Espacios entre primos

Lola Thompson

Oberlin College

August 21, 2017

Espacios entre primos: una breve historia

Conjetura (de Polignac, 1849)

Para todos enteros pares h, hay número infinito de pares de primos $p, p+h$.

Llamamos a tales valores h *"números de Polignac"*.

Preguntas naturales sobre números de Polignac

Surgen algunas preguntas naturales:

Preguntas naturales sobre números de Polignac

Surgen algunas preguntas naturales:

- ¿Qué proporción de enteros pares son números de Polignac?

Preguntas naturales sobre números de Polignac

Surgen algunas preguntas naturales:

- ¿Qué proporción de enteros pares son números de Polignac?
- ¿Hay número infinito de números de Polignac?

Preguntas naturales sobre números de Polignac

Surgen algunas preguntas naturales:

- ¿Qué proporción de enteros pares son números de Polignac?
- ¿Hay número infinito de números de Polignac?
- ¿Cual es el número de Polignac más pequeño?

Preguntas naturales sobre números de Polignac

Surgen algunas preguntas naturales:

- ¿Qué proporción de enteros pares son números de Polignac?
- ¿Hay número infinito de números de Polignac?
- ¿Cual es el número de Polignac más pequeño?
- ¿¿¿Existen los números de Polignac???

Preguntas naturales sobre de Polignac numbers

Surgen algunas preguntas naturales:

- ¿Qué proporción de enteros pares son números de Polignac?
- ¿Hay número infinito de números de Polignac?
- ¿Cual es el número de Polignac más pequeño?
- ¿¿¿Existen los números de Polignac???

Preguntas naturales sobre de Polignac numbers

Surgen algunas preguntas naturales:

- ¿Qué proporción de enteros pares son números de Polignac?
- ¿Hay número infinito de números de Polignac?
- ¿Cual es el número de Polignac más pequeño?
- ¿¿¿Existen los números de Polignac???

Se conjectura que $h = 2$ es el más pequeño número de Polignac, i.e., hay número infinito de pares de **primos gemelos**.

Un enfoque heurístico burdo

Un lema heurístico

Teorema (Chebyshev, 1852)

Aproximadamente $\frac{1}{\log x}$ *de los enteros en* $[1, x]$ *son primos.*

Un enfoque heurístico burdo

Para los enteros en $[1, x]$:

Un enfoque heurístico burdo

Para los enteros en $[1, x]$:

- $P(p \text{ es primo}) = \frac{1}{\log x}$

Un enfoque heurístico burdo

Espacios entre primos

Lola Thompson

Introducción

Trabajos recientes sobre espacios entre primos

El método de Maynard-Tao

Variantes del teorema de Maynard-Tao

Aplicaciones a secuencias de primos consecutivos

Para los enteros en $[1, x]$:

- $P(p \text{ es primo}) = \frac{1}{\log x}$
- $P(p + 2 \text{ es primo}) = \frac{1}{\log x}$

Un enfoque heurístico burdo

Para los enteros en $[1, x]$:

- $P(p \text{ es primo}) = \frac{1}{\log x}$
- $P(p + 2 \text{ es primo}) = \frac{1}{\log x}$

Si los dos eventos fueran **independientes**, entonces

$$\begin{aligned} P(p \text{ y } p+2 \text{ primos}) &= P(p \text{ primo}) \cdot P(p+2 \text{ primo}) \\ &= \frac{1}{\log x} \cdot \frac{1}{\log x} \\ &= \left(\frac{1}{\log x}\right)^2. \end{aligned}$$

Un enfoque heurístico burdo

Por lo tanto, esperaríamos

$$\#\{p \leq x : p \text{ y } p+2 \text{ primos}\} \approx \frac{x}{(\log x)^2}.$$

Puesto que $\lim_{x\to\infty} \frac{x}{(\log x)^2} = \infty$, esto nos da razón de creer que hay número infinito de pares de primos gemelos...

Una problema con nuestro heurístico burdo

Problema: ¡Los eventos "p es primo" y "$p+2$ es primo" no son independientes!

Una problema con nuestro heurístico burdo

Problema: ¡Los eventos "p es primo" y "$p+2$ es primo" no son independientes!

¡Se podría mostrar (utilizando un argumento análogo) que

$$\#\{p \leq x : p \text{ y } p+1 \text{ primo}\} \approx \frac{x}{(\log x)^2},$$

lo cual es falso por supuesto!

Refinando nuestra heurística...

Una heurística mejorada

Para corregir la no independencia, sea p y p' números elegidos independientemente al azar. Miremos:

$$\frac{P(p, p+2 \text{ no ambos divisibles por } q)}{P(p, p' \text{ no ambos divisibles por } q)},$$

para cada primo pequeño q.

Una heurística mejorada

Para corregir la no independencia, sea p y p' números elegidos independientemente al azar. Miremos:

$$\frac{P(p, p+2 \text{ no ambos divisibles por } q)}{P(p, p' \text{ no ambos divisibles por } q)},$$

para cada primo pequeño q.

Puesto que

$$P(q \mid p) = \frac{1}{q},$$

tenemos que

$$P(q \nmid p) = 1 - \frac{1}{q}.$$

Una heurística mejorada

Para corregir la no independencia, sea p y p' números elegidos independientemente al azar. Miremos:

$$\frac{P(p, p+2 \text{ no ambos divisibles por } q)}{P(p, p' \text{ no ambos divisibles por } q)},$$

para cada primo pequeño q.

Puesto que

$$P(q \mid p) = \frac{1}{q},$$

tenemos que

$$P(q \nmid p) = 1 - \frac{1}{q}.$$

Por lo tanto,

$$P(q \nmid p \text{ y } q \nmid p') = \left(1 - \frac{1}{q}\right)^2.$$

Una heurística mejorada

$$P(q \nmid p \text{ y } q \nmid (p+2)) = P(p \not\equiv 0 \text{ o } -2 \pmod{q})$$

Una heurística mejorada

$$P(q \nmid p \text{ y } q \nmid (p+2)) = P(p \not\equiv 0 \text{ o } -2 \pmod{q})$$

Observemos que

$$P(p \not\equiv 0 \text{ o } -2 \pmod{q}) = \begin{cases} 1 - 2/q & \text{si } q > 2 \\ 1 - 1/2 & \text{si } q = 2 \end{cases}$$

Una heurística mejorada

$$P(q \nmid p \text{ y } q \nmid (p+2)) = P(p \not\equiv 0 \text{ o } -2 \pmod{q})$$

Observemos que

$$P(p \not\equiv 0 \text{ o } -2 \pmod{q}) = \begin{cases} 1 - 2/q & \text{si } q > 2 \\ 1 - 1/2 & \text{si } q = 2 \end{cases}$$

Así, si $q > 2$, entonces el factor de corrección para la divisibilidad por q es

$$\frac{(1 - \frac{2}{q})}{(1 - \frac{1}{q})^2}.$$

Una heurística mejorada

$$P(q \nmid p \text{ y } q \nmid (p+2)) = P(p \not\equiv 0 \text{ o } -2 \pmod{q})$$

Observemos que

$$P(p \not\equiv 0 \text{ o } -2 \pmod{q}) = \begin{cases} 1 - 2/q & \text{si } q > 2 \\ 1 - 1/2 & \text{si } q = 2 \end{cases}$$

Así, si $q > 2$, entonces el factor de corrección para la divisibilidad por q es

$$\frac{(1 - \frac{2}{q})}{(1 - \frac{1}{q})^2}.$$

Si $q = 2$ entonces el factor de corrección es

$$\frac{1 - \frac{1}{2}}{(1 - \frac{1}{2})^2} = 2.$$

La heurística con factor de corrección

Entonces, definimos

$$C := 2 \prod_{\substack{q \text{ prime} \\ q \geq 3}} \frac{(1-2/q)}{(1-1/q)^2} \approx 1{,}3203236\ldots.$$

Esto sugiere que

$$\#\{p \leq x : p \text{ y } p+2 \text{ primo}\} \approx C \frac{x}{(\log x)^2}.$$

Cuando las heurísticas fallan

El argumento heurístico depende en gran medida de la suposición que los primos p están *distribuidos uniformemente* en las clases de residuos $\pmod{q}$.

Sea $\pi(x; q, a) := \#\{p \leq x : p \equiv a \pmod{q}\}$.

Si los primos **estuvieran** distribuidos uniformamente (mod q), esperaríamos que

$$\pi(x; q, a) \approx \frac{\pi(x)}{\varphi(q)},$$

cuando $\gcd(a, q) = 1$.

Equidistribución para q "pequeño"

Teorema (Bombieri-Vinogradov)

Para cualquier $A > 0$, existe $B = B(A)$ tal que

$$\sum_{q \le Q} \max_{\substack{a \pmod q \\ (a,q)=1}} \left| \pi(x;q,a) - \frac{\pi(x)}{\varphi(q)} \right| \ll_A \frac{x}{(\log x)^A},$$

donde $Q = \frac{x^{1/2}}{(\log x)^B}$.

Equidistribución para todo q?

Conjetura (Elliott-Halberstam)

El teorema Bombieri-Vinogradov es cierto aún si $Q = x^{\theta}$, para todo $\theta < 1$.

Decimos que θ es el *nivel de distribución* del conjunto de primos.

Trabajos recientes sobre espacios entre primos

k-tuplas admisibles

Definición

Decimos que una k-tupla $(h_1, ..., h_k)$ de enteros no negativos es admisible si no cubre todos los posibles restos (mod p) para ningun primo p.

Example: $(0, 2, 6, 8, 12)$ es una 5-tupla admisible.

Clases de residuos no cubiertas:
$1 \pmod 2$
$1 \pmod 3$
$4 \pmod 5$
$3 \pmod 7$
$3 \pmod{11}$

Espacios entre primos
Lola Thompson
Introducción
Trabajos recientes sobre espacios entre primos
El método de Maynard-Tao
Variantes del teorema de Maynard-Tao
Aplicaciones a secuencias de primos consecutivos

G P Y

Teorema (Goldston, Pintz and Yıldırım, 2009)

Si $(h_1, ..., h_k)$ es admisible y la conjectura de Elliot-Halberstam es cierta para $Q = x^{1/2+\eta}$, entonces hay un número infinito de n tal que al menos 2 de $n + h_1, ..., n + h_k$ son primos.

La "relajación" de Zhang

Teorema (Zhang, 2013)

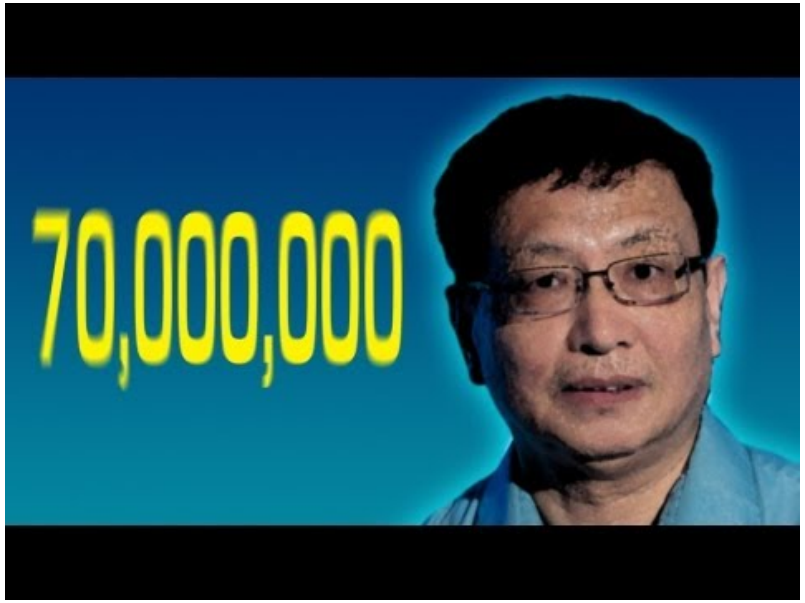
Existen $\eta, \delta > 0$ *tal que para cualquier dado* a,

$$\sum_{\substack{q \le Q \\ (q,a)=1}} \left| \pi(x;q,a) - \frac{x}{\varphi(q)\log x} \right| \ll_A \frac{x}{(\log x)^A},$$

q sin factores cuadrados & y -suave

donde $Q = x^{1/2+\eta}$ *y* $y = x^{\delta}$.

Espacios acotados entre primos (finalmente!)



Corollary (Zhang, 2013)

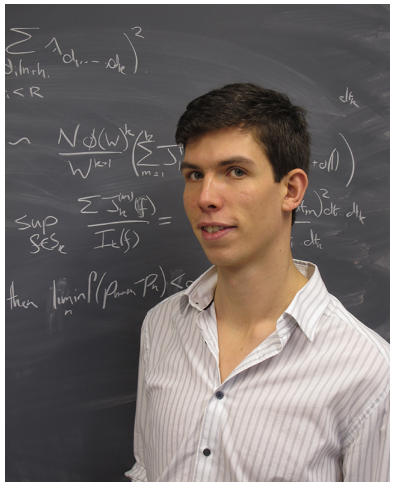
Hay un número infinito de pares de primos que difieren por lo más $70,000,000$.

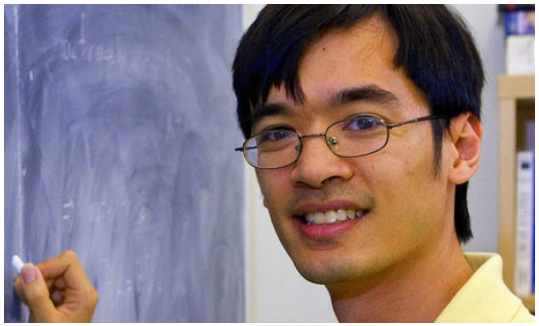
Una conjectura más fuerte: k-tuplas de primos

Conjetura (Hardy-Littlewood prime k-tuplas)

Sea $\mathcal{H} = (h_1, ..., h_k)$ admisible. Entonces hay un número infinito de enteros n tales que $n + h_1$,...,$n + h_k$ son todos primos.

El trabajo independiente de Maynard y Tao





Teorema (Maynard-Tao, November 2013)

Sea $m \geq 2$. Entonces para cualquier k-tupla admisible $\mathcal{H} = (h_1, ..., h_k)$ con k "suficientemente grande" (relativo a m), hay un número infinito de números n tales que al menos m de $n + h_1, ..., n + h_k$ son primos.

El estado actual de las cosas

Teorema (D. H. J. Polymath, 2014)

Hay un número infinito de pares de primos que están menos de 246 *aparte.*

El estado actual de las cosas

Teorema (D. H. J. Polymath, 2014)

Hay un número infinito de pares de primos que están menos de 246 *aparte.*

Asumiendo la conjectura "Elliot–Halberstam Generalizada," este número se puede reducir a 6!!!

El método de Maynard-Tao

Un bosquejo del método de Maynard-Tao

Meta: Encontrar valores de n para los cuales la tupla $n + h_1, ..., n + h_k$ contiene varios primos.

Pasos preparativos: Para N grande, buscamos n en el intervalo diádico $[N, 2N)$.

Sea $W := \prod_{p \leq \log_3 N} p$. Como $\mathcal{H}$ es admisible, podemos elegir un entero ν tal que $\gcd(\nu + h_i, W) = 1$ para todos los $1 \leq i \leq k$.

El truco W: Pre-cribar el conjunto, manteniendo solamente aquellos n tales que $n \equiv \nu \pmod{W}$.

Por lo tanto, nuestro espacio de muestra se hace

$$\Omega := \{N \leq n < 2N : n \equiv \nu \pmod{W}\}.$$

Un bosquejo del método de Maynard-Tao

Denote $w(n)$ pesos no negativos y denote $\chi_{\mathcal{P}}$ la función característica del conjunto $\mathcal{P}$ de primos. Consideremos

$$S_1 := \sum_{\substack{N \le n < 2N \\ n \equiv \nu \pmod{W}}} w(n)$$

$$S_2 := \sum_{\substack{N \le n < 2N \\ n \equiv \nu \pmod{W}}} \left(\sum_{i=1}^{k} \chi_{\mathcal{P}}(n + h_i) \right) w(n).$$

La fracción S_2/S_1 es el promedio ponderado del número de primos en $n + h_1, ..., n + h_k$ dentro de Ω.

Un bosquejo del método de Maynard-Tao

Idea clave: Si $S_2/S_1 > (m-1)$ para algún $m \in \mathbb{Z}^+$, entonces existe un $n \in \Omega$ tal que al menos m de $n+h_1, ..., n+h_k$ son primos.

Para que este método funcione, necesitamos seleccionar los pesos $w(n)$ de tal manera que:

1. S_2 y S_1 pueden estimarse usando las herramientas del análisis asintótico;

Un bosquejo del método de Maynard-Tao

Idea clave: Si $S_2/S_1 > (m-1)$ para algún $m \in \mathbb{Z}^+$, entonces existe un $n \in \Omega$ tal que al menos m de $n+h_1, ..., n+h_k$ son primos.

Para que este método funcione, necesitamos seleccionar los pesos $w(n)$ de tal manera que:

1. S_2 y S_1 pueden estimarse usando las herramientas del análisis asintótico;
2. S_2/S_1 es grande.

Variantes del teorema de Maynard-Tao

Maynard-Tao para cuerpos de números

Teorema (Castillo, Hall, Lemke Oliver, Pollack, T., 2014)

Sea $m \geq 2$. Dado un cuerpo de números K, hay un entero $k_0 := k_0(m, K)$ tal que para cualquier k-tupla admisible $(h_1, ..., h_k)$ en $\mathcal{O}_K$ con $k \geq k_0$, hay un número infinito de $\alpha \in \mathcal{O}_K$ tales que al menos m de $\alpha + h_1, ..., \alpha + h_k$ son primos.

Maynard-Tao por conjuntos Chebotarev

Un conjunto de primos $q_1, q_2, \ldots$ tiene la *propiedad de distancias acotadas* si $\liminf_{n\to\infty} q_{n+m} - q_n < \infty$ para cada m.

Teorema (Thorner, 2014)

Conjuntos Chebotarev tiene la propiedad de distancias acotadas.

Maynard-Tao por conjuntos Chebotarev

Ejemplos de conjuntos Chebotarev:

Maynard-Tao por conjuntos Chebotarev

Ejemplos de conjuntos Chebotarev:

- El conjunto de primos $p \equiv 1 \pmod 3$ tales que 2 es un cubo $\pmod p$.

Maynard-Tao por conjuntos Chebotarev

Ejemplos de conjuntos Chebotarev:

- El conjunto de primos $p \equiv 1 \pmod 3$ tales que 2 es un cubo $\pmod p$.
- Sea $n \in \mathbb{Z}^+$. El conjunto de primos que pueden expresarse en la forma $x^2 + ny^2$.

Maynard-Tao por conjuntos Chebotarev

Ejemplos de conjuntos Chebotarev:

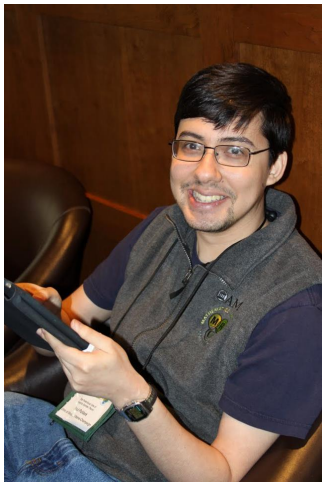
- El conjunto de primos $p \equiv 1 \pmod 3$ tales que 2 es un cubo $\pmod p$.
- Sea $n \in \mathbb{Z}^+$. El conjunto de primos que pueden expresarse en la forma $x^2 + ny^2$.
- Sea τ la función tau de Ramanujan. El conjunto de primos p tales que $\tau(p) \equiv 0 \pmod d$ para cualquier entero positivo d.

Maynard-Tao por conjuntos Chebotarev

Ejemplos de conjuntos Chebotarev:

- El conjunto de primos $p \equiv 1 \pmod 3$ tales que 2 es un cubo $\pmod p$.
- Sea $n \in \mathbb{Z}^+$. El conjunto de primos que pueden expresarse en la forma $x^2 + ny^2$.
- Sea τ la función tau de Ramanujan. El conjunto de primos p tales que $\tau(p) \equiv 0 \pmod d$ para cualquier entero positivo d.
- El conjunto de primos p tales que $\#E(\mathbb{F}_p) \equiv p + 1 \pmod d$ para cada entero positivo d.

Polinomios gemelos primos: Dos disertaciónes



Teorema (Hall, Ph.D. 2006; Pollack, Ph.D. 2008)

Si $q \geq 3$, algún $a \in \mathbb{F}_q$ (excluyendo $a = 0$) ocurre con frequencia infinitamente como una distancia entre polinomios irreducibles.

($q > 3$ debido a Hall; $q = 3$ debido a Pollack)

Una mejora del trabajo de Hall y Pollack

Teorema (Castillo, Hall, Lemke Oliver, Pollack, T., 2014)

Sea $m \geq 2$. Hay un entero $k_0 := k_0(m)$ tal que para cada k-tupla admisible $(h_1, ..., h_k)$ de polinomios en $\mathbb{F}_q[x]$ con $k \geq k_0$, hay un número infinito de polinomios $f \in \mathbb{F}_q[x]$ tales que al menos m de $f + h_1, ..., f + h_k$ son irreducibles.

Aplicaciones a secuencias de primos consecutivos

Primos consecutivos en progresiones aritméticas

Teorema (Shiu, 2000)

Cada conjunto de residuos $a \pmod{q}$ *con* $\gcd(a, q) = 1$ *contiene secuencias arbitrariamente largas de primos consecutivos.*

Un cambio de paradigma

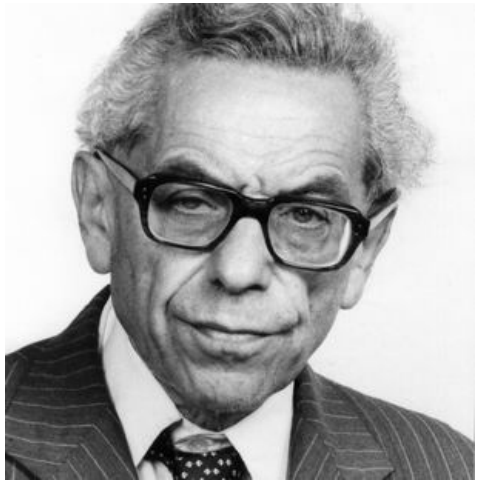
En un papel en 2013, Banks, Freiberg y Turnage-Butterbaugh utilizaron el método de Maynard-Tao para obtener una segunda prueba sorprendentemente simple del teorema de Shiu.

Un cambio de paradigma

En un papel en 2013, Banks, Freiberg y Turnage-Butterbaugh utilizaron el método de Maynard-Tao para obtener una segunda prueba sorprendentemente simple del teorema de Shiu.

Esto plantea la pregunta: ¿puede el método de Maynard-Tao ser usado para tratar otros problemas de primos consecutivos?

Una conjectura de Erdős y Turan



Para cada k, sea $d_k = p_{k+1} - p_k$.

Conjetura (Erdős, Turan 1948)

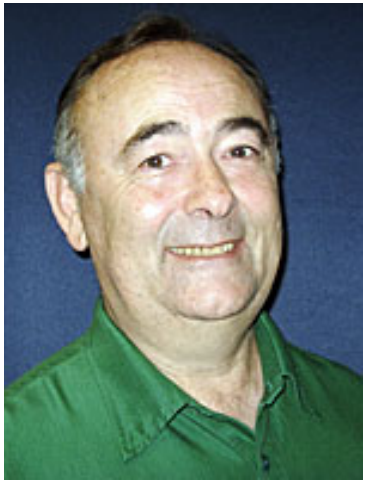
La secuencia $\{d_k\}$ contiene secuencias crecientes y decrecientes arbitrariamente largas.

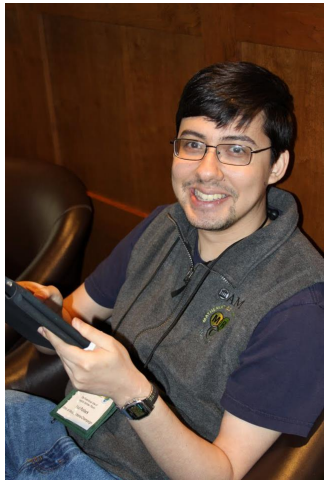
Secuencias de espacios entre primos

Teorema (Banks, Freiberg, Turnage-Butterbaugh, 2013)

La sequencia $\{d_k\}$ contiene secuencias crecientes y decrecientes arbitrariamente largas.

Primos consecutivos con $E(\mathbb{F}_p)$ cíclico





Teorema (Baker y Pollack, 2016)

Suponiendo GRH, fijemos una curva elíptica $E/\mathbb{Q}$. Hay secuencias arbitrariamente largas de primos consecutivos p tales que $E(\mathbb{F}_p)$ es cíclico.

Funciones aritméticas en primos desplazados consecutivos

Teorema (Pollack, T., 2015)

Sea $f = \varphi, \sigma, \omega, \Omega, \tau$. Hay secuencias arbitrariamente largas de primos consecutivos p tales que $f(p-1)$ es decreciente. Lo mismo vale para $f(p-1)$ creciente.

Un bosquejo para $\varphi(p-1)$ decreciente

La misma configuración básica como en Maynard-Tao:

Disposición: Para N grande, sea $W := \prod_{p \leq \log_3 N} p$. Definimos

$$S_1 := \sum_{\substack{N \leq n < 2N \\ n \equiv \nu \pmod{W}}} w(n)$$

,

$$S_2 := \sum_{\substack{N \leq n < 2N \\ n \equiv \nu \pmod{W}}} \left(\sum_{i=1}^{k} \chi_{\mathcal{P}}(n+h_i) \right) w(n).$$

Queremos $\frac{S_2}{S_1} > m-1$ para que por lo menos m de $n+h_1, ..., n+h_k$ sean primos para $n \in \Omega$.

Un bosquejo para $\varphi(p-1)$ decreciente

Innovación clave: **Modificamos el truco W.**

Fijamos $\mathcal{H} = \{h_1, ..., h_k\}$ donde $h_i = (i-1)(2k)!$. Con esta $\mathcal{H}$, queremos elegir $\nu \pmod{W}$ tal que:

1. (Primos consecutivos) Para $n \in \Omega$, cualquier primo en $[n + h_1, n + h_k]$ está en $n + \mathcal{H}$.
2. (Valores φ decrecientes) Con probabilidad $1 + o(1)$,

$$\frac{n + h_i - 1}{\varphi(n + h_i - 1)} \in (2^{4i}, 2^{4i+3}]$$

por $1 \leq i \leq k$.

Variaciones

Teorema (Pollack, T., 2015)

Sea $f = \varphi, \sigma, \omega, \Omega, \tau$. Hay secuencias arbitrariamente largas de primos consecutivos p tal que $f(p-1)$ es decreciente. Lo mismo vale para $f(p-1)$ creciente.

Variación	Modificación
Creciente φ's	Reemplazamos $\mathcal{H}$ por $-\mathcal{H}$
Creciente σ's	Reemplazamos $\frac{n+h_i-1}{\varphi(n+h_i-1)}$ por $\frac{\sigma(n+h_i-1)}{n+h_i-1}$.
Decreciente σ's	Como creciente σ's; reemplazamos $\mathcal{H}$ por $-\mathcal{H}$.

**Necesitamos modificaciones adicionales para manejar ω, Ω, τ.

Sumando dígitos de primos consecutivos

Definición

Sea $s_g(n)$ denota la suma de los base-g dígitos de n.

Ejemplo: $s_{10}(523) = 5 + 2 + 3 = 10$

$$s_{10}(541) = 5 + 4 + 1 = 10$$

Pregunta (Sierpinski, 1961): Hay secuencias arbitrariamente largas de primos consecutivos p en las que $s_g(p)$ es constante? creciente? decreciente?

Sumando dígitos de primos consecutivos

Espacios entre primos

Lola Thompson

Introducción

Trabajos recientes sobre espacios entre primos

El método de Maynard-Tao

Variantes del teorema de Maynard-Tao

Aplicaciones a secuencias de primos consecutivos

Una breve historia:

Sumando dígitos de primos consecutivos

Una breve historia:

- Sierpinski (1961): $s_{10}(p_n) < s_{10}(p_{n+1})$ infinitamente a menudo.

Sumando dígitos de primos consecutivos

Una breve historia:

- Sierpinski (1961): $s_{10}(p_n) < s_{10}(p_{n+1})$ infinitamente a menudo.
- Erdős (1962): $s_{10}(p_n) > s_{10}(p_{n+1})$ infinitamente a menudo.

Sumando dígitos de primos consecutivos

Una breve historia:

- Sierpinski (1961): $s_{10}(p_n) < s_{10}(p_{n+1})$ infinitamente a menudo.
- Erdős (1962): $s_{10}(p_n) > s_{10}(p_{n+1})$ infinitamente a menudo.
- Sierpinski (1968): **Asumiendo la conjectura de k-tuplas de primos de Dickson**, $s_{10}(p_n) > s_{10}(p_{n+1}) > s_{10}(p_{n+2})$ infinitamente a menudo.

Sumando dígitos de primos consecutivos

Una breve historia:

- Sierpinski (1961): $s_{10}(p_n) < s_{10}(p_{n+1})$ infinitamente a menudo.
- Erdős (1962): $s_{10}(p_n) > s_{10}(p_{n+1})$ infinitamente a menudo.
- Sierpinski (1968): **Asumiendo la conjectura de k-tuplas de primos de Dickson**, $s_{10}(p_n) > s_{10}(p_{n+1}) > s_{10}(p_{n+2})$ infinitamente a menudo.
- Schinzel (aseveración no publicada): **Asumiendo Hipótesis H**, hay secuencias arbitrariamente largas de primos p en las que $s_{10}(p)$ es creciente (decreciente).

Sumando dígitos de primos consecutivos

Teorema (Pollack, T., 2015)

Para cualquier base g, hay secuencias arbitrariamente largas de primos p en las que $s_g(p)$ es constante/creciente/decreciente.

¡Gracias!