

Caminatas aleatorias y números primos

Carlos G. Pacheco

Departamento de Matemáticas, CINVESTAV

Modelo de probabilidad finito

Piense en N monedas justas: $\omega = \{\omega_1, \dots, \omega_N\}$ cada $\omega_i \in \{0, 1\}$.

$$Prob(\omega_1 = 1, \omega_2 = 0, \dots, \omega_N = 1) = \left(\frac{1}{2}\right)^N$$

$$Prob(k \text{ son } 0 \text{ y } N - k \text{ son } 1) = \binom{N}{k} \left(\frac{1}{2}\right)^k \left(\frac{1}{2}\right)^{N-k} = \frac{\binom{N}{k}}{2^N}$$

Si $N = \infty$, podemos codificar (encapsular, caracterizar) la sucesión de 0, 1's usando la siguiente variable:

$$X(\omega) = \sum_{i=1}^{\infty} \frac{\omega_i}{2^i} \in [0, 1]$$

Nota. un ω representa dos cosas, una sucesión de 0's y 1's o un número en $[0, 1]$

Podemos preguntar lo siguiente:

¿ $Prob(X \in (a, b))$? con $(a, b) \subset [0, 1]$

Respuesta: $Prob(X \in (a, b)) = b - a$

En general queremos $Prob(X \in A)$ con $A \subset [0, 1]$

¿Qué tan arbitrario puede ser A ?

La **teoría de la medida** responde precisamente esta pregunta, y por eso en 1933 **Andrei N. Kolmogorov** propuso usarla para fundar las bases de la probabilidad.

**FOUNDATIONS
OF THE
THEORY OF PROBABILITY**

**BY
A. N. KOLMOGOROV**

TRANSLATION EDITED BY
NATHAN MORRISON

Modelo de probabilidad general

Modelo correcto para X es la estructura $(\Omega, \mathcal{F}, P)$, donde

i) $\Omega = [0, 1]$

ii) $\mathcal{F}$ es una σ -álgebra de conjuntos de Ω

iii) P es la medida de Lebesgue

Def. Una σ -álgebra $\mathcal{F}$ es la clase de conjuntos de Ω tales que

a) $\Omega \in \mathcal{F}$,

b) si $A \in \mathcal{F}$, entonces $A^c \in \mathcal{F}$,

c) si $A_1, A_2, \dots \in \mathcal{F}$, entonces $\bigcup_{i=1}^{\infty} A_i \in \mathcal{F}$

Def. Una **medida de probabilidad** P sobre $\mathcal{F}$ es tal que

1) $P(A) \geq 0$,

2) $P(\Omega) = 1$,

3) si $A_1, A_2, \dots \in \mathcal{F}$ son disjuntos, entonces

$$P\left(\bigcup_{i=1}^{\infty} A_i\right) = \sum_{i=1}^{\infty} P(A_i)$$

Conclusión: $Prob(X \in A) = P(A) = P(\{\omega : X(\omega) \in A\})$,
para $A \in \mathcal{F}$

Modelo de probabilidad: propiedades

Proposición: Sean $A_1 \subset A_2 \subset \dots \in \mathcal{F}$, entonces

$$P\left(\bigcup_{i=1}^{\infty} A_i\right) = \lim_{n \rightarrow \infty} P(A_n)$$

Dem. Sean $B_1 = A_1$, $B_2 = A_2 - B_1$, $B_3 = A_3 - B_2, \dots$, luego $\bigcup_{i=1}^{\infty} B_i = \bigcup_{i=1}^{\infty} A_i$.

Por las propiedad de la σ -álgebra, los B_i 's pertenecen a $\mathcal{F}$, y como son disjuntos, por la propiedad 3),

$$\begin{aligned} P\left(\bigcup_{i=1}^{\infty} A_i\right) &= P\left(\bigcup_{i=1}^{\infty} B_i\right) \\ &= \sum_{i=1}^{\infty} P(B_i) = \lim_{n \rightarrow \infty} \sum_{i=1}^n P(B_i) = \lim_{n \rightarrow \infty} P(A_n). \end{aligned}$$

Similarmente: Si $A_{n+1} \subset A_n$, entonces

$$P\left(\bigcap_{i=1}^{\infty} A_i\right) = \lim_{n \rightarrow \infty} P(A_n)$$

Def: Sean $A_1, A_2, \dots \in \mathcal{F}$.

$$\limsup_n A_n := \bigcap_{n=1}^{\infty} \bigcup_{k=n}^{\infty} A_k$$

Nota: $\omega \in \limsup_n A_n$ significa que ω está en una infinidad de A_n s

Lema de Borel-Cantelli:

- i) Si $\sum_{n=1}^{\infty} P(A_n) < \infty$, entonces $P(\limsup A_n) = 0$.
- ii) Si $\sum_{n=1}^{\infty} P(A_n) = \infty$ y los eventos A_n son *independientes* (i.e. $P(A_n \cap A_m) = P(A_n)P(A_m)$), entonces $P(\limsup A_n) = 1$.

Dem: i) Usando la Proposición,

$$P\left(\bigcap_{n=1}^{\infty} \bigcup_{k=n}^{\infty} A_k\right) = \lim_{n \rightarrow \infty} P\left(\bigcup_{k=n}^{\infty} A_k\right) \leq \lim_{n \rightarrow \infty} \sum_{k=n}^{\infty} P(A_k) = 0.$$

ii) Por demostrar, que $P((\limsup A_n)^c) = 0$. Vemos que

$$(\limsup A_n)^c = \bigcup_{n=1}^{\infty} \bigcap_{k=n}^{\infty} A_k^c.$$

Así, usando que los complementos A_k^c son también eventos independientes (ejercicio!), y otra vez la Proposición,

$$\begin{aligned} P((\limsup A_n)^c) &= \lim_{n \rightarrow \infty} P\left(\bigcap_{k=n}^{\infty} A_k^c\right) = \lim_{n \rightarrow \infty} \lim_{m \rightarrow \infty} P\left(\bigcap_{k=n}^m A_k^c\right) \\ &= \lim_{n \rightarrow \infty} \lim_{m \rightarrow \infty} \prod_{k=n}^m (1 - P(A_k)) \leq \lim_{n \rightarrow \infty} \prod_{k=n}^{\infty} e^{-P(A_k)} \\ &= \lim_{n \rightarrow \infty} e^{-\sum_{k=n}^{\infty} P(A_k)} = 0, \end{aligned}$$

donde hemos usado que $e^{-x} \geq 1 - x$ para $x \geq 0$.

Modelo de probabilidad: objetos

Def. Una **variable aleatoria** es una función $X : \Omega \rightarrow \mathbb{R}$, $E[X]$ es su **esperanza** y su **función de distribución** es $F(x) = P(\{\omega : X(\omega) < x\}) = \text{Prob}(X < x)$.

Ejemplos 1.

$$Y(\omega) := I_{[0,1/2]}(\omega) = \begin{cases} 1 & \omega \in [0, 1/2] \\ 0 & \omega \notin [0, 1/2] \end{cases}$$

Así, $\text{Prob}(Y = 1) = 1/2$ y $\text{Prob}(Y = 0) = 1/2$.

Usaremos $X = 2Y - 1 \in \{1, -1\}$

Ejemplos 2. Si $X \sim \exp(\lambda)$, $F(x) = 1 - e^{-\lambda}$.

En este caso

$$X(\omega) = -\frac{\log(1 - \omega)}{\lambda}$$

Def. Dos variables X y Y son **independientes** si $\text{Prob}(X \in A \text{ y } Y \in B) = \text{Prob}(X \in A)\text{Prob}(Y \in B)$

- X y Y independientes $\Rightarrow$, $E[XY] = E[X]E[Y]$
- Desigualdad de Markov: $X > 0$, $P(X > a) \leq E[X]/a$
- Desigualdad de Chebyshev: $P(|X| > a) \leq E[X^2]/a^2$
- $S_n = X_1 + \dots + X_n \Rightarrow E[S_n^{2k}] = O(n^k)$
Ejemplos. $E[S_n^2] = n$, $E[S_n^4] = 3n^2 - 2n$.
- $E[e^{tS_n}] = \left(\frac{e^t + e^{-t}}{2}\right)^n$
- $E[e^{S_n/\sqrt{n}}] \rightarrow e^{1/2}$

Aplicación de Borel-Cantelli.

Sean $X_1, X_2, \dots$ v.v.aa i.i.d. $\sim \text{Exp}(1)$. Entonces, para casi todo ω ,

$$\limsup_{n \rightarrow \infty} \sup_{k \geq n} \frac{X_k(\omega)}{\log k} = 1$$

Dem. Sea $\epsilon > 0$ arbitrario y $A_n(\epsilon) := \left\{ \omega : \frac{X_n(\omega)}{\log n} \geq 1 + \epsilon \right\}$.

Estudiamos $P(\limsup A_n(\epsilon))$, lo cual representa la probabilidad de que para un cantidad infinita de índices n se cumple la desigualdad

$$\frac{X_n(\omega)}{\log n} \geq 1 + \epsilon.$$

Paso 1. Primero vemos que

$$P(A_n(\epsilon)) = P(X_n \geq (1 + \epsilon) \log n) = e^{-(1+\epsilon) \log n} = \frac{1}{n^{1+\epsilon}}.$$

De aquí se sigue que $\sum_{n=1}^{\infty} P(A_n(\epsilon)) < \infty$. Luego, por el Lemma de BC, $P(\limsup A_n(\epsilon)) = 0$, y también $P(\limsup A_n)^c = 1$.

Aplicación de Borel-Cantelli.

Entonces

$$P\left(\bigcup_{n=1}^{\infty} \bigcap_{k=n}^{\infty} \left\{ \frac{X_k(\omega)}{\log k} < 1 + \epsilon \right\}\right) = 1.$$

Así, para casi todo ω , existe $N(\omega)$ tal que para todo $n > N(\omega)$, $\frac{X_n(\omega)}{\log n} < 1 + \epsilon$. Esto implica que $\limsup \frac{X_n(\omega)}{\log n} < 1 + \epsilon$. Tomando $\epsilon \rightarrow 0$, concluimos que

$$\limsup \frac{X_n(\omega)}{\log n} \leq 1$$

Paso 2. Ahora definimos $B_n(\epsilon) = \left\{ \omega : \frac{X_n(\omega)}{\log n} \geq 1 - \epsilon \right\}$ y $q = P(\limsup B_n(\epsilon))$. Luego, como anteriormente, $P(B_n(\epsilon)) = \frac{1}{n^{1-\epsilon}}$, lo cual implica $\sum_{n=1}^{\infty} P(B_n) = \infty$. Finalmente, de la independencia de las vv.aa. resulta que los eventos $B_n(\epsilon)$ son independientes. Luego por el Lema de BC $q = 1$. Así, para casi cualquier ω , hay $N_\epsilon(\omega)$, tal que $n > N_\epsilon(\omega) \Rightarrow \frac{X_n(\omega)}{\log n} \geq 1 - \epsilon$.

Luego, $\limsup \frac{X_n(\omega)}{\log n} \geq 1 - \epsilon$. Tomando $\epsilon \rightarrow 0$, $\limsup \frac{X_n(\omega)}{\log n} \geq 1$

Teorema de Borel (1909)

Considere las v.a.s i.i.d. (Bernoulli)

$$X_n = \begin{cases} +1 & 1/2 \\ -1 & 1/2 \end{cases},$$

y defina la **caminata aleatoria** $S_n = X_1 + \dots + X_n$. Entonces, para casi todas las ω 's,

$$\lim_{n \rightarrow \infty} \frac{S_n(\omega)}{n} = 0.$$

Nota. Versión de la ley fuerte de los grande números.

Dem. $E \left[\frac{S_n}{n} \right] = 0$ y $E \left[\left(\frac{S_n}{n} \right)^2 \right] = \frac{1}{n}$. Por la desigualdad de Chebyshev, para $\epsilon > 0$

$$P \left(\left| \frac{S_n}{n} \right| \geq \epsilon \right) \leq \frac{E \left[\left(\frac{S_n}{n} \right)^2 \right]}{\epsilon^2} = \frac{1}{\epsilon^2 n}.$$

Demostración

Si $A_n = \left\{ \omega : \left| \frac{S_{n^2}(\omega)}{n^2} \right| \geq \epsilon \right\}$, entonces $\sum_{n=1}^{\infty} P(A_n) < \infty$. Así

$$0 = P(\limsup A_n) = P \left(\begin{array}{c} \text{Para una infinidad de } k \\ \left| \frac{S_{k^2}}{k^2} \right| \geq \epsilon \end{array} \right).$$

Entonces

$$1 = P((\limsup A_n)^c) = P \left(\begin{array}{c} \text{A partir de un } N, \\ \left| \frac{S_{k^2}}{k^2} \right| < \epsilon, \text{ cuando } k \geq N \end{array} \right).$$

Y como ϵ es arbitrario, $\lim_{n \rightarrow \infty} \frac{S_{n^2}}{n^2} = 0$

Finalmente, para k arbitrario hay n tal que $n^2 \leq k < (n+1)^2$, y

$$\left| \frac{S_k}{k} \right| = \left| \frac{S_{n^2}}{n^2} \frac{n^2}{k} + \frac{S_k - S_{n^2}}{k} \right| \leq \left| \frac{S_{n^2}}{n^2} \right| + \frac{(n+1)^2 - n^2}{k}.$$

De donde surge lo deseado.

Teorema de Hausdorff (1913)

Sea $\epsilon > 0$. Para casi todo ω , $\lim_{n \rightarrow \infty} \frac{S_n(\omega)}{n^{1/2+\epsilon}} = 0$.

Nota. El TLC dice que la distribución de $\lim_{n \rightarrow \infty} \frac{S_n}{n^{1/2}}$ es $N(0,1)$.

Dem. Para k entero $E[S_n^{2k}] = O(n^k)$, i.e. $\sup_n \frac{O(n^k)}{n^k} < \infty$.

$\delta > 0$. Con la desigualdad de Markov, y k grande para que $k\epsilon > 1$,

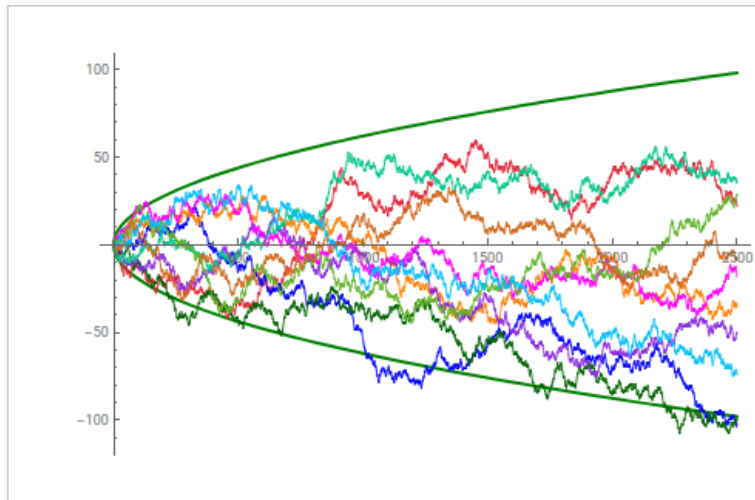
$$\begin{aligned} P(|S_n| \geq \delta n^{1/2+\epsilon}) &= P(S_n^{2k} \geq \delta^{2k} n^{k+2k\epsilon}) \\ &\leq \frac{E[S_n^{2k}]}{\delta^{2k} n^k n^{2k\epsilon}} \leq \frac{E[S_n^{2k}]}{\delta^{2k} n^k} \frac{1}{n^{2k\epsilon}}. \end{aligned}$$

Así, $\sum_{n=1}^{\infty} P(A_n) < \infty$. Por el Lema BC $P((\limsup A_n)^c) = 1$. i.e.

$$P\left(\bigcup_{n=1}^{\infty} \bigcap_{k=n}^{\infty} \left\{ \frac{S_n}{n^{1/2+\epsilon}} < \delta \right\}\right) = 1.$$

Esto es: para casi toda ω , hay $N_\delta(\omega)$ tal que, si $n > N_\delta(\omega)$, entonces $\frac{S_n(\omega)}{n^{1/2+\epsilon}} < \delta$.

Simulaciones



Para casi todo ω , $\lim_{n \rightarrow \infty} \sup_{k \geq n} \frac{|S_n(\omega)|}{\sqrt{k} \log k} \leq 1$.

Dem. Sea $\epsilon > 0$ arbitrario. $P(S_n \geq (1 + \epsilon)\sqrt{n} \log n) =$

$$P\left(e^{\frac{S_n}{\sqrt{n}}} \geq e^{(1+\epsilon) \log n} = n^{1+\epsilon}\right) \leq \frac{E\left[e^{\frac{S_n}{\sqrt{n}}}\right]}{n^{1+\epsilon}}.$$

Por el Lema BC

$$P\left(\bigcup_{n=1}^{\infty} \bigcap_{k=n}^{\infty} \left\{ \frac{S_n}{\sqrt{n} \log n} < 1 + \epsilon \right\}\right) = 1.$$

Esto es: para casi toda ω , hay $N_{\epsilon}(\omega)$ tal que, si $n > N_{\epsilon}(\omega)$, entonces $\frac{S_n(\omega)}{\sqrt{n} \log n} < 1 + \epsilon$. Usando $\tilde{S}_n := -S_n$ podemos concluir.

Ley del logaritmo iterado, Khinchine (1923)

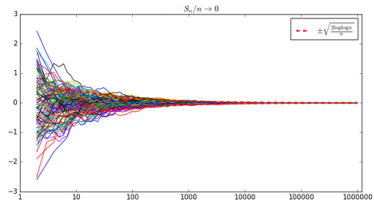
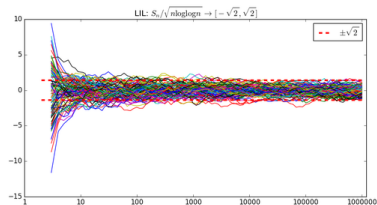
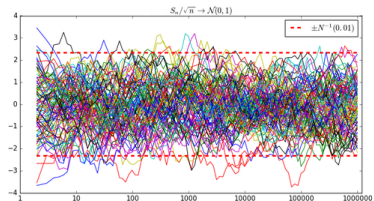
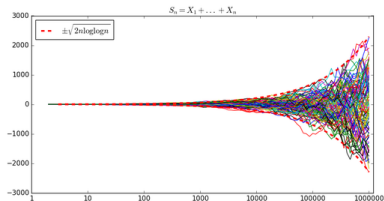
Para casi todo ω ,

$$\lim_{n \rightarrow \infty} \sup_{k \geq n} \frac{|S_k(\omega)|}{b_k} = 1,$$

donde

$$b_n = \sqrt{2n \log \log n}.$$

Simulaciones



Simulaciones



cantidad de primos antes de x

$\pi(x)$ = cantidad de primos antes de x

$\pi(4) = 2$, $\pi(7.5) = 4, \dots$

Gauss conjeturó en 1793 que $\pi(x)$ se puede aproximar con la función

$$li(x) = \int_2^x \frac{1}{\log t} dt$$

Teorema de los números primos.

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{li(x)} = 1$$

Los demostraron Hadamard y de la Vallée-Poussin en 1896.

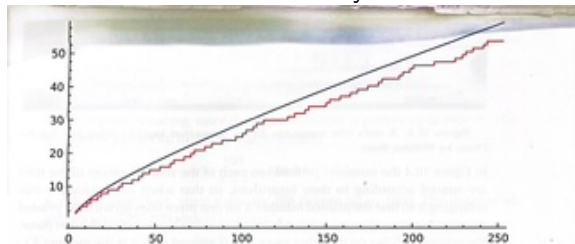


Figure 10.2 Plot of $\pi(x)$ and Gauss's smooth curve $li(x)$

error entre $li(x)$ y $\pi(x)$

Error: $E(x) = \pi(x) - li(x)$

Observe:

$$\begin{aligned}\pi(x) &= (\pi(x) - \pi(x-1)) + (\pi(x-1) - \pi(x-2)) + \dots \\ &\quad + (\pi(3) - \pi(2)) + (\pi(2) - \pi(1)) \\ &= (\pi(2) - \pi(1)) + (\pi(3) - \pi(2)) + \dots + (\pi(x) - \pi(x-1))\end{aligned}$$

$$\begin{aligned}li(x) &= \int_2^x \frac{1}{\log t} dt \\ &= \int_2^3 \frac{1}{\log t} dt + \int_3^4 \frac{1}{\log t} dt + \dots + \int_{x-1}^x \frac{1}{\log t} dt \\ &\approx \frac{1}{\log(3)} + \frac{1}{\log(4)} + \dots + \frac{1}{\log(x)}\end{aligned}$$

error entre $li(x)$ y $\pi(x)$: parte II

Definimos los "brincos"

$$B(x) = \begin{cases} 1 - \frac{1}{\log(x)} & x \text{ es primo} \\ \frac{1}{\log(x)} & x \text{ no es primo} \end{cases}$$

Entonces, estamos diciendo que

$$E(x) = \pi(x) - li(x) \approx B(2) + B(3) + \dots + B(x)$$

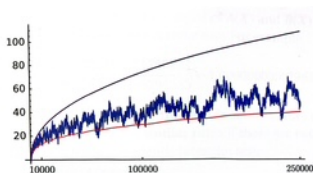


Figure 16.1. $Li(X) - \pi(X)$ (blue middle), its Cesàro smoothing (red bottom), and $\sqrt{\frac{2}{x}} \cdot \sqrt{X/\log(X)}$ (top), all for $X \leq 250,000$

- ¿tiene esto un comportamiento como una caminata aleatoria?

Resultado de de la Vallée Poussin (1899):

$$E(x) = \pi(x) - li(x) = O\left(xe^{-a\sqrt{\log x}}\right)$$

Conjetura de Helge von Koch (1901):

$$E(x) = \pi(x) - li(x) = O(\sqrt{x} \log(x))$$

Resultado de J.E. Littlewood (1914):

$$E(x) = \Omega\left(\sqrt{x} \frac{\log \log \log(x)}{\log(x)}\right) = \Omega(f(x))$$

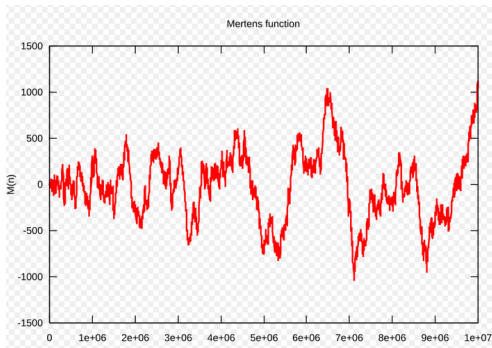
Esto es, hay constantes c_1, c_2 positivas tales que
 $\liminf_x E(x) < -f(x)c_1$ y $\limsup_x E(x) > c_2 f(x)$.

Primer valor donde cambia: $x \sim 10^{316}$

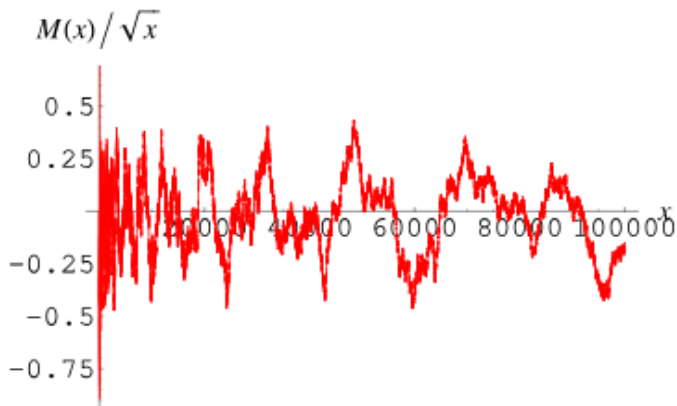
Conjetura de Mertens

$$\text{Función de Möbius } \mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^k & n = p_1 \dots p_k \\ 0 & \text{e.o.c.} \end{cases}$$

$$|M(x)| = \sum_{k=1}^x \mu(k) \leq x^{1/2+\epsilon}, \text{ para } \epsilon > 0?$$

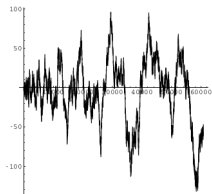


Conjetura de Mertens



- $\limsup_x \frac{1}{\sqrt{2x \log \log x}} \left| \sum_{k=1}^x \mu(l_k) \right| \leq 1?$

l_k índices cuando $\mu(k) \neq 0$, i.e. $\mu(k) = 1$ ó -1 .



- $\limsup_x \frac{1}{\sqrt{x}(\log \log \log x)^{5/4}} \left| \sum_{k=1}^x \mu(k) \right| \leq 1?$

Teorema de la función de Möbius

Para $x \geq 10$

$$\left| \sum_{k \leq x} \mu(k) \right| \leq 70x \log(x) e^{-\left(\frac{\log x}{6}\right)^{1/10}}$$

La demostración usa teoría de números (funciones multiplicativas).

- Random walk in random and non-random environment, P.Révész.
- Prime numbers and the Riemann Hypothesis, B.Mazur and W.Stein
- **Wikipedia:**
https://en.wikipedia.org/wiki/Prime_number_theorem
- **Conjetura de Mertens:**
https://en.wikipedia.org/wiki/Mertens_conjecture
- **Grokipedia:**
https://grokipedia.com/page/Prime-counting_function#ref-20
- Excursions in Multiplicative Number Theory, O.Ramaré.