Premios del Departamento de Matemáticas de la Universidad Autónoma de Madrid para Estudiantes de Secundaria

Sexta Edición, 2011/2012

TRABAJO: Sobre la espiral de Ulam y la distribución de los primos a lo largo de una sucesión de enteros positivos generada por un polinomio de Bouniakowsky

GANADOR EN LA CATEGORÍA DE BACHILLERATO

AUTORES:

- Diego Caro Martín
- Pablo Gómez Pérez
- Raúl González Molina
- Sergio Hernández Cuenca
- Elena Méndez Cancelas

TUTOR:

- Alfonso Camaño Liceras
- Salvador Fernández Casares

CENTRO: IES San Mateo (Madrid)

Sobre la espiral de Ulam y la distribución de los primos a lo largo de una sucesión de enteros positivos generada por un polinomio de Bouniakowsky

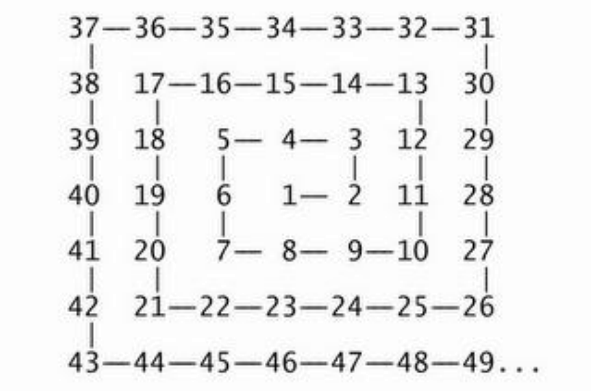
27/01/2012

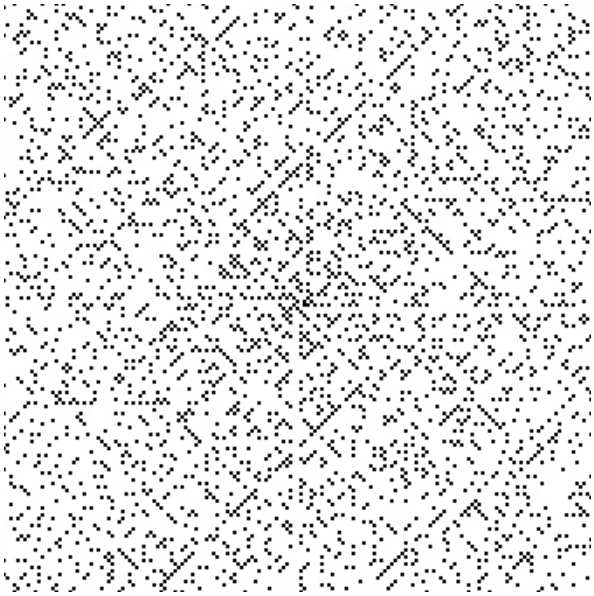
SOBRE LA ESPIRAL DE ULAM Y LA DISTRIBUCIÓN DE LOS PRIMOS A LO LARGO DE UNA SUCESIÓN DE ENTEROS POSITIVOS GENERADA POR UN POLINOMIO DE BOUNIAKOWSKY

Contenido

1. Introducción y Antecedentes: Espiral de Ulam

La espiral de Ulam es un modo de presentar la sucesión de los enteros positivos en el que los números se suceden a lo largo de una línea quebrada que se pliega alrededor de sí misma a modo de espiral cuadrangular, como en la figura.





Primos en la Espiral de Ulam representados como puntos

Los números primos aparecen en negro sobre fondo blanco, y se observan patrones de distribución curiosos que afectan a la distribución de los números primos entre los enteros positivos. Por ejemplo, la concentración de los mismos a lo largo de determinadas rectas horizontales verticales y diagonales.

Conforme se amplía el área cubierta y el número de vueltas de la espiral, algunos patrones de distribución de primos y de compuestos se confirman.

A pesar del interés de estos patrones no se puede olvidar en ningún momento que estamos ante la sucesión de enteros positivos plegada de una determinada forma, donde los primos son, simplemente, una subsucesión de ellos.

Lo que se conoce sobre la distribución de los primos entre los enteros positivos sigue siendo válido en la espiral de Ulam como lo es cuando disponemos los números primos a lo largo de la semirrecta real positiva. Lo que sucede es que la espiral de Ulam revele algunos patrones adicionales de la distribución.

Por este motivo, conviene comenzar recordando algunos resultados conocidos y probados sobre la distribución de los primos en $\mathbb{R}^+$.

2. DISTRIBUCIÓN DE LOS PRIMOS ENTRE LOS REALES POSITIVOS

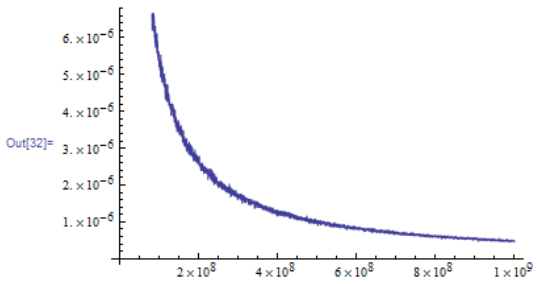
Para estudiar la distribución de los primos se utiliza la función $\pi(x): \mathbb{R}^+ \longrightarrow \mathbb{N}$,

que asocia a cada real positivo el número de primos inferiores o iguales a él.

Esta función monótona creciente encierra el secreto de la densidad de los primos en cualquier conjunto de reales positivos, por ejemplo en el intervalo $[0, x]$ el ratio $\frac{\pi(x)}{x}$ indica la densidad de primos en el citado intervalo.

Esta densidad es decreciente y tiende hacia cero como quedó probado en el Teorema de los números primos al que nos referiremos más adelante.

```
In[32]:= Plot[(PrimePi[n + 10 000] - PrimePi[n])/n, {n, 1, 1 000 000 000}]
```



El gráfico ilustra la evolución de la proporción de números primos a intervalos de 10000 enteros positivos consecutivos. Se pone de manifiesto que los primos son cada vez más raros.

El teorema de los números primos conjeturado por Gauss a partir de algunos resultados de Euler y demostrado por J. Hadamard establece que las tres funciones:

$$\pi(x), \quad Li(x) = \int_2^x \frac{dt}{log(t)} \quad y \quad \frac{x}{log(x)}$$

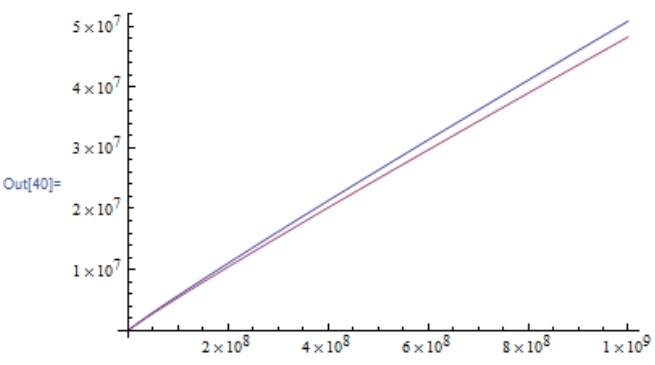
son infinitos equivalentes, o sea que:

$$\lim_{x\to\infty} \frac{\pi(x)}{Li(x)} = 1, \ \lim_{x\to\infty} \frac{Li(x)}{\frac{x}{log(x)}} = 1 \quad , \ \lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{log(x)}} = 1$$

Donde $\pi(x)$ hace referencia al número exacto de primos hasta $x \in \mathbb{R}$, y las otras dos funciones constituyen estimaciones más o menos precisas de $\pi(x)$ por medio de $Li(x)$ y $\frac{x}{log(x)}$

La estimación de $\pi(x)$ dada por la función $\frac{x}{log(x)}$ es peor que la proporcionada por la integral logarítmica. La mera visualización de ambas funciones lo pone de manifiesto. Pero nos aclara que los números primos son cada vez más raros a lo largo de la sucesión de enteros positivos y que entre 0 y n existe un primo aproximadamente cada $log(n)$.

```
In[40]:= Plot[{PrimePi[n], n/Log[n]}, {n, 1, 1 000 000 000}]
```



Evidentemente lo que se conoce sobre la distribución de los primos es aplicable a la espiral de Ulam, concretamente, cada vuelta de la espiral es un intervalo de enteros positivos. Si se considera final de cada vuelta el punto "norte", se conforma una sucesión que es una subsucesión de la de los enteros positivos: 1, 4, 15, 34, 61 ... Esta semirrecta vertical de puntos norte corresponde al polinomio $4n^2 - 9n + 6$ que toma los valores de la sucesión de puntos norte para $n = 1, 2, 3$ ...

Las diferencias finitas de primer y segundo orden de esta subsucesión son:

$$\begin{array}{ccccccc} 1 & & 4 & & 15 & 34 & 61 \ldots \\ & 3 & & 11 & 19 & 27 \ldots & \\ & & 8 & 8 & 8 \ldots & & \end{array}$$

O sea, que las diferencias finitas de segundo orden de los elementos que conforman la sucesión de puntos norte de cada vuelta son constantes e iguales a 8.

No es el único caso en que las diferencias segundas son constantes e iguales a 8, sino que se ha observado esto en diversas semirrectas verticales, semirrectas horizontales y semirrectas diagonales de 45º. Que las diferencias finitas de segundo orden sean constantes implica que el término general de estas subsucesiones sea un polinomio de segundo grado:

$$p(n) = an^2 + bn + c$$
$$p(n+1) = a(n+1)^2 + b(n+1) + c$$
$$p(n+2) = a(n+2)^2 + b(n+2) + c$$

$$\Delta(n) = p(n+1) - p(n) = 2an + a + b; \qquad \Delta(n+1) = p(n+2) - p(n+1) = 2an + 3a + b$$

$$\Delta^2(n) = \Delta(n+1) - \Delta(n) = 2a$$

Siendo la diferencia de orden dos igual a 8; $2a = 8 \Rightarrow a = 4$. Luego la forma de los polinomios que definen semirrectas en la espiral de Ulam será $4n^2 + bn + c \quad b, c \in \mathbb{Z}$ y la variable n toma valores enteros crecientes a partir de un determinado valor (positivo o negativo) de modo que el polinomio tome solo valores enteros positivos.

3. Polinomios cuadráticos en la espiral de Ulam

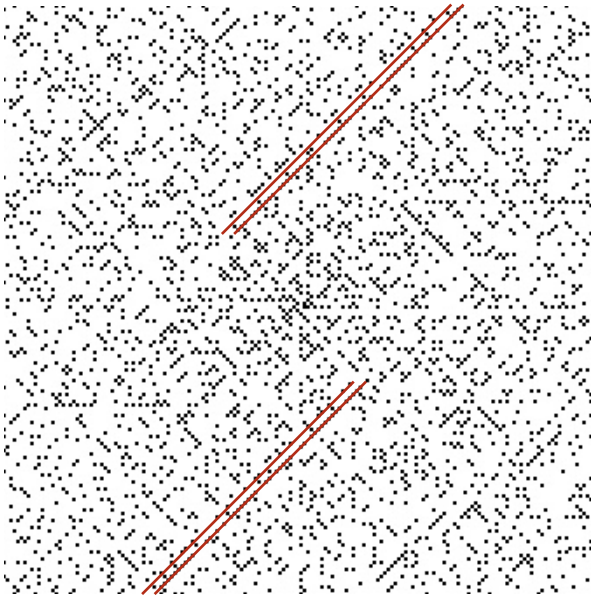
Resulta interesante observar los polinomios que corresponden a las semirrectas de la espiral de Ulam más densas en primos. La observación de la espiral muestra en concreto 2 semirrectas especialmente densas que son las señaladas en la figura.

Los polinomios generadores de cada una de las semirrectas han sido calculados conociendo que $a = 4$, y empleando 2 términos correspondientes a cada una de las rectas,

consiguiendo así determinar los otros coeficientes de cada polinomio, donde n recorre los enteros positivos más el cero $p(n) = 4n^2 + 150n + 1447$ y $q(n) = 4n^2 + 154n + 1523$

Puede comprobarse que ambos polinomios pueden obtenerse del conocido polinomio de Euler $m^2 + m + 41$ realizando el cambio de variable:

$$m = (2n) + 37 \quad o \quad m = (2n + 1) + 37$$



Por consiguiente el polinomio de Euler está detrás de ambas semirrectas, en un caso para valores impares de la variable y en el otro para valores pares. Cabe preguntarse: ¿se mantendrá esta capacidad de generar primos a lo largo de todos los enteros positivos y no sólo a esta porción de la espiral? ¿Habrá polinomios que generen aún más primos? ¿Qué relación guarda el polinomio con la capacidad de generar primos?

4. Conjetura y polinomios de Bouniakowsky

Interesan los polinomios o, mejor dicho, las funciones polinómicas con coeficientes enteros $p: \mathbb{N} \longrightarrow \mathbb{Z} \quad p(n) = a_0 + a_1 n + a_2 n^2 + \cdots . + a_k n^k$ con $a_0, a_1, a_2, \ldots . , a_n \in \mathbb{Z}$ capaces de generar abundantes primos cuando la variable recorre el dominio de los naturales.

Hay varias condiciones necesarias adicionales para que estos polinomios sean generadores de abundantes primos. En primer lugar el coeficiente del término de mayor grado debe ser positivo o, de lo contrario el polinomio solo tomará un número finito de valores naturales e infinitos enteros negativos, por tanto solo interesan los polinomios que verifican $a_k \geq 1$. El signo positivo del coeficiente del término de mayor grado implica que, aunque la función polinómica puede tomar valores enteros negativos, existirá un valor natural a partir del cual la función polinómica es monótona creciente.

Otra condición necesaria para que un polinomio de cualquier grado con coeficientes enteros genere abundantes primos es que sea irreducible en $\mathbb{Z}[n]$, dado que si el polinomio es factorizable, todos los elementos que genera serán factorizables. No obstante, que un polinomio sea irreducible no es condición suficiente. Por ejemplo, el polinomio $3n^2 - n + 2$ es irreducible en $\mathbb{Z}[n]$ pero sólo genera números pares 4, 12, 26, 46... puesto que:

$$3n^2 - n + 2 = n(3n - 1) + 2$$

y como n o $3n - 1$ es par, el polinomio siempre toma valores pares.

El matemático ruso Viktor Bouniakowsky propuso en 1857 la siguiente conjetura que, aunque no ha sido demostrada, tampoco existe contraejemplo que permita rechazarla:

"Los polinomios irreducibles en $\mathbb{Z}[n]$ ***de grado 2 o superior con coeficiente del término de mayor grado mayor o igual que 1 considerados como funciones polinómicas*** $p: \mathbb{N} \longrightarrow \mathbb{Z}$ ***cumplen una y sólo una de las dos condiciones siguientes:***

a) Generan infinitos primos

b) Existe un divisor común mayor que 1 de todos los enteros positivos que genera, por tanto no genera más de un primo (el divisor común por sí solo)"

El polinomio $3n^2 - n + 2$ es irreducible pero es del tipo b) ya que todos los elementos que genera son divisibles por 2.

A los polinomios de $\mathbb{Z}[n]$ de grado 2 o superior que generan infinitos primos cuando se consideran funciones polinómicas de $\mathbb{N}$ en $\mathbb{Z}$ se les denomina polinomios de Bouniakowsky.

5. Distribución de imágenes primas en polinomios de Bouniakowsky.

En esta sección se consideran únicamente polinomios de Bouniakowsky tal y como se han definido en la sección anterior. Generan infinitos primos y nos interesa estudiar la distribución de los mismos. Vamos a verificar que estos polinomios, salvo por un factor de escala, preservan la distribución de los primos propia de los enteros positivos. Cada polinomio tiene un factor de escala característico, los polinomios más ricos en primos tienen factores de escala mayores.

Para estudiar la distribución de primos se utiliza el ratio entre el número de primos existentes en las imágenes y el número de primos existentes en el intervalo que hace de dominio $\frac{\mu(p(I_k))}{\mu(I_k)}$, donde $\mu(A)$ es la función que asocia a cada subconjunto finito de enteros positivos el número de primos que contiene.

Con el siguiente programa se ha analizado el conocido polinomio de Euler

$$p(n) = n^2 + n + 41$$

y se ha computando para intervalos estancos consecutivos de 10^7 enteros positivos el ratio de numero de imágenes primas sobre números primos en el dominio.

Los resultados del análisis practicado por este programa aparecen en la matriz que aparece a continuación en la que puede observarse que en todos los subintervalos considerados las imágenes primas del polinomio triplican las de su dominio.

```
p[n_] := n^2 + n + 41;
fin = 10 000 000;
ite = 20;
MU = Table[{0, 0, 0, 0, 0, 0, 0}, {k, 1, ite}];
Do[num = 0;
  Do[If[PrimeQ[p[k]], num++], {k, (m - 1) * fin, m * fin}];
  MU[[m, 1]] = (m - 1) * fin;
  MU[[m, 2]] = m * fin;
  MU[[m, 3]] = num;
  MU[[m, 4]] = num * 1. / fin;
  MU[[m, 5]] = (PrimePi[m * fin] - PrimePi[(m - 1) * fin]);
  MU[[m, 6]] = MU[[m, 5]] * 1. / fin;
  MU[[m, 7]] = MU[[m, 3]] * 1. / MU[[m, 5]],
  {m, 1, ite}];
MatrixForm[MU]
```

Intervalo de enteros positivos I_k

Primos en la imagen del subintervalo $\mu(p(I_k))$

Proporción de primos en la imagen del subintervalo $p(I_k)$

0	10 000 000	2 208 197	0.22082	664 579	0.0664579	3.3227
10 000 000	20 000 000	2 011 729	0.201173	606 028	0.0606028	3.31953
20 000 000	30 000 000	1 950 344	0.195034	587 252	0.0587252	3.32114
30 000 000	40 000 000	1 911 978	0.191198	575 795	0.0575795	3.32059
40 000 000	50 000 000	1 885 271	0.188527	567 480	0.056748	3.32218
50 000 000	60 000 000	1 863 462	0.186346	560 981	0.0560981	3.32179
60 000 000	70 000 000	1 844 355	0.184436	555 949	0.0555949	3.31749
70 000 000	80 000 000	1 831 172	0.183117	551 318	0.0551318	3.32144
80 000 000	90 000 000	1 819 368	0.181937	547 572	0.0547572	3.32261
90 000 000	100 000 000	1 806 780	0.180678	544 501	0.0544501	3.31823
100 000 000	110 000 000	1 797 924	0.179792	541 854	0.0541854	3.3181
110 000 000	120 000 000	1 789 056	0.178906	538 339	0.0538339	3.32329
120 000 000	130 000 000	1 781 400	0.17814	536 539	0.0536539	3.32017
130 000 000	140 000 000	1 773 238	0.177324	534 012	0.0534012	3.3206
140 000 000	150 000 000	1 767 012	0.176701	532 197	0.0532197	3.32022
150 000 000	160 000 000	1 761 370	0.176137	530 062	0.0530062	3.32295
160 000 000	170 000 000	1 753 886	0.175389	528 625	0.0528625	3.31783
170 000 000	180 000 000	1 747 918	0.174792	527 302	0.0527302	3.31483
180 000 000	190 000 000	1 744 133	0.174413	525 088	0.0525088	3.3216
190 000 000	200 000 000	1 738 427	0.173843	523 464	0.0523464	3.32101

Primos en el subintervalo $\mu(I_k)$

Proporción de primos en el subintervalo I_k

Ratio $\frac{\mu(p(I_k))}{\mu(I_k)}$

El ratio $\frac{\mu(p(I_k))}{\mu(I_k)}$ para el polinomio de Euler $n^2 + n + 41$ es estable en los intervalos analizados alrededor del valor 3,32, de modo que multiplica por este factor el número de primos que se encuentra en su dominio. Como no puede ser de otro modo por el TNP, el número de primos en la imagen de los intervalos va decreciendo como también decrece el número de primos en el intervalo. No obstante, el ratio representado por la última columna de la matriz es prácticamente estable.

La estabilidad de este ratio no es una característica exclusiva del polinomio de Euler. No importa el grado del polinomio; si es un polinomio de Bouniakowsky, el ratio que representa la última columna se estabiliza en un valor que es característico del propio polinomio. El siguiente polinomio de Bouniakowsky:

$$n^4 - 97n^3 - 3294n^2 - 45458n + 213589$$

también genera un ratio estable 1.22 mayor que la unidad. Otro polinomio $n^2 + n + 17$ genera un ratio de 2.09.

La estabilidad del ratio observada en intervalos estancos disjuntos debe ser incluso mayor cuando se consideran siempre intervalos encajados de la forma $[1,\ a \cdot 10^n]$ con a constante y n entero positivo creciente. De modo que cabe esperar que la sucesión $\left\{\frac{\mu(p([1,a\cdot 10^n]))}{\mu([1,a\cdot 10^n])}\right\}_{n\in\mathbb{N}}$ sea convergente hacia un límite real**.** Con el siguiente programa se pretende aproximar el límite

$$\lim_{n\to\infty} \frac{\mu(p([1,a\cdot 10^n]))}{\mu([1,a\cdot 10^n])}$$

correspondiente a cualquier polinomio de Bouniakowsky. Los resultados con algunos polinomios han sido los siguientes:

```
p[n_] := 4 n^2 - 11 n + 8;
fin = 300 000 000;
MU = Table[{0, 0, 0, 0, 0}, {k, 1}];
num = 0;
Do[If[PrimeQ[p[k]], num++], {k, 0, fin}];
MU[[1, 1]] = 0;
MU[[1, 2]] = fin;
MU[[1, 3]] = num;
MU[[1, 4]] = PrimePi[fin];
MU[[1, 5]] = MU[[1, 3]] * 1. / MU[[1, 4]];
MatrixForm[MU]
( 0  300 000 000  15 453 341  16 252 325  0.950839 )
```

```
p[n_] := n^2 + n + 41;
( 0  300 000 000  53 958 075  16 252 325  3.32002 )

p[n_] := n^2 + n + 17;
( 0  300 000 000  33 924 554  16 252 325  2.08737 )

p[n_] := n^4 - 97 n^3 - 3294 n^2 - 45 458 n + 213 58
( 0  300 000 000  19 944 253  16 252 325  1.22716 )
```

En todos los casos analizados, el ratio estimado converge hacia un valor característico del polinomio por lo que nos parece que se puede conjeturar lo siguiente:

"Las sucesiones de enteros positivos obtenidas mediante polinomios de Bouniakowsky verifican que, si la función μ asocia a cualquier conjunto de enteros positivos el número de primos que contiene, entonces la sucesión de números reales $\left\{\frac{\mu(p((0,10^n])))}{\mu((0,10^n])}\right\}_{n\in\mathbb{N}}$ ***es convergente hacia un número real característico del propio polinomio,***

que podemos denominar ratio de densidad de primos del polinomio $p(n)$ y que se nota como $RDP(p)$:

$$\boldsymbol{RDP(p) = lim_{n\to\infty} \frac{\mu(p([1,10^n]))}{\mu([1,10^n])}} \quad \text{„}$$

Naturalmente, una conjetura así conduce a otras preguntas como ¿qué relación existe entre el $RDP(p)$ de un polinomio de Bouniakowsky $p(n)$ y sus coeficientes? ¿Puede determinarse de algún modo funcional el ratio correspondiente a un polinomio a partir de sus coeficientes? ¿Qué hace que unos polinomios tengan ratios muy altos y otros más bajos?

6. Polinomios de Bouniakowsky cuadráticos y su $RDP(p)$.

Habiendo partido en el estudio de la espiral de Ulam, es lógico que nos concentremos en los polinomios de Bouniakowsky de segundo grado, ya que representan semirrectas de la espiral. Vamos a hacer algunas consideraciones sobre estos polinomios que nos van a ser útiles para la búsqueda de polinomios con $RDP(p)$ alto, o sea grandes generadores de primos.

Polinomios irreducibles distintos como $p(n) = n^2 + n + 17$ y $q(m) = m^2 - 19m + 107$, generan, sin embargo, la misma imagen salvo en un conjunto finito de valores:

n	p(n)	m	q(m)
1	19	1	89
2	23	2	73
3	29	3	59
4	37	4	47
5	47	5	37
6	59	6	29
7	73	7	23
8	89	8	19
9	107	9	17
10	127	10	17
11	149	11	19
12	173	12	23
13	199	13	29
14	227	14	37
15	257	15	47
16	289	16	59
17	323	17	73

Las imágenes de ambos polinomios son coincidentes con un desfase en el dominio. Estos dos polinomios generarán eventualmente los mismos primos salvo un número finito que irá perdiendo peso relativo y ambos tendrán el mismo ratio de generación $RDP(p) = RDP(q)$.

En realidad, lo que hace que estos polinomios tengan el mismo ratio es que uno se obtiene del otro mediante un desplazamiento o traslación del dominio:

$p(m-10) = (m-10)^2 + (m-10) + 17 = m^2 - 19m + 107 = q(m)$;

Luego se tiene la siguiente proposición:

"Dados dos polinomios de Bouniakowsky de segundo grado:

$\boldsymbol{p(n) = a_2n^2 + a_1n + a_0}$ ***y*** $\boldsymbol{q(n) = b_2n^2 + b_1n + b_0}$

entonces si existe un natural $\boldsymbol{k \in \mathbb{N}}$ ***tal que*** $\boldsymbol{q(n+k) = p(n)}$ ***para todo natural n entonces*** $\boldsymbol{p(\mathbb{N}) \subset q(\mathbb{N})}$ ***y ambos polinomios tienen asociado el mismo ratio"***

La demostración de esta proposición es evidente ya que $p(n)$ genera las mismas imágenes que $q(m)$ y el numerador del ratio correspondiente a cualquier intervalo sólo puede diferir en un número finito que se diluirá conforme el intervalo se haga más grande. Podría haber, eso sí, polinomios de Bouniakowsky con el mismo ratio y no por ello que uno se obtenga como desplazamiento del otro.

Podemos definir una relación de equivalencia entre los polinomios de Bouniakowsky de segundo grado: $p(n)$ se relaciona con $q(n)$ por definición si tienen el mismo ratio de densidad de primos:

$p(n) \sim q(n) \quad \Leftrightarrow \quad RDP(p) = RDP(q)$

Esta relación divide al conjunto de los polinomios de Bouniakowsky en clases de equivalencia de polinomios con el mismo RDP. Cada clase contiene un polinomio $p(n)$ y todos los que tienen el mismo ratio de densidad de primos. Entre ellos estarán todos los desplazados de $p(n)$, es decir, todos los polinomios de la forma $p(n-k)$.

Otra proposición útil a los efectos de la búsqueda de polinomios con alto ratio es la siguiente:

"Cualquier polinomio de Bouniakowsky de segundo grado $\boldsymbol{p(n) = an^2 + bn + c}$ ***tiene polinomios de su misma clase de equivalencia cuyos coeficientes son todos ellos mayores o iguales que 1"***

En efecto, dado el polinomio $p(n) = an^2 + bn + c$, se consideran los polinomios que se obtienen mediante desplazamientos del mismo:

$p(m+k) = a(m+k)^2 + b(m+k) + c = am^2 + 2akm + ak^2 + bm + bk + c$

$p(m+k) = am^2 + (2ak + b)m + (ak^2 + bk + c)$

El coeficiente $a > 0$ como en todos los polinomios de Bouniakowsky, además:

$$\left.\begin{matrix} 2ak+b>0 \\ ak^2+bk+c>0 \end{matrix}\right\}$$

La primera condición es equivalente a $k > \frac{-b}{2a}$. En cuanto a la segunda condición caben tres posibilidades:

a) Discriminante $b^2-4ac<0$ en cuyo caso dado que $a>0$ la parábola no corta al eje de las abscisas y está siempre por encima, es decir que $ak^2+bk+c>0$ para cualquier valor de k . En este caso para cualquier valor $k > \frac{-b}{2a}$ los tres coeficientes de $p(m+k)=am^2+(2ak+b)m+(ak^2+bk+c)$ son positivos y la proposición sería cierta.

b) Discriminante $b^2-4ac=0$ en cuyo caso dado que $a>0$ la parábola tiene el vértice en el eje de las abscisas que coincide con el punto de abscisa $\frac{-b}{2a}$ y eligiendo $k > \frac{-b}{2a}$ se está seguro de que $ak^2+bk+c>0$ y los tres coeficientes del polinomio trasladado $p(m+k)=am^2+(2ak+b)m+(ak^2+bk+c)$ son positivos y la proposición también sería cierta.

c) Discriminante $b^2-4ac>0$ en cuyo caso dado que $a>0$ la parábola corta al eje de las abscisas y tienen un mínimo en el vértice. Los puntos de corte con el eje de las abscisas son:

$$\frac{-b}{2a}-\frac{\sqrt{b^2-4ac}}{2a} \quad y \quad \frac{-b}{2a}+\frac{\sqrt{b^2-4ac}}{2a}$$

Eligiendo $k > \frac{-b}{2a}+\frac{\sqrt{b^2-4ac}}{2a}$ se verifica que $k > \frac{-b}{2a}$ y que $ak^2+bk+c>0$, o sea que los tres coeficientes de $p(m+k)=am^2+(2ak+b)m+(ak^2+bk+c)$ son positivos y la proposición también sería cierta.

Todas las clases de equivalencia de polinomios de Bouniakowsky con el mismo ratio de densidad de primos cuentan con polinomios cuyos coeficientes son enteros positivos. Por este motivo, la búsqueda de polinomios con altos ratios de densidad se puede restringir exclusivamente a los polinomios de Bouniakowsky con coeficientes naturales.

7. BÚSQUEDA DEL POLINOMIO CON MAYOR $RDP(p)$.

Ahora se trata de buscar polinomios de Bouniakowsky de segundo grado con mayor RDP que el 3,32 del polinomio de Euler. Esto requiere una gran potencia de cálculo, ya que se trabaja con todas las combinaciones posibles de polinomios cuyos coeficientes se encuentren en cierto intervalo.

La siguiente proposición nos deja claro que no deben tenerse expectativas maximalistas en la búsqueda:

"Ningún polinomio de Bouniakowsky de segundo grado genera exclusivamente primos".

En efecto, si el polinomio no tuviera término independiente no sería irreducible y, por tanto, generaría números compuestos. En caso de que tenga término independiente como:

$$p(n) = an^2 + bn + c = (an + b)n + c$$

entonces para valores de n que sean múltiplos de c es evidente que $c|p(n)$ luego el polinomio no genera sólo primos.

En la búsqueda se han incorporado algunos criterios cuya justificación es heurística pero basada en la observación de los polinomios analizados con ratio alto.

En primer lugar, centramos nuestro interés en el término independiente. Los polinomios con término independiente primo tienen generalmente ratio alto, al fin y al cabo si c tuviera muchos divisores, entonces para cualquier n múltiplo de cualquiera de los divisores se tendrá que $p(n)$ será divisible por dicho divisor de c, por tanto no primo. Cuantos más divisores tenga c, más valores de n no generarán primos. Cuantos menos divisores tenga el término independiente, menos compuestos generará. Por estas razones, aun reconociendo la naturaleza heurística del argumento, nos limitaremos a polinomios cuyo término independiente sea primo.

Con el término independiente primo en nuestro análisis, luego impar (excluyendo el 2), el resto del polinomio debe tomar valores pares o, de lo contrario, el resultado será múltiplo de dos. De esta forma tenemos:

$p(n) = an^2 + bn + c = (an + b)n + c$ donde $(an + b)n$ ha de ser par.

Para que sea par, observemos que ocurre según la paridad de a y b:

a	b	n	(an+b)n
Par	**Par**	**Par**	**Par**
Par	**Par**	**Impar**	**Par**
Par	Impar	Par	Par
Par	Impar	Impar	Impar
Impar	Par	Par	Par
Impar	Par	Impar	Impar
Impar	**Impar**	**Par**	**Par**
Impar	**Impar**	**Impar**	**Par**

Lo más efectivo será que todo n sea capaz de dar un valor par a la expresión. Esto sucede cuando los coeficientes a y b comparten paridad. En los casos en que a y b no comparten paridad, se reduce en un 50% el conjunto de las preimagenes capaces de generar primos, lo que supone una notable criba y cabe esperar que estos polinomios tengan ratios menores.

También se ha observado que, a medida que aumenta el coeficiente a, se ve muy reducida la cantidad de polinomios con ratio alto. Podría ser por el mayor índice de crecimiento junto con el hecho de que los primos son cada vez más raros. Por este motivo, el intervalo de variación del coeficiente a que se ha utilizado para la búsqueda es inferior a los considerados para b y c.

La eliminación del análisis de los polinomios equivalentes también supone una gran reducción de los polinomios a examinar. Para despreciar un polinomio de nuestro análisis, tenemos que verificar que ya ha sido analizado otro de su clase de equivalencia previamente. El análisis se realiza de forma creciente para los valores de los coeficientes, así que asumimos que para cada clase de equivalencia existe un polinomio $p(n)$ con los mínimos valores para sus coeficientes dentro del intervalo considerado, el cual será el primero en analizarse de su clase. Cualesquiera otros polinomios equivalentes a éste, con coeficientes positivos mayores, entre los demás polinomios que se estudien, podrán ser despreciados. Estos provendrán de un cambio de variable de $p(n)$, como $p(n+1),\ p(n+2), \dots,\ p(n+k) \dots \quad k \in \mathbb{N}$

Tan sólo nos interesa analizar $p(n) = an^2 + bn + c$, el mínimo de su clase, para el que no existe un $p(n-1)$ con todos sus coeficientes enteros positivos (incluyendo $b = 0$). En los

casos en que existe, como para $q(m) = p(n+k)$ $k \in \mathbb{N}$, basta con comprobar lo que le ocurre a los coeficientes de $q(m-1)$ para despreciarlo:

$$q(m-1) = a(m-1)^2 + b(m-1) + c = an^2 - 2n + 1 + bn - b + c.$$

Identificando coeficientes $q(m-1) = a'm^2 + b'm + c' = am^2 + (b-2a)m + (a-b+c)$.

Tratándose de un polinomio equivalente despreciable, sucede que $a' = a, b' \geq 0$ y $c' > 0$. Resulta siembre que $b > b'$, lo que nos permite afirmar con seguridad que el orden de análisis (que aparece más adelante) concuerda con el orden de aparición de polinomios equivalentes: $p(n),\ p(n+1),\ p(n+2)$ ... luego siempre encontraremos en primer lugar $p(n)$. Éste es el único que nos interesa, el primero de cada clase de equivalencia, para el que se cumple al menos una de las siguientes condiciones:

$$b - 2a < 0$$
$$a - b + c \leq 0$$

Si esto se verifica, el polinomio será analizado.

Por otro lado, la comprobación de si el polinomio es irreducible en $\mathbb{Z}$, incluyendo el caso de que los coeficientes no sean primos entre sí, también reduce considerablemente el conjunto de polinomios a ser analizados.

Finalmente, el rango de polinomios analizados se encuentra entre los coeficientes que cumplen con $a = [1,10],\ b = [0,4000],\ c = [1,4000]$.

a	1									2			…	10		
b	0				1			…	4000	0	…	4000	…	0	…	4000
c	1	2	…	4000	1	…	4000	…	4000	1	…	4000	…	1	…	4000

Los polinomios que finalmente se han analizado son muchos menos de los 160 040 000 contenidos en el rango de posibles valores de los coeficientes, gracias a los criterios.

El programa lleva a cabo el análisis con todos los criterios citados, y almacena los polinomios que superen el 50% de imágenes primas para $n \in [1,800]$:

```
fin = 800;
a = 0;
While[a < 10, s[n_] := a n^2 + b n + c;
 b = 0;
 a++;
 k = 2;
 If[OddQ[a], i = -1, i = 0];
 While[b ≤ 4000,
  c = 1;
  While[c ≤ 4000,
   p = 0;
   z = a - b + c;
   v = b - 2 a;
   If[(z ≤ 0 ∨ v < 0) ∧ (GCD[a, b, c] == 1 ∨ b == 0) ∧ ¬ IntegerQ[(-b + √(b^2 - 4 ac))/2],
    Do[If[PrimeQ[s[k]], p++], {k, 1, fin}];
    If[p > 400, p >>> MP.txt; a >>> MA.txt; b >>> MB.txt; c >>> MC.txt]];
   c = NextPrime[c]];
  b = i + k;
  i = b]]
```

Con este procedimiento se ha localizado el polinomio $n^2 + 2329n + 1697$, posteriormente se ha computado su ratio para un dominio mucho mayor [1, 300 000 000] con objeto de comprobar que la generación de primos permanece. Su ratio asociado es 4,33 notablemente mayor que el del polinomio de Euler.

Aunque el alto valor del $RDP(p)$ de este polinomio es incuestionable, no obstante, no se puede estar seguro de que sea el máximo dentro del rango analizado por dos motivos:

Primero, porque la criba realizada se basa en muchos casos en criterios heurísticos observados empíricamente y pueden haberse eliminado polinomios cuyo ratio sea más alto.

Segundo, porque la búsqueda ha tenido que realizarse utilizando un dominio reducido con la variable n tomando valores naturales entre 1 y 800, no es descartable que algún polinomio genere pocos primos entre los primeros 800 naturales, y posteriormente genere muchos más.

En todo caso, el polinomio encontrado $n^2 + 2329n + 1697$ tiene un ratio extraordinariamente alto y cualquier análisis más exhaustivo pasaría por la utilización de recursos informáticos más potentes que permitan ampliar el rango de polinomios analizados, reducir y suprimir algunos criterios heurísticos de eliminación y ampliar el rango de la variable para el análisis.

RESUMEN

OBJETIVOS

En un principio la idea de este trabajo fue explorar los patrones de distribución de los números primos que se observan como rectas en la espiral de Ulam. Enseguida se descubrió que las rectas se correspondían con sucesiones de naturales cuyo término general era un polinomio de segundo grado con coeficientes enteros.

Al observar cómo unos polinomios daban lugar a grandes concentraciones de primos y otros no, se llegó conocer la conjetura de Bouniakowsky, que lleva más de 150 años sin demostrarse ni refutarse. El análisis de estos polinomios reveló que todos ellos, los que generan alta densidad de primos y los que generan densidades menores, tienen en común que actúan como una lente de aumento o disminución sobre la cantidad de primos que pasan por su dominio.

El polinomio de Euler genera 3,32 primos por cada uno que se encuentra en su dominio. Otros polinomios generan menos, pero cada uno de ellos tiene un multiplicador característico. Esta estabilidad observada empíricamente en todos los polinomios de Bouniakowsky de cualquier grado es, sin duda, el mayor resultado de este trabajo. No puede decirse que fuera un objetivo inicial, pero acabó siendo un resultado que nos interesó.

A continuación, la curiosidad por ver si el polinomio de Euler era campeón de generación de primos nos movió a localizar polinomios de segundo grado con el ratio lo más alto posible. Esta búsqueda requería grandes recursos informáticos. Algunos análisis de búsqueda han estado ejecutándose varios días en ordenadores personales de última generación. Se ha encontrado un polinomio como $n^2 + 2329n + 1697$ cuyo ratio es de 4,33, pero la búsqueda se efectuó sobre un conjunto finito de polinomios.

RESULTADOS Y CONCLUSIONES

Como ya se ha comentado, el principal resultado del trabajo ha sido la observación empírica de la estabilidad en la generación de primos para los polinomios de Bouniakowsky. El número de primos que salen como imagen de una de estas funciones polinómicas es proporcional al número de primos que entran y la constante de proporcionalidad es característica del polinomio.

Se intentó encontrar una relación entre el ratio de cada polinomio y sus coeficientes pero dicha relación, si existe es muy compleja. A veces, pequeñas variaciones en uno de los coeficientes del polinomio cambian radicalmente su capacidad para generar primos.

Se ha localizado un polinomio que genera 4,33 primos por cada uno que encuentra en su dominio. Es un verdadero generador de primos. Con mayores recursos informáticos probablemente se pueden descubrir polinomios aún más eficientes.

La estabilidad plantea: ¿el conjunto de ratios posibles está acotado? En caso afirmativo, ¿existiría un extremo superior? Pero, ¿habrá un polinomio campeón?

BIBLIOGRAFÍA

"An Introduction to the theory of numbers", G. Hardy et al.

"Elementary number theory", Gareth A. Jones et al.

"Introduction to Analytic Number Theory", Tom M. Apostol

Artículos sobre la espiral de Ulam en http://www.wikipedia.org