Algunos resultados Derivados del estudio de la Sucesión de Fibonacci módulo m

Carlos Arturo Rodriguez
Yzel Wlly Alay Gómez

Escuela de Matemáticas
Universidad Industrial de Santander
Grupo Alcom

Agosto 15 de 2014

Definición

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 entero positivo tal que* $n \geq 2$ *,* $F_1 = 1$ *y* $F_2 = 1$.

Definición

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 entero positivo tal que $n \geq 2$, $F_1 = 1$ y $F_2 = 1$.

Una forma de obtener los números de la sucesión de Fibonacci mediante una expresión cerrada, es a través de la conocida formula de Binet.

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

Esta expresión es conocida como la formula de Binet.

Proposición

Los números F_n de la sucesión de fibonacci, cumplen que: $F_n \mid F_{k \cdot n}$ para toda pareja de naturales k, n.

Proposición

Los números F_n de la sucesión de fibonacci, cumplen que: $F_n \mid F_{k \cdot n}$ para toda pareja de naturales k, n.

Corolario

Si $m \mid F_n$ entonces $m \mid F_{k\,n}$, $\forall k \in \mathbb{N}$.

Observación

Descomponiendo los números Fibonacci en factores primos, puede notarse que cada número (excepto F_6 y F_{12}) posee un factor primo que no es factor de ningún número de Fibonacci anterior. Una prueba de ello puede encontrarse en [3].

Observación

Descomponiendo los números Fibonacci en factores primos, puede notarse que cada número (excepto F_6 y F_{12}) posee un factor primo que no es factor de ningún número de Fibonacci anterior. Una prueba de ello puede encontrarse en [3].
A estos factores se les conoce como factores característicos.

Observación

Descomponiendo los números Fibonacci en factores primos, puede notarse que cada número (excepto F_6 y F_{12}) posee un factor primo que no es factor de ningún número de Fibonacci anterior. Una prueba de ello puede encontrarse en [3].
A estos factores se les conoce como factores característicos.

Proposición

F_n y F_{n+1} son primos relativos, $\forall k \in \mathbb{N}$.

Teorema

$m \mid n$ *si y solo si* $F_m \mid F_n$

Teorema

$m \mid n$ *si y solo si* $F_m \mid F_n$

Proposición

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

En la prueba del siguiente resultado se prueba adicionalmente que:

- La sucesión de Fibonacci es periódica vista modulo un entero positivo m.
- La primer pareja de residuos que se repite es la $(1, 1)$

En la prueba del siguiente resultado se prueba adicionalmente que:

- La sucesión de Fibonacci es periódica vista modulo un entero positivo m.
- La primer pareja de residuos que se repite es la $(1, 1)$

Teorema

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

Observación

Aunque la sucesión de Lucas sigue la misma ecuación de recurrencia que la sucesión de Fibonacci, no se cumple en ella el resultado anterior.

Observación

Aunque la sucesión de Lucas sigue la misma ecuación de recurrencia que la sucesión de Fibonacci, no se cumple en ella el resultado anterior.

Se concluye analogamente de la prueba del anterior resultado que en la sucesión de Lucas la primer pareja que se repite es la $(1, 3)$*, pero a partir de ella no se puede garantizar que siguiendo la recurrencia de forma inversa se obtenga un residuo* 0 *para todo* m *en los enteros positivos.*

Definición (Rango de Aparición)

Sea $m > 1$. Al menor índice $r(m)$ tal que $F_{r(m)} \equiv 0 \pmod m$, se le llama el rango de aparición de m.

Definición (Rango de Aparición)

Sea $m > 1$. Al menor índice $r(m)$ tal que $F_{r(m)} \equiv 0 \pmod m$, se le llama el rango de aparición de m.

Ejemplo

1) $r(2) = 3$ pues $F_3 = 2$ es el menor número de Fibonacci tal que $2 \mid F_i$ para algún $i \in \mathbb{Z}$

n	0	1	2	3	4	5	6	7	8	9	10
F_n	0	1	1	2	3	5	8	13	21	34	55

2) $r(13) = 7$ pues $F_7 = 13$ es el menor número de Fibonacci tal que $13 \mid F_i$ para algún $i \in \mathbb{Z}$

n	0	1	2	3	4	5	6	7	8	9	10
F_n	0	1	1	2	3	5	8	13	21	34	55

2) $r(13) = 7$ pues $F_7 = 13$ es el menor número de Fibonacci tal que $13 \mid F_i$ para algún $i \in \mathbb{Z}$

n	0	1	2	3	4	5	6	7	8	9	10
F_n	0	1	1	2	3	5	8	13	21	34	55

3) $r(10) = 15$ pues $F_{15} = 610$ es el menor número de Fibonacci tal que $10 \mid F_i$ para algún $i \in \mathbb{Z}$

n	11	12	13	14	15	16	17
F_n	89	144	233	377	610	987	1597

Definición

El periodo de repetición de la sucesión de Fibonacci módulo un entero positivo m, es el menor entero positivo $l(m)$ tal que

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

Definición

El periodo 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 concluye que

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

Observación

$F_{r(m)} \mid F_{k\cdot r(m)}$ *con* $k \in \mathbb{Z}^+$, *ahora como* $m \mid F_{r(m)}$ *entonces* $m \mid F_{k\cdot r(m)}$.

Luego resulta evidente que los indices 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* $r\,(m)$.

Observación

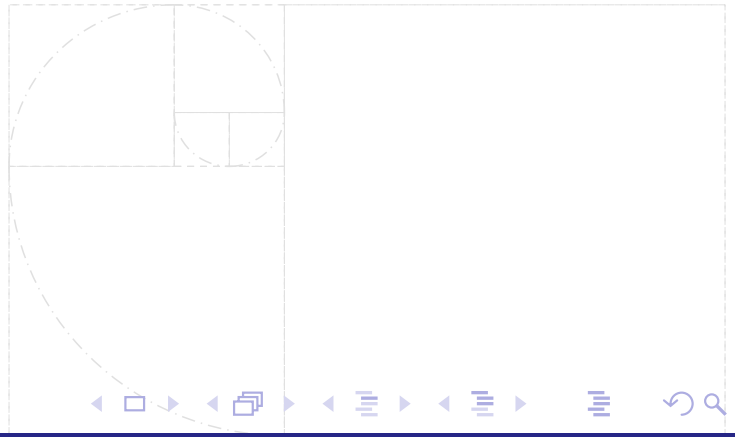
$F_{r(m)} \mid F_{k\cdot r(m)}$ *con* $k \in \mathbb{Z}^+$, *ahora como* $m \mid F_{r(m)}$ *entonces* $m \mid F_{k\cdot r(m)}$.
Luego resulta evidente que los indices para los cuales $F_n \equiv 0 \pmod m$ *forman una progresión aritmética. Además se puede notar que* $l(m) = r(m) \cdot t$, *esto es* $l(m)$ *es múltiplo de* $r(m)$.

Teorema

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

Corolario

Sea m un entero positivo. Entonces $m \mid F_n$ si y solo si $r(m) \mid n$



Corolario

Sea m un entero positivo. Entonces $m \mid F_n$ si y solo si $r(m) \mid n$

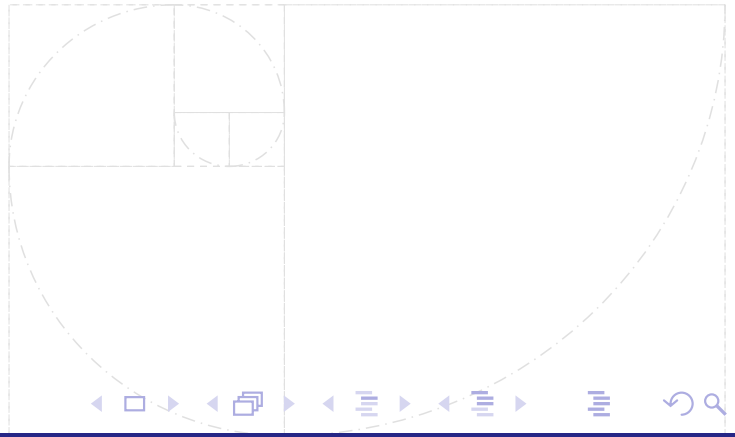
Teorema

Sea m un entero con factorización prima $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Entonces el rango de aparición de m está dado por

$$r(m) = lcm[r(p_1^{\alpha_1}), \ldots, r(p_k^{\alpha_k})]$$

Teorema

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



Teorema

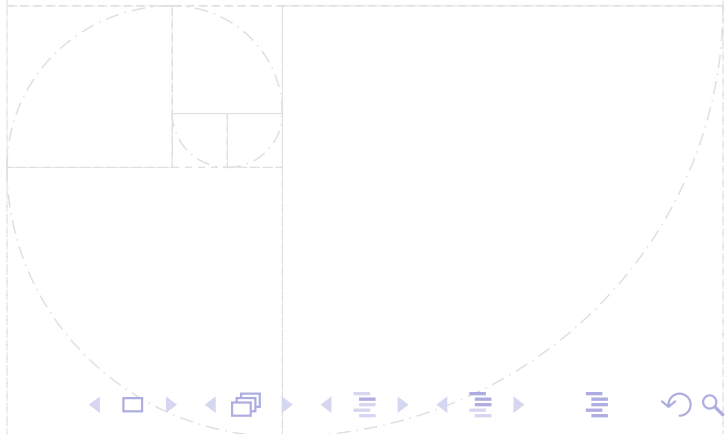
$r(m) \mid r(m \cdot n)$, *para todo par de enteros positivos* m *y* n.

Definición

- *Sea* $s(m)$ *el residuo de* $F_{r(m)+1}$ *módulo* m.
- *Sea* $\alpha(m)$ *el orden de* $s(m)$ *módulo* 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

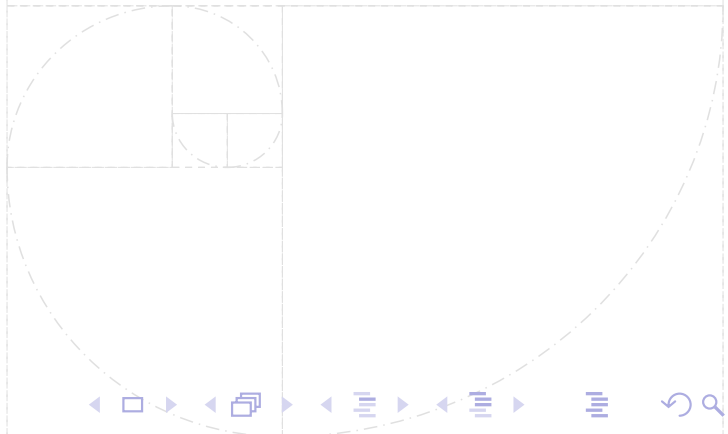
Sea $m = 13$, como $F_7 = 13$ entonces $r(13) = 7$.



Ejemplo

Sea $m = 13$, como $F_7 = 13$ entonces $r(13) = 7$.

$F_{r(13)+1} = F_8 = 21 \equiv 8 \pmod{13}$, así $s(13) = 8$

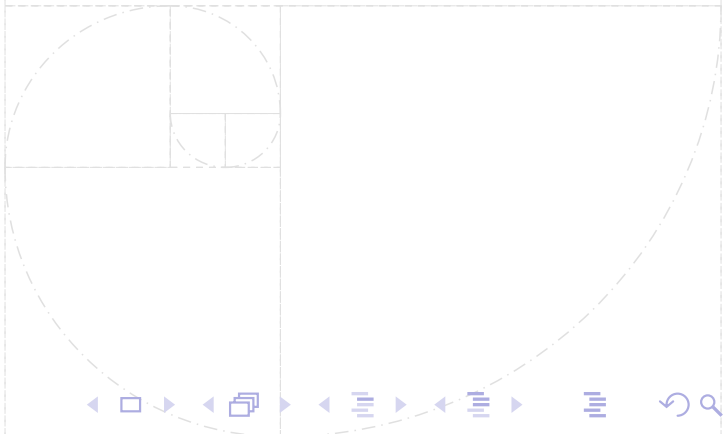


Ejemplo

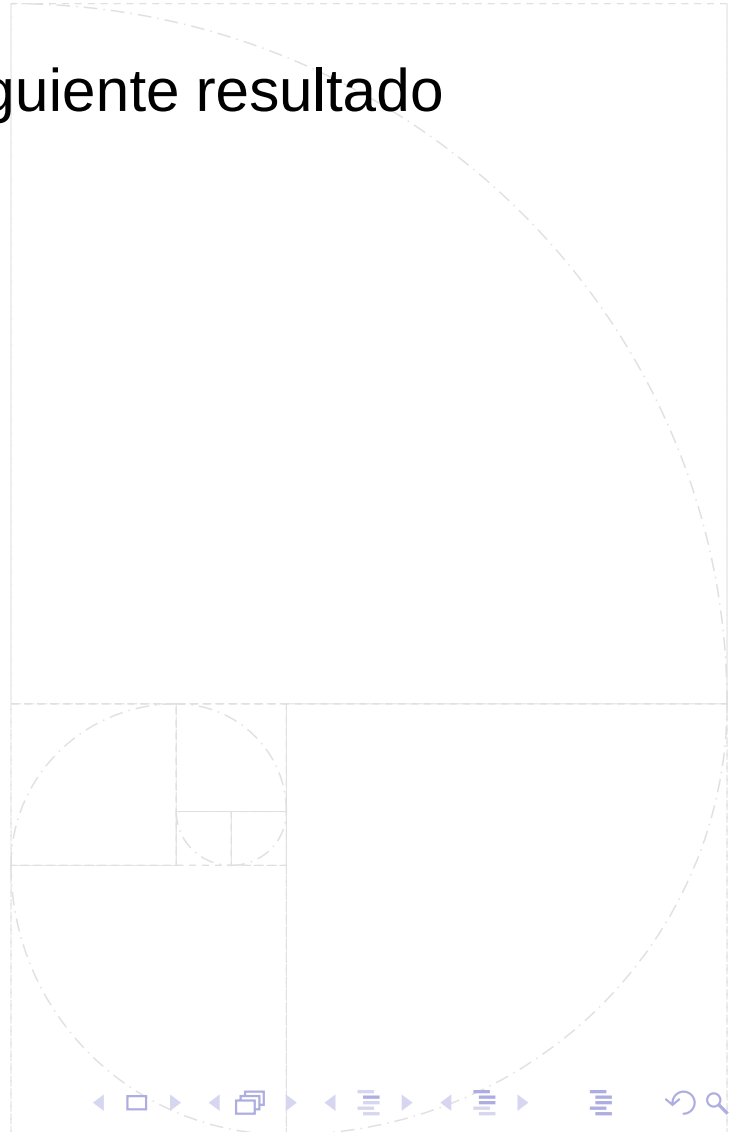
Sea $m = 13$, como $F_7 = 13$ entonces $r(13) = 7$.

$F_{r(13)+1} = F_8 = 21 \equiv 8 \pmod{13}$, así $s(13) = 8$

Por otro lado $s(13)^4 = 4096 \equiv 1 \pmod{13}$ y se verifica que para $t < 4$ $s(13)^t \not\equiv 1 \pmod{13}$



Ya vimos que $l(m) = r(m) \cdot t$, con el siguiente resultado caracterizaremos a t



Ya vimos que $l(m) = r(m) \cdot t$, con el siguiente resultado caracterizaremos a t

Teorema ([2])

$l(m) = r(m) \cdot \alpha(m)$

Ya vimos que $l(m) = r(m) \cdot t$, con el siguiente resultado caracterizaremos a t

Teorema ([2])

$l(m) = r(m) \cdot \alpha(m)$

Demostración

Consideremos un periodo simple de F_n módulo m.

Ya vimos que $l(m) = r(m) \cdot t$, con el siguiente resultado caracterizaremos a t

Teorema ([2])

$l(m) = r(m) \cdot \alpha(m)$

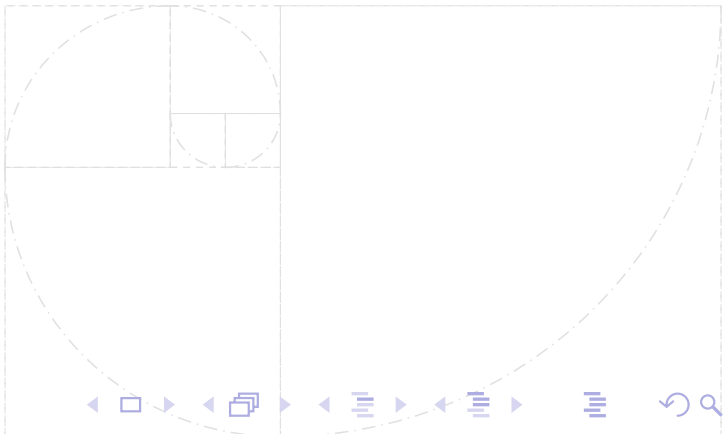
Demostración

Consideremos un periodo simple de F_n módulo m.

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

Particionemos ahora este periodo en subsecuencias así,

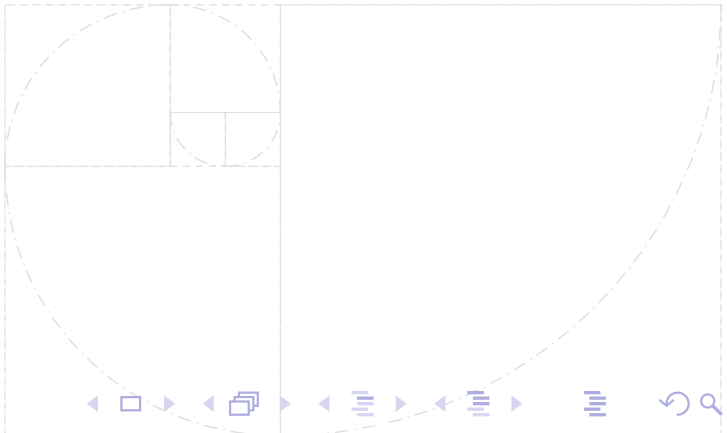
$$\underbrace{0\,1\,1\,\ldots\,s_1}_{A_0}\ \underbrace{0\,s_1\,s_1\,\ldots\,s_2}_{A_1}\ \underbrace{0\,s_2\,s_2\,\ldots\,s_3}_{A_2}\ 0\,s_3\,s_3\,\ldots\ldots\,0\,1$$



Particionemos ahora este periodo en subsecuencias 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 todas las A_i tiene la misma cantidad de elementos, a saber $r(m)$ términos con un solo un cero.
Observando detenidamente se nota que $s_1 = s(m)$ y que cada secuencia A_i es múltiplo de A_0, es decir $A_i \equiv A_0 \pmod m$

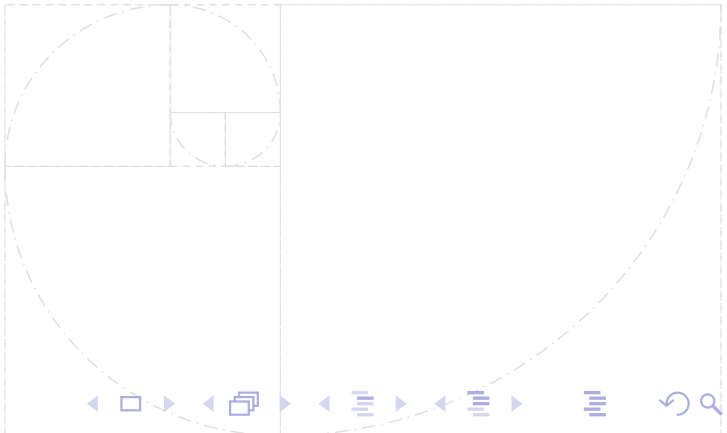


Particionemos ahora este periodo en subsecuencias así,

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

De tal forma que todas las A_i tiene la misma cantidad de elementos, a saber $r(m)$ términos con un solo un cero.
Observando detenidamente se nota que $s_1 = s(m)$ y que cada secuencia A_i es múltiplo de A_0, es decir $A_i \equiv A_0 \pmod m$

Más precisamente



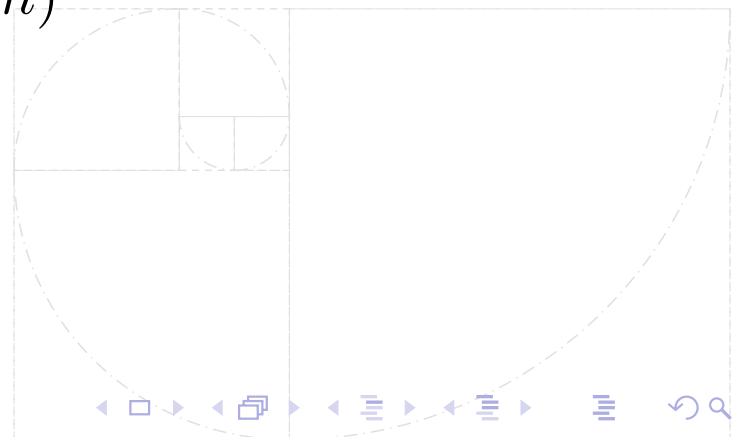
Particionemos ahora este periodo en subsecuencias así,

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

De tal forma que todas las A_i tiene la misma cantidad de elementos, a saber $r(m)$ términos con un solo un cero.
Observando detenidamente se nota que $s_1 = s(m)$ y que cada secuencia A_i es múltiplo de A_0, es decir $A_i \equiv A_0 \pmod m$

Más precisamente

$$A_1 \equiv s_1 A_0 \pmod m$$



Particionemos ahora este periodo en subsecuencias 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 todas las A_i tiene la misma cantidad de elementos, a saber $r(m)$ términos con un solo un cero.
Observando detenidamente se nota que $s_1 = s(m)$ y que cada secuencia A_i es múltiplo de A_0, es decir $A_i \equiv A_0 \pmod m$

Más precisamente

$$A_1 \equiv s_1 A_0 \pmod m$$
$$A_2 \equiv s_2 A_0 \pmod m$$

Particionemos ahora este periodo en subsecuencias así,

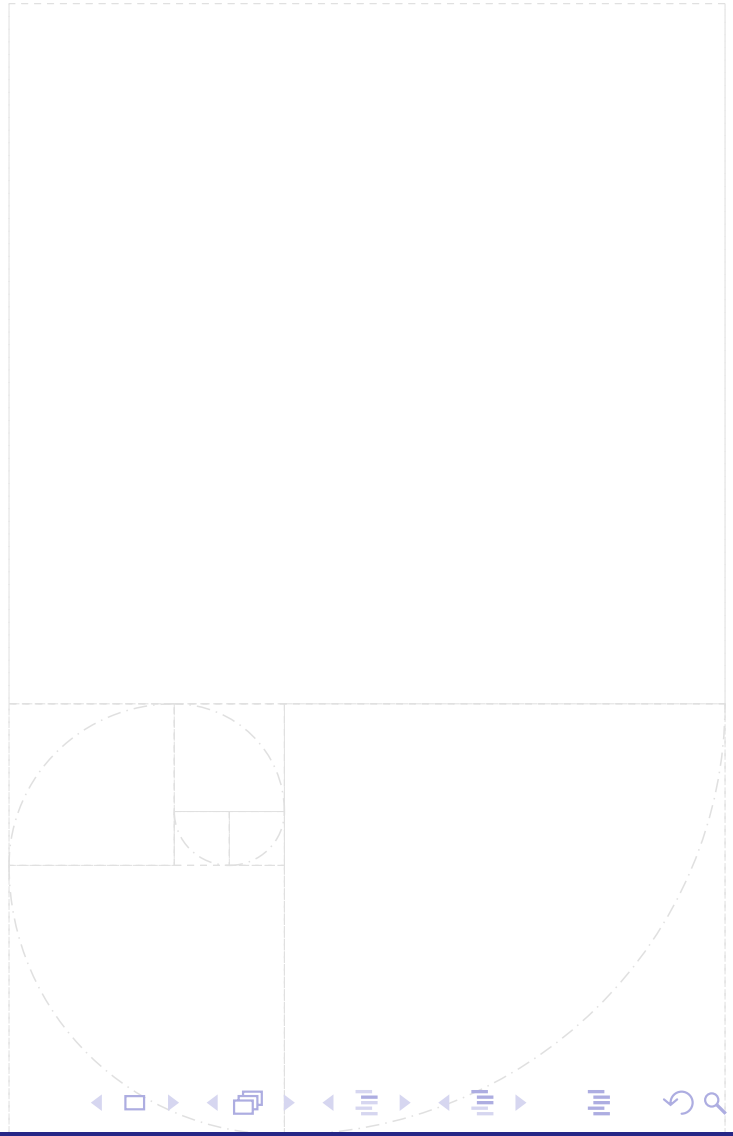
$$\underbrace{0\,1\,1\,\ldots\,s_1}_{A_0}\ \underbrace{0\,s_1\,s_1\,\ldots\,s_2}_{A_1}\ \underbrace{0\,s_2\,s_2\,\ldots\,s_3}_{A_2}\ 0\,s_3\,s_3\,\ldots\ldots\,0\,1$$

De tal forma que todas las A_i tiene la misma cantidad de elementos, a saber $r(m)$ términos con un solo un cero.
Observando detenidamente se nota que $s_1 = s(m)$ y que cada secuencia A_i es múltiplo de A_0, es decir $A_i \equiv A_0 \pmod m$

Más precisamente

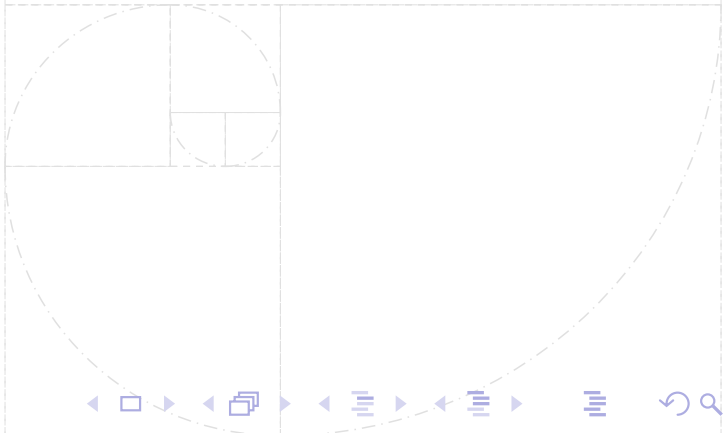
$$\begin{aligned} A_1 &\equiv s_1 A_0 \pmod m \\ A_2 &\equiv s_2 A_0 \pmod m \\ &\vdots \\ A_k &\equiv s_k A_0 \pmod m \\ &\vdots \end{aligned}$$

Se sigue inmediatamente que



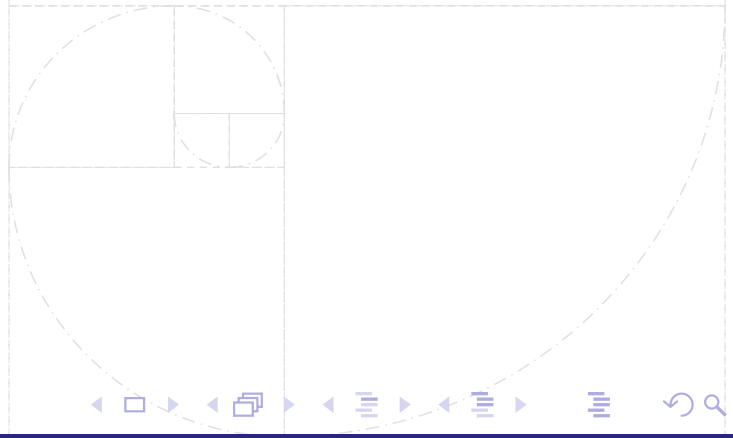
Se sigue inmediatamente que

$$s_k \equiv s_{k-1} \cdot s_1 \pmod m$$



Se sigue inmediatamente que

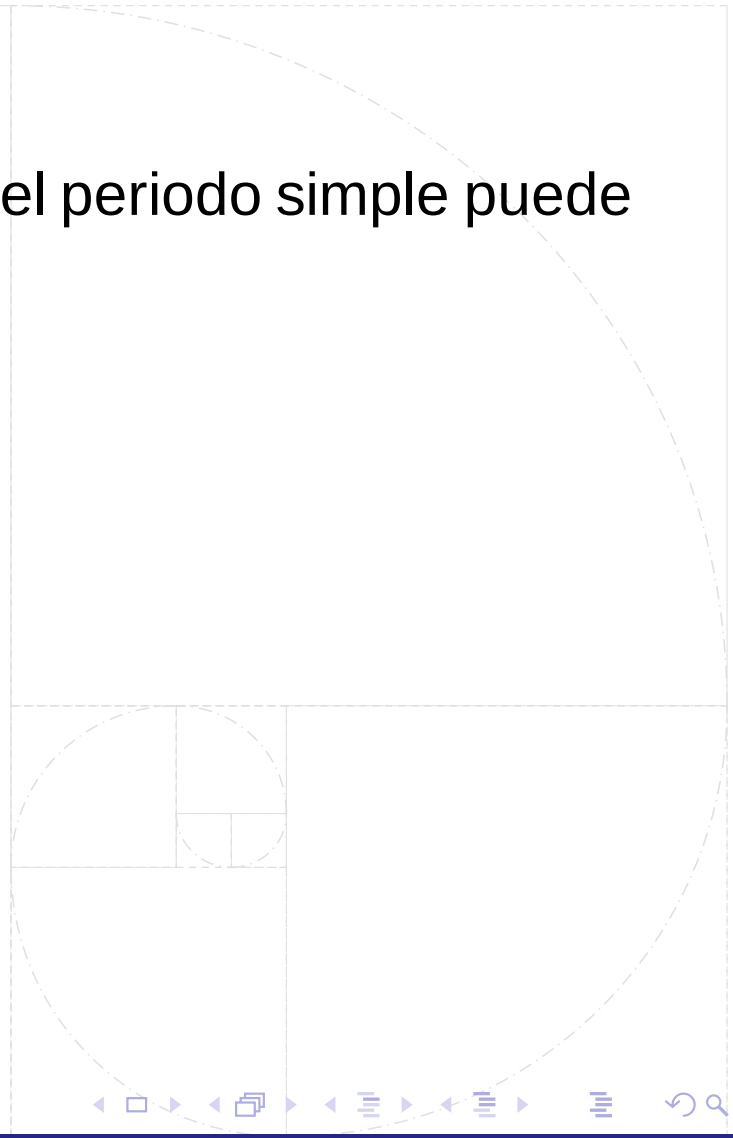
$$s_k \equiv s_{k-1} \cdot s_1 \pmod m$$
$$s_k \equiv s_{k-2} \cdot s_1^2 \pmod m$$



Se sigue inmediatamente que

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

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



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

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

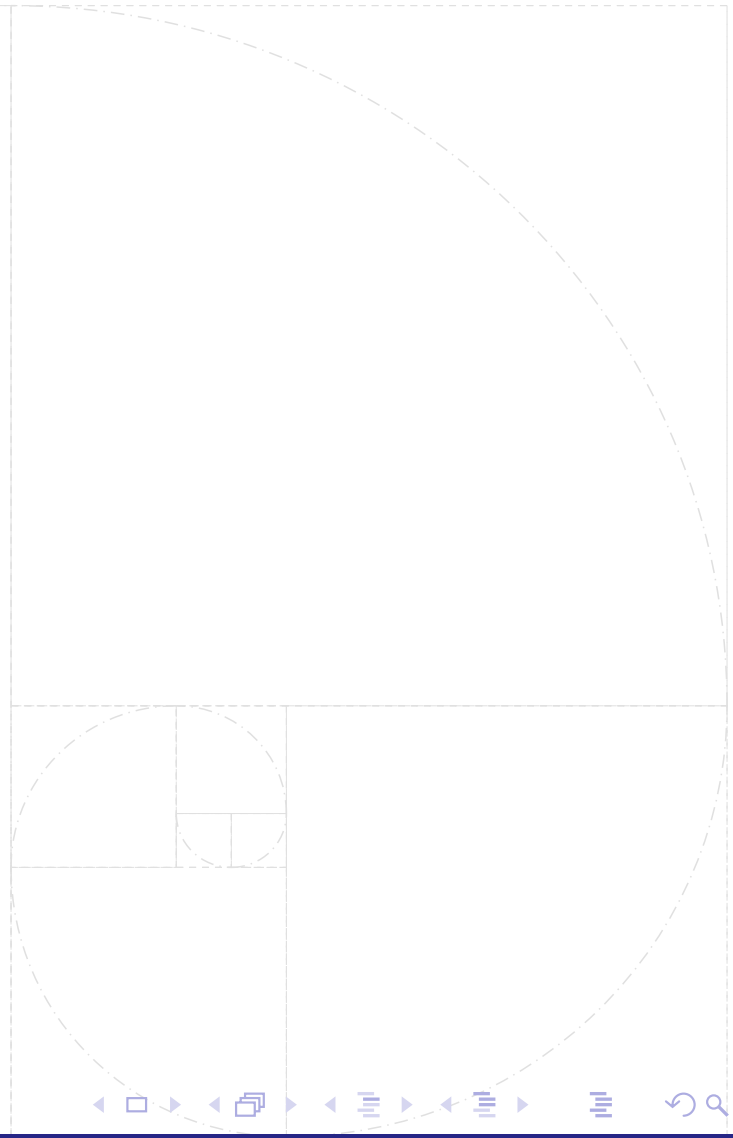
Como $\alpha(m)$ es el orden de s_1, entonces el periodo simple puede ser reescrito así:

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

Directamente se relaciona a $\alpha(m)$ con el número de ceros en un periodo simple. Se sigue que $l\,(m) = r\,(m) \cdot \alpha\,(m)$

Identidad

$$F_{n\cdot r(m)+t} \equiv F^n_{r(m)+1} \cdot F_t \pmod m$$



Identidad

$$F_{n\cdot r(m)+t} \equiv F^n_{r(m)+1} \cdot F_t \pmod m$$

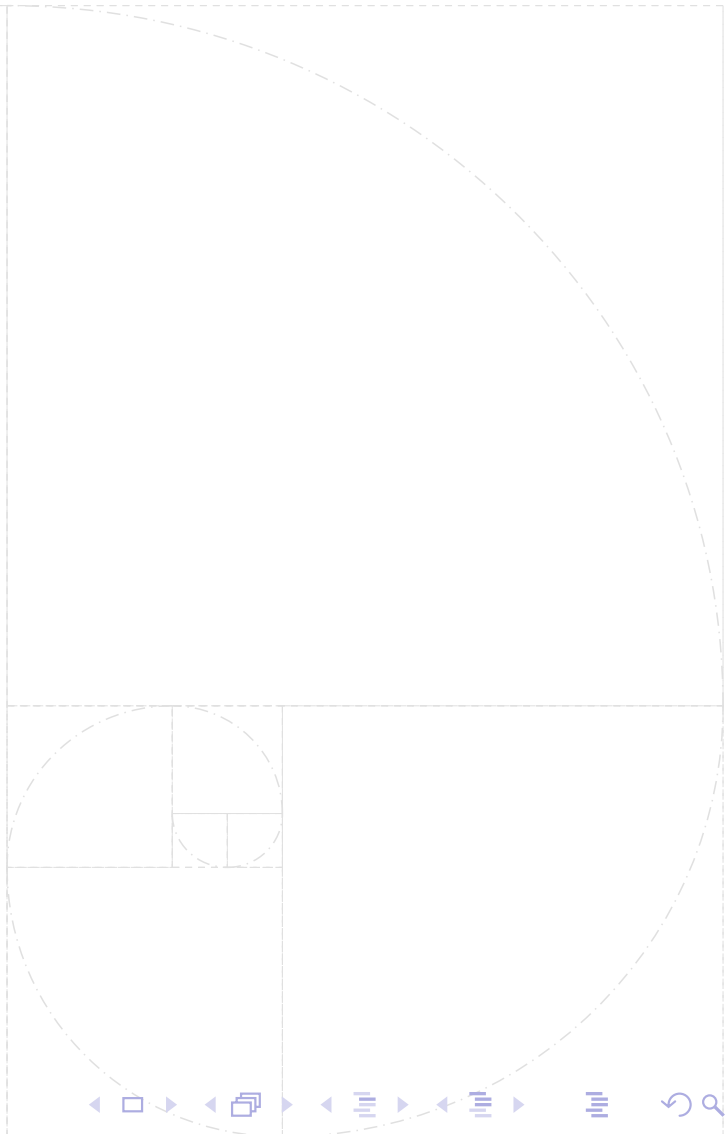
Teorema

$$l(m) = gcd(2, \alpha(m)) \cdot lcm(r(m), \theta(m))$$

donde $\theta(2) = 1$ *y* $\theta(m) = 2$ *para* $m > 2$.

Corolario

$l(m)$ es par para cada $m > 2$.

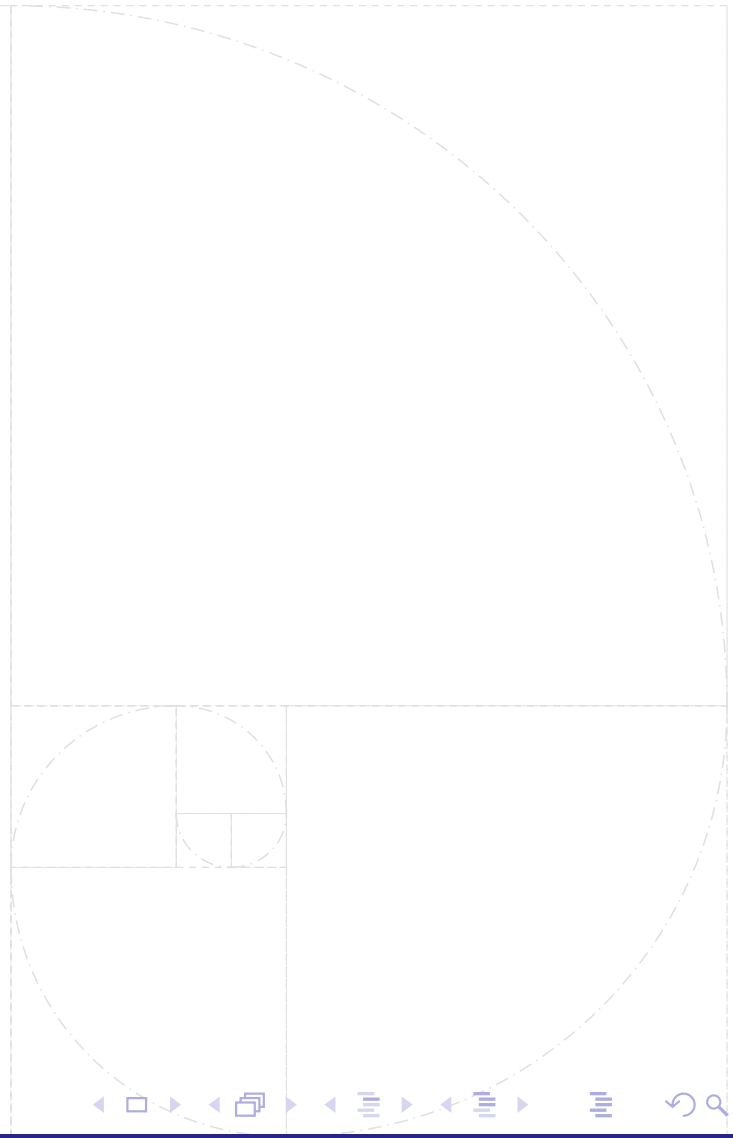


Corolario

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

Corolario

$\alpha(m) = 1$, 2, *ó* 4



Preguntas formuladas

- Comparando computacionalmete los periodos de la sucesión de Lucas y Fibonacci, se observa que estos periodos son iguales en 4 de cada 5 de ellos.

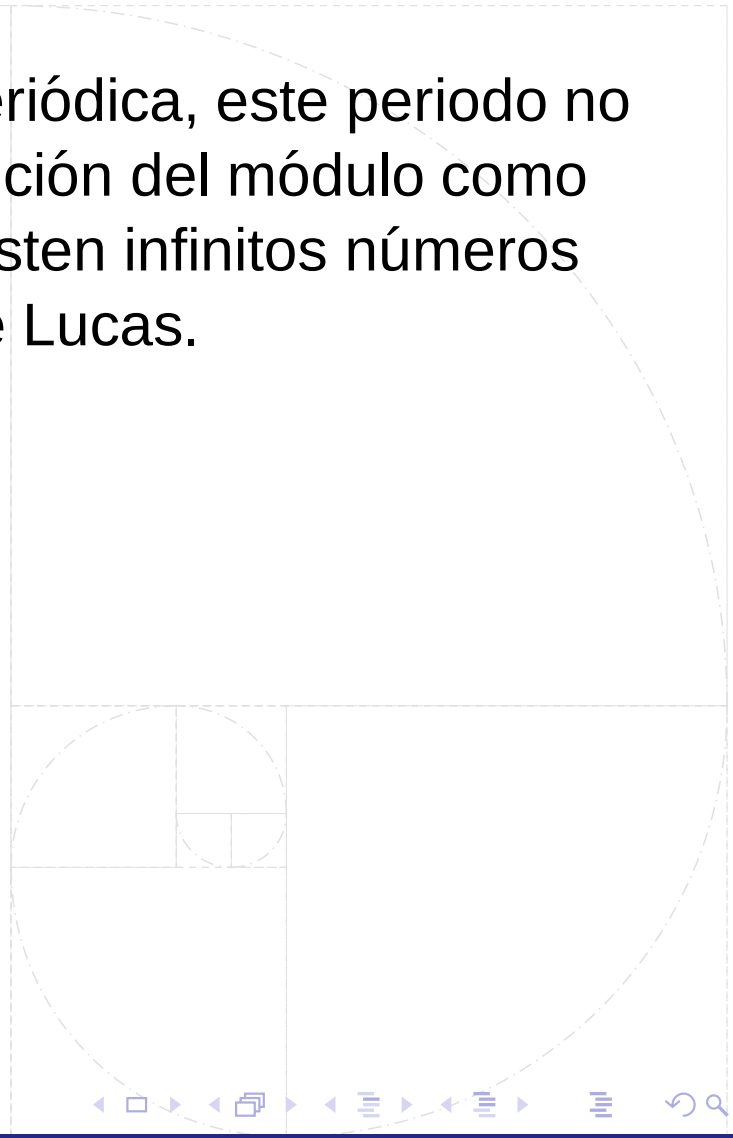
Preguntas formuladas

- Comparando computacionalmete los periodos de la sucesión de Lucas y Fibonacci, se observa que estos periodos son iguales en 4 de cada 5 de ellos.

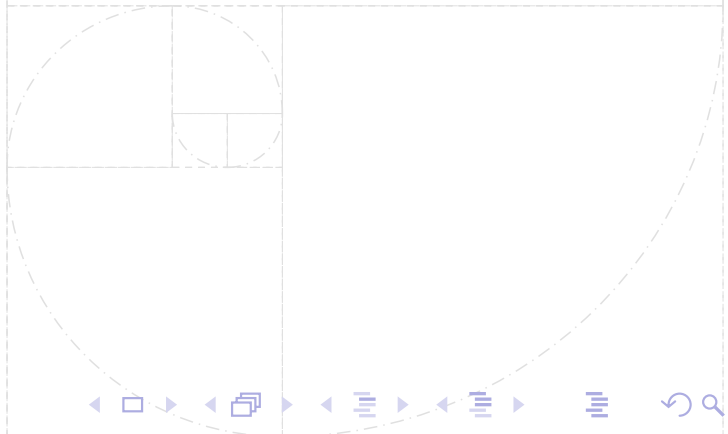
Conjetura

Los periodos de las sucesiones de Lucas y Fibonacci modulo m, son iguales excepto cuando el m es múltiplo de 5, en tales casos el periodo para Fibonacci es cinco veces mayor.

- Si bien la sucesión de Lucas es periódica, este periodo 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.



- Si bien la sucesión de Lucas es periódica, este periodo 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.
  ¿Es posible caracterizar los números que no dividen a ningún número de Lucas?



- Si bien la sucesión de Lucas es periódica, este periodo 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.
  ¿Es posible caracterizar los números que no dividen a ningún número de Lucas?

- Es posible determinar si en la sucesión de Lucas sus términos también poseen *factores característicos* como en la sucesión de Fibonacci.

- Ocejo Monge,Adriana. *Factorización de los números de Fibonacci*. *Tercer taller de teoría de números del centro-sureste 2008.*
- Renault, Marc. *The Fibonacci secuence under varius moduli. 1996*
- Yabuta, M. *A simple proof of CarmichaeVs theorem on primitive divisors, Fibonacci Quaterly, Vol. 39, 2001, p. 439-443.*
- Luca, Florian. *Fibonacci and Lucas numbers with only one distinct digit*. *Portugaliae Mathematica*, vol. 57 fasiculo 2, 2000.
- Riasat, Samin. $\mathbb{Z}[(\varphi)]$ *and the Fibonacci secuence modulo* n. *Mathematical Reflections 1, 2011*

Gracias por su atención