UNA INTRODUCCIÓN A LOS NÚMEROS DE CARMICHAEL

BRAYAN ARLEY PANTOJA MORA

FACULTAD DE CIENCIAS EXACTAS Y NATURALES
DEPARTAMENTO DE MATEMÁTICAS Y ESTADÍSTICA
UNIVERSIDAD DE NARIÑO
SAN JUAN DE PASTO
2017

UNA INTRODUCCIÓN A LOS NÚMEROS DE CARMICHAEL

BRAYAN ARLEY PANTOJA MORA

Trabajo presentado como requisito parcial para optar al título de Licenciado en Matemáticas

Asesor
John Hermes Castillo Gómez
Doctor en Matemáticas

FACULTAD DE CIENCIAS EXACTAS Y NATURALES
DEPARTAMENTO DE MATEMÁTICAS Y ESTADÍSTICA
UNIVERSIDAD DE NARIÑO
SAN JUAN DE PASTO
2017

Nota de Responsabilidad

Todas las ideas y conclusiones aportadas en el siguiente trabajo son responsabilidad exclusiva de los autores.

Artículo 1^{ro} del Acuerdo No. 324 de octubre 11 de 1966 emanado por el Honorable Consejo Directivo de la Universidad de Nariño.

Nota de aceptación

_____

_____

_____

_____

JOHN HERMES CASTILLO GÓMEZ

_____

Director.

GIBERTO GARCÍA PULGARÍN

_____

Jurado 1.

WILSON FERNANDO MUTIS CANTERO

_____

Jurado 2.

San Juan de Pasto, noviembre 20 de 2017

Este trabajo está dedicado a:
Mi madre Rosa Mora como reconocimiento a su amor, apoyo, consejos y por todos sus esfuerzos por sacarme adelante.
Brayan

Agradecimientos

Al término de este trabajo de grado es ineludible expresar mis sentimientos de agradecimiento primeramente a Dios por regalarme la vida y la salud, como también su sabiduría, conocimiento y fortaleza en cualquier momento de dificultad en toda esta larga etapa.

En segundo lugar agradezco a mi madre Rosa Mora quien con su gran amor y sabios concejos inculcó en mi valores de humildad, respeto, responsabilidad, paciencia y dedicación. Con sus palabras llenas de amor y bondad a hecho de mi una mejor persona, y me ha enseñado a creer en mi, a no rendirme ante nada y a que todo en la vida tiene una solución. Finalmente le doy las gracias por todos los esfuerzos realizados para que nunca me falte nada y hoy en día pueda alcanzar esta meta.

En tercer lugar expreso mis sentimientos de gratitud al profesor John Castillo, puesto que con su calidad profesional y humana siempre mostró buena disposición al momento de asesorar este trabajo, como también gracias a su amistad y concejos motivadores han generado en mi cierto interés en el estudio del álgebra y la teoría de números.

Finalmente agradezco a mi padre Jesus Pantoja por todo el apoyo brindado durante el transcurso de mi carrera profesional, a los profesores del departamento de matemáticas y estadística, a mis amigos y a mi querida Universidad de Nariño que tanto quiero y respeto.

Resumen

El Pequeño Teorema de Fermat, formulado por Pierre de Fermat en 1636 y demostrado por primera vez por Leonhard Euler en 1736, establece que si p es primo y a un entero primo relativo con p, entonces el resto de la división de a^{p-1} entre p es 1. Sin embargo, esto no solo sucede con los primos, puesto que también existen enteros compuestos impares n para los cuales el residuo de dividir a^{n-1} entre n es 1 para todo a primo relativo con n. Estos enteros se llaman números de Carmichael, debido a que fue Robert Carmichael el que encontró el primero de ellos, el 561, en 1910.

En este trabajo se estudian algunas de las características principales de estos números, algunos métodos que permiten encontrarlos y una generalización de ellos, conocida recientemente como números super-Carmichael. Además, se presentan ejemplos para aclarar los conceptos estudiados, algunos de ellos mediante algoritmos implementados en el sistema de computo libre de matemáticas `SAGE`. Estas implementaciones se dan en el Apéndice, puesto que se espera que las mismas puedan ser utilizadas en futuros trabajos de investigación.

Abstract

Fermat's little theorem, was formulated by Pierre de Fermat on 1636 and demonstrated by the first time for Leonhard Euler in 1736. It states that if p is a prime number and a is relatively prime to p, then the remainder of the division of a^{p-1} between p is 1. However, this does not only happens with prime numbers, in fact there are also compounds odd numbers n for which this result is also true. Such as integers are called Carmichael numbers, in honour of Robert Carmichael who found the first example, 561, in 1910.

In this thesis, we study some of the main characteristics of these numbers, some methods that allow us to find them and a recent generalization, called super-Carmichael numbers. In addition, examples are presented to clarify the concepts studied, some of them by means of algorithms implemented in the free open-source mathematics software system called `SAGE`.

Índice general

Introducción

Alrededor del año 1636, Pierre de Fermat enunció un teorema interesante relacionado con números primos. Este como se menciona en [4], aparece en una de sus cartas a su confidente Frénicle de Bessy, fechada el 18 de octubre de 1640. Escrito en notación moderna este resultado dice: $a^{p-1} \equiv 1$ (mód p) cuando p sea primo y a sea primo relativo con p, y se conoce como el Pequeño Teorema de Fermat.

Adicionalmente, surge la pregunta: ¿existen enteros compuestos positivos impares n tal $a^{n-1} \equiv 1$ (mód n) para algún a primo relativo con n? En respuesta a este interrogante, en 1819 Pierre Sarrus probó que para el número compuesto 341, $2^{340} \equiv 1$ (mód 341), por lo que se tenía el primer ejemplo de tales enteros compuestos impares n que cumplían con el teorema planteado por Fermat. En realidad, estos enteros luego fueron llamados *Seudoprimos* y su generalización *Seudoprimos base* a cuando a es diferente de 2. Un siglo más tarde, en 1912 Robert Daniel Carmichael encontró el primer ejemplo de un número compuesto impar n, tal que, $a^{n-1} \equiv 1$ (mód n) para todo entero a primo relativo con n. Estos números reciben el nombre de *Seudoprimos absolutos* o *números de Carmichael*, en honor de su descubridor.

El objetivo en este trabajo es recopilar y presentar de forma ordenada algunos resultados y aspectos teóricos conocidos acerca de los números de Carmichael, y con base en ellos implementar algoritmos en el sistema de cómputo libre `SAGE` [7] que permitan ejemplificar la teoría estudiada.

Este trabajo está dividido en 4 capítulos. En el Capítulo 1 se muestran algunos resultados que son necesarios para la comprensión de los capítulos subsecuentes. En el Capítulo 2 se presenta una introducción al estudio de los números seudoprimos y unas características básicas de los números de Carmichael. En el tercer capítulo, se expone un método de la autoría de J. Chernick[3], que sirve para construir números de Carmichael con tres divisores primos, y su extensión para $d \geq 3$ factores primos. Además, se demuestra un resultado de H. Duparc, ver [6], donde se prueba, que dado un entero impar libre de cuadrado P, existe un número finito de números de Carmichael de la forma Pqr, con q, r primos y $P < q < r$.

Adicionalmente en el Capítulo 4, se exhibe una generalización de los números de Carmichael, llamados *super-Carmichael*, por R. McIntosh [11] y se muestra algunas propiedades que los identifican.

Finalmente, en el Apéndice 4.1, se encuentran los algoritmos que permiten ejemplificar algunos de los resultados presentados en este trabajo, que fueron implementados en el sistema de cómputo libre `SAGE` [7].

Capítulo 1

Preliminares

Se estudian en este capítulo algunos conceptos de aritmética general y álgebra, que son la base para la temática estudiada en este trabajo. Por ser una recopilación de temas básicos de cualquier curso de teoría elemental de números y grupos, encontrados por ejemplo en [15] y [10], se omitirán las pruebas de estos mismos.

1.1. Divisibilidad

Definición 1.1. Se dice que un entero b es divisible por un entero $a \neq 0$, y se denota por $a \mid b$ si existe un entero c tal que

$$b = ac.$$

Con $a \nmid b$ se denota que b no es divisible por a. Es fácil verificar que para todo entero k, $1|k$ y si $k \neq 0$, $k|k$. Además, para decir que b es divisible por a, también se puede decir que

a es un divisor de b,
a es un factor de b,
b es un múltiplo de a.

Teorema 1.1. *Supongamos que a, b y c son números enteros. Entonces.*

1. *Si $a \neq 0$ entonces $a|0$, $a|a$, $a|(-a)$.*
2. *$1|a$, $(-1)|a$.*
3. *Si $a|b$ entonces $a|bc$.*
4. *Si $a|b$ y $b|c$ entonces $a|c$.*

5. *Si* $a|b$ *y* $a|c$ *entonces para todo* $x, y \in Z$, $a|(bx + cy)$.

6. *Si* $a|b$ *y* $b \neq 0$ *entonces* $|a| \leq |b|$.

7. *Si* $a|b$ *y* $b|a$ *entonces* $a = b$ *o* $a = (-b)$.

Definición 1.2 (Máximo común divisor)**.** Dados dos enteros a y b (con al menos uno de los dos diferentes de cero), el mayor entero que divide a y b se denomina el máximo común divisor de a y b, y se denota por (a, b).

Es decir, si $(a, b) = d$ entonces

1. $d|a$ y $d|b$.

2. Si $c|a$ y $c|b$, entonces $c \leq d$.

Teorema 1.2 (Algoritmo de la División)**.** *Dados dos enteros* a *y* b, *con* $b > 0$, *existen unos únicos enteros* q *y* r *tales que*

$$a = bq + r \qquad 0 \leq r < b.$$

Los enteros q *y* r *se llaman, respectivamente, el cociente y el residuo en la división de* a *por* b.

Definición 1.3. Dos enteros positivos a y b se dice que son primos relativos si $(a, b) = 1$. Esto es, si el único factor común positivo que tienen es 1.

Lema 1.1 (Euclides)**.** *Si* $a \mid bc$ *y* $(a, b) = 1$, *entonces* $a \mid c$.

Definición 1.4. Un entero $p > 1$ se llama un número primo, o simplemente un primo, si sus únicos divisores positivos son 1 y p. Un entero mayor que 1 que no es primo se denomina compuesto.

De este modo si p es primo y $p \mid ab$, del lema de Euclides se sigue que $p \mid a$ ó $p \mid b$.

Teorema 1.3. *Sean* $p, p_1, p_2, \ldots, p_n$ *primos y* $c, a_1, a_2, \ldots, a_m$ *enteros. Entonces*

1. *Si* $p|a_1 a_2 \cdots a_m$, *entonces* $p|a_i$ *para algún* i, $1 \leq i \leq m$.

2. *Si* $p|p_1 p_2 \cdots p_n$, *entonces* $p = p_i$ *para algún* $i, 1 \leq i \leq n$.

3. *Si* $a_1, a_2, \ldots, a_m$ *son enteros primos relativos dos a dos y para cada* $i = 1, 2, \ldots, m$ $a_i|c$, *entonces* $a_1 a_2 \cdots a_n|c$.

Un resultado muy importante en la matemática, particularmente en teoría de números y que se usará con mucha frecuencia en los resultados subsecuentes de este y los posteriores capítulos es el siguiente.

Teorema 1.4 (Fundamental de la aritmética)**.** *Todo entero positivo $n > 1$ se puede expresar como un producto de primos, $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, donde cada k_i es un entero positivo. Esta representación es única, sin tener en cuenta el orden en el que aparecen los factores.*

Definición 1.5 (Mínimo común múltiplo)**.** El mínimo común múltiplo de dos enteros a y b, denotado por $\text{mcm}(a, b)$, es el menor entero positivo m tal que

1. $a \mid m$ y $b \mid m$.
2. si $a \mid c$ y $b \mid c$, entonces $m \leq c$. Donde c es un entero positivo.

Teorema 1.5. *Sean $a_1, a_2, \ldots, a_n$ enteros positivos. Entonces*

$$\text{mcm}(a_1, a_2, \ldots, a_n) = \text{mcm}(\text{mcm}(a_1, a_2, \ldots, a_{n-1}), a_n).$$

Corolario 1.1. *Sean $a_1, a_2, \ldots, a_n$ y b enteros positivos tal que $a_i \mid b$ para $1 \leq i \leq n$. Entonces* $\text{mcm}(a_1, a_2, \ldots, a_n) \mid b$.

Corolario 1.2. *Sean $a_1, a_2, \ldots, a_n$ enteros positivos primos relativos, entonces el* $\text{mcm}(a_1, a_2, \ldots, a_n) = a_1 a_2 \cdots a_n$.

1.2. Congruencias

Congruencia es un término usado en Teoría de Números para designar que dos números a y b dejan el mismo residuo al dividirlos por un número natural m diferente de cero llamado módulo. La noción de congruencia fue introducida por Carl Friedrich Gauss, y se expresa utilizando la notación

$$a \equiv b \pmod{m}.$$

Y se dice que a es congruente con b módulo m. Una definición alternativa es la siguiente.

Definición 1.6. Sea m un entero fijo. Dos enteros a y b se dice que son congruentes módulo m, y se denota por $a \equiv b \pmod{m}$. Si $m \mid a - b$. Es decir, existe k en los enteros, tal que $a - b = km$.

Cuando $m \nmid a - b$, se dice que a y b son incongruentes módulo m y se denota $a \not\equiv b \pmod{m}$.

Teorema 1.6 (Propiedades)**.** *Sea $m > 0$ y a, b, c enteros arbitrarios, entonces.*

1. $a \equiv a \pmod{m}$.
2. *Si* $a \equiv b \pmod{m}$, *entonces* $b \equiv a \pmod{m}$.
3. *Si* $a \equiv b \pmod{m}$ *y* $b \equiv c \pmod{m}$, *entonces* $a \equiv c \pmod{m}$.

4. *Si* $a \equiv b \pmod{m}$ *y* $c \equiv d \pmod{m}$, *entonces* $a + c \equiv b + d \pmod{m}$, $ac \equiv bd \pmod{m}$.

5. *Si* $a \equiv b \pmod{m}$, *entonces* $a + c \equiv b + c \pmod{m}$, $ac \equiv bc \pmod{m}$.

6. *Si* $a \equiv b \pmod{m}$, *entonces* $a^k \equiv b^k \pmod{m}$, *para cualquier entero positivo* k.

Teorema 1.7. *Si* $ac \equiv bc \pmod{m}$, *entonces* $a \equiv b \pmod{\frac{m}{(c,m)}}$.

Teorema 1.8. *Si* $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_n}$. *Entonces* $a \equiv b \pmod{\text{mcm}(m_1, m_2, \ldots, m_n)}$.

Particularmente, cuando los m_i son primos relativos, por el Corolario 1.2, $a \equiv b \pmod{m_1 m_2 \cdots m_n}$.

Lema 1.2. *Sea* p *primo y* a *un entero tal que* $p \nmid a$. *Entonces los menores residuos de los enteros* a, $2a$, $3a$,..., $(p-1)a$ *módulo* p, *son una permutación de los enteros* 1, 2, 3,..., $(p-1)$.

Lema 1.3. *Sea* p *primo y* k *un entero tal que* $1 \leq k \leq p-1$. *Entonces* $\binom{p}{k} \equiv 0 \pmod{p}$, *donde el coeficiente binómico* $\binom{p}{k}$ *esta dado por*

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\cdots(p-k+1)}{1 \cdot 2 \cdots k}$$

Teorema 1.9. *La congruencia lineal* $ax \equiv b \pmod{m}$ *tiene solución si y solo si* $(a, m) \mid b$. *Si* $(a, m) \mid b$ *la congruencia tiene* (a, m) *soluciones módulo* m.

Un resultado importante conocido por los antiguos chinos utilizado para resolver sistemas de congruencias lineales con módulos primos relativos dos a dos es el siguiente.

Teorema 1.10 (Chino del residuo)**.** *Sean* $a_1, a_2, \ldots, a_n$ *enteros arbitrarios y* $m_1, m_2, \ldots, m_n$ *primos relativos dos a dos. Existe un único entero* x, *módulo*

$$m = \prod_{i=1}^{n} m_i,$$

tal que $x \equiv a_i \pmod{m_i}$.

1.3. Función ϕ de Euler

Una función aritmética es una aplicación f cuyo dominio de definición es el conjunto de enteros positivos.

Definición 1.7. Sea n un entero mayor que 1, por $\phi(n)$ se denota el número de enteros positivos menores o iguales que n que son primos relativos con n.

Definición 1.8. La función aritmética f es multiplicativa si para todo par de enteros positivos primos relativos n y m

$$f(mn) = f(m)f(n).$$

Teorema 1.11. *La función ϕ es una función multiplicativa.*

Es decir, si n y m son enteros positivos y $(n, m) = 1$, entonces $\phi(mn) = \phi(m)\phi(n)$.

Lema 1.4. *Si p es primo y $k > 1$, entonces*

$$\phi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p}).$$

De ahí que cuando $n > 1$ tiene la factorización prima $n = p_1^{k_1} p_2^{k_2} \cdots p_d^{k_d}$, entonces

$$\phi(n) = \prod_{i=1}^{d} (p_i^{(k_i-1)}(p_i - 1)).$$

Lema 1.5. *Sea $n > 1$ y $(a, n) = 1$. Si $a_1, a_2, \ldots, a_{\phi(n)}$ son los enteros positivos menores que n y primos relativos con n, entonces $aa_1, aa_2, \ldots, aa_{\phi(n)}$ son congruentes módulo n en algún orden con $a_1, a_2, \ldots, a_{\phi(n)}$.*

1.4. Grupos

Definición 1.9 (Operación binaria)**.** Sea G un conjunto. Una operación binaria en G es una función que asigna a cada pareja ordenada de elementos de G un elemento en G.

Definición 1.10 (Grupo)**.** Sea G un conjunto con una operación binaria (usualmente llamada multiplicación), que asigna a cada pareja ordenada (a, b) de elementos de G un elemento en G denotado por ab. Se dice que G es un grupo bajo esta operación si se satisfacen las siguientes propiedades.

1. *Asociativa.* La operación es asociativa, esto es, $a(bc) = (ab)c$ para todo a, b, c en G.
2. *Identidad.* Existe un elemento e (llamado identidad) en G tal que $ae = ea = a$ para todo a en G.
3. *Inverso.* Para cada elemento a en G, existe un elemento b en G (llamado el inverso de a) tal que $ab = ba = e$.

En adelante, en este trabajo se denotara como 1 al elemento identidad de un grupo G y como a^{-1} al inverso de un elemento a en G.

Definición 1.11. Si G es un grupo (finito o infinito), el número de elementos en G se denomina su orden y se denota como $|G|$.

Definición 1.12. El orden de un elemento a en un grupo G es el menor entero positivo n tal que $a^n = 1$, siendo 1 el elemento identidad del grupo.

Definición 1.13 (Grupos cíclicos)**.** Un grupo G se dice que es cíclico si existe un elemento a, en G, tal que $G = \{a^n; n \in \mathbb{Z}\}$. En este caso diremos que a es un generador de G.

Teorema 1.12. *El conjunto* $\mathbb{U}_n = \{a \in \mathbb{Z}; 1 < a < n,\ y\ (a, n) = 1\}$*, conjunto de enteros positivos inferiores a* n *y primos relativos con* n*, es un grupo multiplicativo.*

Teorema 1.13. *Sea* m *un entero positivo. El grupo* $\mathbb{U}_n$ *es cíclico si y solo si* n *pertenece al conjunto* $\{2, 4, p^n, 2p^n\}$*, para* $p > 2$ *siendo* p *un primo.*

Teorema 1.14. *Sea* G *un grupo.* 1 *su elemento identidad y* $a \in G$ *de orden* h*, entonces* $a^t = 1$ *si y solo si* $h \mid t$*.*

Teorema 1.15. *Si* G *es un grupo cíclico de orden* n *y* 1 *su elemento identidad, la ecuación* $x^m = 1$ *tiene exactamente* (m, n) *soluciones.*

1.5. Polinomios ciclotomicos

El n-ésimo polinomio ciclotómico $\Phi_n(X)$, en $\mathbb{Q}[X]$, es el polinomio mónico cuyos ceros son exactamente las raíces primitivas n-ésimas de la unidad. Es decir, $\Phi_n(X)$ es el producto de los binomios de la forma $(X - w)$ donde w recorre los números complejos tales que $w^n = 1$ y $w^k \neq 1$ si $k < n$. Por tanto su grado es $\phi(n)$. Este polinomio puede definirse en un cuerpo cualquiera, en este caso solo se trabajará en el campo $\mathbb{Q}$ de los números racionales, Así

$$\Phi_n(X) = \prod_{w_i \in G_n^*} (X - w_i).$$

Donde G_n^* designa el conjunto de las raices n-ésimas primitivas de la unidad. Por ejemplo

$$\Phi_1(X) = X - 1,$$

$$\Phi_2(X) = X + 1,$$

$$\Phi_4(X) = (X - i)(X + i) = X^2 + 1.$$

Teorema 1.16. *Para todo $n \geq 3$ se tiene*

1. *$\Phi_n(X)$ tiene coeficientes reales.*
2. *$\Phi_n(0) = 1$.*
3. *$\Phi_n(b) > 0$ para todo real b.*

Teorema 1.17. *Para todo $n \geq 1$ se tiene*

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

Como consecuencia del teorema anterior, se tiene que si t es divisor de n, entonces

$$\frac{X^n - 1}{X^t - 1} = \prod_{\substack{d|n \\ d\nmid t}} \Phi_d(X).$$

Al hacer $n = p$ y $t = 1$, con p primo, se tiene el siguiente teorema.

Teorema 1.18. *Si p es primo, entonces*

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = 1 + X + X^2 + \cdots + X^{(p-1)}.$$

Es posible demostrar por inducción a partir de la relación en el Teorema 1.17 que $\Phi_n(X)$ es siempre un polinomio con coeficientes enteros. En particular, es posible evaluarlos en los elementos de $\mathbb{Z}_n$ (o más generalmente, de cualquier anillo).

Capítulo 2

Seudoprimos y números de Carmichael

El propósito de este capítulo es presentar la definición de seudoprimo y la de número de Carmichael en su condición de seudoprimo absoluto. El prefijo **seudo** significa *falso*. Así, al hablar de seudoprimo se hace referencia a un número que es un falso primo. Estas ideas surgieron a través de una reconsideración de un teorema enunciado por Pierre de Fermat, alrededor de 1636. En la actualidad, este resultado escrito en notación moderna afirma que si p es primo y $p \nmid a$, entonces $a^{p-1} \equiv 1 \pmod{p}$, y se conoce como el Pequeño Teorema de Fermat. En este capítulo se presentará su enunciado formal, su demostración y sus influencias para definir los conceptos centrales de la temática estudiada en gran parte del contenido de esta monografía. Adicionalmente, se presentan tablas que exhiben números relacionados con este trabajo. Algunas de estas tablas se pueden obtener por medio de los algoritmos presentados en el Apéndice 4.1 y se pueden encontrar en el sitio web *The On-Line Encyclopedia of Integer Sequences*, ver [14].

2.1. El Pequeño Teorema de Fermat

El 18 de octubre de 1640, Pierre de Fermat escribió una carta a Bernhard Frenicle de Bessy (1605 - 1675), un funcionario de la casa de la moneda francesa quien fue un alumno talentoso de teoría de números. En su carta, Fermat comunicó el siguiente resultado: Si p es un primo y p no divide a a, entonces p divide a $a^{p-1} - 1$. Fermat no proporcionó una prueba de este resultado, pero adjuntó una nota prometiendo que él enviaría luego una prueba, siempre que ésta no fuese demasiado larga. Sin embargo, la primera demostración del Pequeño Teorema de Fermat fue dada en 1736, por Leonhard Euler, ver [8].

Posteriormente, diversos estudiosos en matemáticas han presentado diferentes pruebas del resultado antes mencionado, utilizando distintas herramientas como aritmética modular, teoría de grupos, teoría de anillos, teoría de campos finitos, etc. La demostración presentada en este trabajo es por medio de aritmética modular, se usará por tanto algunos de los lemas y teoremas presentados en el Capítulo 1.

Teorema 2.1 (Pequeño Teorema de Fermat, P. Fermat, 1640)**.** *Sea p un primo y a un entero tal que $p \nmid a$, entonces $a^{p-1} \equiv 1 \pmod{p}$.*

Demostración. Por el Lema 1.2, los menores residuos de los enteros a, $2a$, $3a$,..., $(p-1)a$ módulo p son los enteros 1, 2, 3,..., $(p-1)$ en algún orden, así sus productos son congruentes módulo p; esto es,

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}.$$

En otras palabras, $(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}$. Pero $((p-1)!, p) = 1$, así por el Teorema 1.7, $a^{p-1} \equiv 1 \pmod{p}$. □

En otras ocasiones el Pequeño Teorema de Fermat también se enuncia como se muestra en el siguiente corolario.

Corolario 2.1. *Si p es primo, entonces $a^p \equiv a \pmod{p}$ para cualquier entero a.*

Demostración. Si $p \mid a$, claramente $a^p \equiv a \pmod{p}$. Ahora si $p \nmid a$, del teorema anterior $a^{p-1} \equiv 1 \pmod{p}$, multiplicando por a en ambos lados de esta congruencia se tiene el resultado. □

Ejemplo 2.1. Algunos ejemplos son

$$3^{42} \equiv 1 \pmod{43},$$
$$2^{97} \equiv 2 \pmod{97}.$$

Euler no solo probó el Pequeño Teorema de Fermat. En 1760, generalizó este resultado de un primo p a un entero arbitrario n. Este memorable resultado dice que: si a y n son primos relativos, entonces $a^{\phi(n)} \equiv 1 \pmod{n}$.

Teorema 2.2 (L. Euler, 1760)**.** *Sean a y n enteros tales que $(a, n) = 1$, entonces*

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

Demostración. Sin pérdida de generalidad se puede suponer que n es un entero mayor que 1. Sean $a_1, a_2, \ldots, a_{\phi(n)}$ los enteros menores que n y primos relativos con n. Como $(a, n) = 1$, se sigue del lema 1.5 que los enteros $aa_1, aa_2, \ldots, aa_{\phi(n)}$ son congruentes en algún orden a $a_1, a_2, \ldots, a_{\phi(n)}$. Entonces

$$(aa_1)(aa_2)\cdots(aa_{\phi(n)}) \equiv a_1a_2\cdots a_{\phi(n)} \pmod{n},$$

de donde

$$a^{\phi(n)}(a_1a_2\cdots a_{\phi(n)}) \equiv a_1a_2\cdots a_{\phi(n)} \pmod{n}.$$

Como $(a_i, n) = 1$ para cada i, entonces $(a_1a_2\cdots a_{\phi(n)}, n) = 1$, por tanto

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

□

Particularmente si p es primo, $\phi(p) = p - 1$; de aquí, cuando $(a, p) = 1$, se tiene que $a^{p-1} \equiv a^{\phi(p)} \equiv 1 \pmod{p}$.

2.2. Seudoprimos base a

Se podría pensar que el Pequeño Teorema de Fermat da condiciones necesarias y suficientes para garantizar que un entero positivo impar n es primo. Más precisamente, se imaginaría que si n es un entero tal que $2^{n-1} \equiv 1 \pmod{n}$ entonces n es primo. Sin embargo esto no siempre es cierto, puesto que en 1819, Pierre Sarrus probó que $2^{340} \equiv 1 \pmod{341}$ y $341 = 11 \times 31$ no es primo, por lo que el Pequeño Teorema de Fermat solo da condiciones necesarias para que un entero positivo sea primo, más no dá condiciones suficientes. Enteros como 341 motivan la siguientes definiciones.

Definición 2.1. Sea n un entero positivo impar compuesto. Se dice que n es seudoprimo, y se denota por $sp(2)$ si

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

Ejemplo 2.2. Los primeros seis seudoprimos son 341, 561, 645, 1105, 1387 y 1729. Ver A001567

Del mismo modo, para otras bases a diferente de 2, existen enteros positivos compuestos impares n tales que $a^{n-1} \equiv 1 \pmod{n}$. Por ejemplo, se puede verificar que $3^{90} \equiv 1 \pmod{91}$ y $4^{14} \equiv 1 \pmod{15}$.

Definición 2.2 (Seudoprimos base a)**.** Sean n un entero impar compuesto y a un entero primo relativo con n, se dice que n es seudoprimo base a si

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

y se escribe n es $sp(a)$.

Ejemplo 2.3. En la siguiente tabla se muestra los menores seudoprimos para las bases dadas.

Base a	**Menor** $sp(a)$
2	$341 = 11 \times 31$
3	$91 = 13 \times 7$
5	$217 = 7 \times 31$
7	$25 = 5 \times 5$

Tabla 2.1: Menor seudoprimo para algunas bases dadas.

Ejemplo 2.4. En la tabla se muestra los menores n que son seudoprimos simultáneamente para las bases dadas.

Base a	**Menor** $sp(a)$
$2, 3$	$1105 = 5 \times 13 \times 17$
$2, 5$	$561 = 3 \times 11 \times 17$
$3, 5$	$1541 = 23 \times 67$
$2, 3, 5$	$1729 = 13 \times 7 \times 19$
$2, 3, 5, 7$	$29341 = 13 \times 37 \times 61$

Tabla 2.2: Menor seudoprimo para un conjunto de bases dadas.

Nótese que en los ejemplos de la tabla anterior todos los seudoprimos son libres de cuadrado. Sin embargo esto no es una característica propia de ellos, puesto que se han encontrado seudoprimos que no son libres de cuadrado. Para la base 2 los menores contraejemplos son: $1194649 = 1093^2$, $12327121 = 3511^2$ y $3914864773 = 29 \times 13 \times 1093^2$.

Por otro lado, el contrareciproco del Pequeño Teorema de Fermat sirve como herramienta para determinar cuando un entero es compuesto. Así, el Pequeño Teorema de Fermat es un criterio de no primalidad del entero n. Este criterio se conoce como el criterio de Fermat y decide la *compositez* o *composición* -calidad de ser compuesto- de un entero n sin hallar ningún factor de n. Por ejemplo, en el caso de 341, a pesar de que $2^{340} \equiv 1 \pmod{341}$, $3^{340} \not\equiv 1 \pmod{341}$. Es decir, 3 decide la compositez de 341. Este hecho lleva a definir el siguiente concepto.

Definición 2.3 (Testigo de compositez)**.** Si a y n son primos relativos y $a^{n-1} \not\equiv 1 \pmod{n}$, se dice que a es un testigo de composición o compositez de n, bajo el criterio de Fermat. Si no se sabe si n

es primo o compuesto y se verifica que $a^{n-1} \equiv 1 \pmod{n}$ se dice que n es un probable primo base a.

Ejemplo 2.5. Para los enteros 217 y 1541, 3 y 2 son testigos de compositez respectivamente, puesto que $3^{216} \not\equiv 1 \pmod{217}$ y $2^{1540} \not\equiv 1 \pmod{1541}$, lo que muestra que son compuestos.

En la siguiente proposición, se presentan algunas propiedades que poseen los seudoprimos base a.

Proposición 2.1. *Sean n, a y b enteros con $(n, a) = 1$ y $(n, b) = 1$. Entonces se satisfacen las siguientes propiedades.*

1. *Si n es $sp(a)$ y n es $sp(b)$, entonces n es $sp(ab)$.*
2. *Si n es $sp(a)$ y a^{-1} es el inverso de a módulo n, entonces n es $sp(a^{-1})$.*
3. *Si n tiene algún testigo de compositez, entonces n tiene al menos, $\frac{\phi(n)}{2}$ testigos de compositez menores que n.*

Demostración. Para probar la primera afirmación, como $a^{n-1} \equiv 1 \pmod{n}$ y $b^{n-1} \equiv 1 \pmod{n}$, por el cuarto ítem del Teorema 1.6 se tiene $(ab)^{n-1} \equiv 1 \pmod{n}$. Por lo que n es $sp(ab)$.

En el segundo caso, dado que $a^{n-1} \equiv 1 \pmod{n}$, y como $aa^{-1} \equiv 1 \pmod{n}$. Por el sexto ítem del Teorema 1.6, $(a)^{n-1}(a^{-1})^{n-1} \equiv 1 \pmod{n}$. Es decir, $(a^{-1})^{n-1} \equiv 1 \pmod{n}$, así n es $sp(a^{-1})$.

Por último, sean $S \subseteq \mathbb{U}_n$ el conjunto de bases para las que n es seudoprimo y $T \subseteq \mathbb{U}_n$ el conjunto de testigos de compositez de n.
Sea $b_j \in T$. Si n es $sp(b_j a_i)$ para algunos i, j. Se sigue de 1 y 2 que n es $sp(b_j a_i a_i^{-1})$, es decir, n es $sp(b_j)$ lo que contradice la elección de b_j. De este modo, $b_j a_i \in T$ para cualquier i.
Por lo tanto, si n tiene algún testigo de compositez, n no sería seudoprimo para ninguna base o existe una aplicación inyectiva f entre las bases para las cuales n es seudoprimo y los testigos de compositez, esto es

$$\begin{aligned} f : S &\longmapsto T \\ a_i &\longmapsto b_j a_i. \end{aligned}$$

Esto implica que $|S| \leq |T|$, y como $\mathbb{U}_n = S \cup T$ y, S y T son conjuntos disjuntos, entonces $\phi(n) = |S| + |T|$, se tiene que

$$\phi(n) = |S| + |T| \leq 2\,|T|\,,$$

lo que muestra que $|T| \geq \frac{\phi(n)}{2}$. □

Ejemplo 2.6. De la Tabla 2.4, se sabe que el entero 1105 es $sp(2)$ y $sp(3)$, por tanto es $sp(6)$, $sp(12)$, $sp(18), \ldots, sp(6k)$, y claramente también es $sp(2^{k_1})$ y $sp(3^{k_2})$, para cualquier $k, k_1, k_2 \in \mathbb{Z}^+$.

Existen resultados que permiten producir seudoprimos, y además sirven para demostrar la infinitud de estos. A continuación se presentan algunos de ellos.

Teorema 2.3. *Si n es un $sp(2)$, entonces $m = 2^n - 1$ es $sp(2)$.*

Demostración. Sea $n = ab$, con $a > 1$ y $b > 1$, entonces,

$$m = 2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 1),$$

lo que muestra que m es compuesto. Ahora se prueba que $m \mid 2^{m-1} - 1$ con lo cual se habrá demostrado que m es $sp(2)$.

Como n es $sp(2)$ se tiene que $n \mid 2^{n-1} - 1$. Dado que $m - 1 = 2^n - 2$ entonces, $\frac{m-1}{2} = 2^{n-1} - 1$. Así $n \mid \frac{m-1}{2}$ luego $n \mid m - 1$ es decir, $m - 1 = nk$ para algún $k \in \mathbb{Z}$. De este modo,

$$2^{m-1} - 1 = 2^{nk} - 1 = (2^n - 1)(2^{n(k-1)} + 2^{n(k-2)} + \cdots + 1).$$

Por lo que $2^n - 1 \mid 2^{m-1} - 1$ es decir, $m \mid 2^{m-1} - 1$.

□

Corolario 2.2. *Existen infinitos seudoprimos.*

Demostración. Por el resultado anterior, se pueden construir un número infinito de seudoprimos $n_{i+1} = 2^{n_i} - 1$ para $i = 1, 2, 3, \ldots$ a partir de un seudoprimo. □

Es bien conocido, como se dijo anteriormente, que 341 es el menor seudoprimo. Con el procedimiento planteado en la demostración podemos formar un nuevo seudoprimo $n_1 = 2^{341} - 1$, y a partir de este uno nuevo, obteniendo los seudoprimos $341 < n_1 < n_2 < \cdots$. Sin embargo, este procedimiento no permite generarlos a todos. Por ejemplo, $n = 561$ y $n = 1105$, son seudoprimos y ninguno de los dos cae en la construcción anterior.

El siguiente resultado es una generalización del Teorema 2.3, puesto que permite construir seudoprimos para cualquier base a.

Teorema 2.4 (M. Cipolla, 1904)**.** *Sean $a \geq 2$ entero y p un primo impar no divisor de $a(a^2 - 1)$. Si*

$$n_1 = \frac{a^p - 1}{a - 1}, \quad n_2 = \frac{a^p + 1}{a + 1}$$

y $n = n_1 n_2$. *Entonces* n *es* $sp(a)$.

Demostración. Es claro que n es impar, $n_1 \equiv 1 \pmod 2$ y que $n_2 \equiv 1 \pmod 2$.
Ahora, $(a-1)n_1 = a^p - 1$. Por el Corolario 2.1 y el quinto ítem del Teorema 1.6, se sigue que

$$a^p - 1 \equiv a - 1 \pmod p \text{ y } a^p + 1 \equiv a + 1 \pmod p,$$

es decir, $(a-1)n_1 \equiv a - 1 \pmod p$ y del mismo modo $(a+1)n_2 \equiv a + 1 \pmod p$.
Como $(p, a \pm 1) = 1$, entonces por el Teorema 1.7

$$n_1 \equiv 1 \pmod p \quad \text{y} \quad n_2 \equiv 1 \pmod p,$$

así, por el Teorema 1.8, $n_1 \equiv 1 \pmod{2p}$, y $n_2 \equiv 1 \pmod{2p}$, lo que implica

$$n \equiv 1 \pmod{2p}. \tag{2.2.1}$$

Por otro lado, como $a^{2p} - 1 = (a^p + 1)(a^p - 1) = n(a-1)(a+1)$, se sigue que $a^{2p} - 1$ es divisible por n, esto es

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

De la congruencia (2.2.1) se tiene que $n - 1 = 2pk$ para algún $k \in \mathbb{Z}$, así

$$a^{n-1} = (a^{2p})^k \equiv 1^k \equiv 1 \pmod n.$$

□

Observación 2.1. En la demostración anterior los enteros n_1 y n_2 pueden verse como evaluaciones del p-ésimo polinomio ciclótomico $\Phi_p(X)$, ya que por el Teorema 1.18, $n_1 = \Phi_p(a) = 1 + a + a^2 \cdots + a^{p-1}$ y $n_2 = \Phi_p(-a) = 1 - a + a^2 - a^3 + \cdots + a^{p-1}$.

Corolario 2.3. *Si* $a \geq 2$ *es un entero, existen infinitos seudoprimos base* a.

Demostración. Sea $a \geq 2$ un entero. Dado que existen infinitos números primos p no divisores de $a(a^2 - 1)$, puesto que el conjunto de primos es infinito. Así, por el método usado en la demostración anterior, se puede construir un número infinito de enteros $n_1 = \frac{a^p - 1}{a-1}$ y $n_2 = \frac{a^p + 1}{a+1}$, tales que su producto $n = n_1 n_2$ es seudoprimo para la base a. □

2.3. Número de bases para las que un entero es probable primo

Se estudia en esta unidad, el problema de determinar para cuántas bases un entero n es probable primo. Esto es, contar el número de enteros a en $\mathbb{U}_n$ tales que $a^{n-1} \equiv 1 \pmod{n}$. Del tercer ítem de la Proposición 2.1, se sabe que este número es a lo más $\frac{\phi(n)}{2}$. El resultado que cuenta el número exacto de enteros a primos relativos con n, para los que n es probable primo se presenta a continuación.

Teorema 2.5. *Sea $n = \prod_{i=1}^{d} p_i^{k_i}$ la descomposición de n en factores primos. Entonces el número de enteros a con $1 \leq a \leq n$ y $(a, n) = 1$, tales que n es probable primo base a es*

$$B_{pp}(n) = \prod_{i=1}^{d} (p_i - 1, n - 1).$$

Demostración. Sea $n = \prod_{i=1}^{d} p_i^{k_i}$ la factorización prima de n. Por el Teorema Chino del residuo, ver Teorema 1.10, se pueden construir tales a a partir de soluciones a_i de $a_i^{n-1} \equiv 1 \pmod{p_i^{k_i}}$. Por el Teorema 1.13, cada grupo $\mathbb{U}_{p_i^{k_i}}$ de orden $\phi(p_i^{k_i})$ es cíclico, así por el Teorema 1.15, el número de soluciones para esta última congruencia es, $(\phi(p_i^{k_i}), n - 1)$. De este modo el número de bases para las cuales n es probable primo es

$$\prod_{i=1}^{d} (\phi(p_i^{k_i}), n - 1).$$

Pero por el Lema 1.5, $(\phi(p_i^{k_i}), n - 1) = (p_i^{k_i - 1}(p_i - 1), n - 1)$, y dado que p_i es un divisor primo de n, entonces $(p_i^{k_i - 1}, n - 1) = 1$. Por lo tanto

$$B_{pp}(n) = \prod_{i=1}^{d} (\phi(p_i^{k_i}), n - 1) = \prod_{i=1}^{d} (p_i - 1, n - 1).$$

□

Ejemplo 2.7. La siguiente tabla muestra el número de bases a para las cuales el entero n es probable primo, estos valores fueron calculados con el Algoritmo A.1.

Por ejemplo, para calcular el número de bases para las cuales $n = 1729$ es un probable primo usando el Algoritmo A.1 en `SAGE` se hace lo siguiente.

```
Bpp(1729)
  1296
```

n	B_{pp}	n	B_{pp}
341	100	3501	8
561	320	8911	7128
1051	1050	10501	10500
1729	1296	29431	324

Tabla 2.3: Número de bases de probable primalidad para algunos enteros dados.

Observe que en la tabla anterior, los enteros compuestos 561, 1729 y 8911 poseen $\phi(n)$ bases de probable primalidad. Es decir, para estos enteros n, $a^{n-1} \equiv 1 \pmod{n}$ para toda base a primo relativo con n. Estos números como se menciona en [4] (página 93), fueron caracterizados primero por A. R. Korselt en 1899, pero al parecer, Korselt no fue capaz de encontrar ningún número con esas características, y hubo que esperar a que en el año 1912 Robert Daniel Carmichael encontrara el menor de ellos, 561. En honor a él reciben el nombre de *números de Carmchael*.

Los números de Carmichael desafortunadamente son los culpables de que el criterio de Fermat falle como un criterio de no primalidad, puesto que ellos no tienen testigos de composición. Pero afortunadamente para la teoría de números son otro campo de investigación. En lo que sigue, en este trabajo se estudiarán algunos resultados que los caracterizan, puesto que son el tema central de estudio en esta monografía.

2.4. Números de Carmichael

En esta sección se presentan la definición de número de Carmichael en su calidad de *seudoprimo absoluto* y algunas propiedades que los identifican y con n_d se denota a un número de Carmichael producto de d primos.

Definición 2.4. Sea n un entero impar compuesto, si $a^{n-1} \equiv 1 \pmod{n}$ para todo entero a primo relativo con n. Se dice que n es un número de Carmichael.

Ejemplo 2.8. El ejemplo más pequeño de un número de Carmichael es $561 = 3 \times 11 \times 17$. Puesto que

$$B_{pp}(561) = \prod_{p=1}^{3}(p_i - 1, n - 1) = 2 \times 10 \times 16 = \phi(561).$$

Ejemplo 2.9. En la siguiente tabla se muestran los primeros siete números de Carmichael, estos se verifican en la lista de números de Carmichael hasta 10^4 generada por el Algoritmo A.2.

Que la lista anterior esté formada por números de Carmichael resulta el siguiente teorema planteado por A. Korselt. Este establece condiciones necesarias y suficientes para que un entero n sea un número de Carmichael.

561	$3 \times 11 \times 17$
1105	$5 \times 13 \times 17$
1729	$7 \times 13 \times 19$
2465	$5 \times 17 \times 29$
2821	$7 \times 13 \times 31$
6601	$7 \times 23 \times 41$
8911	$7 \times 19 \times 67$

Tabla 2.4: Menores números de Carmichael, ver A002997.

Teorema 2.6 (Criterio de Korselt, A. Korselt, 1899)**.** *Sea n un entero impar y compuesto.*

1. *Si n es un número de Carmichael, entonces n es libre de cuadrados, y*
2. *Si $n = p_1 p_2 \cdots p_d$, con los p_i primos distintos, entonces n es un número de Carmichael si y solo si $p_i - 1 \mid n - 1$, para $i = 1, 2, \ldots, d$.*

Demostración. Sabemos que n es un número de Carmichael si y solo si

$$B_{pp}(n) = \prod_{p|n} (p - 1, n - 1) = \phi(n). \tag{2.4.1}$$

De este modo si n no es libre de cuadrados y p es un primo tal que $p^2 \mid n$, entonces $p \mid \phi(n)$. Pero tal p no es divisor de $\prod_{p|n}(p - 1, n - 1)$, así n debe ser libre de cuadrados, pues de lo contrario se contradice la ecuación (2.4.1).

Para la segunda parte supongamos que n es libre de cuadrados, $n = p_1 p_2 \cdots p_d$ con los p_i primos distintos. Para que n sea un número de Carmichael debe satisfacer la ecuación (2.4.1), esto es

$$(p_1 - 1, n - 1)(p_2 - 1, n - 1) \cdots (p_d - 1, n - 1) = \phi(p_1)\phi(p_2) \cdots \phi(p_d),$$

es decir,

$$(p_1 - 1, n - 1)(p_2 - 1, n - 1) \cdots (p_d - 1, n - 1) = (p_1 - 1)(p_2 - 1) \cdots (p_d - 1). \tag{2.4.2}$$

La ecuación (2.4.2) es cierta si y solo si $(p_i - 1, n - 1) = (p_i - 1)$ es decir, $p_i - 1 \mid n - 1$ para $1 \leq i \leq d$. □

Corolario 2.4. *Sea n un entero impar y compuesto, n es un número de Carmichael si y solo si n es libre de cuadrados y $\frac{n}{p} \equiv 1 \pmod{p-1}$ para todo $p \mid n$.*

Demostración. Por el Criterio de Korselt, n es un número de Carmichael si y solo si es libre de cuadrados y $n \equiv 1 \pmod{p-1}$ para todo primo p divisor de n. Resta probar que $\frac{n}{p} \equiv 1 \pmod{p-1}$ para todo p que divide a n.

Como $n \equiv \frac{n}{p} \pmod{p-1}$ se tiene que

$$\begin{aligned} p-1 \mid & \frac{n}{p}(p-1) \\ p-1 \mid & n - \frac{n}{p} + 1 - 1 \\ p-1 \mid & (n-1) - (\frac{n}{p} - 1). \end{aligned}$$

Esto es, si y solo si $\frac{n}{p} \equiv 1 \pmod{p-1}$. □

La pregunta a seguir es ¿el conjunto de números de Carmichael es infinito? La respuesta es afirmativa, fueron W. R. Alford, A. Granville y C. Pomerance quienes en 1992 probaron por primera vez la existencia de infinitos números de Carmichael. El resultado se presenta a continuación y aunque la prueba no esté al alcance de este trabajo, puede encontrarse en [1].

Teorema 2.7 (W. Alford, A. Granville, C. Pomerance, 1992)**.** *Existen infinitos números de Carmichael. En particular, para x suficientemente grande, el numero $C(x)$ de números de Carmichael que no exceden a x satisface $C(x) > x^{2/7}$.*

Capítulo 3

Números de Carmichael producto de tres primos

Una vez presentada la definición de número de Carmichael y el Criterio de Korselt en el Teorema 2.6, como criterio fundamental que establece condiciones necesarias y suficientes para que un entero positivo impar sea un número de Carmichael. En este capítulo se presenta inicialmente una característica importante de estos números. Esta es la que afirma que todo número de Carmichael tiene en su descomposición prima como mínimo tres factores primos impares. Con base en esto, el objetivo principal de este capítulo, es mostrar unos resultados que permiten encontrar o construir números de Carmichael con $d \geq 3$ factores primos, los que pueden encontrarse fundamentalmente en [3] y [6]. Además, se muestran tablas que exhiben ejemplos de este tipo de números, la cuales se pueden crear por medio de los algoritmos que se encuentran en el Apéndice 4.1 y algunas de ellas se pueden verificar en el sitio web *The On-Line Encyclopedia of Integer Sequences*, ver [14].

3.1. Números de Carmichael producto de tres primos

En el Ejemplo 2.9, se mostraron los menores números de Carmichael, todos ellos tienen una particularidad; son producto de tres números primos. Esta no es ninguna casualidad, en realidad es una característica propia de ellos, puesto que no existen números de Carmichael con dos factores primos. Para demostrar este hecho, primero se prueba el siguiente lema.

Lema 3.1. *Sea $n = uv$, entonces $v - 1$ divide a $n - 1$ si y solo si $v - 1$ divide a $u - 1$.*

Demostración. Considere $n - u = vu - u$, sumando y restando 1 al lado izquierdo de esta igualdad y factorizando en ambos lados se tiene

$$n - u + 1 - 1 = (n - 1) - (u - 1) = u(v - 1),$$

por tanto, $v-1 \mid n-1$ si y solo si $v-1 \mid u-1$. □

Proposición 3.1. *Un número de Carmichael tiene al menos tres factores primos.*

Demostración. Sea $n = pq$ con p y q primos y $p > q$. Entonces $p-1 > q-1$, como $p-1 \nmid q-1$, por el lema anterior, $p-1 \nmid n-1$. Es decir, n no cumple las condiciones del Teorema 2.6. Por tanto, n no es un número de Carmichael. □

Ejemplo 3.1. Por medio del Algoritmo A.2, se pueden calcular algunos de los elementos de la siguiente tabla. Esta hace parte de la secuencia A006931, la cual está compuesta por los menores números de Camichael con d factores primos, para $d = 1, 2 \ldots, 10$.

d	n_d	Factores de n_d
3	561	$3 \times 11 \times 17$
4	41041	$7 \times 11 \times 13 \times 41$
5	825265	$5 \times 7 \times 17 \times 19 \times 73$
6	321197185	$5 \times 19 \times 23 \times 29 \times 37 \times 137$
7	5394826801	$7 \times 13 \times 17 \times 23 \times 31 \times 67 \times 73$
8	232250619601	$7 \times 11 \times 13 \times 17 \times 31 \times 37 \times 73 \times 163$
9	9746347772161	$7 \times 11 \times 13 \times 17 \times 19 \times 31 \times 37 \times 41 \times 641$
10	1436697831295441	$11 \times 13 \times 19 \times 29 \times 31 \times 37 \times 41 \times 43 \times 71 \times 127$

Tabla 3.1: Menores números de Carmichael, con d factores primos.

En el Capítulo 2, los teoremas 2.3 y 2.4, se mostraron como una herramienta para generar seudoprimos y seudoprimos base a. Del mismo modo, existen algunos resultados que permiten construir números de Carmichael, más no garantizan la infinitud de estos. Por ejemplo, en 1939 Jack Chernick en un artículo titulado "On Fermat's simple theorem" [3], presenta un método que sirve para encontrar números de Carmichael producto de tres números primos, y su generalización, que permite construir números de Carmichael con d factores primos. Los resultados se presentan a continuación.

Teorema 3.1 (Chernick, 1939)**.** *Sea $n_3 = p_1p_2p_3$ un número de Carmichael. Entonces n_3 puede escribirse de la forma $(2r_1h+1)(2r_2h+1)(2r_3h+1)$ donde los $r's$ son primos relativos dos a dos y h es un divisor del máximo común divisor de los $p_i - 1$.*

Demostración. Sea $n_3 = p_1p_2p_3$ un número de Carmichael. Además, considere a $p_i = r_ik + 1$; $1 \leq i \leq 3$, donde $k = (p_1 - 1, p_2 - 1, p_3 - 1)$. Por el Criterio de Korselt, ver Teorema 2.6, se sabe que

$$(r_1k+1)(r_2k+1)(r_3k+1) \equiv 1 \pmod{kr_i}.$$

Al efectuar los productos de la parte izquierda de esta congruencia y por el Teorema 1.7 se obtiene

$$k(r_1r_2 + r_1r_3 + r_2r_3) + r_1 + r_2 + r_3 \equiv 0 \pmod{r_i}. \tag{3.1.1}$$

Se puede ver que para la congruencia (3.1.1) los $r's$ son primos relativos dos a dos, pues si dos de ellos tienen algún factor en común, también lo hace el tercero, lo que iría en contradicción con la definición de k. Como k debe ser par, entonces $p_i = 2r_ih + 1$, así

$$n_3 = (2r_1h + 1)(2r_2h + 1)(2r_3h + 1).$$

□

Ejemplo 3.2. En la siguiente tabla se muestran los menores números de Carmichael escritos en la forma del teorema anterior.

n_3	$(2r_1h + 1)(2r_2h + 1)(2r_3h + 1)$
$561 = 3 \times 11 \times 17$	$(2 \times 1 \times 1 + 1)(2 \times 5 \times 1 + 1)(2 \times 8 \times 1 + 1)$
$1105 = 5 \times 13 \times 17$	$(2 \times 1 \times 2 + 1)(2 \times 3 \times 2 + 1)(2 \times 4 \times 2 + 1)$
$1729 = 7 \times 13 \times 19$	$(2 \times 1 \times 3 + 1)(2 \times 2 \times 3 + 1)(2 \times 3 \times 3 + 1)$
$2465 = 5 \times 17 \times 29$	$(2 \times 1 \times 2 + 1)(2 \times 4 \times 2 + 1)(2 \times 7 \times 2 + 1)$
$2821 = 7 \times 13 \times 31$	$(2 \times 1 \times 3 + 1)(2 \times 2 \times 3 + 1)(2 \times 5 \times 3 + 1)$

Tabla 3.2: Primeros números de Carmichael, escritos de la forma $(2r_1h + 1)(2r_2h + 1)(2r_3h + 1)$.

Observe que la congruencia (3.1.1) puede escribirse como

$$k(r_1r_2 + r_1r_3 + r_2r_3) \equiv -(r_1 + r_2 + r_3) \pmod{r_1r_2r_3},$$

la cual a su vez es una congruencia lineal en k. Luego por el Teorema 1.9, la congruencia (3.1.1) tiene solución única, dado que el coeficiente de k es primo relativo al módulo. Ahora dado que la solución de esta congruencia es

$$k \equiv -(r_1 + r_2 + r_3)(r_1r_2 + r_1r_3 + r_2r_3)^{-1} \pmod{r_1r_2r_3},$$

por el Teorema 2.2,

$$(r_1r_2 + r_1r_3 + r_2r_3)^{-1} \equiv (r_1r_2 + r_1r_3 + r_2r_3)^{\phi(r_1r_2r_3)-1} \pmod{r_1r_2r_3},$$

de este modo

$$k \equiv -(r_1 + r_2 + r_3)(r_1r_2 + r_1r_3 + r_2r_3)^{\phi(r_1r_2r_3)-1} \pmod{r_1r_2r_3},$$

así, $k = mr_1r_2r_3 - (r_1 + r_2 + r_3)(r_1r_2 + r_1r_3 + r_2r_3)^{\phi(r_1r_2r_3)-1}$, para algún entero m.

En particular, si $r_1 = 1$, $r_2 = 2$ y $r_3 = 3$, entonces $k = 6m$. A partir de esto, J. Chernick [3], establece el siguiente teorema que se conoce como *formas universales*, y facilita encontrar números de Carmichael con tres divisores primos.

Teorema 3.2 (Formas universales)**.** *Sea $m \geq 1$ un entero tal que $6m + 1$, $12m + 1$ y $18m + 1$ son primos, entonces*

$$n_3(m) = (6m + 1)(12m + 1)(18m + 1),$$

es un número de Carmichael.

Ejemplo 3.3. La siguiente tabla muestra los menores números de Carmichael que se obtienen de esta forma.

m	$n_3(m)$	m	$n_3(m)$	m	$n_3(m)$
1	$7 \times 13 \times 19$	45	$271 \times 541 \times 811$	56	$337 \times 673 \times 1009$
6	$37 \times 73 \times 109$	51	$307 \times 613 \times 919$	100	$601 \times 1201 \times 1801$
35	$211 \times 421 \times 631$	55	$331 \times 661 \times 991$	121	$727 \times 1453 \times 2179$

Tabla 3.3: Menores números de Carmichael de la forma $(6m + 1)(12m + 1)(18m + 1)$.

Observación 3.1. Notoriamente la forma del Teorema 3.2, es solo un caso particular del Teorema 3.1, puesto que la solución de la congruencia (3.1.1), tomando a $r_1 = 1$, $r_2 = 2$ y $r_3 = 3$ es $k = 6m$. Similarmente, si se toman valores diferentes en los $r's$, se obtiene otras soluciones para la congruencia (3.1.1), y así mismo nuevas formas universales, $n_3(m)$. En la siguiente tabla se indican algunos ejemplos de formas universales que se obtienen para algunos valores de los $r's$ dados.

r_1, r_2, r_3	$n_3(m)$
$1, 2, 5$	$(10m + 7)(20m + 13)(50m + 31)$
$1, 3, 8$	$(24m + 13)(72m + 37)(192m + 97)$
$2, 3, 5$	$(60m + 41)(90m + 61)(150m + 101)$

Tabla 3.4: Distintas formas universales $n_3(m)$.

Hoy en día, no se sabe la existencia de infinitos números de Carmichael producto de tres primos. El teorema anterior no sirve para dar una respuesta afirmativa a esta pregunta, pues no se tiene seguridad acerca de la existencia de infinitos m tales que $n_3(m)$ sea un número de Carmichael.

La existencia de infinitos enteros m, tal que $6m+1$, $12m+1$ y $18m+1$ son simultáneamente primos, se conoce como *the prime k-tuples conjecture*. Particularmente, en 2002 Harvey Dubner calculó, por medio de un método probabilistico, el número $C_3(x)$ de números de Carmichael producto de tres primos y el número $N(x)$ de tales números de la forma $n_3(m) = (6m+1)(12m+1)(18m+1)$ hasta 10^n, para cada $n \leq 42$. A partir de esto, Dubner estimó que a esta forma pertenecen el 2.2 % de números de Carmichael con tres divisores primos, y además que es la que contiene mayor número de números de Carmichael más que cualquier otra familia de la forma $n_3(m)$, ver [5].

3.2. Números de Carmichael producto de d primos

En esta sección se presenta, una extensión de los resultados anteriores, estos permiten construir números de Carmichael hasta con $d \geq 3$ divisores primos.

Teorema 3.3. *Sea $n_d = p_1 p_2 \cdots p_d$, donde los p_i son primos. Si se toma a k_1 como el máximo común divisor de $p_i - 1$, $r_i = \frac{p_i - 1}{k_1}$ y R el mínimo común múltiplo de r_i; donde $1 \leq i \leq d$, entonces*

$$n_d(m) = \prod_{i=1}^{d} (r_i R m + p_i), \tag{3.2.1}$$

es una forma universal, con la condición de que si los $r's$ son todos impares, m se remplaza por $2m$.

Demostración. Por el Teorema 2.6 se sabe que

$$n_d - 1 \equiv 0 \pmod{p_i - 1}. \tag{3.2.2}$$

Escribiendo a cada $p_i = r_i k_1 + 1$, la congruencia (3.2.2) se transcribe como

$$\prod_{i=1}^{d} (r_i k_1 + 1) - 1 \equiv 0 \pmod{r_i k_1},$$

es decir,

$$\left[\prod_{i=1}^{d} (r_i k_1 + 1) - 1 \right] / k_1 \equiv 0 \pmod{r_i}.$$

De ahí por el Corolario 1.1, se obtiene que

$$\left[\prod_{i=1}^{d} (r_i k_1 + 1) - 1 \right] / k_1 \equiv 0 \pmod{R}. \tag{3.2.3}$$

Luego k es una solución de la congruencia

$$\left[\prod_{i=1}^{d}(r_i k+1)-1\right]/k \equiv 0 \pmod{R}. \tag{3.2.4}$$

si $k \equiv k_1 \pmod{R}$. De esta manera $k = Rm + k_1$, para algún $m \in \mathbb{Z}$. Remplazando k_1 por k en la congruencia (3.2.4) y regresando el proceso anterior, se obtiene la forma del teorema.

La forma (3.2.1) satisface las condiciones de una forma universal; esto es, cada uno de sus factores es impar y son diferentes entre sí. En efecto, si algún r_i es par, entonces Rm es par, y si ningún r_i es par, se remplaza a m por $2m$. Así cualquier factor $(r_i Rm + p_i)$ es impar, además cualesquiera dos factores $(r_i Rm+p_i)$, $(r_j Rm+p_j)$ son distintos, puesto que si $p_i > p_j$, por definición $r_i > r_j$. □

El Teorema anterior indica un método para generar diversas formas universales que permiten encontrar números de Carmichel con d divisores primos, a partir de algún número de Carmichael n_d dado. En el Algoritmo A.5, se implementa este teorema, esto es, el algoritmo recibe la lista de factores primos de un número de Carmichael dado, y para m dado verifica si la forma universal (3.2.1) produce un nuevo número de Carmichael con d factores primos. Por ejemplo, cuando se ingresa la factorización prima de 561 y $m = 1$ se obtiene

```
universalm(prime_divisors(561),1)
```

```
[[43, 211, 337], 0]
```

Esto significa que $3057601 = 43 \times 211 \times 337$ es un número de Carmichael con tres factores primos. Otros ejemplos, que se pueden obtener usando este algoritmo se presentan en la siguiente tabla.

d	n_d	m	Nuevo número de Carmichael n_d
3	$41 \times 61 \times 101$	1	$101 \times 151 \times 251$
3	$7 \times 73 \times 103$	10	$211 \times 2521 \times 3571$
3	$41 \times 61 \times 101$	7	$461 \times 691 \times 1151$
4	$7 \times 11 \times 13 \times 101$	8	$3607 \times 6011 \times 7213 \times 60101$
4	$13 \times 17 \times 23 \times 67$	1	$1597 \times 2129 \times 2927 \times 8779$
5	$11 \times 13 \times 17 \times 31 \times 241$	50	$30011 \times 36013 \times 48017 \times 90031 \times 720241$

Tabla 3.5: Nuevos números de Carmichael n_d generados a partir de algunos n_d dados.

Al final del enunciado del Teorema 3.3, se afirma que cuando los $r's$ sean impares, se cambia m por $2m$; el primer ejemplo donde sucede esto es cuando el número de Carmichael ingresado es

$8911 = 7 \times 19 \times 67$ y $m = 4$, obteniendo el número de Carmichael $652969351 = 271 \times 811 \times 2971$, puesto que cuando se ingresa 8911 en el Algoritmo A.5 se obtiene

```
universalm(prime_divisors(8911),4)
```

```
[[271, 811, 2971], 1]
```

Ejemplos adicionales en los que también sucede esto, se presentan en la tabla a continuación.

d	n_d	m	Nuevo n_d
3	$7 \times 19 \times 67$	5	$337 \times 1009 \times 3697$
3	$13 \times 37 \times 61$	1	$43 \times 127 \times 211$
3	$13 \times 37 \times 61$	5	$163 \times 487 \times 811$
4	$13 \times 37 \times 61 \times 181$	1	$43 \times 127 \times 21 \times 631$
4	$7 \times 19 \times 67 \times 991$	1	$337 \times 1009 \times 3697 \times 55441$

Tabla 3.6: Números de Carmichael que se generan cuando m se remplaza por $2m$.

El siguiente resultado permite construir números de Carmichael n_d, partiendo de algún n_{d-1} dado.

Teorema 3.4. *Sea $n_{d-1} = p_1 p_2 \cdots p_{d-1}$, donde los p_i son primos diferentes, q el mínimo común múltiplo de $p_i - 1$; donde $1 \leq i \leq d-1$, y $r = \frac{n_{d-1}-1}{q}$. Si $p_d = qt + 1$, donde t es algún divisor de r y p_d es un primo distinto de p_i, entonces $n_d = p_1 p_2 \cdots p_d$ es un número de Carmichael producto de d factores primos.*

Demostración. Por el Teorema 2.6 se debe probar que $n_d \equiv 1 \pmod{p_i - 1}$; $1 \leq i \leq d$.
Dado que $p_d r q \equiv 0 \pmod{q}$ y $p_d - 1 \equiv 0 \pmod{q}$, se sigue que

$$n_d = n_{d-1} p_d \equiv p_d \equiv 1 \pmod{q}. \tag{3.2.5}$$

Por otro lado, como t es un divisor de r y $n_{d-1} - 1 = rq \equiv 0 \pmod{p_d - 1}$, se tiene

$$n_d = n_{d-1} p_d \equiv n_{d-1} \equiv 1 \pmod{p_d - 1}. \tag{3.2.6}$$

Así, de las congruencias (3.2.5) y (3.2.6), se concluye que $n_d \equiv 1 \pmod{p_i - 1}$, para cada $1 \leq i \leq d$. □

Ejemplo 3.4. Sea $n_3 = 7 \times 13 \times 19$ un número de Carmichael. Entonces $q = \text{mcm}(6, 12, 18) = 36$ y $r = 48$. El teorema anterior afirma que se pueden encontrar los primos $p_4 = 37, 73, 109, 443$ y 577 para formar números de Carmichael con cuatro factores primos a partir de n_3. En el Algoritmo A.6 se implementa este teorema, esto es, el algoritmo recibe el número de Carmichael n_{d-1} y retorna la lista de primos p_d para los cuales $n_d = n_{d-1} p_d$ es un número de Carmichael. Por ejemplo, al ingresar 670033 se produce

```
semilla(670033)
```

```
[397, 2377, 7129, 55837, 74449]
```

En la siguiente tabla se repite este proceso para algunos n_3 dados y se encuentra la siguiente sucesión.

Observación 3.2. Si se supone que $n_3(m) = (6m+1)(12m+1)(9 \times 2m + 1)$ es un número de Carmichael, para algún entero m. Entonces por el teorema anterior, $q = 9 \times 2^2 m$, y tomado $t = 1$, se obtiene

$$n_4(m) = (6m+1)(12m+1)(9 \times 2m + 1)(9 \times 2^2 m + 1).$$

Si se repite el proceso para $n_4(m)$, nuevamente $q = 9 \times 2^2 m$, lo que implica,

$$n_5(m) = (6m+1)(12m+1)(9 \times 2m + 1)(9 \times 2^2 m + 1)(9 \times 2^2 m + 1),$$

n_3	$5 \times 17 \times 29$	$7 \times 13 \times 31$
n_4	$5 \times 17 \times 29 \times 113$	$7 \times 13 \times 31 \times 61$
n_5	$5 \times 17 \times 29 \times 113 \times 337$	$7 \times 13 \times 31 \times 61 \times 181$
n_6	$5 \times 17 \times 29 \times 113 \times 337 \times 673$	$7 \times 13 \times 31 \times 61 \times 181 \times 541$
n_7	$5 \times 17 \times 29 \times 113 \times 337 \times 673 \times 2689$	$7 \times 13 \times 31 \times 61 \times 181 \times 541 \times 2161$

Tabla 3.7: Números de Carmichael construidos a partir de algún n_3 dado.

el cual no es libre de cuadros y por tanto no es un Carmichael. Sin embargo, cuando $m \equiv 0 \pmod 2$, $q = 9 \times 2^3 m_1$ y por tanto,

$$n_5(m_1) = (6m_1 + 1)(12m_1 + 1)(9 \times 2m_1 + 1)(9 \times 2^2 m_1 + 1)(9 \times 2^3 m_1 + 1).$$

Similarmente, si $m \equiv 0 \pmod{2^2}$ se obtiene

$$n_6(m_2) = (6m_2 + 1)(12m_2 + 1)(9 \times 2m_2 + 1)(9 \times 2^2 m_2 + 1)(9 \times 2^3 m_2 + 1)(9 \times 2^4 m_2 + 1).$$

Estas observaciones se generalizan en el siguiente resultado.

Teorema 3.5 (J. Chernick, 1939)**.** *Si $d \geq 4$ y $m \geq 1$ son enteros tales que $6m + 1, 12m + 1$, y $9 \times 2^i m + 1$ son primos para $i = 1, 2, \ldots, d - 2$ y si $2^{d-4} | m$ y se define*

$$n_d(m) = (6m + 1)(12m + 1) \prod_{i=1}^{d-2} (9 \times 2^i m + 1),$$

entonces $n_d(m)$ es un número de Carmichael.

Demostración. Por el Teorema 3.4, $q = 9 \times 2^{d-2} m$, como $2^{d-4} | m$, se garantiza que $(9 \times 2^i m + 1)$ es diferente de $(9 \times 2^j m + 1)$ para $1 \leq i \neq j \leq d - 2$. Por tanto, por el Colorario 1.1 y el Teorema 2.6, $n_d(m)$ es un número de Carmichael. □

Por ejemplo, para $d = 6$ se obtiene $n_6(m) = (6m + 1)(12m + 1)(18m + 1)(36m + 1)(72m + 1)(144m + 1)$. La cual produce algunos números de Carmichael como se indica en la tabla a continuación.

En la descripción de este capítulo, se habló de un resultado relacionado a la infinitud de números de Carmichael con tres divisores primos. El siguiente teorema, podría ayudar a estimar la no existencia de infinitos números de Carmichael producto de tres primos. El resultado muestra, que dado un primo p, existe un número finito de números de Carmichael de la forma pqr, con q, r primos y $p < q < r$. Esta conclusión fue probada en 1950 por N. Beeger [2]. Y su generalización en 1952 por H. Duparc, ver [6] para cualquier entero impar P libre de cuadrados. Para su demostración se

m	$n_6(m)$
380	$2281 \times 4561 \times 6841 \times 13681 \times 27361 \times 54721$
9025	$54151 \times 108301 \times 162451 \times 324901 \times 649801 \times 1299601$
38460	$230761 \times 461521 \times 692281 \times 1384561 \times 2769121 \times 5538241$
40420	$242521 \times 485041 \times 727561 \times 1455121 \times 2910241 \times 5820481$
38460	$230761 \times 461521 \times 692281 \times 1384561 \times 2769121 \times 5538241$
40420	$242521 \times 485041 \times 727561 \times 1455121 \times 2910241 \times 5820481$

Tabla 3.8: Números de Carmichael de la forma dados por el Teorema 3.5, con $d = 6$ y $1 \leq m \leq 10^4$.

hace las siguientes consideraciones.

Sea $n = Pqr$ un número de Carmichael, con $P < q < r$, P no necesariamente primo y q, r primos. Por el Corolario 2.4, se sigue que $Pq \equiv 1 \pmod{r-1}$ y $Pr \equiv 1 \pmod{q-1}$, entonces

$$t_q = \frac{Pr-1}{q-1} \quad y \quad t_r = \frac{Pq-1}{r-1}, \tag{3.2.7}$$

son enteros positivos. Como $P(r-q) > P-1$, $P(q-r) < 1-P$, de donde se sigue que $t_r < P$. Además $P(q-r) < P-1$, lo que lleva a $P < t_q$. Por último, $r(q-P) > r-1$, $r(P-q) < 1-r$, lo que conduce a $t_q < r$, se tiene por tanto que

$$2 \leq t_r < P < t_q < r.$$

De las ecuaciones en (3.2.7) tenemos

$$t_q(q-1) = Pr - 1 = P\left(\tfrac{Pq-1}{t_r} + 1\right) - 1 \quad \text{y} \quad t_r(r-1) = P\left(\tfrac{Pr-1}{t_q} + 1\right) - 1,$$

es decir,

$$t_r t_q(q-1) = P^2 q - P + Pt_r - t_r \quad \text{y} \quad t_r t_q(r-1) = P^2 r - P + Pt_q - t_q.$$

Sumando a las anteriores igualdades P^2, transponiendo términos y factorizando, se obtiene

$$(t_r t_q - P^2)(q-1) = (P + t_r)(P-1),$$
$$(t_r t_q - P^2)(r-1) = (P + t_q)(P-1).$$

Se tiene por tanto el siguiente resultado

Teorema 3.6 (N. Beeger - H. Duparc)**.** *Si $n = Pqr$ es un número de Carmichael con q, r primos y $P < q < r$ y si*

$$t_q = \frac{Pr-1}{q-1} \quad y \quad t_r = \frac{Pq-1}{r-1}, \tag{3.2.8}$$

entonces $2 \leq t_r < P < t_q < r$ *y*

$$(t_r t_q - P^2)(q-1) = (P + t_r)(P-1), \tag{3.2.9}$$

y

$$(t_r t_q - P^2)(r-1) = (P + t_q)(P-1). \tag{3.2.10}$$

En particular dado un entero $P = \prod_{i=1}^{d-2} p_i$ *donde* $p_1 < p_2 < \cdots < p_{d-2}$*, existen finitos números de Carmichael de la forma* $n = Pqr$*, producto de* d *factores primos.*

Demostración. De los comentarios anteriores y la igualdad en (3.2.9) se tiene

$$(t_r t_q - P^2)(q-1) = (P + t_r)(P-1) > 0,$$

lo que implica

$$q - 1 \leq (P + t_r)(P-1) < P^2 + Pt_r - P,$$

de este modo

$$q - 1 < P^2 + P(t_r - 1), \tag{3.2.11}$$

así, $q < P^2 + P(t_r - 1) < 2P^2$, puesto que si se admite la igualdad q no sería primo, por tanto $q < 2P^2$.

Por otro lado, como $r - 1 = \dfrac{Pq-1}{t_r}$, de la desigualdad (3.2.11), se sigue

$$r - 1 = \frac{Pq-1}{t_r} < \frac{P^3 + P^2(t_r - 1)}{t_r},$$

es decir,

$$r < \frac{P^3 + P^2(t_r - 1)}{t_r} < P^3,$$

ya que $2 \leq t_r < P$ y r es primo, así se concluye que $r < P^3$.

En conclusión se probó que dado el entero impar libre de cuadrado P, existen únicamente un número finito de valores para q y r. □

Ejemplo 3.5. La siguiente tabla muestra los primeros números de Carmichael de la forma Pqr dado el entero libre de cuadros P. Estos ejemplos se calcularon con el Algoritmo A.7.

P	Pqr	P	Pqr	P	Pqr
3	$3 \times 11 \times 17$	23	$23 \times 199 \times 353$		$41 \times 241 \times 521$
5	$5 \times 13 \times 17$	29	$29 \times 113 \times 1093$		$41 \times 241 \times 761$
	$5 \times 17 \times 29$		$29 \times 197 \times 953$		$41 \times 881 \times 12041$
	$5 \times 29 \times 73$	31	$31 \times 61 \times 211$		$41 \times 1721 \times 35281$
7	$7 \times 13 \times 19$		$31 \times 61 \times 271$	43	$43 \times 127 \times 211$
	$7 \times 13 \times 31$		$31 \times 61 \times 631$		$43 \times 127 \times 1093$
	$7 \times 19 \times 67$		$31 \times 151 \times 1171$		$43 \times 127 \times 2731$
	$7 \times 23 \times 41$		$31 \times 181 \times 331$		$43 \times 211 \times 337$
	$7 \times 31 \times 73$		$31 \times 991 \times 15361$		$43 \times 211 \times 757$
	$7 \times 73 \times 103$	33	$33 \times 101 \times 197$		$43 \times 271 \times 5827$
13	$13 \times 37 \times 61$	35	$35 \times 443 \times 3877$		$43 \times 433 \times 643$
	$13 \times 37 \times 97$		$35 \times 647 \times 7549$		$43 \times 547 \times 673$
	$13 \times 37 \times 241$	37	$37 \times 73 \times 109$		$43 \times 631 \times 1597$
	$13 \times 61 \times 397$		$37 \times 73 \times 181$		$43 \times 631 \times 13567$
	$13 \times 97 \times 421$		$37 \times 73 \times 541$		$43 \times 3361 \times 3907$
15	$15 \times 47 \times 89$		$37 \times 109 \times 2017$		
17	$17 \times 41 \times 233$		$37 \times 613 \times 1621$		
	$17 \times 353 \times 1201$	41	$41 \times 61 \times 101$		
19	$19 \times 43 \times 409$		$41 \times 73 \times 137$		
	$19 \times 199 \times 271$		$41 \times 101 \times 461$		

Tabla 3.9: Primeros números de Carmichael de la forma Pqr, para un P dado.

Capítulo 4

Números de Carmichael con $(p+1) \mid (n-1)$

Actualmente han surgido algunas variaciones del concepto de número de Carmichael. Por ejemplo, R. McIntosh y M. Dipra, presentan generalizaciones de estos, ver [11, 12]. El objetivo de este último capítulo, es estudiar la definición y dos principales características de una de esta generalizaciones, encontrada en el artículo "Carmichael numbers with $(p+1) \mid (n-1)$", [11].

4.1. Números super-Carmichael

El Criterio de Korselt, ver Teorema 2.6, es la principal herramienta que permite encontrar y generar números de Carmichael. Este, es la semilla de todos los métodos de construcción de números de Carmichael que se presentaron en el Capítulo 3, además también se puede ver como una definición alternativa para el concepto de número de Carmichael. Si se mira como esta última, se podría pensar en una generalización de esta. Es decir, considerar y garantizar la existencia de enteros positivos impares N, libres de cuadrado, tales que $p \pm 1$ divida a $N-1$ para todo primo p divisor de N. Este concepto, ha sido estudiado recientemente por R. McIntosh [11], con la siguiente definición.

Definición 4.1. Un número de Carmichael N es llamado un super-Carmichael, si y solo si $p \pm 1 \mid N-1$ para todo $p \mid N$.

Ejemplo 4.1. El entero más pequeño con estas características encontrado en 1993 por Richard Pinch en [13], y conocido como seudoprimo fuerte de Fibonacci en dicho artículo es

$$17 \times 31 \times 41 \times 43 \times 89 \times 97 \times 167 \times 331.$$

Como se mencionó en el Capítulo 2, existen infinitos números de Carmichael [1]. Es decir, infinitos números N libres de cuadrado tal que $p-1 \mid N-1$ para todo primo $p \mid N$. Además, también se ha probado que existen infinitos números N libres de cuadrado tales que $p+1 \mid N-1$ para todo primo $p \mid N$, ver [16]. Sin embargo, hasta hoy en día, no se conoce si la intersección de estos conjuntos es infinita. Esto es, no se ha garantizado la existencia de infinitos números super-Carmichael.

En el artículo "Carmichael numbers with $(p+1) \mid (n-1)$"[11], se prueba que un número super-Carmichael debe tener al menos cuatro factores primos y que existe un número finito (posiblemente ninguno) de números super-Carmichael, $N = \prod_{i=1}^{d} p_i$, para un conjunto dado de $d-3$ primos $p_1, \ldots, p_{d-3}$. En esta monografía se ilustra de forma detallada la prueba de estos resultados. Para ello se considera las siguientes propiedades.

Sea $N = \prod_{i=1}^{d} p_i$, con los primos $p_1 < p_2 < \cdots < p_d$ un número super-Carmichael. Como $(p_i \pm 1) \mid N-1$, se sigue que p_j no divide a $(p_i \pm 1)$ para todo $1 \leq i, j \leq d$. En efecto, si $p_j \mid (p_i \pm 1)$ para algunos i, j, entonces $p_j \mid N-1$ por lo que N no sería super-Carmichael. Esto obliga a $p_1 \geq 5$.

Observe que para cada primo p divisor de N se satisface lo siguiente

$$N - 1 = (p-1)\left(\frac{N}{p} + 1\right) + \frac{N}{p} - p, \tag{4.1.1}$$

y

$$N - 1 = (p+1)\left(\frac{N}{p} - 1\right) - \frac{N}{p} + p. \tag{4.1.2}$$

Igualando las ecuaciones (4.1.1) y (4.1.2), transponiendo términos, y multiplicando por $\frac{p-1}{p-1}$ y $\frac{p+1}{p+1}$ se tiene

$$2\left(\tfrac{N}{p} - p\right) = (p+1)\left(\tfrac{N}{p} - 1\right) - (p-1)\left(\tfrac{N}{p} + 1\right) = \tfrac{p^2-1}{p-1}\left(\tfrac{N}{p} - 1\right) - \tfrac{p^2-1}{p+1}\left(\tfrac{N}{p} + 1\right).$$

Así

$$\left(\tfrac{N}{p} - p\right) = \tfrac{p^2-1}{2}\left[\tfrac{1}{p-1}\left(\tfrac{N}{p} - 1\right) - \tfrac{1}{p+1}\left(\tfrac{N}{p} + 1\right)\right],$$

lo que muestra que

$$\frac{p^2-1}{2} \mid \frac{N}{p} - p. \tag{4.1.3}$$

Por otro lado, si se escribe a $N = Pqrs$, donde $P = \prod_{i=1}^{d-3} p_i$, $q = p_{d-2}$, $r = p_{d-1}$ y $s = p_d$. A partir de la divisibilidad en (4.1.3) se define los enteros positivos

$$t_q = \frac{2Prs - 2q}{q^2 - 1}, \quad t_r = \frac{2Pqs - 2r}{r^2 - 1}, \quad t_s = \frac{2Pqr - 2s}{s^2 - 1}. \tag{4.1.4}$$

Donde $t_q > t_r > t_s$.

De las expresiones en (4.1.4), se obtiene las ecuaciones

$$t_q(q^2-1)+2q = 2Prs, \tag{4.1.5}$$

$$t_r(r^2-1)+2r = 2Pqs, \tag{4.1.6}$$

$$t_s(s^2-1)+2s = 2Pqr. \tag{4.1.7}$$

Observe que $(t_q t_r t_s, N) = 1$. En efecto, puesto que si $t_q \equiv 0 \pmod{q}$, se sigue que $2Prs \equiv 0 \pmod{q}$, lo que es imposible. Es decir, el $(t_q, q) = 1$, similarmente se puede mostrar que el $(t_r, r) = (t_s, s) = 1$.

De la ecuación (4.1.5),

$$s = \frac{t_q(q^2-1)+2q}{2Pr},$$

sustituyendo en la ecuación (4.1.6) se obtiene

$$r(t_r r^2 + 2r - t_r) = q(t_q q^2 + 2q - t_q).$$

Es decir, el r-polinomio cubico

$$t_r r^3 + 2r^2 - t_r r - q(t_q q^2 + 2q - t_q) = 0. \tag{4.1.8}$$

Remplazando s en la ecuación (4.1.7), resulta el r-polinomio cubico

$$8P^3 q r^3 + 4P^2 t_s r^2 - 4P(t_q q^2 + 2q - t_q)r - t_s(t_q q^2 + 2q - t_q)^2 = 0. \tag{4.1.9}$$

Multiplicando por $8P^3 q$ la ecuación (4.1.8) y por t_r la ecuación (4.1.9), y restando estas dos ecuaciones se consigue el polinomio r-cuadrático

$$\begin{aligned} 4P^2(t_r t_s - 4Pq)r^2 - 4Pt_r(t_q q^2 + 2q - t_q - 2P^2 q)r \\ - t_r t_s(t_q q^2 + 2q - t_q)^2 + 8P^3 q^2(t_q q^2 + 2q - t_q) = 0. \end{aligned} \tag{4.1.10}$$

Como $q \nmid t_r t_s$, el coeficiente principal de este polinomio es diferente de cero.

Teorema 4.1. *No existen números super-Carmichael N con tres factores primos.*

Demostración. Supongamos que $N = Pqrs$, con $P = 1$ y $q < r < s$, con q, r, s primos, es un número super-Carmichael.

Como $s^2-1 > qr$, de la ecuación (4.1.7) se sigue que $t_s(s^2-1) = 2qr-2s < 2qr$, lo que obliga a $t_s = 1$. Así $s^2 = 2qr-2s+1 < 2qr$, y como $r < s$, entonces $2qr < 2qs$, por tanto

$$s^2 < 2qr < 2qs. \tag{4.1.11}$$

De las ecuaciones (4.1.6) y (4.1.11), se sigue que $t_r(r^2-1) = 2qs-2r < 4q^2-2r < 4(q^2-1)$, lo que implica $t_r(r^2-1) < 4(q^2-1)$, por lo que $t_r < 4$. Como $t_s < t_r$, $t_r = 2$ o $t_r = 3$.
Ahora de la desigualdad (4.1.11), se tiene que $q^2s^2 < 2q^3r < 2r^4$, así $qs < \sqrt{2}r^2$, de donde se sigue que $2qs < 2\sqrt{2}r^2 < 3r^2+2r-3$, de este modo $t_r(r^2-1) = 2qs-2r < 3(r^2-1)$ y por tanto $t_r = 2$.

Por otro lado, la desigualdad (4.1.11) conduce a que $s < 2q$, como $r < s$ entonces $rs < 4q^2$, es decir $2rs < 8q^2$. Entonces de la ecuación (4.1.5), $t_q(q^2-1) = 2rs-2q < 8q^2-2q < 8(q^2-1)$, por lo que $t_q(q^2-1) < 8(q^2-1)$, por lo tanto $t_q < 8$.
De la ecuación (4.1.5), sabemos que $t_qq^2 = 2rs-2q+t_q$, entonces $t_qq^3 = q(2rs-2q+t_q) = 2N-(2q-tq)q < 2N$, por tanto

$$t_qq^3 < 2N. \tag{4.1.12}$$

Multiplicando por s la desigualdad (4.1.11), se tiene que

$$s^3 < 2N. \tag{4.1.13}$$

De la definición de t_q en (4.1.4) y sabiendo que $t_r = 2$, se sigue que $2(r^2-1) = 2qs-2r$, así $r^2 = qs-r+1$. Entonces $r^3 = rqs-r^2+r = N-r(r-1) < N$, es decir

$$r^3 < N. \tag{4.1.14}$$

De este modo de las desigualdades (4.1.13) y (4.1.14), se tiene que $N^3 = q^3r^3s^3 < 2q^3N^2$, lo que implica que $2N < 4q^3$, así de la desigualdad (4.1.12) se concluye que $t_qq^3 < 4q^3$ y por tanto $t_q = 3$, puesto que $t_q > t_r = 2$.

Con $t_s = 1$, $t_r = 2$, $t_q = 3$ y $P = 1$, las ecuaciones (4.1.8) y (4.1.10) se convierten respectivamente en

$$2r^3+2r^2-2r-(3q^2+2q-3)q = 0, \tag{4.1.15}$$

y

$$4(2q-1)r^2+12(q^2-1)r-(q^2-2q+3)(3q^2+2q-3) = 0. \tag{4.1.16}$$

De la ecuación (4.1.16),

$$r^2 = \frac{(3q^2+2q-3)(q^2-2q+3)-12(q^2-1)}{4(2q-1)}r, \tag{4.1.17}$$

multiplicando por r la anterior ecuación y remplazando en la ecuación (4.1.15), asociando términos y factorizando se obtiene

$$\frac{(3q^2+2q-3)(q^2-2q+3)-4(2q-1)}{2(2q-1)}r+\frac{2(2q-1)-6(q^2-1)}{2q-1}r^2-q(3q^2+2q-3)=0.$$

Sustituyendo en esta ecuación el equivalente de r^2 en la ecuación (4.1.17), agrupando términos simplificando y factorizando resulta la ecuación

$$(q+1)(6q^2+19q-29)r-3(q^2+2)(3q^2+2q-3)=0.$$

Por tanto,

$$r=\frac{3(q^2+2)(3q^2+2q-3)}{(q+1)(6q^2+19q-29)}.$$

Remplazando esto en la ecuación (4.1.16), agrupando términos y factorizando se obtiene

$$(3q^4-16q^3-78q^2-168q-1)(3q^2+2q-3)^2(2q-1)^2=0,$$

como $(3q^2+2q-3)^2(2q-1)^2>0$, se sigue que

$$(3q^3-16q^2-78q-168)q=1,$$

lo cual es imposible. Esto completa la prueba.

□

Teorema 4.2. *Dado* $P=\prod_{i=1}^{d-3}p_i$ *con los primos* $p_1<p_2<\ldots<p_{d-3}$*, existen finitos números super-carmichael* $N=Pqrs$ *donde* $p_{d-3}<q<r<s$*.*

Demostración. Considerando el producto de los enteros $t_qt_rt_s$ se tiene,

$$t_qt_rt_s=\frac{(2Prs-2q)(2Pqs-2r)(2Pqr-2s)}{(q^2-1)(r^2-1)(s^2-1)}.$$

Multiplicando y dividiendo por $P^3q^2r^2s^2$ el lado derecho de la anterior igualdad, y luego agrupando y factorizando términos se obtiene

$$t_qt_rt_s=8P^3\left(\frac{Prs-q}{Prs}\right)\left(\frac{Pqs-r}{Pqs}\right)\left(\frac{Pqr-s}{Pqr}\right)\left(\frac{q^2}{q^2-1}\right)\left(\frac{r^2}{r^2-1}\right)\left(\frac{s^2}{s^2-1}\right),$$

$$=8P^3\left(1-\frac{q}{Prs}\right)\left(1-\frac{r}{Pqs}\right)\left(1-\frac{s}{Pqr}\right)\left(1+\frac{1}{q^2-1}\right)\left(1+\frac{1}{r^2-1}\right)\left(1+\frac{1}{s^2-1}\right).$$

Claramente, $\left(1+\frac{1}{q^2-1}\right) > \left(1+\frac{1}{r^2-1}\right) > \left(1+\frac{1}{s^2-1}\right)$, de este modo

$$\left(1+\frac{1}{q^2-1}\right)\left(1+\frac{1}{r^2-1}\right)\left(1+\frac{1}{s^2-1}\right) < \left(1+\frac{1}{q^2-1}\right)^3. \tag{4.1.18}$$

Además, como $2P > \left(1-\frac{q}{Prs}\right)$, $2P > \left(1-\frac{r}{Pqs}\right)$ y $2P > \left(1-\frac{s}{Pqr}\right)$, se sigue que

$$\left(1-\frac{q}{Prs}\right)\left(1-\frac{r}{Pqs}\right)\left(1-\frac{s}{Pqr}\right) < 8P^3. \tag{4.1.19}$$

Por tanto, del producto $t_q t_r t_s$ y las desigualdades (4.1.18) y (4.1.19) se concluye que

$$t_q t_r t_s < 8P^3\left(1+\frac{1}{q^2-1}\right)^3.$$

Note que para valores grandes de q, $\left(1+\frac{1}{q^2-1}\right)^3$ se aproxima a 1; esto implica

$$8P^3\left(1+\frac{1}{q^2-1}\right)^3 < 8P^3+1,$$

y por tanto para valores grandes de q

$$t_q t_r t_s < 8P^3+1. \tag{4.1.20}$$

Por otro lado, de la definición de t_s, se tiene que $s^2 < 2Pqr$. Entonces $\left(\frac{s}{r}\right)^2 < \frac{2Pq}{r} < 2P$, lo que implica que $s < r\sqrt{2P}$.

Ahora, como $Pqs < Prs$, entonces $P^2s^2r - Pqs > P^2s^2r - Prs$. Es decir, $Ps(Psr-q) > Psr(Ps-1)$, y de ahí se sigue que

$$\left(1-\frac{q}{Prs}\right) > \left(1-\frac{1}{Ps}\right). \tag{4.1.21}$$

Además, puesto que $Pqr < Pqs$, entonces $P^2q^2s - Pqr > P^2q^2s - Pqs$. Es decir, $Pq(Pqs-r) > Pqs(Pq-1)$, y de esta desigualdad se tiene que

$$\left(1-\frac{r}{Pqs}\right) > \left(1-\frac{1}{Pq}\right). \tag{4.1.22}$$

Por lo tanto, teniendo en cuenta el producto $t_q t_r t_s$ y las desigualdades (4.1.21) y (4.1.22) se concluye que

$$t_q t_r t_s > 8P^3\left(1-\frac{1}{Ps}\right)\left(1-\frac{1}{Pq}\right)\left(1-\frac{s}{Pqr}\right).$$

Dado que $\frac{1}{Ps} < \frac{1}{Pq}$, entonces $\left(1-\frac{1}{Ps}\right) > \left(1-\frac{1}{Pq}\right)$, esto conduce a que

$$\left(1-\frac{1}{Pq}\right)^2 < \left(1-\frac{1}{Ps}\right)\left(1-\frac{1}{Pq}\right). \tag{4.1.23}$$

Como $\frac{s}{r} < \sqrt{2P} = \sqrt{\frac{2}{P}}P$, entonces $sq\sqrt{P} < Pqr\sqrt{2}$. Es decir, $\frac{\sqrt{2}}{\sqrt{Pq}} > \frac{s}{Pqr}$, de este modo

$$\left(1-\frac{\sqrt{2}}{\sqrt{Pq}}\right) < \left(1-\frac{s}{Pqr}\right). \tag{4.1.24}$$

Así, las desigualdades (4.1.23) y (4.1.24) implican que

$$t_q t_r t_s > 8P^3\left(1-\frac{1}{Ps}\right)\left(1-\frac{1}{Pq}\right)\left(1-\frac{s}{Pqr}\right) > 8P^3\left(1-\frac{1}{Pq}\right)^2\left(1-\frac{\sqrt{2}}{\sqrt{Pq}}\right). \tag{4.1.25}$$

Ahora como $P \geq 5$, observe que si $q > 20P^{5/2}$. Entonces $q > 20P^{5/2} = 12P^{5/2} + 8P^{5/2} > 8\sqrt{2}P^{5/2} + 8P^{5/2} > 8\sqrt{2}P^{5/2} + 16P^2$, es decir

$$16P^2 + 8\sqrt{2}P^{5/2} < q.$$

Pasando q a dividir y multiplicando por -1 a la anterior igualdad, se tiene

$$-\frac{16P^2}{q} - \frac{8\sqrt{2}P^{5/2}}{q} > -1,$$

sumando $8P^3$ a esta igualdad, y como $\frac{16P^2}{q} = \frac{16P^3}{Pq}$ y $\frac{8\sqrt{2}P^{5/2}}{q} = \frac{8\sqrt{2}P^3}{\sqrt{Pq}}$, entonces

$$8P^3 - 1 < 8P^3 - \frac{16P^3}{Pq} - \frac{8\sqrt{2}P^3}{\sqrt{Pq}} = 8P^3\left(1-\frac{2}{Pq}-\frac{\sqrt{2}}{\sqrt{Pq}}\right).$$

Pero, $8P^3\left(1-\frac{2}{Pq}-\frac{\sqrt{2}}{\sqrt{Pq}}\right) < 8P^3\left(1-\frac{2}{Pq}-\frac{\sqrt{2}}{\sqrt{Pq}}+\frac{2\sqrt{2}}{P\sqrt{Pq^2}}\right) = 8P^3\left(1-\frac{2}{Pq}\right)\left(1-\frac{\sqrt{2}}{\sqrt{Pq}}\right)$. Así,

$$8P^3 - 1 < 8P^3\left(1-\frac{2}{Pq}\right)\left(1-\frac{\sqrt{2}}{\sqrt{Pq}}\right) < 8P^3\left(1-\frac{1}{Pq}\right)^2\left(1-\frac{\sqrt{2}}{\sqrt{Pq}}\right) \tag{4.1.26}$$

Por lo tanto, de las desigualdades (4.1.25) y (4.1.26) se concluye que

$$t_q t_r t_s > 8P^3 - 1. \tag{4.1.27}$$

Observe que de las desigualdades (4.1.20) y (4.1.27) se tiene que cuando $q > 20P^{5/2}$, entonces $8P^3 - 1 < t_q t_r t_s < 8P^3 + 1$, y como $(P, t_q t_r t_s) = 1$, entonces $8P^3$ es diferente de $t_q t_r t_s$. De esta

manera, $q < 20P^{5/2}$, por lo tanto, dado P existen finitos valores para q. Como $r^2 < s^2 < 2Pqr$, se tiene que $r < 2Pq$ y $s^2 < 2Pqr < 2Pqs$, es decir $s < \sqrt{2Pq} < 2Pq$.
En conclusión se probó que para P dado, existen únicamente un número finito de valores para q, r, y s. □

Observación 4.1. R. McIntosh en [11] organiza una búsqueda que ayuda a encontrar números super-Carmichael, pero antes menciona que recurrió a la lista [9], de todos los seudoprimos de Fermat para la base 2 inferiores a 2^{64}, comprobando cuales de estos eran números super-Carmichael, encontrando los siguientes seis ejemplos.

$$17 \times 31 \times 41 \times 43 \times 89 \times 97 \times 167 \times 331,$$
$$41 \times 53 \times 79 \times 103 \times 239 \times 271 \times 509,$$
$$17 \times 37 \times 41 \times 71 \times 79 \times 97 \times 113 \times 131 \times 191,$$
$$17 \times 61 \times 71 \times 89 \times 197 \times 311 \times 769 \times 272,$$
$$19 \times 41 \times 43 \times 71 \times 89 \times 127 \times 199 \times 449 \times 991,$$
$$29 \times 37 \times 79 \times 181 \times 191 \times 449 \times 701 \times 3457.$$

Además muestra que a pesar de que no se conocen ejemplos de números super-Carmichael con cuatro factores primos, si existiera un super-Carmichael $N = p_1p_2p_3p_4$, con $p_1 < p_2 < p_3 < p_4$, entonces $p_1 > 4000$ y $N > 10^{24}$. Pero estos resultados se escapan del objetivo de este trabajo, por tanto no se presentan formalmente dichas conclusiones.

Conclusiones

- En este trabajo se recopilan y presentan de forma ordenada algunos de los aspectos teóricos alrededor de los números de Carmichael, y los resultados preliminares que son necesarios para estudiarlos.
- Con base en la teoría estudiada se construyeron algunos algoritmos en el sistema de cómputo libre `SAGE`, los cuales permitieron ejemplificar algunas de sus características y propiedades.
- En el Capítulo 3 se pudo ver que los resultados presentados y los algoritmos implementados son herramientas que permiten encontrar o construir números de Carmichael con tres o más factores primos.
- En el Capítulo 4 se presenta y estudia una generalzación reciente del concepto de número de Carmichael. Cabe notar que estos números conocidos como números super-Carmichael, son números de Carmichael que cumplen una condición extra, por lo que son una subfamilia del concepto inicial. Las pruebas de los dos teoremas mostrados consisten en unas cuentas un tanto extensas y tediosas. Esto último lleva a que el cálculo de ejemplos sea un poco difícil; sin embargo se presentan los ejemplos dados en el artículo [11].

Apéndice

Este apéndice tiene el propósito de presentar algoritmos implementados en el sistema de computo libre SAGE. Estos permitieron ejemplificar algunas características referentes a la teoría abordada en este trabajo.

A.1. Algoritmo para calcular el número de bases de probable primalidad

Dado el entero positivo n. Este algoritmo retorna el número de bases para las cuales n es probable primo, resultado que se presentó en el Teorema 2.5.

```
def Bpp(n):
    P=1
    D=prime_divisors(n)
    for i in D:
        d=gcd(n-1,i-1)
        P=P*d
    return(P)
```

A.2. Algoritmo para calcular números de Carmichael hasta 10^n

Dado el entero positivo n. Este algoritmo imprime la lista de números de Carmichael existentes en un rango de 560 hasta 10^n. Esto, partiendo de que 561 es el menor de este tipo de números como se dijo en la Sección 2.4. Este algoritmo fue implementando en SAGE haciendo uso del algoritmo para calcular el número de bases de probable primalidad. Cabe resaltar que aunque esta implementación no es muy eficiente, puesto sirve para valores "pequeños" de n, sirve para dar los primeros ejemplos de números de Carmichael.

```
def nc10n(n):
    k =[]
    for i in range(560, 10^n):
         if not is_even(i) and not is_prime(i):
            if Bpp(i) == euler_phi(i):
                k.append(i)
```

```
    return k
```

A.3. Algoritmo para calcular el máximo común divisor de una lista dada de enteros

Dada la lista A de enteros positivos. Este algoritmo retorna el máximo común divisor de la lista A.

```
def gcd_list(A):
    res = A[0]
    for c in A[1::]:
        res = gcd(res , c)
    return res
```

A.4. Algoritmo para calcular el mínimo común múltiplo de una lista de enteros dada

Dada una la lista A de enteros positivos. Este algoritmo retorna el mínimo común múltiplo de la lista A.

```
def lcm_list(A):
    res=A[0]
    for c in A[1::]:
        res=lcm(res,c)
    return res
```

A.5. Algoritmo para generar números de Carmichael con d factores primos a partir de un n_d dado

Dado un número de Carmichael n_d y un entero positivo m. Este algoritmo aplica el Teorema 3.3 y regresa la lista de los factores primos de un nuevo número de Carmichael con d divisores primos. Este se implementó en `SAGE` haciendo uso de los algoritmos que calculan el máximo común divisor y el mínimo común múltiplo de una lista A.

```
def universalm(P,m):
    s=len(P)
    Ri=[x-1 for x in P]
    k1=gcd_list(Ri)
    L=[Integer((x-1)/k1) for x in P]
    R=lcm_list(L)
    T=[]
    B=0 # esta bandera es para saber cuando k1 es par(0) o impar(1)
```

```
    if R%2==1:
        m=2*m
        B=1
    for i in [0..s-1]:
        p=L[i]*R*m+P[i]
        if is_prime(p)==True:
            T.append(p)
        else:
            return [[],0]
    return [T,B]
```

A.6. Algoritmo para construir números de Carmichael con d factores primos dado un n_{d-1}

Dado el número de Carmichael n_{d-1}. Este algoritmo devuelve la lista de primos p_d para los cuales $n_d = n_{d-1}p_d$ es un número de Carmichael. Resultado que se presentó en el Teorema 3.4. Este algoritmo fue implemento en `SAGE` haciendo uso del algoritmo que calcula el mínimo común múltiplo de una lista A.

```
def semilla(nd1):
    P=prime_divisors(nd1)
    l=len(P)
    Pi=[x-1 for x in P]
    q=lcm_list(Pi)
    r=Integer((nd1-1)/q)
    D=divisors(r)
    S=[]
    for t in D:
        p=q*t+1
        if is_prime(p)==True and p>P[l-1]:
            S.append(p)
    return S
```

A.7. Algoritmo para calcular números de Carmichael de la forma Pqr

Dado el entero positivo P (no necesariamente primo). Este algoritmo retorna la lista finita de números de Carmichael de la forma Pqr, con q, r primos y $P < q < r$.

```
def NumCarTres(P):
    A =[]
    c = P^2
```

```
    L= prime_divisors(P)
    n=len(L)
    for i in range(2,P):
        if (c+1) % i == 0:
                j = (c+1)
        else:
                j = (floor((c+1)/i)*i)+i
        b = (P-1)*(P+i)
        s = (floor(b/(P+1))+c)
        while j <=s:
            a=j-c
            [q1,rs]=b.quo_rem(a)
            if rs==0:
                q=q1+1
                h=P*q-1
                r=h.quo_rem(i)[0]+1
                if q.is_prime()==True and r.is_prime()==True and(P*q*r-1)%(q-1)==0
and (P*q*r-1)%(r-1)==0:
                    v=0
                    for k in L:
                        if  (P*q*r-1)%(k-1)==0:
                            v=v+1
                    if v==n:
                        A.append([q,r])
            j=j+i
    return A
```

Bibliografía

[1] W. R. Alford, A. Granville, and C. Pomerance. There are infinitely many Carmichael numbers. *Ann. of Math. (2)*, 139(3):703–722, 1994.

[2] N. G. W. H. Beeger. On composite numbers n for which $a^{n-1} \equiv (\mathrm{mod}\, n)$ for every a prime to n. *Scripta Math.*, 16:133–135, 1950.

[3] J. Chernick. On Fermat's simple theorem. *Bull. Amer. Math. Soc.*, 45(4):269–274, 1939.

[4] L. Dickson. *History of the theory of numbers*. Chelsea, New York, 1992.

[5] H. Dubner. Carmichael numbers of the form $(6m + 1)(12m + 1)(18m + 1)$. *J. Integer Seq.*, 5(2):Article 02.2.1, 8, 2002.

[6] H. J. A. Duparc. On Carmichael numbers. *Simon Stevin*, 29:21–24, 1952.

[7] W. S. et al. *Sage Mathematics Software (Version V.7.2)*. The Sage Development Team, 2016. `http://www.sagemath.org`.

[8] L. Euler. Theorematum quorundam ad numeros primos spectantium demonstratio. *Commentarii academiae scientiarum Petropolitanae*, 8:141–146, 1741.

[9] J. Feitsma. List of all base 2 fermat pseudoprimes below 2^{64} computed by J. Feitsma and edited by W. Galway, oct 2017.

[10] T. Koshy. *Elementary number theory with applications*. Academic Press, 2007.

[11] R. J. McIntosh. Carmichael numbers with $(p + 1) \mid (n - 1)$. *Integers*, 14:Paper No. A59, 9, 2014.

[12] R. J. McIntosh and M. Dipra. Carmichael numbers with $p + 1 \mid n + 1$. *J. Number Theory*, 147:81–91, 2015.

[13] R. G. E. Pinch. The Carmichael numbers up to 10^{15}. *Math. Comp.*, 61(203):381–391, 1993.

[14] N. J. A. Sloane. The encyclopedia of integer sequences, published electronically at https://oeis.org, Octubre de 2017.

[15] A. Vazzana, M. Erickson, and D. Garth. *Introduction to Number Theory*. Textbooks in Mathematics. Taylor & Francis, 2007.

[16] T. Wright. There are infinitely many elliptic carmichael numbers. *arXiv preprint arXiv:1609.00231*, 2016.