congruencia, obtenemos que $a^n \equiv a \pmod{p_i}$.

Ahora notamos que $\operatorname{mcm}(p_1, p_2, \dots, p_r) = n$, de lo que se sigue que $a^n \equiv a \pmod{n}$.

($\Leftarrow$) Sea a coprimo con n. Entonces, podemos cancelar a de la congruencia $a^n \equiv a \pmod{n}$, de forma que $a^{n-1} \equiv 1 \pmod{n}$. □

Si p es un número primo, se tiene el interesante resultado

$$(a + b)^p \equiv a^p + b^p \pmod{p}$$

para cualesquiera enteros a y b[5] . Esta congruencia también se cumple si n es un número de Carmichael. En efecto, si a y b son enteros arbitrarios, la proposición anterior implica que

$$(a + b)^n \equiv a + b \equiv a^n + b^n \pmod{n}.$$

[5]Esto tiene un agradable parecido con el *freshman's dream*: asumir, erróneamente, que $(x + y)^n = x^n + y^n$ cuando n es un número natural y x, y son reales arbitrarios.

n	n-ésimo número de Carmichael	Factorización en primos
1	561	$3 \cdot 11 \cdot 17$
2	1105	$5 \cdot 13 \cdot 17$
3	1729	$7 \cdot 13 \cdot 19$
4	2465	$5 \cdot 17 \cdot 29$
5	2821	$7 \cdot 13 \cdot 31$
6	6601	$7 \cdot 23 \cdot 41$
7	8911	$7 \cdot 19 \cdot 67$
8	10585	$5 \cdot 29 \cdot 73$
9	15841	$7 \cdot 31 \cdot 73$
10	29341	$13 \cdot 37 \cdot 61$
11	41041	$7 \cdot 11 \cdot 13 \cdot 41$
12	46657	$13 \cdot 37 \cdot 97$
13	52663	$7 \cdot 73 \cdot 103$
14	62745	$7 \cdot 5 \cdot 47 \cdot 89$
15	63973	$7 \cdot 13 \cdot 19 \cdot 37$
16	75361	$11 \cdot 13 \cdot 17 \cdot 31$
17	10101	$7 \cdot 11 \cdot 13 \cdot 101$
18	115921	$13 \cdot 37 \cdot 141$
19	126217	$7 \cdot 13 \cdot 19 \cdot 73$
20	162401	$17 \cdot 41 \cdot 233$

Tabla I. Los primeros veinte números de Carmichael (sucesión A002997 en OEIS) y su factorización en primos.

En los datos anteriores, podemos notar que los primeros números de Carmichael son el producto de al menos 3 primos distintos. Esto resulta ser, en general, verdadero.

Proposición 5. Todo número de Carmichael es el producto de al menos tres primos distintos.

Demostración. Argumentamos por contradicción. Sea $n = pq$ un número de Carmichael, donde p y q son primos distintos. Supongamos, sin pérdida de generalidad, que $p > q$. Entonces, $p - 1 > q - 1$. Puesto que n es un número de Carmichael, tenemos que

$$n - 1 \equiv 0 \pmod{p-1}.$$

Sin embargo,

$$n - 1 \equiv pq - 1 \equiv (p - 1 + 1)q - 1 \equiv q - 1 \pmod{p-1},$$

de forma que $q-1 \equiv 0 \pmod{p-1}$. Esto implica que $p-1 < q-1$, lo cual es una contradicción. Por tanto, n, siendo un número de Carmichael, no puede estar compuesto solo de dos factores. □

Notamos que si n es un número de Carmichael, no existen raíces primitivas en $(\mathbb{Z}/n\mathbb{Z})^\times$: siendo n un número impar, libre de cuadrados y compuesto por al menos 3 factores primos distintos, no puede ser de ninguna de las formas $2, 4, p^\alpha$ o $2p^\alpha$ con p primo impar.

Si n es un número compuesto, sabemos que tiene al menos un divisor primo p que cumple que $p \leq \sqrt{n}$. Tomemos como ejemplo $28 = 7 \cdot 2^2$. Tenemos que $\sqrt{28} \approx 5.29$, $2 < \sqrt{28}$, pero $7 > \sqrt{28}$. Todo lo que sabemos es que *al menos* un divisor primo cumple con esto. Si n es un número de Carmichael, podemos decir más.

Proposición 6. Si n es un número de Carmichael, se tiene que $p < \sqrt{n}$ para todo divisor primo p de n.

Demostración. Tenemos que

$$n - 1 \equiv 0 \pmod{p-1},$$

de forma que

$$\begin{aligned} 0 \equiv n - 1 \equiv \left(\frac{n}{p}\right) p - 1 &\equiv \left(\frac{n}{p}\right) p - \frac{n}{p} + \frac{n}{p} - 1 \pmod{p-1} \\ &\equiv \left(\frac{n}{p}\right)(p-1) + \frac{n}{p} - 1 \pmod{p-1} \\ &\equiv \frac{n}{p} - 1 \pmod{p-1}, \end{aligned}$$

de lo que deducimos que $p - 1 \mid \frac{n}{p} - 1$. Por tanto, $p \leq \frac{n}{p}$. La desigualdad debe ser estricta: de lo contrario n sería un cuadrado. Así, concluimos que $p < \sqrt{n}$. □

En su artículo[6] de 1939, J. Chernick mostró formas de construir números de Carmichael. Presentamos la más popular (la que ha llegado a los libros de texto) a continuación.

Proposición 7. Sea k un entero tal que $6k + 1$, $12k + 1$ y $18k + 1$ son primos. Entonces, $n = (6k + 1)(18k + 1)(36k + 1)$ es un número de Carmichael.

Demostración. Verificamos que n satisface las condiciones del criterio de Korselt. Sean

$$p_1 := 6k + 1$$

$$p_2 := 12k + 1$$

$$p_3 := 18k + 1.$$

Primero notamos que n es, en efecto, libre de cuadrados: su factorización es $n = p_1 p_2 p_3$ y p_1, p_2, p_3 son, por hipótesis, primos distintos. Para comprobar la segunda condición del criterio de Korselt, calculamos $n - 1$:

$$\begin{aligned} n - 1 &= (6k + 1)(12k + 1)(18k + 1) - 1 \\ &= (6 \cdot 12k^2 + 18k + 1)(18k + 1) - 1 \\ &= 6 \cdot 12 \cdot 18k^3 + (6 \cdot 12 + 18^2)k^2 + 2 \cdot 18k + 1 - 1 \\ &= 18k(6 \cdot 12k^2 + 22k + 2). \end{aligned}$$

De lo anterior, podemos notar que $n - 1$ es divisible entre $p_1 - 1$, $p_2 - 1$ y $p_3 - 1$. Por tanto, n es un número de Carmichael. □

[6] J. Chernick, *On Fermat's simple theorem*, Bull. Amer. Math. Soc. **45** (1939). Disponible aquí.

A pesar que los números de Carmichael se seguían estudiando a lo largo del siglo XX, no fue hasta 1994 que se demostró, en un artículo[7] dedicado a Paul Erdős por su octogésimo cumpleaños, el siguiente resultado.

Teorema 8 (Alford, Granville y Pomerance).

Existen infinitos números de Carmichael.

Demostración. El artículo se encuentra disponible aquí. □

III. Referencias

[1] Noel Koblitz, *A Course in Number Theory and Cryptography. Graduate Texts in Mathematics*, Springer-Verlag (1987), capítulo V, sección 1.

[2] Keith Conrad, *Carmichael Numbers and Korselt's Criterion.* Recuperado de https://kconrad.math.uconn.edu/blurbs/ugradnumthy/carmichaelkorselt.pdf.

[3] Andrew Granville, *Primality Testing and Carmichael Numbers.* Recuperado de https://dms.umontreal.ca/~andrew/PDF/Notices1.pdf.

[7] W.R. Alford, Andrew Granville y Carl Pomerance, *There are infinitely many Carmichael numbers*, Annals of Math. **140** (1994), 703-722.