UNIVERSIDAD DE PANAMÁ

VICERRECTORIA DE INVESTIGACIÓN Y POSTGRADO

FACULTAD DE CIENCIAS NATURALES EXACTAS Y TECNOLOGÍA

PROGRAMA DE MAESTRIA EN MATEMÁTICA

“ECUACIÓN DE RECURRENCIA DE LOS NÚMEROS DE MERSENNE”

POR

EDGAR AMETH ATENCIO DE GRACIA

TESIS PRESENTADA COMO REQUISITO PARCIAL PARA OPTAR POR EL TITULO DE MAGÍSTER EN MATEMÁTICA

PANAMÁ, REPÚBLICA DE PANAMÁ

2019

AGRADECIMIENTO

A Dios todo poderoso por darme las habilidades de comprender la matemática.

Al Doctor Jaime Gutiérrez, por sugerirme el tema de la presente investigación y revisión de la misma.

Familiares, amigos y colegas que siempre motivaron a que culminara este proyecto.

ÍNDICE GENERAL

SUMARIO

Los números de Mersenne $M_n = 2^n - 1$ han generado una serie de resultados importantes pero existen algunos, que aún no han sido demostrados formalmente, como es el caso de ¿Cuántos números primos hay en la sucesión de Mersenne?

Con base en lo anterior se examinan los siguientes problemas. La relación de recurrencia de la sucesión de Mersenne y la solución algebraica de la misma. Analizar cuantos números primos dentro de la sucesión de Mersenne y su importancia en la actualidad. También veremos las raíces primas primitivos de los números de Mersenne.

Y utilizamos el álgebra computacional con el Software: Mathematica, para mostrar aspectos relevantes de la sucesión de Mersenne.

SUMMARY

The numbers of Mersenne $M_n = 2^n - 1$ and a series of important results have already been generated, they have not yet been formally demonstrated, as is the case of How many prime numbers there in the succession of Mersenne?

Based on the above, the following problems are examined. The recurrence relation of Mersenne's succession and the algebraic solution of it. How many prime numbers are in the succession of Mersenne and their importance today. We will also see the primitive roots of the Mersenne numbers.

And we use computational algebra with the software: Mathematica, to show relevant aspects of the Mersenne succession.

INTRODUCCIÓN

En la historia con la Matemática han existido conceptos y teorías que en un momento se consideraban inalcanzables, pero gracias al esfuerzo de notables matemáticos hoy día sus esfuerzos nos sirven como base para nuevos descubrimientos en Matemática.

Los aportes de eminentes matemáticos en siglos pasados han creado con sus demostraciones algunos tipos especiales de números primos, como “Los números primos de Mersenne”, los números primos de la forma $2^n - 1$.

Dentro de toda la teoría que encierra los números primos de Mersenne, nos enfocaremos en estudiar la sucesión de recurrencia de los números de Mersenne, y los divisores primos primitivos de dicha sucesión.
Se plantean definiciones, ejemplos, demostraciones e imágenes de resultados del álgebra computacional.

Actualmente el número primo más grande conocido es de esta sucesión, razón por la que en esta investigación se quiere promover el análisis de los números de Mersenne, apoyándonos en software para validar la primalidad o descomposición factorial de estos números.

El presente trabajo consta de tres capítulos, a saber:

En el capítulo 1 estudiaremos las propiedades de los números primos, funciones especiales en Teoría de Números y raíces primitivas de un número; en el capítulo 2, se presentan propiedades de la ecuación en diferencias y las relaciones de recurrencia. Además, se establece la ecuación de recurrencia de las sucesiones de los números de: Fibonacci, Lucas y Mersenne. En el capítulo 3, se presentan algoritmos de programación con apoyo del Álgebra computacional (software Mathematica 10), el cual permite el análisis de algunos resultados de los números primos de Mersenne, divisores primos primitivos entre otros aspectos.

Finalmente, presentamos nuestras conclusiones y recomendaciones.

Capítulo N° 1

NÚMEROS PRIMOS DE MERSENNE

1-NÚMEROS PRIMOS

Es el caso de los números primos, algo tan elemental, en su definiciones y tan complejo para demostrar que ha motivado a personas, estudiosas o no de la Matemática, a querer dilucidar estas grandes encrucijadas que ha proporcionado los números primos a través de los siglos.

Definición 1.1.1: Se dice que un entero $p > 1$ es un número primo, o simplemente que es un primo, en caso de que no exista divisor d de p que satisfaga $1 < d < p$. Si un entero $a > 1$ no es primo, entonces se dice número compuesto.

Ejemplo 1.1.1: 2, 3,5,7, … son primos, mientras que 4, 6, 8, 9, … son compuestos.

Definición 1.1.2: Dos número $a\,, b \in \mathbb{Z}$ se le llaman primos relativos (coprimos o primos entre sí) si $mcd(a, b) = 1$

Proposición 1.1.1: Dos números $a\,, b \in \mathbb{Z}$ diferentes de cero, son primos relativos si y solamente si existen $x_1, y_1 \in \mathbb{Z}$ tal que $ax_1 + b\,y_1 = 1$

Demostración: Considérense las combinaciones lineales $ax_1 + by_1$, donde $x_1, y_1 \in \mathbb{Z}$**.** Este conjunto de enteros $\{ax_1 + b\, y_1\}$ incluye valores positivos y negativos, y también cero 0 seleccionando $x_1 = y_1 = 0$.

Escójanse $x_0\, y\, y_0$ de manera que $ax_0 + by_0$ sea el menor entero positivo k en el conjunto; así $k = ax_0 + by_0$.

Lo anterior nos indica que $k|a$ y $k|b$. Se establecerá la primera propiedad, la segunda se deduce por analogía. Se dará una demostración indirecta de que $k|a$, esto es, se supone que $k \nmid a$ y se obtiene una contradicción. A partir de que $k \nmid a$ se deducen que existen los enteros $q\, y\, r$ tales que $a = kq + r$ con 0< r<k. De aquí se tiene que $r = a - kq = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-ay_0)$. Por tanto, r está en el conjunto $\{ax_1 + b\, y_1\}$. Esto contradice el hecho de que k es el menor entero positivo en el conjunto $\{ax_1 + b\, y_1\}$.

Ahora, puesto que $a\, y\ b$ son primos relativos, 1 es el máximo común divisor de $a\ \ y\ \ b$, $mcd(a, b) = 1$. Donde se deduce $1|a$ y $1|b$ entonces, $a = 1 \cdot a$ y $b = 1 \cdot b$ por consiguiente $k = 1 \cdot ax_0 + 1 \cdot by_0 = 1 \cdot (ax_0 + by_0) = 1 \cdot k$ lo que significa que $1|k$ y que $1 \leq k$; pero $1 < k$ es imposible porque $mcd(a, b)$ =1, necesariamente $1 = k = ax_1 + b\, y_1$.

Teorema 1.1.1: (Teorema de Euclides) El conjunto $\mathbb{p}$ de los números primos es infinito.

Demostración: Supongamos que el conjunto $\mathbb{p} = \{p_1, p_2, p_3, \ldots, p_{r-1}, p_r\}$ es un conjunto finito. Consideremos el número natural $n = p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_r + 1$

Por el teorema fundamental de la aritmética, este $n > 1$ es divisible por algún primo q. Supongamos que $q = p_k$ para algún $k \in \{1, 2, 3, \ldots, r\}$ lo cual es un absurdo (contradicción) $q|1$. Luego $\mathbb{p}$ no es un conjunto finito.

Definición 1.1.3: Si $M_n = 2^n - 1$ es primo, con n un entero positivo, entonces es llamado número primo de Mersenne.

Ejemplo 1.1.2: Los cinco primeros números primos de Mersenne y los primos que lo generan. $\{M_n\} = \{3, 7, 31, 127, 8191, \ldots\}$

n	$M_n = 2^n - 1$
2	3
3	7
5	31
7	127
13	8191

Cuadro 1

1.2- HISTORIA DE LOS NÚMEROS PRIMOS DE MERSENNE.

Ya desde el Génesis de la Aritmética, se mencionan los números primos. Desde entonces la búsqueda de estos particulares números ha fascinado a grandes matemáticos a lo largo de toda la historia.

En este proyecto nos centraremos en la búsqueda de unos números primos más concretos, los números primos de Mersenne.

Aunque reciben su denominación en honor a Marín Mersenne, a lo largo de la Historia estos números han sido analizados en varias ocasiones por matemáticos de renombre, incluso anteriores a Mersenne, y han sido protagonistas de varias anécdotas curiosas.

Inicialmente se pensaba que cualquier número de la forma $2^p - 1$ (con p primo) sería primo en todos los casos. No fue hasta 1536 que Hudalricus Regius fue capaz de demostrar que esto no era cierto para el caso $2^{11} - 1$, dado que es el resultado de la multiplicación 23*89.

Años después, Pietro Cataldi confirmó que $2^{17} - 1$ y $2^{19} - 1$ son primos, sin embargo, afirmó lo mismo para los exponentes 23, 29, 31 y 37, afirmación que acabó mostrándose incorrecta, para los números 29 y 31 en 1640, por intervención de Fermat y mucho más tarde, en 1738, por Euler.

En 1644, fue, por fin, Mersenne, en su Cognitata Physica-Mathematica, quien postuló que los números de la forma $2^n - 1$ eran números primos para : $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ y 257. Y afirmando para todos los exponentes menores que 257 el hecho de que $2^n - 1$ no era primo.

Como podemos observar Mersenne incluyó en su lista erróneamente los exponentes 67 y 257 que no son primos.

El propio Mersenne reconoció que no había podido comprobar la primalidad de todos aquellos números, pero tampoco lo logró ninguno de sus contemporáneos. Fue necesario esperar alrededor de cien años, para ver confirmada la primalidad de $2^{31} - 1$, gracias a Leonhard Euler en el año 1772, cabe destacar que $2^{31} - 1$ se consideró el número primo más grande hasta el año 1867.

Fue entonces cuando aparecieron las primeras calculadoras mecánicas; los siguientes primos de Mersenne fueron encontrados haciendo uso de ellas:

en 1876 Édouard Lucas verifica la primalidad de $2^{127} - 1$ y siete años más tarde Ivan Mikheevich Pervushin demuestra que $2^{61} - 1$ es primo. Por tanto, es así como se encuentra la primera omisión en la lista de Mersenne.

Más tarde, en 1903 F.N.Cole en una reunión de la American Mathematical Society demostró que $2^{257} - 1$ correspondía al resultado de la multiplicación de 193707721 y 761838257287.

En 1911 y 1914 Ralph Ernest Powers demuestra dos omisiones más en la lista de números primos de Mersenne, $2^{89} - 1$ y $2^{107} - 1$.

Sin embargo, no es hasta 1947 que el rango $n < 258$ se ve totalmente comprobado y se determina que la lista correcta es:

$n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107\ y\ 127$.

Gracias al Test de Lucas-Lehmer y a los inicios del desarrollo de la computación, la verificación de primos de Mersenne avanzó significativamente. En esta nueva etapa de la búsqueda de primos de Mersenne podemos resaltar cómo se encontró M_{521}, en enero de 1952, gracias al programa escrito y ejecutado por el profesor R.M. Robinson bajo la dirección de Lehmer, con sólo unas horas más tarde encontró M_{607}. Durante los meses siguientes fueron encontrados M_{1279}, M_{2203}, y M_{2281}. Posteriormente, los siguientes primos de Mersenne fueron descubiertos incrementando la potencia de cálculo con computadores como el Cray I o el IBM 7090.

En la actualidad la búsqueda se basa en la computación distribuida. En 1996, surge el proyecto GIMPS, el cual se dedica a la búsqueda de números primos de Mersenne mediante el uso colaborativo de recursos a través de la red y la computación distribuida.

Desde el inicio del proyecto, se han encontrado 17 nuevos primos de Mersenne, el último fue encontrado el 7 de diciembre de 2018, $M_{82.589.933}$ con la nada despreciable longitud de 24.862.048 cifras.

En total, a lo largo de la Historia, tan solo se conocen 51 primos de Mersenne.

No se conoce si existen más números primos de Mersenne entre el 47º ($M_{43.112.609}$) y el 51º ($M_{82.589.933}$) por lo tanto, esta tabla es provisional. Por poner un ejemplo histórico, el 29º número primo de Mersenne fue descubierto después del 30º y el 31º.

1.3- FUNCIONES ESPECIALES EN TEORÍA DE NÚMEROS

La función φ de Euler es una función importante en la Teoría de Números.

Definición 1.3.1.: Si n es un número entero positivo, entonces $\varphi(n)$ se define como el número positivo menor o igual a n y coprimos con n, es decir:

$$\varphi(n) = |\{k \in \mathbb{N}/1 \leq k \leq n \ \wedge \ mcd(n,k) = 1\}|$$

Se le conoce como función $\varphi(n)$ de Euler.

Teorema 1.3.1: (Teorema de Euler) Si $n \in \mathbb{N}$ y a enteros con $mcd(a,n) = 1$ primos relativos, entonces $a^{\varphi(n)} \equiv 1\ (mod\ n)$.

Demostración: Podemos suponer $n \geq 2$. Sean $1 = b_1 < b_2 < \ldots < b_{\varphi(n)} = n-1$ Los restos entre $0, 1, 2, \ldots, n-1$ y primos relativos con n. Tenemos que $\{b_1, b_2, \ldots, b_{\varphi(n)}\}$ es un sistema reducido de restos $(mod\ n)$, $\forall\ i, j = 1,2,\ldots,\varphi(n)$: $ab_i \equiv ab_j\ (mod\ n) \Rightarrow b_i = b_j \Rightarrow$ i = j

Por otro lado, $ab_1 \cdot ab_2 \cdot \ldots \cdot ab_{\varphi(n)} \equiv b_1 \cdot b_2 \cdot \ldots \cdot b_{\varphi(n)}\ (mod\ n)$,

Ósea $a^{\varphi(n)} \cdot b_1 \cdot b_2 \cdot \ldots \cdot b_{\varphi(n)} \equiv b_1 \cdot b_2 \cdot \ldots \cdot b_{\varphi(n)}\ (mod\ n)$.

Como $mcd\ (b_1 \cdot b_2 \cdot \ldots \cdot b_{\varphi(n)}, n) = 1$, podemos cancelar este factor de congruencia y obtenemos $a^{\varphi(n)} \equiv 1\ (mod\ n)$.

Definición 1.3.2: (Función Sigma (σ)) Para cada $n \in \mathbb{Z}$, la función sigma se define por $\sigma(n) = \sum_{(d|n)} d$. Es decir, la suma de los divisores positivos de n.

Definición 1.3.3: (Números Perfectos) Decimos que un entero positivo n es perfecto si la suma de sus divisores menores que n coincide con $2n$, Es decir, si $\sigma(n) = 2n$.

Ejemplo 1.3.1: Tabla con los números de elementos de $\varphi(n)$ para $n = 1\ a\ 30$

n	$\varphi(n)$	n	$\varphi(n)$	n	$\varphi(n)$
1	1	11	10	21	12
2	1	12	4	22	10
3	2	13	12	23	22
4	2	14	6	24	8
5	4	15	8	25	20
6	2	16	8	26	12
7	6	17	16	27	18
8	4	18	6	28	12
9	6	19	18	29	28
10	4	20	8	30	8

Cuadro 2

Observación: Es claro que, $n = p$ = primo, se tiene que $\varphi(p) = p - 1$.

Propiedades de la función Sigma:

1- La función sigma de n es multiplicativa

2- Si p es un número primo, entonces $\sigma(p) = p + 1$

3- Si p es un número primo $\sigma(p^{\alpha}) = \frac{p^{\alpha+1}-1}{p}$

La función sigma σ de n está relacionada con el clásico problema de los números perfectos, que encierra temas abiertos de Teoría de Números:

a) Determinar si existen infinitos números perfectos.

b) Demostrar la imposibilidad de un número perfecto impar o encontrar uno.

Ejemplo 1.3.3: El primer número perfecto es el 6 cuyos divisores son: 1; 2; 3 y 6. Ósea, $\sigma(6) = 1 + 2 + 3 + 6 = 12 = 2(6)$.

El siguiente número perfecto es el 48.

Ejemplo 1.3.2.: Los divisores de 8 son: 1; 2; 4; 8, entonces

$\sigma(8) = 1 + 2 + 4 + 8 = 15$

Para distintos valores podemos hacer una tabla para la función sigma.

n	1	2	3	4	5	6	7	8	9	10
$\sigma(n)$	1	3	4	7	6	12	8	15	13	18

Cuadro 3

Teorema 1.3.2: Consideremos la clasificación de Euclides y Euler de los números perfectos pares. Un número natural $n \in \mathbb{N}$ es perfecto si $\sigma(n) = 2n$

a) (Euclides) si $k \geq 2$ es tal que $p = 2^k - 1$ es primo, Entonces

$n = 2^{k-1}(2^k - 1)$ es perfecto.

b) (Euler) Todo número perfecto par es obtenido por el método a)

Demostración:

a) Sea $k \geq 2$ es tal que $p = 2^k - 1$ es primo. Como $mcd(2^{k-1}, 2^k - 1) = 1$. Calculemos:

$\sigma(n) = \sigma(2^{k-1}(2^k - 1)) = \sigma(2^{k-1}) \cdot \sigma\,(2^k - 1) = (1 + 2 + \ldots + 2^{k-1}) \cdot (1 + p)$

$= (2^k - 1) \cdot (1 + p) = (2^k - 1) \cdot 2^k = 2 \cdot 2^{k-1} \cdot (2^k - 1) = 2n,$

Mostrando que $n = 2^{k-1}(2^k - 1)$ es perfecto.

b) Sea n cualquier número perfecto par. Podemos escribirlo como $n = 2^{k-1} \cdot m$ con $k \geq 2$ y m impar. Como n es perfecto, concluimos

$2^k \cdot m = 2n = \sigma(n) = \sigma(2^{k-1} \cdot m) = \sigma(2^{k-1}) \cdot \sigma(m) = (2^k - 1) \cdot \sigma(m)$

Entonces, $(2^k - 1) | 2^k \cdot m$ como $mcd(2^k - 1, 2^k) = 1$, concluimos $2^k - 1 | m$

Luego existe un $T \in \mathbb{N}$ con $(2^k - 1)T = m$. Además, para $t \neq m$, pues $k \geq 2$ tal que, $2^k \cdot (2^k - 1)T = 2^k \cdot m = (2^k - 1)\,\sigma(m)$.

Ósea, $2^k \cdot T = \sigma(m) \geq m + T = 2^k \cdot T$

Por tanto, $\sigma(m) = T + m$. Concluimos que T y m son los únicos divisores de m. Particularmente, $T = 1$ y $m = 2^k - 1$ es primo. Luego el n –ésimo término de la forma $n = 2^{k-1}(2^k - 1)$ con $2^k - 1$ primo.

Proposición 1.3.1: Si $M_k = 2^k - 1$ es primo, entonces $k = p$ es primo. Esta condición es necesaria, pero no es suficiente.

Demostración: (Contraejemplo: considerando el número primos 11, no se cumple) $M_{11} = 20147 = 23 \cdot 89$ no es primo, a pesar de que $k = 11$ es primo.

Teorema 1.3.3: Sean $2 \leq a, k \in N$. Si $a^k - 1$ primo, entonces $a = 2$ y k es primo.

Demostración: Tenemos $a^k - 1 = (a-1)(1 + a + a^2 + \ldots + a^{k-1})$ con $(1 + a + a^2 + \ldots + a^{k-1}) > 1$, pues $k \geq 2$. Ahora si $a^k - 1$ es primo, concluimos $a - 1 = 1$, ósea $a = 2$.

Sea $k = rs$ tal que $1 < s \leq r < k$. con $a = 2^r$ y $n + 1 = s$ tenemos que la descomposición $2^k - 1 = (2^r - 1)(1 + 2^r + 2^{2r} + \ldots + 2^{(k-1)r})$ en el cual $2^r - 1 > 1$ y $1 + 2^r + 2^{2r} + \ldots + 2^{(k-1)r} > 1$, pues $s > 1$. Luego $2^k - 1$ no es primo cuando *k* es compuesto.

1.4- RAÍCES PRIMITIVAS

Definición 1.4.1: El orden de Raíces primitivas módulo n: Para $n \in \mathbb{N}$ y $a \in \mathbb{Z}$ con $mcd(a,n) = 1$ por el teorema 1.3.1 tenemos $a^{\varphi(n)} \equiv 1\ (mod\ n)$ Particularmente, existe un exponente $k > 0$ (por ejemplo $k = \varphi(n)$) tal que: $a^k \equiv 1\ (mod\ n)$.

Definición 1.4.2: Sea $n \in \mathbb{N}$ y $a \in \mathbb{Z}$ con $mcd(a,n) = 1$. El menor número $k_0 \epsilon \mathbb{N}$ tal que $a^{k_0} \equiv 1\ (mod\ n)$. Indicado por $k_0 = 0_n(a)$ se le conoce como el orden de a módulo n.

Observemos que el teorema 1.3.1 (Teorema de Euler) garantiza: $0_n(a) \leq \varphi(n)$
Es claro que si $0_n(a) = 1 \Leftrightarrow a \equiv 1\ (mod\ n)$. Además, como
$n - 1 \equiv -1\ (mod\ n)$ tenemos que $0_n(n-1) = 2$, si $n \geq 3$.
Cabe destacar que el símbolo $0_n(a)$ no está definida, si $mcd(a,n) > 1$!

Teorema 1.4.1.: Sea $n \in \mathbb{N}, a \in \mathbb{Z}$ *con* $mcd(a,n) = 1$ y supongamos $a^k \equiv 1\ (mod\ n)$ para algún $k \in \mathbb{N}$. Entonces $o_n(a)|k$, particularmente $o_n(a)|\varphi(n)$

Demostración: La división de k por $o_n(a)$ es $k = l \cdot o_n(a) + r$ con $0 \leq r \leq o_n(a) - 1$ se tiene:

$$1 \equiv a^k = a^{l \cdot o_n(a) + r} = \left(a^{\cdot o_n(a)}\right)^l \cdot a^r \equiv (1)^l \cdot a^r \equiv a^r \ (mod\ n).$$

Concluimos $r = 0$, por la minimalidad de $o_n(a)$. Luego $o_n(a)|k$

Teorema 1.4.2: Sea $n \in \mathbb{N}, a \in \mathbb{Z}$ *con* $mcd(a,n) = 1$, supongamos $i, j \in \mathbb{N}_0$

$$a^i \equiv a^j \ (mod\ n) \Leftrightarrow i \equiv j \ (mod\ o_n(a)).$$

Demostración:

" ⇐ " $i \equiv j \ (mod\ o_n(a))$ significa $i = j + l \cdot o_n(a)$ con $l \in \mathbb{N}_0$ quedando $i \geq j$.

Tenemos: $a^i = a^{j + l \cdot o_n(a)} = \left(a^{\cdot o_n(a)}\right)^l \cdot a^j \equiv (1)^l \cdot a^j \equiv a^j \ (mod\ n)$.

" ⇒ " Supongamos que $a^i \equiv a^j \ (mod\ n)$ con $i \geq j$. Tal que $a^{i-j} \equiv 1 \ (mod\ n)$ por teorema 1.4.1 concluimos $o_n(a)|\ (i - j)$, que sea $i \equiv j \ (mod\ o_n(a))$.

Teorema 1.4.3: Los números $\{1, a, a^2, a^3, \ldots, a^{o_n(a)-1}\}$ son incongruentes módulo n.

Demostración: De $a^i \equiv a^j \ (mod\ n)$, con $0 \leq i\ ,\ j \leq o_n(a) - 1$ entonces $i \equiv j \ (mod\ o_n(a))$ por teorema 1.4.2 entonces $i = j$

Lema 1.4.1: Sea $o_n(a) = \varphi(n)$. Entonces $\{a, a^2, a^3, \ldots, a^{\varphi(n)-1},\ a^{\varphi(n)} \equiv 1\}$ es un sistema reducido de restos módulo n.

Generalizando si encontramos un resto a que sea primo relativo con n, del máximo orden posible, a saber, $o_n(a) = \varphi(n)$, conseguimos un sistema reducido de residuos, lo cual consiste en las potencias de a.

Definición 1.4.3: Sea $n \in \mathbb{N}$, un número $a \in \mathbb{Z}$ tal que: $o_n(a) = \varphi(n)$, es llamada una raíz primitiva módulo n .

Proposición 1.4.1.: sea $n \in \mathbb{N}, a \in \mathbb{Z}$ *con* $mcd(a,n) = 1$ *y sea* $h \in \mathbb{N}$ entonces

$$o_n(a^h) = \frac{o_n(a)}{mcd(h, o_n(a))}$$

Demostración: Sea $r = o_n(a^h)$, $k_0 = o_n(a)$ *y* $d = mcd(h, k_0)$.

Escribamos $h = h_1 d$ *y* $k_0 = k_1 d$ *con* $mcd(h_1, k_1) = 1$.

De $(a^h)^{k_1} = (a^{h_1 d})^{\frac{k_0}{d}} = a^{h_1 k_0} = (a^{k_0})^{h_1} \equiv 1^{h_1} \equiv 1 \ (mod\ n)$

Concluimos que $r = o_n(a^h) | k_1$ particularmente, $r \leq k_1$

$(a^h)^r \equiv 1 \ (mod\ n)$ entonces $a^{hr} \equiv 1 \ (mod\ n)$ lo cual significa que:

$k_0 = o_n(a) | hr \Rightarrow k_1 d | h_1 dr \Rightarrow k_1 | h_1 r \Rightarrow k_1 | r$

Entonces $k_1 \leq r$ *y así* $o_n(a^h) = r = k_1 = \frac{k_0}{d} = \frac{o_n(a)}{mcd(h, o_n(a))}$.

Lema 1.4.2: $o_n(a^h) = o_n(a) \Leftrightarrow mcd(h, o_n(a)) = 1$

Lema 1.4.3: Sea a una raíz primitiva módulo n. Entonces existen exactamente $\varphi(\varphi(n))$ raíces primitivas incongruentes módulo n.

Demostración: $\{a, a^2, a^3, \ldots, a^{\varphi(n)-1},\ a^{\varphi(n)} \equiv 1\}$ es un sistema reducido de restos $mod\ n$ como $o_n(a) = \varphi(n)$. Para $h \in \{1, 2, \ldots, \varphi(n)\}$ tenemos que a^h es raíz primitiva sí y sólo sí $o_n(a^h) = o_n(a)$, sí y sólo sí $mcd(h, \varphi(n)) = 1$ Existen $\varphi(\varphi(n))$ tal que h en los $1, 2, \ldots, \varphi(n)$.

Teorema 1.4.4: Para todo $k \geq 3$ y $\forall\ a \in \mathbb{Z}$ impar, se tiene $a^{2^{k-2}} \equiv 1\ (mod\ 2^k)$.

Demostración: Esta afirmación es verdadera para $k = 3$, pues siempre $a^2 \equiv 1\ (mod\ 8)$. Probemos la afirmación por inducción sobre k: Supongamos $a^{2^{k-2}} \equiv 1\ (mod\ 2^k)$ ya probado para algún $k \geq 3$. Entonces, $a^{2^{k-2}} = 1 + \ell \cdot 2^k$ para algún $\ell \in \mathbb{Z}$ de donde $a^{2^{k-1}} = \left(a^{2^{k-2}}\right)^2 = (1 + \ell\, 2^k)^2 = 1 + 2\ell\, 2^k + \ell^2\, 2^{2k}$ $= 1 + \ell\,(1 + \ell \cdot 2^{k-1})2^{k+1} \equiv 1\ (mod\ 2^{k+1})$. Por lo tanto, $a^{2^{k-2}} \equiv 1\ (mod\ 2^k)$ para todo $k \geq 3$ y para todo $a \in \mathbb{Z}$ impar.

Ejemplo 1.4.1: Para $n = 7$ tenemos $o_7(3) = 6 = \varphi(7)$ y $\{3, 3^2, 3^3, 3^4, 3^5, 3^6\}$ es un sistema reducido de restos $mod\ 7$ porque

$$3 \equiv 3,\ \ 3^2 \equiv 2,\ \ 3^3 \equiv 6,\qquad 3^4 \equiv 4,\ \ 3^5 \equiv 5,\ \ 3^6 \equiv 1\ (mod\ 7)$$

Lo mismo ocurre para $\{5, 5^2, 5^3, 5^4, 5^5, 5^6\}$.

Ejemplo 1.4.2: Para algunos valores de n, las tablas de los menores restos no negativos de a, coprimos con n, y sus ordenes $0_n(a)$

$n=3$	a	1 2
$\varphi(3)=2$	$o_3(a)$	1 2

$n=4$	a	1 3
$\varphi(4)=2$	$o_4(a)$	1 2

$n=5$	a	1 2 3 4
$\varphi(5)=4$	$o_5(a)$	1 4 4 2

$n=6$	a	1 5
$\varphi(6)=2$	$o_6(a)$	1 2

$n=7$	a	1 2 3 4 5 6
$\varphi(7)=6$	$o_7(a)$	1 3 6 3 6 2

$n=8$	a	1 3 5 7
$\varphi(8)=4$	$o_8(a)$	1 2 2 2

$n=9$	a	1 2 4 5 7 8
$\varphi(9)=6$	$o_9(a)$	1 6 3 6 3 2

$n=12$	a	1 5 7 11
$\varphi(12)=4$	$o_{12}(a)$	1 2 2 2

Cuadro 4

Ejemplos 1.4.3: Para $n=22$ se tiene que: $\varphi(22)=\varphi(2)\varphi(11)=1\cdot 10=10$

Los menores restos no negativos y primos relativos con 22 son:

$n=22$	a	1 3 5 7 9 13 15 17 19 21
$\varphi(22)=10$	$o_{22}(a)$	1 5 5 10 5 10 5 10 10 2

Cuadro 5

El orden de cualquiera de estos números a es un divisor de 10 , ósea $o_{22}(a) = \{1, 2, 5, 10\}\ \forall a \in \{1, 3, 5, 7, 9, 13, 15, 17, 19, 21\}$.

Las raíces primitivas $mod\ 22$ son $\{7, 13, 17, 19\}$ por ejemplo $\{7, 7^2, 7^3, \ldots, 7^9, 7^{10} \equiv 1\}$ y es también, un sistema reducido de restos $mod\ 22$. Tenemos $\varphi(\varphi(22)) = \varphi(10) = 4$ y los 4 números primos relativos con 10 son $\mathrm{h} = 1, 3, 7, 9$. Entonces $\{7, 7^3, 7^7, 7^9\}$ son raíces primitivas $\mathrm{mod}\ 22$ que son incongruentes. Ellas claramente son congruentes a $\{7, 13, 17, 19\}$.

Ejemplos 1.4.4: En los cuadros anteriores del ejemplo 1.4.1 se mostró

a) 2 es una raíz primitiva $mod\ 3$
b) 3 es un a raíz primitiva $mod\ 4$
c) 2 y 3 son raíces primitivas $mod\ 5$
d) 5 es una raíz primitiva $mod\ 6$
e) 5 y 3 son raíces primitivas $mod\ 7$
f) No hay raíz primitiva $mod\ 8$
g) 2 y 5 son raíces primitivas $mod\ 9$
h) No hay raíz primitiva $mod\ 12$

Definición 1.4.3: (Divisores primos primitivos)
Un número primitivo p es llamado divisor primitivo de la sucesión $\{P\}$. Si p divide al término P_n distinto de cero y es co-primo a todos los términos P_m distintos de cero para $m < n$.

Lema 1.4.4: un número primo p es un divisor primitivo de P_n sí y sólo sí p divide a P_n y $p > 2n$.

Capítulo N° 2

RECURRENCIA DE LOS NÚMEROS DE MERSENNE

RECURRENCIA DE LOS NÚMEROS DE MERSENNE

Para estudiar el comportamiento de los elementos de la sucesión de Mersenne, nos apoyamos de la teoría de recurrencia. En especial de las ecuaciones de recurrencia lineales de segundo orden.

2.1- SUCESIÓN DE NÚMEROS DE MERSENNE para $n \geq 1$

$$\{M_n\} = \{1, 3, 7, 15, 31, 63, 127, 255, 511, 1023, \ldots, 2^n - 1, \ldots\}$$

n	$M_n = 2^n - 1$	Descomposición en factores primos
1	1	1
2	3	3
3	7	7
4	15	$3 * 5$
5	31	31
6	63	$3^2 * 7$
7	127	127
8	255	$3 * 5 * 17$
9	511	$7 * 73$
10	1023	$3 * 11 * 31$
⋮	⋮	⋮

Cuadro 6

Considerando la definición 1.4.3 sacamos los primos primitivos asociados a la sucesión de Mersenne.

n	$M_n = 2^n - 1$	Descomposición en factores primos	Factores primos	Primos primitivos
1	1	–	–	–
2	3	3	3	3
3	7	7	7	7
4	15	$3 * 5$	3, 5	5
5	31	31	31	31
6	63	$3^2 * 7$	3, 7	–
7	127	127	127	127
8	255	$3 * 5 * 17$	3, 5, 17	17
9	511	$7 * 73$	7, 73	73
10	1023	$3 * 11 * 31$	3, 11, 31	11
11	2047	$23 * 89$	23, 89	23, 89
12	4095	$3^2 * 5 * 7 * 13$	3, 5, 7, 13	13
13	8191	8191	8191	8191
14	16383	$3 * 43 * 127$	3, 43, 127	43

Cuadro 7

2.2. Ecuación en Diferencias

Definición 2.2.1: Una ecuación en diferencias es una expresión del tipo:

$$(f(n), f(n+1), \ldots, f(n+k)) = 0, \quad \forall n \epsilon\, \mathbb{Z},$$

donde f es una función.

Si después de simplificar esta expresión, obtenemos los términos $f(n+k_1)$ y $f(n+k_2)$ como el mayor y el menor, respectivamente, se dice que la ecuación es de orden $k = k_1 - k_2$

Definición 2.2.2: Una ecuación en diferencias de orden k se dice lineal si puede expresarse de la forma:

$$p_0(n)f(n+k) + p_1(n)f(n+k-1) + \ldots + p_k(n)f(n) = g(n) \qquad (1)$$

donde los coeficientes p_i son funciones definidas en $\mathbb{Z}$.

El caso más sencillo es cuando los coeficientes son constantes

$$a_0 f(n+k) + a_1 f(n+k-1) + \ldots + a_k f(n) = g(n).$$

La ecuación en diferencias se dice homogénea en el caso de que $g(n) = 0$, y completa en el caso contrario.

Teorema 2.2.1: Dada la ecuación en diferencias lineal de coeficientes constantes y de orden *k* .

$$a_0 f(n\ +\ k)\ +\ a_1 f(n\ +\ k-1) + \ldots + a_k f(n)\ =\ g(n)$$

el problema de hallar una función f definida en $\mathbb{Z}$, que verifique la ecuación, y tal que en los k enteros consecutivos $n_0, n_0+1, \ldots, n_0+k-1$ tome los valores dados $c_0, \mathrm{c}_1, \ldots, \mathrm{c}_{\mathrm{k}-1}$, tiene solución única.

Demostración:

Sea la ecuación en diferencias lineal homogénea de coeficientes constantes y de orden k :

$$a_0 f(n+k) + a_1 f(n+k-1) + \ldots + a_k f(n)\ =\ 0, \forall n \in Z.$$

Buscaremos soluciones del tipo $f(n)\ =\ r^n$, $r \neq 0$

Entonces:

$$r^n(a_0 r^k + a_1 r^{k-1} + \cdots +\ a_k) = 0$$

$$a_0 r^k\ +\ a_1 r^{k-1} + \ldots + a_k\ =\ 0$$

Por tanto, r_k es raíz k-ésima de la ecuación característica asociada a la ecuación en diferencia.

$$a_0 r^k\ +\ a_1 r^{k-1} + \ldots + a_k = 0 \qquad (2)$$

Sean $r_1, r_2, \ldots, r_k$ las k raíces de la ecuación característica. Se definen entonces las funciones: $f_j(n) = r_j^n$, j $= 1, \ldots,$ k. Entonces $\{f_1, \ldots, f_k\}$ es un sistema fundamental de soluciones (funciones linealmente independientes), lo cual nos permite resolver la ecuación. Se tiene que la solución general es la combinación lineal del conjunto fundamental de soluciones, para cualquier valor constante C_k:

$$f = C_1 f_1 + C_2 f_2 \ldots + C_k f_k.$$

Considerando las condiciones iniciales se produce un valor propio para cada C_k.siendo entonces una solución única asociada.

Definición 2.2.3: Una ecuación de recurrencia lineal (de orden k) es de la forma:

$$\sum_{i=0}^{k} C_i a_{n+i} = f_n$$

para $n \geq 0$ donde $i = 1,2, \ldots, k$; $C_i \in \{\mathbb{R}, \mathbb{C}\}$ y (f_n) es una sucesión conocida.

Las relaciones de recurrencia ocurren naturalmente al momento de modelar problemas de conteo, por consiguiente, esto genera retos de cómo resolver estas relaciones de recurrencia algebraicamente.

En este proyecto, las recursiones y las relaciones de recurrencia juegan un papel primordial para poder definir la forma algebraica de las sucesiones de números de Mersenne y así poder analizar sus raíces primas primitivas.

La ecuación en diferencias nos permite ver en las funciones polinomiales la solución en recurrencia a partir raíces de polinomios asociados.

2.3- Relación de Recurrencia:

Definición 2.3.1: Una relación de recurrencia de orden n para la sucesión $\{a_n\}$ es una ecuación que expresa $\{a_n\}$ en términos de $\{a_0, a_1, \ldots, a_{n-1}\}$, para todo entero $n \geq n_0$.

A los valores de los términos necesarios para empezar a calcular la relación de recurrencia se les conoce como condiciones iniciales.

Definición 2.3.2: Una relación de recurrencia lineal homogénea que tiene coeficientes enteros es de la forma:

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}, \qquad (3)$$

donde $c_1, c_2, \ldots, c_k$ son números reales y $c_k \neq 0$. Decimos que la relación en este caso es de grado k.

Sabemos que una sucesión, es una solución de la relación de recurrencia si su término general verifica dicha relación.

De (2) esto es cierto sí y sólo sí:

$$r^n = c_1 r^{n-1} + c_2 r^{n-2} + \cdots + c_k r^{n-k}$$

O equivalentemente para $\mathrm{n} = \mathrm{k}$ tenemos:

$$r^k - c_1 r^{k-1} - c_2 r^{k-2} - \cdots - c_k = 0. \qquad (4)$$

Por tanto, la sucesión $\{a_n\} = r^n$ es una solución a la relación de recurrencia sí y sólo sí es solución de la ecuación (4) (llamada ecuación característica).

La idea es tratar de buscar soluciones de la forma r^n , donde r es una constante. En el caso particular, estudiaremos relaciones de recurrencia de segundo grado.

Definición 2.3.3: Para c_1, c_2 constantes, una ecuación de recurrencia de segundo grado es:

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} \qquad (5)$$

De (4) su polinomio característico asociado es:

$$r^2 - c_1 r - c_2 = 0 \qquad (6)$$

Teorema 2.3.1: Sean c_1, c_2 números reales y $k = 2$ tenemos:

$r^2 - c_1 r - c_2 = 0$ con dos raíces distintas r_1 y r_2. Entonces la sucesión $\{a_n\}$ es una solución a la relación de recurrencia $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ sí y sólo sí, $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ para $n = 0, 1, 2, \ldots$ donde α_1 y α_2 son constantes.

Demostración:

($\Longleftarrow$) Si $\{a_n\} = \alpha_1 r_1^n + \alpha_2 r_2^n$ para $n = 0, 1, 2, \ldots$ donde α_1 y α_2 son constantes. Entonces, la sucesión $\{a_n\}$ es una solución a la relación de recurrencia $\{a_n\} = c_1 a_{n-1} + c_2 a_{n-2}$

Sea $\{a_n\} = \alpha_1 r_1^n + \alpha_2 r_2^n$ y como r_1 y r_2 son raíces, entonces:

$$r_1^2 = c_1 r_1 + c_2 \quad \text{y} \quad r_2^2 = c_1 r_2 + c_2$$

Por tanto,

$c_1 a_{n-1} + c_2 a_{n-2}$

$= c_1(\alpha_1 r_1^{n-1} + \alpha_2 r_2^{n-1}) + c_2(\alpha_1 r_1^{n-2} + \alpha_2 r_2^{n-2})$

$= \alpha_1 r_1^{n-2}(c_1 r_1 + c_2) + \alpha_2 r_2^{n-2}(c_1 r_2 + c_2)$

$= \alpha_1 r_1^n + \alpha_2 r_2^n$

$= a_n$

Concluimos que $\{a_n\} = \{\alpha_1 r_1^n + \alpha_2 r_2^n\}$ es una solución a la relación de recurrencia.

Si la sucesión $\{a_n\}$, es una solución a la relación de recurrencia

$$\{a_n\} = c_1 a_{n-1} + c_2 a_{n-2}$$

entonces,

$$\{a_n\} = \alpha_1 r_1^n + \alpha_2 r_2^n$$

para $n = 0, 1, 2, \ldots$ donde α_1 y α_2 son constantes.

(⇒) Asumamos ahora que $\{a_n\}$ es solución para $\boldsymbol{a_n = c_1 a_{n-1} + c_2 a_{n-2}}$ **.** Por tanto, demostraremos que $\{a_n\} = \alpha_1 r_1^n + \alpha_2 r_2^n$, para algún α_1 y α_2.

Consideremos condiciones iniciales

$$a_o = c_0 \quad \text{y} \quad a_1 = c_1.$$

Donde

$$a_o = c_0 = \alpha_1 + \alpha_2 \quad \text{y} \quad a_1 = c_1 = \alpha_1 r_1 + \alpha_2 r_2$$

Entonces se obtiene que:

$$\alpha_1 = \frac{(c_1 - c_0 r_2)}{r_1 - r_2}$$

$$\alpha_2 = \frac{(c_0 r_1 - c_1)}{r_1 - r_2}$$

Con los cálculos recientes de α_1 y α_2 , sabemos que $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ es solución. Además, satisface las condiciones iniciales.

De donde, $\{a_n\} = \{\alpha_1 r_1^n + \alpha_2 r_2^n\}$ es la solución, porque sólo existe una solución para $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ que satisface las condiciones iniciales.

Ejemplo 2.3.1: La relación de recurrencia $\boldsymbol{a_n = a_{n-1} + 2a_{n-2}}$, con las condiciones iniciales $a_0 = 2$ y $a_1 = 7$.

Solución: Consideremos el polinomio característico $\boldsymbol{r^2 - r - 2 = 0}$ asociado a $\boldsymbol{a_n = a_{n-1} + 2a_{n-2}}$.

Sus raíces son: $r_1 = -1$ y $r_2 = 2$.

Busquemos los valores de α_1 y α_2 que hacen que $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ sea una solución de $a_n = a_{n-1} + 2a_{n-2}$, para $n = 0, 1, 2, \ldots$

Tenemos que: $a_o = 2$ y $a_1 = 7$ son las condiciones iniciales

Por otro lado,

$$a_o = \alpha_1 + \alpha_2 \quad \text{y} \quad a_1 = \alpha_1 r_1 + \alpha_2 r_2,$$

forma el siguiente sistema de ecuaciones

$$\begin{cases} \alpha_1 + \alpha_2 = 2 \\ -\alpha_1 + 2\alpha_2 = 7 \end{cases}$$

cuya solución es: $\alpha_1 = -1$ y $\alpha_2 = 3$.

Por tanto,

$$\{a_n\} = -1(-1)^n + 3(2)^n = (-1)^{n+1} + 3(2)^n$$

es una solución para $a_n = a_{n-1} + 2a_{n-2}$ con $a_0 = 2$ y $a_1 = 7$.

2.4- Ecuación de recurrencia de la sucesión de Fibonacci

Teorema 2.4.1: La solución explícita a la sucesión de los números de Fibonacci está dada por la siguiente ecuación de recurrencia:

$f_n = f_{n-1} + f_{n-2}$ con $f_0 = 1$ y $f_1 = 1$ para todo $n \geq 1$.

Demostración**:** Consideremos el polinomio característico $r^2 - r - 1 = 0$ asociado a

$$f_n = f_{n-1} + f_{n-2}$$

cuyas raíces son:

$$r_1 = \frac{1+\sqrt{5}}{2} \quad \text{y} \quad r_2 = \frac{1-\sqrt{5}}{2}$$

Sabemos que el número $\frac{1+\sqrt{5}}{2} = \varphi$ es conocido como el número de oro y su conjugado es $\frac{1-\sqrt{5}}{2} = 1 - \varphi$. Ahora consideremos $r_1 = \varphi$ y $r_2 = 1 - \varphi$ para buscar los valores de α_1 y α_2 que hacen que $\{f_n\} = \alpha_1 r_1^n + \alpha_2 r_2^n$ sea una solución de $f_n = f_{n-1} + f_{n-2}$, para $n = 0, 1, 2, \ldots$

Tenemos que*:* $f_o = 1$ y $f_1 = 1$.

Por otro lado, $f_o = \alpha_1 + \alpha_2$ y $f_1 = \alpha_1 r_1 + \alpha_2 r_2$, forma el siguiente sistema de ecuaciones

$$\begin{cases} \alpha_1 + \alpha_2 = 1 \\ \varphi\alpha_1 + (1 - \varphi)\alpha_2 = 1 \end{cases}$$

Cuya solución es:

$$\alpha_1 = \frac{-\varphi}{1-2\varphi} \quad \text{y} \quad \alpha_2 = \frac{1-\varphi}{1-2\varphi}$$

Por tanto,

$$f_n = \alpha_1 r_1^n + \alpha_2 r_2^n$$

$$= \frac{-\varphi}{1-2\varphi}(\varphi)^n + \frac{1-\varphi}{1-2\varphi}(1 - \varphi)^n$$

Reducen la expresión anterior a:

$$\{f_n\} = \frac{-1}{1-2\varphi}(\varphi)^{n+1} + \frac{1}{1-2\varphi}(1 - \varphi)^{n+1}$$

Tenemos que:

$$\frac{1}{1-2\varphi} = \frac{\sqrt{5}}{5}$$

así:

$$\{f_n\} = \frac{\sqrt{5}}{5}(1 - \varphi)^{n+1} - \frac{\sqrt{5}}{5}(\varphi)^{n+1}$$

Es solución para la sucesión de números de Fibonacci.

2.5- Ecuación de recurrencia de la sucesión de Lucas

Teorema 2.5.1: La solución a la relación de recurrencia de los números de Lucas. $\boldsymbol{l_n = l_{n-1} + l_{n-2}}$, para $n = 2,3,4,5,\ldots$ con $l_0 = 2$ y $l_1 = 1$.

Demostración: La sucesión de Lucas tiene una gran similitud con la sucesión de Fibonacci.

Consideremos el polinomio característico $\boldsymbol{r^2 - r - 1 = 0}$ asociado a $\boldsymbol{l_n = l_{n-1} + l_{n-2}}$ **,** cuyas raíces son:

$$r_1 = \frac{1+\sqrt{5}}{2} = \varphi \quad \text{y} \quad r_2 = \frac{1-\sqrt{5}}{2} = 1 - \varphi$$

Ahora consideremos $r_1 = \varphi$ y $r_2 = 1 - \varphi$ para buscar los valores de α_1 y α_2 que hacen que $\{l_n\} = \{\alpha_1 r_1^n + \alpha_2 r_2^n\}$ sea una solución de $l_n = l_{n-1} + l_{n-2}$, para $n = 0,1,2,\ldots$ Por otro lado, $l_o = \alpha_1 + \alpha_2$ y $l_1 = \alpha_1 r_1 + \alpha_2 r_2$,

Tenemos que*:* $l_o = 2$ *y* $l_1 = 1$ forma el siguiente sistema de ecuaciones

$$\begin{cases} \alpha_1 + \alpha_2 = 2 \\ \varphi\alpha_1 + (1 - \varphi)\alpha_2 = 1 \end{cases}$$

La solución de es sistema es:

$$\alpha_1 = 3 - 2\varphi \quad \text{y} \quad \alpha_2 = 2\varphi - 1$$

Por tanto,

$$\{l_n\} = \alpha_1 r_1^n + \alpha_2 r_2^n$$

$$\{l_n\} = (3 - 2\varphi)(\varphi)^n + (2\varphi - 1)(1 - \varphi)^n$$

$$\{l_n\} = (2 - \sqrt{5})\varphi^n + \sqrt{5}(1 - \varphi)^n$$

Es la sucesión de números de Lucas.

2.6- Ecuación de Recurrencia de la sucesión de Mersenne:

Teorema 2.6.1: La sucesión de los números de Mersenne está dada por la siguiente ecuación de recurrencia:

$M_n = 3M_{n-1} - 2M_{n-2}$ con $M_0 = 0$ y $M_1 = 1$, $M \geq 2$

Demostración: Consideremos el polinomio característico asociado a

$$M_n = 3M_{n-1} - 2M_{n-2} \text{ ,}$$

$$r^2 - 3r + 2 = 0$$

cuyas raíces son:

$$r_1 = 1 \text{ y } r_2 = 2$$

Busquemos los valores de α_1 y α_2 que hacen que $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ sea una solución de $M_n = 3M_{n-1} - 2M_{n-2}$, para $n = 0, 1, 2, \ldots$

Tenemos que: $M_o = 0$ y $M_1 = 1$ son las condiciones iniciales.

Por otro lado, $M_o = \alpha_1 + \alpha_2$ y $M_1 = \alpha_1 r_1 + \alpha_2 r_2$, forma el siguiente sistema de ecuaciones $\begin{cases} \alpha_1 + \alpha_2 = 0 \\ \alpha_1 + 2\alpha_2 = 1 \end{cases}$

Que tiene como solución: $\alpha_1 = -1$ y $\alpha_2 = 1$.

Por tanto, $\{a_n\} = -1(1)^n + 1(2)^n = 2^n - 1$ es solución para la sucesión de números de Mersenne.

Capítulo N° 3

ÁLGEBRA COMPUTACIONAL

ÁLGEBRA COMPUTACIONAL

Una característica perfectamente reconocible de los números primos de Mersenne es su rápido crecimiento. Se trata de números que crecen de manera exponencial. En otras palabras, poseen una gran magnitud, por lo que son difíciles de representar y almacenar. Este problema conlleva otra dificultad: a mayor tamaño, el número tardará más en ser analizado. En otras palabras, también tendremos un problema de rendimiento.

Todos estos números primos son de gran importancia, especialmente en aplicaciones criptográficas como por ejemplo el protocolo RSA, ya que los números primos más grandes que se conocen son números primos de Mersenne. Debido a sus propiedades, algunas de las cuales ya hemos mencionado, es posible acelerar procesos asociados a la criptografía de clave pública y a los procesos de criptografía basados en curvas elípticas.

3.1-Test de Lucas-Lehmer

La primera versión de este test fue descubierta por Édouard Lucas, y ella fue capaz de demostrar la primalidad de $2^{127} - 1$ en 1876, el mayor primo calculado sin asistencia computacional

Años más tarde, en 1930 el test de Lucas fue mejorado por Derrick Henry Lehmer, dando lugar al test que se utiliza actualmente para comprobar la primalidad de los números de Mersenne y que también se utilizará en este proyecto. El test de Lucas Lehmer [8] se basa en la comprobación siguiente:

Sea S_n definido con la fórmula recursiva $S_n = S_{n-1}^2 - 2$, dado un número de Mersenne $M_p = 2^p - 1$:

$2^p - 1$ es primo ⇔ El módulo de $S_{p-1} \mid 2^p - 1$ es 0.

En 1951 Ferrier, adapta el test de Lucas- Lehmer para primos de Mersenne a la tecnología digital, gracias a que en sistemas binarios la división por $2^p - 1$ se reduce a sumas y rotaciones de cifras. Esto ha hecho que todos los records de tamaños de primos los haya ostentando desde entonces los primos de Mersenne. La búsqueda de la primalidad: el test de Lucas-Lehmer

Lucas_Lehmer_Test(p):
$s := 4$;
for i from 2 to $p - 1$ do $s := s^2 - 2 \; mod \; 2^p - 1$;
if $s == 0$ then
$2^p - 1$ is prime
else
$2^p - 1$ is composite;
End

3.2- Proyecto GIMPS

En 1995 George Woltman, programador y entusiasta de la teoría de números, crea un programa optimizado para la búsqueda de primos de Mersenne y lo cuelga en la red. Así comienza el proyecto GIMPS (Great Internet Mersenne Prime Search). Los primos de Mersenne son extremadamente raros, solo 51 son conocidos. GIMPS, fundado en 1996, ha descubierto los últimos 17 primos Mersenne.

Chris Caldwell mantiene un sitio web autorizado sobre la historia de los primos de Mersenne , así como los primos más grandes conocidos . La prueba de primalidad llevó 39 días de computación sin parar en una de las computadoras de la Universidad de Central Missouri. Para establecer que no hubo errores durante la prueba, el nuevo primo se verificó independientemente utilizando diferentes programas que se ejecutan en hardware diferente.

Jerry Hallett lo verificó usando CUDALucas ejecutándose en una GPU NVidia en 3,6 días. El Dr. Jeff Gilchrist verificó el descubrimiento utilizando el software GIMPS estándar en una CPU Intel i7 en 4,5 días.

Para el análisis de los números primos de Mersenne, existen diversos softwares; en esta investigación utilizaremos el software Mathematica 10 donde analizo la primalidad de los números de Mersenne, la descomposición factorial de los números compuestos de Mersenne.

3.3. Software Wolfram Mathematica:

Mathematica es un programa utilizado en áreas científicas, de ingeniería, matemática y áreas computacionales. Originalmente fue concebido por Stephen Wolfram, quien continúa siendo el líder del grupo de matemáticos y programadores que desarrollan el producto en Wolfram Research, compañía ubicada en Champaign, Illinois. Comúnmente considerado como un sistema de álgebra computacional, Mathematica es también un poderoso lenguaje de programación de propósito general.

La primera versión de Mathematica se puso a la venta en 1988. La versión 10.3, fue lanzada el 15 de octubre de 2015, se encuentra disponible para una gran variedad de sistemas operativos.

Mathematica se divide en dos partes, el "kernel" o núcleo (en informática) que desempeña los cálculos. Y el "front end" o interfaz, que despliega los resultados y permite al usuario interactuar con el núcleo como si fuera un documento.

En la comunicación entre el kernel y la interfaz (o cualquier otro cliente) Mathematica usa el protocolo MathLink, a menudo sobre una red. Es posible que diferentes interfaces se conecten al mismo núcleo, y también que una interfaz se conecte a varios núcleos.

A diferencia de otros sistemas de álgebra computacional, por ejemplo Maxima o Maple, Mathematica intenta usar las reglas de transformación que conoce en cada momento tanto como sea posible, tratando de alcanzar un punto estable.

Algunas funciones del Software Mathematica que se usa en este proyecto:

Input[ ]: función que solicita introducir un dato.

Print[ ]: función que imprime los resultados de las rutinas.

FactorInteger[ ]: función que obtiene los factores primos de un número, indicando el número primo y su multiplicidad.

Length[ ]: función que determina la longitud de elementos de un conjunto

Prime$Q$[ ]: función que verifica si un número es primo o no

Append [,]: función que adiciona valores en un la lista vacía.

If[,]: Si, entonces, (condicional)

For [$i = 1$, $i \leq$ **condición** , i **++, función]** es una función cíclica que evalúa los elementos de una lista basándose en una condición.

Table[f, {i, 1, n}]: recorre una cantidad finita de valores por una función.

MatrixForm [{ , , }, TableDirections → {Row, Column}] esta función muestra los datos de una lista en forma matricial (filas y columnas).

3.4 Algoritmos y rutinas para analizar la Sucesión de los números de Mersenne usando el Software Mathematica 10

Algoritmo 3.4.1: Al introducir un número natural se generará el término de la sucesión de Mersenne ubicado en la posición de ese valor.

```
l = Input[" Introduzca un número natural para obtener el valor del término de la sucesión de Mersenne asociada a ese valor"]; num = 2^l − 1;
Print[ "Respuesta: El número de Mersenne en la posición", l , "de la sucesión de Mersenne es el número", num]
```

En esta rutina el Software Mathematica reemplaza el valor l introducido en la función **num =** $2^l - 1$ para generar el número de la sucesión de Mersenne asociado.

Algoritmo 3.4.2: Dado un valor natural, se verifica si es un número de Mersenne y lo clasifica entre número primo o compuesto.

m = Input["Introduzca un número natural para saber si es un número primo de Mersenne**"];**

A= FactorInteger[m]; $k = m + 1$;

B= FactorInteger[k];

u = Length[A]; bas1 = A[[1]] [[1]]; exp1 = A[[1]] [[2]];

v = Length[B]; bas2 = B[[1]] [[1]]; exp2 = B[[1]] [[2]];

If [Prime$Q$[m], Print[m ," es un número Primo**"], Print[m ,"** es un número compuesto**"]];**

If [bas1==2, Print[" pero no es un número de la sucesión de Mersenne**"],**
If [v==1, Print[" que ocupa la posición n = **", exp2 ,"** en la sucesión de Mersenne**"], Print["** que no es un número de la sucesión de Mersenne**"]]]**

En esta rutina el Software Mathematica verifica, si el valor m introducido es un número primo o no mediante la función la función **Prime$Q$[ ]** y usa la función si condicional **If [,]** para responder " es un número Primo " o " es un número Compuesto". Después vuelve a usar la función si condicional **If [,]** indicar si el número m es un elemento de la sucesión de Mersenne o no, de serlo indica la posición en dicha sucesión.

- **Algoritmo 3.4.3:** Al introducir un valor natural, se genera la sucesión de los números de Mersenne indicando, si son números primos o no y muestra su descompoción factorial.

n = Input["Introduzca la cantidad de números de términos que desea ver de la sucesión de Mersenne**"]; Mer = Table [$M_n = 2^i - 1$, {i, 1, n}];**

long = Length[Mer]; fac = FactorInteger[Mer]; v = Length[fac];

lista = { }; For[$i = 1$, $i \leq$ v, i ++, lista = Append [lista, fac[[i ,1]]]];

v = Length[lista];

fac = FactorInteger[Mer]; num = Table [j, { j , 1, n}];

Print["Los**", long , "** primeros elementos de la sucesión de Mersenne están escritos en la segunda columna, en la tercera columna nos indican si se trata de un número de Mersenne primo o no, y en la cuarta columna se muestra la descomposición factorial colocando primero la base y después los exponentes que indica su multiplicidad**"];**

MatrixForm [{num , " " Mer , " " Prime$Q$[Mer] , fac }, TableDirections → {Row, Column}]

En esta rutina el Software Mathematica muestra, los n valores correspondientes en la sucesión de Mersenne utilizando funciones tales como **Table,** ciclo **For** y entrega en forma matricial los resultados de usando **MatrixForm**.

Rutinas ilustrativas, aplicando los algoritmos anteriores.

Ejemplo 3.4.1: Usando el algoritmo 3.4.1, introduciendo el valor: 30

El número de Mersenne en la posición $\mathbf{30}$ de la sucesión de Mersenne es el número**: 1073741823**

Ejemplo 3.4.2: Usando el algoritmo 3.4.2, introduciendo los valores: 63, 127, 89, 11, 3 y 524 287

- 63 es un número compuesto, que ocupa la posición 6 en la sucesión de Mersenne.
- 127 es un número primo, que ocupa la posición 7 en la sucesión de Mersenne.
- 89 es un número primo, que no es un número de la sucesión de Mersenne.
- 11 es un número primo, que no es un número de la sucesión de Mersenne
- 3 es un número primo, que ocupa la posición 2 en la sucesión de Mersenne.
- 524 287 es un número primo, que ocupa la posición 19 en la sucesión de Mersenne.

Ejemplo 3.5.3: Usando el algoritmo 3.4.3, introduciendo el valor: 19

1		False	{{1, 1}}
2	3	True	{{3, 1}}
3	7	True	{{7, 1}}
4	15	False	{{3, 1}, {5, 1}}
5	31	True	{{31, 1}}
6	63	False	{{3, 2}, {7, 1}}
7	127	True	{{127, 1}}
8	255	False	{{3, 1}, {5, 1}, {17, 1}}
9	511	False	{{7, 1}, {73, 1}}
10	1023	False	{{3, 1}, {11, 1}, {31, 1}}
11	2047	False	{{23, 1}, {89, 1}}
12	4095	False	{{3, 2}, {5, 1}, {7, 1}, {13, 1}}
13	8191	True	{{8191, 1}}
14	16383	False	{{3, 1}, {43, 1}, {127, 1}}
15	32767	False	{{7, 1}, {31, 1}, {151, 1}}
16	65535	False	{{3, 1}, {5, 1}, {17, 1}, {257, 1}}
17	131071	True	{{131071, 1}}
18	262143	False	{{3, 3}, {7, 1}, {19, 1}, {73, 1}}
19	524287	True	{{524287, 1}}

CONCLUSIONES

- A través de la historia los números primos han sido objeto de largas investigaciones y estudios.
- Los números de Mersenne ostentan la máxima posición de números primos conocidos.
- El estudio de los números primos de Mersenne es importante dado que por sus características son especialmente útiles en distintas aplicaciones, especialmente criptográficas, como el protocolo RSA o la criptografía basada en curvas elípticas.
- La relación de recurrencia da paso al Álgebra computacional, basándose en la sucesión y recursión de los números de Mersenne.
- El proyecto GIMPS dio paso a la optimización en la búsqueda de los números primos de mayores cifras, al grado de ofrecer premios a los usuarios que enlacen sus computadores a este proyecto de un número primo más grande.
- Primos primitivos son aquellos primos que tienen potencia uno y que no hayan salido anteriormente en la sucesión de bases primas.
- Entre los factores primos de los elementos de la sucesión de Mersenne se puede observar que existen bases cuadradas.

- Los números de Mersenne son unidad de repetición de la base binaria, esta propiedad resulta interesante, sobre todo al realizar operaciones con computadores, ya que éstos trabajan en base binaria, puesto que ciertos cálculos se simplifican en extremo.
- Los números perfectos es un problema abierto de investigación y estos números guardan una estrecha relación con los números primos de Mersenne, dado el hecho de que si M es un número primo de Mersenne entonces $\frac{M\cdot(M+1)}{2}$ es un número perfecto.
- La utilización de software Mathematica nos permiten visualizar la obtención de la sucesión de Mersenne y la descomposición factorial. Así como validar si se trata o no de un número primo de Mersenne.

RECOMENDACIONES

- Realizar con mayor detenimiento un estudio de los diferentes tipos de números primos que han surgido a través de la historia, sus propiedades y aportes a nuevas investigaciones.
- Revisar otros campos de la Matemática que puedan demostrar las conjeturas alrededor de los números primos, en particular los números primos de Mersenne y los números perfectos.
- Crear nuevos programas usando el álgebra computacional, como el proyecto GIMPS, que utilicen la tecnología avanzada que puedan dar resultados con mayor optimización del tiempo y los recursos, que incentive a las nuevas generaciones a los descubrimientos de los nuevos números primos.
- Presentar y comparar diferentes rutinas de programación usando software diferentes o nuevas versiones del software Mathematica
- Analizando los primos primitos asociados a la sucesión de Mersenne se podría crear rutinas que generen esos primos primitivos.
- Estudiar cuales números de la sucesión de Mersenne no es libre de cuadrados (Tiene cuadrados en sus factores primos).

REFERENCIA BIBLIOGRAFICA

Burton, David. (1980). Elementary Number Theory. Revised Printing. University of new Hampshire. Allyn and Bacon, Inc. Boston.217-235.

Everest, Graham; Stevens,Shoun; Tamsett, Duncan y Ward, Tom. (2006). Primes Generated by Recurrence Sequences, Recuperado de: http://www.uea.ac.uk/~h008/research/primes.pdf

GIMPS Home. (1996) (En línea). (Consultado 16 de junio de 2013) Disponible en: http://www.mersenne.org/.

Lemmermeyer, Franz. (1962). Riprocity Laws. From Euler to Eisenstein. Springer Monographs in Mathematics. 4,12,56-57,70.

Lucas-Lehmer test - Mersennewiki. (En línea). (Consultado 12 de junio de 2013) Recuperado de: http://mersennewiki.org/index.php/Lucas-Lehmer_Test.

Pomerance, Carl. (1986). On primitive divisors of Mersenne numbers. Acta Arithmetica, Recuperado de: http://www.math.dartmouth.edu/~carlp/PDF/paper56.pdf

Rice, Brian. (2006). Primitive Prime Divisors of First-Order Polynomial Recurrence Sequences, Recuperado de: http://www.math.wisc.edu/~ono/reu06ppdivisor.pdf

«Prime95 - Mersennewiki». (En línea). (Consultado 16 de junio de 2013) Recuperado de: http://mersennewiki.org/index.php/Prime95.

Anexo

La siguiente tabla muestra los números primos de Mersenne conocidos, fecha del descubrimiento y descubridor hasta el año 2018.

#	N	Mn	Nº de cifras de Mn	Fecha del descubrimiento	Descubridor
1	2	3	1	antigüedad	Euclides
2	3	7	1	antigüedad	Euclides
3	5	31	2	antigüedad	Euclides
4	7	127	3	antigüedad	Euclides
5	13	8191	4	1456	anónimo
6	17	131071	6	1588	Cataldi
7	19	524287	6	1588	Cataldi

8	31	2147483647	10	1772	Euler
9	61	2305843009213693951	19	1883	Pervushin
10	89	618970019…449562111	27	1911	Powers
11	107	162259276…010288127	33	1914	Powers
12	127	170141183…884105727	39	1876	Lucas
13	521	686479766…115057151	157	30-01-1952	Robinson (SWAC)
14	607	531137992…031728127	183	30-01-1952	Robinson (SWAC)
15	1.279	104079321…168729087	386	25-06-1952	Robinson (SWAC)
16	2.203	147597991…697771007	664	07-10-1952	Robinson (SWAC)
17	2.281	446087557…132836351	687	09-10-1952	Robinson (SWAC)
18	3.217	259117086…909315071	969	08-09-1957	Riesel

19	4.253	190797007…350484991	1.281	03-11-1961	Hurwitz
20	4.423	285542542…608580607	1.332	03-11-1961	Hurwitz
21	9.689	478220278…225754111	2.917	11-05-1963	Gillies
22	9.941	346088282…789463551	2.993	16-05-1963	Gillies
23	11.213	281411201…696392191	3.376	02-06-1963	Gillies
24	19.937	431542479…968041471	6.002	04-03-1971	Tuckerman
25	21.701	448679166…511882751	6.533	30-10-1978	Noll y Nickel
26	23.209	402874115…779264511	6.987	09-02-1979	Noll
27	44.497	854509824…011228671	13.395	08-04-1979	Nelson y Slowinski
28	86.243	536927995…433438207	25.962	25-09-1982	Slowinski
29	110.503	521928313…465515007	33.265	28-01-1988	Colquitt y Welsh

30	132.049	512740276…730061311	39.751	20-09-1983	Slowinski
31	216.091	746093103…815528447	65.050	06-09-1985	Slowinski
32	756.839	174135906…544677887	227.832	19-02-1992	Slowinski y Gage
33	859.433	129498125…500142591	258.716	10-01-1994	Slowinski y Gage
34	1.257.787	412245773…089366527	378.632	03-09-1996	Slowinski y Gage
35	1.398.269	814717564…451315711	420.921	13-11-1996	GIMPS / Joel Armengaud
36	2.976.221	623340076…729201151	895.932	24-08-1997	GIMPS / Gordon Spence
37	3.021.377	127411683…024694271	909.526	27-01-1998	GIMPS / Roland Clarkson
38	6.972.593	437075744…924193791	2.098.960	01-06-1999	GIMPS /
39	13.466.917	924947738…256259071	4.053.946	14-11-2001	GIMPS / Michael Cameron

40	20.996.011	125976895…855682047	6.320.430	17-11-2003	GIMPS / Michael Shafer
41	24.036.583	299410429…733969407	7.235.733	15-05-2004	GIMPS / Josh Findley
42	25.964.951	122164630…577077247	7.816.230	18-02-2005	GIMPS / Martin Nowak
43	30.402.457	315416475…652943871	9.152.052	15-12-2005	GIMPS / Curtis Cooper y Steven Boone
44	32.582.657	124575026…053967871	9.808.358	04-09-2006	GIMPS / Curtis Cooper y Steven Boone
45	37.156.667	202254406…308220927	11.185.272	06-09-2008	GIMPS / Hans-Michael Elvenich
46	42.643.801	169873516…562314751	12.837.064	12-04-2009	GIMPS / Odd M. Strindmo
47	43.112.609	316470269…697152511	12.978.189	23-08-2008	GIMPS / Edson Smith

48	57.885.161	581887266…724285951	17.425.170	25-01-2013	GIMPS / Curtis Cooper
49	74.207.281	300376418…086436351	22.338.618	07-01-2016	GIMPS / Curtis Cooper
50	77.232.917	467333183…762179071	23.249.425	26-12-2017	GIMPS / Jonathan Pace
51	82.589.933	148894445…217902591	24.862.048	07-12-2018	GIMPS / Patrick Laroche