Números Primos y Criptografía

Daniel Prelat, Martín Maulhardt, Tomás Cordero

Enero - Febrero 2014

Resumen. En el año 2013 probamos que en el conjunto de los números primos se satisface infinitas veces la desigualdad $p_{n+2} - p_{n+1} \leq p_{n+1} - p_n$. Hemos mencionado también que este resultado había sido probado previamente por Paul Erdős y Pal Turán en 1948 por un método diferente al nuestro. El valor de nuestro método se demostró en el hallazgo y la prueba de la generalización de la desigualdad mencionada. Concretamente hemos probado que en el conjunto de los números primos se satisface infinitas veces la desigualdad $p_{n+k} - p_n \leq p_n - p_{n-k}$ para cada valor entero positivo de k. Desafortunadamente no hay hasta el momento una medida de la proporción de veces que ocurre la desigualdad en cuestión. En este trabajo responderemos en esta dirección definiendo un nuevo concepto a través del cual podremos dar una cota inferior para el número de veces en que se verifica la desigualdad $p_{n+2} - p_{n+1} \leq p_{n+1} - p_n$.

1. CONCEPTOS FUNDAMENTALES

Definición : Sea $a_n : n \in N$ una sucesión creciente de números naturales. Sea $d_n = a_{n+1} - a_n$ la sucesión de diferencias primeras de a_n. Decimos que dicha sucesión satisface la propiedad de separación si la sucesión d_n es estrictamente creciente, i.e. $d_{n+1} > d_n$.

Veamos algunos ejemplos de sucesiones que satisfacen la propiedad de separación y de otras que no.

Ejemplos.

1. Sea $a_n = n^2$ i.e. $1, 4, 9, 16, \ldots n^2 \ldots$ Sus diferencias $d_n = a_{n+1} - a_n = 2n + 1$ forman una sucesión creciente. Luego la sucesión $a_n = n^2$ satisface la propiedad de separación.

2. Sea $a_n = 1, 2, 4, 5, 7, 8, \ldots 3n+1, 3n+2, \ldots$ La sucesión a_n no satisface la propiedad de separación pues $d_{2n} = 2$ y $d_{2n-1} = 1$ i.e. $d_n = 1, 2, 1, 2, 1, 2, \ldots$

Observación. Si una sucesión a_n satisface la propiedad de separación a partir de un cierto n_0 diremos indistintamente que la sucesión a_n tiene la propiedad de separación. Sólo si es necesario aclararemos a partir de qué n_0 se satisface dicha propiedad.

Ahora bien, si se introduce una nueva noción en matemática es porque uno va a aplicar dicha noción para concluir alguna propiedad. La consecuencia fundamental de la propiedad de separación se enuncia en el criterio de convergencia a continuación y el cual creemos es nuevo en la literatura matemática.

Teorema 1 (Criterio de convergencia). Sea a_n una sucesión de numeros naturales que satisface la propiedad de separación i.e. $d_{n+1} > d_n$. donde $d_n = a_{n+1} - a_n$. Entonces la serie $\sum_{n=1}^{\infty} \frac{1}{a_n}$ converge.

Demostración. Puede verse la demostración de este criterio en el trabajo correspondiente al año 2013.

Definición. Sea a_n una sucesión creciente de números naturales. Sea A el conjunto formado por los elementos de dicha sucesión. Se dice que el conjunto A es grande si la serie de sus recíprocos diverge i.e. $\sum_{n=1}^{\infty} \frac{1}{a_n} = \infty$

Nota. Nos interesa resaltar esta definición y la sintetizamos así :

$$A = \{a_n : n \in N\} \quad es \quad grande \Longleftrightarrow \sum_{n=1}^{\infty} \frac{1}{a_n} = \infty$$

Algunos ejemplos triviales de conjuntos grandes son el conjunto N de los números naturales, cualquier progresión aritmética infinita y también el conjunto P de los números primos (Euler, 1737).

Observemos ahora el contrarrecíproco del *Teorema 1.* Como una serie de terminos positivos necesariamente converge o diverge (no hay posibilidad de oscilación o de no existencia del límite de las sumas parciales si se considera como posible límite al infinito) deducimos una condición necesaria para que un conjunto sea grande. Concretamente el contrarrecíproco del *Teorema 1* es el siguiente *Corolario 2.*

Corolario 2. Sea a_n una sucesión creciente de números naturales tal que la serie $\sum_{n=1}^{\infty} \frac{1}{a_n} = \infty$. Entonces la sucesión de sus diferencias d_n satisface infinitas veces la desigualdad $d_{n+1} \leq d_n$ i.e.

$$a_{n+2} - a_{n+1} \leq a_{n+1} - a_n.$$

Este contrarrecíproco es nuestro verdadero aporte al trabajo de Erdős y Turán, porque nuestra demostración comprende a todos los conjuntos grandes y no sólo al conjunto de los números primos. Si se aplica el *Colorario 2* al conjunto de los números primos obtenemos que infinitas veces ocurre la desigualdad

$$p_{n+2} - p_{n+1} \leq p_{n+1} - p_n.$$

La obtención de dichas desigualdades es una propiedad intrínseca de la divergencia de sus recíprocos y no de que todo número natural se exprese de manera única como producto de números primos. Se puede aplicar, como haremos a continuación a los primos cuyo índice es solo par, impar, y en general a cualquier subconjunto de números primos que satisfaga la definición anterior de conjunto grande.

Antes de pasar a la sección 2 resumimos el colorario anterior en la siguiente implicación logica :

$$\sum_{n=1}^{\infty} \frac{1}{a_n} = \infty \quad \Longrightarrow \quad infinitas \;\; veces \quad d_{n+1} \leq d_n$$

2. GENERALIZACIÓN. AVANCES.

Hasta este punto hemos probado de una manera más simple que Erdős y Turán que el conjunto de los números primos no tiene la propiedad de separación. Nuestra prueba extiende esta propiedad a todos los conjuntos grandes. Es decir, todo conjunto grande no posee la propiedad de separación. Apliquemos esta idea para obtener algunos resultados nuevos en Teoría de números.

Erdős y Turán han probado, cambiando de índices, que se satisface infinitas veces en el conjunto de los números primos la desigualdad

$$p_{n+1} - p_n \leq p_n - p_{n-1}.$$

Geométricamente este resultado se puede interpretar así : La distancia de un determinado número primo al siguiente primo hacia la derecha es menor o igual que la distancia de dicho primo hacia el primo de la izquierda infinitas veces. Dos ejemplos de ternas de primos consecutivos que satisfacen dicha desigualdad son $(7, 11, 13)$ y $(23, 29, 31)$. De este tipo de ternas hay, según el *corolario 2* aplicado al conjunto P de los números primos una infinidad.

Los primeros resultados de este tipo se encuentran el su paper conjunto *"On some new questions on the distribution of prime numbers, 1948"*. Al final de dicho paper se preguntan por varias posibles generalizaciones de su resultado sin dar respuesta. Sin embargo, parece, han olvidado una. Concretamente, habrá infinitas ternas de primos que satisfagan la desgualdad

$$p_{n+2} - p_n \leq p_n - p_{n-2}.$$

o más general aún

$$p_{n+r} - p_n \leq p_n - p_{n-r}.$$

de la cual el caso $r = 1$ es sólo un caso particular?

La respuesta a esta pregunta es afirmativa y constituye el núcleo de esta sección.

Definición. Sea $p_1, p_2, p_3, p_4 \ldots, p_n \ldots$ la sucesión de números primos. La subsucesión $p_1, p_3, \ldots, p_{2n+1}, \ldots$ constituye el conjunto de los primos de índice impar y $p_2, p_4, \ldots, p_{2n}, \ldots$ constituye el conjunto de los primos de índice par.

Nota. Sin riesgo de confusión alguna diremos que un primo de índice par es un primo par y un primo de índice impar diremos que es un primo impar.

Teorema 3. El conjunto de los primos pares es un conjunto grande y también lo es el conjunto de los primos impares.

Demostración. Si uno de ellos no es un conjunto grande (por ejemplo el de los primos de índice par) entonces la serie de sus recíprocos converge i.e. $\sum_{n=1}^{\infty} \frac{1}{p_{2n}} < \infty$. Pero entonces converge también $\sum_{n=1}^{\infty} \frac{1}{p_{2n+1}} < \infty$. Y sumando ambas series obtendríamos la contradicción $\sum_{n=1}^{\infty} \frac{1}{p_n} < \infty$.

Teorema 4. En el conjunto de los números primos se satisface infinitas veces la desigualdad

$$p_{n+2} - p_n \leq p_n - p_{n-2}.$$

Demostración. De acuerdo al *Teorema 3* el conjunto de los primos pares es un conjunto grande i.e. la serie $\sum_{n=1}^{\infty} \frac{1}{p_{2n}} = \infty$. Luego, por el *Corolario 2* se satiface infinitas veces la desigualdad

$$a_{n+2} - a_{n+1} \leq a_{n+1} - a_n$$

Ahora bien, el conjunto de los primos pares se define por la identidad $a_n = p_{2n}$. Luego sustituyendo obtenemos infinitas veces

$$p_{2n+4} - p_{2n+2} \leq p_{2n+2} - p_{2n}$$

o lo que es lo mismo

$$p_{n+2} - p_n \leq p_n - p_{n-2}$$

como queríamos demostrar.

Nota. El *Teorema 4* es la generalización de la desigualdad de Erdős y Turán que mencionamos al comienzo de esta sección. Está probada en detalle para $r = 2$ pero nuestros razonamientos se extienden inmediatamente para cada $r \in N$ resultando infinitas veces en la desigualdad

$$p_{n+r} - p_n \leq p_n - p_{n-r}.$$

Finalizamos esta sección con la siguiente síntesis :

$$\sum_{n=1}^{\infty} \frac{1}{a_n} = \infty \Longrightarrow infinitas \;\; veces \quad a_{n+k} - a_n \leq a_n - a_{n-k}$$

3. DENSIDADES. FRECUENCIA CON QUE $d_{n+1} \leq d_n$