Universidad de Valladolid

Facultad de Ciencias

Trabajo Fin de Grado

Grado en Matemáticas

Título del Trabajo

Números de Carmichael

Autor:

Camila A. Gaitán Quintero

Tutor/es:

José Enrique Marcos Naveira

Índice general

Introducción

La teoría de números es una rama de las matemáticas que tiene una presencia constante a lo largo del grado en matemáticas a pesar de no contar con una asignatura propia. Uno de los temas más recurrentes en esa materia son los números primos, cómo calcularlos y cómo diferenciarlos de los compuestos. Es aquí donde entran en juego los pseudoprimos y en particular los números de Carmichael. Se trata de unos números que, sin ser primos, tienen en ciertos aspectos un comportamiento similar a los números primos. El objetivo de este trabajo es exponer los resultados más comunes sobre estos números e ilustrarlos con listas hechas en Maple.

Para comenzar, se recordarán cuestiones básicas sobre los números primos. También se introducirán los tests de primalidad y la noción de pseudoprimalidad.

En el segundo capítulo se presentarán formalmente los números de Carmichael como *pseudoprimos absolutos* y sus propiedades básicas. Antes de sumergirse totalmente en el tema, se dedicará un capítulo a la función λ de Carmichael que, además de facilitar la notación en las demostraciones posteriores y estar relacionada con la conocida φ de Euler, permite demostrar nuevas propiedades que ayudarán a limitar la búsqueda de números de Carmichael.
En el resto del trabajo se trata, en general, de dar métodos para calcular números de Carmichael. Por esta razón, el cuarto capítulo está dedicado a los números de Carmichael en su factorización más sencilla, con 3 factores primos.
El capítulo 5 es el más extenso pues en él se pretende generalizar algunos de los métodos usados en el anterior y dar algunos nuevos. La idea es partir de 3 factores primos e ir añadiendo más. Se introducen las *formas universales*, un producto de formas lineales que cumple las propiedades de los números de Carmichael y por tanto sirven como fórmula para construirlos.
Los 3 capítulos siguientes vienen motivados por su similitud con los números primos. Se abordarán las cuestiones siguientes:

- Si se pueden añadir factores primos a un número de Carmichael sin alterar sus propiedades, ¿se podrá añadir un número de Carmichael que también las mantenga?
- Es conocido el estudio de números primos en sucesiones aritméticas, ¿qué se puede decir de los números de Carmichael en ellas?
- La principal aplicación práctica de los números primos es en criptografía, ¿tienen alguna aplicación los números de Carmichael en esta área?

En el penúltimo capítulo se describirán modificaciones de algunas propiedades de los números de Carmichael para conseguir, o bien números nuevos, o bien números de Carmichael especiales. Para finalizar, se añadieron anexos de algunas listas que pueden ser de interés y un resumen de problemas abiertos en esta materia.

Capítulo 1

Criterios de primalidad

Empezamos hablando de números primos y algunas de sus propiedades, pues de su estudio se deriva el de pseudoprimos y en particular el de los números de Carmichael.

Los números primos han llamado la atención a lo largo de la historia, sobre todo hoy en día gracias a sus aplicaciones en criptografía. Naturalmente, con su descubrimiento se inicia una búsqueda de propiedades con el fin de caracterizarlos más allá de la propia definición.

Así, se demostró que existen infinitos números primos, y con la criba de Erastótenes se encontró un sistema relativamente práctico para encontrarlos, al menos para la época. El pequeño teorema de Fermat es quizá uno de los primeros grandes enunciados en esta materia.

Antes de enunciarlo, recordemos algunas definiciones.

Definición 1. *Orden*

- *Se define el* ***orden de*** b ***mod*** n*, y se denota* $ord(b)$ $mod\ n$*, como el menor exponente* $k \in \mathbb{N}$ *tal que* $b^k \equiv 1\ mod\ n$*.*
- *Sea* G *un grupo y* b *un elemento suyo. Se define el* ***orden de*** b*, y se denota* $ord(b)$*, como el menor exponente* $k \in \mathbb{N}$ *tal que* $b^k = 1$*.*
- *El orden de un grupo es su cardinal* $|G|$*.*

Nota*: Sea* $ord(b) = k$*. Si existe* $h \neq k \in \mathbb{N}$ *tal que* $b^h \equiv 1\ mod\ n$ *entonces* k *divide a* h*.*

Definición 2. *Dado un entero* p *primo, se dice que un entero positivo* $b < p$ *es una* ***raíz primitiva módulo*** p *si su orden módulo* p *es* $p - 1$*.*

Definición 3 (Función φ de Euler)**.** *Se define de la siguiente manera:*

$\varphi : \mathbb{N} \longrightarrow \mathbb{N}$

$n \longrightarrow cardinal\{k \in \mathbb{N} : m.c.d.(k, n) = 1, \quad 1 \leq k \leq n\}$

Se deduce fácilmente de la propia definición que n es primo si y solo si $\varphi(n) = n-1$. Además, $\varphi(p^k) = p^{k-1}(p-1)$, siendo p primo y k un entero positivo.

Teorema 1 (Euler)**.** *Sea* $a, n \in \mathbb{Z}$*. Si* $m.c.d.(a, n) = 1$ *entonces* $a^{\varphi(n)} \equiv 1\ mod\ n$*.*

Proposición 2. *Sea* G *un grupo finito y* $g \in G$*. Entonces:*

- *el* $ord(g)$ *divide a* $|G|$ *y se da la igualdad si* $< g >= G$*.*

- *si* $< g >= G$*, entonces* G *tiene exactamente* $\varphi(d)$ *elementos de orden* d *para cada divisor* d *del orden de* g*.*

Definición 4. *Sea* p *un número primo y* a *un entero no divisible por* p*. Se dice que* a *es un residuo cuadrático módulo* p *si existe otro entero* b *tal que*

$$a \equiv b^2 \ mod \ p$$

Definición 5 (Símbolos de Legendre y Jacobi)**.** *Sea* a *un entero positivo y* p *un número primo.*

- *Se define el símbolo de Legendre de* a *y* p *de la siguiente manera:*

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & si \quad a \text{ es residuo cuadrático módulo } p \\ -1 & si \quad a \text{ no es residuo cuadrático módulo } p \\ 0 & si \quad a \text{ es múltiplo de } p \end{cases}$$

- *Sea* $b = \prod_{p|b} p^{e_p}$ *un entero impar tal que* $m.c.d.(a, b) = 1$*. Entonces el símbolo de Jacobi generaliza el de Legendre para* a *y* b*:*

$$\left(\frac{a}{b}\right) = \prod_{p|b} \left(\frac{a}{p}\right)^{e_p}$$

$$\left(\frac{a}{-b}\right) = \begin{cases} \left(\frac{a}{b}\right) & si \quad a > 0 \\ - \left(\frac{a}{b}\right) & si \quad a < 0 \end{cases}$$

Es útil saber que la computación de requerida para calcular estos dos símbolos es aproximadamente la misma que para calcular el máximo común divisor.

1.1. Tests de primalidad

Para empezar esta sección, se dan algunos criterios teóricos.

Proposición 3. $p \in \mathbb{Z}$ *es primo si y solo si* $\mathbb{Z}/(p)$ *es un cuerpo.*

Aunque el siguiente teorema sea una equivalencia, resulta poco práctico a la hora de aplicarlo pues es computacionalmente muy caro.

Teorema 4 (Wilson)**.** *Sea* $p \in \mathbb{N}$*,* $p \geq 2$*. Entonces* p *es primo si y solo si* $(p-1)! \equiv -1 \ mod \ p$*.*

Teorema 5 (Dirichlet,1837)**.** *Sea* $d \geq 2$ *y* $a \neq 0$ *tales que* $m.c.d.(d, a) = 1$*. Se considera la sucesión* $\{u_k\}_{k \geq 0}$ *definida por* $u_k = a + kd$*. Entonces existen infinitos* k *para los cuales* u_k *es un número primo.*

Lema 6. *Si* $a^n + 1$ *es un número primo, entonces* n *es una potencia de* 2*.*

Demostración. Sea $n = gd$, siendo g un entero mayor o igual que 1 y d impar. Puesto que d es impar, -1 es raíz de $x^d + 1$. Se considera entonces el polinomio $x^n + 1$ que se puede factorizar como sigue:

$$((x^g)^d + 1) = (x^g + 1)(x^{g(d-1)} - x^{g(d-2)} + x^{g(d-3)} - ... - x^g + 1)$$

Ninguno de los dos factores puede ser unidad y por tanto $a^n + 1$ es compuesto. □

Lema 7. *Si $a^n - 1$ es un número primo, entonces a es 2 y n es primo.*

Demostración. Se considera el polinomio

$$x^{pq} - 1 = (x^p - 1)(x^{p(q-1)} + x^{p(q-2)} + ... + x^p + 1)$$

Si n es compuesto, por ejemplo $n = pq$ con $1 < p, q < n$, entonces $a^{pq} - 1$ es divisible por $a^p - 1$, es decir, $a^{pq} - 1$ es compuesto.

Sean n y $a^n - 1$ números primos. Se considera

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + ... + x + 1)$$

Se tiene que $a - 1$ es un divisor de $a^n - 1$ y, por consiguiente, $a - 1 = 1$ □

El recíproco no es cierto. Basta tomar, por ejemplo, $n = 11$ y ver que $2^{11} - 1 = 23 \cdot 89$.

Definición 6. *Se dice que un número es de Mersenne si es de la forma $2^n - 1$ y de Fermat si es de la forma $2^{2^n} + 1$. De la misma manera se dice que un primo es de Mersenne (respectivamente de Fermat) si es un número de Mersenne (respectivamente de Fermat) que es primo.*

Fermat pensaba que todos los números de Fermat eran primos, pero Euler rebatió esta idea al calcular un divisor de $2^{2^5} + 1$. Desde entonces la conjetura de los primos de Fermat afirma que n solo puede ser $1, 2, 4, 8$ o 16.

El estudio de la distancia entre k números primos en cualquier conjunto de enteros consecutivos ha dado lugar a varias conjeturas y aquí veremos una en particular. Para enunciarla correctamente hay que dar primero unas condiciones sobre estos conjuntos de manera que no haya ningún problema para encontrar los k números primos buscados. Por ejemplo, en un conjunto de la forma $\{2n, 2n + 1, 2n + 2\}$, la única forma de encontrar dos números primos es que n sea 1, si no, se encuentra máximo un número primo, que sería el único impar del conjunto.

Definición 7 (Admisible)**.** *Sea $D = \{a_1 z + b_1, ..., a_k z + b_k\}$, con a_i, $b_i \in \mathbb{Z}$. Se dice que D es admisible si para todo primo p existe un $z \in \mathbb{N}$ tal que p no divide a $(a_1 z + b_1) \cdot (a_2 z + b_2) \cdot ... \cdot (a_k z + b_k)$.*

La conjetura de Dickson afirma que dado un conjunto $D = \{a_1 z + b_1, ..., a_k z + b_k\}$ admisible, si $k \geq 2$, entonces existen infinitos $z \in \mathbb{N}$ de manera que todos los elementos de D sean primos simultáneamente. Un caso particular de esta conjetura es la de los primos gemelos, en la que D es el conjunto $\{p, p + 2\}$.

Teorema 8 (Pequeño teorema de Fermat)**.** *Si p es primo, entonces para todo $a \in \mathbb{Z}$ se tiene $a^p \equiv a \ mod\ p$. En particular, si $p \nmid a$ entonces $a^{p-1} \equiv 1 \ mod\ p$.*

Hoy en día es bien sabido que la recíproca de este teorema no es cierta, pero durante mucho tiempo no fue así. En cualquiera de los dos casos, si se escribe $p = 2^s d+1$ donde d es un número impar, entonces para que $a^{p-1} \equiv 1 \bmod p$, basta con que $a^d \equiv 1 \bmod p$ o que $a^{2^s} \equiv 1 \bmod p$, y de hecho, esta última condición se da si $a^{2^i} \equiv \pm 1 \bmod p$ para algún $0 < i < s$.
Estas condiciones son más fuertes y han servido para construir tests de primalidad que buscan dar una pseudorecíproca del pequeño teorema de Fermat.

Teorema 9 (Test de Lucas(1891))**.** *Sea $n \in \mathbb{N}$, $n > 1$. Si existe $b \in \mathbb{Z}$ tal que*

- $b^{n-1} \equiv 1$ *mod* n
- $b^m \not\equiv 1$ *mod* n *para cada* $m < n$ *que sea divisor de* $n-1$

Entonces n es primo.

Demostración. De la primera condición se deduce que el orden de b en $\mathbb{Z}/(n)$ divide a $n-1$ y por la segunda condición, ningún otro $m < n$ que divide a $n-1$ puede ser igual a $ord(b)$. Se concluye entonces que el orden de b módulo n es $n-1$.

El orden de b divide al del grupo multiplicativo $(\mathbb{Z}/(n))^*$ (unidades de $\mathbb{Z}/(n)$) y por tanto$(\mathbb{Z}/(n))^* = (\mathbb{Z}/(n)) \setminus \{0\}$. Esto implica que $\mathbb{Z}/(n)$ es un cuerpo y por lo tanto n es primo. □

Este test fue perfeccionado posteriormente por Brillhart, Lehmer y Selfridge en 1967.

Teorema 10. *Sea $n \in \mathbb{N}$, $n > 1$, y se supone que para cada factor primo q de $n-1$ existe un entero $b_q > 1$ tal que:*

- $b_q^{n-1} \equiv 1$ *mod* n
- $b_q^{(n-1)/q} \not\equiv 1$ *mod* n

Entonces n es primo.

Demostración. Como $\varphi(n) \leq n-1$, si probamos que $n-1 | \varphi(n)$ entonces $\varphi(n) = n-1$ y estará probada la primalidad de n.
Supongamos que $n-1 \nmid \varphi(n)$, entonces existe un primo q y un exponente r tal que $q^r | n-1$ y $q^r \nmid \varphi(n)$. Por hipótesis, existe un b_q tal que $ord(b_q) | n-1$ (1ª condición) y tal que $ord(b_q) \nmid (n-1)/q$ (2ª condición).

Por tanto, $q^r | ord(b_q)$.

Como $b^{\varphi(n)} \equiv 1 \bmod n$ (teorema de Euler), se tiene $ord(b) | \varphi(n)$, luego $q^r | \varphi(n)$,lo que contradice lo anterior.

□

Teorema 11 (Test de Pocklington)**.**
Sea $n \in \mathbb{N}$, $n > 1$ tal que $n-1 = F \cdot R$ con $F, R \in \mathbb{N}$ y $F \geq \sqrt{n}$.
Se supone además que la factorización de F es conocida y que existe $b \in \mathbb{Z}$ tal que

- $b^{n-1} \equiv 1$ *mod* n
- $m.c.d(b^{(n-1)/q} - 1, n) = 1$ *para cada primo q que divide a F.*

Entonces n es primo.

Demostración. Sea p un factor primo de n, veamos que p es de la forma $kF+1$.
Como p divide a n y n divide a $b^{n-1}-1$ (por la primera condición), entonces $b^{n-1} \equiv 1 \bmod p$ o, lo que es lo mismo, $(b^R)^F \equiv 1 \bmod p$. Se deduce que el orden de $b^R \bmod p$ divide a F.

Por otro lado, como $m.c.d(b^{(n-1)/q}-1, n) = 1$ para cada primo q que divide a F y p es un divisor primo de n, se tiene que $b^{(n-1)/q} = (b^R)^{F/q} \not\equiv 1 \bmod p$. Luego el orden de $b^R \bmod p$ no es un divisor propio de F y en consecuencia $ord(b^R) \bmod p = F$.

Finalmente, por el pequeño teorema de Fermat, $(b^R)^{p-1} \equiv 1 \bmod p$, por lo tanto $ord(b^R) = F$ divide a $p-1$. Reescribiendo, queda $p = kF+1$ para algún $k \in \mathbb{Z}$.

Para concluir, basta con ver que $F \geq \sqrt{n}$ implica $p > \sqrt{n}$ y por lo tanto n es primo. □

Teorema 12 (Test de Proth)**.** *Sea $n = 2^k h + 1$ con $2^k > h$.*
Si existe $b \in \mathbb{Z}$ tal que $b^{(n-1)/2} \equiv -1$ mod n, entonces n es primo.

Demostración. Escribiendo $F = 2^k$ y $R = h$, queda comprobar que se cumplen las hipótesis del test de Pocklington.
Primero, está claro que $b^{n-1} \equiv 1 \bmod n$.
Segundo, el único primo que divide a F es 2, entonces se tiene $m.c.d.(b^{(n-1)/2}-1, n) = m.c.d.((b^{(n-1)/2}+1)-2, n) = m.c.d.(kn-2, n) = m.c.d.(-2, n)$ y por ser n impar, este $m.c.d.$ es 1.
Finalmente, $2^k > h \Rightarrow 2^{2k} > 2^k h \Rightarrow F^2 > n-1 \Rightarrow F^2 \geq n$. Por el teorema anterior, n es primo. □

Teorema 13 (Test de Miller)**.** *Sea $n \in \mathbb{Z}$ impar. Sea $s \geq 0$ y d un entero impar tal que $n = 2^s d + 1$. Si existe algún $a \in \mathbb{Z}$ que cumpla :*

- $1 < a < 2 \cdot log(n)^2$
- $m.c.d(a, n) = 1$
- $a^d \not\equiv 1$ *mod* n
- $a^{2^r d} \not\equiv -1$ *mod* n, $0 \leq r < s$

entonces n es compuesto. Si no, n es primo.

El siguiente test está basado en el de Miller.

Teorema 14 (Test de Rabin-Miller)**.** *Sea $n \in \mathbb{Z}$. Se escribe $n-1 = 2^s d$, siendo d un entero impar y $s \geq 0$.*

- *Se escogen aleatoriamente $k \geq 1$ números a tales que $1 < a < n$ y $m.c.d(a, n) = 1$.*
- *Se verifica sucesivamente si para cada base a escogida se cumple una de las dos condiciones siguientes: (i) $a^d \equiv 1$ mod n (ii) $a^{2^r d} \equiv -1$ mod n para algún $0 \leq r < s$.*

Si se encuentra un a para el cual no se cumple ni (i) ni (ii), entonces n es compuesto. Si no, la probabilidad de que N sea primo es al menos $1 - 1/4^k$.

Estos son solo algunos ejemplos para ilustrar los tests de primalidad. Además de la importancia de algunos, por ejemplo el de Rabin-Miller que proporciona un método eficiente para encontrar números primos, lo interesante es que la mayoría tiene una primera hipótesis muy similar al pequeño teorema de Fermat.

Hay otros tipos, por ejemplo los basados en las sucesiones de Lucas que también han sido objeto de estudio y aunque aquí no es interesante desarrollar este tema, se introducirán dichas sucesiones que servirán para explicar el test de Baillie-PSW. Se pueden definir recurrentemente dando los primeros términos o solucionando la correspondiente ecuación en diferencias, son equivalentes las dos cosas.

Definición 8 (Sucesiones de Lucas)**.** *Sean P y Q dos enteros no nulos. Dados los términos iniciales $U_0 = 0$ y $U_1 = 1$, se define la recurrencia:*

$$U_n = PU_{n-1} - QU_{n-2}$$

De la misma manera, dados $V_0 = 2$ y $V_1 = P$, se define:

$$V_n = PV_{n-1} - QV_{n-2}$$

Ahora, se considera el polinomio mónico característico de las sucesiones: $X^2 - PX + Q$, su discriminante $\delta = P^2 - 4Q$ y sus raíces $\dfrac{P \pm \sqrt{\delta}}{2}$. La solución general es

$$A\left(\frac{P - \sqrt{\delta}}{2}\right)^n + B\left(\frac{P + \sqrt{\delta}}{2}\right)^n$$

Imponiendo las condiciones iniciales de la definición se obtiene $A = \dfrac{1}{\frac{P+\sqrt{\delta}}{2} - \frac{P-\sqrt{\delta}}{2}}$ y $B = \dfrac{-1}{\frac{P+\sqrt{\delta}}{2} - \frac{P-\sqrt{\delta}}{2}}$ para el caso de $\{U_n\}$ y $A = B = 1$ para $\{V_n\}$.

Ejemplos $\{V_n\}$ con parámetros $P = 1$ y $Q = -1$ y $\{U_n\}$ es la sucesión de Fibonacci:

$$2, 1, 3, 4, 7, 11, ...$$

$\{U_n\}$ con parámetros $P = 3$ y $Q = 2$ es la sucesión de números de Mersenne:

$$0, 1, 3, 7, 15, 31, ...$$

Nota: En muchos casos, en vez de decir cuánto valen exactamente P y Q, se da solo el valor de Δ.

Teorema 15. *Se considera la sucesisón de Lucas definida antes $\{U_n\}_{n\geq 0}$ y sea p un número primo tal que m.c.d.$(p, 2Q\Delta) = 1$. Se tiene:*

$$U_{p-(\frac{\Delta}{p})} \equiv 0 \ mod\ p$$

Cabe aclarar que hoy en día los mayores avances en tests de primalidad han sido con curvas elípticas y enteros algebraicos que aquí no mencionaremos.

1.2. Pseudoprimos, Pseudoprimos fuertes y pseudoprimos de Lucas

Después de definirlos, se darán unas propiedades que, o bien se utilizarán más adelante, o bien tendrán su análogo para los números de Carmichael.

El primer tipo de números son los que cumplen la hipótesis común a todos los tests de la sección anterior, es decir, los que cumplen la conclusión del teorema de Fermat para un b particular que llamaremos **base**.

Definición 9 (Pseudoprimo en base a)**.** *Es un número compuesto $n \in \mathbb{Z}$ tal que $a^{n-1} \equiv 1$ mod n.*

Históricamente, los pseudoprimos en base 2 (también llamados pseudoprimos o números de Poulet) son los más importantes, pues durante mucho tiempo se dijo que en la antigua China se consideraba la definición de este tipo de números como un criterio de primalidad, y de hecho terminó siendo una importante conjetura conocida como *Problema Chino* que, al parecer, algunos matemáticos dieron por sentada [31], por ejemplo Leibniz(1680). Incluso en el artículo [13], de los años 90, Granville afirma que fueron los *antiguos chinos* quienes hicieron dicha afirmación.

Creer que la definición 9 fuera un criterio de primalidad no es de extrañar, teniendo en cuenta la falta de tecnología en la época y que relativamente a la cantidad de números primos, hay muy pocos pseudroprimos de este tipo. Por ejemplo, hay 450 millones de primos menores que 10^{10}, pero solo hay alrededor de 15 mil pseudoprimos en base 2 en el mismo rango [13]. Por esta razón, hubo un tiempo en el que se creyó que había una cantidad limitada, pero Malo demostró en 1903 que existía una contrucción recurrente.

El teorema de Malo se puede ver como una pseudo-recíproca del lema 7.

Teorema 16. *Si $n \in \mathbb{N}$ es un pseudoprimo en base 2, entonces $m = 2^n - 1$ también lo es.*

Demostración.
1. m **no es primo.** Para esto, basta con encontrar 2 divisores propios distintos. Se escribe $n = ab$, con $a, b \notin \{1, n\}$. Como $2^a \equiv 1 \bmod (2^a - 1)$, se tiene $2^{ab} \equiv 1^b \bmod (2^a - 1)$, es decir, $2^a - 1$ divide a $2^{ab} - 1$. Análogamente, $2^b - 1$ divide a $2^{ab} - 1$.
2. [$2^{m-1} \equiv 1$ **mod** m] Se sabe que $2^{n-1} \equiv 1 \bmod n \Rightarrow 2^n \equiv 2 \bmod n$. Como $2^n - 2 = m - 1$, entonces n divide a $m - 1$. Por un razonamiento análogo al de **1**, se tiene que $2^n - 1$ divide a $2^{m-1} - 1$ y esto es lo que se quería demostrar. □

Para que la recurrencia de Malo tenga sentido, debe existir al menos un pseudoprimo y el primero en encontrarlo fue Sarrus en 1819 [33]

$$n = 341 = 11 \cdot 31 \text{ y } 2^{340} \equiv 1 \bmod 341$$

Su demostración fue la siguiente:
De $2^5 - 1 = 31$ y $2^5 + 1 = 33$ se deduce $2^{10} - 1 = 33 \cdot 31 = 341 \cdot 3$. Por tanto,

$$2^{170} = (341 \cdot 3 + 1)^{17} \Rightarrow 2^{170} = 341 \cdot k + 1 \text{ con } k \text{ natural}$$

Es decir $2^{170} \equiv 1 \bmod n \Rightarrow 2^{170 \cdot 2} \equiv 1 \bmod n$.

Antes se mencionó un ejemplo de la cantidad de pseudoprimos en base 2 que se pueden encontrar. Como parecen pocos, hubo un breve lapso de tiempo en el que se consideró la

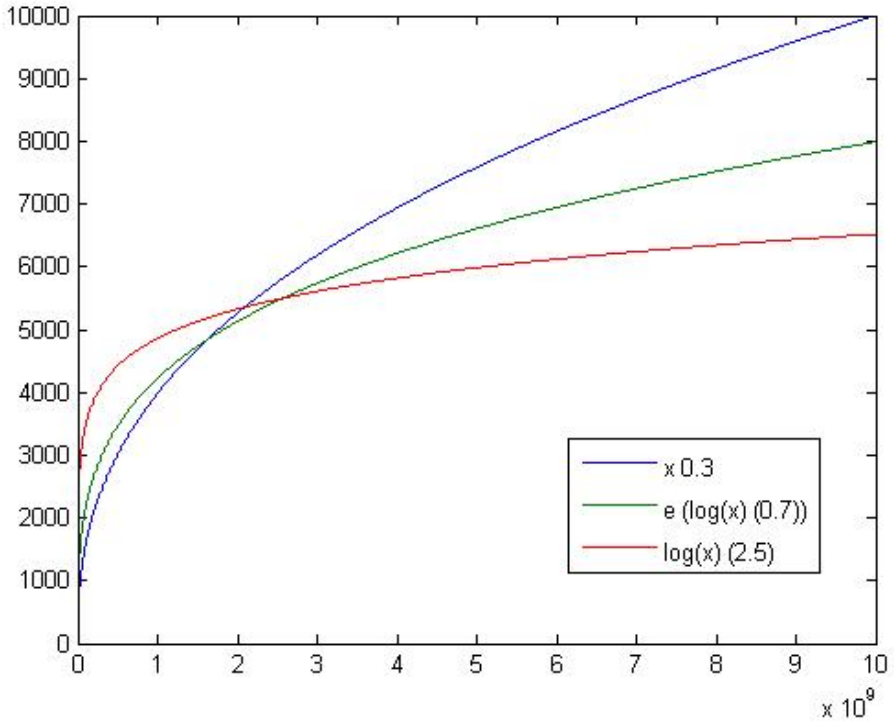


Figura 1.1: Ejemplo para ilustrar el crecimiento de $\mathcal{P}(x) > e^{log(x)^\alpha}$

posibilidad de listarlos hasta cierto valor x, según la necesidad, de manera que se pudiera afirmar, sin ninguna duda, la primalidad de un número n que dividiera a $2^n - 2$ y no estuviera en la lista.

Proposición 17 ([27]). *Sea $\mathcal{P}(x)$ la cantidad de pseudoprimos en base 2 menores que un $x \in \mathbb{R}$ dado y α una constante positiva menor que la unidad. Entonces*

$$\mathcal{P}(x) > e^{log(x)^\alpha}$$

Está claro que la idea no iba a funcionar, pues para un x muy grande la lista ya sería inmanejable.

Se ha desarrollado el caso particular para base 2, sin embargo se puede demostrar en general que hay infinitos pseudoprimos en base a. Hay muchas pruebas de este hecho, por ejemplo:

Teorema 18 (Cipolla, 1904). *Sea $a \geq 2$ un entero y p un primo impar que no sea un divisor de $(a^2 - 1)$. Entonces el producto*

$$n = \frac{a^p - 1}{a - 1} \cdot \frac{a^p + 1}{a + 1}$$

es un pseudoprimo en base a.

Demostración. Evidentemente, n es compuesto. Basta con probar que $a^{n-1} \equiv 1 \bmod n$ para ver que es pseudoprimo en base a. Se tiene:

$$n - 1 = \frac{a^{2p} - a^2}{a^2 - 1}$$

y por el pequeño teorema de Fermat,

$$a^{2p} \equiv a^2 \mod p$$

por tanto p divide a $a^{2p} - a^2 = (n-1)(a^2-1)$ y puesto que por hipótesis p no divide a $a^2 - 1$, se concluye que p divide a $n-1$.
Por otro lado, escribiendo $n = (a^{2p}-1)/(a^2-1)$, se identifica n con las sumas parciales de una serie geométrica de razón a^2, por lo tanto se puede escribir $n = 1 + a^2 + ... + a^{2(p-1)}$. Como p es impar, $n-1$ se puede expresar como la suma de una cantidad par de términos de misma paridad lo que implica que $n-1$ es par.

En consecuencia, $2p$ divide a $n-1$ y se puede escribir $n-1 = 2pH$. Teniendo en cuenta que $a^{2p} \equiv 1 \mod (a^{2p}-1)$, se deduce que $a^{2p}-1$ divide a $a^{2pH}-1 = a^{n-1}-1$ o lo que es lo mismo, $n(a^2-1)$ divide a $a^{n-1}-1$. □

Este teorema demuestra que hay infinitos pseudoprimos en cualquier base pues al haber infinitos primos, existen infinitos productos para cada a.

Teorema 19 (Crocker [9])**.** *Sea a un entero par que no se pueda escribir como 2^{2^r}, $r \in \mathbb{N}\setminus\{0\}$. Entonces para todo $n \geq 1$, $a^{a^n}+1$ es un pseudoprimo en base a.*

Demostración. Veamos que $a^{a^n}+1$ es compuesto. Supongamos que $a^{a^n}+1$ es primo y apliquemos el lema 6. Se tiene $a^n = 2^k$, en particular $a = 2^m$ y por hipótesis $m \neq 2^r$, por tanto será $m = 2^r d$, con $d > 1$ impar. Luego, $a^{a^n}+1 = 2^{2^r d a^n}+1 = 2^{2^{r+k}d}+1$ y volviendo a aplicar el lema 6, $2^{r+k}d$ debe ser una potencia de 2. Contradicción.

Por otro lado, como consecuencia de la paridad de a, 2 divide a a^{a^n-n}. Dicho de otra manera, existe un entero H tal que $a^{a^n-n} = 2H$ y por tanto $a^{a^n} = 2a^n H$.

$$a^{2a^n} \equiv 1 \mod (a^{2a^n}-1), \text{ luego } a^{2a^n H} = a^{a^{a^n}} \equiv 1 \mod (a^{2a^n}-1)$$

Para concluir, basta con observar que $a^{2a^n}-1 = (a^{a^n}-1)(a^{a^n}+1)$ implica que $a^{a^n}+1 = N$ divide a $a^{a^{a^n}}-1 = a^{N-1}-1$ □

A diferencia del teorema de Cipolla, el de Crocker no utiliza números primos en su construcción, lo que lo vuelve más práctico a la hora de calcular pseudoprimos en bases pares.

La siguiente pregunta es qué se puede saber sobre la factorización de estos números, por ejemplo si pueden tener un número arbitrario de factores primos. En 1958, Schinzel demostró que para cualquier base a, existen infinitos pseudoprimos con exactamente 2 factores primos y en su tesis doctoral, Lieuwens (1971) demostró que en general para cualquier base a hay infinitos pseudoprimos en base a que son producto de exactamente k factores primos. (ver [31], capítulo VIII).

Ya estudiamos cómo construir pseudoprimos en cualquier base y sabemos que pueden tener un número arbitrario de factores primos, pero aún no hemos visto que además se pueden construir pseudoprimos con tantos factores primos como se quiera o que sean pseudoprimos para más de una base. Este capítulo estará limitado a dar un pequeño ejemplo de construcción que es muy similar al de las formas de Chernick que se verán más adelante.

Proposición 20 (Shanks, 1978)**.** *Sea m un entero tal que $12m+1$ y $24m+1$ sean primos simultáneamente. Entonces el producto $(12m+1)(24m+1)$ es un pseudoprimo para las bases 2 y 3.*

Hemos calculado algunos ejemplos de este teorema:

m	$12m+1$	$24m+1$
3	37	73
8	97	193
13	157	313
19	229	457
28	337	673
48	577	1153
50	601	1201
55	661	1321
69	829	1657

Es más, dado un entero natural n, está demostrado que el número de bases, coprimas con n, para las cuales n es pseudoprimo está dado por

$$\prod_{p|n} m.c.d.(n-1, p-1) - 1$$

Como consecuencia, cualquier entero impar n que no sea una potencia de 3 es pseudoprimo para al menos dos bases menores que $n-1$. Por ejemplo, el número $7 \cdot 5$ es pseudoprimo para las bases 6, 29 y 34 y el número $7 \cdot 5 \cdot 13$ es pseudoprimo para 7 bases menores que $7 \cdot 5 \cdot 13 - 1$.

Otra propiedad interesante sobre la factorización de pseudoprimos es que son « casi libres de cuadrados»:

Proposición 21. *([29]) Sean $r > 1$ un entero, p un primo y n un pseudoprimo en base a tales que $p^r | n$. Entonces $a^{p-1} \equiv 1 \ mod\ p^r$. Recíprocamente, si $a^{p-1} \equiv 1 \ mod\ p^r$ para algún primo impar p y $r > 1$, entonces p^r es un pseudoprimo en base a.*

Demostración. Se supone primero que $n = p^r t$ es pseudoprimo en base a. Por definición se tiene:

$$a^{n-1} \equiv 1 \bmod n \Rightarrow a^n \equiv a \bmod n \Rightarrow a^n \equiv a \bmod p^r \Rightarrow (a^n)^{p-1} \equiv a^{p-1} \bmod p^r$$

Por tanto,

$$a^{p-1} \equiv a^{n(p-1)} \equiv a^{p^r t(p-1)} \equiv a^{tp^r(p-1)} \bmod p^r$$

Y reescribiendo $p^r(p-1) = pp^{r-1}(p-1) = p\varphi(p^r)$, se aplica el teorema de Euler para obtener el resultado buscado:

$$a^{p-1} \equiv a^{\varphi(p^r)tp} \equiv 1^{tp} \bmod p^r$$

□

En particular, que un pseudoprimo n en base a tenga algún factor cuadrado equivale a aplicar el teorema anterior con $r = 2$, y entonces se cumpliría que $a^{p-1} \equiv 1 \bmod p^2$ para algún factor primo p de n. Pero esta congruencia es rara, por ejemplo, solo existen 4 pseudoprimos en base 2 menores que $25 \cdot 10^9$ con algún factor cuadrado [29]. Como veremos más adelante, esta propiedad se reafirma con los números de Carmichael.

Para la siguiente definición, viene bien recordar los tests de primalidad basados en el teorema 8.

Definición 10. *Sea n un número impar compuesto y tal que $n-1 = d2^s$, con d impar y $s > 1$. Entonces n es un pseudoprimo fuerte si cumple alguna de las siguientes condiciones:*

- $a^d \equiv 1 \ mod\ n$
- $a^{d2^i} \equiv -1 \ mod\ n$ *para algún* $0 \leq i < s$

Dos ejemplos de pseudoprimos fuertes en base 2 son los ya mencionados números de Fermat y los números de Mersenne que sean de la forma $2^p - 1$, con p primo, excluyendo, por supuesto, los casos primos. De hecho se puede completar el teorema 16 (de Malo)con la siguiente proposición:

Proposición 22. *([29]) Si n es un pseudoprimo en base 2, entonces $2^n - 1$ es un pseudoprimo* ***fuerte*** *en base 2.*

Para terminar el capítulo, se definen los pseudoprimos de Lucas, que son al teorema 15 lo que los pseudoprimos son al pequeño teorema de Fermat.

Definición 11. *Sea P y Q dos enteros no nulos y $\Delta = P^2 - 4Q$. Se considera la sucesión de lucas $\{U_n\}_{n\geq 0}$ como se definió en 8. Si un entero compuesto n cumple $U_{n-(\frac{\Delta}{n})} \equiv 0 \ mod\ n$ entonces se dice que es un pseudoprimo de Lucas.*

Si $\{U_n\}$ se toma, como antes, con parámetros $P = 1$ y $Q = -1$, entonces dichos pseudoprimos se llaman pseudoprimos de Fibonacci.

Nota: Cuando se hable de *test de pseudoprimalidad*, de *test de pseudoprimalidad fuerte* o de *test de pseudoprimalidad de Lucas* se trata simplemente de verificar si el número testado cumple las condiciones para ser un pseudoprimo, un pseudoprimo fuerte o un pseudoprimo de Lucas; si es el caso, puede o bien ser un tal pseudoprimo o bien ser primo.

Para terminar el capítulo, se dará un último test de primalidad que combina dos tipos de tests de pseudoprimalidad.

Teorema 23 (test de Baillie-PSW)**.** *Sea $n \in \mathbb{Z}$.*

- *(Opcional)Se verifica divisibilidad por primos pequeños y si no se encuentran divisores propios se pasa al paso siguiente.*
- *Se efectúa un test de pseudoprimalidad fuerte en base 2. Si falla, entonces n es compuesto, si no, se pasa al paso siguiente.*
- *En la sucesión de Lucas $5, -7, 9, -11, 13, ...$ se busca el primer Δ tal que el símbolo de Jacobi $\left(\frac{\Delta}{n}\right)$ sea -1. Entonces se hace un test de pseudoprimalidad de Lucas con discriminante Δ. Si falla entonces n es compuesto, si no, es 'muy probablemente' primo.*

No se entrará en detalles, pero la fiabilidad de este test está reflejada en su uso práctico. Por ejemplo, la función *isprime* de Maple [1] o la función *PrimeQ* de Mathematica [2] que primero verifica que el número testado no sea divisible por primos pequeños, luego efectúa test de pseudoprimalidad fuerte en bases 2 y 3 y finalmente hace un test de Lucas. Pese a que no está rigurosamente probado que demuestre la primalidad de un número, a día de hoy no se ha encontrado ningún contraejemplo.

[1] Ver http://www.maplesoft.com/support/help/maple/view.aspx?path=isprime
[2] Ver https://reference.wolfram.com/language/tutorial/SomeNotesOnInternalImplementation.html

Capítulo 2

Números de Carmichael

Recordemos que al principio de la sección anterior se introdujeron los pseudoprimos y se hizo un pequeño estudio de factorización y bases, así que es natural preguntarse qué pasa con los números que son pseudoprimos para cualquier base, es decir los que cumplen exactamente la recíproca de Fermat. Estos son los números que se llaman de Carmichael y que constituyen el principal objeto de estudio de este trabajo.

Definición 12 (Número de Carmichael)**.**

Un número $n \in \mathbb{N}\backslash\{1\}$ es de Carmichael si no es primo y cumple que $a^{n-1} \equiv 1$ mod n, para todo a, $1 < a < n$ tal que $mcd(a, n) = 1$.

De manera equivalente a la definición que dio Carmichael en 1912, se puede escribir:

Un número compuesto $n \in \mathbb{N}\backslash\{1\}$ es de Carmichael si $a^n \equiv a$ mod n para cada $a \in \mathbb{Z}$.

Después del enunciado de Fermat en 1640, en la búsqueda por saber si la recíproca era cierta o no, Korselt probó en 1899 el siguiente teorema que proporciona una definición alternativa para los números de Carmichael.

Teorema 24. *Sea $n \in \mathbb{N}$. Se tiene que $a^n \equiv a$ mod n, para todo entero a, si y solo si n cumple las siguientes condiciones:*

- *n es libre de cuadrados*
- *$p - 1|n - 1$ para todos los divisores primos p de n.*

Demostración.

- Se supone primero que para todo $a \in \mathbb{Z}$, $a^n \equiv a \bmod n$.

  Veamos que n no tiene factores cuadrados. Sea p un divisor primo de n. Por hipótesis, $p^n \equiv p \bmod n$, es decir, $n|p^n - p$ y $p^n - p = p(p^{n-1} - 1)$. Si p^2 dividiera a n, en particular dividiría a cualquier múltiplo suyo como lo es $p(p^{n-1} - 1)$; esto significaría que $p|p^{n-1} - 1$ y hemos llegado a un absurdo.

  Ahora veamos que $p - 1|n - 1$ si p es primo y $p|n$. Sea p como acabamos de decir y sea a una raíz primitiva módulo p. Se tiene,

$$a^n \equiv a \bmod n \Rightarrow a^n \equiv a \bmod p$$

Obviamente p no divide a a, por lo tanto $a^{n-1} \equiv 1 \bmod p$. Esto implica que $ord(a) \bmod p$ divide a $n-1$ y, por definición, el orden de a módulo p es justamente $p-1$.

- Ahora se supone que n cumple las dos condiciones del enunciado y veamos que $a^n \equiv a \bmod n$, para todo entero a.

  Teniendo en cuenta que n no tiene ningún factor cuadrado, por el teorema chino de los restos, basta con ver que para todo entero a, $a^n \equiv a \bmod p$ para todo factor primo p de n.

  Por el pequeño teorema de Fermat, dado un p de estos, se tiene $a^p \equiv a \bmod p$. Además hay 2 opciones: o bien $p \nmid a$ o bien $p|a$.

  En el primer caso se tiene que $a^{p-1} \equiv 1 \bmod p$ y por la segunda condición, $n-1 = (p-1)k$, $k \in \mathbb{N}$. Por tanto $a^{n-1} = a^{(p-1)k} \equiv 1 \bmod p$ y así $a^n \equiv a \bmod p$.

  En el segundo caso, $p|a$ es lo mismo que decir $a \equiv 0 \bmod p$ y está claro que $a^n \equiv a \bmod p$.

□

Viendo la importancia de este teorema, resulta inevitable pensar que los números de Carmichael en realidad deberían haberse llamado números de Korselt. El problema es que Korselt no encontró (o al menos no publicó) ningún número n con las propiedades enunciadas y por lo tanto no probó realmente que la recíproca del teorema 8 es falsa; en su publicación pretendía demostrar que el *problema chino* era falso, así que se limitó a dar un contraejemplo para probar la no primalidad de lo que hoy se llama un pseudoprimo en base 2. Como en ese momento ya se sabía que existían pseudoprimos(ver sección 1.2), el artículo no supuso ninguna novedad. El teorema 24 fue una adición bastante importante pero que pasó desapercibida.

Este teorema es una herramienta para demostrar la equivalencia de los dos enunciados dados en la definición 12. Veámoslo [20]:

Veamos que si para todo a coprimo con n, n cumple que $a^{n-1} \equiv 1 \bmod n$, entonces se verifican las hipótesis del teorema 24.
Supongamos que n tiene un factor primo cuadrado, $n = p_1^2 p_2 ... p_{k-1}$. Entonces $ord((\mathbb{Z}/(n))^*) = \varphi(n) = p_1(p_1-1)(p_2-1)...(p_{k-1}-1)$, y por el teorema de Cauchy para grupos, por ser p_1 primo, existe un elemento $a \in \mathbb{Z}$ tal que $ord(a) = p_1$. Por hipótesis,

$$a^{n-1} \equiv 1 \bmod n \text{ y } m.c.d.(a,n) = 1, \text{ luego } a^{n-1} = 1 \text{ en } (\mathbb{Z}/(n))^*$$

y por tanto $ord(a) = p_1$ divide a $n-1$, lo que no es posible pues p_1 divide a n.

Entonces $n = p_1 ... p_k$ es un producto de primos distintos, por lo tanto se tiene el isomorfismo de anillos

$$\mathbb{Z}/(n) \cong \mathbb{Z}/(p_1) \times ... \times \mathbb{Z}/(p_k)$$

y también el de sus correspondientes anillos de unidades (teniendo en cuenta que dados dos anillos A y B, $(A \times B)^* = A^* \times B^*$).
Como $\mathbb{Z}/(p_i)$ es un cuerpo finito para todo i, entonces $(\mathbb{Z}/(p_i))^*$ es un grupo cíclico de orden $p_i - 1$, por lo tanto existe un elemento $a_i \in (\mathbb{Z}/(p_i))^*$ de orden $p_i - 1$.
Así, el elemento $\alpha_i = (1, ..., 1, a_i, 1, ..., 1) \in (\mathbb{Z}/(n))^*$ tiene también orden $p_i - 1$. Como por hipótesis, $\alpha_i^{n-1} \equiv 1 \bmod n$, se puede concluir que $p_i - 1$ divide a $n-1$.

De esta manera hemos probado que la primera definición implica la segunda.

Recíprocamente, está claro que si $a^n \equiv a \bmod n$ para todo entero a, entonces n divide a $a^n - a = a(a^{n-1} - 1)$. Si además $m.c.d.(a, n) = 1$, entonces n no divide a a y por tanto divide a $a^{n-1} - 1$.

Ejemplo: Primeros números de Carmichael factorizados

$$3 \cdot 11 \cdot 17$$
$$5 \cdot 13 \cdot 17$$
$$7 \cdot 13 \cdot 19$$
$$5 \cdot 17 \cdot 29$$
$$7 \cdot 13 \cdot 31$$
$$7 \cdot 23 \cdot 41$$
$$7 \cdot 19 \cdot 67$$
$$5 \cdot 29 \cdot 73$$
$$7 \cdot 31 \cdot 73$$
$$13 \cdot 37 \cdot 61$$
$$7 \cdot 11 \cdot 13 \cdot 41$$
$$13 \cdot 37 \cdot 97$$
$$7 \cdot 73 \cdot 103$$
$$3 \cdot 5 \cdot 47 \cdot 89$$
$$7 \cdot 13 \cdot 19 \cdot 37$$
$$11 \cdot 13 \cdot 17 \cdot 31$$
$$7 \cdot 11 \cdot 13 \cdot 101$$

Capítulo 3

Función λ de Carmichael

3.1. La función λ y la función φ

Ya hemos utilizado la bien conocida función φ de Euler. Veamos ahora cómo está relacionada con los números de Carmichael.

Se sabe que $\varphi(p) = p-1$ si p es primo. En particular, $\varphi(p)$ divide a $p-1$. De ahí el siguiente planteamiento:

¿Existe algún n natural y no primo tal que $\varphi(n)$ sea un divisor (propio) de $n-1$?

Este problema fue expuesto por D.H Lehmer y sigue sin estar resuelto hoy en día, pero lo que sí está claro es que si dicho número existiera, sería de Carmichael. En efecto, por el teorema de Euler, para cada entero a tal que $m.c.d.(a,n) = 1$, se tiene que $a^{\varphi(n)} \equiv 1 \bmod n$ y como por hipótesis $\varphi(n) \cdot k = n-1$, siendo k un entero positivo no nulo, está claro que $a^{\varphi(n)k} \equiv 1 \bmod n$, es decir, $a^{n-1} \equiv 1 \bmod n$.

Además, Lehmer también probó en su momento que si $n-1 = k \cdot \varphi(n)$, entonces para $k = 2$, n debe tener al menos 7 factores primos y para $k = 3$, más de 32. En los años 80 se elevó la cifra a 14 para un k cualquiera y por si fuera poco, se demostró que n es mayor que 10^{20} [40, 31]. Para hacerse una idea comparativa, el menor número de Carmichael es producto de 3 primos y menor que 600.

Definición 13. *Se define la función λ* ***de Carmichael*** *de la siguiente manera:*

- *Para primos y potencias de primos:*

  $\lambda(2^r) = 2^{r-2}$ *para* $r \geq 3$

  $\lambda(p^r) = p^{r-1}(p-1)$ *para p primo impar o* $r \leq 2$

- *Para números compuestos:*

  $\lambda(2^r p_1^{r_1} ... p_s^{r_s}) = m.c.m.\{\lambda(2^r), \lambda(p_1^{r_1}), ..., \lambda(p_s^{r_s})\}$

Como consecuencia inmediata de la definición, si a y b son dos enteros positivos, entonces $\lambda(m.c.m.(a,b)) = m.c.m.(\lambda(a), \lambda(b))$.

La relación entre esta función y la de Euler es innegable, la diferencia entre una y otra es la que hay entre un producto y el mínimo común múltiplo de sus factores. Más precisamente:

Proposición 25. *Sea n un entero positivo. Se cumplen las siguientes propiedades.*

- *$\lambda(n)$ divide siempre a $\varphi(n)$. Si n es compuesto y lo dividen al menos 2 primos distintos, entonces se trata de un divisor propio.*
- *Existe un entero a, primo con n, tal que el orden de a módulo n es $\lambda(n)$. En cambio, si n es producto de 2 primos impares distintos o un múltiplo de $4p$, con p primo impar, entonces no existe ningún a tal que $ord(a) = \varphi(n)$ mod n.*

Nota: En particular, si n es una potencia de un primo, entonces siempre existe un entero a tal que $(ord(a) \bmod n) = \lambda(n) = \varphi(n)$.

El objeto principal del artículo donde Carmichael publicó la definición de su función por primera vez era, entre otros, enunciar varios teoremas entre los cuales encontramos la siguiente generalización del teorema de Euler.

Teorema 26 (R.D. Carmichael [5])**.** *Sea $a, n \in \mathbb{N} \setminus \{0\}$. Si $m.c.d.(a, n) = 1$ entonces*

$$a^{\lambda(n)} \equiv 1 \ mod\ n$$

Demostración. Sea $n = p_1^{s_1} p_2^{s_2} ... p_k^{s_k}$, donde los p_i son primos distintos.
Por el teorema de Euler, para cada $p_i^{s_i}$ se tiene: $a^{\varphi(p_i^{s_i})} \equiv 1 \bmod p_i^{s_i}$
Como los p_i son primos, se tiene $\lambda(p_i^{s_i}) = \varphi(p_i^{s_i})$. Además
$\lambda(n) = m.c.m.(\lambda(p_1^{s_1}), \lambda(p_2^{s_2}), ..., \lambda(p_k^{s_k}))$, con lo cual cada $\lambda(p_i^{s_i})$ divide a $\lambda(n)$, por tanto existen enteros H_i tales que $\lambda(n) = H_i \lambda(p_i^{s_i})$. Se tiene:

$$a^{\lambda(p_i^{s_i})} \equiv 1 \bmod p_i^{s_i}$$

$$\Downarrow$$

$$a^{H_i \lambda(p_i^{s_i})} \equiv 1 \bmod p_i^{s_i}$$

Es decir, para cada p_i se tiene $a^{\lambda(n)} \equiv 1 \bmod p_i^{s_i}$. Luego, por el teorema chino del resto,

$$a^{\lambda(n)} \equiv 1 \bmod \prod_{i=1}^{k} p_i^{s_i}$$

□

3.2. La función λ y los números de Carmichael

Ahora que ya conocemos la función λ, se puede buscar una relación con los números de Carmichael, más allá de la persona que les dio nombre.

Para empezar, se puede dar una definición alternativa para estos números:

Teorema 27. *Sea $n \in \mathbb{N} \setminus \{1\}$ un número compuesto. Entonces n es de Carmichael si y solo si $n \equiv 1$ mod $\lambda(n)$.*

Es un buen momento para comentar que, cuando Korselt enunció el teorema 24, en realidad estaba enunciando algo más parecido a esta versión. En la segunda condición, en vez de escribir que $p-1$ divide a $n-1$ para cada divisor primo p de n, escribió que el $m.c.m(p_1 - 1, ..., p_k - 1)$ divide a $n = p_1 ... p_k$. Algunos autores son fieles al criterio original ([37]), otros lo enuncian como hemos hecho aquí([18, 20], ver teorema 24) e incluso alguno atribuye a Carmichael el primer enunciado ([7]). Como son definiciones equivalentes y demostrarlo es sencillo, no daremos más importancia a este hecho.

Demostración.

- Supongamos primero que n es de Carmichael: $n = p_1...p_k$ con todos los p_i distintos y $a^{n-1} \equiv 1 \bmod n$ para cada a primo con n. Por la proposición 25, se puede elegir un a_0 de manera que $\lambda(n)$ sea el orden de a_0 mod n, y por tanto $\lambda(n)$ divide a $n-1$.

- Ahora supongamos que n cumple la hipótesis del teorema. Entonces $m.c.d.(\lambda(n), n) = 1$ (si no, existiría al menos un primo q que divide a $\lambda(n)$ y a n, luego dividiría a $n-1$ y a n). Primero, n no tiene factores cuadrados, pues en ese caso $\lambda(n) = m.c.m.(p_1-1, ..., \lambda(p_i^2), ..., p_k-1)$, con $\lambda(p_i^2) = \varphi(p_i^2) = p_i(p_i-1)$, y por tanto p_i dividiría simultáneamente a $\lambda(n)$ y a n, lo que, como se acaba de ver, no puede ser.
  Segundo, es obvio que cada $p_i - 1$ divide a $\lambda(n)$, que a su vez divide a $n-1$.
  Finalmente, como por hipótesis n no es primo, por el teorema 26, n es de Carmichael.

□

Este teorema permite empezar a demostrar algunas propiedades importantes de los números de Carmichael, por ejemplo:

Proposición 28. *Sea n un número de Carmichael. Entonces n es impar y tiene al menos 3 factores primos.*

Demostración. Como n es compuesto, supongamos que $n = q \cdot p$ con $p > q$, los dos primos. Por el teorema 24, $p-1$ divide a $n-1 = pq-1 = (p-1)q + (q-1)$, y por dividir al primer sumando, debe dividir también a $q-1$, lo que es absurdo pues $p-1 > q-1$.

Por otro lado, si n fuese par, entonces $n-1$ sería impar y divisible por $\lambda(n) = \lambda(2p_2...p_k) = m.c.m.(1, p_2-1, ..., p_k-1) = m.c.m.(p_2-1, ..., p_k-1)$. Para que esto sea impar, todos los $p_i - 1$ deben ser impares y la única posibilidad para que esto pase es que todos los p_i sean 2, pero ya sabemos que no puede haber factores repetidos. □

Otras propiedades de los números de Carmichael vienen directamente de restringir las posibilidades para λ y para eso basta con estudiar qué pasa cuando se aplica a un número de Carmichael. El resto de resultados de esta sección están recogidos en el artículo [37] de T.Wright.

Teorema 29. *Sea n un número de Carmichael y $l \in \mathbb{N}$. Entonces $\lambda(n)$ no puede ser de la forma 2^l.*

Demostración. Se supone que n es de Carmichael y $\lambda(n) = 2^l$. Como cada factor primo p_i de n debe cumplir que $p_i - 1$ divide a $\lambda(n) = m.c.m.(p_1 - 1, ..., p_k - 1)$, entonces cada p_i debe ser de la forma $2^{s_i} + 1$. Por lo tanto se puede escribir

$$n = \prod_{i=1}^{k} (2^{s_i} + 1)$$

Además, puesto que n es libre de cuadrados, todos los s_i han de ser distintos y en consecuencia, sin pérdida de generalidad, se puede suponer que $s_1 < s_2 < ... < s_k \Leftrightarrow s_1 + 1 \leq s_2 < ... < s_k$. De esta manera, 2^{s_1+1} divide a 2^{s_i} para todo $i \in \{2, ..., k\}$ y reduciendo módulo 2^{s_1+1} queda:

$$n \equiv 2^{s_1} + 1 \bmod (2^{s_1+1}) \tag{3.1}$$

Por el teorema 27, $\lambda(n) = 2^{max\{s_1,...,s_k\}} = 2^{s_k}$ divide a $n-1$, luego 2^{s_1+1} también es un divisor de $n-1$, es decir

$$n \equiv 1 \bmod 2^{s_1+1} \tag{3.2}$$

Reemplazando (3.2) en (3.1) obtenemos

$$1 \equiv 2^{s_1} + 1 \bmod 2^{s_1+1}, \text{ luego } 2^{s_1+1} \text{ divide a } 2^{s_1}$$

Contradicción. □

Corolario 30. *Un número de Carmichael no puede ser de la forma $2^l + 1$, $l \in \mathbb{N}$, ni estar totalmente compuesto por primos de Fermat.*

Demostración. Si un número n se escribe como producto de primos de Fermat $(2^{s_1}+1)\cdot ... \cdot (2^{s_k}+1)$, entonces $\lambda(n) = m.c.m.(2^{s_1}, ..., 2^{s_k}) = 2^{max\{s_1,...,s_k\}}$ y por el teorema anterior, n no puede ser de Carmichael.

De la misma manera, si $n = 2^l + 1$ es de Carmichael, entonces $\lambda(n)$ divide a 2^l, por lo tanto ha de ser una potencia de 2, lo que contradice el teorema. □

Se considera entonces $\lambda(n) = 2^l \cdot P$, con P primo impar. En este caso, cada factor primo p de n debe ser tal que $p-1$ divida a $\lambda(n)$, por tanto será de la forma $2^{s_i}+1$ o $2^{r_j}P+1$.

Proposición 31. *Sea $n = p_1...p_k$ un número de Carmichael tal que $\lambda(n) = 2^l P$, con P primo. Entonces hay por lo menos un índice i y un índice j tales que $p_i = 2^{r_i}+1$ es un primo de Fermat y $p_j = 2^{s_j}P + 1$. Además, el menor de los r_i es igual al menor de los s_j.*

Demostración. Por el corolario 30, ya se sabe que los factores primos de n no pueden ser todos de Fermat. Ahora, supongamos que

$$n = \prod_{j=1}^{k} (2^{s_j}P + 1)$$

Se llega a una contradicción si se sigue la demostración del teorema 29 desde que se escribe n como producto de primos de Fermat, cambiando 2^{r_i} por $2^{s_j}P$.
Luego podemos escribir

$$n = \prod_{i=1}^{k_1} (2^{r_i}+1) \prod_{j=1}^{k_2} (2^{s_j}P + 1), \text{ con } r_1 < ... < r_{k_1} \text{ y } s_1 < ... < s_{k_2}$$

Supongamos que $r_1 < r_2 \leq s_1$. Se razona igual que para el teorema 29:
2^{r_1+1} divide a 2^{r_i} y a 2^{s_j} para todo $i \in \{2, ..., k_1\}$ y $j \in \{1, ..., k_2\}$, luego $n \equiv 2^{r_1}+1 \bmod 2^{r_1+1}$.
Además, $\lambda(n) = 2^l P = 2^{r_1+1}A$, $A \in \mathbb{Z}$, así que 2^{r_1+1} divide a $\lambda(n)$ y en consecuencia divide también a $n-1$.

$$\left.\begin{array}{ll} n \equiv 2^{r_1}+1 & \bmod 2^{r_1+1} \\ n \equiv 1 & \bmod 2^{r_1+1} \end{array}\right\} \Rightarrow 2^{r_1+1} \text{ divide a } 2^{r_1} \tag{3.3}$$

Se ha llegado a una contradicción. De manera análoga, se prueba que tampoco puede ser $s_1 < s_2 \leq r_1$. Por tanto debe ser $r_1 < s_1 < \cdots$ o $s_1 < r_1 < \cdots$. De nuevo, siguiendo la misma estructura de demostración, se demuestra que ninguno de los casos se puede dar y por tanto $r_1 = s_1$. □

Los resultados anteriores son una selección de los que hay en el artículo de Thomas Wright [37]. Estos, junto con razonamientos en algunos ideales de $\mathbb{Z}$, permiten enunciar el teorema siguiente:

Teorema 32 ([37])**.** *Sea n un número de Carmichael tal que $\lambda(n) = 2^l P$, con P primo. Asumiendo que la conjetura de los primos de Fermat es cierta, entonces P solo puede ser* 3*,* 5*,* 7 *o* 127 *y n será uno de los siguientes números de Carmichael.*

$$5 \cdot 13 \cdot 17$$
$$5 \cdot 13 \cdot 193 \cdot 257$$
$$5 \cdot 13 \cdot 193 \cdot 257 \cdot 769$$
$$3 \cdot 11 \cdot 17$$
$$5 \cdot 17 \cdot 29$$
$$5 \cdot 17 \cdot 29 \cdot 113$$
$$5 \cdot 29 \cdot 113 \cdot 65537 \cdot 114689$$
$$5 \cdot 17 \cdot 257 \cdot 509$$

Nota: Si se encuentra un número de Carmichael n que no está en la lista y tal que $\lambda(n) = 2^l P$, entonces n es divisible por un primo de Fermat a día de hoy desconocido.

Capítulo 4

Números de Carmichael con 3 factores primos

De acuerdo con la sección anterior, esta es la factorización más simple que puede tener un número de Carmichael. Restringiéndolos a esta forma, estudiarlos es más sencillo. Para empezar, se pueden simplificar las condiciones de Korselt:

Lema 33. *Si $n = pqr$ siendo p, q, r primos impares distintos, entonces n es de Carmichael si y solo si $p-1$ divide a $qr-1$, $q-1$ divide a $pr-1$ y $r-1$ divide a $pq-1$.*

Demostración. Usando el teorema 24, n es de Carmichael si y solo si $p-1$, $q-1$ y $r-1$ dividen a $pqr-1 = pq(r-1)+pq-1 = pr(q-1)+pr-1 = qr(p-1)+qr-1$, pues por hipótesis, n es un número natural compuesto y libre de cuadrados. El razonamiento es evidente: si $p-1$ divide a $n-1$, como obviamente divide a $qr(p-1)$, entonces divide necesariamente al sumando restante $qr-1$; recíprocamente, si $p-1$ divide a $qr-1$, como divide al segundo término, entonces divide a la suma, que es justamente $n-1$. □

En resumen, la primera tentativa de un número de Carmichael debe ser $3qr$, con q y r primos impares y como $3-1=2$ siempre divide a $qr-1$ por ser un número par, las tres condiciones del lema se reducen a dos. En realidad solo existe un número así, y lo presentó Carmichael por primera vez en 1912: $3 \times 11 \times 17 = 561$. También explicó el método utilizado para encontrar algunos números (de Carmichael) con 3 factores primos, fijando el primero, e incluso publicó uno con 4 factores primos. Además, en un breve pie de página, sugirió que la lista de números que cumplen la recíproca del Pequeño Teorema de Fermat se extendía indefinidamente.

Esta sugerencia no era ninguna nimiedad y de hecho estuvo sin respuesta durante aproximadamente 90 años, aunque dada la cantidad de números que se fueron encontrando gracias a los avances tecnológicos, no era de extrañar que terminara siendo cierta, tal y como lo demostraron Alford, Granville y Pomerance en 1992 [1].

Volviendo a los números de Carmichael con 3 factores primos, en los años 50 N.G.W.H. Beeger y H.J.A. Duparc enunciaron y demostraron que si se fija un primo p, entonces existe una cantidad finita de números de Carmichael de la forma pqr, con $p < q < r$ primos. El resultado está recogido en las notas de G.J.O. Jameson.

Para demostrar esto, es útil el siguiente lema:

Lema 34. *Sea pqr de Carmichael. Siguiendo la notación del lema 33, sean* $d_1 = \frac{qr-1}{p-1}$, $d_2 = \frac{pr-1}{q-1}$ *y* $d_3 = \frac{pq-1}{r-1}$. *Entonces*

$$2 \leq d_3 \leq p-1 \tag{4.1}$$

$$q - 1 = \frac{(p-1)(p+d_3)}{d_2 d_3 - p^2} \tag{4.2}$$

Demostración. Primero cabe aclarar que d_1,d_2 y d_3 son números enteros positivos bien definidos pues, al ser pqr de Carmichael, se cumple el teorema de Korselt y $3 \leq p < q < r$.
Para probar la desigualdad (4.1), se parte de $r > q$, o equivalentemente por ser q y r impares, de $r - 1 > q$.
Luego $pq = d_3(r-1) + 1 > d_3 q + 1$ implica $pq > d_3 q$ y por tanto $p - 1 \geq d_3$. Además $d_3 > 1$ porque, en caso contrario, $pq - 1 = r - 1$, lo que contradice la primalidad de r.

Para la igualdad (4.2), se parte de la definición de d_2.

$$d_2 = \frac{pr-1}{q-1} = \frac{p(r-1)+(p-1)}{q-1}$$

Por definición de d_3, se tiene $r-1 = \frac{pq-1}{d_3}$. Reemplazando en la igualdad $r-1$ por esta expresión y multiplicando por $d_3(q-1)$ queda:
$d_2 d_3(q-1) = p(pq-1)+d_3(p-1) = p(p(q-1)+(p-1))+d_3(p-1) = p^2(q-1)+p(p-1)+d_3(p-1)$
luego $(d_2 d_3 - p^2)(q-1) = (p+d_3)(p-1)$, lo que prueba la segunda parte del lema. □

Proposición 35 ([17])**.** *Se define* $f_3(p)$ *como la cantidad de números de Carmichael con exactamente 3 divisores primos p,q,r, de los cuales p es el menor. Se tiene:*

$$f_3(p) \leq (p-2)(log(p)+2)$$

Demostración. Sea d_3 como en el lema anterior. Se denota por Δ al denominador de (4.2): $\Delta = \frac{(p-1)(p+d_3)}{q-1}$. Como $p < q$, obviamente $\frac{p-1}{q-1} < 1$, luego $\Delta = (p+d_3)\frac{p-1}{q-1} < p + d_3$, es decir $\Delta \leq p + d_3 - 1$. Además, por cómo está definido el cociente (4.2) y por ser los factores de un número de Carmichael mayores que 2, está claro que Δ es un entero estrictamente positivo. De $\Delta = d_2 d_3 - p^2$, se tiene $\Delta + p^2 \equiv 0 \mod d_3$, y por tanto solo hay un posible Δ en cada intervalo de tamaño d_3 (si no, habría dos múltiplos de d_3 en un intervalo de tamaño d_3).
Ahora ya se pueden acotar superiormente las posibles elecciones para Δ:

$$\frac{p+d_3-2}{d_3} + 1 = \frac{p-2}{d_3} + 2$$

De esta manera, se puede a su vez acotar superiormente $f_3(p)$ pues al haber elegido d_3 y Δ, q queda inmendiatamente determinado por (4.2) y en seguida se saca r por la propia definición de $d_3 = \frac{pq-1}{r-1}$. Por tanto, para dar la cota buscada, hay que sumar la cota anterior para Δ según los posibles valores de d_3:

$$f_3(p) \leq \sum_{d=2}^{p-1} \left(\frac{p-2}{d} + 2 \right)$$

Por último, recordar que el logaritmo acota superiormente las sumas parciales de la serie armónica en un intervalo dado y por tanto:

$$f_3(p) \leq 2(p-1-2+1) + (p-2) \sum_{d=2}^{p-1} \frac{1}{d} = (p-2)(2 + \sum_{d=2}^{p-1} \frac{1}{d}) < (p-2)(log(p)+2)$$

□

Esta demostración, al expresar q y r en función de d_3 y Δ, no solo da un método para construir números de Carmichael con 3 factores primos, sino que fijado p, se pueden encontrar todos los productos pqr. Por ejemplo, con $p = 3$, (4.1) implica $d_3 = 2$ y (4.2) que Δ divide a $(p-1)(p+d_3) = 10$. Adicionalmente, de la demostración anterior se tienen dos condiciones más para Δ:

- $1 \leq \Delta < p + d_3$
- d_3 divide a $\Delta + p^2$

La primera condición en este caso es $1 \leq \Delta < 5$ y la segunda implica que Δ es impar ($\Delta + 9$ es divisible por 2). La única posibilidad es $\Delta = 1$. Por consiguiente, $q - 1 = 10$. Notemos que la condición (4.2) asegura que q es entero, pero no se puede decir si es primo o no. En este ejemplo lo es, por tanto se prosigue calculando $r - 1 = (pq-1)/d_3 = 16$ y de nuevo se sabe que r calculado de esta forma siempre será entero. Para verificar este hecho, básicamente hay que hacer la segunda parte de la demostración del lema 34 al revés:
d_3 divide a $\Delta + p^2$, luego divide a $(\Delta + p^2)(q-1)$ y por la expresión (4.2) esto es $(p-1)(p+d_3) + p^2(q-1) = d_3(p-1) + p(pq-1)$. Es evidente que el primer sumando es múltiplo de d_3 y en consecuencia existe un entero H tal que $p(pq-1) = Hd_3$. Ahora, como p es primo, d_3 debe dividir a $pq-1$.
Después de verificar esto, hay que comprobar que r es primo, que en este caso lo es. Habiendo construido ya 3 factores primos, veamos si cumplen las condiciones para que su producto sea de Carmichael, aplicando el lema 33. Por construcción, $r-1$ divide a $pq-1$, y para verificar que $q-1$ divide a $pr-1$ basta con tener en cuenta que hemos elegido d_3 como divisor de $\Delta + p^2$ (de nuevo estos cálculos son los mismos que en la demostración del lema 34)

$$\frac{\Delta + p^2}{d_3} = \frac{\frac{(p-1)(p+d_3)}{q-1} + p^2}{d_3} = \frac{p^2 + pd_3 - p - d_3 + p^2q - p^2}{d_3(q-1)} = \frac{p-1}{q-1} + \frac{p(pq-1)}{\frac{pq-1}{r-1}(q-1)} = \frac{pr-1}{q-1}$$

Queda por comprobar que $p-1$ divide a $qr-1$, pero esto no se puede deducir de las construcciones, así que se debe verificar cada vez. En nuestro ejemplo se cumple que $11 \cdot 17 - 1 = 1286$ es par y por tanto hemos encontrado el único número de Carmichael con 3 factores primos que es múltiplo de 3.

Ahora elegimos $p = 5$ y repetimos el proceso. Se tiene $2 \leq d_3 \leq 4$.

$d_3 = 2$
Las condiciones sobre Δ son **(i)** Δ divide a $2^2 7$ **(ii)** 2 divide a $\Delta + 25$ **(iii)** $1 \leq \Delta < 7$. Por tanto $\Delta = 1$, $q = (p-1)(p+d_3)+1 = 29$ que es primo, al igual que $r = (pq-1)/d_3 + 1 = 73$ y se verifica $73 \cdot 29 \equiv 1 \bmod 4$.

$d_3 = 3$
Las condiciones sobre Δ son **(i)** Δ divide a 2^5 **(ii)** 3 divide a $\Delta + 25$ **(iii)** $1 \leq \Delta < 8$. Por tanto $\Delta = 2$, $q = (p-1)(p+d_3)/\Delta + 1 = 17$ que es primo, al igual que $r = (pq-1)/d_3 + 1 = 29$ y se verifica $17 \cdot 29 \equiv 1 \bmod 4$.

$d_3 = 4$
Las condiciones sobre Δ son **(i)** Δ divide a $2^2 3^2$ **(ii)** 4 divide a $\Delta + 25$ **(iii)** $1 \leq \Delta < 9$. Por tanto $\Delta = 3$, $q = (p-1)(p+d_3)/\Delta + 1 = 13$ que es primo, al igual que $r = (pq-1)/d_3 + 1 = 17$ y se verifica $13 \cdot 17 \equiv 1 \bmod 4$.

Siguiendo esta construcción se encuentran todos los números de Carmichael con 3 factores primos que son múltiplos de 7:

$$7 \cdot 19 \cdot 67$$
$$7 \cdot 31 \cdot 73$$
$$7 \cdot 13 \cdot 31$$
$$7 \cdot 23 \cdot 41$$
$$7 \cdot 73 \cdot 103$$
$$7 \cdot 13 \cdot 19$$

Hay más formas de construir números de Carmichael y sin duda uno de los resultados más importantes a este respecto es el dado por Chernick en 1939[7].

Teorema 36. *Sea $m \in \mathbb{N}$. Si los números*

$$6m+1, 12m+1, 18m+1$$

son primos simultáneamente, entonces su producto es un número de Carmichael.

Demostración. Puesto que obviamente el número en cuestión es compuesto y libre de cuadrados, usando el lema 33 basta con ver que $6m$ divide a $(12m+1)(18m+1)-1$, $12m$ divide a $(6m+1)(18m+1)-1$ y $18m$ divide a $(6m+1)(12m+1)-1$, lo cual es obvio.

El artículo de Chernick, donde se incluye este resultado, es constructivo y ver el camino que siguió es útil para encontrar más números de Carmichael, así que se dará una segunda demostración de este teorema:

Sea $n = pqr$ de Carmichael. Se puede escribir $p = a_p d + 1$, $q = a_q d + 1$ y $r = a_r d + 1$, donde $d = m.c.d.(p-1, q-1, r-1)$. Por el teorema 24, $p-1$, $q-1$ y $r-1$ dividen a $n-1$:

$$(da_p + 1)(da_q + 1)(da_r + 1) \equiv 1 \bmod da_i \text{ con } i \in \{p, q, r\}$$

desarrollando los miembros de la derecha y diviendo por d, queda:

$$d(a_pa_q + a_pa_r + a_qa_r) + a_p + a_q + a_r \equiv 0 \bmod a_k,\ k \in \{p, q, r\}$$

Veamos que los a_i son primos dos a dos. Supongamos que a_p y a_q tienen un factor común h. Para $k = p$, la congruencia anterior queda:

$$da_qa_r + a_q + a_r \equiv 0 \bmod a_p$$

Como h divide a a_p entonces h divide a $da_qa_r + a_q + a_r$ y puesto que también divide a a_q, debe dividir a a_r, pero por definición, se sabe que $m.c.d.(a_p, a_q, a_r) = 1$. De la misma manera se demuestra para los otros pares.

De esta manera se puede poner una única condición:

$$d(a_pa_q + a_pa_r + a_qa_r) + a_p + a_q + a_r \equiv 0 \bmod a_pa_qa_r \tag{4.3}$$

Si se pone d como incógnita entonces esta congruencia es lineal. Como su coeficiente principal es primo con el módulo, entonces tiene inverso y se puede dar una solución general que tiene un parámetro libre.

Ahora basta con dar valores a a_p, a_q y a_r de manera que cumplan las condiciones. Lo más natural es elegir 1, 2 y 3. Reemplazando en (4.3):
$d(1 \cdot 2 + 1 \cdot 3 + 2 \cdot 3) + 1 + 2 + 3 \equiv 0 \bmod 1 \cdot 2 \cdot 3 \Leftrightarrow 5d \equiv 0 \bmod 6$, es decir, $d = 6m$, $m \in \mathbb{N}$, lo que prueba el teorema.

□

Notas:

- Puesto que p, q y r son primos impares y no se exige nada sobre la paridad de los a_i, se tiene que d siempre es par. De esta manera, *todo número de Carmichael que es producto de* 3 *primos se puede escribir de la forma* $(2ha_p + 1)(2ha_q + 1)(2ha_r + 1)$.

- Una forma equivalente de escribir el teorema 36 es definiendo $p = 6m + 1$ y así queda $n = p(2p - 1)(3p - 2)$. Con esta definición hay que exigir que $p \equiv 1 \bmod 6$, lo que inmediatamente implica que $2p - 1 \equiv 1 \bmod 6$ y $3p - 2 \equiv 1 \bmod 6$.

- Dubner [10] propuso un método similar al de Chernick para construir números de Carmichael con 3 factores primos, con la diferencia de que, en vez de tres, exige encontrar solo dos primos simultáneamente.

El primer ejemplo de este tipo de números es $n = 7 \cdot 13 \cdot 19 = 1729$, obtenido con $m = 1$ (o equivalentemente, $p = 7$). Curiosamente este número es el primero que se puede escribir como suma de cubos de dos maneras, $1^3 + 12^3 = 9^3 + 10^3$, y es más conocido como número de Hardy-Ramanujan.
Cualquier persona con un ordenador podrá calcular números de Chernick hasta donde su paciencia o la capacidad de la máquina se lo permita, a continuación un pequeño ejemplo de cómo

m	$6m+1$	$12m+1$	$18m+1$
1	7	13	19
6	37	73	109
35	211	421	631
45	271	541	811
51	307	613	919
55	331	661	991
56	337	673	1009
100	601	1201	1801
121	727	1453	2179
195	1171	2341	3511
206	1237	2473	3709
216	1297	2593	3889
255	1531	3061	4591
276	1657	3313	4969
370	2221	4441	6661
380	2281	4561	6841
426	2557	5113	7669
506	3037	6073	9109
510	3061	6121	9181

Cuadro 4.1: Primeros números de Chernick

hacerlo con Maple.

```
> restart
> a := 6 m + 1 : b := 12 m + 1 : c := 18 m + 1 :
> simplify((c·a − 1)/(b − 1)); simplify((b·a − 1)/(c − 1)); simplify((c·b − 1)/(a − 1));
                                  9 m + 2
                                  4 m + 1
                                 36 m + 5                                  (1)
> cont := 0 : NN := 100000 :
  for m from 1 to NN do
  if isprime(a) and isprime(b) and isprime(c) then
  cont := cont + 1;
  #print( [a, b, c] ) :
  fi
   od;
  cont
                                    842                                    (2)
>
```

De esta manera se ha calculado que hay 842 números de Chernick para m menor que 100 000. Si se quiere conocer la factorización de dichos números, hay que descomentar la línea *# print([a,b,c]):*. La tabla 4.1 muestra los primeros 20 números que se calcularon con maple. A día de hoy no se ha podido probar que la lista es infinita (o que no lo es).

Siguiendo la construcción de Chernick, variando a_p, a_q y a_r, se pueden encontrar nuevas formas, por ejemplo con $a_p = 1$, $a_q = 5$ y $a_r = 8$, la condición (4.3) sobre d queda $13d + 14 \equiv 0$

mod 40 cuya solución es de la forma $d = 40m + x$. Hay que encontrar x tal que $13x + 14 \equiv 0$ mod 40,que en este caso es fácil de calcular pues $40 - 14 = 26 = 13 \cdot 2$, por lo tanto $d = 40m + 2$. Finalmente se hace una pequeña verificación del lema 33, poniendo $p = 40m + 3$, $q = 200m + 11$ y $r = 320m + 17$ para tener

$$\frac{pq-1}{r-1} = 25m + 2, \frac{pr-1}{q-1} = 64m + 5 \text{ y } \frac{qr-1}{p-1} = 1600m + 93$$

Hemos encontrado que si $40m + 3$, $200m + 11$ y $320m + 17$ son primos simultáneamente entonces su producto es un número de Carmichael, por lo tanto $43 \cdot 211 \cdot 337$ es un número de Carmichael.

En la factorización de estos dos ejemplos ($43 \cdot 211 \cdot 337$ y $7 \cdot 13 \cdot 19$), por ser $m = 1$, se puede intuir la forma genérica de Chernick que produjo cada caso. Es por esto que se puede pensar que el proceso también funciona a la inversa y hay que hacerse la pregunta:

Dada la factorización de un número de Carmichael, ¿se podrá construir una fórmula que permita calcular otros?

La respuesta es afirmativa pero, al igual que la pregunta, poco rigurosa y debe responderse empíricamente, al menos por ahora:

Se toma algún número de Carmichael que tenga una factorización sencilla,por ejemplo $7 \cdot 13 \cdot 31$, que es igual al primer número de Chernick en los dos primeros términos pero no en el tercero. Ahora, teniendo en cuenta que todo número de Carmichael que sea producto de 3 factores primos se puede escribir como $(2ha_p + 1)(2ha_q + 1)(2ha_r + 1)$, la opción más evidente es $p \cdot q \cdot r$, con $p = (6m + 1)$, $q = (12m + 1)$ y $r = (30m + 1)$. En este caso, se cumplen 2 de las condiciones del lema 33,

$$\frac{pr-1}{q-1} = 15m + 3 \text{ y } \frac{qr-1}{p-1} = 60m + 7$$

pero,

$$\frac{pq-1}{r-1} = \frac{1}{5}(12m + 3)$$

Se puede probar quitándole a r el factor que no se está simplificando pero quedaría $p = r$. Veamos dos formas de solucionar este problema:

Razonar en $\mathbb{Z}/(5)$
En este caso, buscamos una condición sobre m para que se cumpla la condición que nos hace falta, es decir $12m + 3 \equiv 0$ mod 5. Debe ser $m = 5m' + 1$ y los nuevos p, q y r son $30m' + 7$, $60m' + 13$ y $150m' + 31$. Por construcción, se verifican las condiciones para que el producto pqr sea un número de Carmichael, siempre que p, q, y r sean primos simultáneamente. La tabla 4.2 muestra algunos ejemplos, incluido el número de partida para $m' = 0$. Hemos calculado que para $m \leq 10^7$ existen exactamente 24146 números de Carmichael de esta forma. Están acotados por 10^{25}.

m	$30m+7$	$60m+13$	$150m+31$
0	7	13	31
1	37	73	181
10	307	613	1531
12	367	733	1831
18	547	1093	2731
24	727	1453	3631
32	967	1933	4831
43	1297	2593	6481
85	2557	5113	12781
102	3067	6133	15331
123	3697	7393	18481
129	3877	7753	19381
150	4507	9013	22531
201	6037	12073	30181
207	6217	12433	31081
256	7687	15373	38431
304	9127	18253	45631
309	9277	18553	46381
330	9907	19813	49531
353	10597	21193	52981

Cuadro 4.2: Números de Carmichael de la forma $(30m+7)(60m+13)(150m+31)$

Adaptar uno de los factores como producto de los otros dos

Si queremos conservar $p=(6m+1)$ y $q=(12m+1)$ como factores primos, debemos encontrar un r tal que, si se le quita una unidad, divida a $(6m+1)(12m+1)-1=72m^2+18m$. Sea $r=\frac{72m^2+18m}{6}+1$. Dividimos por 6 pues al ser un divisor común, permite simplificar la expresión, pero $\frac{qr-1}{p-1}=24m^2+8m+5/2$. Se prueba entonces $r=\frac{72m^2+18m}{3}+1$ y ya se tiene:

$$\frac{pq-1}{r-1}=3,\ \frac{pr-1}{q-1}=12m^2+5m+1 \text{ y } \frac{qr-1}{p-1}=48m^2+16m+3$$

De esta manera, si $6m+1$, $12m+1$ y $24m^2+6m+1$ son primos simultáneamente, entonces su producto es un número de Carmichael. Se calculó una pequeña lista (ver cuadro 4.3) para ver que efectivamente hay números de esta forma y notemos que para $m=1$ se tiene el número de partida.

Con ayuda de estos dos procedimientos se consiguieron las siguientes fórmulas a partir de $31\cdot 61\cdot 211$ y de $13\cdot 97\cdot 421$

$$(210m+31)(420m+61)(1470m+211) \text{ y } (30m+1)(60m+1)(600m^2+30m+1)$$

$$(840m+13)(6720m+97)(29400m+421)$$

Otras fórmulas:

$$(10m+1)(20m+1)(30m+1) \text{ es la lista A206347 de la OEIS}$$

$(18m+1)(36m+1)(54m+1)$ y $(36m+1)(72m+1)(108m+1)$ son modificaciones de Chernick

m	$6m+1$	$12m+1$	$24m^2+6m+1$
1	7	13	31
5	31	61	631
26	157	313	16381
35	211	421	29611
45	271	541	48871
51	307	613	62731
55	331	661	72931
61	367	733	89671
121	727	1453	352111
135	811	1621	438211
161	967	1933	623071
195	1171	2341	913771
206	1237	2473	1019701
255	1531	3061	1562131
335	2011	4021	2695411
370	2221	4441	3287821
385	2311	4621	3559711
475	2851	5701	5417851
511	3067	6133	6269971

Cuadro 4.3: Números de Carmichael de la forma $(6m+1)(12m+1)(24m^2+6m+1)$

Capítulo 5

Números de Carmichael con k factores primos

Para empezar este capítulo, es importante aclarar, tal y como lo hacen U. Cerruti [34] y Wagstaff [35], que no hay que ceñirse a las condiciones del teorema 36. Es decir, existen números de Carmichael que se pueden escribir como $(6m+1)(12m+1)(18m+1)$ sin que sean todos primos, lo que lleva a encontrar números de Carmichael con 4, 5 o más factores primos. Por ejemplo, $(6 \cdot 5+1)(12 \cdot 5+1)(18 \cdot 5+1) = 7 \cdot 13 \cdot 31 \cdot 61$ es de Carmichael y producto de 4 factores primos. Sin embargo, de aquí en adelante cuando nos refiramos a números de Carmichael construidos con este tipo de fórmula, se asumirá que se han construido siguiendo el teorema y por tanto su número de factores primos quedará determinado por la expresión genérica correspondiente.

Para construir números de Carmichael con más factores primos, se puede intentar seguir la misma construcción que para 3 y así conseguir fórmulas para 4 factores primos, pero a partir de ahí las expresiones se vuelven inmanejables, así que se siguen otras estrategias.

Definición 14. *Sean $a_i m + b_i$, $i \in \{1, 2, ..., k\}$, k formas lineales impares y distintas. Se dice que el producto $\prod_{i=1}^{k}(a_i m + b_i)$ es una forma universal si $(a_1 m + b_1)(a_2 m + b_2)...(a_k m + b_k) \equiv 1$ mod $(a_i m + b_i - 1)$, para todo $i \in \{1, 2, ..., k\}$, con $k \geq 3$.*

Dada una forma universal, si existe un m tal que $a_i m + b_i$ sea primo para $i \in \{1, ..., k\}$, entonces queda definido un número de Carmichael.

Teorema 37. *[7] Sea $n = p_1...p_k$ un número de Carmichael y $d = m.c.d.(p_1 - 1, ..., p_k - 1)$. Se definen $r_1, ..., r_k$ de manera que $p_i - 1 = dr_i$. Finalmente, sea $R = m.c.m.(r_1, ..., r_k)$. Entonces,*

$$\prod_{i=1}^{k}(r_i R m + p_i)$$

es una forma universal, bajo la condición de que, si todos los r_i son impares, entonces se puede reemplazar m por $2m$.

Demostración. Para empezar, no hay dos formas $r_i R m + p_i$ iguales, pues al ser n libre de cuadrados todos los p se pueden ordenar (estrictamente) y para cada $p_i < p_j$ se tiene $r_i < r_j$.

Además, son formas impares pues R es par y los p_i son primos impares. El único caso en el que R puede ser impar es cuando todos los r_i también lo sean, y si esto pasa, se exige que m sea par.

Veamos ahora que d es solución de

$$\frac{1}{X}\left[\prod_{j=1}^{k}(r_jX+1)-1\right]\equiv 0 \bmod R \tag{5.1}$$

Se tiene por un lado,

$$\begin{aligned}\lambda(n) &= m.c.m.(p_1-1,...,p_k-1)\\ &= m.c.m.(dr_1,...,dr_k)\\ &= d\cdot m.c.m.(r_1,...,r_k)=dR\end{aligned}$$

Y por otro,

$$n-1=p_1...p_k-1=(dr_1+1)...(dr_k+1)-1$$

Por el teorema 27, $\lambda(n)$ divide a $n-1$ y en consecuencia, R divide a $\frac{1}{d}(\prod_{j=1}^{k}(r_jd+1)-1)$, o lo que es lo mismo, d es solución de (5.1), De esta manera, cualquier otro $D\equiv d \bmod R$ cumple la congruencia (5.1), es decir $R(Rm+d)$ divide a $\prod_{j=1}^{k}[r_j(Rm+d)+1]-1=\prod_{j=1}^{k}[r_jRm+r_jd+1]-1=\prod_{j=1}^{k}(r_jRm+p_j)-1$. Además, está claro que por ser R múltiplo de r_i, $R(Rm+d)$ es a su vez es múltiplo de $r_i(Rm+d)=r_iRm+p_i-1$ y por lo tanto se cumplen las condiciones de universalidad.

□

Se toma, por ejemplo, el número de Carmichael $7\cdot 13\cdot 31$ y se sigue la construcción del teorema:

1. $m.c.d.(6,12,30)=6$
2. $r_1=\frac{6}{6}$, $r_2=\frac{12}{6}$, $r_1=\frac{30}{6}$
3. $R=m.c.m.(1,2,5)=10$
4. $(1\cdot 10\cdot m+7)(2\cdot 10\cdot m+13)(5\cdot 10\cdot m+31)$

Por lo tanto, el producto $(10m+7)(20m+13)(50m+31)$ es una forma universal. El número de partida de este ejemplo es el mismo que se utilizó al final del capítulo anterior, y de hecho la forma obtenida es la misma si se cambia m por $3m$. Es más, la tabla es exactamente igual en los dos casos. Así que los ejemplos están en la tabla 4.2, multiplicando el valor de m por 3.

Los números de Chernick estudiados en el capítulo anterior son también un ejemplo de forma universal, y se pueden generalizar gracias al teorema siguiente.

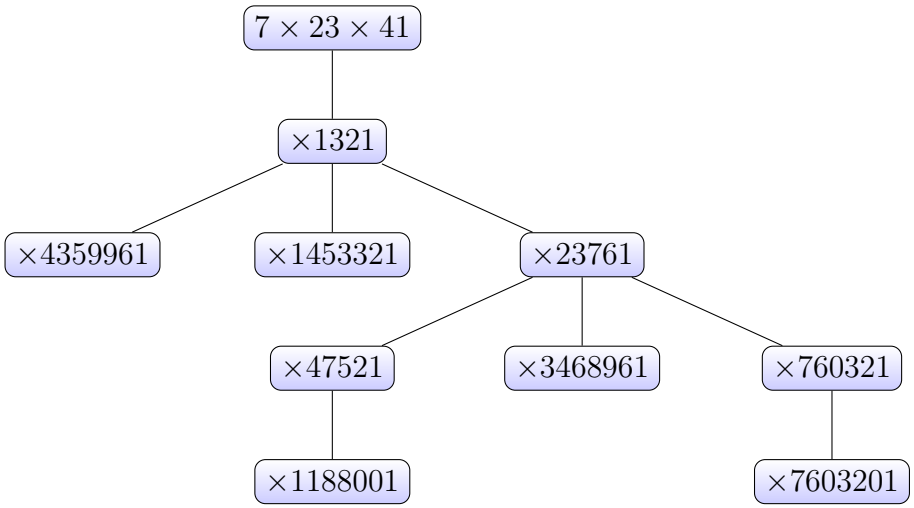
Teorema 38 ([7]). *Sea n un número de Carmichael. Si se encuentra un número primo p coprimo con n tal que:*

- *$\lambda(n)$ divide a $p-1$*
- *$p-1$ divide a $n-1$*

Entonces np es un número de Carmichael.

Demostración. Se tiene $np-1=(n-1)+(p-1)+(n-1)(p-1)$. Puesto que $\lambda(n)$ divide a $n-1$ por ser n de Carmichael y a $p-1$ por hipótesis, también divide a $np-1$. De la misma forma, la segunda condición dice que $p-1$ divide a $n-1$, así que también divide a $np-1$. Por tanto $\lambda(np)=\lambda(m.c.m.(n,p))=m.c.m.(\lambda(n),\lambda(p))=m.c.m.(\lambda(n),p-1)$ divide a $np-1$ y por el teorema 27, np es de Carmichael. □

El siguiente diagrama es un ejemplo de aplicación. Partiendo de un número de Carmichael n, se buscan todos los $p<10^7$ que cumplen las condiciones del teorema 38, para luego iterar el proceso con cada np. De esta manera, partiendo de $7\cdot 23\cdot 41$, se consiguen los números de Carmichael $7\cdot 23\cdot 41\cdot 1321$, $7\cdot 23\cdot 41\cdot 1321\cdot 1453321$, etc. y en el último nivel del árbol tenemos dos números de Carmichael con 7 factores primos, $7\cdot 23\cdot 41\cdot 1321\cdot 23761\cdot 47521\cdot 1188001$ y $7\cdot 23\cdot 41\cdot 1321\cdot 23761\cdot 760321\cdot 7603201$



Corolario 39. *Sean $p_1,...,p_k$ primos distintos y $n=p_1\cdots p_k$ un número de Carmichael. Si $(p_1\cdots p_k+1)/2$ es un número primo y cada p_i-1 divide a $(p_1\cdots p_k-1)/2$, entonces*

$$p_1\cdots p_k\cdot\left(\frac{p_1\cdots p_k+1}{2}\right)$$

es un número de Carmichael.

En el ejemplo anterior, se puede aplicar el corolario 39 a $7\cdot 23\cdot 41\cdot 1321$ para ver que $7\cdot 23\cdot 41\cdot 1321\cdot 4359961$ es un número de Carmichael.

Apliquemos el teorema 38 a los números de Chernick en su forma genérica $n=(6m+1)(12m+1)(18m+1)$. Se quiere encontrar p que no divida a n y tal que $p-1$ sea múltiplo de

$$\lambda((6m+1)-1,(12m+1)-1,(18m+1)-1)=36m$$

Es decir, $p-1=k\cdot 36m$. Con un cálculo rápido, se ve que para $k=1$ ya se cumple la segunda condición del teorema. En consecuencia, el producto $(6m+1)(12m+1)(18m+1)(36m+1)$ es una forma universal, a la que llamaremos U_4.
Análogamente, para calcular U_5 a partir de $n=U_4$, la primera condición implica que p sea de la forma $p-1=k\cdot 36m$. Puesto que p no puede dividir a n, k debe ser distinto de 1, por ejemplo $k=2$. Se verifica si se cumple que $(n-1)/(p-1)$ sea entero:

$$\frac{(6m+1)(12m+1)(18m+1)(36m+1)-1}{72m}=648m^4+216m^3+1908m^2+\frac{47}{2}m+1$$

Aquí basta con observar que el único sumando que no es entero está multiplicando a m, por lo tanto si se reemplaza m por $2m$, o lo que es lo mismo, se exige $m \equiv 0 \bmod 2$, queda solventado el problema.
De manera análoga, se tiene que $U_6 = (6m+1)(12m+1)(18m+1)(36m+1)(72m+1)(144m+1)$ es una forma universal siempre que $m \equiv 0 \bmod 4$.

Generalización Sea U_n una forma universal. Se quiere encontrar un p que cumpla las condiciones del teorema 38.

$$U_n = (6m+1)(12m+1)\prod_{i=1}^{n-2}\left(9\cdot 2^i m+1\right), \text{ con } n \geq 3 \text{ y } m \equiv 0 \bmod 2^{n-4} \text{ si } n > 4$$

Se tiene $\lambda(U_n) = m.c.m.(6m, 12m, 9{\cdot}2m, ..., 9{\cdot}2^{n-2}m) = 9{\cdot}2^{n-2}m$, por lo tanto $p{-}1 = k{\cdot}9{\cdot}2^{n-2}m$ y puesto que con $k = 1$ se repite un término, se toma $k = 2$:

$$p - 1 = 9 \cdot 2^{n-1}m$$

Para verificar la segunda condición del teorema, se desarrolla la expresión de U_n como un polinomio en m:

$$U_n - 1 = (6 + 12 + 18 + ... + 9 \cdot 2^{n-2})m + Pm^2$$

Siendo $P = P(m)$ un polinomio en m por tanto $U_n - 1 = 2^{n-1}9m + Pm^2$. Ahora, imponiendo que $n-1$ sea mútiplo de $p-1$, se tiene $U_n - 1 \equiv 0 \bmod p-1 \Leftrightarrow Pm \equiv 0 \bmod 2^{n-1}$ y de esta manera debe ser $m \equiv 0 \bmod 2^{n-1}$.

En las tablas 5 hay ejemplos para esta generalización en el caso $n = 3, 4, 5, 6$. El caso $n = 3$ está detallado en el cuadro 4.1.

Como es de esperarse, igual que para los números de Chernick, no está probado que haya infinitos números de Carmichael de cada una de estas formas. Lo que sí se sabe es que la conjetura de Dickson implica este resultado (ver página 7). En 2013 se probó una versión débil de esta conjetura:

Teorema 40 (Maynard & Tao [21])**.** *Sea $D = \{a_1n{+}b_1, ..., a_kn{+}b_k\}$ admisible, es decir que para todo primo p existe un $n(p)$ natural de manera que p no divide a $(a_1n(p){+}b_1)...(a_kn(p){+}b_k)$ (ver definición 7). Entonces para todo entero $m \geq 2$, existe una constante C tal que, si $k > Ce^{8m}$, entonces m de las formas en D son primas simultáneamente infinitas veces.*

[1] Puesto que la conjetura está estrechamente relacionada con los números de Carmichael, es evidente preguntarse qué supone este avance: nada. La cota es demasiado grande como para que permita demostrar que en D hay suficientes primos del tipo buscado. T. Wright estudió las condiciones necesarias y basta con que la cota sea polinomial en vez de exponencial:

[1] De hecho la cota se ha mejorado hasta Ce^{4m} gracias al Polymath project. En el blog de Terrence Tao viene más detallado este tema https://terrytao.wordpress.com/2013/11/19/polymath8b-bounded-intervals-with-many-primes-after-maynard/. Ttambién http://arxiv.org/abs/1505.01815

m tales que $U_3(m)$ es de Carmichael
1
6
35
45
51
55
56
100
121
195

m tales que $U_4(m)$ es de Carmichael
1
45
56
121
206
255
380
506
511
710

m tales que $U_5(m)$ es de Carmichael
380
506
3796
6006
8976
9186
10920
12896
14476
14800

m tales que $U_6(m)$ es de Carmichael
380
38460
40420
419260
458180
780320
784840
950560
1006600
1027840

Cuadro 5.1: Primeros valores de m para los que $U_k(m)$ es un número de Carmichael con k factores primos, $k = 3, 4, 5, 6$

Puesto que

- $U_3(m) = (6m + 1)(12m + 1)(18m + 1)$
- $U_4(m) = (6m + 1)(12m + 1)(18m + 1)(36m + 1)$
- $U_5(m) = (6m + 1)(12m + 1)(18m + 1)(36m + 1)(72m + 1)$, $m = 2m'$
- $U_6(m) = (6m + 1)(12m + 1)(18m + 1)(36m + 1)(72m + 1)(144m + 1)$, $m = 4m'$

Está claro que cada tabla está contenida en la anterior, por lo tanto los correspondientes números de Carmichael se dividen sucesivamente.

- 41 (Conjetura débil)**.** *Sea $D = \{a_1n+b_1, ..., a_kn+b_k\}$ admisible. Entonces existe una constante $T > 0$ tal que, para todo $m \geq 2$, si $k \geq m^T$, entonces m de las formas en D son primas simultáneamente infinitas veces.*

Teorema 42 ([38])**.** *Se asume que la conjetura anterior es cierta. Sea $C_R(x)$ la cantidad de números de Carmichael con exactamente R factores primos. Entonces hay infinitos R para los cuales $C_R(x)$ diverge con x.*

La demostración de este teorema sigue los pasos de la que prueba que hay infinitos números de Carmichael, y su complejidad se escapa al nivel de este trabajo.

Volviendo a las formas universales U_k, ya se sabe que si un entero compuesto n es tal que $\varphi(n)$ divide a $n-1$, entonces n es de Carmichael (ver sección 3.1). Así que nos preguntamos qué papel desempeñan las U_k en este problema.

Teorema 43 ([35])**.** *Sea $n = U_k(m)$ de manera que n sea un número de Carmichael con k factores primos. Entonces $\varphi(n)$* ***no*** *divide a $n-1$.*

Demostración. Se tiene:

$$\frac{n}{\varphi(n)} = (1+\frac{1}{6m})(1+\frac{1}{12m})\prod_{i=1}^{k-2}\left(1+\frac{1}{9\cdot 2^i m}\right)$$

Tomando logaritmos:

$$ln\left(\frac{n}{\varphi(n)}\right) = ln(1+\frac{1}{6m}) + ln(1+\frac{1}{12m}) + \sum_{i=1}^{k-2} ln\left(1+\frac{1}{9\cdot 2^i m}\right)$$

Como $ln(1+x) < x$ cuando x es distinto de 0, queda:

$$ln\left(\frac{n}{\varphi(n)}\right) < \frac{1}{6m} + \frac{1}{12m} + \sum_{i=1}^{k-2}\frac{1}{9\cdot 2^i m} = \frac{1}{6m} + \frac{1}{12m} + \frac{1}{9m}\sum_{i=1}^{k-2}\frac{1}{2^i}$$

$$< \frac{1}{6m} + \frac{1}{12m} + \frac{1}{9m}\sum_{i=1}^{\infty}\frac{1}{2^i} = \frac{13}{36m} \leq \frac{13}{36} < ln(2)$$

Finalmente, como $\frac{n-1}{\varphi(n)} < \frac{n}{\varphi(n)}$ y el logaritmo es monótono,

$$\frac{n-1}{\varphi(n)} < 2 \text{ es decir } n-1 < 2\varphi(n)$$

En consecuencia, $n-1$ no puede ser un múltiplo de $\varphi(n)$. □

La construcción de las formas U_k se puede hacer para otras formas. En el capítulo anterior se calculó la fórmula genérica $G_3 = (6m+1)(12m+1)(24m^2+6m+1)$ a la que se le puede aplicar el teorema 38. Puesto que $\lambda(G_3) = 12m(4m+1)$, se tiene $p-1 = k12m(4m+1)$, y es fácil ver que para $k=1$, $p-1$ divide a $(6m+1)(12m+1)(24m^2+6m+1)-1$, luego

$$(6m+1)(12m+1)(24m^2+6m+1)(48m^2+12m+1)$$

es un número de Carmichael siempre que $6m+1$, $12m+1$, $24m^2+6m+1$, $48m^2+12m+1$ sean primos simultáneamente. Notemos ahora que con $k=2$ se tiene

$$\frac{G_3-1}{p-1} = \frac{G_3-1}{2\lambda(G_3)} = \frac{G_3-1}{2\cdot 12m(4m+1)} = 18m^2+(9/2)m+1$$

que es entero siempre que m sea par, y por tanto, podemos definir la siguiente fórmula:

$$G_4 = (6m+1)(12m+1)(24m^2+6m+1)(2\cdot 12m(4m+1)+1),\ m \equiv 0 \bmod 2$$

Por el teorema 38, G_4 es de Carmichael, siempre que los 4 factores de la fórmula sean primos simultáneamente.

Se define la recurrencia

$$G_{n+1} = G_n p_n \text{ y } p_n = (2\lambda(G_n)+1),\ n \geq 3$$

Veamos que, en este caso, $\lambda(G_n) = 2^{n-2}6m(4m+1)$, $n \geq 3$. Ya vimos que $\lambda(G_3) = 12m(4m+1)$ y supongamos que la fórmula se cumple para $\lambda(G_n)$. Se tiene $\lambda(G_{n+1}) = \lambda(G_n p_n) = m.c.m.(\lambda(G_n),\lambda(p_n)) = m.c.m.(\lambda(G_n), p_n-1) = m.c.m.(\lambda(G_n), 2\lambda(G_n)) = 2\lambda(G_n)$ y por hipótesis de inducción esto es $2\cdot 2^{n-2}6m(4m+1) = 2^{(n+1)-2}6m(4m+1)$, como se quería ver.

Se obtiene la fórmula general para $n \geq 3$

$$\begin{aligned} G_n &= (6m+1)(12m+1)(6m(4m+1)+1)\prod_{i=1}^{n-3}[2^i 12m(4m+1)+1] \\ &= Qm+1, \text{ siendo } Q \text{ un polinomio en } m \end{aligned}$$

Supongamos que G_n es tal que $\dfrac{G_n-1}{\lambda(G_n)} = mP+2$ donde $P = P(m)$ es un polinomio en m tal que mP toma valores enteros si $m \equiv 0 \bmod 2^{n-3}$.
Probemos que, en este caso G_{n+1}, construido como se dijo, también cumple estas propiedades.

$$\begin{aligned} \frac{G_{n+1}-1}{\lambda(G_{n+1})} &= \frac{G_n p_n - 1}{2\lambda(G_n)} \\ &= \frac{G_n(2\lambda(G_n)+1)-1}{2\lambda(G_n)} \\ &= G_n + \frac{G_n-1}{2\lambda(G_n)} = Qm+1+\frac{Pm}{2}+1 = m\left(Q+\frac{P}{2}\right)+2 \end{aligned}$$

Como mP toma valores enteros si $m = 2^{n-3}m'$, $mP/2$ tomará valores enteros siempre que $m = 2^{n-2}m'$.

Ahora, por el teorema 27, G_n es un número de Carmichael siempre que los factores de su fórmula sean primos simultáneamente.

m tales que G_3 es de Carmichael
1
5
26
35
45
51
55
61
121
135

m tales que G_4 es de Carmichael
26
800
1526
1720
2280
3930
4510
9550
12630
14646

m tales que G_5 es de Carmichael
1720
19780
79296
80656
116496
120080
144920
270916
297096
405036

m tales que G_6 es de Carmichael
1720
415280
593760
2616376
6943816
12934760
13062096
16754920
35026600
36912840

Cuadro 5.2: Primeros valores de m para los que $G_k(m)$ es un número de Carmichael con k factores primos, $k = 3, 4, 5, 6$

Recordemos :

- $G_3(m) = (6m+1)(12m+1)(24m^2+6m+1)$
- $G_4(m) = (6m+1)(12m+1)(24m^2+6m+1)(24m(4m+1)+1)$
- $G_5(m) = (6m+1)(12m+1)(24m^2+6m+1)(24m(4m+1)+1)(48m(4m+1)+1)$
- $G_6(m) =$
  $(6m+1)(12m+1)(24m^2+6m+1)(24m(4m+1)+1)(48m(4m+1)+1)(96m(4m+1)+1)$

Nota: A diferencia del capítulo anterior, en el que mostramos técnicas para conseguir **todos** los números de Carmichael con 3 factores primos, fijando uno de ellos, en este capítulo nos hemos centrado en la construcción de fórmulas. Pinch ha publicado varios artículos en los que lista todos los números de Carmichael menores que una cantidad X. Para ello, utiliza técnicas de criba y la siguiente generalización del teorema 35:

Teorema 44. *[25] Sea $d \geq 3$ un entero. Dado un conjunto de $d-2$ primos distintos, solo existe una cantidad finita de números de Carmichael con d factores primos.*

Capítulo 6

Números de Carmichael producto de otros dos

En principio, el producto de dos números de Carmichael no tiene ningún motivo para ser de Carmichael. Siguiendo la idea del capítulo anterior, se pueden buscar condiciones para que sea posible. En particular, las condiciones del teorema 38 se pueden adaptar para este fin.

Teorema 45 ([40])**.** *Sea n_1 y n_2 dos números de Carmichael primos entre sí y tales que $\lambda(n_1)$ divide a $n_2 - 1$ y $\lambda(n_2)$ divide a $n_1 - 1$. Entonces $n_1 n_2$ es un número de Carmichael.*

Demostración. Sea $n_1 = p_1...p_k$ y $n_2 = q_1...q_l$. Está claro que, por ser primos entre sí, $p_i \neq q_j$ para todo i, j. Veamos que $n_1 n_2$ cumple las condiciones del teorema 27:

$$n_1 n_2 - 1 = (n_1 - 1) + (n_2 - 1) + (n_1 - 1)(n_2 - 1)$$

Por ser n_1 de Carmichael, $\lambda(n_1)$ divide a $n_1 - 1$ y por hipótesis divide también a $n_2 - 1$, por lo tanto $\lambda(n_1)$ divide a $n_1 n_2 - 1$. Análogamente, $\lambda(n_2)$ divide a $n_1 n_2 - 1$. Además,

$$\begin{aligned}
\lambda(n_1 n_2) &= \lambda(p_1...p_k q_1...q_l) \\
&= m.c.m.(p_1 - 1, ..., p_k - 1, q_1 - 1, ..., q_l - 1) \\
&= m.c.m.(m.c.m.(p_1 - 1, ..., p_k - 1), m.c.m(q_1 - 1, ..., q_l - 1)) \\
&= m.c.m.(\lambda(n_1), \lambda(n_2))
\end{aligned}$$

Como $n_1 n_2 - 1$ es un múltiplo de $\lambda(n_1)$ y de $\lambda(n_2)$, ha de ser divisible por su mínimo común mútiplo, luego $\lambda(n_1 n_2)$ divide a $n_1 n_2 - 1$ y por tanto $n_1 n_2$ es un número de Carmichael. □

Los ejemplos que hemos calculado no son una aplicación directa de este teorema, sino que a una lista de números de Carmichael se le han aplicado los siguientes corolarios, por separado.

Corolario 46. *Sean n_1 y n_2 números de Carmichael primos entre sí. Si $\lambda(n_1)$ divide a $\lambda(n_2)$ y $\lambda(n_2)$ divide a $n_1 - 1$, entonces el producto $n_1 n_2$ es de Carmichael.*

Corolario 47. *Sean n_1 y n_2 números de Carmichael primos entre sí y tales que $\lambda(n_1) = \lambda(n_2)$. Entonces $n_1 n_2$ es de Carmichael.*

Las demostraciones son directas pues son fácilmente reducibles al teorema principal.

n_1	n_2	$\lambda(n_1) = \lambda(n_2)$
$13 \cdot 37 \cdot 241$	$7 \cdot 17 \cdot 19 \cdot 41 \cdot 181$	720
$13 \cdot 37 \cdot 241$	$11 \cdot 17 \cdot 31 \cdot 73 \cdot 181$	720
$13 \cdot 37 \cdot 241$	$17 \cdot 41 \cdot 61 \cdot 73 \cdot 181$	720
$13 \cdot 61 \cdot 397$	$31 \cdot 181 \cdot 331$	1980
$13 \cdot 61 \cdot 397$	$331 \cdot 661 \cdot 991$	1980
$19 \cdot 43 \cdot 409$	$37 \cdot 73 \cdot 127 \cdot 307$	8568
$31 \cdot 61 \cdot 271$	$7 \cdot 13 \cdot 19 \cdot 109 \cdot 541$	540
$31 \cdot 61 \cdot 631$	$11 \cdot 13 \cdot 37 \cdot 71 \cdot 181$	1260
$31 \cdot 61 \cdot 631$	$11 \cdot 19 \cdot 29 \cdot 181 \cdot 421$	1260
$31 \cdot 61 \cdot 631$	$11 \cdot 29 \cdot 37 \cdot 127 \cdot 421$	1260
$37 \cdot 73 \cdot 541$	$11 \cdot 19 \cdot 41 \cdot 109 \cdot 181$	1080
$31 \cdot 181 \cdot 331$	$7 \cdot 19 \cdot 397 \cdot 661$	1980
$13 \cdot 19 \cdot 61 \cdot 163$	$271 \cdot 541 \cdot 811$	1620
$11 \cdot 29 \cdot 61 \cdot 139$	$277 \cdot 1381 \cdot 1933$	9660
$43 \cdot 211 \cdot 337$	$61 \cdot 241 \cdot 421$	1680
$43 \cdot 211 \cdot 337$	$17 \cdot 61 \cdot 113 \cdot 421$	1680
$43 \cdot 211 \cdot 337$	$11 \cdot 13 \cdot 17 \cdot 31 \cdot 41 \cdot 281$	1680
$13 \cdot 31 \cdot 37 \cdot 211$	$11 \cdot 19 \cdot 29 \cdot 181 \cdot 421$	1260
$11 \cdot 31 \cdot 73 \cdot 197$	$29 \cdot 41 \cdot 181 \cdot 3529$	17640

Cuadro 6.1: Ejemplo de aplicación del corolario 47

n_1	n_2	$\lambda(n_1)$	$\lambda(n_2)$
$7 \cdot 13 \cdot 19$	$37 \cdot 73 \cdot 109$	36	216
$5 \cdot 17 \cdot 29$	$89 \cdot 353 \cdot 617$	112	2464
$7 \cdot 31 \cdot 73$	$13 \cdot 37 \cdot 241$	360	720
$7 \cdot 11 \cdot 13 \cdot 41$	$37 \cdot 73 \cdot 181$	120	360
$7 \cdot 11 \cdot 13 \cdot 41$	$37 \cdot 73 \cdot 541$	120	1080
$7 \cdot 11 \cdot 13 \cdot 41$	$17 \cdot 31 \cdot 191 \cdot 433$	120	41040
$13 \cdot 37 \cdot 241$	$17 \cdot 19 \cdot 47 \cdot 1381$	720	16560
$13 \cdot 37 \cdot 241$	$61 \cdot 181 \cdot 5521$	720	16560
$13 \cdot 37 \cdot 241$	$17 \cdot 19 \cdot 29 \cdot 71 \cdot 113$	720	5040
$7 \cdot 13 \cdot 31 \cdot 61$	$37 \cdot 73 \cdot 181$	60	360
$7 \cdot 13 \cdot 31 \cdot 61$	$17 \cdot 41 \cdot 73 \cdot 241$	60	720
$7 \cdot 13 \cdot 19 \cdot 109$	$31 \cdot 61 \cdot 271$	108	540
$31 \cdot 61 \cdot 211$	$281 \cdot 421 \cdot 701$	420	4200
$37 \cdot 73 \cdot 181$	$17 \cdot 19 \cdot 29 \cdot 71 \cdot 113$	360	5040
$37 \cdot 73 \cdot 181$	$43 \cdot 61 \cdot 127 \cdot 241$	360	5040
$13 \cdot 17 \cdot 41 \cdot 61$	$43 \cdot 211 \cdot 337$	240	1680
$7 \cdot 13 \cdot 61 \cdot 151$	$31 \cdot 41 \cdot 101 \cdot 331$	300	6600
$31 \cdot 181 \cdot 331$	$61 \cdot 661 \cdot 2521$	1980	27720
$11 \cdot 29 \cdot 61 \cdot 139$	$47 \cdot 1151 \cdot 1933$	9660	48300

Cuadro 6.2: Ejemplo de aplicación del corolario 46

La lista A207041 de la OEIS se titula «Carmichael numbers that can be written as a product of two Carmichael numbers» y está calculada a partir de la definición. Se buscan todos los pares (n, m) de números de Carmichael primos entre sí, se multiplican, se factorizan y finalmente se verifica que para cada factor primo p de nm, $p-1$ divida a $nm-1$. Evidentemente esto no es barato de hacer, pero queda asegurado haber encontrado todos los posibles productos en una lista determinada.

Divisibilidad Después de pensar en multiplicar números es inevitable pensar en la operación inversa. Está claro que las tablas que acabamos de calcular dan lugar a números de Carmichael que son divisibles, cada uno, por otros 2 números de Carmichael. También hay números divisibles solo por un número de Carmichael, basta con fijarse en un número n de este tipo y encontrar algún p que cumpla el teorema 38 de manera que np sea de Carmichael. De hecho, habiendo notado esto, si se toma la construcción de las formas universales de Chernick U_k, se tiene que dado un k, U_k es divisible por U_{k-1}, U_{k-2},..., U_3 y lo mismo pasa en el caso de las formas universales G_k, o cualquier otra fórmula construida recursivamente como estas. Por ejemplo, para $m = 380$, U_k es de Carmichael para $k \leq 6$ y por tanto:

$$(6 \cdot 380 + 1)(12 \cdot 380 + 1)(18 \cdot 380 + 1)(36 \cdot 380 + 1)(72 \cdot 380 + 1)(144 \cdot 380 + 1)$$

es un número de Carmichael que tiene tres divisores propios que también son de Carmichael. Los anexos E y F tienen más ejemplos.

Capítulo 7

Números de Carmichael módulo 4 y 6

Tal y como se dijo en la sección de pseudoprimos, los números de Carmichael pasaron durante mucho tiempo un test de primalidad (el pequeño teorema de Fermat), y es lógico preguntarse si lo siguen haciendo. Hoy en día, con los tests y los ordenadores modernos, eso es prácticamente imposible, pero es interesante estudiar un poco este tema.

La mayoría de los números de Carmichael cumplen que $n \equiv 1 \bmod 4$. Por ejemplo, los números de Chernick:

$$(6m+1)(12m+1)(18m+1) \equiv (2m+1)(2m+1) \equiv 1 \bmod 4$$

De los primeros 1124 números de Carmichael, solo 24 son de la forma $4k+3$ y se recogen en la tabla 7.1. Para entender este hecho, veamos qué condiciones tiene que cumplir un número de Carmichael $n = p_1 ... p_k = 4m+3$.

- Cada p_i debe ser a su vez de la forma $4h+3$
- k debe ser impar

Demostración. Si existiera un i tal que $p_i \not\equiv 3 \bmod 4$, entonces $p_i \equiv 1 \bmod 4$ y por el criterio de Korselt, $p_i - 1 = 4h$ dividiría a $n-1 = 2(2m+1)$, o equivalentemente, $2h$ a $2m+1$, lo que no es posible.
Para la paridad de factores primos, basta con observar que $3 \cdot 3 \equiv 1 \bmod 4$. □

Teniendo esto en cuenta, queda claro que para $n \equiv 1 \bmod 4$ hay muchas más formas de combinar primos que para el caso $n \equiv 3 \bmod 4$.

Nota: Si se lee la demostración de la cota del test de Rabin-Miller , se puede ver que el peor caso, es decir con probabilidad de fallo igual a $1/4$, se da justamente si el número que va a pasar el test es un número de Carmichael con 3 factores primos congruente con 3 módulo 4 [25].

Otro ejemplo similar es considerar los números de Carmichael en $\mathbb{Z}/(6)$. En este caso también la mayoría pertenece a la clase del 1. De los primeros 624, solo 23 no cumplen esta propiedad y se recogen en la tabla 7.2. Igual que para el caso anterior, se pueden estudiar las condiciones para que un número se pueda escribir como $6m+5$ o $6m+3$.

Sea n un número de Carmichael tal que $n \equiv 3$ o $5 \bmod 6$. Si p es un factor primo de n, debe ser a su vez congruente con 3 o 5 módulo 6, pues en caso contrario, $p - 1 = 6m$ dividiría a $n - 1 = 6k + 2 = 2(3k+1)$ (respectivamente a $n - 1 = 6k + 4 = 2(3k+2)$), es decir $3m$

n	factorización
8911	$7 \cdot 19 \cdot 67$
1024651	$19 \cdot 199 \cdot 271$
1152271	$43 \cdot 127 \cdot 211$
5481451	$31 \cdot 151 \cdot 1171$
10267951	$67 \cdot 331 \cdot 463$
14913991	$43 \cdot 127 \cdot 2731$
64377991	$163 \cdot 487 \cdot 811$
67902031	$43 \cdot 271 \cdot 5827$
139952671	$131 \cdot 571 \cdot 1871$
178482151	$151 \cdot 331 \cdot 3571$
368113411	$43 \cdot 631 \cdot 13567$
395044651	$199 \cdot 859 \cdot 2311$
612816751	$251 \cdot 751 \cdot 3251$
652969351	$271 \cdot 811 \cdot 2971$
743404663	$103 \cdot 1123 \cdot 6427$
1419339691	$7 \cdot 11 \cdot 19 \cdot 103 \cdot 9419$
1588247851	$211 \cdot 4111 \cdot 1831$
2000436751	$487 \cdot 1531 \cdot 2683$
2199931651	$379 \cdot 631 \cdot 9199$
2560600351	$239 \cdot 1667 \cdot 6427$
3102234751	$7 \cdot 11 \cdot 151 \cdot 251 \cdot 1063$
3215031751	$151 \cdot 751 \cdot 28351$
3411338491	$11 \cdot 71 \cdot 127 \cdot 163 \cdot 211$
4340265931	$19 \cdot 43 \cdot 107 \cdot 131 \cdot 379$

Cuadro 7.1: Primeros números de Carmichael n tales que $n \equiv 3 \bmod 4$

n	factorización	$n \bmod 6$
561	$3 \cdot 11 \cdot 17$	3
2465	$5 \cdot 17 \cdot 29$	5
62745	$3 \cdot 5 \cdot 47 \cdot 89$	3
162401	$17 \cdot 41 \cdot 233$	5
656601	$3 \cdot 11 \cdot 101 \cdot 197$	3
1909001	$41 \cdot 101 \cdot 461$	5
5444489	$29 \cdot 197 \cdot 953$	5
11921001	$3 \cdot 29 \cdot 263 \cdot 521$	3
19384289	$89 \cdot 353 \cdot 617$	5
26719701	$3 \cdot 29 \cdot 197 \cdot 1559$	3
45318561	$3 \cdot 29 \cdot 173 \cdot 3011$	3
84350561	$107 \cdot 743 \cdot 1061$	5
151530401	$11 \cdot 17 \cdot 71 \cdot 101 \cdot 113$	5
174352641	$3 \cdot 71 \cdot 641 \cdot 1277$	3
221884001	$131 \cdot 521 \cdot 3251$	5
230996949	$3 \cdot 53 \cdot 317 \cdot 4583$	3
275283401	$71 \cdot 701 \cdot 5531$	5
434932961	$41 \cdot 881 \cdot 12041$	5
662086041	$3 \cdot 89 \cdot 617 \cdot 4019$	3
684106401	$3 \cdot 11 \cdot 17 \cdot 401 \cdot 3041$	3
689880801	$3 \cdot 41 \cdot 71 \cdot 197 \cdot 401$	3
710382401	$137 \cdot 953 \cdot 5441$	5
939947009	$263 \cdot 1049 \cdot 3407$	5

Cuadro 7.2: Primeros números de Carmichael n tales que $n \not\equiv 1 \bmod 6$

dividiría a $3k+1$ (respectivamente a $3k+2$), lo que no es posible.
Se tiene

$$5^i \bmod 6 = \begin{cases} 1 & \text{si } i \text{ es par} \\ 5 & \text{si } i \text{ es impar} \end{cases}$$

En el caso en el que $p = 6m+3 = 3(2m+1)$ es primo, debe ser $m = 0$ y $p = 3$. Por último, $3 \cdot 5 \equiv 3 \bmod 6$. Conluyendo, si $n \equiv 3 \bmod 6$:

- evidentemente debe ser múltiplo de 3
- cualquier otro factor primo distinto de 3 debe ser de la forma $6m+5$

y si $n \equiv 5 \bmod 6$,

- los factores primos de n deben ser a su vez de la forma $6m+5$
- n debe tener un número impar de factores primos

Como última observación, a la vista de la tabla 7.2, se puede ver que hay una cantidad comparable de números de Carmichael congruentes con 3 y con 5 módulo 6.

A diferencia de otros números de Carmichael presentados en este trabajo, en 2012 se demostró que existen infinitos ejemplos de los tipos mencionados. El teorema que enunciamos a continuación, es el análogo para números de Carmichael del teorema de Dirichlet (ver página 6) sobre números primos en progresiones aritméticas.

Teorema 48 (T. Wright,[36])**.** *Sean a y m dos enteros positivos primos entre sí. Entonces existen infinitos números de Carmichael n tales que $n \equiv a \ mod \ m$.*

La demostración de este resultado sigue las líneas generales de [1] y no se corresponde con el nivel de este trabajo.

Nota: Queda demostrado que existen infinitos números de Carmichael en la sucesión $\{am+b\}$, sin embargo, puesto que $m.c.d.(a,b) = 1$, b no puede ser 0 si $a > 1$. Es decir, no se sabe si existen infinitos números de Carmichael de la forma bm.

Capítulo 8

Criptografía: el RSA

En general los números de Carmichael no constituyen ninguna amenaza para la fiabilidad de un test, pero supongamos que se da el caso y dicho número de Carmichael es usado en vez de un primo. Un caso interesante en este supuesto es el criptosistema de clave pública RSA [32]. Recordemos brevemente cómo funciona:

1. Se eligen dos primos (grandes) p y q.
2. Se calcula $n = p \cdot q$ y $(p-1)(q-1)$
3. Se escoge un entero positivo d menor que $(p-1)(q-1)$ y tal que $m.c.d.(d,(p-1)(q-1)) = 1$
4. Se calcula el inverso de d: $e \equiv d^{-1} \bmod (p-1)(q-1)$

La clave pública de un usuario es (e,n) y la clave privada (d,n). De esta manera, si se le quiere enviar un mensaje $m < n$ a este usuario, para cifrarlo basta con calcular $c = m^e \bmod n$ y para descifrarlo $m = c^d \bmod n$. En efecto, por ser p y q primos, se tiene $(p-1)(q-1) = \varphi(p) \cdot \varphi(q) = \varphi(pq)$, luego podemos escribir $e \cdot d = 1 + k\varphi(n)$ para algún k natural. Así,

$$m^{ed} \equiv m \cdot (m^{\varphi(n)})^k \equiv m \cdot 1 \bmod n$$

Se está aplicando el teorema de Euler, por lo tanto m y n deben ser primos entre sí, pero puede no darse el caso. Veamos que, en esa situación, el cifrado y el descifrado siguen funcionando: m debe ser menor que n entonces o bien p divide a m o bien q divide a m. Supongamos que p divide a m (lo que implica $m.c.d.(m,q) = 1$), entonces $m \equiv 0 \bmod p$ y trivialmente $m^{ed} \equiv m \bmod p$. Por otro lado, por el pequeño teorema de Fermat, $m^{q-1} \equiv 1 \bmod q$ y como $\varphi(n) = (q-1)(p-1)$, se tiene $m^{\varphi(n)} \equiv 1 \bmod q$ y así $m^{ed} \equiv m \bmod q$. Por tanto, como p y q son primos, $m^{ed} \equiv m \bmod pq$.

El siguiente lema sirve para demostrar que aunque no se usen números primos, el cifrado y el descifrado pueden seguir siendo funcionales.

Lema 49 (Huthnance y Warndof [16])**.** *Sea $n \in \mathbb{Z}$ tal que $a^n \equiv a \bmod n$ para cualquier entero a. Es decir, n es primo o de Carmichael. Entonces, para cualquier entero k*

$$a^{(n-1)k+1} \equiv a \bmod n$$

Demostración. Se probará que $a^{(n-1)k+1} - a$ es múltiplo de $a^n - a$ que, por hipótesis, es divisible por n.

$$\begin{aligned} a^{(n-1)k+1} - a &= a(a^{(n-1)k} - 1) \\ &= a(a^{n-1} - 1)(a^{(n-1)(k-1)} + a^{(n-1)(k-2)} + ... + a^{n-1} + a + 1) \\ &= (a^n - a)(a^{(n-1)(k-1)} + ... + a + 1) \end{aligned}$$

□

Veamos qué pasa si elegimos dos números de Carmichael p y q, primos entre sí, y los utilizamos en el RSA. Se siguen los pasos 2, 3 y 4 del algoritmo. Sea $m < p \cdot q$ el mensaje y m^e mod pq el mensaje cifrado. Hay que ver que $(m^e)^d$ mod pq efectivamente descifra el mensaje. Por cómo se definieron e y d, existe un k tal que $ed - 1 = (p-1)(q-1)k$. Aplicando el lema al número de Carmichael p y al producto $(q-1)k$ se demuestra el descifrado.

$$a^{(p-1)[(q-1)k]+1} \equiv a \bmod p \Leftrightarrow a^{ed-1+1} = a^{ed} \equiv a \bmod p$$

Huthnance y Warndof describieron un algoritmo para encontrar enteros que cumplieran el teorema de Fermat cuyo costo computacional es considerablemente más bajo que el de un test de primalidad estándar, alegando que ahorrarían cálculos sin reducir la seguridad. Afirman que aunque sea más fácil factorizar $n = pq$, esto se ve compensado por el problema combinatorio que supone encontrar cuáles son de hecho p y q. Una década después de haber publicado ese artículo, Pinch [26] advirtió del riesgo para la seguridad del sistema si efectivamente se utilizaban números compuestos.
Con la notación anterior, sea m^e mod n el mensaje cifrado. Si un espía es capaz de factorizar $n = p \cdot q$ siendo p y q números de Carmichael, entonces no le hace falta conocer la llave d, pues puede calcular fácilmente una clave privada alternativa $d' \equiv e^{-1} \bmod \lambda(n)$ para descifrar m^e. Para justificar la existencia de este inverso basta con notar que por ser p y q de Carmichael, $\lambda(p)$ divide a $p-1$ y $\lambda(q)$ divide a $q-1$. Además, $\lambda(n) = \lambda(m.c.m.(p,q))$ pues p y q son primos entre sí. Por tanto, como $\lambda(p)$ y $\lambda(q)$ dividen a $(p-1)(q-1)$, está claro que $\lambda(n) = m.c.m.(\lambda(p), \lambda(q))$ también divide a $(p-1)(q-1)$ y puesto que e no divide a $(p-1)(q-1)$, tampoco divide a ninguno de sus divisores. Es decir, $m.c.d.(e, \lambda(n)) = 1$ y e tiene inverso módulo $\lambda(n)$.

Si n y m son primos entre sí, se aplica el teorema 26 directamente para ver que d' efectivamente descifra el mensaje. Si no, como n no tiene factores primos repetidos, se puede escribir $n = p_1...p_k$ y examinar cada caso módulo p_i razonando igual que para el RSA estándar. Si p_i divide a m entonces la clase de m es 0, si no, se aplica el pequeño teorema de Fermat.

Capítulo 9

Generalizaciones

Las definiciones que se verán a continuación son fruto de la modificación del criterio de Korselt.

9.1. Super-números de Carmichael

El nombre de esta sección está dado por McIntosh [22].

Definición 15. *Sea un n un número de Carmichael. Se dice que n es un súper número de Carmichael si para todo primo p que divide a n, $p+1$ divide a $n-1$. Es decir, $n-1$ es múltiplo de $p-1$ y $p+1$.*

Recordemos que el test de Baillie-PSW (ver teorema 23) tenía dos pasos, uno de pseudoprimalidad fuerte en base 2 y uno de pseudoprimalidad de Lucas : si en el segundo paso no se exige que el símbolo de Jacobi $\left(\frac{D}{n}\right)$ sea -1, entonces un súper número de Carmichael pasa el test.

Lema 50. *Sea n un súper número de Carmichael. Entonces cada factor primo p de n cumple que $\dfrac{p^2-1}{2}$ divide a $\dfrac{n}{p}-p$.*

Demostración.

$$\begin{aligned} n-1 &= (p-1)\left(\frac{n}{p}+1\right)+\frac{n}{p}-p \\ &= (p+1)\left(\frac{n}{p}-1\right)-\frac{n}{p}+p = (p+1)\left(\frac{n}{p}-1\right)-\left(\frac{n}{p}-p\right) \end{aligned}$$

Como $p\pm 1$ divide a $n-1$, también debe dividir a $n/p-p$, por lo tanto $m.c.m.(p+1,p-1)$ divide a $n/p-p$. Como $p+1=(p-1)+2$ y $p\pm 1$ es par, $(p+1)(p-1)/2$ debe ser un divisor de $n-1$.

□

Teorema 51. *Sea n un súper-número de Carmichael. Entonces n tiene al menos 4 factores primos y el menor es mayor o igual que 5. Además $n\equiv 1$ mod 12.*

Demostración. Por ser n de Carmichael, ya se sabe que debe tener al menos 3 factores primos, todos impares. Sea $n=p_1\cdots p_k$ su factorización en números primos. En el conjunto $\{p_j-1,p_j,p_j+1\}$ hay al menos un múltiplo de 3 y si algún p_i fuera 3, tendría que dividir al

menos a uno de ellos. A p_j no lo puede dividir por ser primos distintos. Si p_i dividiera a $p_j \pm 1$, dividiría a su vez a $n-1$. Contradicción.

Por otro lado, como cada p es impar, debe ser $p \equiv 1$ o $3 \bmod 4$, con lo cual $p+1$ o $p-1$ es múltiplo de 4 y el otro de 2. Además, también uno de los dos debe ser múltiplo de 3, por lo tanto $(p^2-1)/2$ es múltiplo de 12. Por el lema anterior, $n/p - p$ también es múltiplo de 12, entonces $n \equiv p^2 \bmod 12$ y por tanto $n \equiv 1 \bmod 12$.

Para ver que tiene al menos 4 factores primos, se puede consultar [22]. □

Algunos ejemplos publicados por McIntosh:

$$17 \cdot 31 \cdot 41 \cdot 43 \cdot 89 \cdot 97 \cdot 167 \cdot 331$$
$$41 \cdot 53 \cdot 79 \cdot 103 \cdot 239 \cdot 271 \cdot 509$$
$$17 \cdot 37 \cdot 41 \cdot 71 \cdot 79 \cdot 97 \cdot 113 \cdot 131 \cdot 191$$
$$17 \cdot 61 \cdot 71 \cdot 89 \cdot 197 \cdot 311 \cdot 769 \cdot 2729$$
$$19 \cdot 41 \cdot 43 \cdot 71 \cdot 89 \cdot 127 \cdot 199 \cdot 449 \cdot 991$$
$$29 \cdot 37 \cdot 79 \cdot 181 \cdot 191 \cdot 449 \cdot 701 \cdot 3457$$
$$17 \cdot 29 \cdot 37 \cdot 41 \cdot 151 \cdot 199 \cdot 449 \cdot 571 \cdot 5851$$
$$41 \cdot 53 \cdot 79 \cdot 137 \cdot 139 \cdot 181 \cdot 239 \cdot 271 \cdot 1429$$
$$13 \cdot 17 \cdot 19 \cdot 29 \cdot 41 \cdot 89 \cdot 97 \cdot 127 \cdot 199 \cdot 251 \cdot 449$$
$$17 \cdot 23 \cdot 29 \cdot 37 \cdot 41 \cdot 43 \cdot 61 \cdot 109 \cdot 199 \cdot 419 \cdot 881$$

Para terminar esta sección, mencionaremos los números de William, denominados así por O.Echi [11].

Definición 16. *Se dice que un número de Carmichael n es un número de William si para todo primo p que divide a n, $p+1$ divide a $n+1$.*

Está demostrado que existen infinitos enteros tales que $p+1$ divide a $n+1$ para todo divisor primo p de n, y como ya sabemos, también está demostrado que existen infinitos enteros tales que $p-1$ divide a $n-1$ para todo divisor primo p de n. Los números de William son justamente la intersección de estos dos conjuntos de números. Sin embargo, a día de hoy, no se sabe si dichos conjuntos son disjuntos o no.

9.2. Orden

En [15], E.Howe define los números de Carmichael algebraicamente.

Teorema 52. *Un entero **compuesto** n es de Carmichael si y solo si la aplicación $x \mapsto x^n$ es un endomorfismo de $\mathbb{Z}/(n)$.*

Demostración.
Sea $n \in \mathbb{N}$ de Carmichael. Basta con probar que $(a+b)^n \equiv a^n + b^n \bmod n$, pues el resto de propiedades para que $x \mapsto x^n$ sea un endomorfismo de $\mathbb{Z}/(n)$ son inmediatas. Utilizando la segunda definición de la definición 12, se tiene por un lado $(a+b)^n \equiv a+b \bmod n$ y por otro

lado, $a^n \equiv a \bmod n$ y $b^n \equiv b \bmod n$, luego $a^n + b^n \equiv a + b \bmod n$.

Recíprocamente, veamos que si $(a+b)^n \equiv a^n + b^n \bmod n$, entonces n es de Carmichael. Para 1, se cumple la definición: $1^n \equiv 1 \bmod n$. Supongamos que se cumple para un a y veamos que sigue siendo cierto para $a+1$. Por hipótesis,

$$(a+1)^n \equiv a^n + 1 \bmod n$$

y por hipótesis de inducción $a^n \equiv a \bmod n$, por tanto $(a+1)^n \equiv a+1 \bmod n$ y n es de Carmichael. □

A partir de este teorema se consigue un nuevo tipo de números de Carmichael, los de orden m.

Definición 17. *Se dice que n es un número de Carmichael de orden m si es compuesto y la aplicación $x \mapsto x^n$ es un endomorfismo de cada $\mathbb{Z}/(n)$-álgebra que se puede generar como un $\mathbb{Z}/(n)$-módulo por m elementos.*

Definición equivalente.

Definición 18. *Sea n un entero compuesto y $m \in \mathbb{N}$. Entonces n es de Carmichael de orden m si y solo si*

- *n es libre de cuadrados*
- *Para todo divisor primo p de n, y para todo entero r tal que $0 < r \leq m$, existe un entero $i \geq 0$ que cumple $n \equiv p^i \bmod (p^r - 1)$.*

El caso particular en el que i es siempre nulo, se tiene la siguiente definición.

Definición 19. *Sea n un número de Carmichael. Se dice que es rígido de orden m si $p^r - 1$ divide a $n-1$ para todo divisor primo p de n y para todo entero r tal que $0 < r \leq m$.*

Notas:

- Es inmediato ver que todo número de Carmichael rígido de orden 2 es un súper-número de Carmichael, pues $p^2 - 1 = (p+1)(p-1)$ divide a $n-1$.
- Todos los números de Carmichael son rígidos de orden 1.
- El número $17 \cdot 31 \cdot 41 \cdot 43 \cdot 89 \cdot 97 \cdot 167 \cdot 331$ es el único número de Carmichael rígido de orden 2 menor que 10^{16}.

Otros ejemplos son:

$$31 \cdot 37 \cdot 101 \cdot 103 \cdot 109 \cdot 199 \cdot 419 \cdot 449 \cdot 521 \cdot 571 \cdot 911 \cdot 2089 \cdot 2551 \cdot 5851 \cdot 11969$$
$$41 \cdot 67 \cdot 79 \cdot 181 \cdot 199 \cdot 233 \cdot 239 \cdot 307 \cdot 449 \cdot 521 \cdot 1217 \cdot 1871 \cdot 4159 \cdot 5851 \cdot 9281$$
$$23 \cdot 43 \cdot 59 \cdot 61 \cdot 79 \cdot 89 \cdot 113 \cdot 131 \cdot 151 \cdot 191 \cdot 307 \cdot 311 \cdot 373 \cdot 419 \cdot 433 \cdot 463 \cdot 701 \cdot 1217 \cdot 2551$$

El número

$$23{\cdot}67{\cdot}71{\cdot}89{\cdot}109{\cdot}113{\cdot}191{\cdot}199{\cdot}233{\cdot}239{\cdot}271{\cdot}307{\cdot}373{\cdot}419{\cdot}521{\cdot}911{\cdot}929{\cdot}1153{\cdot}1217{\cdot}1429{\cdot}2089{\cdot}2729{\cdot}23561$$

también tiene orden 2 pero no es rígido pues es congruente con 1153 módulo $1153^2 - 1$.

En estos números, tomados de [15], observamos una gran cantidad de factores primos. Los siguientes resultados dan una cota inferior para el número de factores primo, aunque no es la que se esperaría a la vista de los ejemplos dados.

Proposición 53. *[12] Si m es un número de Carmichael de orden m entonces tiene al menos $m+2$ factores primos.*

Proposición 54. *[12] Si m es un número de Carmichael rígido de orden m entonces tiene al menos $s+2$ factores primos, donde*

$$s = \sum_{k \leq m} \varphi(k)$$

siendo $\varphi(k)$ la función de Euler.

9.3. a-número de Korselt

También llamados a-números de Carmichael, toman su nombre del criterio de Korselt (ver [11], [3]).

Definición 20. *Sea $n \in \mathbb{N} - \{0,1\}$ no primo y a un entero no nulo. Se dice que $n \neq a$ es un a-número de Korselt si cumple:*

- *n es libre de cuadrados*
- *$p - a$ divide a $n - a$ para todo divisor primo p de n.*

Nota: Los números de Carmichael son exactamente los 1-números de Korselt y los números de William los ± 1-números de Korselt.

Proposición 55 ([3])**.** *Sea n un a-número de Korselt. Se cumple:*

- *Si $a \leq 1$ entonces un a-número de Korselt tiene al menos 3 factores primos.*
- *Si $a > 1$, $p < q$ son dos números primos y $n = pq$, entonces $q \leq 4a - 3$. En particular, fijado a, hay una cantidad finita de a-números de Korselt con 2 factores primos.*
- *Si $a \neq 0$ y p y q son respectivamente el menor y el mayor de los factores primos de n, entonces $2q - n + 1 \leq a \leq \frac{n+p}{2}$*

Teorema 56 ([3])**.** *Sean p y q dos primos impares distintos y $a = p + q - 1$. Entonces $n = pq$ es un a-número de Korselt*

Demostración. Por definición, n es compuesto y libre de cuadrados. Además, $n - a = pq - p - q + 1 = (p-1)(q-1)$ es divisible por $p - a = -(q-1)$ y por $q - a = -(p-1)$, por tanto n es un a-número de Korselt. □

Teorema 57. *Sea p un número primo tal que $3p-2$ y $3p+2$ sean primos también. Sea $a \in \{\pm 3p, 5p\}$ Entonces $n = p(3p-2)(3p+2)$ es un a-número de Korselt.*

Demostración. Igual que en la demostración anterior, n es compuesto y libre de cuadrados. Falta ver que $q - a$ divide a $n - a$ para cada divisor primo q de n. Notemos que si p es 2, entonces $3p - 2$ no es primo y que si $3p + 2 = 2$ o si $3p - 2 = 2$, entonces p no es primo. Por lo tanto n es producto de 3 primos impares.

$p(3p-2)(3p+2)$	$5p$	$3p$
$3 \cdot 11 \cdot 7$	15	9
$5 \cdot 17 \cdot 13$	25	15
$7 \cdot 23 \cdot 19$	35	21
$13 \cdot 41 \cdot 37$	65	39
$23 \cdot 71 \cdot 67$	115	69
$37 \cdot 113 \cdot 109$	185	111
$43 \cdot 131 \cdot 127$	215	129

Cuadro 9.1: Los productos $p(3p-2)(3p+2)$ de esta tabla son $5p$ y $\pm 3p$-números de Korselt

$a = 3p$ Como n y p son impares, $n-3p$ es par y está claro que $(3p-2)-3p = -2$ y $(3p+2)-3p = 2$ dividen a $n-a$. Además, desarrollando $n-3p = 9p^3-7p = p(9p^2-7)$ se ve que es múltiplo de $p-3p = -2p$.

$a = -3p$ Para este caso escribimos $n-a = n+3p = 9p^3-p = p(3p-1)(3p+1)$ y observamos que $3p \pm 1$ es par y en consecuencia $n-a$ es divisible por 4. Es fácil deducir que $p+3p = 4p$, $(3p+2)+3p = 2(3p+1)$ y $(3p-2)+3p = 2(3p-1)$ son divisores de $n+3p$.

$a = 5p$ Igual que en el caso anterior, es fácil ver que $p-5p = -4p$, $(3p+2)-5p = -2(p-1)$ y $(3p-2)-5p = -2(p+1)$ dividen a $n-5p = 9p(p+1)(p-1)$.

□

9.4. Números de Knödel

Los números de Knödel son un ejemplo de generalización en la que no se modifica el criterio de Korselt, sino directamente la definición.

Definición 21. *Dado $i \in \mathbb{N}\backslash\{0\}$, se dice que un entero compuesto n está en el conjunto de Knödel C_i si $a^{n-i} \equiv 1$ mod n para todo a coprimo con n tal que $1 < a < n$.*

Teorema 58 (Makowski, ver [31] capítulo 2, Sección IX)**.** *Si $i \geq 2$, entonces cada C_i es infinito.*

Demostración. Dado i, se define $A = \{a \in \mathbb{Z} : \ 1 < a < i, \ m.c.d.(a,i) = 1\}$ y r_a como el orden de a módulo i. Sea

$$r = \prod_{a \in A} r_a$$

Por definición de r, $a^r \equiv 1 \bmod i$ para todo $a \in A$. Por otro lado, existen infinitos primos p tales que $p \equiv 1 \bmod r$ (aplicar teorema 5 con $u_k = 1+kr$). Para cada $p > i$, se pone $n = ip$ y veamos que n cumple la definición:

$$a^{n-i} = a^{ip-i} = a^{i(p-1)} = a^{ikr} \equiv 1 \bmod i$$

y por el pequeño teorema de Fermat

$$a^{n-i} = a^{i(p-1)} \equiv 1 \bmod p$$

Ahora, como p es primo y mayor que i, son primos entre sí y por tanto su producto divide a $a^{n-i}-1$, o equivalentemente, n pertenece a C_i. Puesto que hay infinitos p, también hay infinitos i. □

Gracias al trabajo de Alford, Granville y Pomerance [1], el teorema se puede extender a $i = 1$, que es el conjunto de los números de Carmichael. Comparada con la demostración de este resultado, la prueba del teorema 58 es muy elemental. En la siguiente tabla se muestran algunos números que pertenecen a un conjunto de Knödel (fuente: oeis.org)

C_2	C_3	C_4	C_5
4	9	6	25
6	15	8	65
8	21	12	85
10	33	16	145
12	39	20	165
14	51	24	185
22	57	28	205
24	63	40	265

Capítulo 10

Problemas abiertos y resueltos

Lo siguientes enunciados son problemas abiertos

- Erdös conjeturó lo siguiente: si $C(x)$ es la cantidad de números de Carmichael menores que x, entonces $C(x) > x^{1-\varepsilon}$ para algún $1 > \varepsilon > 0$
- ¿Existen infinitos números de Chernick? Es decir, números de Carmichael con 3 factores primos que se pueden descomponer como $n = (6m+1)(12m+1)(18m+1)$ y en general, ¿existen infinitos números de Carmichael construidos a partir de una forma universal cualquiera?
- ¿Existen infinitos números de Carmichael con exactamente k factores primos?
- ¿Existen infinitos números de Carmichael múltiplos de un $k \in \mathbb{Z}$ concreto?
- ¿Existen infinitos números de Carmichael que sean producto de otros dos?
- Dar un ejemplo de un número de Williams.
- Enumerar los tres primeros números de Carmichael de orden 2
- Dar un ejemplo de un número de Carmichael de orden 3.
- ¿Existen infinitos números de Carmichael de orden 2?
- ¿Existe alguna sucesión de números de Carmichael de manera que se vayan dividiendo sucesivamente?

A continuación veremos algunos resultados que estuvieron abiertos mucho tiempo. El primero y más importante es el de Alford, Granville y Pomerance en 1991 que demuestra que hay infinitos números de Carmichael (ver página 25), en particular demostraron que $C(x) > x^{2/7}$, cota que se ha mejorado hasta $x^{0,33}$ [14]. La demostración que dieron sirvió como modelo para la mayoría de los avances en esta materia. Por ejemplo, el artículo [36] de T. Wright que demuestra que si $m.c.d.(a,b) = 1$, entonces la sucesión $\{an+b\}_{n\in\mathbb{N}}$ contiene infinitos números de Carmichael, sigue las mismas técnicas y además se puede modificar para demostrar que existen infinitos números n tales que si p es primo y divide a n entonces $p+1$ divide a $n+1$. Otro ejemplo más reciente, es el artículo [2] de W. D. Banks y T. Freiberg en donde se prueba que hay infinitos números de Carmichael de manera que todos sus factores primos son de la forma $1+a^2+b^2$, siendo a y b primos entre sí.

J. Cilleruelo, J. Luca y A. Pizarro-Madariaga publicaron en 2016 un artículo en el que se prueba que solo hay una cantidad finita de números de Carmichael en la sucesión $\{k2^n + 1\}_{n \geq 1}$ (ver [8]).

Bibliografía

[1] Alford, W. R., Granville, A., & Pomerance, C. There are infinitely many Carmichael numbers. Annals of Mathematics, pág. 703-722, 1994.

[2] Banks, W. D., & Freiberg, T. Carmichael numbers and the sieve. Journal of Number Theory, vol. 165, (August) pág. 15-29, 2016.

[3] Bouallègue, K., Echi, O., & Pinch, R. G. Korselt numbers and sets. International Journal Of Number Theory, vol. 6, núm. 02, pág. 257-269, 2010.

[4] Buchmann, J. Introduction to cryptography. Springer Science & Business Media, 2013.

[5] Carmichael, R. D. Note on a new number theory function. Bulletin of the American Mathematical Society, vol. 16, núm. 5, pág. 232-238, 1910.

[6] Carmichael, R. D. On Composite Numbers P Which Satisfy the Fermat Congruence $a^P - 1 \equiv 1 \bmod P$. The American Mathematical Monthly, vol. 19, núm. 2, pág. 22-27, 1912.

[7] Chernick, J. On Fermat's simple theorem. Bulletin of the American Mathematical Society, vol. 45, núm. 4, pág. 269-274, 1939.

[8] Cilleruelo, J., Luca, F. & Pizarro-Madariaga, A. Carmichael Numbers in the sequence $(2^n k + 1)_{n \geq 1}$. Mathematics of Computation, vol. 85, núm. 297, pág. 357-377, 2016.

[9] Crocker, R. A theorem on pseudo-primes. The American Mathematical Monthly, vol 69, núm. 6, pág. 540, 1962.

[10] Dubner, H. A new method for producing large Carmichael numbers. Mathematics of Computation, vol. 53, núm. 187, pág. 411-414, 1989.

[11] Echi, O. Williams numbers. Mathematical Reports of the Academy of Sciences, vol. 29, núm. 2, pág. 41-47, 2007.

[12] Eterevsky, O. & Vsemirnov, M. On the number of primes divisors of high-order Carmichael numbers. Fibonacci Quarterly, vol. 42, núm. 2, pág. 141-148, 2004.

[13] Granville, A. Primality testing and Carmichael numbers. Notices of the American Mathematical Society, vol. 39, núm. 6, pág. 696-700, 1992.

[14] Harman, G. On the number of Carmichael numbers up to x. Bulletin of the London Mathematical Society, vol. 37, núm. 5, pág. 641-650, 2005.

[15] Howe, E. Higher-order Carmichael numbers. Mathematics of Computation of the American Mathematical Society, vol. 69, núm. 232, pág. 1711-1719, 2000.

[16] Huthnance, E. D., & Warndof, J. On using primes for public key encryption systems. Applied Mathematics Letters, vol. 1, núm. 3, pág. 225-227, 1988.

[17] Jameson, G. J. Finding Carmichael numbers. The Mathematical Gazette, vol. 95, núm. 533, pág. 244-255, 2011.

[18] Krizek, M., Luca, F., & Somer, L. 17 lectures on Fermat numbers: from number theory to geometry. Springer Science & Business Media, pág. 130-146, 2013.

[19] Korselt, A. Problème chinois. L'intermédiaire des mathématiciens, vol. 6,pág. 142-143, 1899.

[20] Marcos J.E. Teoría de números. Apuntes de clase,pág. 1-35, 2013.

[21] Maynard, J. Small gaps between primes. Annals of Mathematics, vol. 181, núm.1, pág. 383-413, 2015.

[22] McIntosh, R.J. Carmichael numbers with $(p+1)|(n-1)$. Integers14, núm. A59, 2014.

[23] McIntosh, R. J., & Dipra, M. Carmichael numbers with $p+1|n+1$. Journal of Number Theory, vol. 147, pág. 81-91, 2015.

[24] The On-Line Encyclopedia of Integer Sequences, sequence A002997.

[25] Pinch, R. G. The Carmichael numbers up to 10^{15}. Mathematics of Computation, vol. 61, núm. 203, pág. 381-391, 1993.

[26] Pinch, R. G. (1997). On using Carmichael numbers for public key encryption systems. En Crytography and Coding, pág. 265-269. Springer Berlin Heidelberg, 1997.

[27] Pomerance, C. A new lower bound for the pseudoprime counting function. Illinois J. Math, vol. 26,pág. 4-9, 1982.

[28] Pomerance, C. On composite n for which $\varphi(n)|n-1$. II. Pacific Journal of Mathematics, vol. 69, núm. 1, pág. 177-186, 1977.

[29] Pomerance, C., Selfridge, J. L., & Wagstaff, S. S. The pseudoprimes to $25{\cdot}10^9$. Mathematics of Computation, vol. 35, núm. 151, 1003-1026, 1980.

[30] Puertas, M. J. S. La Teoría Elemental de Números Y Su Historia. Aebius. pág. 89-95, 2012 .

[31] Ribenboim, P. The little book of bigger primes. Springer Science & Business Media, 2004.

[32] Rivest, R. L., Shamir, A., & Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, vol. 21, núm. 2, pág. 120-126, 1978

[33] Sarrus, F. Questions résolues. Démonstration de la fausseté du théorème énoncé à la page 320 du IX. e volume de ce recueil. Annales de Gergonne, vol. 10, pág. 184-187, 1819.

[34] Cerruti, U. Pseudoprimi di Fermat e numeri di Carmichael, página web personal de la Universidad de Turín.

[35] Wagstaff, S.S., Jr. Large Carmichael numbers. Math. J. Okayama University, vol. 22, pág. 33-41, 1980.

[36] Wright, T. Infinitely many Carmichael numbers in arithmetic progressions. Bulletin of the London Mathematical Society, vol. 45, núm. 5, pág. 943-952, 2012.

[37] Wright, T. The impossibility of certain types of Carmichael numbers. Integers12, núm. A31, 2012.

[38] Wright, T. Factors of Carmichael numbers and a weak k-tuples conjecture. Journal of the Australian Mathematical Society, First View Article, publicado en línea 17 noviembre de 2015.

[39] Woods, D., & Huenemann, J. Larger Carmichael numbers. Computers & Mathematics with Applications, vol. 8, núm. 3, pág. 215-216, 1982.

[40] Yorinaga, M. Carmichael numbers with many prime factors. Math. J. Okayama Univ, vol. 22, pág. 169-184, 1980.

[41] Yorinaga, M. Numerical computation of Carmichael numbers. Math. J. Okayama Univ, vol. 20, núm.2, artículo 7, 1978.

Apéndice A

Números de Carmichael

561	$3 \cdot 11 \cdot 17$	512461	$31 \cdot 61 \cdot 271$	3146221	$13 \cdot 31 \cdot 37 \cdot 211$
1105	$5 \cdot 13 \cdot 17$	530881	$13 \cdot 97 \cdot 421$	3224065	$5 \cdot 13 \cdot 193 \cdot 257$
1729	$7 \cdot 13 \cdot 19$	552721	$13 \cdot 17 \cdot 41 \cdot 61$	3581761	$29 \cdot 113 \cdot 1093$
2465	$5 \cdot 17 \cdot 29$	656601	$3 \cdot 11 \cdot 101 \cdot 197$	3664585	$5 \cdot 29 \cdot 127 \cdot 199$
2821	$7 \cdot 13 \cdot 31$	658801	$11 \cdot 13 \cdot 17 \cdot 271$	3828001	$101 \cdot 151 \cdot 251$
6601	$7 \cdot 23 \cdot 41$	670033	$7 \cdot 13 \cdot 37 \cdot 199$	4335241	$53 \cdot 157 \cdot 521$
8911	$7 \cdot 19 \cdot 67$	748657	$7 \cdot 13 \cdot 19 \cdot 433$	4463641	$7 \cdot 13 \cdot 181 \cdot 271$
10585	$5 \cdot 29 \cdot 73$	825265	$5 \cdot 7 \cdot 17 \cdot 19 \cdot 73$	4767841	$13 \cdot 19 \cdot 97 \cdot 199$
15841	$7 \cdot 31 \cdot 73$	838201	$7 \cdot 13 \cdot 61 \cdot 151$	4903921	$11 \cdot 31 \cdot 73 \cdot 197$
29341	$13 \cdot 37 \cdot 61$	852841	$11 \cdot 31 \cdot 41 \cdot 61$	4909177	$7 \cdot 13 \cdot 73 \cdot 739$
41041	$7 \cdot 11 \cdot 13 \cdot 41$	997633	$7 \cdot 13 \cdot 19 \cdot 577$	5031181	$19 \cdot 23 \cdot 29 \cdot 397$
46657	$13 \cdot 37 \cdot 97$	1024651	$19 \cdot 199 \cdot 271$	5049001	$31 \cdot 271 \cdot 601$
52633	$7 \cdot 73 \cdot 103$	1033669	$7 \cdot 13 \cdot 37 \cdot 307$	5148001	$41 \cdot 241 \cdot 521$
62745	$3 \cdot 5 \cdot 47 \cdot 89$	1050985	$5 \cdot 13 \cdot 19 \cdot 23 \cdot 37$	5310721	$13 \cdot 37 \cdot 61 \cdot 181$
63973	$7 \cdot 13 \cdot 19 \cdot 37$	1082809	$7 \cdot 13 \cdot 73 \cdot 163$	5444489	$29 \cdot 197 \cdot 953$
75361	$11 \cdot 13 \cdot 17 \cdot 31$	1152271	$43 \cdot 127 \cdot 211$	5481451	$31 \cdot 151 \cdot 1171$
101101	$7 \cdot 11 \cdot 13 \cdot 101$	1193221	$31 \cdot 61 \cdot 631$	5632705	$5 \cdot 13 \cdot 193 \cdot 449$
115921	$13 \cdot 37 \cdot 241$	1461241	$37 \cdot 73 \cdot 541$	5968873	$43 \cdot 127 \cdot 1093$
126217	$7 \cdot 13 \cdot 19 \cdot 73$	1569457	$17 \cdot 19 \cdot 43 \cdot 113$	6049681	$11 \cdot 31 \cdot 113 \cdot 157$
162401	$17 \cdot 41 \cdot 233$	1615681	$23 \cdot 199 \cdot 353$	6054985	$5 \cdot 53 \cdot 73 \cdot 313$
172081	$7 \cdot 13 \cdot 31 \cdot 61$	1773289	$7 \cdot 19 \cdot 67 \cdot 199$	6189121	$61 \cdot 241 \cdot 421$
188461	$7 \cdot 13 \cdot 19 \cdot 109$	1857241	$31 \cdot 181 \cdot 331$	6313681	$11 \cdot 17 \cdot 19 \cdot 1777$
252601	$41 \cdot 61 \cdot 101$	1909001	$41 \cdot 101 \cdot 461$	6733693	$109 \cdot 163 \cdot 379$
278545	$5 \cdot 17 \cdot 29 \cdot 113$	2100901	$11 \cdot 31 \cdot 61 \cdot 101$	6840001	$7 \cdot 17 \cdot 229 \cdot 251$
294409	$37 \cdot 73 \cdot 109$	2113921	$19 \cdot 31 \cdot 37 \cdot 97$	6868261	$43 \cdot 211 \cdot 757$
314821	$13 \cdot 61 \cdot 397$	2433601	$17 \cdot 37 \cdot 53 \cdot 73$	7207201	$17 \cdot 353 \cdot 1201$
334153	$19 \cdot 43 \cdot 409$	2455921	$13 \cdot 19 \cdot 61 \cdot 163$	7519441	$41 \cdot 241 \cdot 761$
340561	$13 \cdot 17 \cdot 23 \cdot 67$	2508013	$53 \cdot 79 \cdot 599$	7995169	$7 \cdot 13 \cdot 103 \cdot 853$
399001	$31 \cdot 61 \cdot 211$	2531845	$5 \cdot 19 \cdot 29 \cdot 919$	8134561	$37 \cdot 109 \cdot 2017$
410041	$41 \cdot 73 \cdot 137$	2628073	$7 \cdot 37 \cdot 73 \cdot 139$	8341201	$11 \cdot 31 \cdot 61 \cdot 401$
449065	$5 \cdot 19 \cdot 29 \cdot 163$	2704801	$11 \cdot 29 \cdot 61 \cdot 139$	8355841	$13 \cdot 41 \cdot 61 \cdot 257$
488881	$37 \cdot 73 \cdot 181$	3057601	$43 \cdot 211 \cdot 337$	8719309	$19 \cdot 37 \cdot 79 \cdot 157$

Fuente: OEIS, lista A002997

Apéndice B

Números de Carmichael con 3 factores primos

561	$3 \cdot 11 \cdot 17$	3581761	$29 \cdot 113 \cdot 1093$	35703361	$61 \cdot 277 \cdot 2113$
1105	$5 \cdot 13 \cdot 17$	3828001	$101 \cdot 151 \cdot 251$	36765901	$37 \cdot 613 \cdot 1621$
1729	$7 \cdot 13 \cdot 19$	4335241	$53 \cdot 157 \cdot 521$	37964809	$109 \cdot 379 \cdot 919$
2465	$5 \cdot 17 \cdot 29$	5049001	$31 \cdot 271 \cdot 601$	43331401	$43 \cdot 631 \cdot 1597$
2821	$7 \cdot 13 \cdot 31$	5148001	$41 \cdot 241 \cdot 521$	50201089	$97 \cdot 673 \cdot 769$
6601	$7 \cdot 23 \cdot 41$	5444489	$29 \cdot 197 \cdot 953$	53711113	$157 \cdot 313 \cdot 1093$
8911	$7 \cdot 19 \cdot 67$	5481451	$31 \cdot 151 \cdot 1171$	56052361	$211 \cdot 421 \cdot 631$
10585	$5 \cdot 29 \cdot 73$	5968873	$43 \cdot 127 \cdot 1093$	60957361	$61 \cdot 181 \cdot 5521$
15841	$7 \cdot 31 \cdot 73$	6189121	$61 \cdot 241 \cdot 421$	62756641	$109 \cdot 241 \cdot 2389$
29341	$13 \cdot 37 \cdot 61$	6733693	$109 \cdot 163 \cdot 379$	64377991	$163 \cdot 487 \cdot 811$
46657	$13 \cdot 37 \cdot 97$	6868261	$43 \cdot 211 \cdot 757$	67902031	$43 \cdot 271 \cdot 5827$
52633	$7 \cdot 73 \cdot 103$	7207201	$17 \cdot 353 \cdot 1201$	68154001	$151 \cdot 601 \cdot 751$
115921	$13 \cdot 37 \cdot 241$	7519441	$41 \cdot 241 \cdot 761$	79411201	$193 \cdot 257 \cdot 1601$
162401	$17 \cdot 41 \cdot 233$	8134561	$37 \cdot 109 \cdot 2017$	79624621	$139 \cdot 691 \cdot 829$
252601	$41 \cdot 61 \cdot 101$	9439201	$61 \cdot 271 \cdot 571$	82929001	$281 \cdot 421 \cdot 701$
294409	$37 \cdot 73 \cdot 109$	10024561	$71 \cdot 271 \cdot 521$	84350561	$107 \cdot 743 \cdot 1061$
314821	$13 \cdot 61 \cdot 397$	10267951	$67 \cdot 331 \cdot 463$	90698401	$103 \cdot 647 \cdot 1361$
334153	$19 \cdot 43 \cdot 409$	11972017	$43 \cdot 433 \cdot 643$	92625121	$181 \cdot 631 \cdot 811$
399001	$31 \cdot 61 \cdot 211$	14469841	$73 \cdot 379 \cdot 523$	96895441	$109 \cdot 433 \cdot 2053$
410041	$41 \cdot 73 \cdot 137$	14676481	$71 \cdot 421 \cdot 491$	99036001	$61 \cdot 541 \cdot 3001$
488881	$37 \cdot 73 \cdot 181$	14913991	$43 \cdot 127 \cdot 2731$	101649241	$61 \cdot 661 \cdot 2521$
512461	$31 \cdot 61 \cdot 271$	15247621	$61 \cdot 181 \cdot 1381$	104569501	$47 \cdot 1151 \cdot 1933$
530881	$13 \cdot 97 \cdot 421$	15829633	$43 \cdot 547 \cdot 673$	114910489	$127 \cdot 659 \cdot 1373$
1024651	$19 \cdot 199 \cdot 271$	17098369	$113 \cdot 337 \cdot 449$	115039081	$157 \cdot 313 \cdot 2341$
1152271	$43 \cdot 127 \cdot 211$	17236801	$151 \cdot 211 \cdot 541$	116682721	$281 \cdot 617 \cdot 673$
1193221	$31 \cdot 61 \cdot 631$	17316001	$53 \cdot 157 \cdot 2081$	118901521	$271 \cdot 541 \cdot 811$
1461241	$37 \cdot 73 \cdot 541$	19384289	$89 \cdot 353 \cdot 617$	124630273	$109 \cdot 229 \cdot 4993$
1615681	$23 \cdot 199 \cdot 353$	23382529	$97 \cdot 193 \cdot 1249$	127664461	$71 \cdot 421 \cdot 4271$
1857241	$31 \cdot 181 \cdot 331$	26280073	$73 \cdot 157 \cdot 2293$	133800661	$109 \cdot 541 \cdot 2269$
1909001	$41 \cdot 101 \cdot 461$	29111881	$211 \cdot 281 \cdot 491$	139952671	$131 \cdot 571 \cdot 1871$
2508013	$53 \cdot 79 \cdot 599$	31405501	$71 \cdot 631 \cdot 701$	146843929	$163 \cdot 379 \cdot 2377$
3057601	$43 \cdot 211 \cdot 337$	34657141	$191 \cdot 421 \cdot 431$	153589801	$151 \cdot 701 \cdot 1451$

Fuente: OEIS, lista A087788

Apéndice C

Números de Carmichael con 5 factores primos

825265	$5 \cdot 7 \cdot 17 \cdot 19 \cdot 73$
1050985	$5 \cdot 13 \cdot 19 \cdot 23 \cdot 37$
9890881	$7 \cdot 11 \cdot 13 \cdot 41 \cdot 241$
10877581	$11 \cdot 13 \cdot 29 \cdot 43 \cdot 61$
12945745	$5 \cdot 19 \cdot 29 \cdot 37 \cdot 127$
13992265	$5 \cdot 7 \cdot 19 \cdot 53 \cdot 397$
16778881	$7 \cdot 17 \cdot 19 \cdot 41 \cdot 181$
18162001	$11 \cdot 13 \cdot 17 \cdot 31 \cdot 241$
27336673	$7 \cdot 13 \cdot 23 \cdot 37 \cdot 353$
28787185	$5 \cdot 7 \cdot 19 \cdot 73 \cdot 593$
31146661	$7 \cdot 13 \cdot 31 \cdot 61 \cdot 181$
36121345	$5 \cdot 13 \cdot 17 \cdot 97 \cdot 337$
37167361	$7 \cdot 11 \cdot 41 \cdot 61 \cdot 193$
40280065	$5 \cdot 7 \cdot 67 \cdot 89 \cdot 193$
41298985	$5 \cdot 7 \cdot 13 \cdot 139 \cdot 653$
41341321	$7 \cdot 19 \cdot 31 \cdot 37 \cdot 271$
41471521	$7 \cdot 13 \cdot 31 \cdot 61 \cdot 241$
47006785	$5 \cdot 7 \cdot 17 \cdot 199 \cdot 397$
67371265	$5 \cdot 13 \cdot 37 \cdot 109 \cdot 257$
67994641	$11 \cdot 13 \cdot 37 \cdot 71 \cdot 181$
69331969	$7 \cdot 19 \cdot 37 \cdot 73 \cdot 193$
74165065	$5 \cdot 13 \cdot 59 \cdot 83 \cdot 233$
75151441	$17 \cdot 19 \cdot 29 \cdot 71 \cdot 113$
76595761	$11 \cdot 17 \cdot 31 \cdot 73 \cdot 181$
88689601	$7 \cdot 11 \cdot 13 \cdot 41 \cdot 2161$
93614521	$7 \cdot 11 \cdot 13 \cdot 41 \cdot 2281$
93869665	$5 \cdot 17 \cdot 29 \cdot 113 \cdot 337$
100427041	$11 \cdot 13 \cdot 17 \cdot 109 \cdot 379$
101957401	$7 \cdot 13 \cdot 19 \cdot 109 \cdot 541$
102090781	$13 \cdot 19 \cdot 31 \cdot 67 \cdot 199$
105117481	$7 \cdot 19 \cdot 37 \cdot 41 \cdot 521$

115542505	$5 \cdot 13 \cdot 43 \cdot 67 \cdot 617$
129255841	$11 \cdot 13 \cdot 19 \cdot 113 \cdot 421$
130032865	$5 \cdot 19 \cdot 97 \cdot 103 \cdot 137$
133205761	$13 \cdot 17 \cdot 41 \cdot 61 \cdot 241$
134857801	$13 \cdot 19 \cdot 29 \cdot 67 \cdot 281$
140241361	$13 \cdot 29 \cdot 41 \cdot 43 \cdot 211$
145124785	$5 \cdot 13 \cdot 43 \cdot 137 \cdot 379$
151530401	$11 \cdot 17 \cdot 71 \cdot 101 \cdot 113$
158404141	$7 \cdot 31 \cdot 37 \cdot 109 \cdot 181$
161242705	$5 \cdot 13 \cdot 17 \cdot 337 \cdot 433$
161913961	$11 \cdot 31 \cdot 37 \cdot 41 \cdot 313$
169057801	$11 \cdot 19 \cdot 41 \cdot 109 \cdot 181$
169570801	$17 \cdot 19 \cdot 29 \cdot 43 \cdot 421$
172430401	$11 \cdot 13 \cdot 31 \cdot 97 \cdot 401$
173085121	$11 \cdot 31 \cdot 53 \cdot 61 \cdot 157$
175997185	$5 \cdot 7 \cdot 13 \cdot 503 \cdot 769$
181154701	$7 \cdot 13 \cdot 37 \cdot 173 \cdot 311$
182356993	$7 \cdot 13 \cdot 73 \cdot 97 \cdot 283$
187188001	$7 \cdot 11 \cdot 13 \cdot 41 \cdot 4561$
188689501	$7 \cdot 11 \cdot 13 \cdot 251 \cdot 751$
193708801	$11 \cdot 13 \cdot 31 \cdot 37 \cdot 1181$
225745345	$5 \cdot 7 \cdot 23 \cdot 193 \cdot 1453$
241242001	$7 \cdot 11 \cdot 13 \cdot 401 \cdot 601$
242641153	$17 \cdot 19 \cdot 37 \cdot 79 \cdot 257$
266003101	$7 \cdot 13 \cdot 37 \cdot 199 \cdot 397$
270857521	$11 \cdot 19 \cdot 41 \cdot 73 \cdot 433$
280761481	$7 \cdot 11 \cdot 13 \cdot 41 \cdot 6841$
292776121	$11 \cdot 31 \cdot 41 \cdot 43 \cdot 487$
296559361	$7 \cdot 31 \cdot 73 \cdot 97 \cdot 193$
301704985	$5 \cdot 43 \cdot 47 \cdot 73 \cdot 409$
302751505	$5 \cdot 7 \cdot 103 \cdot 137 \cdot 613$

Fuente: OEIS, lista A112428

Apéndice D

Números de Carmichael con 7 y 9 factores primos

Números de Carmichael con 7 factores primos	
5394826801	$7 \cdot 13 \cdot 17 \cdot 23 \cdot 31 \cdot 67 \cdot 73$
6295936465	$5 \cdot 7 \cdot 13 \cdot 37 \cdot 47 \cdot 73 \cdot 109$
12452890681	$7 \cdot 11 \cdot 19 \cdot 31 \cdot 37 \cdot 41 \cdot 181$
13577445505	$5 \cdot 13 \cdot 17 \cdot 19 \cdot 59 \cdot 97 \cdot 113$
15182481601	$7 \cdot 17 \cdot 19 \cdot 31 \cdot 53 \cdot 61 \cdot 67$
20064165121	$7 \cdot 11 \cdot 13 \cdot 37 \cdot 41 \cdot 73 \cdot 181$
22541365441	$7 \cdot 17 \cdot 23 \cdot 37 \cdot 41 \cdot 61 \cdot 89$
24673060945	$5 \cdot 13 \cdot 19 \cdot 29 \cdot 37 \cdot 43 \cdot 433$
26242929505	$5 \cdot 13 \cdot 23 \cdot 37 \cdot 67 \cdot 73 \cdot 97$
26602340401	$7 \cdot 13 \cdot 17 \cdot 19 \cdot 37 \cdot 61 \cdot 401$
27405110161	$11 \cdot 13 \cdot 19 \cdot 37 \cdot 41 \cdot 61 \cdot 109$
28553256865	$5 \cdot 7 \cdot 17 \cdot 37 \cdot 73 \cdot 109 \cdot 163$
33203881585	$5 \cdot 7 \cdot 17 \cdot 19 \cdot 37 \cdot 163 \cdot 487$
38059298641	$7 \cdot 13 \cdot 17 \cdot 31 \cdot 37 \cdot 89 \cdot 241$
39696166081	$11 \cdot 13 \cdot 17 \cdot 19 \cdot 61 \cdot 73 \cdot 193$
40460634865	$5 \cdot 7 \cdot 17 \cdot 53 \cdot 79 \cdot 109 \cdot 149$

Números de Carmichael con 9 factores primos	
9746347772161	$7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 31 \cdot 37 \cdot 41 \cdot 641$
11537919313921	$7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 37 \cdot 61 \cdot 97 \cdot 163$
11985185775745	$5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 37 \cdot 73 \cdot 109 \cdot 277$
14292786468961	$7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 31 \cdot 61 \cdot 97 \cdot 241$
23239986511105	$5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 67 \cdot 89 \cdot 1153$
24465723528961	$11 \cdot 13 \cdot 19 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 61 \cdot 73$
26491881502801	$11 \cdot 13 \cdot 17 \cdot 19 \cdot 29 \cdot 31 \cdot 37 \cdot 43 \cdot 401$
27607174936705	$5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 67 \cdot 73 \cdot 193 \cdot 199$
30614445878401	$7 \cdot 11 \cdot 17 \cdot 19 \cdot 31 \cdot 37 \cdot 61 \cdot 73 \cdot 241$
30912473358481	$11 \cdot 13 \cdot 17 \cdot 29 \cdot 31 \cdot 41 \cdot 43 \cdot 71 \cdot 113$
34830684315505	$5 \cdot 13 \cdot 17 \cdot 23 \cdot 29 \cdot 37 \cdot 89 \cdot 113 \cdot 127$
51620128928641	$7 \cdot 13 \cdot 17 \cdot 31 \cdot 37 \cdot 47 \cdot 61 \cdot 73 \cdot 139$

Fuente: OEIS, listas A112430 y A112432

Apéndice E

Números de Carmichael que son producto de otros 2

n_1		n_2		n_1n_2
1729	$7 \cdot 13 \cdot 19$	294409	$37 \cdot 73 \cdot 109$	509033161
15841	$7 \cdot 31 \cdot 73$	115921	$13 \cdot 37 \cdot 241$	1836304561
15841	$7 \cdot 31 \cdot 73$	340561	$13 \cdot 17 \cdot 23 \cdot 67$	5394826801
488881	$37 \cdot 73 \cdot 181$	41041	$7 \cdot 11 \cdot 13 \cdot 41$	20064165121
15841	$7 \cdot 31 \cdot 73$	1615681	$23 \cdot 199 \cdot 353$	25594002721
2465	$5 \cdot 17 \cdot 29$	19384289	$89 \cdot 353 \cdot 617$	47782272385
1461241	$37 \cdot 73 \cdot 541$	41041	$7 \cdot 11 \cdot 13 \cdot 41$	59970791881
15841	$7 \cdot 31 \cdot 73$	4767841	$13 \cdot 19 \cdot 97 \cdot 199$	75527369281
15841	$7 \cdot 31 \cdot 73$	5310721	$13 \cdot 37 \cdot 61 \cdot 181$	84127131361
512461	$31 \cdot 61 \cdot 271$	188461	$7 \cdot 13 \cdot 19 \cdot 109$	96578912521
6601	$7 \cdot 23 \cdot 41$	17586361	$13 \cdot 61 \cdot 67 \cdot 331$	116087568961
15841	$7 \cdot 31 \cdot 73$	17586361	$13 \cdot 61 \cdot 67 \cdot 331$	278585544601
9439201	$61 \cdot 271 \cdot 571$	41041	$7 \cdot 11 \cdot 13 \cdot 41$	387394248241
488881	$37 \cdot 73 \cdot 181$	852841	$11 \cdot 31 \cdot 41 \cdot 61$	416937760921
314821	$13 \cdot 61 \cdot 397$	1857241	$31 \cdot 181 \cdot 331$	584698468861
530881	$13 \cdot 97 \cdot 421$	3057601	$43 \cdot 211 \cdot 337$	1623222276481
3057601	$43 \cdot 211 \cdot 337$	552721	$13 \cdot 17 \cdot 41 \cdot 61$	1690000282321
41041	$7 \cdot 11 \cdot 13 \cdot 41$	43584481	$17 \cdot 31 \cdot 191 \cdot 433$	1788750684721
115921	$13 \cdot 37 \cdot 241$	16778881	$7 \cdot 17 \cdot 19 \cdot 41 \cdot 181$	1945024664401
15841	$7 \cdot 31 \cdot 73$	133205761	$13 \cdot 17 \cdot 41 \cdot 61 \cdot 241$	2110112460001
115921	$13 \cdot 37 \cdot 241$	20964961	$17 \cdot 19 \cdot 47 \cdot 1381$	2430279244081
314821	$13 \cdot 61 \cdot 397$	8830801	$7 \cdot 19 \cdot 67 \cdot 991$	2780121601621
488881	$37 \cdot 73 \cdot 181$	6189121	$61 \cdot 241 \cdot 421$	3025743663601
115921	$13 \cdot 37 \cdot 241$	27402481	$31 \cdot 43 \cdot 61 \cdot 337$	3176523000001
15841	$7 \cdot 31 \cdot 73$	216821881	$331 \cdot 661 \cdot 991$	3434675416921
1461241	$37 \cdot 73 \cdot 541$	2455921	$13 \cdot 19 \cdot 61 \cdot 163$	3588692457961
115921	$13 \cdot 37 \cdot 241$	34196401	$17 \cdot 47 \cdot 127 \cdot 337$	3964081000321
96895441	$109 \cdot 433 \cdot 2053$	41041	$7 \cdot 11 \cdot 13 \cdot 41$	3976685794081
15841	$7 \cdot 31 \cdot 73$	346808881	$19 \cdot 23 \cdot 37 \cdot 89 \cdot 241$	5493799483921
8911	$7 \cdot 19 \cdot 67$	652969351	$271 \cdot 811 \cdot 2971$	5818609886761
1461241	$37 \cdot 73 \cdot 541$	4463641	$7 \cdot 13 \cdot 181 \cdot 271$	6522455238481

n_1		n_2		n_1n_2
115921	$13 \cdot 37 \cdot 241$	60957361	$61 \cdot 181 \cdot 5521$	7066238244481
14676481	$71 \cdot 421 \cdot 491$	552721	$13 \cdot 17 \cdot 41 \cdot 61$	8111999254801
314821	$13 \cdot 61 \cdot 397$	26474581	$7 \cdot 19 \cdot 67 \cdot 2971$	8334754065001
115921	$13 \cdot 37 \cdot 241$	75151441	$17 \cdot 19 \cdot 29 \cdot 71 \cdot 113$	8711630192161
115921	$13 \cdot 37 \cdot 241$	76595761	$11 \cdot 17 \cdot 31 \cdot 73 \cdot 181$	8879057210881
1857241	$31 \cdot 181 \cdot 331$	5031181	$19 \cdot 23 \cdot 29 \cdot 397$	9344115631621
46657	$13 \cdot 37 \cdot 97$	214850881	$7 \cdot 109 \cdot 193 \cdot 1459$	10024297554817
3581761	$29 \cdot 113 \cdot 1093$	3057601	$43 \cdot 211 \cdot 337$	10951596015361
41041	$7 \cdot 11 \cdot 13 \cdot 41$	277241401	$31 \cdot 61 \cdot 271 \cdot 541$	11378264338441
5148001	$41 \cdot 241 \cdot 521$	2433601	$17 \cdot 37 \cdot 53 \cdot 73$	12528180381601
334153	$19 \cdot 43 \cdot 409$	37964809	$109 \cdot 379 \cdot 919$	12686054821777
1461241	$37 \cdot 73 \cdot 541$	8719921	$7 \cdot 23 \cdot 41 \cdot 1321$	12741906081961
488881	$37 \cdot 73 \cdot 181$	27402481	$31 \cdot 43 \cdot 61 \cdot 337$	13396552313761
115921	$13 \cdot 37 \cdot 241$	119327041	$61 \cdot 73 \cdot 127 \cdot 211$	13832509919761
10585	$5 \cdot 29 \cdot 73$	1349671681	$37 \cdot 109 \cdot 379 \cdot 883$	14286274743385
3146221	$13 \cdot 31 \cdot 37 \cdot 211$	5031181	$19 \cdot 23 \cdot 29 \cdot 397$	15829207317001
1857241	$31 \cdot 181 \cdot 331$	8719921	$7 \cdot 23 \cdot 41 \cdot 1321$	16194994797961
1857241	$31 \cdot 181 \cdot 331$	8830801	$7 \cdot 19 \cdot 67 \cdot 991$	16400925680041
3057601	$43 \cdot 211 \cdot 337$	6049681	$11 \cdot 31 \cdot 113 \cdot 157$	18497510675281
3057601	$43 \cdot 211 \cdot 337$	6189121	$61 \cdot 241 \cdot 421$	18923862558721
115921	$13 \cdot 37 \cdot 241$	169570801	$17 \cdot 19 \cdot 29 \cdot 43 \cdot 421$	19656816822721
15841	$7 \cdot 31 \cdot 73$	1295577361	$13 \cdot 17 \cdot 89 \cdot 199 \cdot 331$	20523240975601
15841	$7 \cdot 31 \cdot 73$	1376844481	$19 \cdot 37 \cdot 61 \cdot 97 \cdot 331$	21810593423521
3057601	$43 \cdot 211 \cdot 337$	8341201	$11 \cdot 31 \cdot 61 \cdot 401$	25504064518801
488881	$37 \cdot 73 \cdot 181$	56052361	$211 \cdot 421 \cdot 631$	27402934298041
115921	$13 \cdot 37 \cdot 241$	250200721	$19 \cdot 31 \cdot 421 \cdot 1009$	29003517779041
15841	$7 \cdot 31 \cdot 73$	1932608161	$11 \cdot 17 \cdot 19 \cdot 37 \cdot 61 \cdot 241$	30614445878401
3057601	$43 \cdot 211 \cdot 337$	10402561	$13 \cdot 29 \cdot 41 \cdot 673$	31806880916161
399001	$31 \cdot 61 \cdot 211$	82929001	$281 \cdot 421 \cdot 701$	33088754328001
334153	$19 \cdot 43 \cdot 409$	105309289	$37 \cdot 73 \cdot 127 \cdot 307$	35189414847217
838201	$7 \cdot 13 \cdot 61 \cdot 151$	42490801	$31 \cdot 41 \cdot 101 \cdot 331$	35615831889001

Este apéndice se calculó a partir de la lista A207041 de la OEIS que se corresponde con la columna n_1n_2 de la tabla. Con ayuda de *MAPLE* se buscaron los correspondientes n_1 y n_2.

Apéndice F

Números de Carmichael divisibles por otro número de Carmichael

Múltiplos de otro número de Carmichael: $n \cdot m$ donde n es de Carmichael	
$1729 \cdot 37$	$(7 \cdot 13 \cdot 19) \cdot 37$
$1729 \cdot 73$	$(7 \cdot 13 \cdot 19) \cdot 73$
$2821 \cdot 61$	$(7 \cdot 13 \cdot 31) \cdot 61$
$1729 \cdot 109$	$(7 \cdot 13 \cdot 19) \cdot 109$
$2465 \cdot 113$	$(5 \cdot 17 \cdot 29) \cdot 113$
$1729 \cdot 433$	$(7 \cdot 13 \cdot 19) \cdot 433$
$1729 \cdot 577$	$(7 \cdot 13 \cdot 19) \cdot 577$
$8911 \cdot 199$	$(7 \cdot 19 \cdot 67) \cdot 199$
$29341 \cdot 181$	$(13 \cdot 37 \cdot 61) \cdot 181$
$6601 \cdot 1321$	$(7 \cdot 23 \cdot 41) \cdot 1321$
$8911 \cdot 991$	$(7 \cdot 19 \cdot 67) \cdot 991$
$41041 \cdot 241$	$(7 \cdot 11 \cdot 13 \cdot 41) \cdot 241$
$8911 \cdot 1783$	$(7 \cdot 19 \cdot 67) \cdot 1783$
$75361 \cdot 241$	$(11 \cdot 13 \cdot 17 \cdot 31) \cdot 241$
$8911 \cdot 2971$	$(7 \cdot 19 \cdot 67) \cdot 2971$
$46657 \cdot 577$	$(13 \cdot 37 \cdot 97) \cdot 577$
$2821 \cdot 11041$	$(7 \cdot 13 \cdot 31) \cdot 61 \cdot 181$
$1105 \cdot 32689$	$(5 \cdot 13 \cdot 17) \cdot 97 \cdot 337$
$10585 \cdot 3529$	$(5 \cdot 29 \cdot 73) \cdot 3529$
$2821 \cdot 14701$	$(7 \cdot 13 \cdot 31) \cdot 61 \cdot 241$
$41041 \cdot 2281$	$(7 \cdot 11 \cdot 13 \cdot 41) \cdot 2281$
$2465 \cdot 38081$	$(5 \cdot 17 \cdot 29) \cdot 113 \cdot 337$
$1729 \cdot 58969$	$(7 \cdot 13 \cdot 19) \cdot 109 \cdot 541$
$46657 \cdot 2593$	$(13 \cdot 37 \cdot 97) \cdot 2593$
$252601 \cdot 601$	$(41 \cdot 61 \cdot 101) \cdot 601$

Números de Carmichael múltiplos de 1729
$1729 \cdot (37)$
$1729 \cdot (73)$
$1729 \cdot (109)$
$1729 \cdot (433)$
$1729 \cdot (577)$
$1729 \cdot (109 \cdot 541)$
$1729 \cdot (37 \cdot 73 \cdot 109)$
$1729 \cdot (193 \cdot 2113)$
$1729 \cdot (577 \cdot 1153)$
$1729 \cdot (37 \cdot 73 \cdot 397)$
$1729 \cdot (61 \cdot 97 \cdot 277)$
$1729 \cdot (109 \cdot 37693)$
$1729 \cdot (37 \cdot 109 \cdot 1153)$
$1729 \cdot (619 \cdot 8563)$
$1729 \cdot (31 \cdot 271 \cdot 709)$
$1729 \cdot (3889 \cdot 2161)$
$1729 \cdot (919 \cdot 14851)$
$1729 \cdot (109 \cdot 271 \cdot 811)$
$1729 \cdot (23 \cdot 1063 \cdot 1181)$
$1729 \cdot (41 \cdot 461 \cdot 1549)$
$1729 \cdot (193 \cdot 166849)$
$1729 \cdot (37 \cdot 41 \cdot 137 \cdot 181)$

Esta lista está contenida en la anterior

Fuente: OEIS, listas A214758 y A212920