Algunos Resultados Derivados Del Estudio De La Sucesión de Fibonacci Módulo m

Yzel Wlly Alay Gómez Espíndola

Universidad Industrial de Santander
Facultad de Ciencias
Escuela de Matemáticas
Matemáticas
Bucaramanga
2015

Algunos Resultados Derivados Del Estudio De La Sucesión de Fibonacci Módulo m

Autor

Yzel Wlly Alay Gómez Espíndola

Trabajo de grado como requisito

parcial para optar el título de

Matemático

Director

Carlos Arturo Rodríguez Palma

Magíster en Matemáticas

Universidad Industrial de Santander
Facultad de Ciencias
Escuela de Matemáticas
Matemáticas
Bucaramanga
2015

Agradecimientos

- Agradezco a ese ser todopoderoso, inmaterial y omnipresente en el que creo, por ofrecerme la oportunidad de vivir, darme salud y sabiduría.
- Agradezco a mis familiares y seres amados por brindarme su apoyo incondicional durante todo mi proceso de formación académica y crecimiento personal.
- Agradezco especialmente a mi director de proyecto, el profesor Carlos Arturo Rodríguez su colaboración e interés en este trabajo y por todos sus consejos.
- Agradezco a los profesores que contribuyeron en mi formación académica y personal.
- A todas las personas que de una u otra manera hicieron posible este logro.

Índice general

Introducción

Mientras el municipio de Pisa, Italia se adentraba en el último tercio del siglo XII, sólo tres años antes del inicio de la obra de una de las torres más populares de Europa, nació un personaje que traería a este municipio de la región de la Toscana aún más orgullo, me refiero a Leonardo de Pisa, más conocido como Fibonacci quien ha tenido y tiene gran reconocimiento no sólo en la atmósfera matemática sino también en el arte, la biología, etc. Se le conoce principalmente por la invención de la sucesión que lleva su nombre, surgida como consecuencia del estudio del crecimiento de las poblaciones de conejos.

El nombre por el que es reconocido se lo debe a su padre Guglielmo, quien fuera apodado Bonacci (simple o bien intencionado). Leonardo recibió póstumamente el apodo de Fibonacci (por filius Bonacci, hijo de Bonacci). Guglielmo dirigía un puesto de comercio en Bugía en el norte de África (hoy Bejaia, Argelia), y de joven Leonardo viajo allí para ayudarlo. Afortunadamente su formación matemática tuvo gran influencia de ideas musulmanas y aprendió así el sistema de numeración indoarábiga. Estuvo estudiando con matemáticos árabes destacados de la época hasta principios del siglo XIII, poco después publicaría su libro Liber abaci (Libro del ábaco), el cual no tardó mucho en volverse popular. En sus páginas describe el cero, el sistema posicional, la descomposición en factores primos, los criterios de divisibilidad, y muestra las ventajas del nuevo sistema de numeración aplicándolo a la contabilidad comercial, conversión de pesos y medidas, cálculo, intereses, cambio de moneda, y otras numerosas aplicaciones. El libro fue recibido con entusiasmo en la Europa ilustrada y tuvo un impacto profundo en el pensamiento matemático europeo.

Tal como lo hubiese hecho un francés del siglo anterior al de su nacimiento, Leonardo escribió en el margen de su libro Liber Abaci la secuencia de números

1; 1; 2; 3, 5; 8; 13; 21; 34; 55; 89....

junto al conocido “problema de los conejos”, que en lenguaje actual sería:

“Una pareja de conejos tarda un mes en alcanzar la edad fértil, a partir de ese momento cada vez engendra una pareja de conejos, que a su vez, tras ser fértiles engendrarán cada mes una pareja de conejos. ¿Cuántos conejos habrá al cabo de un determinado número de meses?”

El conocimiento de esta sencilla y hermosa sucesión ha inspirado el trabajo de personas en diversas áreas, uno de ellos fue el matemático francés François Édouard Anatole Lucas quien generalizó las sucesiones que se regían por la misma ecuación de recurrencia que la sucesión de Fibonacci variando los valores iniciales, la más sencilla de estas sucesiones es la llamada sucesión de Lucas que toma 2 y 1 como valores iniciales.

Estas dos sucesiones guardan una relación más fuerte de la que es perceptible a simple vista, de ellas se han desentrañado numerosas e interesantes propiedades, algunas de estas se mostrarán en este trabajo. Una característica interesante de los números en la sucesión de Fibonacci y en la de Lucas, es que si calculamos los residuos de estos números módulo un entero *m* se aprecia que estos residuos aparecen con regularidad, de forma cíclica. Esta característica será estudiada y se establecerán similitudes y diferencias del comportamiento de la dos sucesiones vistas modulo *m*. Esta característica nos será de gran utilidad para probar lo siguiente:

1. *En la sucesión de Fibonacci el único elemento con más de una cifra, que es formado solo por un dígito es* $F_{10} = 55$.
2. *En la sucesión de Lucas el único elemento con más de una cifra, que es formado solo por un dígito es* $L_5 = 11$.

Es natural cuestionarnos si estos resultados son producto de la reunión de condiciones ideales, o si por otro lado al variar la naturaleza en la que viven los números de estas sucesiones se pueden obtener resultados análogos. Estudiaremos la variación de dos aspectos: en primer lugar variaremos los términos iniciales; en segundo lugar variaremos la base numérica *b* en que estas expresados los números, más precisamente nos interesaremos por responder la pregunta; ¿Existen números de Fibonacci y Lucas que al expresarlos en un sistema numérico en base *b* estén formados por solo un dígito?

Capítulo 1

Preliminares

1.1. Sucesión de Fibonacci y de Lucas

Inicialmente vamos a deducir expresiones explícitas para los números en la sucesión de Fibonacci y de Lucas, partiendo de la ecuación de recurrencia conocida para cada una de ellas.

Una ecuación de recurrencia es una expresión que permite determinar los elementos de una sucesión, si se conoce:
i) El dominio de validez de la ecuación en términos de la variable.
ii) Un conjunto suficiente de valores particulares de la sucesión.

Definición 1. *Se dice que una sucesión u_n satisface una ecuación de recurrencia lineal homogénea de orden k si*

$$u_n = a_1 u_{n-1} + a_2 u_{n-2} + \ldots + a_k u_{n-k}, \text{ con } n \geq k$$

para ciertas constantes $a_1, a_2, \ldots, a_k$ y un conjunto de k valores iniciales (usualmente conocidos) $u_{n-1}, u_{n-2}, \ldots, u_{n-k}$.

Resolviendo algunos problemas de conteo, encontramos que las soluciones de los casos particulares forman sucesiones que siguen alguna ecuación de recurrencia, ilustramos esto en el siguiente ejemplo.

Ejemplo 1. *Consideremos el problema de determinar el número s_n, de todas las cadenas de* 0´*s y* 1´*s de longitud n de tal forma que no haya dos ceros seguidos.*

Si $n = 3$ *tenemos que las cadenas de longitud* 3 *que podemos construir sin dos ceros seguidos son*

$$111 \qquad 110 \qquad 101 \qquad 011 \qquad 010$$

Luego $s_3 = 5$. *Ahora, para obtener una ecuación de recurrencia para* s_n *observemos que:*
► *Si agregamos un* 1 *al final de las cadenas de longitud* $n - 1$ *sin dos ceros seguidos, obtenemos las cadenas de longitud n que terminan en* 1.
► *Si agregamos* 10 *al final de las cadenas de longitud* $n-2$ *sin dos ceros seguidos, obtenemos las cadenas de longitud n que terminan en* 0.

De esta forma tenemos que la ecuación de recurrencia para s_n *esta dada por* $s_n = s_{n-1} + s_{n-2}$, *valida para cualquier entero positivo* $n \geq 2$, *con valores iniciales* $s_1 = 2$ *y* $s_2 = 3$. *Así, obtenemos la sucesión*

$$2, 3, 5, 8, 13, 21, \ldots$$

La sucesión s_n y la sucesión de Fibonacci tienen la misma ecuación de recurrencia, de hecho producen la misma sucesión si no consideramos los primeros elementos.

Definición 2. *La sucesión de Fibonacci sigue la ecuación de recurrencia lineal homogénea de orden* 2

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

donde n es un natural tal que $n \geq 2$, $F_0 = 0$ *y* $F_1 = 1$.

Definición 3. *La sucesión de Lucas sigue la ecuación de recurrencia lineal homogénea de orden* 2

$$L_n = L_{n-1} + L_{n-2}$$

donde n es un natural tal que $n \geq 2$, $L_0 = 2$ *y* $L_1 = 1$

Determinar una expresión que permitiera calcular en una cantidad fija de pasos cualquier número de Fibonacci, fue un problema que ocupó a algunos matemáticos de los siglos XVIII y XIX. El descubrimiento de una expresión con estas características se le atribuye a Jacques P. M. Binet, aunque poco más de 100 años antes Abraham DeMoivre encontró esta misma expresión. La siguiente es la expresión en cuestión

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right).$$

Dada la importancia que tomó la sucesión de Lucas, no es extraño que haya surgido una formula tipo Binet para los números de la sucesión de Lucas.

$$L_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Existen diversas relaciones entre la sucesión de Fibonacci y la de Lucas, algunas de ellas se hacen evidentes en las siguientes identidades. Algunas de estas pruebas están disponibles en [4] y [2].

Identidad 1. *Sean F_n la sucesión de Fibonacci y L_n la sucesión de Lucas. Se cumplen las siguientes identidades:*

a) $F_{m+n} = F_{m-1}F_n + F_mF_{n+1}$.

b) $F_m \mid F_{m\cdot n}$ *para toda pareja de enteros* m, n.

c) $F_{2n} = F_nL_n$ *para* $n \geq 0$.

d) $L_{2n} = L_n^2 + 2(-1)^{n+1}$ *para* $n \geq 0$.

e) $L_n^2 - 5F_n^2 = 4(-1)^n$ *para* $n \geq 0$.

f) $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$.

g) F_n *y* F_{n+1} *son primos relativos.*

Demostración. Sean n y m enteros positivos.

a) Fijemos m y hagamos inducción sobre n. Veamos que la propiedad se cumple para $n = 1$ y 2.

$$\begin{aligned} F_{m+1} &= F_{m-1} \cdot F_1 + F_m \cdot F_2 = F_{m-1} + F_m, \\ F_{m+2} &= F_{m-1} \cdot F_2 + F_m \cdot F_3 = F_{m-1} + F_m + F_m = F_{m+1} + F_m \end{aligned}$$

Supongamos ahora que la propiedad se cumple para $n = 1, 2, \ldots, k$ y veamos que se cumple para $n = k + 1$. En efecto

$$\begin{aligned} F_{m+(k+1)} &= F_{m+k} + F_{m+(k-1)} \\ &= [F_{m-1} \cdot F_k + F_m \cdot F_{k+1}] + [F_{m-1} \cdot F_{k-1} + F_m \cdot F_k] \\ &= F_{m-1}[F_k + F_{k-1}] + F_m[F_k + F_{k+1}] \\ &= F_{m-1} \cdot F_{k+1} + F_m \cdot F_{k+2}. \end{aligned}$$

b) Fijemos m y hagamos inducción sobre n. Para $n = 1$ tenemos que $F_m \mid F_m$. Supongamos que la propiedad se cumple para $n = k$ es decir $F_m \mid F_{km}$ y veamos que

$$F_{(k+1)\cdot m} = F_{mk+m} = F_{mk-1} \cdot F_m + F_{mk} \cdot F_{m+1}$$

lo cual implica que $F_m \mid F_{(k+1)\cdot m}$.

c) Probemos primero que $L_n = F_{n-1} + F_{n+1}$, para todo n positivo. Cuando $n = 1$ se cumple que $L_1 = 1 = F_0 + F_2$. Ahora supongamos que el resultado se cumple para $n = 1, \ldots, k$, en particular se cumple que

$$\begin{aligned} L_{k-1} &= F_{k-2} + F_k, \\ L_k &= F_{k-1} + F_{k+1} \end{aligned}$$

Sumando estas expresiones obtenemos $L_{k+1} = F_k + F_{k+2}$.

Probemos ahora que $F_{2n} = F_n L_n$. Usando el literal *a* escribimos $F_{2n} = F_{n+n} = F_{n-1} \cdot F_n + F_n F_{n+1} = F_n \cdot (F_{n-1} + F_{n+1})$. Sabemos que $L_n = F_{n-1} + F_{n+1}$, por lo tanto $F_{2n} = F_n \cdot L_n$.

d) Sean $r = \dfrac{1+\sqrt{5}}{2}$ y $s = \dfrac{1-\sqrt{5}}{2}$, entonces $F_n = \dfrac{1}{\sqrt{5}}(r^n - s^n)$ y $L_n = r^n + s^n$. En consecuencia

$$\begin{aligned} F_n^2 &= \frac{1}{5}(r^n - s^n)^2 = \frac{1}{5}(r^{2n} + s^{2n} - 2r^n s^n) \\ L_n^2 &= r^{2n} + s^{2n} + 2r^n s^n. \end{aligned}$$

Así $L_n^2 - 5F_n^2 = r^{2n} + s^{2n} + 2r^n s^n - (r^{2n} + s^{2n} - 2r^n s^n) = 4(r \cdot s)^n = 4(-1)^n$.

e) Sean $r = \dfrac{1+\sqrt{5}}{2}$ y $s = \dfrac{1-\sqrt{5}}{2}$, entonces $L_n = r^n + s^n$. Veamos que

$$\begin{aligned} L_{2n} &= L_n^2 - 2(-1)^n \\ r^{2n} + s^{2n} &= r^{2n} + 2r^n s^n + s^{2n} - 2(-1)^n \\ r^{2n} + s^{2n} &= r^{2n} + 2(r \cdot s)^n + s^{2n} - 2(-1)^n \\ r^{2n} + s^{2n} &= r^{2n} + 2(-1)^n + s^{2n} - 2(-1)^n \\ r^{2n} + s^{2n} &= r^{2n} + s^{2n}. \end{aligned}$$

f)

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

Siguiendo el mismo procedimiento con $F_n F_{n-2} - F_{n-1}^2$, $F_{n-1}F_{n-3} - F_{n-2}^2$, sucesivamente obtenemos

$$
\begin{aligned}
-(F_nF_{n-2} - F_{n-1}^2) &= (-1)^2(F_{n-1}F_{n-3} - F_{n-2}^2) \\
&= (-1)^3(F_{n-2}F_{n-4} - F_{n-3}^2) \\
&\vdots \\
&= (-1)^n(F_1F_{-1} - F_0^2) \\
&= (-1)^n
\end{aligned}
$$

g) Supongamos que $d = gcd(F_n, F_{n-1})$. Entonces d divide a cualquier combinación lineal entre F_n y F_{n-1}, en particular d divide a la diferencia $F_{n+1} - F_n = F_{n-1}$. De igual manera, d divide a $F_n - F_{n-1} = F_{n-2}$, seguimos así sucesivamente hasta obtener que d divide a $F_2 = 1$ y a $F_1 = 1$. Por lo tanto, necesariamente $d = 1$.

□

1.2. Sucesiones de Fibonacci módulo *m*

La majestuosa sucesión de Fibonacci entró a circular en el mundo matemático en el siglo XII. Siglos antes, en el mundo oriental se abrieron los telones para ver el surgimiento de las ideas que tomaron forma y hoy conocemos como congruencias modulares. No es para nada descabellado que alguien hubiese querido estudiar esta sucesión aplicando congruencias modulares. El uso conjunto de estas ideas amplió el estudio de dicha sucesión y permitió afrontar problemas desde otra perspectiva.

Al modular los términos de la sucesión de Fibonacci módulo un entero positivo m, obtenemos una sucesión de residuos. Nos referiremos a esta sucesión simplemente como la sucesión de residuos de Fibonacci módulo m. [4] y [2] son buenas referencias para seguir la teoría que desarrollaremos en esta sección.

En esta sección denotaremos al residuo de F_n módulo m por r_n.

Teorema 1. *La sucesión de residuos de la sucesión de Fibonacci vista módulo m sigue la misma ecuación de recurrencia que la sucesión de Fibonacci.*

Demostración. Según la notación tenemos

$$\begin{aligned} F_{n-1} &\equiv r_{n-1} \pmod{m}, \\ F_{n-2} &\equiv r_{n-2} \pmod{m}, \\ F_n = F_{n-2} + F_{n-1} &\equiv r_{n-2} + r_{n-1} \pmod{m}, \\ r_n &\equiv r_{n-2} + r_{n-1} \pmod{m}. \end{aligned}$$

□

Corolario 1. *Si* $F_n \equiv 0 \pmod{m}$*, si y solo si* $F_{n-1} \equiv F_{n+1} \pmod{m}$.

Demostración. Sabemos que $F_{n-1} + F_n = F_{n+1}$, de ahí que $F_{n-1} + F_n \equiv F_{n+1} \pmod{m}$. Por hipótesis $F_n \equiv 0 \pmod{m}$, se sigue que $F_{n-1} \equiv F_{n+1} \pmod{m}$. Recíprocamente, sabemos que $F_n = F_{n+1} - F_{n-1}$, de ahí $F_n \equiv F_{n+1} - F_{n-1} \pmod{m} \equiv 0 \pmod{m}$, pues por hipótesis $F_{n-1} \equiv F_{n+1} \pmod{m}$. □

Teorema 2. *Dado un entero m, existe n con* $1 \leq n \leq m^2$*, tal que* F_n *es divisible por m.*

Demostración. Consideremos la sucesión de residuos de la sucesión de Fibonacci módulo m, y formemos parejas con estos residuos de la siguiente forma

$$(r_1, r_2), (r_2, r_3), (r_3, r_4), \ldots, (r_k, r_{k+1}), \ldots$$

Cada pareja puede ser de una de las m^2 parejas distintas posibles, entonces si tomamos $m^2 + 1$ parejas de residuos al menos deben existir dos parejas iguales, es decir en algún instante encontramos una pareja que se repite. Por el teorema anterior, se concluye que la sucesión de Fibonacci es periódica vista módulo un entero positivo m.

Supongamos que la primera pareja que se repite es (r_s, r_{s+1}), con $s \in \mathbb{Z}^+$ y supongamos que $s > 1$. Entonces existe una pareja tal que $(r_s, r_{s+1}) = (r_t, r_{t+1})$, con $s < t \leq m^2 + 1$. Usando el teorema anterior podemos afirmar que

$$(r_{s-1}, r_s) = (r_{t-1}, r_t)$$

Esto implica que la pareja (r_{s-1}, r_s) se repite antes que la pareja (r_s, r_{s+1}), lo cual es contradictorio y por lo tanto se concluye que $s = 1$. De ahí que la primera pareja de residuos que se repite es $(1, 1)$, entonces existe $n \in \mathbb{Z}^+$ tal que $(1, 1) = (r_{n+1}, r_{n+2})$ y por el corolario anterior tenemos que $F_n \equiv 0 \pmod{m}$. □

Observación: *En la prueba del teorema anterior se muestra que el* 0 *aparece en la sucesión de residuos, además la sucesión de residuos es periódica vista modulo m, entonces el* 0 *aparece infinitas veces en la sucesión de residuos. Esto implica que cada entero positivo m divide a infinitos números de Fibonacci.*

Observación: *Se prueba usando un razonamiento análogo al usado en la prueba del teorema anterior, que es periódica la sucesión de residuos módulo m de cualquier sucesión de números enteros que siga la misma ecuación de recurrencia que la sucesión de Fibonacci.*
Resulta ahora conveniente caracterizar la aparición de estos residuos en uno de estos ciclos.

Definición 4. ***Rango de Aparición***
Sea $m > 1$. *Al menor índice i tal que* $F_i \equiv 0 \pmod{m}$, *se le llama el rango de aparición de m y lo denotamos por* $r(m)$.

Ejemplo 2.

a) $r(2) = 3$, *pues* $F_3 = 2$ *es el menor número de Fibonacci que es divisible por* 2.

b) $r(13) = 7$, *ya que* $F_7 = 13$ *es el menor número de Fibonacci que es divisible por* 13.

Definición 5. *El período de repetición de la sucesión de Fibonacci módulo un entero positivo m, es el menor entero positivo* $l(m)$ *tal que*

$$F_{l(m)} \equiv 0 \pmod{m} \text{ y } F_{l(m)+1} \equiv 1 \pmod{m}$$

Directamente de esta definición se sigue que para cualquier $k \in \mathbb{N}$

$$F_k \equiv 0 \pmod{n} \text{ y } F_{k+1} \equiv 1 \pmod{n} \Leftrightarrow l(n) \mid k$$

Observación: *Por definición* $m \mid F_{r(m)}$ *y de la identidad 1-b* $F_{r(m)} \mid F_{k\cdot r(m)}$ *con* $k \in \mathbb{Z}^+$, *entonces* $m \mid F_{k\cdot r(m)}$. *Luego resulta evidente que los índices para los cuales* $F_n \equiv 0 \pmod{m}$ *forman una progresión aritmética. Además se puede notar que* $l(m) = r(m) \cdot t$, *esto es* $l(m)$ *es múltiplo de* $r(m)$.

Teorema 3. *Sea* p *un primo. Entonces* $p \mid F_n$ *si y solo si* $r(p) \mid n$.

Demostración. Supongamos primero que $p \mid F_n$ y que $r(p) \nmid n$, por el algoritmo de la división existen enteros a y b tales que

$$n = r(p) \cdot a + b, \quad \text{con} \quad 0 < b < r(p)$$

Usando la identidad 1-a escribamos $F_n = F_{r(p)\cdot a+b} = F_{r(p)\cdot a-1}F_b + F_{r(p)\cdot a}F_{b+1}$. Como $p \mid F_n$ y $p \mid F_{r(p)\cdot a}$, entonces $p \mid F_{r(p)\cdot a-1}F_b$. De la identidad 1-g, $F_{r(p)\cdot a-1}$ y $F_{r(p)\cdot a}$ son primos relativos, entonces $p \mid F_b$ pero $b < r(p)$ lo cual es contradictorio, pues $r(p)$ es el menor índice de un número de Fibonacci que tiene a p como factor.
Supongamos ahora que $r(p) \mid n$, entonces existe $t \in \mathbb{Z}$ tal que $n = r(p) \cdot t$, por definición tenemos que $p \mid F_{r(p)}$ y usando la identidad 1-b, obtenemos que $p \mid F_{r(p)} \mid F_{r(p)\cdot t} = F_n$. □

Observemos que en la demostración del teorema anterior, no se usa el hecho que p es primo, por tanto esta demostración también es válida usando un entero cualquiera t en lugar de un primo, obteniendo el siguiente resultado.

Corolario 2. *Sean* n, m *enteros. Entonces* $m \mid F_n$ *si y solo si* $r(m) \mid n$.

1.3. Sucesiones de Lucas módulo *m*

La sucesión de Lucas en varios sentidos es muy similar a la sucesión de Fibonacci, siguen la misma ecuación de recurrencia, existe una expresión cerrada que la determina, dicha expresión involucra la sección áurea, etc. Sin embargo, estas hermanas no son gemelas idénticas. Veremos que la sucesión de Lucas vista módulo un entero positivo m no se cumplen algunas de las propiedades que se cumplen en la de Fibonacci.

Al modular los términos de la sucesión de Lucas módulo un entero positivo m, obtenemos una sucesión de residuos. Nos referiremos a esta sucesión simplemente como la sucesión de residuos de Lucas módulo m.

Proposición 1. *La sucesión de residuos de Lucas módulo m sigue la misma ecuación de recurrencia que la sucesión de Lucas.*

Demostración. Denotemos al residuo de L_n módulo m por r_n. Entonces

$$\begin{aligned} L_{n-1} &\equiv r_{n-1} \pmod{m}, \\ L_{n-2} &\equiv r_{n-2} \pmod{m}, \\ L_n = L_{n-2} + L_{n-1} &\equiv r_{n-2} + r_{n-1} \pmod{m}, \\ r_n &\equiv r_{n-2} + r_{n-1} \pmod{m}. \end{aligned}$$

□

Corolario 3. *Si* $L_n \equiv 0 \pmod{m}$, *entonces* $L_{n-1} \equiv L_{n+1} \pmod{m}$.

Demostración. Sabemos que $L_{n-1} + L_n = L_{n+1}$, de ahí que $L_{n-1} + L_n \equiv L_{n+1} \pmod{m}$. Por hipótesis $L_n \equiv 0 \pmod{m}$, se sigue que $L_{n-1} \equiv L_{n+1} \pmod{m}$.Recíprocamente, sabemos que $L_n = L_{n+1} - L_{n-1}$, de ahí $L_n \equiv L_{n+1} - L_{n-1} \pmod{m} \equiv 0 \pmod{m}$, pues por hipótesis $L_{n-1} \equiv L_{n+1} \pmod{m}$. □

Teorema 4. *La sucesión de Lucas es periódica vista modulo un entero positivo m.*

Demostración. La sucesión de Lucas es periódica vista módulo un entero positivo m por observación de la sección anterior y la primer pareja de residuos que se repite es (r_1, r_2), donde $L_i \equiv r_i \pmod{m}$. □

Observación: *No es posible probar en la sucesión de Lucas que todo entero m divide a algún número de Lucas, pues no hay garantía que* $r_2 - r_1 = 0$. *Vemos que si* $m = 2$ *entonces* $r_2 = 1$ *y en este caso hay ceros en la sucesión de Lucas módulo* 2. *Sin embargo existen enteros positivos m para los cuales no existe un número de Lucas que sea divisible por m, con el siguiente ejemplo ilustraremos esto.*

Ejemplo 3. *Sea* $m = 8$*, y veamos los primeros números de Lucas módulo* 8*.*

$$\boldsymbol{2,1,3,4,7,3,2,5,7,4,3,7}, 2, 1, 3, \ldots$$

Observe que la sucesión de 12 *residuos en negrita, vuelve a aparecer. Entre esos* 12 *residuos no aparece el cero* 0 *y por lo tanto no aparecerá en ningún momento, es decir no existe un número de Lucas que sea divisible por* 8*.*

Dado que no siempre existe algún número de Lucas que sea divisible por un entero *m*, nos vemos forzados a hacer algunas consideraciones adicionales para definir el rango de aparición de un entero positivo como factor de un número de Lucas.

Sea $m > 1$ y considere el conjunto $R := \{r' \in \mathbb{Z} : L_{r'} \equiv 0 \pmod{m}\}$, si $R \neq \phi$ por el principio del buen orden tenemos que R posee mínimo, este valor será el rango de aparición de m y lo notaremos $r'(m)$.

Definición 6. ***Rango de Aparición***

Sea $m > 1$*. Considere el conjunto* $R := \{r' \in \mathbb{Z} : L_{r'} \equiv 0 \pmod{m}\}$*:*

a) Si $R \neq \phi$*, el rango de aparición de m es* $r'(m) = \text{mín}(R)$*.*

b) Si $R = \phi$*, decimos que el rango de aparición* $r'(m)$ *no existe.*

Ejemplo 4.

a) $r'(5)$ *no existe pues ningún número de Lucas es múltiplo de* 5*, observando el apéndice E notamos que ninguno de los residuos es* 0*.*

b) $r'(14) = 12$*, pues* $L_{12} = 322$ *es el menor número de Lucas que es divisible en* 14*.*

Definición 7. *El período de repetición de la sucesión de Lucas módulo un entero positivo m, es el menor entero positivo* $l'(m)$ *tal que*

$$L_{l'(m)} \equiv 2 \pmod{m} \text{ y } L_{l'(m)+1} \equiv 1 \pmod{m}$$

De esta definición se sigue que para cualquier $k \in \mathbb{Z}$

$$L_k \equiv 2 \pmod{m} \text{ y } L_{k+1} \equiv 1 \pmod{m} \Leftrightarrow l'(m) \mid k$$

Observación: *En el apéndice E se puede ver que a diferencia de lo que sucede en la sucesión de Fibonacci, en la de Lucas los índices para los cuales* $L_n \equiv 0 \pmod{m}$ *no forman una progresión aritmética. En consecuencia no es posible afirmar que* $l'(m) = r'(m) \cdot t$*, aún cuando* $r'(m)$ *exista.*

Las siguientes conjeturas se pueden verificar computacionalmente, sin embargo las pruebas que se desarrollan para la sucesión de Fibonacci no pueden ser aplicadas a la sucesión de Lucas, dado que las identidades usadas no tienen un análogo para ella. Para nuestros intereses, bastará con la verificación computacional de estos resultados para casos especiales, con ayuda de los datos consignados en los apéndices.

Conjetura 1. *Sea p un primo. Entonces,* $p \mid L_m$ *si y solo si* $r'(p)$ *existe y* $r'(p) \mid m$.

Conjetura 2. *Sea n un entero.Entonces,* $n \mid L_m$ *si y solo si* $r'(p)$ *existe y* $r'(n) \mid m$.

1.4. Caracterización de un período simple de F_n módulo m

En la sección 1.2 probamos que el período de repetición de los residuos módulo m de la sucesión de Fibonacci, es múltiplo del rango, es decir $l(m) = r(m) \cdot t$. En este capítulo caracterizaremos completamente a $l(m)$, es decir caracterizaremos el factor aún desconocido t de $r(m)$. Los resultados que mostraremos en este capítulo fueron presentados por Marc Renault en el año 1,996 en [4].

Teorema 5. $r(m) \mid r(m \cdot n)$*, para todo par de enteros positivos m y n.*

Demostración. Dado que $m \cdot n \mid F_{r(m \cdot n)}$, de ahí que $m \mid F_{r(m \cdot n)}$. Luego, del corolario 2, $r(m) \mid r(m \cdot n)$. □

Observación: Sea m un entero positivo, entonces:

a) Al residuo de $F_{r(m)+1}$ módulo m lo denotaremos por $s(m)$.

b) Al orden de $s(m)$ módulo m lo denotaremos por $\alpha(m)$; es decir $s(m)^{\alpha(m)} \equiv 1 \pmod{m}$ y si $t < \alpha(m)$ entonces $s(m)^t \not\equiv 1 \pmod{m}$.

Ejemplo 5.

Sea $m = 13$, *sabemos que* $r(13) = 7$, *luego* $F_{r(13)+1} = F_8 = 21 \equiv 8 \pmod{13}$, *de ahí que* $s(13) = 8$. *Como* $s(13)^4 = 8^4 \equiv 1 \pmod{13}$ *y se verifica que para* $t < 4$ *se cumple que* $s(13)^t \not\equiv 1 \pmod{13}$, *entonces* $\alpha(13) = 4$.

Teorema 6. $l(m) = r(m) \cdot \alpha(m)$, *para todo entero positivo m.*

Demostración. Un período simple de F_n módulo m, se puede escribir así

$$0\,1\,1\,\ldots\,s_1\,0\,s_1\,s_1\,\ldots\,s_2\,0\,s_2\,s_2\,\ldots\,s_3\,0\,s_3\,s_3\,\ldots\ldots\,0\,1$$

Dividamos ahora este período en cadenas así,

$$\underbrace{0\,1\,1\,\ldots\,s_1}_{A_0}\ \underbrace{0\,s_1\,s_1\,\ldots\,s_2}_{A_1}\ \underbrace{0\,s_2\,s_2\,\ldots\,s_3}_{A_2}\ 0\,s_3\,s_3\,\ldots\ldots\,0\,1,$$

de tal forma que cada A_i tiene $r(m)$ términos, en los cuales aparece un solo cero.
Observando detenidamente se nota que $s_1 = s(m)$ y que cada cadena A_i es múltiplo de A_0, es decir $A_i \equiv k_i \cdot A_0 \pmod{m}$, donde cada $k_i \in \mathbb{Z}$.

Más precisamente,

$$\begin{aligned}
A_1 &\equiv s_1 A_0 \pmod{m}\\
A_2 &\equiv s_2 A_0 \pmod{m}\\
A_3 &\equiv s_3 A_0 \pmod{m}\\
&\vdots\\
A_{k-1} &\equiv s_{k-1} A_0 \pmod{m}\\
A_k &\equiv s_k A_0 \pmod{m}\\
&\vdots
\end{aligned}$$

Como el último término en A_k es s_{k+1} y el último en A_0 es s_1, tenemos que:

$$s_k \equiv s_{k-1} \cdot s_1 \pmod{m}$$
$$s_k \equiv s_{k-2} \cdot s_1^2 \pmod{m}$$
$$s_k \equiv s_{k-3} \cdot s_1^3 \pmod{m}$$
$$s_k \equiv s_{k-4} \cdot s_1^4 \pmod{m}$$
$$\vdots$$
$$s_k \equiv s_1^k \pmod{m}$$

Como $\alpha(m)$ es el orden de s_1, entonces el período simple puede ser reescrito así:

$$0\,1\,1\,\ldots\,s_1\,0\,s_1\,s_1\,\ldots\,s_1^2\,0\,s_1^2\,s_1^2\,\ldots\,s_1^3\,0\,s_1^3\,s_1^3\,\ldots\ldots\,s_1^{\alpha(m)-1},0\,s_1^{\alpha(m)-1}\ldots 0\,1$$

Lo cual relaciona directamente a $\alpha(m)$ con el número de ceros en un período simple y por lo tanto sigue que $l(m) = r(m) \cdot \alpha(m)$. □

En el siguiente teorema se muestra una forma de calcular el período en términos del rango $r(m)$, del orden de $s(m)$ y del orden de -1 módulo m que lo notaremos por $\gamma(m)$, esto se muestra a continuación.

Teorema 7. *$l(m) = gcd(2, \alpha(m)) \cdot lcm(r(m), \gamma(m))$, donde $\gamma(2) = 1$ y $\gamma(m) = 2$ para $m > 2$.*

Demostración. De la identidad 1-f tenemos que

$$F_{r(m)}^2 - F_{r(m)+1}F_{r(m)-1} = (-1)^{r(m)+1}$$

Dado que $F_{r(m)} \equiv 0 \pmod{m}$ y $F_{r(m)+1} \equiv F_{r(m)-1} \pmod{m}$, se sigue que

$$-F_{r(m)+1}^2 \equiv (-1)^{r(m)+1} \pmod{m}.$$

Esto es,

$$(s(m))^2 \equiv (-1)^{r(m)} \pmod{m}.$$

De ahí que $s(m)^2$ y $(-1)^{r(m)}$ tienen el mismo orden módulo m. Más precisamente

$$Ord_m(s(m)^2) = \frac{\alpha(m)}{gcd(2, \alpha(m))} = \frac{\gamma(m)}{gcd(r(m), \gamma(m))} = Ord_m((-1)^{r(m)}$$

de donde

$$l(m) = r(m) \cdot \alpha(m) = gcd(2, \alpha(m)) \cdot \frac{r(m) \cdot \gamma(m)}{gcd(r(m), \gamma(m))},$$
$$l(m) = gcd(2, \alpha(m)) \cdot lcm(r(m), \gamma(m)).$$

□

En la exploración computacional pueden apreciarse algunas regularidades con respecto al período, a continuación presentaremos dos corolarios que nos permiten estudiar formalmente la paridad del período y los posibles valores que toma el orden de $s(m)$.

Corolario 4. *$l(m)$ es par, para cada $m > 2$.*

Demostración. Si $l(m)$ es impar entonces $lcm[r(m), \gamma(m)]$ y $gcd(2, \alpha(m))$ deben ser impares. En particular, $lcm[r(m), \gamma(m)]$ es impar sólo cuando $m = 2$ y para todo $m > 2$ tenemos que $\gamma(m) = 2$, de ahí que $lcm[r(m), \gamma(m)]$ es par y en consecuencia $l(m)$ es par. □

Corolario 5. *$\alpha(m) = 1$ ó 2 ó 4*

Demostración. Del Teorema tenemos que

$$\begin{aligned} l(m) &= gcd(2, \alpha(m)) \cdot lcm[r(m), \gamma(m)] \\ &= (1 \text{ ó } 2) \cdot [r(m) \text{ ó } 2r(m)] \\ &= r(m) \text{ ó } 2r(m) \text{ ó } 4r(m). \end{aligned}$$

En virtud del teorema 6 se concluye que $\alpha(m) = 1$ ó 2 ó 4 para todo $m \in \mathbb{N}$. □

1.5. Residuos cuadráticos y Símbolo de Legendre

En el estudio de congruencias modulares surge el problema natural de encontrar un valor apropiado x que satisfaga la congruencia $x \equiv a \pmod{n}$. Pero el estudio de estas ecuaciones no se quedó ahí, tal como se desarrolla el estudio de ecuaciones usuales se pensó en modificar

la naturaleza de la ecuación. Surge entonces el estudio de ecuaciones cuadráticas y por tanto de residuos cuadráticos. Presentaremos un breve recorrido por los conceptos básicos y los que consideramos necesarios para el desarrollo de ideas en el capítulo posterior.

Definición 8. *Sean p un primo impar y a un entero tal que $gcd(a, p) = 1$. Si la congruencia cuadrática*

$$x^2 \equiv a \pmod{p}$$

tiene solución, decimos que a es un residuo cuadrático de p. De no tener solución decimos que a no es un residuo cuadrático de p.

Leonard Euler dió una caracterización para los residuos cuadráticos en términos de congruencias, esta caracterización se conoce como el *Criterio de Euler*.

Teorema 8. ***(Criterio de Euler)***
Sea p un primo impar y a un entero tal que $gcd(a, p) = 1$. Entonces a es un residuo cuadrático de p si y sólo si $a^{(p-1)/2} \equiv 1 \pmod{p}$.

Corolario 6. *Sean p un primo impar y a un entero tal que $gcd(a, p) = 1$. Entonces, a es un residuo cuadrático de p si y sólo si $a^{(p-1)/2} \equiv 1 \pmod{p}$ y no es un residuo cuadrático si y sólo si $a^{(p-1)/2} \equiv -1 \pmod{p}$.*

Definición 9. *Sean p un primo impar y a un entero tal que $gcd(a, p) = 1$. Entonces el símbolo de Legendre denotado por $(a|p)$, se define como*

$$(a|p) = \begin{cases} 1, & \text{si } a \text{ es un residuo cuadrático de } p \\ -1, & \text{si } a \text{ no es un residuo cuadrático de } p \end{cases}$$

Teorema 9. *Sea p un primo impar y sean a, b primos relativos. El símbolo de Legendre tiene las siguientes propiedades.*

a) Si $a \equiv b \pmod{p}$, *entonces* $(a|p) = (b|p)$.

b) $(a^2|p) = 1$.

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

d) $(ab|p) = (a|p)(b|p)$.

e) $(1|p) = 1$ *y* $(-1|p) = (-1)^{(p-1)/2}$.

Corolario 7. *Si p es un primo impar, entonces*

$$(-1|p) = \begin{cases} 1, & si \quad p \equiv 1 \pmod{4} \\ -1, & si \quad p \equiv 3 \pmod{4} \end{cases}$$

Teorema 10. *Si p es un primo impar entonces*

$$\sum_{a=1}^{p-1} (a|p) = 0,$$

por tanto hay $\frac{p-1}{2}$ *residuos cuadráticos y* $\frac{p-1}{2}$ *no residuos cuadráticos.*

Lema 1. *Si p es un primo impar y a un entero impar, con* $gcd(a, p) = 1$ *entonces*

$$(a|p) = (-1)^{\sum_{k=1}^{(p-1)/2} [ka/p]}$$

Teorema 11. ***(Ley de Reciprocidad cuadrática de Gauss)***
Si p y q son primos impares distintos entonces

$$(p|q)(q|p) = (-1)^{((p-1)/2)\times((q-1)/2)}$$

Usando este teorema y las propiedades del símbolo de Legendre se prueban los siguientes resultados.

Corolario 8. *Sean p y q primos impares y distintos. Entonces*

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

y,

$$(q|p) = \begin{cases} (p|q), & si \quad p \equiv 1 \pmod 4 \ o \ q \equiv 1 \pmod 4 \\ -(p|q), & si \quad p \equiv q \equiv 3 \pmod 4 \end{cases}$$

Los siguientes resultados aparecen como ejercicios propuestos en 1 en la página 190 y 209 respectivamente.

Proposición 2. *Sea p un primo impar y gcd*$(a, p) = gcd(b, p) = 1$. *Entonces de las siguientes tres congruencias*

$$x^2 \equiv a \pmod p, \quad x^2 \equiv b \pmod p, \quad x^2 \equiv ab \pmod p$$

todas tienen solución ó exactamente una de ellas admite solución.

Proposición 3. *Si p es un primo impar, entonces*

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

Capítulo 2

Números de Fibonacci y Lucas formados con sólo un dígito

En al año 2000 Florian Luca publicó un artículo ([3]) en el cual prueba que el mayor número con más de una cifra en la sucesión de Fibonacci formado con solo un dígito es el 55; y que el mayor número con más de una cifra en la sucesión de Lucas formado con solo un dígito es el 11. En este capítulo reescribiremos las pruebas de estos resultados con lujo de detalles, usando los conceptos teóricos del capítulo anterior.

Una prueba del resultado para la sucesión de Fibonacci fue publicada en 2012 usando *Formas lineales en logaritmos*, en esta prueba se obtienen cotas superiores para los números que están formados por solo un dígito, luego se encuentran computacionalmente estos números, obteniendo así el resultado.

2.1. Números con solo un dígito en la sucesión de Fibonacci

El resultado probado por F. Luca sobre los números de Fibonacci formados por un solo dígito se presenta a continuación.

Teorema 12. *Si*

$$F_n = a \cdot \frac{10^m - 1}{9}$$

para algún $0 \leq a \leq 9$*, entonces* $n = 0, 1, 2, 3, 4, 5, 6, 10$.

Demostración. En el apéndice *A* se verifica que los valores $n = 0, 1, 2, 3, 4, 5, 6, 10$ son los únicos enteros $0 \leq n \leq 20$ tal que

$$F_n = a \cdot \tfrac{10^m - 1}{9}$$

para algún $m \geq 1$ y $1 \leq a \leq 9$.
Algunos valores de $l(m)$ serán usados, estos pueden ser verificados en el apéndice *B* y los elementos que están en un período simple módulo *m* pueden ser verificados en el apéndice *C*.

Vamos a proceder por reducción al absurdo para probar el resultado. En adelante supondremos que $n \geq 21$, en particular $F_n \geq F_{21} = 10946 > 10^4$, luego $m \geq 5$. Consideraremos primero el caso $a = 5$ en el cual obtendremos una condición importante para *m*, lo cual facilitará sustancialmente el análisis de algunos casos.

Caso $a = 5$

En este caso

$$F_n = 5 \cdot \frac{10^m - 1}{9}$$

Como $10^4 \equiv 0 \pmod{16}$ y $m \geq 5$ entonces

$$10^m \equiv 0 \pmod{16}$$
$$10^m - 1 \equiv -1 \pmod{16}$$

El inverso multiplicativo de 9 módulo 16 es 9, así

$$9^{-1}(10^m - 1) \equiv 9^{-1}(-1) \pmod{16}$$
$$\frac{10^m - 1}{9} \equiv -9 \pmod{16}$$
$$\frac{10^m - 1}{9} \equiv 7 \pmod{16}$$

$$5 \cdot \frac{10^m - 1}{9} \equiv 3 \pmod{16}$$

Esto es, $F_n \equiv 3 \pmod{16}$.

Sabemos que $l(16) = 24$, y que entre esos 24 residuos el 3 aparece solo una vez. Como $F_4 = 3$ entonces $n \equiv 4 \pmod{24}$, esto es $n = 4 + 24t$, de donde $4 \mid n$. Por otro lado, usando el Corolario 2 podemos decir que $5 \mid n$ pues $5 \mid F_n$, así $20 \mid n$. Ahora como $l(11) = 10$ y $F_0 = 0$ entonces $F_n \equiv 0 \pmod{11}$. Es decir

$$11 \mid F_n = 5 \cdot \frac{10^m - 1}{9}$$

Dado que 11 y 5 son primos relativos se sigue $11 \mid \frac{10^m - 1}{9}$, y usando el criterio de divisibilidad por 11 concluimos que m debe ser par.

Por otro lado $l(3) = 8$, se puede ver que entre esos ocho residuos módulo 3 solo dos son múltiplo de 3, de hecho en los primeros números de la sucesión se ve que $F_0 = 0$ y $F_4 = 3$. Se concluye que si $t = 4k$ con k entero entonces $F_t \equiv 0 \pmod{3}$. Así

$$F_n \equiv 0 \pmod{3}.$$

Se sigue que $3 \mid \frac{10^m - 1}{9}$, y usando el criterio de divisibilidad por 3 obtenemos que m es múltiplo de 3, además es par, por lo tanto es múltiplo de 6. Ahora, si $m = 6r$ con r entero y dado que

$$10^6 \equiv 1 \pmod{7},$$

entonces

$$10^{6r} \equiv 1 \pmod{7},$$

$$10^m \equiv 1 \pmod{7},$$

$$10^m - 1 \equiv 0 \pmod{7}.$$

Por otro lado el inverso multiplicativo de 9 módulo 7 es 4, así

$$\frac{10^m - 1}{9} \equiv 0 \pmod{7}$$

Esto es $7 \mid F_n$. Por otro lado $l(7) = 16$ y en esos 16 residuos el cero aparece cada 8 términos, luego podemos afirmar ahora que $8 \mid n$. Ahora $n = 8t_1$ y $n = 24t - 4$ con t_1, t enteros positivos, igualando tenemos

$$24t - 4 = 8t_1,$$
$$6t - 1 = 2t_1.$$

Observemos que la parte izquierda es un número impar y la derecha es un número par, esto es imposible y por tanto $a \neq 5$.

Ahora sabemos que $a \neq 5$ y supongamos que m es par. Entonces $11 \mid \frac{10^m - 1}{9}$, del Corolario 2 se sigue que $r(11) = 10 \mid n$. Usando la identidad 1-b se verifica que $5 \mid F_{10} \mid F_n$, así

$$5 \mid a \cdot \frac{10^m - 1}{9}$$

como $gcd\left(5, \frac{10^m - 1}{9}\right) = 1$, entonces $5 \mid a$ lo cual es imposible pues $a \neq 5$. De esta forma concluimos que m debe ser impar, hecho que asumiremos en los demás casos de la prueba.

Caso $a = 1$

En este caso tenemos

$$F_n = \frac{10^m - 1}{9}$$

Como $m \geq 5$, entonces $10^m - 1 \equiv -1 \pmod{16}$ y dado que el inverso multiplicativo de 9 módulo 16 es 9, tenemos:

$$\frac{10^m - 1}{9} \equiv 7 \pmod{16}.$$

Sabemos que $l(16) = 24$ y observando los residuos módulo 16 concluimos que $n \equiv 10 \pmod{24}$, de ahí que n es par, por tanto existen enteros k y t tales que:

$$n \equiv 10 \pmod{24} \text{ y } n = 2k$$

implica

$$2k - 10 = 24t,$$
$$k - 5 = 12t,$$
$$k \equiv 5 \pmod{12},$$

Ahora de la identidad 1-c,

$$F_{2k} = F_k \cdot L_k = \frac{10^m - 1}{9}$$

Usando la identidad 1-e y el hecho de que k es impar concluimos que

$$L_k^2 - 5F_k^2 = -4.$$

Sea p un divisor primo de L_k, claramente $p \neq 2$ y $p \neq 5$.

$$-5F_k^2 \equiv -4 \pmod{p},$$

de donde,

$$(5F_k)^2 \equiv 20 \pmod{p}$$

Por lo tanto la congruencia $x^2 \equiv 20 \pmod{p}$ tiene solución, y dado que la congruencia $x^2 \equiv 4 \pmod{p}$ tiene solución, en virtud de la proposición 2 se deduce que la congruencia $x^2 \equiv 5 \pmod{p}$ tiene solución. Por otro lado, usando la Ley de Reciprocidad Cuadrática de Gauss encontramos que $(5|p) = (p|5)$. Esto implica que $(p|5) = (5|p) = 1$. Escribamos $L_k = p_1 \cdot p_2 \cdot p_3 \cdot p_s$, como p es un primo arbitrario que divide a L_k se sigue que $(p_i|5) = 1$, para todo $1 \leq i \leq s$. Por el literal d del teorema 9 tenemos que

$$(L_k|5) = (p_1|5) \cdot (p_2|5) \cdot (p_3|5) \cdots (p_s|5)$$

de donde,

$$(L_k|5) = 1. \tag{2.1}$$

Ahora, sea p un divisor primo de F_k y como $L_k^2 - 5F_k^2 = -4$, entonces:

$$L_k^2 \equiv -4 \pmod{p}$$

Esto implica que la congruencia $x^2 \equiv -4 \pmod{p}$ tiene solución, y dado que la congruencia $x^2 \equiv 4 \pmod{p}$ tiene solución, de la proposición 2 la congruencia $x^2 \equiv -1 \pmod{p}$ tiene solución, de donde $(-1|p) = 1$, así del Corolario 7, $p \equiv 1 \pmod{4}$. Escribamos ahora

$$F_k = \prod_{i=1}^{t} \left(p_i^{\alpha_i}\right) \cdot \prod_{j=1}^{s} \left(q_j^{\beta_j}\right) \tag{2.2}$$

Para $t \geq 0$ y $s \geq 0$, donde p_i y q_j son primos distintos de tal forma que $p_i \equiv 1 \pmod 8$ para todo $i = 1, 2, \ldots, t$ y $q_j \equiv 5 \pmod 8$ para todo $j = 1, 2, \ldots, s$. Por otro lado si p es un primo divisor de F_k, entonces $p \mid (10^m - 1)$, de ahí que $10^m \equiv 1 \pmod p$. Como m es impar podemos reescribir la congruencia así

$$10 \cdot \left(10^{(m-1)/2}\right)^2 \equiv 1 \pmod p,$$
$$\left(10 \cdot 10^{(m-1)/2}\right)^2 \equiv 10 \pmod p,$$

de donde $(10|p) = 1$.

Si $p = p_i \equiv 1 \pmod 8$, del Corolario 8 sigue que $(2|p_i) = 1$. Luego del literal *d* del teorema 9 tenemos que $(5|p_i) = 1$, así por la Ley de Reciprocidad Cuadrática de Gauss $(p_i|5) = 1$.

Si $p = q_j \equiv 5 \pmod 8$, del Corolario 8 que $(2|q_j) = -1$. Luego del literal *d* del teorema 9 tenemos que $(5|q_j) = -1$, así por la Ley de Reciprocidad Cuadrática de Gauss $(q_j|5) = -1$. Usando un argumento análogo con las ecuaciones 2.1 y 2.2 obtenemos que

$$\left(\frac{F_n}{5}\right) = \left(\frac{F_k \cdot L_k}{5}\right) = \left(\frac{F_k}{5}\right) \cdot \left(\frac{L_k}{5}\right) = \left(\frac{F_k}{5}\right) = (-1)^{\sum_{j=1}^{s} \beta_j}$$

Por otro lado, como

$$10^m \equiv 0 \pmod 5,$$
$$10^m - 1 \equiv 4 \pmod 5,$$

el inverso multiplicativo de 9 módulo 5 es 4, así

$$F_n = \frac{10^m - 1}{9} \equiv 1 \pmod 5$$

Ahora $F_n^2 \equiv 1 \pmod 5$, de aquí que $(F_n|5) = 1$. Esto implica que $\sum_{j=1}^{s} \beta_j$ es par. Dado que el producto de dos enteros de la forma $8k + 1$ es de la misma forma y el producto de dos enteros de la forma $8k + 5$ es de la forma $8k + 1$. Se sigue que $F_k \equiv 1 \pmod 8$. Sabemos que $l(8) = 12$ y recordando que $k \equiv 5 \pmod{12}$ tenemos que

$$F_k \equiv F_5 \equiv 5 \pmod 8$$

Lo cual es contradictorio, por lo tanto este caso es imposible.

Caso $a = 2$

En este caso tenemos

$$F_n = 2 \cdot \frac{10^m - 1}{9}$$

Como $10^4 \equiv 0 \pmod{16}$ y $m \geq 5$, entonces

$$10^m \equiv 0 \pmod{16},$$

$$10^m - 1 \equiv -1 \pmod{16}$$

Dado que el inverso multiplicativo de 9 módulo 16 es precisamente el mismo, tenemos que:

$$9^{-1}(10^m - 1) \equiv 9^{-1}(-1) \pmod{16},$$

$$\frac{10^m - 1}{9} \equiv -9 \pmod{16},$$

$$\frac{10^m - 1}{9} \equiv 7 \pmod{16},$$

$$2 \cdot \frac{10^m - 1}{9} \equiv -2 \pmod{16},$$

Así

$$F_n \equiv -2 \pmod{16}.$$

Dado que $l(16) = 24$ y que ninguno de los residuos en el período es 14, es decir no existe $0 \leq k \leq 23$ tal que $F_k \equiv -2 \equiv 14 \pmod{16}$, este caso es imposible.

Caso $a = 3$

En este caso, tenemos

$$F_n = 3 \cdot \frac{10^m - 1}{9},$$

de ahí que $3 \mid F_n$, y en virtud del Corolario 2 $r(3) = 4 \mid n$. Ahora, como

$$\frac{10^m - 1}{9} \equiv 7 \pmod{16},$$
$$3\frac{10^m - 1}{9} \equiv 5 \pmod{16}$$

Entonces $F_n \equiv 5 \pmod{16}$. Sabemos que $l(16) = 24$ y verificamos en el apéndice C que el único valor de n $(0 \leq n \leq 23)$ tal que $F_n \equiv 5 \pmod{16}$ y $4 \mid n$ es $n = 8$. En general, si $F_n \equiv 5 \pmod{16}$ y $4 \mid n$ entonces $n \equiv 8 \pmod{24}$, de donde $8 \mid n$. Como $F_m \mid F_{m \cdot n}$, en particular tenemos que:

$$7 \mid F_8 = 21 \mid F_n = 3 \cdot \frac{10^m - 1}{9}$$

Ahora 3 y 7 son primos relativos entonces $7 \mid (10^m - 1)$, luego por el criterio de divisibilidad por 7 tenemos que $\underbrace{1 + 3 \times 1 + 2 \times 1 - 1 - 3 \times 1 - 2 \times 1 + \cdots}_{m-sumandos}$ debe ser múltiplo de 7, lo cual ocurre solo cuando m es múltiplo de 6 y esto no es posible dado que m es impar.

Caso $a = 4$

En este caso,

$$F_n = 4 \cdot \frac{10^m - 1}{9}$$

De aquí que $4 \mid F_n$, se sigue que $r(4) = 6 \mid n$. Esto implica que

$$8 = F_6 \mid F_n = 4 \cdot \frac{10^m - 1}{9},$$

y en consecuencia $2 \mid \frac{10^m - 1}{9}$, lo cual es imposible pues $\frac{10^m - 1}{9}$ es impar.

Caso $a = 6$

En este caso,

$$F_n = 6 \cdot \frac{10^m - 1}{9},$$

Luego $6 \mid F_n$, de donde $r(6) = 12 \mid n$. Se tiene entonces que:

$$16 \mid F_{12} \mid F_n = 6 \cdot \frac{10^m - 1}{9},$$

y en consecuencia $8 \mid 3 \cdot \frac{10^m-1}{9}$. Como 3 y 8 son primos relativos tenemos que $8 \mid \frac{10^m-1}{9}$, en particular $2 \mid \frac{10^m-1}{9}$ lo cual imposible pues $\frac{10^m-1}{9}$ es impar.

Caso $a = 7$

En este caso tenemos

$$F_n = 7 \cdot \frac{10^m - 1}{9},$$

Como $7 \mid F_n$ entonces $r(7) = 8 \mid n$. Por otro lado

$$\frac{10^m - 1}{9} \equiv 7 \pmod{16},$$

$$7\frac{10^m - 1}{9} \equiv 1 \pmod{16}.$$

Sabemos que $l(16) = 24$ y dado que $F_n \equiv 1 \pmod{16}$ entonces $n \equiv 1, 2 \text{ ó } 23 \pmod{16}$, esto contradice el hecho que $8 \mid n$. Por tanto este caso resulta imposible.

Caso $a = 8$

En este caso tenemos

$$F_n = 8 \cdot \frac{10^m - 1}{9}$$

De aquí que $8 \mid F_n$, esto implica que $r(8) = 6 \mid n$. Como $10^5 \equiv 0 \pmod{32}$ y $m \geq 5$, se sigue que

$$10^m \equiv 0 \pmod{32},$$

$$10^m - 1 \equiv -1 \pmod{32},$$

Por otro lado el inverso multiplicativo de 9 módulo 32 es 25, así

$$9^{-1}(10^m - 1) \equiv 9^{-1}(-1) \pmod{32},$$

$$\frac{10^m - 1}{9} \equiv -25 \pmod{32},$$

$$\frac{10^m - 1}{9} \equiv 7 \pmod{32},$$

$$8 \cdot \frac{10^m - 1}{9} \equiv 24 \pmod{32},$$

Sabemos que $l(32) = 48$ y que $F_n \equiv 24 \pmod{32}$ solo cuando $n \equiv 18$ ó $42 \pmod{48}$. Supongamos primero que $n \equiv 42 \pmod{48}$, entonces $n - 42 = 48k$ con $k \in \mathbb{Z}$ en los enteros, esto implica que $n = 10 + 16(3k + 2)$, así $n \equiv 10 \pmod{16}$. Sabemos que $l(7) = 16$, luego $F_n \equiv F_{10} \equiv -1 \pmod{7}$.

Como $F_n = 8 \cdot \frac{10^m - 1}{9} \equiv -1 \pmod{7}$ y 7 8 son primos relativos, entonces $\frac{10^m - 1}{9} \equiv -1 \pmod{7}$. Observemos que

$$\frac{10^m - 1}{9} + 1 = \underbrace{111\ldots12}_{m-cifras}$$

del criterio de divisibilidad por 7, concluimos que esto sucede solo cuando $m \equiv 3 \pmod{6}$. En particular $3 \mid m$ y como $\frac{10^m - 1}{9}$ es un número con m unos (1's) entonces $3 \mid \frac{10^m - 1}{9} \mid 8 \cdot \frac{10^m - 1}{9} = F_n$. En virtud del Corolario 2 obtenemos que $r(3) = 4 \mid n$, lo cual contradice que $n \equiv 42 \pmod{48}$.

Ahora, supongamos que $n \equiv 18 \pmod{48}$. Se sigue que $n - 18 = 48k$ con k entero, $n - 2 = 16(3k) + 16 = 16(3k + 1)$, esto es $n \equiv 2 \pmod{16}$. Sabemos que $l(7) = 16$ podemos afirmar que $F_n \equiv F_2 \equiv 1 \pmod{7}$.

Como $F_n = 8 \cdot \frac{10^m - 1}{9} \equiv 1 \pmod{7}$ y 7 y 8 son primos relativos, entonces $\frac{10^m - 1}{9} \equiv 1 \pmod{7}$. Note que $\frac{10^m - 1}{9} - 1 = \underbrace{111\ldots10}_{m-cifras}$, es un número divisible por 7 solo cuando $m \equiv 1 \pmod{6}$. Por otro lado $n \equiv 2 \pmod{8}$ y como $l(3) = 8$, se sigue $F_n \equiv F_2 \equiv 1 \pmod{3}$, es decir

$$8 \cdot \frac{10^m - 1}{9} \equiv 1 \pmod{3},$$
$$16 \cdot \frac{10^m - 1}{9} \equiv 2 \pmod{3}$$

y como $16(-1) \equiv 2 \pmod{3}$ se sigue que

$$16 \cdot \frac{10^m - 1}{9} \equiv 16(-1) \pmod{3}$$

y como $gcd(16, 3) = 1$ entonces

$$\frac{10^m - 1}{9} \equiv -1 \equiv 2 \pmod{3}$$

Usando el criterio de divisibilidad por 3 se tiene que $m \equiv 2 \pmod 3$. Como m es impar se sigue que $m \equiv 5 \pmod 6$, esto contradice el hecho que $m \equiv 1 \pmod 6$.

Con lo probado concluimos que este caso es imposible.

Caso $a = 9$

En este caso tenemos

$$F_n = 9 \cdot \frac{10^m - 1}{9}$$

De ahí que $9 \mid F_n$, esto implica que $r(9) = 12 \mid n$. Ahora

$$18 \mid F_{12} \mid F_n = 9 \cdot \frac{10^m - 1}{9}$$

Esto implica que $2 \mid \frac{10^m - 1}{9}$, lo cual es imposible. □

2.2. Números con solo un dígito en la sucesión de Lucas

Comenzaremos probando el siguiente Lema, que nos permitirá simplificar el análisis en la prueba del resultado principal de esta sección.

Lema 2. *Si*

$$L_n = a \cdot \frac{10^m - 1}{9}$$

para algún $m \geq 3$ y $1 \leq a \leq 9$, entonces n es impar.

Demostración. Supongamos que n es par y probemos que esto implica que m es impar. Procedamos por contradicción y supongamos que m es par. En este caso

$$10^2 \equiv 1 \pmod{11} \Longrightarrow 10^m \equiv 1^{m/2} \pmod{11}$$

$$10^m - 1 \equiv 0 \pmod{11} \Longrightarrow \frac{10^m - 1}{9} \equiv 0 \pmod{11}$$

De ahí que $11 \mid L_n$. Como $l'(11) = 10$, $L_5 = 11$, y $L_i \not\equiv 0 \pmod{11}$ para todo $i \in \{0, 1, 2, 3, 4, 6, 7, 8, 9\}$, entonces $n \equiv 5 \pmod{10}$ y esto contradice el supuesto que n es par. Por lo tanto m es impar.

Dado que n es par, se puede escribir de la forma $n = 2k$.

Se sigue de la identidad 1.d que

$$L_n = L_{2k} = L_k^2 \pm 2 = a \cdot \frac{10^m - 1}{9}$$

El signo dependerá de si k es impar o par respectivamente.Sea p un divisor arbitrario de $\frac{10^m - 1}{9}$ Claramente p es impar y $p \neq 5$. Entonces, si k es impar tenemos

$$L_k^2 + 2 \equiv 0 \pmod{p},$$

$$L_k^2 \equiv -2 \pmod{p}$$

Se sigue que $(-2|p) = 1$. Se sigue de la proposición 3 que $p \equiv 1, 3 \pmod 8$. Como p es un primo arbitrario que divide a $\frac{10^m-1}{9}$ es cierto que

$$\frac{10^m - 1}{9} \equiv 1, 3 \pmod 8$$

Como $m \geq 3$, veamos de otra manera que

$$10^3 \equiv 0 \pmod 8,$$

$$10^m \equiv 0 \pmod 8,$$

$$10^m - 1 \equiv -1 \pmod 8.$$

El inverso multiplicativo de 9 módulo 8 es 1, de donde

$$\frac{10^m - 1}{9} \equiv -1 \pmod 8$$

Lo cual es contradictorio.

Si k es par tenemos

$$L_k^2 - 2 \equiv 0 \pmod{p}$$

$$L_k^2 \equiv 2 \pmod{p}$$

De ahí que $(2 \mid p) = 1$. Ahora, como $10^m - 1 \equiv 0 \pmod{p}$ y m es impar tenemos que

$$10\left(10^{(m-1)/2}\right)^2 \equiv 1 \pmod{p},$$
$$\left(10 \cdot 10^{(m-1)/2}\right)^2 \equiv 10 \pmod{p}.$$

De donde $(10|p) = 1$ y como $(2|p) = 1$, entonces $(5|p) = 1$.

Ahora de la propiedad 1-e,

$$L_n^2 - 5F_n^2 = 4$$

Esto es

$$-5F_n^2 \equiv 4 \pmod{p},$$
$$(5 \cdot F_n)^2 \equiv -20 \pmod{p}$$

De ahí que $(-20|p) = 1$ y sabemos que $(4|p) = 1$, por tanto $(-5|p) = 1$. Ahora como $(5|p) = 1$ y $(-5|p) = 1$, entonces $(-1|p) = 1$. De la proposición 7 $p \equiv 1 \pmod{4}$, además $(2|p) = 1$, de la proposición 8 tenemos que $p \equiv 1 \pmod{8}$. Teniendo en cuenta que p es un primo arbitrario que divide a $(10^m - 1)/9$,

$$\frac{10^m - 1}{9} \equiv 1 \pmod{8}.$$

De otra forma, dado que $m \geq 3$,

$$10^3 \equiv 0 \pmod{8},$$

$$10^m \equiv 0 \pmod{8},$$

$$10^m - 1 \equiv -1 \pmod{8},$$

$$\frac{10^m - 1}{9} \equiv -1 \pmod{8}.$$

Lo cual es contradictorio. Por lo tanto n debe ser impar. □

El resultado probado por F. Luca sobre los números de Lucas formados por un solo dígito se presenta a continuación.

Teorema 13. *Si*

$$L_n = a \cdot \frac{10^m - 1}{9}$$

para algún $0 \leq a \leq 9$*, entonces* $n = 0, 1, 2, 3, 4, 5$.

Demostración. Verificamos en la tabla del apéndice A que los valores $n = 0, 1, 2, 3, 4, 5$ son los únicos que toma $n \leq 19$ tal que

$$L_n = a \cdot \frac{10^m - 1}{9}$$

para algún $m \geq 1$ y $1 \leq a \leq 9$.

Vamos a proceder por reducción al absurdo. En adelante supondremos que $n \geq 20$, en particular $L_n \geq L_{20} = 15127 > 10^4$, encontramos que $m \geq 5$. Los valores usados de $l'(m)$ pueden verificarse en el apéndice D y los residuos módulo m de la sucesión de Lucas puedes observarse en 3.

Caso $a = 1$

En este caso,

$$L_n = \frac{10^m - 1}{9}$$

Como $m \geq 5$, entonces

$$10^4 \equiv 0 \pmod{16},$$

$$10^m \equiv 0 \pmod{16},$$

$$10^m - 1 \equiv -1 \pmod{16}$$

El inverso multiplicativo de 9 módulo 16 es 9, así

$$\frac{10^m - 1}{9} \equiv -9 \pmod{16}$$

$$\frac{10^m - 1}{9} \equiv 7 \pmod{16}$$

Esto sucede solo cuando $n \equiv 4, 11, 20 \pmod{24}$. Como n es impar, entonces $n \equiv 11 \pmod{24}$, esto es $n = 11 + 24k$ con k entero, de ahí que $n \equiv 3 \pmod{8}$.

Sabemos que $l'(3) = 8$, y como $L_3 \equiv 1 \pmod{8}$ se sigue que

$$L_n \equiv L_3 \equiv 1 \pmod{3}$$

Del criterio de divisibilidad por 3 $m \equiv 1 \pmod{3}$. Consideremos ahora dos casos:

1. m es impar. En este caso $m \equiv 1 \pmod{6}$. Entonces,

$$10 \equiv 3 \pmod{7},$$

$$10^7 \equiv 3 \pmod{7},$$

$$10^m \equiv 3 \pmod{7},$$

$$10^m - 1 \equiv 2 \pmod{7},$$

El inverso multiplicativo de 9 módulo 7 es 4, así

$$\frac{10^m - 1}{9} \equiv 1 \pmod{7},$$

Sabemos que $l'(7) = 16$ y que $L_n \equiv 1 \pmod{7}$, verificamos en el apéndice E que esto solo sucede cuando $n \equiv 1, 7 \pmod{16}$. En particular $n \equiv 1, 7 \pmod{8}$ lo cual contradice que $n \equiv 3 \pmod{8}$.

2. m es par. En este caso $m \equiv 4 \pmod{6}$. Entonces,

$$10^4 \equiv 4 \pmod{7},$$

$$10^{10} \equiv 4 \pmod{7},$$

$$10^m \equiv 4 \pmod{7},$$

$$10^m - 1 \equiv 3 \pmod{7},$$

El inverso multiplicativo de 9 módulo 7 es 4, así

$$\frac{10^m - 1}{9} \equiv 5 \pmod{7}$$

Sabemos que $l'(7) = 16$ y verificamos en el apéndice E que para todo $0 \geq k \geq 16$ $L_n \not\equiv 5 \pmod 7$. Por lo tanto este caso es imposible.

Caso $a = 2$

En este caso,

$$L_n = 2 \cdot \frac{10^m - 1}{9}.$$

Como $m \geq 3$ entonces

$$10^m \equiv 0 \pmod 4,$$

$$10^m - 1 \equiv -1 \pmod 4,$$

El inverso multiplicativo de 9 módulo 4 es 1, así

$$\frac{10^m - 1}{9} \equiv -1 \pmod 4,$$
$$2 \cdot \frac{10^m - 1}{9} \equiv 2 \pmod 4.$$

Verificamos en el apéndice E que $L_n \equiv 2 \pmod 4$ si y solo si $n \equiv 0 \pmod 6$, esto implica que $6 \mid n$, lo cual es imposible pues n es impar.

Caso $a = 3$

En este caso,

$$L_n = 3 \cdot \frac{10^m - 1}{9}$$

En particular $3 \mid L_n$. Verificamos en el apéndice D que $r'(3) = 2$ y por tanto $2 \mid n$. Esto último es imposible pues según el lema n es impar.

Caso $a = 4$

En este caso,

$$L_n = 4 \cdot \frac{10^m - 1}{9}$$

En particular L_n es múltiplo de 4. Verificamos en el apéndice E que esto sucede solo cuando $n = 3k$ con k impar.

Más aun, como

$$10^4 \equiv 0 \pmod{16},$$

$$10^m - 1 \equiv -1 \pmod{16}$$

El inverso multiplicativo de 9 módulo 16 es 9, así

$$\frac{10^m - 1}{9} \equiv 7 \pmod{16},$$
$$4 \cdot \frac{10^m - 1}{9} \equiv -4 \pmod{16},$$

Esto es $L_n = 4 \cdot \frac{10^m - 1}{9} \equiv -4 \pmod{16}$. Pero esto sucede solo cuando $n \equiv 9, 21 \pmod{24}$. En particular $n \equiv 1 \pmod{4}$.

Por otro lado, como

$$10 \equiv 0 \pmod{5},$$

$$10^m - 1 \equiv -1 \pmod{5}$$

El inverso multiplicativo de 9 módulo 5 es 4, así

$$\frac{10^m - 1}{9} \equiv 1 \pmod{5},$$
$$4 \cdot \frac{10^m - 1}{9} \equiv 4 \pmod{5}$$

Esto es $L_n = 4 \cdot \frac{10^m - 1}{9} \equiv 4 \pmod{5}$. Sabemos que $l'(5) = 4$ y verificamos que $L_n \equiv 4 \pmod{5}$ solo cuando $n \equiv 3 \pmod{4}$. Esto contradice que $n \equiv 1 \pmod{4}$ por lo tanto este caso es imposible.

Caso $a = 5$

En este caso,

$$L_n = 5 \cdot \frac{10^m - 1}{9}$$

En particular $5 \mid L_n$. Verificamos en el apéndice E que $5 \nmid L_k$ para todo $k \geq 0$, por lo tanto este caso es imposible.

Caso $a = 6$

En este caso,

$$L_n = 6 \cdot \frac{10^m - 1}{9}$$

En particular $6 \mid L_n$. Verificamos en el apéndice D que $r'(6) = 6$ y por tanto $6 \mid n$. Esto último es imposible pues n es impar.

Caso $a = 7$

En este caso,

$$L_n = 7 \cdot \frac{10^m - 1}{9}$$

En particular $7 \mid L_n$. Verificamos en el apéndice D que $r'(7) = 4$ y por tanto $4 \mid n$. Esto último es imposible pues n es impar.

Caso $a = 8$

En este caso,

$$L_n = 8 \cdot \frac{10^m - 1}{9}$$

En particular $8 \mid L_n$. Verificamos en el apéndice E que $L_k \not\equiv 0 \pmod 8$ para todo $k \geq 0$, por lo tanto este caso es imposible.

Caso $a = 9$

En este caso tenemos

$$L_n = 9 \cdot \frac{10^m - 1}{9}$$

En particular $9 \mid L_n$. Verificamos en el apéndice D que $r'(9) = 6$ y por tanto $6 \mid n$. Esto último es imposible pues n es impar. □

2.3. Resultados Análogos Tras Variación De Condiciones

En las secciones 2.1 y 2.2 mostramos en detalle la prueba de los siguientes resultados

1. Si
$$F_n = a \cdot \frac{10^m - 1}{9}$$
para algún $0 \leq a \leq 9$, entonces $n = 0, 1, 2, 3, 4, 5, 6, 10$.

2. Si
$$L_n = a \cdot \frac{10^m - 1}{9}$$
para algún $0 \leq a \leq 9$, entonces $n = 0, 1, 2, 3, 4, 5$.

Resulta natural preguntarnos si estos resultados son producto de la ocurrencia conjunta de factores favorables, o por el contrario se pueden encontrar resultados análogos variando las condiciones “ambientales” de los números que forman estas sucesiones.

En primer lugar analicemos la variación de los elementos iniciales en una sucesión de Fibonacci generalizada. Una sucesión de Fibonacci generalizada es una sucesión de números enteros con términos iniciales g_0 y g_1 y la notaremos por G_n. Claramente si al menos uno de los términos iniciales (g_0 o g_1) son dígitos, entonces existe al menos un número formado por solo un dígito, a saber g_0 o g_1. Usando el algoritmo 7 del apéndice F, podemos observar que tomando un número n de términos de la sucesión en base 10 y tomando g_0 y g_1 dígitos, no siempre encontramos números con más de una cifra formados con solo un dígito. Por ejemplo, si tomamos $g_0 = g_1 = 3$ y $n = 5000$, encontramos que el mayor número(entre los primeros 5000 términos) formado por solo un dígito es el 9.

Ahora supongamos que ni g_0 ni g_1 son dígitos y exploremos computacionalmente la existencia de un resultado análogo a los que se presentan en los teoremas 12 y 13. Para esta exploración usaremos $n = 10^4$, $m = 10$ y $10 \leq g_0, g_1 \leq 20$.

Por comodidad en la lectura de las tablas denotaremos por $M_{F(b)}$ al mayor número de Fibonacci en base b, por $M_{L(b)}$ al mayor número de Lucas en base b. Con la letra F indicaremos que el término pertenece a la sucesión de Fibonacci y con la letra L indicaremos que el término pertenece a la sucesión de Lucas. Usaremos los primeros 5000 términos de cada sucesión.
En la siguiente tabla se resumen los resultados obtenidos. Claramente en estos casos los números de las bases no necesariamente son dígitos, sin embargo nos referiremos a ellos como "dígitos". Cuando el algoritmo no encuentra ningún número con las condiciones especificadas imprime NE (No Encontró).

(g_0, g_1)	$M_{F(10)}$	(g_0, g_1)	$M_{F(10)}$	(g_0, g_1)	$M_{F(10)}$	(g_0, g_1)	$M_{F(10)}$
(10,10)	NE	(11,17)	11	(13,17)	77	(16,16)	NE
(10,11)	11	(11,18)	11	(13,18)	NE	(16,17)	33
(10,12)	22	(11,19)	11	(13,19)	NE	(16,18)	NE
(10,13)	NE	(11,20)	11	(13,20)	33	(16,19)	NE
(10,14)	NE	(12,12)	NE	(14,14)	NE	(16,20)	NE
(10,15)	NE	(12,13)	NE	(14,15)	44	(17,17)	NE
(10,16)	NE	(12,14)	66	(14,16)	NE	(17,18)	88
(10,17)	44	(12,15)	111	(14,17)	333	(17,19)	55
(10,18)	NE	(12,16)	44	(14,18)	NE	(17,20)	NE
(10,19)	77	(12,17)	NE	(14,19)	222	(18,18)	NE
(10,20)	NE	(12,18)	NE	(14,20)	88	(18,19)	NE
(11,11)	88	(12,19)	555	(15,15)	NE	(18,20)	NE
(11,12)	11	(12,20)	NE	(15,16)	NE	(19,19)	NE
(11,13)	11	(13,13)	NE	(15,17)	NE	(19,20)	NE
(11,14)	11	(13,14)	NE	(15,18)	33	(20,20)	NE
(11,15)	11	(13,15)	NE	(15,19)	NE		
(11,16)	11	(13,16)	NE	(15,20)	55		

Tras esta exploración computacional concluimos que la variación de los términos iniciales g_0 y g_1 afectan la existencia de números formados con sólo un “dígito” en una sucesión de Fibonacci generalizada.

Ahora vamos a considerar el problema de determinar si una sucesión de Fibonacci generalizada expresada en un sistema numérico en base *b* posee un elemento máximo que este formado por solo un “dígito”. Para analizar esta situación, usaremos nuevamente el algoritmo 7 del apéndice F, con el cual construiremos *n* términos de la sucesión de Fibonacci y de Lucas, posteriormente pasaremos los números de estas sucesiones a base *m* y examinaremos cuáles de estos números en base *m* están formados con sólo un “dígito”.

Para ilustrar esto consideremos los primeros términos de la sucesión de Fibonacci en base 4 y denotemos por $F_{n,b}$ al n-ésimo término de la sucesión de Fibonacci visto en base *b*.

F_n	1	1	2	3	5	8	13	21	34	55	89
$F_{n,4}$	[1]	[1]	[2]	[3]	[1,1]	[0,2]	[1,3]	[1,1,1]	[2,0,2]	[3,1,3]	[1,2,1,1]

Los números expresados en un sistema numérico en base *b* los escribiremos en corchetes y separando los “dígitos” mediante comas, así evitaremos confusiones cuando las bases consideradas sean mayores que 10 y los “dígitos” no sean lo números del conjunto $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

En la siguientes tablas se resumen los resultados encontrados en la exploración computacional.

Resultados para la sucesión de Fibonacci.

Base *b*	F	$M_{F(b)}$	Base *b*	F	$M_{F(b)}$
2	3	[1,1]	17	144	[8,8]
3	13	[1,1,1]	18	13	[13]
4	21	[1,1,1]	19	13	[13]

5	3	[3]	20	21	[21]
6	21	[3,3]	21	13	[13]
7	8	[1,1]	22	21	[21]
8	5	[5]	23	144	[6,6]
9	8	[8]	24	21	[21]
10	55	[5,5]	25	21	[21]
11	8	[8]	26	21	[21]
12	13	[1,1]	27	21	[21]
13	8	[8]	28	377	[13,13]
14	13	[13]	29	21	[21]
15	144	[9,9]	30	21	[21]
16	34	[2,2]	31	21	[21]

Resultados para la sucesión de Lucas.

Base b	L	$M_{L(b)}$	Base b	L	$M_{L(b)}$
2	7	[1,1,1]	17	18	[1,1]
3	4	[1,1]	18	76	[4,4]
4	3	[3]	19	18	[18]
5	18	[3,3]	20	18	[18]
6	7	[1,1]	21	18	[18]
7	4	[4]	22	322	[14,14]
8	18	[2,2]	23	18	[18]
9	7	[7]	24	18	[18]
10	11	[1,1]	25	18	[18]
11	7	[7]	26	18	[18]
12	11	[11]	27	18	[18]
13	11	[11]	28	29	[1,1]

14	11	[11]	29	18	[18]
15	11	[11]	30	29	[29]
16	11	[11]	31	29	[29]

Después de estas exploraciones computacionales concluimos que al parecer podemos establecer resultados análogos a los teoremas 12 y 13. Sin embargo, en varias bases numéricas podemos encontrar resultados muy poco interesantes, pues los mayores números encontrados son menores que la base. En algunas otras bases numéricas se pueden encontrar resultados interesantes. Por ejemplo en la sucesión de Fibonacci en base 28 se encuentra que el mayor, al menos entre los primeros 5,000 términos, es el 377 que se escribe como $[13, 13]$, y en base 6 se encuentra que el el mayor es 21 que se escribe $[3, 3]$.

Un trabajo interesante sería tratar de probar algunos de los hechos observados en las tablas, es decir, probar por ejemplo que los mayores números de Lucas y Fibonacci en base 2 formados con solo un dígitos son $7([1, 1, 1])$ y $3([1, 1])$ respectivamente.

Capítulo 3

Conclusiones y Problemas abiertos

Como vimos en la sección 1.4, un período simple en la sucesión de residuos de la sucesión de Fibonacci vista módulo *m*, puede ser caracterizado usando el rango de aparición de módulo. Si bien la sucesión de Lucas es periódica, este período no puede depender del rango de aparición del módulo como se mostró para Fibonacci, pues existen infinitos números que no dividen a ningún número de Lucas, esto nos lleva a plantearnos las siguientes preguntas:

¿Es posible caracterizar los números que no dividen a ningún número de Lucas?

¿Puede establecerse una fórmula que permita calcular el período para los residuos de la sucesión de Lucas vista módulo *m*?

Dada la fuerte relación entre las sucesiones de Lucas y de Fibonacci, es natural pretender asociar los períodos para un mismo módulo *m*. En los resultados obtenidos en los apéndices **B** y **D**, se puede ver que comparando computacionalmente los períodos de la sucesión de Lucas y Fibonacci, que estos períodos son iguales en 4 de cada 5 de ellos, más precisamente conjeturamos el siguiente resultado.

Conjetura 3. *Los períodos de las sucesiones de Lucas y Fibonacci modulo m, son iguales excepto cuando el m es múltiplo de* 5*, en tales casos el período para Fibonacci es cinco veces mayor.*

Apéndice A

Primeros 30 Números de Fibonacci y de Lucas

n	F_n			L_n		
1	1			1		
2	1			3		
3	2			4	=	2^2
4	3			7		
5	5			11		
6	8	=	2^3	18	=	$2 \cdot 3^2$
7	13			29		
8	21	=	$3 \cdot 7$	47		
9	34	=	$2 \cdot 17$	76	=	$2^2 \cdot 19$
10	55	=	$5 \cdot 11$	123	=	$3 \cdot 41$
11	89			199		
12	144	=	$2^4 \cdot 3^2$	322	=	$2 \cdot 7 \cdot 23$
13	233			521		
14	377	=	$13 \cdot 29$	843	=	$3 \cdot 281$
15	610	=	$2 \cdot 5 \cdot 61$	1364	=	$2 \cdot 11 \cdot 31$
16	987	=	$3 \cdot 7 \cdot 47$	2207		
17	1597			3571		
18	2584	=	$2^3 \cdot 17 \cdot 19$	5778	=	$2 \cdot 3^3 \cdot 107$
19	4181	=	$37 \cdot 113$	9349		
20	6765	=	$3 \cdot 5 \cdot 11 \cdot 41$	15127	=	$7 \cdot 2161$
21	10946	=	$2 \cdot 13 \cdot 421$	24476	=	$2^2 \cdot 29 \cdot 211$
22	17711	=	$89 \cdot 199$	39603	=	$3 \cdot 43 \cdot 307$
23	28657			64079	=	$139 \cdot 461$
24	46368	=	$2^5 \cdot 3^2 \cdot 7 \cdot 23$	103682	=	$2 \cdot 47 \cdot 1103$
25	75025	=	$5^2 \cdot 3001$	167761	=	$11 \cdot 101 \cdot 161$
26	121393	=	$233 \cdot 521$	271443	=	$3 \cdot 90481$
27	196418	=	$2 \cdot 17 \cdot 53 \cdot 109$	439204	=	$2^2 \cdot 19 \cdot 5779$
28	317811	=	$3 \cdot 13 \cdot 29 \cdot 281$	710647	=	$7^2 \cdot 14503$
29	514229			1149851	=	$59 \cdot 19489$
30	832040	=	$2^3 \cdot 5 \cdot 11 \cdot 31 \cdot 61$	1860498	=	$2 \cdot 3^2 \cdot 41 \cdot 2521$

Apéndice B

$r(n)$ y $l(n)$ para $2 \leq m \leq 121$

n	$r(n)$	$l(n)$	$\alpha(n)$	n	$r(n)$	$l(n)$	$\alpha(n)$	n	$r(n)$	$l(n)$	$\alpha(n)$	n	$r(n)$	$l(n)$	$\alpha(n)$
2	3	3	1	32	24	48	2	62	30	30	1	92	24	48	2
3	4	8	2	33	20	40	2	63	24	48	2	93	60	120	2
4	6	6	1	34	9	36	4	64	48	96	2	94	48	96	2
5	5	20	4	35	40	80	2	65	35	140	4	95	90	180	2
6	12	24	2	36	12	24	2	66	60	120	2	96	24	48	2
7	8	16	2	37	19	76	4	67	68	136	2	97	49	196	4
8	6	12	2	38	18	18	1	68	18	36	2	98	168	336	2
9	12	24	2	39	28	56	2	69	24	48	2	99	60	120	2
10	15	60	4	40	30	60	2	70	120	240	2	100	150	300	2
11	10	10	1	41	20	40	2	71	70	70	1	101	50	50	1
12	12	24	2	42	24	48	2	72	12	24	2	102	36	72	2
13	7	28	4	43	44	88	2	73	37	148	4	103	104	208	2
14	24	48	2	44	30	30	1	74	57	228	4	104	42	84	2
15	20	40	2	45	60	120	2	75	100	200	2	105	40	80	2
16	12	24	2	46	24	48	2	76	18	18	1	106	27	108	4
17	9	36	4	47	16	32	2	77	40	80	2	107	36	72	2
18	12	24	2	48	12	24	2	78	84	168	2	108	36	72	2
19	18	18	1	49	56	112	2	79	78	78	1	109	27	108	4
20	30	60	2	50	75	300	4	80	60	120	2	110	30	60	2
21	8	16	2	51	36	72	2	81	108	216	2	111	76	152	2
22	30	30	1	52	42	84	2	82	60	120	2	112	24	48	2
23	24	48	2	53	27	108	4	83	84	168	2	113	19	76	4
24	12	24	2	54	36	72	2	84	24	48	2	114	36	72	2
25	25	100	4	55	10	20	2	85	45	180	4	115	120	240	2
26	21	84	4	56	24	48	2	86	132	264	2	116	42	42	1
27	36	72	2	57	36	72	2	87	28	56	2	117	84	168	2
28	24	48	2	58	42	42	1	88	30	60	2	118	174	174	1
29	14	14	1	59	58	58	1	89	11	44	4	119	72	144	2
30	60	120	2	60	60	120	2	90	60	120	2	120	60	120	2
31	30	30	1	61	15	60	4	91	56	112	2	121	110	110	1

Apéndice C

Un período simple de $F_n \pmod m$ para $2 \leq m \leq 50$

m																				
2	0	1	1																	
3	0	1	1	2	0	2	2	1												
4	0	1	1	2	3	1														
5	0	1	1	2	3	0	3	3	1	4	0	4	4	3	2	0	2	2	4	1
6	0	1	1	2	3	5	2	1	3	4	1	5	0	5	5	4	3	1	4	5
	3	2	5	1																
7	0	1	1	2	3	5	1	6	0	6	6	5	4	2	6	1				
8	0	1	1	2	3	5	0	5	5	2	7	1								
9	0	1	1	2	3	5	8	4	3	7	1	8	0	8	8	7	6	4	1	5
	6	2	8	1																
10	0	1	1	2	3	5	8	3	1	4	5	9	4	3	7	0	7	7	4	1
	5	6	1	7	8	5	3	8	1	9	0	9	9	8	7	5	2	7	9	6
	5	1	6	7	3	0	3	3	6	9	5	4	9	3	2	5	7	2	9	1
11	0	1	1	2	3	5	8	2	10	1										
12	0	1	1	2	3	5	8	1	9	10	7	5	0	5	5	10	3	1	4	5
	9	2	11	1																
13	0	1	1	2	3	5	8	0	8	8	3	11	1	12	0	12	12	11	10	8
	5	0	5	5	10	2	12	1												
14	0	1	1	2	3	5	8	13	7	6	13	5	4	9	13	8	7	1	8	9
	3	12	1	13	0	13	13	12	11	9	6	1	7	8	1	9	10	5	1	6
	7	13	6	5	11	2	13	1												
15	0	1	1	2	3	5	8	13	6	4	10	14	9	8	2	10	12	7	4	11
	0	11	11	7	3	10	13	8	6	14	5	4	9	13	7	5	12	2	14	1
16	0	1	1	2	3	5	8	13	5	2	7	9	0	9	9	2	11	13	8	5
	13	2	15	1																
17	0	1	1	2	3	5	8	13	4	0	4	4	8	12	3	15	1	16	0	16
	16	15	14	12	9	4	13	0	13	13	9	5	14	2	16	1				
18	0	1	1	2	3	5	8	13	3	16	1	17	0	17	17	16	15	13	10	5
	15	2	17	1																
19	0	1	1	2	3	5	8	13	2	15	17	13	11	5	16	2	18	1		
20	0	1	1	2	3	5	8	13	1	14	15	9	4	13	17	10	7	17	4	1
	5	6	11	17	8	5	13	18	11	9	0	9	9	18	7	5	12	17	9	6
	15	1	16	17	13	10	3	13	16	9	5	14	19	13	12	5	17	2	19	1
21	0	1	1	2	3	5	8	13	0	13	13	5	18	2	20	1				
22	0	1	1	2	3	5	8	13	21	12	11	1	12	13	3	16	19	13	10	1
	11	12	1	13	14	5	19	2	21	1										
23	0	1	1	2	3	5	8	13	21	11	9	20	6	3	9	12	21	10	8	18
	3	21	1	22	0	22	22	21	20	18	15	10	2	12	14	3	17	20	14	11
	2	13	15	5	20	2	22	1												
24	0	1	1	2	3	5	8	13	21	10	7	17	0	17	17	10	3	13	16	5
	21	2	23	1																
25	0	1	1	2	3	5	8	13	21	9	5	14	19	8	2	10	12	22	9	6
	15	21	11	7	18	0	18	18	11	4	15	19	9	3	12	15	2	17	19	11

	5	16	21	12	8	20	3	23	1	24	0	24	24	23	22	20	17	12	4	16
	20	11	6	17	23	15	13	3	16	19	10	4	14	18	7	0	7	7	14	21
	10	6	16	22	13	10	23	8	6	14	20	9	4	13	17	5	22	2	24	1
26	0	1	1	2	3	5	8	13	21	8	3	11	14	25	13	12	25	11	10	21
	5	0	5	5	10	15	25	14	13	1	14	15	3	18	21	13	8	21	3	24
	1	25	0	25	25	24	23	21	18	13	5	18	23	15	12	1	13	14	1	15
	16	5	21	0	21	21	16	11	1	12	13	25	12	11	23	8	5	13	18	5
	23	2	25	1																
27	0	1	1	2	3	5	8	13	21	7	1	8	9	17	26	16	15	4	19	23
	15	11	26	10	9	19	1	20	21	14	8	22	3	25	1	26	0	26	26	25
	24	22	19	14	6	20	26	19	18	10	1	11	12	23	8	4	12	16	1	17
	18	8	26	7	6	13	19	5	24	2	26	1								
28	0	1	1	2	3	5	8	13	21	6	27	5	4	9	13	22	7	1	8	9
	17	26	15	13	0	13	13	26	11	9	20	1	21	22	15	9	24	5	1	6
	7	13	20	5	25	2	27	1												
29	0	1	1	2	3	5	8	13	21	5	26	2	28	1						
30	0	1	1	2	3	5	8	13	21	4	25	29	24	23	17	10	27	7	4	11
	15	26	11	7	18	25	13	8	21	29	20	19	9	28	7	5	12	17	29	16
	15	1	16	17	3	20	23	13	6	19	25	14	9	23	2	25	27	22	19	11
	0	11	11	22	3	25	28	23	21	14	5	19	24	13	7	20	27	17	14	1
	15	16	1	17	18	5	23	28	21	19	10	29	9	8	17	25	12	7	19	26
	15	11	26	7	3	10	13	23	6	29	5	4	9	13	22	5	27	2	29	1
31	0	1	1	2	3	5	8	13	21	3	24	27	20	16	5	21	26	16	11	27
	7	3	10	13	23	5	28	2	30	1										
32	0	1	1	2	3	5	8	13	21	2	23	25	16	9	25	2	27	29	24	21
	13	2	15	17	0	17	17	2	19	21	8	29	5	2	7	9	16	25	9	2
	11	13	24	5	29	2	31	1												
33	0	1	1	2	3	5	8	13	21	1	22	23	12	2	14	16	30	13	10	23
	0	23	23	13	3	16	19	2	21	23	11	1	12	13	25	5	30	2	32	1
34	0	1	1	2	3	5	8	13	21	0	21	21	8	29	3	32	1	33	0	33
	33	32	31	29	26	21	13	0	13	13	26	5	31	2	33	1				
35	0	1	1	2	3	5	8	13	21	34	20	19	4	23	27	15	7	22	29	16
	10	26	1	27	28	20	13	33	11	9	20	29	14	8	22	30	17	12	29	6
	0	6	6	12	18	30	13	8	21	29	15	9	24	33	22	20	7	27	34	26
	25	16	6	22	28	15	8	23	31	19	15	34	14	13	27	5	32	2	34	1
36	0	1	1	2	3	5	8	13	21	34	19	17	0	17	17	34	15	13	28	5
	33	2	35	1																
37	0	1	1	2	3	5	8	13	21	34	18	15	33	11	7	18	25	6	31	0
	31	31	25	19	7	26	33	22	18	3	21	24	8	32	3	35	1	36	0	36
	36	35	34	32	29	24	16	3	19	22	4	26	30	19	12	31	6	0	6	6
	12	18	30	11	4	15	19	34	16	13	29	5	34	2	36	1				
38	0	1	1	2	3	5	8	13	21	34	17	13	30	5	35	2	37	1		
39	0	1	1	2	3	5	8	13	21	34	16	11	27	38	26	25	12	37	10	8
	18	26	5	31	36	28	25	14	0	14	14	28	3	31	34	26	21	8	29	37
	27	25	13	38	12	11	23	34	18	13	31	5	36	2	38	1				
40	0	1	1	2	3	5	8	13	21	34	15	9	24	33	17	10	27	37	24	21
	5	26	31	17	8	25	33	18	11	29	0	29	29	18	7	25	32	17	9	26
	35	21	16	37	13	10	23	33	16	9	25	34	19	13	32	5	37	2	39	1
41	0	1	1	2	3	5	8	13	21	34	14	7	21	28	8	36	3	39	1	40

	0	40	40	39	38	36	33	28	20	7	27	34	20	13	33	5	38	2	40	1
42	0	1	1	2	3	5	8	13	21	34	13	5	18	23	41	22	21	1	22	23
	3	26	29	13	0	13	13	26	39	23	20	1	21	22	1	23	24	5	29	34
	21	13	34	5	39	2	41	1												
43	0	1	1	2	3	5	8	13	21	34	12	3	15	18	33	8	41	6	4	10
	14	24	38	19	14	33	4	37	41	35	33	25	15	40	12	9	21	30	8	38
	3	41	1	42	0	42	42	41	40	38	35	30	22	9	31	40	28	25	10	35
	2	37	39	33	29	19	5	24	29	10	39	6	2	8	10	18	28	3	31	34
	22	13	35	5	40	2	42	1												
44	0	1	1	2	3	5	8	13	21	34	11	1	12	13	25	38	19	13	32	1
	33	34	23	13	36	5	41	2	43	1										
45	0	1	1	2	3	5	8	13	21	34	10	44	9	8	17	25	42	22	19	41
	15	11	26	37	18	10	28	38	21	14	35	4	39	43	37	35	27	17	44	16
	15	31	1	32	33	20	8	28	36	19	10	29	39	23	17	40	12	7	19	26
	0	26	26	7	33	40	28	23	6	29	35	19	9	28	37	20	12	32	44	31
	30	16	1	17	18	35	8	43	6	4	10	14	24	38	17	10	27	37	19	11
	30	41	26	22	3	25	28	8	36	44	35	34	24	13	37	5	42	2	44	1
46	0	1	1	2	3	5	8	13	21	34	9	43	6	3	9	12	21	33	8	41
	3	44	1	45	0	45	45	44	43	41	38	33	25	12	37	3	40	43	37	34
	25	13	38	5	43	2	45	1												
47	0	1	1	2	3	5	8	13	21	34	8	42	3	45	1	46	0	46	46	45
	44	42	39	34	26	13	39	5	44	2	46	1								
48	0	1	1	2	3	5	8	13	21	34	7	41	0	41	41	34	27	13	40	5
	45	2	47	1																
49	0	1	1	2	3	5	8	13	21	34	6	40	46	37	34	22	7	29	36	16
	3	19	22	41	14	6	20	26	46	23	20	43	14	8	22	30	3	33	36	20
	7	27	34	12	46	9	6	15	21	36	8	44	3	47	1	48	0	48	48	47
	46	44	41	36	28	15	43	9	3	12	15	27	42	20	13	33	46	30	27	8
	35	43	29	23	3	26	29	6	35	41	27	19	46	16	13	29	42	22	15	37
	3	40	43	34	28	13	41	5	46	2	48	1								
50	0	1	1	2	3	5	8	13	21	34	5	39	44	33	27	10	37	47	34	31
	15	46	11	7	18	25	43	18	11	29	40	19	9	28	37	15	2	17	19	36
	5	41	46	37	33	20	3	23	26	49	25	24	49	23	22	45	17	12	29	41
	20	11	31	42	23	15	38	3	41	44	35	29	14	43	7	0	7	7	14	21
	35	6	41	47	38	35	23	8	31	39	20	9	29	38	17	5	22	27	49	26
	25	1	26	27	3	30	33	13	46	9	5	14	19	33	2	35	37	22	9	31
	40	21	11	32	43	25	18	43	11	4	15	19	34	3	37	40	27	17	44	11
	5	16	21	37	8	45	3	48	1	49	0	49	49	48	47	45	42	37	29	16
	45	11	6	17	23	40	13	3	16	19	35	4	39	43	32	25	7	32	39	21
	10	31	41	22	13	35	48	33	31	14	45	9	4	13	17	30	47	27	24	1
	25	26	1	27	28	5	33	38	21	9	30	39	19	8	27	35	12	47	9	6
	15	21	36	7	43	0	43	43	36	29	15	44	9	3	12	15	27	42	19	11
	30	41	21	12	33	45	28	23	1	24	25	49	24	23	47	20	17	37	4	41
	45	36	31	17	48	15	13	28	41	19	10	29	39	18	7	25	32	7	39	46
	35	31	16	47	13	10	23	33	6	39	45	34	29	13	42	5	47	2	49	1

Apéndice D

$r'(m)$ y $l'(m)$ para $2 \leq m \leq 121$

m	$r'(m)$	$l'(m)$	m	$r'(m)$	$l'(m)$	m	$r'(m)$	$l'(m)$	m	$r'(m)$	$l'(m)$
2	0	3	32	-	48	62	15	30	92	-	48
3	2	8	33	-	40	63	-	48	93	-	120
4	3	6	34	-	36	64	-	96	94	24	96
5	-	4	35	-	16	65	-	28	95	-	36
6	6	24	36	-	24	66	-	120	96	-	48
7	4	16	37	-	76	67	34	136	97	-	196
8	-	12	38	9	18	68	-	36	98	-	336
9	6	24	39	-	56	69	-	48	99	-	120
10	-	12	40	-	12	70	-	48	100	-	60
11	5	10	41	10	40	71	35	70	101	25	50
12	-	24	42	-	48	72	-	24	102	-	72
13	-	28	43	22	88	73	-	148	103	52	208
14	12	48	44	15	30	74	-	228	104	-	84
15	-	8	45	-	24	75	-	40	105	-	16
16	-	24	46	12	48	76	9	18	106	-	108
17	-	36	47	8	32	77	-	80	107	18	72
18	6	24	48	-	24	78	-	168	108	-	72
19	9	18	49	28	112	79	39	78	109	-	108
20	-	12	50	-	60	80	-	24	110	-	60
21	-	16	51	-	72	81	54	216	111	-	152
22	15	30	52	-	84	82	30	120	112	-	48
23	12	48	53	-	108	83	42	168	113	-	76
24	-	24	54	18	72	84	-	48	114	-	72
25	-	20	55	-	20	85	-	36	115	-	48
26	-	84	56	-	48	86	66	264	116	21	42
27	18	72	57	-	72	87	-	56	117	-	168
28	-	48	58	21	42	88	-	60	118	-	174
29	7	14	59	29	58	89	-	44	119	-	144
30	-	24	60	-	24	90	-	24	120	-	24
31	15	30	61	-	60	91	-	112	121	55	110

Apéndice E

Un período simple de $L_n \pmod m$ para $2 \leq m \leq 50$

m																				
2	0	1	1																	
3	2	1	0	1	1	2	0	2												
4	2	1	3	0	3	3														
5	2	1	3	4																
6	2	1	3	4	1	5	0	5	5	4	3	1	4	5	3	2	5	1	0	1
	1	2	3	5																
7	2	1	3	4	0	4	4	1	5	6	4	3	0	3	3	6				
8	2	1	3	4	7	3	2	5	7	4	3	7								
9	2	1	3	4	7	2	0	2	2	4	6	1	7	8	6	5	2	7	0	7
	7	5	3	8																
10	2	1	3	4	7	1	8	9	7	6	3	9								
11	2	1	3	4	7	0	7	7	3	10										
12	2	1	3	4	7	11	6	5	11	4	3	7	10	5	3	8	11	7	6	1
	7	8	3	11																
13	2	1	3	4	7	11	5	3	8	11	6	4	10	1	11	12	10	9	6	2
	8	10	5	2	7	9	3	12												
14	2	1	3	4	7	11	4	1	5	6	11	3	0	3	3	6	9	1	10	11
	7	4	11	1	12	13	11	10	7	3	10	13	9	8	3	11	0	11	11	8
	5	13	4	3	7	10	3	13												
15	2	1	3	4	7	11	3	14												
16	2	1	3	4	7	11	2	13	15	12	11	7	2	9	11	4	15	3	2	5
	7	12	3	15																

Apéndice F

Algoritmos

En este apéndice vamos a exponer los algoritmos usados para la verificación de algunos resultados y para la construcción de los anteriores apéndices. Estos algoritmos fueron creados en el programa MuPAD.

1. Este algoritmo crea e imprime una lista de *n* parejas, donde los primeros términos forman una sucesión de Fibonacci generalizada con términos iniciales *a* y *b*, los segundos de las parejas forman la sucesión de los primeros términos modulada módulo *m*.

```
/*Crea una lista con los n primeros números de la sucesión, junto
con el número módulo m*/
FiMod:=proc(a,b,n,m)
local i,j,A,B;
begin
A:=[a,b];
B:=[a mod m, b mod m];
for i from 3 to n do
  A:=listlib::insert(A, A[i-1]+A[i-2]);
  B:=listlib::insertAt(B, (B[i-1]+B[i-2])mod m,i);
end_for;
for j from 1 to n do
print([A[j],B[j]]);
end_for;
end_proc;
```

2. Este algoritmo encuentra el rango de aparición de un entero como divisor de algún número de la sucesión de Fibonacci.

```
/*Encuentra r(n)*/
RanFi:=proc(n)
local i,F;
begin
F:=[0,1];
i:=2;
  while (F[i] mod n <> 0) do
  i:=i+1;
  F:=listlib::insert(F, F[i-1]+F[i-2]);
  end_while;
  print(n,i-1, F[i]);
end_proc;
```

3. Este algoritmo calcula la longitud de un período simple de la sucesión de Fibonacci módulo *m*.

```
/*Encunetra l(n)*/
PeriFi:=proc(a,b,n)
local i,F;
begin
F:=[a mod n, b mod n];
i:=2;
  repeat
  i:=i+1;
  F:=listlib::insertAt(F, (F[i-1]+F[i-2]) mod n,i);
  until (i>3 and F[i]=1 and F[i-1]=1 and F[i-2]=0) end_repeat;
  print(i-3);
end_proc;
```

4. Este algoritmo encuentra el rango (si existe) de aparición de un entero como divisor de algún número de la sucesión de Lucas. En caso de no existir dicho rango imprime el texto "NO EXISTE".

```
/*Encuentra r(n) para la sucesión de lucas*/
RanLuc:=proc(n)
local i,L;
begin
L:=[2,1];
i:=2;
  while (L[i] mod n <> 0) do
  if(L[i]<1000000000000000) then
  i:=i+1;
  L:=listlib::insert(L, L[i-1]+L[i-2]);
  else print("NO EXISTE");
  break
  end_if;
  end_while;
  print(i-1, L[i]);
end_proc;
```

5. Este algoritmo calcula la longitud de un período simple de la sucesión de Lucas módulo *m*.

```
/*Encunetra período para lucas n>3*/
Perilu:=proc(a,b,n)
local i,L;
begin
L:=[a mod n, b mod n];
i:=2;
  repeat
  i:=i+1;
  L:=listlib::insertAt(L, (L[i-1]+L[i-2]) mod n,i);
  until (i>3 and L[i]=3 and L[i-1]=1 and L[i-2]=2) end_repeat;
  print(i-3);
end_proc;
```

6. Este algoritmo calcula el cociente entre el período de Fibonacci y el período de Lucas.

```
/*Encuentra el cociente entre el período de Fibonacci y el de Lucas*/
CocPeri:=proc(n)
local j,i,B;
begin
B:=[1,1,1];
for j from 4 to n do
B:=listlib::insertAt(B,[PeriFi(0,1,j)/PeriLu(2,1,j)],j);
end_for;
for i from 1 to n do
print(i,op(B,i));
end_for;
end_proc;
```

7. Este algoritmo toma los primeros *n* términos de una sucesión de Fibonacci generalizada con términos iniciales *a* y *b*, pasa esta sucesión a base *m* y finalmente imprime todos aquellos números que están formados por solo un número menor que la base *m*.

```
/*Crea una lista con los n primeros números de fibonacci en base m
e imprime aquellos formados por solo un "dígito"*/
FiBas:=proc(a,b,n,m)
local i,j,r,t,F,B,C,D;
begin
F:=[a,b];
for i from 3 to n do
  F:=listlib::insertAt(F, (F[i-1]+F[i-2]),i);
end_for;
B:=[];
for j from 1 to n do
B:=listlib::insertAt(B,[numlib::g_adic(op(F,j),m)],j);
end_for;
C:=[];
D:={};
for r from 1 to n do
C:=op(B,r);
t:=nops(C);
D:=set:={op(C,1..t)};
if (nops(D) < 2) then
print(op(F,r),op(B,r));
end_if;
end_for;
end_proc;
```

Bibliografía

[1] BURTON, David M. The Quadrtic Reciprocity Law. En *Elementary Number Theory*,(183-216). ISBN 0 – 205 – 06978 – 9.

[2] OCEJO MONGE, Adriana. Factorización de los números de Fibonacci. En *Tercer taller de teoría de números del centro-sureste*(A. Cuesto Hernández, Ed),(47-70). (2008).Veracruz-Xalapa: Editorial Azcapotzalco.

[3] LUCA, Florian. Fibonacci and Lucas numbers with only one ditinct digit. *Portugaliae Mathematica*. (2000). 57(2), 243-254.

[4] RENAULT, Marc. (1996).*The Fibonacci secuence under varius moduli*. Carolina del Norte.

[5] RIASAT, Samin. $\mathbb{Z}[(\varphi)]$ and the Fibonacci seceunce modulo n. *Mathematical Reflections(1)*.(2011).

[6] WIKIPEDIA. Biografia de Leonardo de pisa [en linea]:
http : //*es.wikipedia.org*/*wiki*/*Leonardo_de_Pisa*