ORDEN p-ÁDICO DE SUCESIONES DE LUCAS

ADRIANA MARIBEL MORA BENAVIDES

UNIVERSIDAD DEL CAUCA

FACULTAD DE CIENCIAS NATURALES, EXACTAS Y DE LA EDUCACIÓN

DEPARTAMENTO DE MATEMÁTICAS

PROGRAMA DE MATEMÁTICAS

POPAYÁN

2024

ORDEN p-ÁDICO DE SUCESIONES DE LUCAS

ADRIANA MARIBEL MORA BENAVIDES

TRABAJO DE INVESTIGACIÓN PRESENTADO COMO REQUISITO PARCIAL
PARA OPTAR AL TÍTULO DE MATEMÁTICA

DIRIGIDO POR:

DR. JHON JAIRO BRAVO GRIJALBA

UNIVERSIDAD DEL CAUCA
FACULTAD DE CIENCIAS NATURALES, EXACTAS Y DE LA EDUCACIÓN
DEPARTAMENTO DE MATEMÁTICAS
PROGRAMA DE MATEMÁTICAS
POPAYÁN

2024

Nota de aceptación

_____

_____

_____

_____

Director _____

Dr. Jhon Jairo Bravo Grijalba

Jurado _____

Dr. Eric Fernando Bravo Montenegro

Jurado _____

Dr. Carlos Andrés Martos Ojeda

Fecha de sustentación: 25 de abril de 2024, Popayán.

Dedicado a Estella, Jarddel y Jemm.

Agradecimientos

En este espacio quiero expresar mi agradecimiento a todas las personas que me han acompañado y apoyado en este proceso.

Al Dr. Jhon Jairo Bravo, director de esta tesis, por tener siempre la disposición de ayudarme a trabajar en lo que quería, por resolver todos los trámites y preguntas que tenía para él, por todas las horas de dedicación, orientación y paciencia. Por los conocimientos transmitidos, por su buena disposición en todo momento. Por poner semillas de amor a la investigación en matemáticas. Además quiero expresar mi respeto y admiración, por todo el trabajo que realiza en su universidad y grupo de investigación.

A mi familia por su confianza y apoyo, especialmente a mi mamá Alba Estella Benavides por darme la oportunidad de estudiar, porque nunca dejo rendirme, por ser mi inspiración en todo momento, por todo su amor.

A mis amigas y amigos que encontré en el camino académico, porque aprendí de ellos, tanto en las aulas, como fuera de ellas, por todo lo que hemos vivido aprendiendo de nuestros profesores como de la vida, gracias por todos los sueños compartidos.

A mis profesores del Departamento de Matemáticas, todos son seres humanos maravillosos y profesionales que admiro, respeto y aprecio. Infinitas gracias por estar siempre para sus estudiantes, no sólo en las aulas.

A la Universidad del Cauca por la formación académica y personal infundida.

Resumen

Sean a y b enteros coprimos no nulos y considere la sucesión de Lucas de primera categoría $(u_n)_{n\geq 0}$ definida por $u_0 = 0$, $u_1 = 1$ y $u_n = au_{n-1} + bu_{n-2}$ para todo $n \geq 2$. Un concepto importante en la teoría de números es el de orden p-ádico, algunas veces llamado valuación p-ádica. Para un primo p y un entero n, el orden p-ádico de n se define como el máximo exponente de p que divide a n. En este trabajo se presentan algunos de los conceptos básicos de la teoría de sucesiones de Lucas y del orden p-ádico, para posteriormente realizar un estudio del orden p-ádico de los términos de sucesiones de Lucas de primera categoría basados en el artículo *"The p-adic valuation of Lucas sequences* [9]" publicado por el Doctor Carlo Sanna en el año 2016. Específicamente, para todo primo p y todo entero positivo n, se presentan fórmulas simples para la valuación p-ádica $v_p(u_n)$ en términos de $v_p(n)$ y el rango de aparición de p en $(u_n)_{n\geq 0}$.

Índice general

Introducción

La sucesión de Fibonacci es una sucesión infinita de números que comienza con 0 y 1, y a partir de ahí, cada elemento es la suma de los dos anteriores. Esta sucesión fue descrita en Europa por Leonardo de Pisa, matemático italiano del siglo XIII también conocido como Fibonacci. Los números de Fibonacci tienen numerosas aplicaciones en ciencias de la computación, matemáticas y teoría de juegos, entre otras (ver [2]).

En el siglo XIX el matemático francés Edouard Anatole Lucas (1842–1891) dio un importante aporte al estudio de las llamadas "sucesiones generalizadas de Fibonacci", las cuales comienzan con dos enteros cualesquiera, y a partir de ahí, cada elemento de la sucesión es una combinación lineal de los dos precedentes. Un conjunto especial de ellas que comienzan con 0 y 1 se conocen como *sucesiones de Lucas*, las cuales representan una familia de sucesiones lineales binarias con bastante interés en la teoría de números. Algunos casos especiales de esta familia de sucesiones habían sido considerados antes por Leonardo de Pisa, Pierre de Fermat y John Pell, entre otros (ver [9]).

Aunque se conocían muchos hechos particulares sobre sucesiones de Lucas, la teoría general fue desarrollada por primera vez por Lucas en un artículo seminal que apareció en el Volumen I del *American Journal of Mathematics* en 1878 (ver [6]). Es un trabajo de rico contenido matemático donde se relacionan las sucesiones de Lucas con muchos temas interesantes, como funciones trigonométricas, fracciones continuas, el número de divisiones en el algoritmo del máximo común divisor como también en pruebas de primalidad.

Contemporáneo a Lucas, el matemático alemán Kurt Wilhelm Sebastián Hensel (1861–1941) (ver [12]) adopta ciertas ideas de algunos matemáticos anteriores, como por ejemplo

de su mentor Ernst Kummer, para describir por primera vez en 1897 la valuación p-ádica u orden p-ádico de un número entero. Para un primo p, la valuación p-ádica de un entero n es el exponente de la potencia más alta de p que divide a n. De manera equivalente, la valuación p-ádica de n es el exponente con el que aparece p en la descomposición en factores primos de n.

El estudio del orden p-ádico fue de gran motivación en la comunidad matemática y sus avances en el tema se volvieron cada vez más importantes en la teoría de números y otros campos durante el siglo XX. La valuación p-ádica es útil para definir un norma p-ádica, que a su vez es la base para definir una distancia en el conjunto de los números p-ádicos, lo que ha permitido usar métodos del análisis para estudiar problemas de teoría de números.

También es interesante en teoría de números estudiar el orden p-ádico de los términos de sucesiones lineales recurrentes. En este sentido, Lengyel en [3] caracterizó completamente el orden p-ádico de los números de Fibonacci. El orden p-ádico de sucesiones lineales recurrentes de orden superior también ha sido estudiado en algunos casos particulares (ver [1, 4]). Bravo, Diaz y Ramirez por ejemplo caracterizaron en [1] el orden 2-ádico y 3-ádico de los números de Tripell.

En el año 2016, el Doctor Carlo Sanna en su artículo *"The p-adic valuation of Lucas sequences* [9]", usando el concepto de rango de aparición de un primo en una sucesión de Lucas, describe en forma compacta los resultados previamente conocidos y proporciona fórmulas simples para la valuación p-ádica de los términos de sucesiones de Lucas, lo cual generaliza el resultado de Lengyel sobre el orden p-ádico de los números de Fibonacci.

El presente trabajo de grado tiene como principal objetivo analizar y estudiar el orden p-ádico de los términos de sucesiones de Lucas basados en el artículo del Doctor Sanna.

Capítulo 1

Preliminares

En este capítulo se presentan algunas definiciones importantes y necesarias para el entendimiento del trabajo presentado a continuación, además de algunos resultados que ayudarán a lo largo del desarrollo de la presente tesis. Las principales referencias utilizadas para abordar estas temáticas son [7, 10–12].

Es de anotar que se entenderá el conjunto de los números naturales $\mathbb{N}$ como el conjunto de los enteros positivos incluido el cero.

1.1. Números algebraicos

Los comienzos de la teoría de números algebraicos se remontan a las ecuaciones de Diofanto, llamado así por el matemático del siglo III Diofanto, quien estudió y desarrolló métodos para la solución de algunos tipos de ecuaciones Diofánticas. [1]

Definición 1.1 *El número $\alpha \in \mathbb{C}$ se llama algebraico si satisface una ecuación polinómica de la forma*

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

para algún $n \geq 1$ y $a_1, a_2, \ldots, a_n \in \mathbb{Q}$. El conjunto de números algebraicos se denota por $\bar{\mathbb{Q}}$.

[1] Se denomina ecuación Diofántica a cualquier ecuación algebraica de una o más incógnitas, cuyos coeficientes recorren el conjunto de los números enteros, de las que se buscan soluciones que pertenezcan al conjunto de los enteros.

Ejemplo 1.2 *Los siguientes son ejemplos de números algebraicos.*

- $\alpha = \dfrac{\sqrt{2}}{2}$, *ya que la siguiente expresión algebraica se verifica para* α,

$$x^2 - \frac{1}{2} = 0.$$

- $\alpha = \sqrt[3]{2} + 1$, *ya que satisface la siguiente ecuación,*

$$(x-1)^3 = 2,$$

o equivalentemente,

$$x^3 - 3x^2 + 3x - 3 = 0.$$

Proposición 1.3

Algunas propiedades de los números algebraicos que merece la pena resaltar son las siguientes.

(1) $\mathbb{Q} \subset \bar{\mathbb{Q}}$.

(2) $\bar{\mathbb{Q}}$ *es un subcampo de* $\mathbb{C}$.

(3) El número $\alpha \in \mathbb{C}$ *es algebraico si, y sólo si, existe un espacio vectorial de dimensión finita* $V \neq 0$ *tal que si* $V \subset \mathbb{C}$, *se garantiza que* $\alpha V \subset V$.

(4) El número $\alpha \in \mathbb{C}$ *es algebraico si, y sólo si, el espacio vectorial sobre* $\mathbb{Q}$, $V = \{1, \alpha, \alpha^2, \ldots\}$, *es de dimensión finita.*

(5) $\bar{\mathbb{Q}}$ *es algebraicamente cerrado. Esto significa que si* $\alpha \in \mathbb{C}$ *satisface la ecuación*

$$x^n + c_1 x^{n-1} + \cdots + c_n = 0$$

con $c_1, c_2, \ldots, c_n \in \bar{\mathbb{Q}}$, *entonces* $\alpha \in \bar{\mathbb{Q}}$.

Definición 1.4 *Se dice que un polinomio* $p(x)$ *es* **mónico** *si su coeficiente principal es* 1, *es decir, si* $p(x)$ *es de la forma,*

$$p(x) = x^n + a_1 x^{n-1} + \cdots + a_n.$$

Proposición 1.5 *Sea α un número algebraico que satisface el polinomio mónico $m(x) \in \mathbb{Q}[x]$[2] de grado mínimo. Para $p(x) \in \mathbb{Q}[x]$, se tiene que si $p(\alpha) = 0$, entonces $m(x) \mid p(x)$.*

Demostración. Dado que $p(x)$ es un polinomio tal que $p(\alpha) = 0$ y teniendo en cuenta el hecho de que $m(x)$ es el polinomio de grado mínimo que satisface la condición $m(\alpha) = 0$, se garantiza que el grado de $p(x)$ es mayor que el grado de $m(x)$. Así, usando el algoritmo de la división existen polinomios $q(x)$ y $r(x)$ tales que $p(x) = m(x)q(x) + r(x)$ donde el grado de $r(x)$ es menor que el grado de $m(x)$. Luego

$$\begin{aligned} p(\alpha) &= m(\alpha)q(\alpha) + r(\alpha) \\ 0 &= 0 \cdot q(\alpha) + r(\alpha) \\ 0 &= r(\alpha). \end{aligned}$$

Pero $m(x)$ es el polinomio de grado mínimo con esta condición, por lo tanto $r(x) = 0$ de donde se garantiza que $m(x) \mid p(x)$. ■

Definición 1.6 *El polinomio $m(x)$ mencionado en la proposición anterior se llama* **polinomio mínimo** *de α. Si $gr(m(x)) = d$, entonces se dice que α es número algebraico de grado d.*

Enteros algebraicos

El número $\alpha \in \mathbb{C}$ es un entero algebraico si satisface una ecuación polinómica de la forma

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

para algunos coeficientes $a_1, a_2, \ldots, a_n \in \mathbb{Z}$.

El conjunto de enteros algebraicos se denota por $\bar{\mathbb{Z}}$.

Observación 1.7 *En teoría de números algebraicos, un número entero algebraico a menudo se llama simplemente un número entero, mientras que los números enteros ordinarios (los elementos de $\mathbb{Z}$) se llaman enteros racionales.*

Ejemplo 1.8 *Los siguientes son ejemplos de enteros algebraicos.*

[2]Se denota por $\mathbb{Q}[x]$ al conjunto de polinomios en la variable x con coeficientes racionales.

- $\alpha = 3\sqrt{2} + 1 \in \bar{\mathbb{Z}}$, *ya que* α *cumple la ecuación* $x^2 - 2x - 17 = 0$.
- $\alpha = \sqrt{2} + \sqrt{3} \in \bar{\mathbb{Z}}$, *dado que* α *satisface la expresión algebraica* $x^4 - 10x^2 + 1 = 0$.

Proposición 1.9

A continuación se mencionan las principales propiedades del conjunto de los enteros algebraicos.

(1) $\mathbb{Z} \subset \bar{\mathbb{Z}}$.

(2) *Si un entero algebraico es racional, entonces éste es un entero racional, es decir,*

$$\bar{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}. \tag{1.1}$$

(3) *Si* $\alpha \in \bar{\mathbb{Q}}$, *entonces* $n\alpha \in \bar{\mathbb{Z}}$ *para algún* $n \in \mathbb{Z}, n \neq 0$.

(4) $\bar{\mathbb{Z}}$ *es un subanillo de* $\mathbb{C}$.

(5) *El número* $\alpha \in \mathbb{C}$ *es un entero algebraico si, y sólo si, existe un grupo abeliano finitamente generado distinto de cero* $B \subset \mathbb{C}$, *tal que* $\alpha B \subset B$.

(6) *El número* $\alpha \in \mathbb{C}$ *es un entero algebraico si, y sólo si, el grupo abeliano* B *definido por* $B = \{1, \alpha, \alpha^2, \ldots\} \subset \mathbb{C}$ *es finitamente generado.*

(7) $\bar{\mathbb{Z}}$ *es integralmente cerrado, es decir, si* $\alpha \in \mathbb{C}$ *satisface la ecuación*

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0,$$

con $a_1, a_2, \ldots, a_n \in \bar{\mathbb{Z}}$, *entonces* $\alpha \in \bar{\mathbb{Z}}$.

1.2. Residuos cuadráticos

La congruencia $x \equiv a \pmod{m}$ es una relación de equivalencia que permite clasificar a los números enteros, y por ende a los naturales, en clases de equivalencia. Estas clases se llaman clases de restos o residuales y están formadas por cada número entero y todos sus congruentes. En este contexto, se llaman así porque cada clase puede representarse por el residuo que resulta al dividir cualquier elemento entre el módulo m. Las clases módulo m se representan por $\mathbb{Z}/m\mathbb{Z}$ o por $\mathbb{Z}_m$.

(1) Para $m = 2$, $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$, son los restos producidos al dividir un entero arbitrario entre 2. El elemento 0 representa a los números pares y el 1 a los impares.

(2) Para $m = 5$, $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$. Aquí, por ejemplo, el elemento 3 representa a los números $\ldots, -12, -7-3, -2, 3, 8, 13, 18, 23, \ldots$, que dan residuo 3 al dividir entre 5.

La clase $\mathbb{Z}/m\mathbb{Z}$ contiene exactamente m elementos a saber: $\{0, 1, 2, 3, 4, 5, 6, \ldots, m-1\}$. En los sistemas algebraicos, las clases de restos tienen estructura de anillo para la suma y el producto módulo m.

Definición 1.10 *Se llama* **sistema completo de restos** *al conjunto de m enteros, tomados cada uno de ellos de una de las clases de restos módulo m $\{0, 1, 3, 4, 5, 6, \ldots, m-1\}$.*

Definición 1.11 *Se llaman* **restos potenciales** *de un número natural n respecto a un módulo m, a los restos producidos al dividir las distintas potencias naturales de n entre m.*

Ejemplo 1.12 *Los restos potenciales de 5 módulo 3 son:*

$$5^0 \equiv 1 \pmod 3,$$
$$5^1 \equiv 2 \pmod 3,$$
$$5^2 \equiv 1 \pmod 3,$$
$$5^3 \equiv 2 \pmod 3,$$

y así sucesivamente. Luego los restos potenciales de 5 módulo 3 son 1 y 2.

Definición 1.13 *Sea $a \in \mathbb{Z}$ y $n \in \mathbb{Z}^+$. Se dice que a es un* ***resto cuadrático*** *(o residuo cuadrático) módulo n, si existe $x \in \mathbb{Z}$ tal que $x^2 \equiv a \pmod n$.*

Observación 1.14 *El producto de dos restos cuadráticos siempre es un resto cuadrático.*

Ejemplo 1.15 *Calculemos los restos cuadráticos respecto al módulo 17. El sistema completo de restos respecto al módulo* 17 *es el conjunto*

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}.$$

Así, el sistema cuadrático de restos, respecto al módulo 17 *es* $\{1, 2, 4, 8, 9, 13, 15, 16\}$*, y se calcula de la siguiente forma:*

$$\begin{array}{llll} 1^2 \equiv 1 & 5^2 \equiv 8 & 9^2 \equiv 13 & 13^2 \equiv 16 \\ 2^2 \equiv 4 & 6^2 \equiv 2 & 10^2 \equiv 15 & 14^2 \equiv 9 \\ 3^2 \equiv 9 & 7^2 \equiv 15 & 11^2 \equiv 2 & 15^2 \equiv 4 \\ 4^2 \equiv 16 & 8^2 \equiv 13 & 12^2 \equiv 8 & 16^2 \equiv 1. \end{array}$$

Observe que los restos cuadráticos respecto a un módulo se pueden dividir en parejas en las cuales la suma de las bases es igual al módulo. Este patrón simétrico permite obtener la totalidad de restos cuadráticos utilizando sólo la mitad de los números base. El procedimiento es el siguiente:

$$\begin{array}{llll} 1^2 \ \ y \ \ 16^2 \equiv 1 \pmod{17}, & & 5^2 \ \ y \ \ 12^2 \equiv 8 \pmod{17}, \\ 2^2 \ \ y \ \ 15^2 \equiv 4 \pmod{17}, & & 6^2 \ \ y \ \ 11^2 \equiv 2 \pmod{17}, \\ 3^2 \ \ y \ \ 14^2 \equiv 9 \pmod{17}, & & 7^2 \ \ y \ \ 10^2 \equiv 15 \pmod{17}, \\ 4^2 \ \ y \ \ 13^2 \equiv 16 \pmod{17}, & & 8^2 \ \ y \ \ 9^2 \equiv 13 \pmod{17}. \end{array}$$

De hecho, si a *es un resto cuadrático módulo* n*, entonces* $n - a$ *también lo es.*

Lema 1.16 *Si* a *es un resto cuadrático módulo* $p \neq 2$*, se garantiza que la congruencia* $x^2 \equiv a \pmod{p}$ *admite* 2 *soluciones.*

Demostración. Si a es resto cuadrático, la congruencia $x^2 \equiv a \pmod{p}$ admite una solución, digamos $x \equiv x_1 \pmod{p}$. Como $(-x_1)^2 \equiv {x_1}^2 \equiv a \pmod{p}$, entonces la congruencia admite una segunda solución $x \equiv -x_1 \pmod{p}$, que es distinta a la anterior porque $p \neq 2$. Luego, $x^2 \equiv a \pmod{p}$ admite como soluciones a x_1 y $-x_1$. ■

1.3. Símbolo de Legendre

El símbolo de Legendre fue introducido por *Adrien-Marie Legendre* en 1798 en el curso de sus intentos de demostrar la ley de reciprocidad cuadrática. Generalizaciones del símbolo incluyen

el símbolo de Jacobi y los caracteres de Dirichlet de orden superior. La conveniencia de la notación del símbolo de Legendre inspiró la introducción de varios otros símbolos utilizados en la teoría algebraíca de números, como el símbolo de Hilbert y el símbolo de Artin.

El símbolo de Legendre es una función multiplicativa utilizada para determinar el *carácter cuadrático* de un número a con respecto a un módulo primo p, es decir, si a es residuo cuadrático o no. Toma como argumentos un entero a y un primo $p > 2$ y devuelve uno de los valores: $0, 1, -1$, dependiendo de si a es o no residuo cuadrático módulo p, es decir, de si la congruencia $x^2 \equiv a \pmod{p}$ tiene solución o no.

Definición 1.17 *Sea $p > 2$ un primo y a un entero. Se define el* ***símbolo de Legendre***[3] *de la siguiente forma,*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & si \quad a \text{ es un resto cuadrático módulo } p, \\ -1, & si \quad a \text{ no es un resto cuadrático módulo } p, \\ 0, & si \quad p \mid a. \end{cases}$$

Ejemplo 1.18

$$\left(\frac{1}{3}\right) = 1, \text{ ya que } 2^2 \equiv 1 \pmod{3}.$$

Proposición 1.19

A continuación se presentan algunas propiedades interesantes del símbolo de Legendre $(a|p)$. Para todo primo impar p se tiene que:

(1) $\left(\frac{1}{p}\right) = 1$. *En efecto,* $1^2 \equiv 1 \pmod{p}$, *por lo que* 1 *es un resto cuadrático.*

(2) $$\left(\frac{-1}{p}\right) = \begin{cases} 1 & si \quad p \equiv 1 \pmod{4}, \\ -1 & si \quad p \equiv 3 \pmod{4}. \end{cases}$$

(3) $$\left(\frac{2}{p}\right) = \begin{cases} 1 & si \quad p \equiv 1, 7 \pmod{8}, \\ -1 & si \quad p \equiv 3, 5 \pmod{8}. \end{cases}$$

(4) $$\left(\frac{3}{p}\right) = \begin{cases} 1 & si \quad p \equiv 1, 11 \pmod{12}, \\ -1 & si \quad p \equiv 5, 7 \pmod{12}. \end{cases}$$

[3] $(a|p)$ también es una notación válida para el símbolo de Legendre.

(5) $\left(\frac{5}{p}\right) = \begin{cases} 1 & si \quad p \equiv 1,4 \pmod 5, \\ -1 & si \quad p \equiv 2,3 \pmod 5. \end{cases}$

(6) $\left(\frac{a^2}{p}\right) = 1.$

(7) Para todo $a, b \in \mathbb{Z}$*, se tiene que* $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

(8) Si $a \equiv b \pmod p$*, entonces* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$*. Esta propiedad se debe a que los números de una misma clase son simultáneamente restos cuadráticos o restos no cuadráticos.*

(9) Si p *y* q *son números primos impares se garantiza que*

$$\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right).$$

Esta propiedad es conocida como Ley de Reciprocidad Cuadrática.

Criterio de Euler

En teoría de números, específicamente en aritmética modular, el Criterio de Euler se emplea para determinar si un entero a es un residuo cuadrático módulo un número primo. Este criterio lleva el nombre del matemático suizo Leonhard Euler.

Teorema 1.20 (Criterio de Euler) *Sea* $p > 2$ *un número primo y* a *un entero coprimo con* p*. Entonces* a *es un residuo cuadrático módulo* p *si, y sólo si,* $a^{(p-1)/2} \equiv 1 \pmod p$.

Demostración. Suponga que $a \equiv x^2 \pmod p$ para algún $x \in \mathbb{Z}$. Como $p \nmid x$, entonces por el Pequeño teorema de Fermat, $x^{p-1} \equiv 1 \pmod p$. Por lo tanto se deduce que

$$a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod p.$$

Recíprocamente, suponga que $a^{(p-1)/2} \equiv 1 \pmod p$. Sea b un elemento primitivo[4] módulo p. Entonces $a \equiv b^i \pmod p$ para algún i. Luego se tiene que $a^{(p-1)/2} \equiv b^{i(p-1)/2} \equiv 1 \pmod p$. Como b es de orden $p-1$, debe darse el caso de que $p-1$ divide a $i(p-1)/2$. Por lo tanto i es par y las raíces cuadradas de a son $\pm b^{i/2}$. ■

[4]Esto significa que b es un generador del grupo multiplicativo $\mathbb{Z}_p^*$.

Como corolario de este teorema se obtiene que si a no es un residuo cuadrático módulo p, entonces $a^{(p-1)/2} \equiv -1 \pmod{p}$. Así, el criterio de Euler puede expresarse de manera más compacta usando el símbolo de Legendre:

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

1.4. Raíces n-ésimas de la unidad

La conceptualización de las raíces de la unidad tiene orígenes históricos que se remontan a las antiguas matemáticas, pero su formalización y comprensión profunda se atribuyen principalmente a Leonhard Euler en el siglo XVIII. Euler, a través de su trabajo en análisis matemático, contribuyó significativamente al entendimiento de los números complejos y las soluciones de ecuaciones polinómicas. Las raíces de la unidad, expresadas como números complejos de la forma $(\cos(\theta)+i\sin(\theta))$, son soluciones clave para ecuaciones polinómicas de grado n y desempeñan un papel central en la teoría de números y el análisis complejo.

Estas raíces poseen propiedades fascinantes y cuentan con aplicaciones extensas en diversos campos. En teoría de números, se utilizan para estudiar propiedades de los números enteros, especialmente en relación con las raíces n-ésimas de la unidad. En análisis matemático, las raíces de la unidad son esenciales para entender series infinitas y convergencia. Además, en ingeniería juegan un papel crucial en el análisis de señales y sistemas, proporcionando una herramienta poderosa para modelar fenómenos cíclicos y oscilatorios. En resumen, las raíces de la unidad representan un concepto matemático fundamental con aplicaciones amplias y profundas en diversas disciplinas.

Observación 1.21 *Encontrar las* **raíces n-ésimas de un complejo** $z \in \mathbb{C}$ *es equivalente a resolver la ecuación* $w^n = z$ *con* $n \in \mathbb{N}$ *y* $w \in \mathbb{C}$.

Definición 1.22 *Se dice que* $z \in \mathbb{C}$ *es una* ***raíz n-ésima de la unidad*** *si* $z^n = 1$ *para algún número natural* n.

Se denota por G_n al conjunto de todas las raíces n-ésimas de la unidad, esto es,

$$G_n = \{z \in \mathbb{C} : z^n = 1\}.$$

Explícitamente,

$$G_n = \left\{ w_k = e^{2\pi ki/n} : 0 \leq k < n-1 \right\},$$

y en consecuencia $\#(G_n) = n$.

Proposición 1.23

Algunas de las principales propiedades de las raíces de la unidad se presentan a continuación.

(1) Para $n \geq 2$, la suma de las n raíces n-ésimas de la unidad es igual a cero.

Demostración. Las raíces n-ésimas de la unidad son $e^{2\pi ki/n}$ para $k = 0, \ldots, n-1$. Su suma es entonces,

$$S = \sum_{k=0}^{n-1} (e^{2\pi i/n})^k.$$

Como $n \geq 2$, se tiene que $e^{2\pi i/n} \neq 1$. Así, usando la fórmula de una suma geométrica se obtiene:

$$S = \frac{(e^{2\pi i/n})^n - 1}{e^{2\pi i/n} - 1} = \frac{1-1}{e^{2\pi i/n} - 1} = 0.$$

■

(2) El producto de raíces n-ésimas de la unidad también es una raíz n-ésima de la unidad.

Demostración. Sean x e y raíces n-ésimas de la unidad, esto es $x^n = 1$ y $y^n = 1$. Entonces

$$x^n y^n = (xy)^n = 1,$$

es decir, xy es raíz n-ésima de la unidad. ■

1.5. Orden p-ádico

Kurt Hensel nació el 29 de diciembre de 1861 en lo que se conoció como Könisberg, Prussia a finales del siglo XIX. Teniendo influencias de distinguidos profesores como Lipschitz, Weierstrass, Borchardt, Kirchhoff, Helmholtz y Kronecker. Este último fue fundamental en su interés por explorar el método de Weierstrass en series de potencias de funciones logrando así la introducción de los números p-ádicos. Inicialmente su interés se centraba en encontrar la

potencia exacta de un número primo que dividiera el discriminante de un cuerpo de números. Posteriormente, introdujo el concepto de cuerpo con valuación, una contribución que tendría un impacto significativo en el estudio del álgebra moderna.

Definición 1.24 *Una* **valuación** *sobre un anillo conmutativo A es una función*

$$v : A \to \mathbb{Z} \cup \{+\infty\}$$

que satisface las siguientes propiedades:

(1) $v(x) = +\infty$ *si, y sólo si,* $x = 0$*;*

(2) $v(xy) = v(x) + v(y)$*;*

(3) *La desigualdad ultramétrica* $v(x + y) \geq \text{mín}\{v(x), v(y)\}$.

Un ejemplo de una valuación sobre $\mathbb{Z}$ se encuentra en la siguiente definición.

Definición 1.25 *Sea p un número primo. La* **valuación p-ádica** *(también conocida como* **orden p-ádico***), de un número entero n, se define de la siguiente forma*

$$v_p(n) = \begin{cases} \text{máx}\{k : p^k \mid n\} \text{ si } n \neq 0, \\ \infty \text{ si } n = 0. \end{cases}$$

Observación 1.26 *En efecto, el orden p-ádico es un ejemplo de una valuación sobre $\mathbb{Z}$, ya que el ítem (1) de la Definición 1.24 se encuentra implícito en la definición anterior de orden p-ádico, mientras que los ítems (2) y (3) se verifican a continuación. Para tal efecto, sean $v_p(x) = m$ y $v_p(y) = n$, esto es $x = p^m t$ y $y = p^n k$ donde $p \nmid t$ y $p \nmid k$.*

- *Observe que $xy = p^m t \cdot p^n k = p^{n+m} kt$ y $p \nmid tk$, de donde se concluye que*

$$v_p(xy) = n + m = v_p(x) + v_p(y).$$

- *Sin pérdida de generalidad suponga que $m > n$. Entonces*

$$x + y = p^m t + p^n k = p^n(p^{m-n} t + k) \text{ y } p \nmid p^{m-n} t + k \text{ ya que } p \nmid k.$$

Por lo tanto,

$$v_p(x+y) = n = \text{mín}\left\{v_p(x), v_p(y)\right\}. \tag{1.2}$$

Si $m = n$, entonces se tiene que

$$v_p(x+y) \geq \text{mín}\left\{v_p(x), v_p(y)\right\}.$$

La valuación p-ádica se puede extender al conjunto de los números racionales como la función $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{+\infty\}$, definida por $v_p(x/y) = v_p(x) - v_p(y)$.

Se dejan los detalles de la prueba para el lector.

Ejemplo 1.27 $v_2(9/8) = v_2(9) - v_2(8) = 0 - 3 = -3$.

Proposición 1.28 (Propiedades elementales del orden p-ádico)

Para $x \in \mathbb{Z}$ y todo primo p se tiene:

(1) $v_p(1) = v_p(-1) = 0$.

Demostración. Como p es un número primo se garantiza que $p \nmid 1$, y por ende, $p \nmid -1$.

Luego $v_p(1) = v_p(-1) = 0$. ■

(2) $v_p(x) = v_p(-x)$.

Demostración. $v_p(-x) = v_p((-1)x) = v_p(-1) + v_p(x) = 0 + v_p(x) = v_p(x)$. ■

(3) $v_p(x^n) = nv_p(x)$, $n \in \mathbb{N}$.

Demostración.

$$v_p(x^n) = v_p\left(\prod_{i=1}^{n} x\right) = \sum_{i=1}^{n} v_p(x) = nv_p(x).$$

■

(4) $v_p(x^{-1}) = -v_p(x)$.

Demostración.

$$v_p(x^{-1}) = v_p(1/x) = v_p(1) - v_p(x) = -v_p(x).$$

■

(5) *Si* $p \nmid x$ *y* $n \in \mathbb{Z}$, *entonces* $v_p(x^n) = 0$.

Demostración.

Note que $v_p(x) = 0$ *ya que* $p \nmid x$. *Luego* $v_p(x^n) = n \cdot v_p(x) = n \cdot 0 = 0$. ■

(6) $v_p\left(\binom{p}{n}\right) = 1$, $n \in \mathbb{N}$, $1 \leq n < p$.

Demostración. Para $n = 1$ *la igualdad se verifica claramente. Ahora para* $1 < n < p$ *se tiene:*

$$\begin{aligned} v_p\left(\binom{p}{n}\right) &= v_p\left(\frac{p!}{n!(p-n)!}\right) \\ &= v_p\left(\frac{(p-n)!(p-n+1)(p-n+2)\cdots(p-1)(p)}{n!(p-n)!}\right) \\ &= v_p\left(\frac{(p-n+1)(p-n+2)\cdots(p-1)(p)}{n!}\right) \\ &= v_p((p-n+1)(p-n+2)\cdots(p-1)(p)) - v_p(n!). \end{aligned}$$

Observando que para todo x *en el conjunto* $\{p-n+1, p-n+2, \ldots, p-1\}$ *se cumple que* $x < p$, *se tiene que* $v_p(x) = 0$. *Similarmente, como* $n < p$ *se sigue que* $v_p(n!) = 0$. *Gracias a que la valuación de un producto es igual a la suma de las valuaciones de sus factores se garantiza que*

$$v_p\left(\binom{p}{n}\right) = 1.$$

■

El siguiente lema, a menudo es utilizado en concursos olímpicos de resolución de problemas, pertenece al folclor matemático y normalmente se atribuye a Lucas y Carmichael.

Lema 1.29 (Lema de elevación del exponente) *Para todo número primo impar* p, *todos los enteros* c *y* d *tales que* $p \nmid cd$ *y* $p \mid c - d$, *y todo entero positivo* n, *se tiene:*

$$v_p(c^n - d^n) = v_p(n) + v_p(c - d).$$

Demostración. Note que

$$c^n - d^n = (c-d)(c^{n-1} + c^{n-2}d + c^{n-3}d^2 + \cdots + cd^{n-2} + d^{n-1}).$$

De la hipótesis $p \mid c-d$, se tiene que $c \equiv d \pmod{p}$ y por tanto

$$\begin{aligned} c^{n-1}+c^{n-2}d+\cdots+cd^{n-2}+d^{n-1} &\equiv c^{n-1}+c^{n-2}c+\cdots+cc^{n-2}+c^{n-1} \pmod{p} \\ &\equiv nc^{n-1} \pmod{p}. \end{aligned}$$

Considere los siguientes casos.

Caso 1. Si $(n,p)=1$, entonces $p \nmid (c^{n-1}+c^{n-2}d+c^{n-3}d^2+\cdots+cd^{n-2}+d^{n-1})$ y así

$$v_p(c^n-d^n)=v_p(c-d).$$

Luego el lema se cumple ya que $v_p(n)=0$.

Caso 2. Si $n=p$, entonces $p \mid (c^{p-1}+c^{p-2}d+c^{p-3}d^2+\cdots+cd^{p-2}+d^{p-1})$. A continuación se prueba que

$$p^2 \nmid (c^{p-1}+c^{p-2}d+c^{p-3}d^2+\cdots+cd^{p-2}+d^{p-1}).$$

En efecto, de la hipótesis $p \mid (c-d)$ se tiene que $d=c+kp$ para algún $k \in \mathbb{Z}$. Para $0 \leq t < p$ se tiene

$$\begin{aligned} c^{p-1-t}d^t &= c^{p-1-t}(c+kp)^t \\ &= c^{p-1-t}\left(c^t+t(kp)c^{t-1}+\frac{t(t-1)}{2}(kp)^2c^{t-2}+\cdots+(kp)^t\right) \\ &\equiv c^{p-1-t}(c^t+tkpc^{t-1}) \pmod{p^2} \\ &\equiv c^{p-1}+tkpc^{p-2} \pmod{p^2}. \end{aligned}$$

Por lo anterior se obtiene

$$\begin{aligned} c^{p-1}+c^{p-2}d+\cdots+d^{p-1} &\equiv c^{p-1}+(c^{p-1}+kpc^{p-2})+\cdots+(c^{p-1}+(p-1)kpc^{p-2}) \pmod{p^2} \\ &\equiv pc^{p-1}+(1+2+3+\cdots+p-1)kpc^{p-2} \\ &\equiv pc^{p-1}+\left(\frac{p-1}{2}\right)kp^2c^{p-2} \\ &\equiv pc^{p-1} \pmod{p^2} \\ &\not\equiv 0 \pmod{p^2}. \end{aligned}$$

Luego

$$v_p(c^p-d^p)=v_p(c-d)+1=v_p(c-d)+v_p(n).$$

Caso 3. Finalmente, si n es de la forma $n = p^\alpha b$ con $(p, b) = 1$, de los Casos 1 y 2 se tiene,

$$\begin{aligned} v_p(c^n - d^n) &= v_p((c^{p^\alpha})^b - (d^{p^\alpha})^b) = v_p(c^{p^\alpha} - d^{p^\alpha}) = v_p((c^{p^{\alpha-1}})^p - (d^{p^{\alpha-1}})^p) \\ &= v_p(c^{p^{\alpha-1}} - d^{p^{\alpha-1}}) + 1 = v_p((c^{p^{\alpha-2}})^p - (d^{p^{\alpha-2}})^p) + 1 \\ &= v_p(c^{p^{\alpha-2}} - d^{p^{\alpha-2}}) + 2 \\ &\vdots \\ &= v_p(c^{p^0} - d^{p^0}) + \alpha \\ &= v_p(c - d) + v_p(n). \end{aligned}$$

■

1.6. Sucesiones lineales recurrentes

Una sucesión de números complejos es una función del conjunto de los números naturales en los complejos $f : \mathbb{N} \to \mathbb{C}$. A continuación se presentan algunas observaciones sobre sucesiones.

- Una sucesión asigna a cada número natural un número complejo determinado de manera única.
- Cada elemento de la sucesión se denota por $f_n = f(n)$.
- La sucesión se denota por $(f_n)_{n\in\mathbb{N}}$ ó simplemente $(f_n)_{n\geq 0}$.
- Al elemento f_n se le llama n-ésimo término de la sucesión.

En este documento se escribirán las sucesiones en la forma

$$u_0, u_1, u_2, \ldots, u_n, \ldots \quad \text{o} \quad (u_n)_{n\geq 0}. \tag{1.3}$$

Definición 1.30 *Si existen números reales o complejos $a_0, a_1, \ldots, a_{k-1}$ tales que el término $(m + k)$-ésimo de la sucesión $(u_n)_{n\geq 0}$ está dado por:*

$$u_{m+k} = a_{k-1}u_{m+k-1} + a_{k-2}u_{m+k-2} + \cdots + a_0u_m \text{ para } m \geq 0, \tag{1.4}$$

entonces la sucesión se llama ***sucesión lineal recurrente de orden*** *k (o simplemente* **recurrencia** *de orden k).*

Definición 1.31 *El* **polinomio característico** *de la sucesión* $(u_n)_{n\geq 0}$ *que satisface* (1.4) *está dado por:*

$$p(X) := X^k - a_{k-1}X^{k-1} - \cdots - a_1X - a_0. \tag{1.5}$$

Definición 1.32 *Si*

$$p(X) = \prod_{j=1}^{s}(X-\gamma_j)^{\sigma_j} : \gamma_i \neq \gamma_k \text{ si } i \neq k, \tag{1.6}$$

es la factorización del polinomio característico $p(X)$ *definido por* (1.5)*, entonces* $\gamma_1, \gamma_1, \ldots, \gamma_s$ *reciben el nombre de* **raíces de la recurrencia**. *Si todas las raíces de la recurrencia son simples, entonces se dice que la recurrencia es simple.*

Teorema 1.33 *Suponga que la sucesión* $(u_n)_{n\geq 0}$ *es simple con raíces* $\gamma_1, \ldots, \gamma_k$*. Entonces* $(u_n)_{n\geq 0}$ *satisface la recurrencia lineal de orden* k *con polinomio característico* $p(X)$ *si, y sólo si, existen constantes* $B_1, \ldots, B_k$*, que no dependen de* n*, tales que*

$$u_n = B_1\gamma_1^n + \cdots + B_k\gamma_k^n \quad \text{para todo} \quad n \geq 0.$$

Ejemplo 1.34 *Las sucesiones lineales recurrentes de orden 1 se refieren a las* **progresiones geométricas**, *en estás cada término se obtiene multiplicando el término anterior por una constante denominada razón o factor de la progresión. Si se denota por* a_{n-1} *al término que ocupa la posición* n *de la sucesión, se puede calcular el valor de cualquier término a partir del primer término* a_0 *y de la razón* r *mediante la siguiente fórmula llamada* **término general**

$$a_{n-1} = a_0 \cdot r^{n-1}.$$

Ejemplo 1.35 *Las sucesiones lineales recurrentes de orden 2 son conocidas como* **sucesiones binarias**. *Un ejemplo notable son las sucesiones de Lucas, que se abordarán a detalle en el siguiente capitulo.*

Uno de los ejemplos más celebrés de sucesiones binarias es la sucesión de Fibonacci $(F_n)_{n\geq 0}$*, cuyos valores iniciales son* $F_0 = 0, F_1 = 1$ *y para* $n \geq 2$ *el* n*-ésimo término está definido por la siguiente expresión*

$$F_n = F_{n-1} + F_{n-2}.$$

Hacia el año 1202, Leonardo de Pisa también conocido como Fibonacci, fue un joven italiano que en sus viajes a oriente descubrió la existencia de los números arábigos. A su regreso, escribió el libro "Liber Abaci"*, en el que trasladó los saberes matemáticos de los orientales a Europa.*

Fibonacci abogaba por el nuevo sistema de números por su conveniencia en asuntos comerciales en contraste con los números romanos utilizados en su época. La inquietud que lo llevó a postular la famosa secuencia que lleva su nombre era su curiosidad sobre los hábitos de apareamiento de los conejos. Al suponer que estos alcanzan la madures sexual al cabo de un mes y cada pareja es capaz de producir una nueva pareja de conejos, llegó a la siguiente conclusión:

- *Durante el primer mes hay un par de conejos y como no tienen edad suficiente, no pueden reproducirse.*
- *Durante el tercer mes, la pareja se reproduce por primera vez, por lo que hay 2 pares de conejos.*
- *En el cuarto mes, el primer par se reproduce otra vez, por lo que hay tres pares.*
- *Durante el quinto mes, el primer par se reproduce y el segundo par también lo hace, aunque el tercer par todavía es muy joven, por lo que hay cinco pares.*

Este patrón de crecimiento continúa.

En la actualidad, la sucesión de Fibonacci desempeña un papel fundamental en diversas disciplinas, como ciencias de la computación, matemáticas y teoría de juegos. Además, se observa en configuraciones biológicas, como por ejemplo las ramas de los árboles, la disposición de las hojas en el tallo, las flores de alcachofas y girasoles, las inflorescencias del brécol romanesco, las piñas de las coníferas, así como en la codificación del crecimiento de formas orgánicas complejas mediante el ADN. De igual manera, se encuentra en la estructura espiral del caparazón de algunos moluscos.

Ejemplo 1.36 *Las sucesiones lineales recurrentes de orden 3 se conocen como* **sucesiones ternarias***. En estos casos, para garantizar que la ecuación característica asociada a la relación de recurrencia esté bien definida, se proporcionan tres términos iniciales. A partir de estos, cada término adicional de la sucesión se define en función de los tres términos anteriores.*

Entre éstas sucesiones recursivas de orden 3, se destacan unos casos especiales como las de Perrin, Padovan y Tribonacci.

Los números de Padovan $(\mathbb{P}_n)_{n\geq 0}$ *están definidos por la relación* $\mathbb{P}_{n+3} = \mathbb{P}_{n+1} + \mathbb{P}_n$ *con condiciones iniciales* $\mathbb{P}_0 = \mathbb{P}_1 = \mathbb{P}_2 = 1$. *Los primeros números de Padovan son:*

$$1, 1, 1, 2, 2, 3, 4, 5, 7, 9, 12, 16, 21, 28, 37, 49, 65, 86, \ldots$$

Los números de Perrin $(R_n)_{n\geq 0}$ *satisfacen la misma ecuación de recurrencia que los números de Padovan, pero con valores iniciales* $R_0 = 3$, $R_1 = 0$ *y* $R_2 = 2$. *Los primeros términos para* $n \geq 0$ *son:*

$$3, 0, 2, 3, 2, 5, 5, 7, 10, 12, 17, 22, 29, 39, 51, 68, 90, \ldots$$

Finalmente, la sucesión de Tribonacci $(T_n)_{n\geq 0}$, *que también es uno de estos casos especiales corresponde a los valores iniciales* $T_0 = 0$ *y* $T_1 = T_2 = 1$ *y su relación de recurrencia está dada por* $T_n = T_{n-1} + T_{n-2} + T_{n-3}$ *para* $n \geq 3$. *Los primeros términos de esta sucesión son:*

$$0, 1, 1, 2, 4, 7, 13, 24, 44, 81, 149, 274, 504, 927, \ldots$$

Capítulo 2

Sucesiones de Lucas

François Édouard Anatole Lucas (4 de abril de 1842 - 3 de octubre de 1891), conocido como Édouard Lucas, fue un reconocido matemático francés. Inicialmente contribuyó en el observatorio de París y más tarde se dedicó a la enseñanza de las matemáticas en dos institutos parisinos: el Liceo de San Luis y el Liceo Carlomagno. Se le recuerda por sus trabajos acerca de la sucesión de Fibonacci, que él denominó de esa manera, y por el test de primalidad que lleva su nombre, pero también porque fue el inventor de algunos juegos recreativos matemáticos muy conocidos, siendo el más destacado el de las Torres de Hanói. En este capítulo se introduce la definición de sucesión de Lucas, se proporcionan ejemplos y se exploran algunas de sus propiedades.

Para iniciar, sean a, b enteros coprimos no nulos, y considere el polinomio

$$p(X) = X^2 - aX - b.$$

El discriminante de $p(X)$ es $\triangle = a^2 + 4b$ y denotamos sus raíces a lo largo de este documento por:

$$\alpha = \frac{a + \sqrt{\triangle}}{2} \quad \text{y} \quad \beta = \frac{a - \sqrt{\triangle}}{2}.$$

Así,

$$\alpha + \beta = a, \quad \alpha - \beta = \sqrt{\triangle} \quad \text{y} \quad \alpha\beta = -b.$$

Observación 2.1 *Como* $\triangle = a^2 + 4b$*, entonces* $\triangle \equiv a^2 \pmod 4$*. Observe que si* a *es par, entonces* $a^2 \equiv 0 \pmod 4$*, mientras que si* a *es impar, entonces* $a^2 \equiv 1 \pmod 4$*. Por tanto,*

$$\triangle \equiv 0, 1 \pmod 4.$$

Para el par (a, b), se definen las sucesiones de números $u(a, b) = (u_n(a, b))_{n\geq 0}$ y $w(a, b) = (w_n(a, b))_{n\geq 0}$ por las fórmulas

$$u_n = u_n(a, b) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{y} \quad w_n = w_n(a, b) = \alpha^n + \beta^n \quad \text{para todo} \quad n \in \mathbb{Z}. \tag{2.1}$$

En particular, $u_0 = 0$ y $u_1 = 1$, mientras que $w_0 = 2$ y $w_1 = a$. Las sucesiones $u(a, b)$ y $w(a, b)$ se llaman **sucesiones de Lucas** de primera y segunda categoría asociadas al par (a, b) y $p(X)$ representa su polinomio característico; estas sucesiones también son conocidas como sucesión de Lucas y sucesión compañera de Lucas respectivamente. De acuerdo a la Definición 1.31 con $m = n - 2$ se cumple que

$$u_n = au_{n-1} + bu_{n-2} \quad \text{y} \quad w_n = aw_{n-1} + bw_{n-2} \quad \text{para todo} \quad n \geq 2. \tag{2.2}$$

Por tal razón, $u(a, b)$ y $w(a, b)$ corresponden a sucesiones lineales recurrentes de orden dos.

Ejemplo 2.2 *Considere el polinomio $p(X) = X^2 - X - 1$ en el cual $a = 1$ y $b = 1$. Su discriminante es $\triangle = 1^2 + 4(1) = 5$ y sus raíces vienen dadas por:*

$$\alpha = \frac{1 + \sqrt{5}}{2} \quad y \quad \beta = \frac{1 - \sqrt{5}}{2}.$$

Note que $\alpha + \beta = a = 1, \alpha - \beta = \sqrt{5}$ y $\alpha\beta = -1$. Para estos valores de a y b, se tiene que $u_0 = 0, u_1 = 1, w_0 = 2$ y $w_1 = a = 1$. Además, $u_n = u_{n-1} + u_{n-2}$ y $w_n = w_{n-1} + w_{n-2}$ para todo $n \geq 2$. En este caso se puede observar que $u(1, 1)$ representa la sucesión de Fibonacci $(F_n)_{n\geq 0}$ y $w(1, 1)$ corresponde a la sucesión compañera conocida como la sucesión de Lucas, usualmente denotada por $(L_n)_{n\geq 0}$.

A continuación, se presenta una tabla con los primeros 14 términos de las sucesiones de Fibonacci y Lucas.

Tabla 2.1: Primeros términos de las sucesiones de Fibonacci y Lucas.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13
$u_n(1, 1)$	0	1	1	2	3	5	8	13	21	34	55	89	144	233
$w_n(1, 1)$	2	1	3	4	7	11	18	29	47	76	123	199	322	521

Ahora utilizando la fórmula $u_n = (\alpha^n - \beta^n)/(\alpha - \beta)$ *se calcula el séptimo término de la sucesión de Lucas asociada al par* $(1,1)$*, es decir* u_6*.*

$$u_6 = \frac{\alpha^6 - \beta^6}{\alpha - \beta} = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^6 - \left(\frac{1-\sqrt{5}}{2}\right)^6}{\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}} = \frac{\frac{(1+\sqrt{5})^6 - (1-\sqrt{5})^6}{2^6}}{\sqrt{5}}.$$

Al aplicar el Teorema del Binomio en la expresión anterior se obtiene que

$$u_6 = \frac{12\sqrt{5} + 40\sqrt{5}^3 + 12\sqrt{5}^5}{2^6\sqrt{5}} = \frac{12 + 40 \cdot 5 + 12 \cdot 25}{2^6} = \frac{512}{64} = 8.$$

Las sucesiones de Lucas para algunos valores de a y b tienen nombres específicos:

Tabla 2.2: Ejemplos de sucesiones de Lucas.

Sucesión asociada al par (a,b)	**Nombre**
$u_n(1,1)$	Números de Fibonacci
$w_n(1,1)$	Números de Lucas
$u_n(2,1)$	Números de Pell
$w_n(2,1)$	Números de Pell-Lucas
$u_n(1,2)$	Números de Jacobsthal
$w_n(1,2)$	Números de Jacobsthal-Lucas
$u_n(3,-2)$	Números de Merssene $2^n - 1$
$w_n(3,-2)$	Números de la forma $2^n + 1$, que incluye a los números de Fermat

Definición 2.3 *Se dice que una sucesión de Lucas asociada al par* (a,b) *es* ***no degenerada*** *si* $b \neq 0$ *y la razón* α/β *de las 2 raíces del polinomio característico* $p(X)$ *no es una raíz de la unidad.*

Lema 2.4 *Sea* $(u_n)_{n\geq 0}$ *una sucesión de Lucas no degenerada cuyo polinomio característico tiene raíces* α *y* β*. Entonces* $\alpha \neq \beta$ *y por tanto el discriminante* $\triangle$ *de* $p(X)$ *es distinto de cero.*

Demostración. Si $\alpha = \beta$, entonces $\alpha/\beta = 1$, lo cual es una contradicción ya que α/β no es una raíz de la unidad. En consecuencia, $\alpha \neq \beta$. Ahora note que,

$$\triangle \neq 0 \Leftrightarrow (\alpha - \beta)^2 \neq 0 \Leftrightarrow \alpha - \beta \neq 0 \Leftrightarrow \alpha \neq \beta.$$

■

Paulo Ribenboim en su libro *"My Numbers, My Friends:Popular Lectures on Number Theory"* [8] prueba el siguiente teorema.

Teorema 2.5 *Sea $(u_n)_{n\geq 0}$ una sucesión de Lucas degenerada asociada al par de enteros coprimos a y b. Entonces se tiene que $(a, b) \in \{(\pm 2, -1), (\pm 1, -1)\}$ y en cada uno de estos casos $(u_n)_{n\geq 0}$ y su sucesión compañera $(w_n)_{n\geq 0}$, cumplen una de las siguientes condiciones:*

- *Es periódica con valores en $\{0, \pm 1, \pm 2\}$.*
- *Es igual a $(n)_{n\geq 0}$.*
- *Es igual a $((-1)^{n-1}n)_{n\geq 0}$.*

Demostración. Sea $\eta = \alpha/\beta$. Entonces

$$\eta + \eta^{-1} = \frac{\alpha}{\beta} + \frac{\beta}{\alpha} = \frac{\alpha^2 + \beta^2}{\alpha\beta} = \frac{\alpha^2 + 2\alpha\beta + \beta^2 - 2\alpha\beta}{\alpha\beta} = \frac{(\alpha + \beta)^2 - 2\alpha\beta}{\alpha\beta} = \frac{a^2 + 2b}{-b}. \quad (2.3)$$

Por lo anterior $\eta + \eta^{-1}$ es un racional. Además dado que $(u_n)_{n\geq 0}$ es no degenerada se tiene que η es una raíz de la unidad y por tanto existe $n \in \mathbb{N}$ tal que $\eta^n = 1$. En consecuencia η es raíz de la ecuación $X^n - 1 = 0$ y por lo tanto es un entero algebraico. Lo mismo ocurre con η^{-1}. Ahora teniendo en cuenta que $\bar{\mathbb{Z}}$ es un subanillo, se garantiza que la suma de enteros algebraicos da como resultado un entero algebraico, es decir, $\eta + \eta^{-1}$ es un entero algebraico. Luego $\eta + \eta^{-1}$ es un entero.

Ahora observe que $\eta^n = 1$ implica que $|\eta| \leq 1$ y $|\eta^{-1}| \leq 1$. Así, por desigualdad triangular se tiene que

$$|\eta + \eta^{-1}| = |\eta| + |\eta^{-1}| \leq 2.$$

De (2.3) se tiene entonces que

$$-2 \leq \frac{a^2 + 2b}{b} \leq 2.$$

Como $(a^2 + 2b)/b$ es entero, se tienen los siguientes casos:

Caso 1. $a^2 + 2b = 0$. En este caso a^2 es par y por tanto a es par. Luego b es divisible por 2 de donde $(a, b) > 1$, lo que contradice la hipótesis $(a, b) = 1$.

Caso 2. $a^2 + 2b = -b$. Esto implica $a^2 = -3b$. Es decir, a^2 es múltiplo de 3 y por tanto a también lo es. De ahí que $(a, b) > 1$, que contradice la hipótesis $(a, b) = 1$.

Caso 3. $a^2 + 2b = 2b$. En este caso $a^2 = 0$, lo cual no es posible.

Caso 4. $a^2 + 2b = -2b$. Esto implica que $a^2 = -4b$. Como $(a, b) = 1$, entonces obligatoriamente debe ocurrir que $b = -1$ para el cual $a = \pm 2$.

Caso 5. $a^2 + 2b = b$. Esto implica que $a^2 = -b$. Como $(a, b) = 1$, entonces la única opción es $a = \pm 1$ y $b = -1$.

Por lo anterior se concluye que $(a, b) \in \{(\pm 1, -1), (\pm 2, -1)\}$. ■

A continuación se describe todas las sucesiones de Lucas degeneradas en las siguientes tablas.

Tabla 2.3: Primeros términos de sucesiones de Lucas degeneradas.

n	$u_n(1,-1)$	$w_n(1,-1)$	$u_n(-1,-1)$	$w_n(-1,-1)$
0	0	2	0	2
1	1	1	1	-1
2	1	-1	-1	-1
3	0	-2	0	2
4	-1	-1	1	-1
5	-1	1	-1	-1
6	0	2	0	2
7	1	1	1	-1
8	1	-1	-1	-1

Tabla 2.4:

n	$u_n(2,-1)$	$w_n(2,-1)$	$u_n(-2,-1)$	$w_n(-2,-1)$
0	0	2	0	2
1	1	2	1	-2
2	2	2	-2	2
3	3	2	3	-2
4	4	2	-4	2
5	5	2	5	-2
6	6	2	-6	2
7	7	2	7	-2
8	8	2	-8	2
9	9	2	9	-2

2.1. Propiedades elementales de sucesiones de Lucas

Teniendo en cuenta los enteros coprimos a y b, a continuación se relacionan algunas propiedades de las sucesiones de Lucas no degeneradas para enteros positivos n y m.

Multiplicación de indices:

(1) $u_{2n} = u_n w_n$, para todo $n \in \mathbb{Z}$.

Demostración. Usando (2.1) se tiene:

$$u_{2n} = \frac{\alpha^{2n} - \beta^{2n}}{\alpha - \beta} = \frac{(\alpha^n - \beta^n)(\alpha^n + \beta^n)}{\alpha - \beta} = \left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)(\alpha^n + \beta^n) = u_n w_n.$$

■

(2) $w_{2n} = w_n^2 - 2(-b)^n$, para todo $n \in \mathbb{Z}$.

Demostración. Usando (2.1) y el hecho que $\alpha\beta = -b$ se obtiene:

$$\begin{aligned} w_{2n} &= \alpha^{2n} + \beta^{2n} = \alpha^{2n} + 2\alpha^n\beta^n + \beta^{2n} - 2\alpha^n\beta^n \\ &= (\alpha^n + \beta^n)^2 - 2(\alpha\beta)^n = w_n^2 - 2(-b)^n. \end{aligned}$$

■

Suma de indices:

(3) $u_{m+n} = u_m w_n - (-b)^n u_{m-n}$, para todo $m, n \in \mathbb{Z}$.

Demostración. De (2.1) y el hecho que $\alpha\beta = -b$ se tiene que:

$$\begin{aligned} u_{m+n} &= \frac{\alpha^{m+n} - \beta^{m+n}}{\alpha - \beta} \\ &= \frac{\alpha^{m+n} + \alpha^m\beta^n - \alpha^n\beta^m - \beta^{m+n} - \alpha^m\beta^n + \alpha^n\beta^m}{\alpha - \beta} \\ &= \frac{\alpha^{m+n} + \alpha^m\beta^n - \alpha^n\beta^m - \beta^{m+n}}{\alpha - \beta} - \frac{\alpha^m\beta^n - \alpha^n\beta^m}{\alpha - \beta} \\ &= \frac{(\alpha^m - \beta^m)(\alpha^n + \beta^n)}{\alpha - \beta} - \frac{(\alpha\beta)^n(\alpha^{m-n} - \beta^{m-n})}{\alpha - \beta} \\ &= \left(\frac{\alpha^m - \beta^m}{\alpha - \beta}\right)(\alpha^n + \beta^n) - (\alpha\beta)^n \left(\frac{\alpha^{m-n} - \beta^{m-n}}{\alpha - \beta}\right) \\ &= u_m w_n - (-b)^n u_{m-n}. \end{aligned}$$

■

(4) $w_{m+n} = w_m w_n - (-b)^n w_{m-n}$ para todo $m, n \in \mathbb{Z}$.

Demostración. De (2.1) y el hecho que $\alpha\beta = -b$ se llega a que:

$$\begin{aligned} w_{m+n} &= \alpha^{m+n} + \beta^{m+n} \\ &= \alpha^{m+n} + \alpha^m\beta^n + \alpha^n\beta^m + \beta^{m+n} - \alpha^m\beta^n - \alpha^n\beta^m \\ &= (\alpha^m + \beta^m)(\alpha^n + \beta^n) - (\alpha\beta)^n(\alpha^{m-n} + \beta^{m-n}) \\ &= w_m w_n - (-b)^n w_{m-n}. \end{aligned}$$

■

Otras fórmulas del mismo tipo son:

(5) $u_m w_n - u_n w_m = 2(-b)^n u_{m-n}$, para todo $m, n \in \mathbb{Z}$.

Demostración. Usando nuevamente (2.1) y el hecho que $\alpha\beta = -b$ se obtiene:

$$\begin{aligned} u_m w_n - u_n w_m &= \frac{\alpha^m - \beta^m}{\alpha - \beta}(\alpha^n + \beta^n) - \frac{\alpha^n - \beta^n}{\alpha - \beta}(\alpha^m + \beta^m) \\ &= \frac{\alpha^{m+n} + \alpha^m\beta^n - \alpha^n\beta^m - \beta^{m+n}}{\alpha - \beta} - \frac{\alpha^{m+n} + \alpha^n\beta^m - \alpha^m\beta^n - \beta^{m+n}}{\alpha - \beta} \\ &= \frac{2\alpha^m\beta^n - 2\alpha^n\beta^m}{\alpha - \beta} = 2(\alpha\beta)^n \left(\frac{\alpha^{m-n} - \beta^{m-n}}{\alpha - \beta}\right) = 2(-b)^n u_{m-n}. \end{aligned}$$

■

(6) $u_m w_n + u_n w_m = 2u_{m+n}$, para todo $m, n \in \mathbb{Z}$.

Demostración. De (2.1) se garantiza:

$$\begin{aligned} u_m w_n + u_n w_m &= \frac{\alpha^m - \beta^m}{\alpha - \beta}(\alpha^n + \beta^n) + \frac{\alpha^n - \beta^n}{\alpha - \beta}(\alpha^m + \beta^m) \\ &= \frac{\alpha^{m+n} + \alpha^m\beta^n - \alpha^n\beta^m - \beta^{m+n} + \alpha^{m+n} + \alpha^n\beta^m - \alpha^m\beta^n - \beta^{m+n}}{\alpha - \beta} \\ &= \frac{2\alpha^{m+n} - 2\beta^{m+n}}{\alpha - \beta} = 2\left(\frac{\alpha^{m+n} - \beta^{m+n}}{\alpha - \beta}\right) = 2u_{m+n}. \end{aligned}$$

■

(7) $u_{m+n} = u_m u_{n+1} + b u_{m-1} u_n$.

Demostración.

$$\begin{aligned} u_{m+n} &= \frac{\alpha^{m+n} - \beta^{m+n}}{\alpha - \beta} = (\alpha - \beta)\frac{\alpha^{m+n} - \beta^{m+n}}{(\alpha - \beta)^2} = \frac{\alpha(\alpha^{m+n} - \beta^{m+n}) - \beta(\alpha^{m+n} - \beta^{m+n})}{(\alpha - \beta)^2} \\ &= \frac{\alpha^{m+n+1} - \alpha^m\beta^{n+1} - \alpha^{n+1}\beta^m + \beta^{m+n+1} - \beta\alpha^{m+n} + \alpha^m\beta^{n+1} + \alpha^{n+1}\beta^m - \alpha\beta^{m+n}}{(\alpha - \beta)^2}. \end{aligned}$$

Luego de factorizar y separar las fracciones, de la anterior expresión se obtiene:

$$\begin{aligned} u_{m+n} &= \frac{(\alpha^m - \beta^m)(\alpha^{n+1} - \beta^{n+1})}{(\alpha - \beta)^2} - \frac{(\alpha\beta)(\alpha^{m+n-1} - \alpha^{m-1}\beta^n - \alpha^n\beta^{m-1} + \beta^{m+n-1})}{(\alpha - \beta)^2} \\ &= \left(\frac{\alpha^m - \beta^m}{\alpha - \beta}\right)\left(\frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta}\right) - (\alpha\beta)\left(\frac{\alpha^{m-1} - \beta^{m-1}}{\alpha - \beta}\right)\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right) \\ &= u_m u_{n+1} + b u_{m-1} u_n. \end{aligned}$$

■

(8) $2w_{m+n} = w_m w_n + \triangle u_m u_n$.

Demostración.

$$\begin{aligned} 2w_{m+n} &= 2(\alpha^{m+n} + \beta^{m+n}) = 2\alpha^{m+n} + 2\beta^{m+n} \\ &= \alpha^{m+n} + \alpha^m\beta^n + \alpha^n\beta^m + \beta^{m+n} + \frac{(\alpha - \beta)^2(\alpha^{m+n} - \alpha^m\beta^n - \alpha^n\beta^m + \beta^{m+n})}{(\alpha - \beta)^2}. \end{aligned}$$

De la expresión anterior, luego de algunos cálculos se observa que

$$\begin{aligned} 2w_{m+n} &= (\alpha^m + \beta^m)(\alpha^n + \beta^n) + \triangle\left(\frac{\alpha^m - \beta^m}{\alpha - \beta}\right)\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right). \\ &= w_m w_n + \triangle u_m u_n. \end{aligned}$$

■

(9) $\triangle u_n = 2w_{n+1} - aw_n$.

Demostración.

$$\triangle u_n = (\alpha-\beta)^2\left(\frac{\alpha^n-\beta^n}{\alpha-\beta}\right) = 2\alpha^{n+1} + 2\beta^{n+1} - \alpha^{n+1} - \alpha\beta^n - \alpha^n\beta - \beta^{n+1},$$

de donde,

$$\triangle u_n = 2(\alpha^{n+1}+\beta^{n+1}) - (\alpha+\beta)(\alpha^n+\beta^n) = 2w_{n+1} - aw_n.$$

■

(10) $w_n = 2u_{n+1} - au_n$.

Demostración.

$$\begin{aligned} w_n = \alpha^n + \beta^n &= \frac{(\alpha-\beta)(\alpha^n+\beta^n)}{\alpha-\beta} = \frac{\alpha^{n+1} + \alpha\beta^n - \alpha^n\beta - \beta^{n+1}}{\alpha-\beta} \\ &= \frac{2\alpha^{n+1} - 2\beta^{n+1} - \alpha^{n+1} + \alpha\beta^n - \alpha^n\beta + \beta^{n+1}}{\alpha-\beta}. \end{aligned}$$

Así,

$$\begin{aligned} w_n &= \frac{2(\alpha^{n+1}-\beta^{n+1}) - (\alpha+\beta)(\alpha^n-\beta^n)}{\alpha-\beta} \\ &= 2\left(\frac{\alpha^{n+1}-\beta^{n+1}}{\alpha-\beta}\right) - (\alpha+\beta)\left(\frac{\alpha^n-\beta^n}{\alpha-\beta}\right) \\ &= 2u_{n+1} - au_n. \end{aligned}$$

■

(11) $u_n^2 = u_{n-1}u_{n+1} + (-b)^{n-1}$.

Demostración.

$$\begin{aligned} u_n^2 = \left(\frac{\alpha^n-\beta^n}{\alpha-\beta}\right)^2 &= \frac{\alpha^{2n} - 2\alpha^n\beta^n + \beta^{2n}}{(\alpha-\beta)^2} \\ &= \frac{\alpha^{2n} - \alpha^{n-1}\beta^{n+1} - \alpha^{n+1}\beta^{n-1} + \beta^{2n} + \alpha^{n+1}\beta^{n-1} - 2\alpha^n\beta^n + \alpha^{n-1}\beta^{n+1}}{(\alpha-\beta)^2}. \end{aligned}$$

Luego,

$$\begin{aligned} u_n^2 &= \frac{(\alpha^{n-1}-\beta^{n-1})(\alpha^{n+1}-\beta^{n+1}) + (\alpha\beta)^{n-1}(\alpha-\beta)^2}{(\alpha-\beta)^2} \\ &= \frac{(\alpha^{n-1}-\beta^{n-1})(\alpha^{n+1}-\beta^{n+1})}{(\alpha-\beta)^2} + (\alpha\beta)^{n-1}, \end{aligned}$$

y en consecuencia,

$$u_n^2 = \left(\frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta}\right)\left(\frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta}\right) + (\alpha\beta)^{n-1} = u_{n-1}u_{n+1} + (-b)^{n-1}.$$

■

Relaciones cuadráticas:

(12) $w_n^2 = \triangle u_n^2 + 4(-b)^n$, para todo $n \in \mathbb{Z}$.

Demostración. De (2.1) se tiene que:

$$w_n^2 = (\alpha^n + \beta^n)^2 = \alpha^{2n} + 2\alpha^n\beta^n + \beta^{2n} = (\alpha - \beta)^2\frac{\alpha^{2n} - 2\alpha^n\beta^n + \beta^{2n}}{(\alpha - \beta)^2} + 4\alpha^n\beta^n.$$

Por lo tanto, nuevamente de (2.1) y de los hechos que $\triangle = (\alpha - \beta)^2$ y $\alpha\beta = -b$ se llega a que

$$w_n^2 = \triangle\frac{(\alpha^n - \beta^n)^2}{(\alpha - \beta)^2} + 4\alpha^n\beta^n = \triangle\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)^2 + 4(-b)^n = \triangle u_n^2 + 4(-b)^n.$$

■

A continuación se enuncia una fórmula bien conocida que relaciona u_n con los coeficientes binomiales.

Lema 2.6 *Para n impar se tiene que*

$$2^{n-1}u_n = \sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k+1} a^{n-(2k+1)}\triangle^k.$$

Demostración. Usando (2.1) y los hechos que $\sqrt{\triangle} = \alpha - \beta$, $\alpha = (a + \sqrt{\triangle})/2$ y $\beta = (a - \sqrt{\triangle})/2$ se obtiene:

$$\begin{aligned} 2^{n-1}u_n &= \frac{2^n(\alpha^n - \beta^n)}{2(\alpha - \beta)} = \frac{(2\alpha)^n - (2\beta)^n}{2\sqrt{\triangle}} \\ &= \frac{(a + \sqrt{\triangle})^n - (a - \sqrt{\triangle})^n}{2\sqrt{\triangle}}. \end{aligned}$$

Aplicando el Teorema del Binomio se garantiza que:

$$\begin{aligned} 2^{n-1}u_n &= \frac{\displaystyle\sum_{k=0}^{n}\binom{n}{k}a^{n-k}(\sqrt{\triangle})^k - \sum_{k=0}^{n}\binom{n}{k}a^{n-k}(-\sqrt{\triangle})^k}{2\sqrt{\triangle}} \\ &= \frac{2\binom{n}{1}a^{n-1}\sqrt{\triangle} + 2\binom{n}{3}a^{n-3}(\sqrt{\triangle})^3 + \cdots + 2\binom{n}{n-2}a^2(\sqrt{\triangle})^{n-2} + 2(\sqrt{\triangle})^n}{2\sqrt{\triangle}}, \end{aligned}$$

de donde,

$$2^{n-1}u_n = \binom{n}{1}a^{n-1} + \binom{n}{3}a^{n-3}\triangle + \binom{n}{5}a^{n-5}\triangle^2 + \cdots + \binom{n}{n-2}a^2\triangle^{(n-3)/2} + \triangle^{(n-1)/2}.$$

En consecuencia

$$2^{n-1}u_n = \sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k+1} a^{n-(2k+1)}\triangle^k.$$

■

Lema 2.7 *Para n impar se tiene que*

$$2^{n-1}w_n = \sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k} a^{n-2k}\triangle^k.$$

Demostración.

$$\begin{aligned} 2^{n-1}w_n &= \frac{2^n}{2}(\alpha^n + \beta^n) = \frac{(2\alpha)^n + (2\beta)^n}{2} \\ &= \frac{(\alpha+\beta+\alpha-\beta)^n + (\alpha+\beta-\alpha+\beta)^n}{2} \\ &= \frac{(a+\sqrt{\triangle})^n + (a-\sqrt{\triangle})^n}{2}. \end{aligned}$$

Utilizando el Teorema del Binomio se tiene,

$$\begin{aligned} 2^{n-1}w_n &= \frac{\sum_{k=0}^{n}\binom{n}{k}a^{n-k}(\sqrt{\triangle})^k + \sum_{k=0}^{n}\binom{n}{k}a^{n-k}(-\sqrt{\triangle})^k}{2} \\ &= \frac{2\binom{n}{0}a^n + 2\binom{n}{2}a^{n-2}\sqrt{\triangle}^2 + 2\binom{n}{4}a^{n-4}\sqrt{\triangle}^4}{2} + \cdots, \end{aligned}$$

y en consecuencia,

$$2^{n-1}w_n = a^n + \binom{n}{2}a^{n-2}\triangle + \binom{n}{4}a^{n-4}\triangle^2 + \cdots + \binom{n}{n-1}a\triangle^{(n-1)/2}.$$

Esto es

$$2^{n-1}w_n = \sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k} a^{n-2k}\triangle^k.$$

■

2.2. Propiedades de divisibilidad de sucesiones de Lucas

Las sucesiones de Lucas no degeneradas poseen propiedades de divisibilidad de gran relevancia que es necesario destacar. Éstas propiedades resultan fundamentales para el desarrollo del próximo capitulo y se describen mediante los siguientes lemas.

Lema 2.8 *Sea p un primo tal que $p \mid b$. Entonces $p \nmid u_n$ para todo $n > 0$.*

Demostración. Suponga que $p \mid b$ y que $p \mid u_n$ para algún $n > 0$, y sea n el mínimo con esta propiedad. Como $u_1 = 1$, es claro que $n \geq 2$. Dado que $u_n = au_{n-1} + bu_{n-2}$ y $p \mid b$, se deduce que $p \mid au_{n-1}$. Como $p \mid b$ y $(a, b) = 1$ se deduce que $p \nmid a$. En consecuencia $p \mid u_{n-1}$, contradiciendo que n es el mínimo con esta condición. ■

Lema 2.9 *Sea p un primo tal que $p \mid b$. Entonces $p \nmid w_n$ para todo $n > 0$.*

La demostración del Lema anterior es similar a la demostración del Lema 2.8.

Ejemplo 2.10 *Considere la sucesión de Jacobsthal y Jacobsthal-Lucas correspondiente al par $(a, b) = (1, 2)$.*

$$(u_n)_{n\geq 0} = \{0, 1, 1, 3, 5, 11, 21, 43, 85, 171, 341, \ldots\}.$$

$$(w_n)_{n\geq 0} = \{2, 1, 5, 7, 17, 31, 65, 127, 257, 511, 1025, \ldots\}.$$

El primo $p = 2$ no divide a ningún número de Jacobsthal ya que $p \mid b$, y entonces todo número de Jacobsthal es impar y todo número de Jacobsthal-Lucas es impar para $n > 0$.

A continuación se presenta una "fórmula de multiplicación".

Lema 2.11 *Para todos los enteros positivos k y n se tiene que $u_{kn} = \bar{u}_k u_n$, donde $(\bar{u}_m)_{m\geq 0}$ es la sucesión de Lucas con polinomio característico $\bar{p}(X) = X^2 - w_n X + (-b)^n$. Además, $(\bar{u}_m)_{m\geq 0}$ es no degenerada, y el discriminante es $\bar{\triangle} = u_n^2 \triangle$.*

Demostración. Teniendo en cuenta (2.1) y aplicando la fórmula cuadrática al polinomio $\bar{p}(X) = X^2 - w_n X + (-b)^n$, se observa que sus ceros son:

$$\bar{\alpha} = \frac{w_n + \sqrt{w_n^2 - 4(-b)^n}}{2} = \frac{\alpha^n + \beta^n + \sqrt{(\alpha^n + \beta^n)^2 - 4(\alpha\beta)^n}}{2}$$
$$= \frac{\alpha^n + \beta^n + \sqrt{(\alpha^n - \beta^n)^2}}{2} = \alpha^n,$$

y

$$\bar{\beta} = \frac{w_n - \sqrt{w_n^2 - 4(-b)^n}}{2} = \frac{\alpha^n + \beta^n - \sqrt{(\alpha^n + \beta^n)^2 - 4(\alpha\beta)^n}}{2}$$
$$= \frac{\alpha^n + \beta^n - \sqrt{(\alpha^n - \beta^n)^2}}{2} = \beta^n.$$

Suponga por contradicción que $(\bar{u}_m)_{m\geq 0}$ es una sucesión degenerada. Esto implica que el cociente de sus raíces $\bar{\alpha}/\bar{\beta}$ es una raíz de la unidad, lo que a su vez significa que existe $k \in \mathbb{Z}^+$ tal que $(\bar{\alpha}/\bar{\beta})^k = 1$. Esto es

$$\left(\frac{\bar{\alpha}}{\bar{\beta}}\right)^k = \frac{\bar{\alpha}^k}{\bar{\beta}^k} = \frac{(\alpha^n)^k}{(\beta^n)^k} = \left(\frac{\alpha}{\beta}\right)^s = 1 \quad \text{donde} \quad s = nk \in \mathbb{Z},$$

lo cual contradice la hipótesis de que $(u_n)_{n\geq 0}$ es no degenerada. En consecuencia $(\bar{u}_m)_{m\geq 0}$ también es no degenerada.

De esto último se tiene de acuerdo al Lema 2.4 que $\bar{\alpha} \neq \bar{\beta}$ y $\bar{\triangle} \neq 0$. Luego, de (2.1) se obtiene

$$\bar{\triangle} = (\bar{\alpha} - \bar{\beta})^2 = (\alpha^n - \beta^n)^2 = \left(\frac{\alpha^n - \beta^n}{\alpha - \beta} \cdot (\alpha - \beta)\right)^2 = u_n^2 \triangle.$$

Finalmente se calcula u_{kn} usando (2.1) como sigue:

$$u_{kn} = \frac{\alpha^{kn} - \beta^{kn}}{\alpha - \beta} = \frac{\bar{\alpha}^k - \bar{\beta}^k}{\alpha - \beta} = \frac{\bar{\alpha}^k - \bar{\beta}^k}{\alpha - \beta} \cdot \frac{\alpha^n - \beta^n}{\bar{\alpha} - \bar{\beta}} = \frac{\bar{\alpha}^k - \bar{\beta}^k}{\bar{\alpha} - \bar{\beta}} \cdot \frac{\alpha^n - \beta^n}{\alpha - \beta} = \bar{u}_k u_n.$$

■

Lema 2.12 *Sea p un primo impar. Entonces*

$$u_p \equiv \left(\frac{\triangle}{p}\right) \pmod{p},$$

Demostración. Para $p > 2$ se sabe por el pequeño Teorema de Fermat que $p \nmid 2^{p-1}$. Por otro lado, del Lema 2.6 se obtiene:

$$2^{p-1} u_p = \sum_{k=0}^{\frac{p-1}{2}} \binom{p}{2k+1} a^{p-(2k+1)} \triangle^k$$
$$= pa^{p-1} + \binom{p}{3} a^{p-3} \triangle + \cdots + \binom{p}{p-2} a^2 \triangle^{(p-3)/2} + \triangle^{(p-1)/2}.$$

- Si $p \mid \triangle$, entonces el lado derecho de la expresión anterior es múltiplo de p. Así, $p \mid 2^{p-1}u_p$ de donde se deduce que $p \mid u_p$. Por lo tanto

$$u_p \equiv 0 \pmod{p} \equiv \left(\frac{\triangle}{p}\right) \pmod{p}.$$

- Suponga ahora que $p \nmid \triangle$. Teniendo en cuenta la propiedad (7) del orden p-ádico Sección 1.5, se tiene que $p \mid \binom{p}{n}$ para $1 \leq n < p$. Entonces del Teorema del Binomio

$$\alpha^p = \left(\frac{a+\sqrt{\triangle}}{2}\right)^p = \frac{1}{2^p}\left(a^p + \sum_{k=1}^{p}\binom{p}{k}a^{p-k}\triangle^{k/2}\right),$$

de donde,

$$2^p\alpha^p \equiv a^p + \triangle^{p/2} \equiv a^p + \triangle^{(p-1)/2}\sqrt{\triangle} \pmod{p}.$$

Similarmente,

$$\beta^p = \left(\frac{a-\sqrt{\triangle}}{2}\right)^p = \frac{1}{2^p}\left(a^p + \sum_{k=1}^{p}\binom{p}{k}a^{p-k}(-1)^k\triangle^{k/2}\right),$$

y así,

$$2^p\beta^p \equiv a^p - \triangle^{p/2} \equiv a^p - \triangle^{(p-1)/2}\sqrt{\triangle} \pmod{p}.$$

Restando las expresiones anteriores se obtiene,

$$2^p\alpha^p - 2^p\beta^p \equiv 2\sqrt{\triangle}\cdot\triangle^{(p-1)/2} \pmod{p},$$

y entonces

$$2^p\left(\frac{\alpha^p-\beta^p}{\sqrt{\triangle}}\right) \equiv 2\triangle^{(p-1)/2} \pmod{p}.$$

De (2.1) se llega a que

$$2^p u_p \equiv 2\triangle^{(p-1)/2} \pmod{p},$$

y en consecuencia

$$u_p \equiv \triangle^{(p-1)/2} \pmod{p}.$$

Ahora, por el Criterio de Euler (Teorema 1.20) se tiene,

$$\triangle^{(p-1)/2} \equiv \left(\frac{\triangle}{p}\right) \pmod{p}.$$

Por lo anterior se deduce que

$$u_p \equiv \left(\frac{\triangle}{p}\right) \pmod{p}.$$

■

Teorema 2.13 *Para un primo impar p y una sucesión de Lucas $(u_n)_{n\geq 0}$ siempre ocurre una de las siguientes opciones.*

(1) *Si $p \nmid b$ y $p \mid \triangle$, entonces $p \mid u_p$.*

(2) *Si $p \nmid \triangle ba$ y $(\triangle|p) = 1$, se concluye que $p \mid u_{p-1}$.*

(3) *Si $p \nmid \triangle ba$ y $(\triangle|p) = -1$, se garantiza que $p \mid u_{p+1}$.*

Demostración. La demostración se divide en los siguientes casos:

Caso 1. La prueba del primer item se tiene como consecuencia inmediata del Lema 2.12, pues bajo la hipótesis $p \mid \triangle$, el símbolo de Legendre $(\triangle|p) = 0$. Luego $u_p \equiv 0 \pmod{p}$, lo que implica que $p \mid u_p$.

Caso 2. Para la demostración de los ítems (2) y (3) bajo las hipótesis $p \nmid \triangle$, $p \nmid b$, $p \nmid a$ y $p > 2$, note que,

$$\alpha^p = \left(\frac{a+\sqrt{\triangle}}{2}\right)^p = \frac{1}{2^p}\left(a^p + \sum_{k=1}^{p}\binom{p}{k}a^{p-k}\triangle^{k/2}\right).$$

Teniendo en cuenta la Proposición 1.28 item (6) del orden p-ádico, se observa que $p \mid \binom{p}{n}$ para $1 \leq n < p$, de donde $2^p\alpha^p \equiv a^p + \triangle^{(p-1)/2}\sqrt{\triangle} \pmod{p}$.

- Si $(\triangle|p) = 1$, entonces por el Criterio de Euler, Teorema 1.20, se tiene la congruencia $\triangle^{(p-1)/2} \equiv 1 \pmod{p}$, así $2^p\alpha^p \equiv 2\alpha \pmod{p}$. Además, $2^p \equiv 2 \pmod{p}$, de donde se garantiza que $\alpha^p \equiv \alpha \pmod{p}$. En consecuencia

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

  Las mismas congruencias se obtienen para β, esto es,

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

Restando las expresiones anteriores se sigue que,

$$(\alpha-\beta)(u_p-1)\equiv 0 \pmod{p} \quad \text{y} \quad (\alpha-\beta)(u_{p+1}-u_2)\equiv 0 \pmod{p}.$$

En particular, $p \mid \triangle(u_p-1)$, $p \mid \triangle(u_{p+1}-u_2)$ y $p \nmid \triangle$. De donde se concluye que $u_{p+1}\equiv u_2$ y $u_p \equiv 1 \pmod{p}$.

La definición de sucesión de Lucas garantiza la congruencia $u_{p+1}\equiv au_p+bu_{p-1} \pmod{p}$. De lo anterior se sigue que $u_2 \equiv a+bu_{p-1} \pmod{p}$. Como $u_2=a$, entonces $p \mid bu_{p-1}$, y como $p \nmid b$ se obtiene finalmente que $p \mid u_{p-1}$.

- Suponga ahora que $(\triangle|p)=-1$. Aquí se tiene que $2^p\alpha^p \equiv a-\sqrt{\triangle} \pmod{p} \equiv 2\beta \pmod{p}$. De donde $\alpha^p \equiv \beta \pmod{p}$ y por tanto $\alpha^{p+1} \equiv \alpha\beta \pmod{p} \equiv -b \pmod{p}$. El mismo argumento prueba que $\beta^{p+1} \equiv -b \pmod{p}$, y restándolas se obtiene $\alpha^{p+1}-\beta^{p+1} \equiv 0 \pmod{p}$. Por lo tanto $p \mid \triangle u_{p+1}$, y como $p \nmid \triangle$, se concluye que $p \mid u_{p+1}$.

■

Observación 2.14 *La anterior demostración no toma en cuenta el caso $p=2$, ya que fácilmente se observa que si $2 \nmid u_2=a$, entonces $2 \mid u_3=a^2+b$.*

Proposición 2.15 *Para todos los enteros positivos m y n se tiene que*

$$\operatorname{mcd}(u_m,u_n)=u_{\operatorname{mcd}(m,n)}.$$

Demostración. Si $m \mid n$, escribiendo $n=m\ell$, se tiene que

$$\frac{u_n}{u_m}=\frac{\alpha^n-\beta^n}{\alpha^m-\beta^m}=\frac{(\alpha^m)^\ell-(\beta^m)^\ell}{\alpha^m-\beta^m}=(\alpha^m)^{\ell-1}+(\alpha^m)^{\ell-2}\beta^m+\cdots+(\beta^m)^{\ell-1}.$$

El miembro derecho de la fórmula anterior es un entero algebraico por ser un polinomio con coeficientes enteros en α y β que son enteros algebraicos, esto se garantiza por la Proposición 1.9 (7) ya que $\bar{\mathbb{Z}}$ es integralmente cerrado. Por otra parte el miembro izquierdo es racional, y nuevamente por la Proposición 1.9 (2) se sabe que u_n/u_m es un entero, lo que implica que $u_n \mid u_m$. Se concluye que si $m \mid n$, entonces $u_m \mid u_n$. Por lo tanto, dados enteros m y n con $d=\operatorname{mcd}(m,n)$, se deduce que $u_d \mid u_n$ y $u_d \mid u_m$, y en consecuencia $u_d \mid \operatorname{mcd}(u_m,u_n)$.

Recíprocamente, suponga primero que m y n son primos relativos. Por inducción sobre máx $\{m, n\}$ se prueba que existen 2 polinomios $P(X)$ y $Q(X)$ con coeficientes enteros tales que

$$\frac{X^m-1}{X-1}P(X)+\frac{X^n-1}{X-1}Q(X)=1.$$

Si $m=n=1$ se toma $P(X)=1$ y $Q(X)=0$. Si $m>n\geq 1$ escribiendo $m=nq+r$ con $0<r<n$ se tiene

$$\frac{X^m-1}{X-1}-\frac{X^n-1}{X-1}\left(\frac{X^{nq}-1}{X^n-1}\right)X^r=\frac{X^r-1}{X-1}. \tag{2.4}$$

Por lo tanto, si se supone por inducción que $P_1(X)$, $Q_1(X)\in\mathbb{Z}[X]$ son tales que

$$\frac{X^n-1}{X-1}P_1(X)+\frac{X^r-1}{X-1}Q_1(X)=1,$$

entonces

$$\begin{aligned}1=&\frac{X^n-1}{X-1}P_1(X)+\left(\frac{X^m-1}{X-1}-\frac{X^n-1}{X-1}\left(\frac{X^{nq}-1}{X^n-1}\right)X^r\right)Q_1(X)\\ =&\frac{X^m-1}{X-1}P(X)+\frac{X^n-1}{X-1}Q(X),\end{aligned}$$

con $P(X)=Q_1(X)$ y $Q(X)=P_1(X)-((X^{nq}-1)/(X^n-1))X^rQ_1(X)$, lo que prueba la existencia de la fórmula (2.4) para el par (m,n). Tomando ahora enteros positivos arbitrarios m, n, escribiendo $m=dm_1$, $n=dn_1$ con $d=\text{mcd}\,(m,n)$ y

$$\frac{X^{m_1}-1}{X-1}P(X)+\frac{X^{n_1}-1}{X-1}Q(X)=1,$$

al cambiar X por X^d se obtiene,

$$\frac{X^m-1}{X-1}P(X^d)+\frac{X^n-1}{X-1}Q(X^d)=\frac{X^d-1}{X-1}.$$

Homogeneizando[1], se tiene

$$\frac{X^m-Y^m}{X-Y}R(X,Y)+\frac{X^n-Y^n}{X-Y}S(X,Y)=\frac{X^d-Y^d}{X-Y},$$

donde $R(X,Y)$ y $S(X,Y)\in\mathbb{Z}[X,Y]$ son las homogeneizaciones de $P(X^d)$ y $Q(X^d)$ respectivamente. Recuerde que si

[1]La homogeneización de funciones es un proceso mediante el cual se ajusta una función para que satisfaga una propiedad de homogeneidad.

$$f(X) = c_0X^k + c_1X^{k-1} + \cdots + c_k,$$

entonces su homogeneización es $f(X,Y) = c_0X^k + c_1X^{k-1}Y + \cdots + c_kY^k$. Sustituyendo $(X,Y) = (\alpha,\beta)$ se tiene

$$u_mR(\alpha,\beta) + u_nS(\alpha,\beta) = u_d.$$

Por lo tanto

$$\frac{u_d}{\text{mcd}\,(u_m,u_n)} = \frac{u_m}{\text{mcd}\,(u_m,u_n)}R(\alpha,\beta) + \frac{u_n}{\text{mcd}\,(u_m,u_n)}S(\alpha,\beta)$$

En esta expresión, el lado izquierdo es un número racional y el lado derecho es un entero algebraico. Así, $\text{mcd}\,(u_m,u_n) \mid u_d$. ■

2.3. Rango de aparición

Del Lema 2.8 se sabe que si $p \mid b$, entonces $p \nmid u_k$ para todo $k \geq 1$. Por el contrario, si $p \nmid b$, entonces por el Teorema 2.13 se sigue que p divide u_p ó a u_{p-1} o a u_{p+1}, por lo que tiene sentido la siguiente definición.

Definición 2.16 *Sea p un número primo tal que $p \nmid b$. El* **rango de aparición** *de p, denotado por $\tau(p)$, se define como el entero positivo más pequeño k tal que $p \mid u_k$. Esto es*

$$\tau(p) := \text{mín}\{k \geq 1 : p \mid u_k\}.$$

El rango de aparición posee propiedades significativas que merece la pena resaltar y son las siguientes.

El siguiente Lema es referenciado por el Doctor Carlo Sanna en su artículo *the p-adic valuation of Lucas sequences* [9].

Lema 2.17 *Sea p un número primo tal que $p \nmid b$. Entonces para cada entero positivo n se cumple que*

$$p \mid u_n \quad \textit{si, y sólo si,} \quad \tau(p) \mid n.$$

Demostración. Sea p tal que $p \mid u_n$. Como $p \mid u_{\tau(p)}$, entonces $p \mid \operatorname{mcd}\left(u_n, u_{\tau(p)}\right)$. Pero por la Proposición 2.15 se tiene que $\operatorname{mcd}\left(u_n, u_{\tau(p)}\right) = u_{\operatorname{mcd}(n,\tau(p))}$ y en consecuencia $p \mid u_{\operatorname{mcd}(n,\tau(p))}$. Luego, por definición de $\tau(p)$, se sigue que $\operatorname{mcd}(n, \tau(p)) = \tau(p)$, de donde $\tau(p) \mid n$.

Recíprocamente, si $\tau(p) \mid n$, entonces se tiene que $u_{\tau(p)} \mid u_n$. Como $p \mid u_{\tau(p)}$ se concluye que $p \mid u_n$. ■

Lema 2.18 *Sea p un número primo tal que $p \nmid b$. Entonces $\tau(p) = p$ si, y sólo si, $p \mid \tau(p)$ si, y sólo si, $p \mid \triangle$.*

Demostrar el lema anterior es equivalente a demostrar las siguientes equivalencias:

(1) $\tau(p) = p$ si, y sólo si, $p \mid \tau(p)$.

(2) $p \mid \tau(p)$ si, y sólo si, $p \mid \triangle$.

Demostración.

(1) Suponga que $\tau(p) = p$. Este caso es trivial pues $p \mid p$. Recíprocamente al suponer que $p \mid \tau(p)$ se tiene que $p \leq \tau(p)$, quedando como única opción $\tau(p) = p$ según el Teorema 2.13.

(2) Suponga que $p \mid \tau(p)$. Del item anterior se tiene que $p = \tau(p)$ y así $p \mid u_p$. Por el Lema 2.6 se garantiza que

$$\begin{aligned} 2^{p-1}u_p &= \sum_{k=0}^{\frac{p-1}{2}} \binom{p}{2k+1} a^{p-(2k+1)} \triangle^k \\ &= \binom{p}{1} a^{p-1} + \binom{p}{3} a^{p-3}\triangle + \binom{p}{5} a^{p-5}\triangle^2 + \cdots + \binom{p}{p-2} a^2 \triangle^{(p-3)/2} + \triangle^{(p-1)/2}. \end{aligned}$$

Por la Proposición 1.28 (6) se sabe que $p \mid \binom{p}{s}$ para todo $1 \leq s < p$, de donde $p \mid \triangle^{(p-1)/2}$. De ahí se concluye que $p \mid \triangle$.

Recíprocamente, al suponer que $p \mid \triangle$ se obtiene del Teorema 2.13 que $p \mid u_p$. Luego por el Lema 2.17 se garantiza que $\tau(p) \mid p$, y por tanto $\tau(p) = p$, pues p es un primo y $p \nmid u_1 = 1$.

■

Ejemplo 2.19 *Considere las sucesiones de Fibonacci* $u(1,1)$*, la sucesión de Pell* $u(2,1)$ *y los primos* $p = 2, 3, 5$*. Para la sucesión de Fibonacci se tiene que* $\tau(2) = 3$*,* $\tau(3) = 4$ *y* $\tau(5) = 5$*; mientras que para la sucesión de Pell se tiene que* $\tau(2) = 2$*,* $\tau(3) = 4$ *y* $\tau(5) = 3$*.*

Tabla 2.5: Primeros términos de las sucesiones de Fibonacci y de Pell.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13
F_n	0	1	1	2	3	5	8	13	21	34	55	89	144	233
P_n	0	1	2	5	12	29	70	169	408	985	2378	5741	13860	33461

Finalmente se puede ver que para la sucesión de Fibonacci se tiene que $2 \mid F_n$ *para* $n = 3k$*;* $3 \mid F_n$ *para* $n = 4k$*;* $5 \mid F_n$ *para* $n = 5k$*,* $k \in \mathbb{N}$*. De igual forma para la sucesión de Pell se tiene que* $2 \mid P_n$ *para* $n = 2k$*;* $3 \mid P_n$ *para* $n = 4k$*;* $5 \mid P_n$ *para* $n = 3k$*,* $k \in \mathbb{N}$*.*

Capítulo 3

Orden p-ádico de sucesiones de Lucas de primera categoría

El orden p-ádico de algunas sucesiones especiales de Lucas había sido estudiado previamente por muchos autores. Lengyel [3] por ejemplo consideró la sucesión de números de Fibonacci $(F_n)_{n\geq 0}$ y probó lo siguiente.

Teorema 3.1 *Para todo entero positivo n y todo número primo $p \neq 2, 5$ se tiene,*

$$v_2(F_n) = \begin{cases} 0, & si \quad n \equiv 1, 2 \pmod 3; \\ 1, & si \quad n \equiv 3 \pmod 6; \\ 3, & si \quad n \equiv 6 \pmod{12}; \\ v_2(n) + 2, & si \quad n \equiv 0 \pmod{12}. \end{cases}$$

$$v_5(F_n) = v_5(n);$$

$$v_p(F_n) = \begin{cases} v_p(n) + v_p(F_{\tau(p)}), & si \quad n \equiv 0 \pmod{\tau(p)}; \\ 0, & si \quad n \not\equiv 0 \pmod{\tau(p)}. \end{cases}$$

3.1. Propiedades

En este capítulo se van a derivar algunas propiedades básicas de $v_p(u_n)$ para demostrar la formula hallada por el Doctor Carlo Sanna en su artículo "*The p-adic valuation of Lucas sequences*" [9]

publicado en 2016. En su trabajo, el autor presenta fórmulas simples para encontrar el orden p-ádico o la valuación p-ádica de términos de sucesiones de Lucas no degeneradas $(u_n)_{n\geq 0}$ en términos de $v_p(n)$ y el rango de aparición de p en $(u_n)_{n\geq 0}$. Se justifica afirmar por Teorema 2.5 que para estudiar $v_p(u_n)$ no hay pérdida de generalidad al suponer que $(u_n)_{n\geq 0}$ es no degenerada. Las sucesiones de Lucas degeneradas corresponden a casos triviales y por tanto carecen de interés.

A continuación consideramos α y β las raíces del polinomio característico de dicha sucesión. Tales propiedades serán usadas posteriormente para probar el teorema principal.

Lema 3.2 *Si α y β son enteros y p es un primo impar tal que $p \nmid b$ y $p \mid \triangle$, entonces $v_p(u_n) = v_p(n)$ para cada entero positivo n.*

Demostración. Primero note que $\alpha \neq \beta$ ya que suponemos que $(u_n)_{n\geq 0}$ es no degenerada. Luego, de 2.1 y del hecho que $v_p(x/y) = v_p(x) - v_p(y)$ se tiene que,

$$v_p(u_n) = v_p\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right) = v_p(\alpha^n - \beta^n) - v_p(\alpha - \beta).$$

Ahora, utilizando el lema de elevación del exponente Lema 1.29 con $c = \alpha$ y $d = \beta$, se observa que

$$v_p(u_n) = v_p(n) + v_p(\alpha - \beta) - v_p(\alpha - \beta) = v_p(n),$$

ya que $p \nmid \alpha\beta = -b$ y $p \mid \alpha - \beta = \sqrt{\triangle}$. ■

Lema 3.3 *Si $p \geq 5$ es un número primo tal que $p \nmid b$ y $p \mid \triangle$, entonces $v_p(u_p) = 1$.*

Demostración. Del Lema 2.6 se tiene,

$$\begin{aligned} 2^{p-1}u_p &= \sum_{k=0}^{\frac{p-1}{2}} \binom{p}{2k+1} a^{p-(2k+1)} \triangle^k \\ &= pa^{p-1} + \binom{p}{3} a^{p-3}\triangle + \binom{p}{5} a^{p-5}\triangle^2 + \cdots + \binom{p}{p-2} a^2 \triangle^{(p-3)/2} + \triangle^{(p-1)/2}. \end{aligned}$$

Observe que $p^2 \mid \triangle^m$ para $m \geq 2$. Además, como $p \mid \binom{p}{3}$ para $p \geq 5$, se tiene que $p^2 \mid \binom{p}{3} a^{p-3}\triangle$. Por lo anterior se garantiza que

$$2^{p-1}u_p \equiv pa^{p-1} \pmod{p^2}.$$

Así, dado que $p \mid \triangle = a^2 + 4b$, $p \nmid b$ y $p \geq 5$ se deduce que $p \nmid a$, de donde

$$v_p(2^{p-1}u_p) = v_p(a^{p-1}p).$$

Esto es

$$v_p(2^{p-1}) + v_p(u_p) = v_p(a^{p-1}) + v_p(p),$$

y en consecuencia

$$v_p(u_p) = v_p(p) = 1.$$

■

Lema 3.4 *Si p es un número primo tal que $p \nmid b$, entonces*

$$v_p(u_{p\tau(p)}) \geq v_p(u_{\tau(p)}) + 1,$$

con igualdad si $p \geq 5$, $p = 3$ y $3 \nmid \triangle$.

Demostración. Del Lema 2.11 se sigue que $u_{p\tau(p)} = \bar{u}_p u_{\tau(p)}$, donde $(\bar{u}_n)_{n\geq 0}$ es la sucesión de Lucas no degenerada con polinomio característico $\bar{p}(X) = X^2 - w_{\tau(p)}X + (-b)^{\tau(p)}$. Luego,

$$v_p(u_{p\tau(p)}) = v_p(\bar{u}_p u_{\tau(p)}) = v_p(\bar{u}_p) + v_p(u_{\tau(p)}). \tag{3.1}$$

Como $p \mid u_{\tau(p)}$ y $\bar{\triangle} = u_{\tau(p)}^2 \triangle$, por el Lema 2.11 se sigue que $p \mid \bar{\triangle}$. Así del Lema 2.12 se tiene que

$$\bar{u}_p \equiv (\bar{\triangle}/p) \equiv 0 \pmod{p}. \tag{3.2}$$

Es decir $p \mid \bar{u}_p$. Por tanto de (3.2) se tiene que $v_p(u_{p\tau(p)}) \geq 1 + v_p(u_{\tau(p)})$. Para el resto, note del Lema 3.3 que si $p \geq 5$, entonces $v_p(\bar{u}_p) = 1$. Así se tiene que

$$v_p(u_{p\tau(p)}) = 1 + v_p(u_{\tau(p)}).$$

Ahora considere el caso $p = 3$ y $3 \nmid \triangle$. En la prueba del Lema 2.11 vimos que $\bar{\alpha} = \alpha^n$y $\bar{\beta} = \beta^n$. Por lo tanto $\bar{\alpha} = \alpha^{\tau(3)}$ y $\bar{\beta} = \beta^{\tau(3)}$. Así que de (2.1) y el hecho que $\alpha\beta = -b$ se obtiene que

$$\begin{aligned} \bar{u}_3 = \frac{\bar{\alpha}^3 - \bar{\beta}^3}{\bar{\alpha} - \bar{\beta}} &= \bar{\alpha}^2 + \bar{\alpha}\bar{\beta} + \bar{\beta}^2 = \alpha^{2\tau(3)} + \alpha^{\tau(3)}\beta^{\tau(3)} + \beta^{2\tau(3)} \\ &= \alpha^{2\tau(3)} + 2(\alpha\beta)^{\tau(3)} + \beta^{2\tau(3)} - (\alpha\beta)^{\tau(3)} = (\alpha^{\tau(3)} + \beta^{\tau(3)})^2 - (\alpha\beta)^{\tau(3)} \\ &= w_{\tau(3)}^2 - (-b)^{\tau(3)}. \end{aligned} \tag{3.3}$$

- Por una parte, si $3 \mid a$, entonces $\tau(3) = 2$ pues $u_0 = 0, u_1 = 1$ y entonces $u_2 = a$. Luego, usando que $\alpha + \beta = a$ y $\alpha\beta = -b$ se sigue para $\bar{u}_3$ que,

$$\begin{aligned}\bar{u}_3 &= w_2^2 - (-b)^2 = (\alpha^2 + \beta^2)^2 - b^2 = (\alpha^2 + 2\alpha\beta + \beta^2 - 2\alpha\beta)^2 - b^2 \\ &= ((\alpha + \beta)^2 - 2\alpha\beta)^2 - b^2 = (a^2 + 2b)^2 - b^2 = a^4 + 4a^2b + 4b^2 - b^2 \\ &= a^4 + 4a^2b + 3b^2 = (a^2 + b)(a^2 + 3b).\end{aligned}$$

  Como $3 \nmid b$ por hipótesis, se tiene que $3 \nmid (a^2 + b)$ y $3||(a^2 + 3b)$, de donde se concluye que $v_3(\bar{u}_3) = 1$. Así que de 3.1 se tiene que $v_3(u_{3\tau(3)}) = 1 + v_3(u_{\tau(3)})$.

- Por otra parte, si $3 \nmid a$, entonces $a^2 \equiv 1 \pmod 3$. De lo anterior y teniendo en cuenta que $\triangle = a^2 + 4b \not\equiv 0 \pmod 3$ y $3 \nmid b$, se sigue que $b \equiv 1 \pmod 3$. En consecuencia $a^2 + b \equiv 2 \pmod 3$ y $a^2 + 2b \equiv 0 \pmod 3$. Como $u_0 = 0, u_1 = 1$, $u_2 = a$, $u_3 = au_2 + bu_1 = a^2 + b$, $u_4 = au_3 + bu_2 = a^3 + 2ab = a(a^2 + 2b)$ se concluye que $\tau(3) = 4$.

  Entonces, de 3.3 y los hechos que $\alpha\beta = -b$ y $\alpha + \beta = a$ se sigue que

$$\begin{aligned}\bar{u}_3 &= w_4^2 - (-b)^4 = (\alpha^4 + \beta^4)^2 - b^4 = ((\alpha^2 + \beta^2)^2 - 2\alpha^2\beta^2)^2 - b^4 \\ &= ((\alpha + \beta)^2 - 2\alpha\beta)^2 - 2\alpha^2\beta^2)^2 - b^4 = ((a^2 + 2b)^2 - 2b^2)^2 - b^4 \\ &= (a^4 + 4a^2b + 4b^2 - 2b^2)^2 - b^4 = (a^4 + 4a^2b + 2b^2)^2 - b^4.\end{aligned}$$

  Esto es,

$$\begin{aligned}\bar{u}_3 &= a^8 + 4a^6b + 2a^4b^2 + 4a^6b + 16a^4b^2 + 8a^2b^3 + 2a^4b^2 + 8a^2b^3 + 4b^4 - b^4 \\ &= a^8 + 8a^6b + 20a^4b^2 + 16a^2b^3 + 3b^4 = (a^4 + 4a^2b + 3b^2)(a^4 + 4a^2b + b^2) \\ &= (a^2 + b)(a^2 + 3b)(a^4 + 4a^2b + b^2).\end{aligned}$$

  Nuevamente $v_3(\bar{u}_3) = 1$, ya que,

$$3 \nmid (a^2 + b)(a^2 + 3b) \text{ y } 3||(a^4 + 4a^2b + b^2) = (a^2 + 2b)^2 - 3b^2.$$

Así que se tiene la igualdad deseada de (3.1) para $p = 3$. ■

Finalizamos los resultados preliminares con el siguiente resultado que concierne a la valuación p-ádica de sucesiones lineales enteras recurrentes en general.

Lema 3.5 *Sea $(\gamma_n)_{n\geq 0}$ una sucesión lineal recurrente de orden $k \geq 2$ dada por*

$$\gamma_n = a_1\gamma_{n-1} + \cdots + a_k\gamma_{n-k} \quad \textit{para cada entero} \quad n \geq k, \tag{3.4}$$

donde $\gamma_0, \gamma_1, \ldots, \gamma_{k-1}$ *y* $a_1, a_2, \ldots, a_k$ *son enteros. Suponga que existe un número primo* p *tal que* $p \nmid a_k$ *y*

$$\min\{v_p(a_j) : 1 \leq j < k\} > \max\{v_p(\gamma_m) - v_p(\gamma_n) : 0 \leq m, n < k\}. \tag{3.5}$$

Entonces $v_p(\gamma_n) = v_p(\gamma_{n \pmod k})$ *para cada entero* $n \geq 0$.

Demostración. Se procede por inducción sobre n. Para $n = 0, 1, \ldots, k-1$ la afirmación es verdadera ya que $n \equiv n \pmod k$. Así asumimos que $n \geq k$ y que la afirmación es válida para todos los enteros no negativos menores que n. Por (3.5) y por hipótesis inductiva, para cada $j = 1, 2, \ldots, k-1$ se tiene

$$\begin{aligned} v_p(a_j\gamma_{n-j}) &= v_p(a_j) + v_p(\gamma_{n-j}) = v_p(a_j) + v_p(\gamma_{n-j \pmod k}) \\ &> v_p(\gamma_{n-k \pmod k}) - v_p(\gamma_{n-j \pmod k}) + v_p(\gamma_{n-j \pmod k}) \\ &= v_p(\gamma_{n-k \pmod k}) = v_p(\gamma_{n-k}) = v_p(a_k\gamma_{n-k}). \end{aligned}$$

Por lo tanto de (3.4) y la hipótesis de inducción se sigue que

$$\begin{aligned} v_p(\gamma_n) &= v_p(a_1\gamma_{n-1} + \cdots + a_k\gamma_{n-k}) = v_p(a_k\gamma_{n-k}) \\ &= v_p(a_k\gamma_{n-k \pmod k}) \\ &= v_p(\gamma_{n \pmod k}), \end{aligned} \tag{3.6}$$

lo que termina la prueba. ■

3.2. Lemas clave para la prueba del Teorema principal

Con todo lo que se ha visto hasta el momento ya se puede iniciar una breve introducción al teorema principal, el cual está substancialmente dividido en 4 lemas que se presentan a continuación:

Lema 3.6 *Si* p *es un número primo tal que* $p \nmid b$ *y* $p \mid \triangle$, *entonces*

$$v_p(u_{pn}) = v_p(u_n) + \begin{cases} 1 & si \quad p \mid n, \\ v_p(u_p) & si \quad p \nmid n, \end{cases}$$

para cada entero positivo n.

Demostración. Del Lema 2.11 se obtiene que $u_{pn} = \bar{u}_p u_n$, donde $(\bar{u}_m)_{m\geq 0}$ es la sucesión de Lucas con polinomio característico $\bar{p}(X) = X^2 - w_n X + (-b)^n$. Luego

$$v_p(u_{pn}) = v_p(u_n) + v_p(\bar{u}_p).$$

De acuerdo a lo que se quiere probar ahora se necesita calcular $v_p(\bar{u}_p)$. Note que $\bar{u}_p = (\bar{\alpha}^p - \bar{\beta}^p)/(\bar{\alpha} - \bar{\beta})$ depende de n puesto que $\bar{\alpha} = \alpha^n$ y $\bar{\beta} = \beta^n$. Si $p \geq 5$, dado que $p \mid \triangle$ y en consecuencia $p \mid \bar{\triangle} = u_n^2 \triangle$, el Lema 3.3 garantiza que $v_p(\bar{u}_p) = v_p(u_p) = 1$, por lo que se verifica la afirmación. Por lo tanto, asumamos que $p = 2$ o $p = 3$ y defina $\gamma_0 := p$ y $\gamma_n := \bar{u}_p = u_p(n)$, para cada entero positivo n.

Suponga primero que $p = 2$. Así, de (2.1) se tiene que

$$\gamma_n = \bar{u}_2 = \frac{\alpha^{2n} - \beta^{2n}}{\alpha^n - \beta^n} = \alpha^n + \beta^n = w_n \text{ para cada } n \geq 0.$$

Por lo tanto, de (2.2) se obtiene que

$$\gamma_n = a\gamma_{n-1} + b\gamma_{n-2} \text{ para todo } n \geq 2.$$

Además $2 \mid a$, ya que por hipótesis $2 \mid \triangle = a^2 + 4b$. Por lo tanto se puede verificar que $(\gamma_n)_{n\geq 0}$ satisface las hipótesis del Lema 3.5 ya que $\gamma_0 = 2, \gamma_1 = a = u_2, b$ son enteros y $2 \nmid b$. Además

$$\text{mín}\left\{v_2(a_j) : 1 \leq j < 2\right\} = v_2(a) > v_2(a) - 1 = \text{máx}\left\{v_2(\gamma_m) - v_2(\gamma_n) : 0 \leq m, n < 2\right\},$$

es decir,

$$\text{mín}\left\{v_2(a_j) : 1 \leq j < 2\right\} > \text{máx}\left\{v_2(\gamma_m) - v_2(\gamma_n) : 0 \leq m, n < 2\right\}.$$

Así, para cada entero $n \geq 0$ se tiene que

$$v_2(\gamma_n) = v_2(\gamma_{n \pmod 2}) = \begin{cases} v_2(\gamma_0), & si \quad 2 \mid n; \\ \\ v_2(\gamma_1), & si \quad 2 \nmid n. \end{cases} = \begin{cases} 1, & si \quad 2 \mid n; \\ \\ v_2(u_2), & si \quad 2 \nmid n. \end{cases}$$

Suponga ahora que $p = 3$. Luego de (2.1)

$$\gamma_n = \bar{u}_3 = \frac{\alpha^{3n} - \beta^{3n}}{\alpha^n - \beta^n} = (\alpha^2)^n + (\beta^2)^n + (\alpha\beta)^n, \tag{3.7}$$

para todo entero positivo n. De hecho, dado que $\gamma_0 = 3$ se tiene que la anterior expresión se cumple también para $n = 0$.

Se sigue entonces que $(\gamma_n)_{n\geq 0}$ es una sucesión linealmente recurrente de orden 3. En efecto, el Teorema 1.33 garantiza que su polinomio característico es

$$\begin{aligned}(X-\alpha^2)(X-\beta^2)(X-\alpha\beta) &= X^3-\alpha\beta X^2-\beta^2X^2+\alpha\beta^3X-\alpha^2X^2+\alpha^3\beta X+\alpha^2\beta^2X-\alpha^3\beta^3\\ &= X^3-(\alpha^2+\beta^2+\alpha\beta)X^2+(\alpha\beta)(\beta^2+\alpha^2+\alpha\beta)X-\alpha^3\beta^3\\ &= X^3-u_3X^2-bu_3X+b^3.\end{aligned}$$

Así que $\gamma_n = u_3\gamma_{n-1}+bu_3\gamma_{n-2}-b^3\gamma_{n-3}$ para cada entero $n\geq 3$. Además $\gamma_0=3$, $\gamma_1=a^2+b=u_3$ y $\gamma_2=w_2^2-b^2=(a^2+b)^2-b^2=(a^2+3b)u_3$, ya que de (3.7), (2.1) y el hecho que $\alpha\beta=-b$ se tiene que $\gamma_n=w_n^2-2(-b)^n$.

Note que $3\nmid a$, ya que por hipótesis $3\mid\triangle=a^2+4b$ y $3\nmid b$. En consecuencia, $v_3(\gamma_1)=v_3(\gamma_2)=v_3(u_3)$, de donde se concluye que $(\gamma_n)_{n\geq 0}$ satisface las hipótesis del Lema 3.5, así:

$$v_3(\gamma_n)=v_3(\gamma_{n\pmod 3})=\begin{cases} v_2(\gamma_0) & si \quad n\equiv 0 \pmod 3;\\ v_2(\gamma_1) & si \quad n\equiv 1 \pmod 3;\\ v_2(\gamma_2) & si \quad n\equiv 2 \pmod 3.\end{cases} = \begin{cases} 1, & si \quad 3\mid n;\\ v_3(u_3), & si \quad 3\nmid n.\end{cases}$$

Lo que completa la prueba. ■

Lema 3.7 *Si p es un número primo tal que $p\nmid b$ y $p\mid\triangle$, entonces*

$$v_p(u_{p^v})=\begin{cases} 0 & si \quad v=0,\\ v+v_p(u_p)-1 & si \quad v>0,\end{cases}$$

para cada entero no negativo v.

Demostración. Se procede por inducción sobre v. Para $v=0$ se tiene la siguiente igualdad $v_p(u_{p^0})=v_p(u_1)=v_p(1)=0$, y para $v=1$, se tiene $v_p(u_{p^1})=1+v_p(u_p)-1=v_p(u_p)$. Suponga ahora que $v\geq 2$ y que la afirmación es verdadera para $v-1$. Dado que $p\mid p^{v-1}$ y $v-1>0$, por Lema 3.6 se obtiene:

$$v_p(u_{p^v})=v_p(u_{p\cdot p^{v-1}})=v_p(u_{p^{v-1}})+1=(v-1)+v_p(u_p)-1+1=v+v_p(u_p)-1,$$

lo cual demuestra la afirmación. ■

Lema 3.8 *Si p es un número primo tal que $p \nmid b$ y $p \mid \triangle$, entonces*

$$v_p(u_n) = \begin{cases} v_p(n) + v_p(u_p) - 1, & si \quad p \mid n; \\ \\ 0, & si \quad p \nmid n. \end{cases}$$

para cada entero positivo n.

Demostración. Sea $n = mp^v$ donde $v \geq 0$ es un entero y m un entero positivo, tal que $p \nmid m$. Sea $(\bar{u}_\ell)_{\ell \geq 0}$ la sucesión de Lucas con polinomio característico $X^2 - w_m X + (-b)^m$. Del Lema 2.11 se sabe que $u_n = \bar{u}_{p^v} u_m$, $u_{pm} = \bar{u}_p u_m$, y $p \mid \bar{\triangle} = u_m^2 \triangle$. Además, ya que $p \mid \triangle$, se obtiene de los Lemas 2.17 y 2.18 que $p \nmid u_m$. Así $v_p(u_n) = v_p(\bar{u}_{p^v})$.

Si $v = 0$, entonces claramente $v_p(u_n) = v_p(\bar{u}_1) = v_p(1) = 0$. Si $v \geq 1$, entonces de los Lemas 3.7 y 3.6 se garantiza que

$$\begin{aligned} v_p(u_n) = v_p(\bar{u}_{p^v}) &= v + v_p(\bar{u}_p) - 1 = v + v_p(u_{pm}) - v_p(u_m) - 1 \\ &= v + v_p(u_p) - 1 = v_p(n) + v_p(u_p) - 1, \end{aligned}$$

que es nuestra afirmación.

■

Lema 3.9 *Si p es un número primo tal que $p \nmid b$, $p \nmid \triangle$, y $\tau(p) \mid n$, entonces*

$$v_p(u_n) = \begin{cases} v_p(n) + v_p(u_{p\tau(p)}) - 1, & si \quad p \mid n; \\ \\ v_p(u_{\tau(p)}), & si \quad p \nmid n. \end{cases}$$

Para cada entero positivo n.

Demostración. Sea $n = m\tau(p)$ donde m es un entero positivo. Sea $(\bar{u}_\ell)_{\ell \geq 0}$ la sucesión de Lucas con polinomio característico $X^2 - w_{\tau(p)} X + (-b)^{\tau(p)}$. Del Lema 2.11 se tiene que $u_n = \bar{u}_m u_{\tau(p)}$, $u_{p\tau(p)} = \bar{u}_p u_{\tau(p)}$ y $p \mid \bar{\triangle} = u_{\tau(p)}^2 \triangle$. Ademas ya que $p \nmid \triangle$, por el Lema 2.18 se sigue que $p \nmid \tau(p)$. En consecuencia $v_p(m) = v_p(n)$.

Por una parte, si $p \mid n$ entonces $p \mid m$ y por Lema 3.8 se obtiene

$$\begin{aligned} v_p(u_n) &= v_p(\bar{u}_m) + v_p(u_{\tau(p)}) = v_p(m) + v_p(\bar{u}_p) - 1 + v_p(u_{\tau(p)}) \\ &= v_p(m) + v_p(u_{p\tau(p)}) - v_p(u_{\tau(p)}) - 1 + v_p(u_{\tau(p)}) \\ &= v_p(m) + v_p(u_{p\tau(p)}) - 1. \end{aligned}$$

Por otra parte, si $p \nmid n$ entonces $p \nmid m$ y nuevamente por Lema 3.8 se garantiza

$$v_p(u_n) = v_p(\bar{u}_m) + v_p(u_{\tau(p)}) = v_p(u_{\tau(p)}),$$

como se afirmó. ■

3.3. Orden p-ádico de sucesiones de Lucas de primera categoría

El principal resultado de este documento es el siguiente teorema, que proporciona fórmulas para $v_p(u_n)$.

Teorema 3.10 *Si p es un número primo tal que $p \nmid b$, entonces*

$$v_p(u_n) = \begin{cases} v_p(n) + v_p(u_p) - 1, & si \quad p \mid \triangle, \quad p \mid n; \\ 0, & si \quad p \mid \triangle, \quad p \nmid n; \\ v_p(n) + v_p(u_{p\tau(p)}) - 1, & si \quad p \nmid \triangle, \quad \tau(p) \mid n, \quad p \mid n; \\ v_p(u_{\tau(p)}), & si \quad p \nmid \triangle, \quad \tau(p) \mid n, \quad p \nmid n; \\ 0, & si \quad \tau(p) \nmid n. \end{cases} \tag{3.8}$$

Para cada entero positivo n.

Demostración. Este teorema se sigue inmediatamente de los Lemas 3.8, 3.9 y 2.17. Teniendo en cuenta que los tres Lemas parten de la hipotesis de que p es un número primo tal que $p \nmid b$ y las conclusiones serán validas para todo entero positivo n, se observa lo siguiente:

Por una parte, el Lema 3.8 enuncia que si $p \mid \triangle$ y $\tau(p) \mid n$, entonces la valuación p-ádica estará dada por $v_p(u_n) = v_p(n) + v_p(u_p) - 1$ si $p \mid n$ y $v_p(u_n) = 0$ si $p \nmid n$. De donde se siguen los primeros dos ítem del teorema principal.

Por otra parte, el Lema 3.9 enuncia que si $\tau(p) \mid n$, $p \nmid \triangle$ y $\tau(p) \mid n$, entonces la valuación p-ádica estará dada por $v_p(u_n) = v_p(n) + v_p(u_{p\tau(p)}) - 1$ si $p \mid n$ y $v_p(u_n) = v_p(u_{\tau(p)})$ si $p \nmid n$. Lo que garantiza la veracidad del tercer y cuarto ítem del teorema principal.

Finalmente, el Lema 2.17 enuncia que para cada entero positivo n se cumple que $p \mid u_n$ si, y sólo si, $\tau(p) \mid n$, De donde se concluye que si $\tau(p) \mid n$ entonces $v_p(u_n) = 0$, lo cual corresponde al último item del teorema principal. ■

Comentario final

En la teoría de números, la resolución de ecuaciones Diofánticas es un campo de estudio que ha generado gran interés debido a su aplicabilidad en diversos problemas matemáticos y computacionales. En particular, las sucesiones de Lucas y sus valuaciones p-ádicas ofrecen un enfoque poderoso para abordar ciertos tipos de ecuaciones Diofánticas. Esto se debe a que la valuación p-ádica de las sucesiones de Lucas proporciona información sobre congruencias y propiedades aritméticas de los números involucrados, lo que a su vez puede conducir a estrategias innovadoras para resolver ecuaciones Diofánticas. Por lo tanto, este trabajo no sólo contribuye al conocimiento teórico de las sucesiones de Lucas, sino que aporta herramientas para la resolución de problemas numéricos y algebraicos en la teoría de números.

Bibliografía

[1] J. J. Bravo, M. Díaz and J. L. Ramírez, *The 2-adic and 3-adic valuation of the Tripell sequence and an application*, Turkish J. Math., **44** (2020), 131–141.

[2] T. Koshy, *Fibonacci and Lucas Numbers with Applications*, WileyInterscience.,**1** (2001).

[3] T. Lengyel, *The order of the Fibonacci and Lucas numbers*, Fibonacci Quart., **33** (1995), 234–239.

[4] T. Lengyel and D. Marques, *The 2-adic Order of the Tribonacci Numbers and the Equation* $T_n = m!$, J. Integer Seq., **17** (2014), Article 14.10.1.

[5] F. Luca, *Ecuaciones diofánticas,* XXI Escuela Venezolana de Matemáticas, Emalca-Venezuela, 2008.

[6] É. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math., **1** (1878), 184–196, 197–240, 289–321.

[7] R. P. Machio. (2010). *Restos cuadráticos y ley de reciprocidad cuadrática*. Hojamat.es. http://hojamat.es/parra/restocuad.pdf.

[8] P. Ribenboim, *My numbers, My friends: Popular lectures on number theory*, SpringerVerlag., (2000).

[9] C. Sanna, *The p-adic valuation of Lucas sequences*, Fibonacci Quart., **54** (2016), 118–124.

[10] L. Serge, *Algebra*, SpringerVerlag., **3** (2002).

[11] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Univ. Press., **1** (1986), 56–63.

[12] P. Somoza, *Números p-ádicos*, Tesis de pregrado, Departamento de Matemáticas Universidad Santiago de Compostela (2018).