UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

POLINOMIOS CUADRÁTICOS QUE GENERAN PRIMOS

MONOGRAFÍA DE TRABAJO DE GRADO PARA OPTAR POR EL TÍTULO DE MATEMÁTICO
PROYECTO CURRICULAR DE MATEMÁTICAS

Fanny Paola Rodríguez Guzmán
Dirigido por: Carlos Orlando Ochoa Castillo

Bogotá DC
Octubre de 2021

Resumen

En el presente trabajo se estudian polinomios cuadráticos que generan números primos consecutivos. Para ello se analizan diferentes características y propiedades que satisfacen estos polinomios; tomando como Polinomio principal, el polinomio de Euler.

Palabras clave: Polinomio, cuadrático, numeros primos.
Clasificación AMS: 11S05
Agradecimientos:
Agradezco a mis padres ejemplo de vida, a quienes me debo por su amor y dedicación; a Alonso por acompañarme y apoyarme durante mi carrera, por sus consejos y cariño. Agradezco a Juan, porque siempre ha creído en mis capacidades y me ha motivado para continuar.

De manera muy especial, agradezco a mi hermosa abuela, porque siempre estuvo pendiente de mis pasos y aunque no esta presente físicamente, sé que ella celebra mis triunfos.

Por último agradezco al Proyecto Curricular de Matemáticas de la Universidad Distrital Francisco José de Caldas por mi formación académica y a cada uno de los docentes que hicieron parte de este proceso, en especial a mi director Carlos Orlando Ochoa Castillo ejemplo de persona y profesional.

1. Introducción

La disciplina matemática que se encarga de las propiedades de los números enteros positivos es la teoría de números, en la que han sido los primos los principales y más curiosos números a estudiar, son tan sorprendentes que aunque no lo parezca, cualquier avance en el conocimiento sobre los números primos, podría ser decisivo en la solución de algún problema de cualquier campo, tanto matemático como físico. En el presente trabajo, se pretende estudiar algunos polinomios cuadráticos que generan números primos, tomando como base el artículo *Prime-Producing Quadratics* (ver [1]).

2. PRINCIPALES POLINOMIOS CUADRÁTICOS QUE GENERAN PRIMOS

2.1. Polinomios más importantes

Polinomio de Euler: el polinomio cuadrático más conocido que genera números primos es el polinomio descubierto por Euler en 1772:

$$x^2 - x + 41$$

Tiene discriminante -163, genera primos para los enteros $x = 1, 2, 3, \ldots, 40$,(ver [2]) que se exhiben en seguida.

41	43	47	53	61
71	83	97	113	131
151	173	197	223	251
281	313	347	383	421
461	503	547	593	641
691	743	797	853	911
971	1033	1097	1163	1231
1301	1373	1447	1523	1601

Cuadro 1: Primos generados por el polinomio de Euler

Polinomio de Legendre: en 1798, Legendre descubrió que el polinomio

$$f(x) = x^2 + x + 41$$

es primo para los enteros $x = 0, 1, 2, \ldots, 39$; este polinomio tiene el mismo discriminante que el polinomio de Euler.
A continuación se exhiben los valores generados por $f(x) = x^2 + x + 41$

41	43	47	53	61
71	83	97	113	131
151	173	197	223	251
281	313	347	383	421
461	503	547	593	641
691	743	797	853	911
971	1033	1097	1163	1231
1301	1373	1447	1523	1601

Cuadro 2: primos generados por el polinomio de Legendre

Se pueden encontrar numerosos polinomios de discriminante -163 que generan primos para al menos 40 valores de x simplemente actuando de manera similar como se hizo el polinomio de Euler. Por ejemplo se produce una familia infinita de polinomios que generan 40 valores primos distintos; considérese el siguiente polinomio $g_n(x)$ para cada $n \in \mathbb{Z}$ logrado a partir de la función $f(x)$ por $x \to 3x - 39 - 3n$, es decir, reemplazando en el polinomio de Legendre:

$$\begin{aligned} f(3x-(39+3n)) &= (3x-(39+3n))^2 + (3x-(39+3n)) + 41 \\ &= (3x)^2 - 2(3x(39+3n)) + (39+3n)^2 + 3x - 39 - 3n + 41 \\ &= 9x^2 - 234x - 18xn + 39^2 + 2(39)(3n) + (3n)^2 + 3x - 39 - 3n + 41 \\ &= 9x^2 - 234x - 18xn + 1521 + 234n + 9n^2 + 3x - 39 - 3n + 41 \\ &= 9x^2 - 231x - 18xn + 9n^2 + 231n + 1523 \\ &= 9x^2 - (18n+231)x + 9n^2 + 231n + 1523 \end{aligned}$$

En consecuencia $g_n(x)$ es el polinomio cuadrático:

$$g_n(x) = 9x^2 - (18n+231)x + 9n^2 + 231n + 1523$$

el cual produce 40 primos distintos para los valores:

$$g_n(x+n) = \begin{cases} f(38-3x) & \text{para } x = 0, 1, \ldots, 12 \\ f(3x-39) & \text{para } x = 13, 14, \ldots, 39 \end{cases}$$

Estos polinomios siguiendo el orden de los números primos saltan uno intermedio; se tiene el discriminante de $g_n(x)$ como $-3^2 \cdot 163$. Véase que si $n = 0$ entonces

$$g_0(x) = 9x^2 - 231x + 1523$$

es primo para $x = 0, 1, 2, \ldots, 39$ este fue el caso especial descubierto por Higgins (ver [3]).

41	47	53	71	83
113	131	173	197	251
281	347	383	461	503
593	641	743	797	911
971	1097	1163	1301	1373
1523	1601	1847	2111	2393
2693	3011	3347	3701	4073
4463	4871	5297	5741	6203

Cuadro 3: primos generados por el polinomio $g_0(x)$

Se puede tener otra familia infinita de polinomios que genera 40 primos distintos para todo $n \in \mathbb{Z}$, este polinomio viene dado a partir de $f(x)$ por $x \to 2x - 39 - 2n$, es decir, reemplazando en el polinomio de Legendre:

$$\begin{aligned} f(2x-(39+2n)) &= (2x-(39+2n))^2 + (2x-(39+2n)) + 41 \\ &= (2x)^2 - 2(2x(39+2n)) + (39+2n)^2 + 2x - 39 - 2n + 41 \\ &= 4x^2 - 156x - 8xn + 39^2 + 2(39)(2n) + (2n)^2 + 2x - 39 - 2n + 41 \\ &= 4x^2 - 156x - 8xn + 1521 + 156n + 4n^2 + 2x - 39 - 2n + 41 \\ &= 4x^2 - 154x - 8xn + 4n^2 + 154n + 1523 \\ &= 4x^2 - (8n+154)x + 4n^2 + 154n + 1523 \\ &= h_n(x) \end{aligned}$$

$$h_n(x) = 4x^2 - (8n+154)x + 4n^2 + 154n + 1523$$

Con discriminante $-2^2 \cdot 163$ y produce 40 primos distintos para los valores:

$$h_n(x+n) = \begin{cases} f(38-2x) & \text{para } x = 0, 1, \ldots, 19 \\ f(2x-39) & \text{para } x = 20, 21, \ldots, 39 \end{cases}$$

Véase, en particular si $n = 0$:

41	43	47	53	61
71	83	97	113	131
151	173	197	223	251
281	313	347	383	421
461	503	547	593	641
691	743	797	853	911
971	1033	1097	1163	1231
1301	1373	1447	1523	1601

Cuadro 4: Polinomio $h_0(x)$

entonces $h_0(x) = 4x^2 - 154x + 1523$ genera:
$h_0(0) = 1523 = f(38)$, $h_0(1) = 1373 = f(36)$,..., $h_0(19) = 41 = f(0)$, $h_0(20) = 43 = f(1)$, $h_0(21) = 53 = f(3)$, ..., $h_0(39) = 1601 = f(39)$.

Se tiene también la familia de polinomios $k_n(x) = x^2 - (2n + 79)x + n^2 + 79n + 1601$, que genera 80 primos, este polinomio viene dado a partir de $f(x)$ por $x \to x - 40 - n$, es decir x es de la forma $x - (40 + n)$, reemplazando en el polinomio de Legendre se tiene:

$$\begin{aligned} f(x-(40+n)) &= (x-(40+n))^2 + (x-(40+n)) + 41 \\ &= (x)^2 - 2(x(40+n)) + (40+n)^2 + (x-(40+n)+41 \\ &= x^2 - 80x - 2xn + 40^2 + 2(40)(n) + (n)^2 + x - 40 - n + 41 \\ &= x^2 - 80x - 2xn + 1600 + 80n + n^2 + x - 40 - n + 41 \\ &= x^2 - 79x - 2xn + n^2 + 79n + 1601 \\ &= x^2 - (2n+79)x + n^2 + 79n + 1601 \\ &= k_n(x) \end{aligned}$$

Entonces

$$k_n(x) = x^2 - (2n + 79)x + n^2 + 79n + 1601$$

tiene discriminante -163, el polinomio es primo para $k_n(n + x) = k_n(n + 79 - x) = f(39 - x)$ para todo $x = 0, 1, \ldots, 39$, es decir k_n toma los valores de $f(39) = 1601$ a $f(0) = 41$ en orden descendente y repite los valores en orden ascendente, luego genera 80 valores primos pero 40 valores primos distintos. El caso particular descubierto por Escott en 1899 (ver[4])

$$k_0(x) = x^2 - 79x + 1601$$

el cual produce valores primos para $x = 0, 1, \ldots, 79$.

Véase, en particular si $n = 0$:

41	43	47	53	61
71	83	97	113	131
151	173	197	223	251
281	313	347	383	421
461	503	547	593	641
691	743	797	853	911
971	1033	1097	1163	1231
1301	1373	1447	1523	1601

Cuadro 5: Polinomio $k_0(x)$

Donde: $k_0(39) = k_0(40) = 41$, $k_0(38) = k_0(41) = 43$, $k_0(37) = k_0(42) = 47$,
$k_0(36) = k_0(43) = 53$, …, $k_0(0) = k_0(79) = 1601$.

Teniendo como polinomio principal el polinomio de Euler, se estudian los polinomios cuadráticos $F(x) = ax^2 + bx + c$ con discriminante $\Delta = b^2 - 4ac < 0$, que generan primos distintos por una cadena de valores empezando por $x = 0$, llamada **cadena inicial de valores primos**. Supóngase $c > 0$ y teniendo en cuenta los polinomios anteriores, se formaliza la noción del número máximo de valores primos distintos producidos por una cuadrática.

Definición 1. *Considérese $F(x) = ax^2 + bx + c$ con $a, b, c \in \mathbb{Z}$, $a \neq 0$ y supóngase que $|F(x)|$ es primo para todos los enteros $x = 0, 1, \ldots, \ell - 1$. Si $\ell \in \mathbb{N}$ es el valor más pequeño tal que $|F(\ell)|$ es compuesto, $|F(\ell)| = 1$ o $|F(\ell)| = |F(x)|$ para algún $x = 0, 1, \ldots, \ell - 1$, entonces $F(x)$ se dice que tiene longitud principal ℓ.*

Por ejemplo la longitud principal para los polinomios $k_0(x), g_0(x)$ y $f(x)$ es 40.

Observación: en la definición anterior, ya que solo se trabajan polinomios de valores positivos $F_\Delta(x) = x^2 + x + A$ el valor absoluto no importa, además $F_\Delta(x) = 1$ si y solo si $x = 0$ y $A = 1$, es decir $\Delta = -3$.

Desde la perspectiva de longitud principal es suficiente ver los discriminantes,
$\Delta \equiv 1 \pmod 4$, $(4|\Delta - 1)$ ya que el otro caso es trivial.
Supóngase que $\Delta < -4$ donde el discriminante de $F(x) = ax^2 + bx + c$ es, $\Delta \equiv 0 \pmod 4$. Si c es par, entonces $F(1)$ es par y compuesto, como $F(0) = c$ debe ser 2, dado que se asume que $\ell \geq 1$. Si c es impar, entonces $F(1)$ es par y compuesto, como b debe ser par cuando $\Delta \equiv 0 \pmod 4$. Entonces la longitud principal no excede 2 cuando $\Delta \equiv 0 \pmod 4$, $\Delta < -4$.

Con el modelo del polinomio de Euler, se hará un estudio de polinomios mónicos, teniendo como centro la forma Euleriana.

$$F_\Delta(x) = x^2 + x + A$$

Donde $\Delta = 1 - 4A$, se observa que $F_\Delta(A-1) = A^2$. Por lo tanto la longitud principal para $F_\Delta(x)$ a lo sumo es $A - 1$.

Proposición 1. *Si $\ell \in \mathbb{N}$ es la longitud principal de $F_\Delta(x)$, entonces $\ell \leq A - 1$, donde $\Delta = 1 - 4A$. Si p es minimo primo impar tal que $\Delta \equiv x^2 \pmod{p}$ para algún $x \in \mathbb{Z}$, entonces $\ell < p$. Además, si $\Delta \neq -7$, y $\ell \geq (A-1)/2$, entonces $A = p$.*

Véase que es posible hacer una clasificación de todos los polinomios de la forma $x^2 + x + A$. Para $x \in \mathbb{Z}$ que tienen longitud principal $\ell = A - 1$; por la Proposición 1, se sabe que si $\ell = A - 1$, entonces A es el menor primo impar para el cual $\Delta < -7$ satisface $\Delta \equiv x^2 \pmod{A}$ Por ejemplo, $A = 41$ es el menor primo para el cual $\Delta = -163$. Para poder realizar esta clasificación se debe contestar el interrogante ¿cuál es la cantidad de valores primos consecutivos que el polinomio $F_\Delta(x)$ puede tomar?, la respuesta es: cualquier cantidad de valores consecutivos; para comprender esto es necesario entender "la conjetura principal de k-tuplas" esta es una generalización de la "conjetura de los primos gemelos" la cual dice que p y $p + 2$ a menudo son primos infinitos.

Sea $R = \{r_1, \ldots, r_k\}$ con $r_i \in \mathbb{Z}$ para $i = 1, 2, \ldots, k$. Si q es un primo tal que $\prod_{i=1}^{k}(n + r_i) \equiv 0 \pmod{q}$, para cada $n \in \mathbb{Z}$ con $1 \leq n \leq q$, entonces no puede existir una cantidad de números infinitos p tal que $\{p + r_i\}_{i=1}^{k}$ son simultáneamente primos, si existe tal q, primo, entonces R se llamará inadmisible, de otra manera R se llamará admisible. Otra forma de ver esto es: R es admisible si y solo si, para todos los primos q, existe un entero a_q con $1 \leq a_q \leq q$, tal que $\prod_{i=1}^{k}(a_q + r_i) \not\equiv 0 \pmod{q}$.

3. CONJETURA PRINCIPAL DE K-TUPLAS Y CRITERIO DE RABINOWITSCH

Para generalizar la última idea del capítulo anterior, se tiene **la conjetura principal de k-tuplas**, antes de enunciarla es necesaria la siguiente definición:

Definición 2. *Dado $m \in \mathbb{Z}$, $m \geq 1$, se dice que $a, b \in \mathbb{Z}$ son congruentes módulo m si y sólo si $m|(a-b)$. Se denota esta relación como $a \equiv b(\pmod{m})$. m es el módulo de la congruencia.*

Ahora se enunciara **la conjetura principal de k-tuplas**

Conjetura 1. *(la conjetura principal de k-tuplas). Si R es un conjunto admisible, entonces hay infinitos enteros n tales que $n + r$ es primo para cada $r \in R$.*

Teniendo en cuenta que: R es admisible si y solo si, para todos los primos q, existe un entero a_q, con $1 \leq a_q \leq q$, tal que $\prod_{i=1}^{k}(a_q + r_i) \not\equiv 0 \pmod{q}$. Se hará un análisis de la conjetura.

Tómese el caso específico $R = \{0, 2\}$, se probará que es un conjunto admisible:

- Dado el conjunto $R = \{0, 2\}$ donde $r_1 = 0$ y $r_2 = 2$; supóngase que para ningún número primo q existe $a_q \in \mathbb{Z}$ tal que

$$\prod_{i=1}^{2}(a_q + r_i) \not\equiv 0 \pmod{q}$$

es decir:

$$\begin{aligned}(a_q + 0)(a_q + 2) &\not\equiv 0 \pmod{q}\\ (a_q)(a_q + 2) &\not\equiv 0 \pmod{q}\end{aligned}$$

Por la Definición 2 de congruencia modular $(a_q)(a_q + 2)$ no es divisible por q.
Ahora, si $q = 2$ y $a_q = 1$ se tiene:

$$\begin{aligned}(1 + 0)(1 + 2) &\not\equiv 0 \pmod{2}\\ (1)(3) &\not\equiv 0 \pmod{2}\\ 3 &\not\equiv 0 \pmod{2}\end{aligned}$$

Ya que por definición de congruencia, 2 no divide a 3. Lo que es una contradicción, así el conjunto $R = \{0, 2\}$ es admisible.

- Se mostrará que: como R es admisible, entonces hay infinitos enteros n tales que $n+r$ es primo para cada $r \in R$.

  Dado $R = \{0, 2\}$ un conjunto admisible, supóngase que hay una lista finita de números enteros $n_1, n_2, n_3, \ldots, n_m$ tales que $n_t + r$ para $t = 1, 2, \ldots, m$ es primo para cada $r \in R$.

  Véase que para $r = 0$

$$\begin{aligned} n_1 + 0 &\text{ es primo} \\ n_2 + 0 &\text{ es primo} \\ n_3 + 0 &\text{ es primo} \\ &\vdots \\ n_m + 0 &\text{ es primo} \end{aligned}$$

  Esto se tiene por la propiedad modulativa de la adición de números enteros cuando el entero n_t es primo, como hay infinitos primos entonces hay infinitos enteros tales que $n + 0$ es primo. Lo que es una contradicción.

  Véase que para $r = 2$

$$\begin{aligned} n_1 + 2 &\text{ es primo} \\ n_2 + 2 &\text{ es primo} \\ n_3 + 2 &\text{ es primo} \\ &\vdots \\ n_m + 2 &\text{ es primo} \end{aligned}$$

  Es decir, que se tiene un conjunto finito de números primos con m elementos:

$$n_1 + 2, n_2 + 2, n_3 + 2, \ldots, n_m + 2$$

  Se puede generar otro número mayor N, tal que

$$N = (n_1 + 2)(n_2 + 2)(n_3 + 2)\ldots(n_m + 2) + 2$$

  Donde N puede ser un número primo o no.

  - Si es primo, se tiene un nuevo número primo y hay un número entero dado por $(n_1 + 2)(n_2 + 2)(n_3 + 2)\ldots(n_m + 2)$ que no pertenece a la lista inicial.
  - Si N no es primo, por el teorema fundamental de la aritmética N debe ser divisible por algún número primo diferente a los del conjunto, ya que si se divide por uno de ellos se tendrá como residuo 2; por lo tanto debe existir otro número primo $n_{m+1} + 2$ con n_{m+1} un entero que no pertenece a la lista.

En ambos casos se ha encontrado un número entero que no está en la lista, lo que es una contradicción, luego hay infinitos enteros n tales que $n+2$ es primo.

En consecuencia como $R=\{0,2\}$ es admisible entonces hay infinitos enteros n tales que $n+r$ es primo para cada $r \in R$.

Antes de enunciar el teorema que se deriva de la conjetura anterior, es necesario hacer refererencia al **teorema del residuo Chino**

Teorema 1. *Sean $n_1, n_2, .., n_k \in \mathbb{N} - \{0\}$, k números naturales de modo que $m.c.d.(ni, nj) = 1$ para todo $i \neq= j$, es decir primos entre si. Sean $a_1, a_2, ..., a_k \in \mathbb{Z}$ y se plantean las siguientes k ecuaciones en congruencias $x \equiv a_i \pmod{n_i}$, para todo $i = 1, 2, ..., k$. Entonces este sistema tiene solución. Además si x e y son dos soluciones de las ecuaciones anteriores se tiene que $x \equiv y \pmod{m.c.m.(n_1, n_2, ..., n_k) = n_1 n_2 .... n_k.}$*

Teorema 2. *Si la conjetura se satisface, entonces para cualquier positivo B, existe un polinomio cuadrático de la forma $F_\Delta(x) = x^2 + x + A$, tal que $F_\Delta(x)$ es primo para todo entero con $0 \leq x \leq B$ en el conjunto admisible.*

Demostración. Sea $r_j = j^2 + j$ para $j = 0, 1, 2, \ldots, B$. Supóngase que el conjunto $\left\{r_j\right\}_{j=0}^{B}$ es admisible.

Si $q = 2$, entonces sea $a_q = 1$. Como cada r_j es par, entonces $\prod_{j=0}^{B}(r_j + 1)$ es impar. Para cada primo impar q sea $b_q \equiv 1 \pmod 4$ por el teorema del residuo chino, es una cuadrática sin residuo módulo q, y sea el conjunto $a_q = (1 - b_q)/4$. Si $\prod_{j=0}^{B}(r_j + a_q) \equiv 0 \pmod q$ entonces para algún $0 \leq j \leq B$, $r_j + a_q \equiv 0 \pmod q$. En otras palabras $r_j \equiv -a \pmod q$. Por lo tanto $(2j+1)^2 = 4r_j + 1 \equiv 1 - 4a_q = b_q \pmod q$ lo que es una contradicción por la suposición inicial.

La conjetura asegura que existe un gran valor arbitrario de A para el cual $\left\{r_j + A\right\}_{j=0}^{B}$ son primos. Para tal A, $F_\Delta(x) = x^2 + x + A$ es primo para $x = 0, 1, 2, \ldots, B$ □

Tómese el conjunto $R = \{0, 2\}$, se sabe que es admisible y que satisface la conjetura, ahora veamos que el Teorema se cumple para este caso, si $A = 5$ se tiene el polinomio $F_\Delta(x) = x^2 + x + 5$, reemplazando x por 0 y 2 se obtiene

$$F_\Delta(0) = 5 \text{ es primo}$$

$$F_\Delta(2) = 11 \text{ es primo}$$

Para $A = 7$ se cumple:

$$F_\Delta(0) = 7 \text{ es primo}$$

$$F_\Delta(2) = 13 \text{ es primo}$$

Para $A = 11$ se cumple:

$$F_\Delta(0) = 11 \quad \text{es primo}$$
$$F_\Delta(2) = 17 \quad \text{es primo}$$

Es posible encontrar más valores para A para los que se satisface el teorema con el conjunto admisible $R = \{0, 2\}$.

Se podría creer que el teorema da la posibilidad de encontrar un polinomio cuadrático de la forma $F_\Delta(x) = x^2 + x + A$ que genere no solo más primos que el polinomio de Euler, sino también tantos como se quieran. Sin embargo aún no se ha encontrado un polinomio de la forma $F_\Delta(x)$ con longitud principal de más de 40, se ha llegado a demostrar que si tal $F_\Delta(x)$ existe, entonces $A > 10^{18}$. Por otro lado la **proposición 1** indica que la longitud principal del polinomio $F_\Delta(x)$ está acotada por $A - 1$ lo que sería una contradicción ya que en el **Teorema 1** puede interpretarse que la longitud principal de un polinomio no está acotada. Lo que realmente está pasando es que en el **Teorema 1**, B debe ser menor que $A - 1$, el número de polinomios asumido por tales polinomios es ilimitado.

Por ejemplo: si se quiere una longitud principal $B = 41$ entonces el valor de A debe ser tan grande como 10^{18} y menor que $A - 1$. Como $A > 10^{18}$, no será un obstáculo para encontrar el polinomio; es decir que para $F_\Delta(x)$ será primo para $x = 0, 1, 2, \ldots, A - 2$. Los polinomios que generan primos cuadráticos serán más interesantes si los polinomios son irreducibles. Debería asumirse que no hay un número primo p que divide a $F_\Delta(x)$ para todo $x \in \mathbb{Z}$, como por ejemplo: $x^2 + x + 4$ es irreducible pero siempre par.

Teorema 3. *$h_\Delta = 1$ si y solo si $-\Delta \in \{3, 4, 7, 8, 11, 19, 43, 67, 163\}$*

Demostración. (ver [5]) □

Teorema 4. *(Criterio de Rabinowitsch) Sea $\Delta < 0$ un discriminante con $\Delta \equiv 1 \pmod 4$. Entonces $F_\Delta(x) = x^2 + x + (1 - \Delta)/4$ es primo para todo $x \in \mathbb{Z}$ con $0 \leq x \leq \lfloor |\Delta|/4 - 1 \rfloor$ si y solo si $h_\Delta = 1$.*

Demostración. $\Rightarrow$ Sean $\Delta < 0$ un discriminante con $\Delta \equiv 1 \pmod 4$, $F_\Delta(x) = x^2 + x + (1 - \Delta)/4$ un polinomio primo para todo $x \in \mathbb{Z}$ con $0 \leq x \leq \lfloor |\Delta|/4 - 1 \rfloor$ y $h_\Delta \neq 1$, por el Teorema 3, como $h_\Delta \neq 1$ entonces $-\Delta \notin \{3, 4, 7, 8, 11, 19, 43, 67, 163\}$; ahora si $\Delta = -167$ con $-167 \equiv 1 \pmod 4$ pues -168 es divisible por 4, se tiene:

$$F_\Delta(x) = x^2 + x + (1 + 167)/4$$
$$F_\Delta(x) = x^2 + x + (168)/4$$
$$F_\Delta(x) = x^2 + x + 42$$

para

$$0 \leq x \leq \lfloor |-167|/4 - 1 \rfloor$$
$$0 \leq x \leq \lfloor 167/4 - 1 \rfloor$$
$$0 \leq x \leq \lfloor 40{,}75 \rfloor$$
$$0 \leq x \leq 40$$

$F_\Delta(x)$ genera los siguientes valores

42	44	48	54	62
72	88	98	114	132
152	174	198	224	252
282	314	348	384	422
462	504	548	594	642
692	744	798	854	912
972	1034	1098	1164	1232
1302	1374	1448	1524	1602
1682				

Cuadro 6: valores generados por $F_\Delta(x)$ con $\Delta = -167$

Véase que los números generados son pares mayores que 2, es decir en sus divisores se tiene principalmente a: 1, 2 y él mismo, es decir, que no son primos lo que es una contradicción. Luego $h_\Delta = 1$.

$\Leftarrow$ Sean $\Delta < 0$ un discriminante con $\Delta \equiv 1 \pmod 4$, $h_\Delta = 1$ y el polinomio $F_\Delta(x) = x^2 + x + (1-\Delta)/4$ no es primo para todo $x \in \mathbb{Z}$ con $0 \leq x \leq \lfloor |\Delta|/4 - 1 \rfloor$. Como $h_\Delta = 1$ por el Teorema 3 $-\Delta \in \{3, 4, 7, 8, 11, 19, 43, 67, 163\}$ pero, dado que $\Delta \equiv 1 \pmod 4$ se tiene que $-\Delta \in \{3, 7, 11, 19, 43, 67, 163\}$; Si $\Delta = -67$ se tiene

$$F_\Delta(x) = x^2 + x + (1 - (-67))/4$$
$$F_\Delta(x) = x^2 + x + (1 + 67)/4$$
$$F_\Delta(x) = x^2 + x + 68/4$$
$$F_\Delta(x) = x^2 + x + 17$$

Para

$$0 \leq x \leq \lfloor |-67|/4 - 1 \rfloor$$

$$0 \leq x \leq \lfloor 67/4 - 1 \rfloor$$
$$0 \leq x \leq \lfloor 15{,}75 \rfloor$$
$$0 \leq x \leq 15$$

$F_\Delta(x) = x^2 + x + 17$ genera los valores que se exhiben enseguida

17	19	23	29
37	47	59	73
89	107	127	149
173	199	227	257

Cuadro 7: valores generados por $F_\Delta(x)$ con $\Delta = -67$

Obsérvese que todos los números generados por el polinomio son primos, lo que es una contradicción. Entonces $F_\Delta(x) = x^2 + x + (1 - \Delta)/4$ es primo para todo x entero $0 \leq x \leq \lfloor |\Delta|/4 - 1 \rfloor$

□

Véase que el polinomio de Legendre $f(x) = x^2 + x + 41$ se ajusta al criterio de Rabinowitsch, ya que $\Delta = -163$ y $-163 \equiv 1 \pmod 4$ pues -164 es divisible por 4, ahora

$$F_\Delta(x) = x^2 + x + (1 - (-163))/4$$
$$F_\Delta(x) = x^2 + x + (1 + 163)/4$$
$$F_\Delta(x) = x^2 + x + 164/4$$
$$F_\Delta(x) = x^2 + x + 41$$

Se tiene que para

$$0 \leq x \leq \lfloor |-163|/4 - 1 \rfloor$$
$$0 \leq x \leq \lfloor 163/4 - 1 \rfloor$$
$$0 \leq x \leq \lfloor 39{,}75 \rfloor$$
$$0 \leq x \leq 39$$

$F_\Delta(x) = x^2 + x + 41$ genera los primos dados en el Cuadro 2. Como $\Delta = -163$ por el Teorema 3 se tiene $h_\Delta = 1$.

Observación: Los Teoremas 3 y 4 muestran que $F_\Delta = x^2+x+A$ no puede generar primos consecutivos para $x = 0, 1, 2, \ldots, A-2$ cuando $A > 41$, ya que para $\Delta = -163$, como $\Delta = b^2 - 4ac$ se tiene que A esta dado por:

$$\begin{aligned} -163 &= 1^2 - 4(1)(A) \\ -163 &= 1 - 4(A) \\ -163 - 1 &= -4(A) \\ -164 &= -4(A) \\ \frac{164}{4} &= A \\ 41 &= A \end{aligned}$$

Así, aunque el Teorema 2 indique que dado cualquier entero $B > 0$, existe un polinomio $x^2 + x + A$ que es primo para todo entero con $0 \leq x \leq B$, los Teoremas 3 y 4 establecen que B no puede ser $A-2$ si $A > 41$. Con esto se establece el polinomio de Euler como generador primario de números primos consecutivos.

4. ALGUNOS POLINOMIOS CUADRÁTICOS QUE GENERAN PRIMOS

Los siguientes polinomios encontrados, son también generadores de números primos.

Polinomio P: $P(x) = x^2 + x + 3$ genera dos números primos consecutivos, para los enteros $x = 0, 1$ se obtienen los primos 3 y 5 respectivamente.

Véase que $P(x)$ tiene discriminante -11 y longitud principal 2 esto por la Definición 1, este polinomio es uno de los que menor cantidad de números primos consecutivos genera.

Polinomio N: Este polinomio, $N(x) = 2x^2 + 11$ es primo para los enteros $x = 0, 1, 2, 3, \ldots, 10$

11	13	19	29	43
61	83	109	139	173
211				

Cuadro 8: Polinomio $N(x)$

El polinomio $N(x)$ es irreducible y tiene discriminante -88, véase que:

$$\begin{aligned} N(11) &= 2(11)^2 + 11 \\ &= 2(121) + 11 \\ &= 242 + 11 \\ &= 253 \end{aligned}$$

253 es un número compuesto cuyos divisores son:1, 11, 23 y 253, además

$$\begin{aligned} N(10) &= 2(10)^2 + 11 \\ &= 2(100) + 11 \\ &= 200 + 11 \\ &= 211 \end{aligned}$$

donde 211 es un número primo, por la **Definición 1** el polinomio $N(x)$ tiene longitud principal 11.

Polinomio D: el polinomio $D(x) = 2x^2+29$ genera números primos para los enteros $x = 0, 1, 2, 3, \ldots, 28$

29	31	37	47	61
79	101	127	157	191
229	271	317	367	421
479	541	607	677	751
829	911	997	1087	1181
1279	1381	1487	1597	

Cuadro 9: Polinomio $D(x)$

el discrimininate de este polinomio es: -232, cuando $x = 29$ se tiene:

$$\begin{aligned} D(29) &= 2(29)^2 + 29 \\ &= 2(841) + 29 \\ &= 1682 + 29 \\ &= 1711 \end{aligned}$$

1711 tiene como divisores a:$1, 29, 59, 1711$ es decir, 1711 es un número compuesto; ahora

$$\begin{aligned} D(28) &= 2(28)^2 + 29 \\ &= 2(784) + 29 \\ &= 1568 + 29 \\ &= 1597 \end{aligned}$$

como 1597 es un número primo, entonces por la **Definición 1** la longitud principal del polinomio $D(x)$ es 29.

Polinomio A: el polinomio $A(x) = x^2 + x + 5$ satisface el Teorema 4, tene discriminante $\Delta = -19$ y genera números primos para los enteros $x = 0, 1, 2, 3$

5	7	11	17

Cuadro 10: Polinomio $A(x)$

Véase que:

$$\begin{aligned} A(4) &= 4^2 + 4 + 5 \\ &= 16 + 4 + 5 \\ &= 25 \end{aligned}$$

25 es un número compuesto cuyos divisores son 1, 5 y 25; además

$$\begin{aligned} A(3) &= 3^2 + 3 + 5 \\ &= 9 + 3 + 5 \\ &= 17 \end{aligned}$$

Como 17 es primo, entonces por la **definición 1** el polinomio $A(x)$ tiene longitud principal 4.

Polinomio B: $B(x) = x^2 + x + 11$ es un polinomio que satisface el criterio de Rabinowtsch, con determinante -43 y genera primos consecutivos para $x = 0, 1, 2, 3, \ldots, 9$ los cuales se presentan en la siguiente tabla

11	13
17	23
31	41
53	67
83	101

Cuadro 11: Polinomio $B(x)$

Se tiene que:

$$\begin{aligned} B(10) &= 10^2 + 10 + 11 \\ &= 100 + 10 + 11 \\ &= 121 \end{aligned}$$

Donde 121 es un número compuesto con 1,11 y 121 como divisores. Ahora

$$\begin{aligned} B(9) &= 9^2 + 9 + 11 \\ &= 81 + 9 + 11 \\ &= 101 \end{aligned}$$

Como 101 es primo por la **Definición 1** la longitud principal de $B(x)$ es 10.

Polinomio M: El polinomio $M(x) = x^2 + x + 17$ tiene discriminante -67 y como se mostró en el capítulo anterior satisface el Teorema 4, este polinomio genera primos consecutivos para $x = 0, 1, 2, \ldots, 15$

como se exhibe en el cuadro 7. para $M(16)$ se tiene:

$$\begin{aligned} M(16) &= 16^2 + 16 + 17 \\ &= 256 + 16 + 17 \\ &= 289 \end{aligned}$$

El número 289 es compuesto, ya que sus divisores son: 1,17 y 289.

Ahora

$$\begin{aligned} M(15) &= 15^2 + 15 + 17 \\ &= 225 + 15 + 17 \\ &= 257 \end{aligned}$$

Siendo 257 un número primo por la **Definición 1** esto implica que la longitud principal del polinomio $M(x)$ es 16.

Polinomio L: $L(x) = 2x^2 + 2x + 19$ es un polinomio con determinante -148 y para los valores $x = 0, 1, 2, \ldots, 17$ genera los primos consecutivos que se muestran a continuación.

19	23	31
43	59	79
103	131	163
199	239	283
331	383	439
499	563	631

Cuadro 12: Polinomio $L(x)$

Véase que:

$$\begin{aligned} L(18) &= 2(18)^2 + 2(18) + 19 \\ &= 2(324) + 36 + 19 \\ &= 648 + 36 + 19 \\ &= 703 \end{aligned}$$

Como 703 es divisible por $1, 19, 37$ y 703 entonces es un número compuesto.

Calculando $L(x)$:

$$\begin{aligned} L(17) &= 2(17)^2 + 2(17) + 19 \\ &= 2(289) + 34 + 19 \\ &= 578 + 34 + 19 \\ &= 631 \end{aligned}$$

Se tiene que 631 es un número primo, luego por la **Definición 1** el polinomio $L(x)$ es de longitud principal 18.

Polinomio R: $R(x) = 6x^2 + 6x + 31$ un polinomio con discriminante -708, que genera primos consecutivos para $x = 0, 1, 2, \ldots, 28$, como se exhibe en el siguiente cuadro

31	43	67	103	151
211	283	367	463	571
691	823	967	1123	1291
1471	1663	1867	2083	2311
2551	2803	3067	3343	3631
3931	4243	4567	4903	

Cuadro 13: Polinomio $R(x)$

Ahora

$$\begin{aligned} R(29) &= 6(29)^2 + 6(29) + 31 \\ &= 6(841) + 174 + 31 \\ &= 5046 + 174 + 31 \\ &= 5251 \end{aligned}$$

5251 es un número compuesto, ya que sus divisores son: $1, 58, 89$ y 5251.

Se tiene también que:

$$\begin{aligned} R(28) &= 6(28)^2 + 6(28) + 31 \\ &= 6(784) + 168 + 31 \\ &= 4704 + 168 + 31 \\ &= 4903 \end{aligned}$$

Con 4903 un número primo, entonces $R(x)$ tiene longitud principal 29 esto por la **Definición 1**.

5. Conclusiones

Los números primos se caracterizan así, por ser divisibles solo por uno y sí mismos, una característica que los hace completamente especiales y la base de los demás números, sin embargo, no se tiene conocimiento de su naturaleza; pero si se conocen maneras de generar a algunos de ellos. Podemos encontrar polinomios cuadráticos $F(x) = ax^2 + bx + c$ que generen primos, pero la verdadera esencia esta en esos polinomios cuadráticos que generan números primos consecutivos.

En el trabajo presentado anteriormente se muestra que aunque los números primos son infinitos, los polinomios cuadráticos que generan primos consecutivos distintos generan solo una cantidad finita de ellos, la principal característica de estos es que tienen discriminante $\Delta < 0$ pero no todos los polinomios con discriminante negativo tiene la capacidad de generar primos.

Finalmente, se tiene que una característica de los polinomios cuadráticos como generadores de primos es que, $\Delta \equiv 1 \pmod 4$ y además su discriminante $\Delta \in \{-163, -67, -43, -19, -11, -7, -3\}$; aun cuando se han encontrado diversos polinomios con estas características, la cantidad de números primos distintos generados no es mayor a 40.

Referencias

[1] R.A. Molling, *Prime-Producing Quadratics.*Amer. Math. Monthly 104 (1997), pags 529-544.

[2] A. BALOG. *The prime k-tuples conjeture on average, in Analityc Number Theory.* (Bruce C. Berndt, Harold G. Diamond, Heini Halberstam, and Adolf Hildebrand, eds), Birkauser, Bostón, Basel, Berlin, 1990, pags 47-75.

[3] O. Higgins, *Another long string of primes.* J.Rec Math. 14(1982), 185.

[4] E. B. Escott, Reponses 1133. *Formule d'Euler et formules analogues* .L'intermédiare des Math. 6(1899), pags 10-11.

[5] D.-A.Cox, *primes of the form* $x^2 + ny^2$. J.Wiley and Sons, New York (1989), pags 149-150.