Estimativas sobre Primos

Alan Reyes-Figueroa

Teoría de Números (Aula 31) 16.noviembre.2021

Estimativas sobre Primos

Complementamos es estudio asintótico de las funciones aritméticas con algunas estimativas sobre el comportamiento de los números primos.

Comenzamos con el siguiente resultado.

Lema

Sea $n \in \mathbb{N}$ un número natural, y sea p primo. Sea θ_p el entero tal que $p^{\theta_p} \leq 2n < p^{\theta_p+1}$. Entonces, el exponente de la mayor potencia de p que divide $\binom{2n}{n}$ es menor o igual a θ_p. En particular, si $p > \sqrt{2n}$, entonces el exponente de esta máxima potencia de p es menor o igual a 1. Además, si $\frac{2}{3}n < p < n$, entonces p no divide a $\frac{2n}{n}$.

<u>Prueba</u>: Sean α y β los exponentes de las mayores potencias de p que dividen $(2n)!$ y $n!$, respectivamente.

Sabemos que

$$\alpha = \left\lfloor \frac{2n}{p} \right\rfloor + \left\lfloor \frac{2n}{p^2} \right\rfloor + \left\lfloor \frac{2n}{p^3} \right\rfloor + \ldots, \qquad \beta = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots$$

Portanto, el exponente de la mayor potencia de p que divide a $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ es

$$\alpha - 2\beta = \sum_{i=1}^{\theta_p} \left(\left\lfloor \frac{2n}{p^i} \right\rfloor - \left\lfloor \frac{n}{p^i} \right\rfloor \right).$$

Pero, como

$$\frac{2n}{p^i} \geq \left\lfloor \frac{2n}{p^i} \right\rfloor > \frac{2n}{p^i} - 1, \text{ y} \qquad -2\left(\frac{n}{p^i} - 1\right) > -2\left\lfloor \frac{n}{p^i} \right\rfloor \geq -2\frac{n}{p^i},$$

sumando obtenemos que

$$2 > \left\lfloor \frac{2n}{p^i} \right\rfloor - \left\lfloor \frac{n}{p^i} \right\rfloor \geq -1.$$

Así, esta última expresión sólo puede tomar los valores 0 ó 1. Concluímos que

$$\alpha - 2\beta \leq \sum_{i=1}^{\theta_p} 1 = \theta_p.$$

Además, si $\frac{2}{3}n < p < n$, entonces $\alpha = 2$ y $\beta = 1 \implies \alpha - 2\beta = 0$. $\square$

Teorema de Chebyshev

Introducimos la función aritmética $\pi : \mathbb{R}^+ \to \mathbb{N}$ dada por

$$\pi(x) = \#\{p : p \text{ es primo y } p \leq x\} = \text{número de primos } \leq x.$$

Teorema (Chebyshev)

Existen constante positivas $0 < c < C$ *tales que*

$$c\,\frac{x}{\log x} < \pi(x) < C\,\frac{x}{\log x}.$$

<u>Prueba</u>: Observemos inicialmente que $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ es múltiplo de todos los primos p que satisfacen $n < p \leq 2n$.

Como

$$\binom{2n}{n} < \sum_{0 \leq k \leq 2n} \binom{2n}{k} = 2^{2n},$$

entonces se sigue que el producto de dos primos entre n y $2n$ es menor que 2^{2n}.

Teorema de Chebyshev

Como hay exactamente $\pi(2n) - \pi(n)$ primos entre n y $2n$, entonces tenemos que $n^{\pi(2n)-\pi(n)} < 2^{2n}$ (pues todos esos primos son mayores que n).

Aplicando logaritmos, se deduce que

$$\big(\pi(2n) - \pi(n)\big) \log n < 2n \log 2 \qquad \Longrightarrow \qquad \pi(2n) - \pi(n) < \frac{2n \log 2}{\log n}.$$

Usando un argumento por inducción, para mostrar que

$$\pi(2^{k+1}) < \frac{5 \cdot 2^k}{k}.$$

- Para $k \leq 4$ esto se verifica fácil, o se deduce de que $\pi(2^k) \leq 2^{k-1}$, para $k \geq 0$.
- Para $k \geq 5$, se tiene el paso inductivo

$$\pi(2^{k+2}) \leq \pi(2^{k+1}) + \frac{2^{k+1} \log 2}{\log 2^{k+1}} \leq \frac{5 \cdot 2^k}{k} + \frac{2^{k+1}}{k+1} \leq \frac{8 \cdot 2^k}{k+1} + \frac{2^{k+1}}{k+1} = \frac{5 \cdot 2^{k+1}}{k+1},$$

Teorema de Chebyshev

pues $\frac{5}{k} \leq \frac{8}{k+1}$, para todo entero positivo $k \geq 2$.

De lo anterior, se sigue que si $2^k < x \leq 2^{k+1}$, entonces

$$\pi(x) \leq \frac{5 \cdot 2^k}{k} < \frac{5 \cdot x}{k+1} < \frac{5x \log 2}{\log x} = C\,\frac{x}{\log x}, \qquad \text{con } C = 5 \log 2.$$

(pues $f(x) = \frac{x \log 2}{\log x}$ es una función creciente para $x \geq 3$).

Mostramos ahora la otra desigualdad. Sea $\binom{2n}{n} = \prod_{p<2n} p^{\alpha_p}$ la factoración en primos de $\binom{2n}{n}$. Por el lema anterior, tenemos que $p^{\alpha_p} \leq 2n \iff \alpha_p \log p \leq \log 2n$. Portanto

$$\log \binom{2n}{n} = \sum_{p<2n} \alpha_p \log p \leq \sum_{p<2n} \log 2n = \pi(2n) \log 2n.$$

Luego, $\pi(2n) \geq \dfrac{\log \binom{2n}{n}}{\log 2n}$

y como

$$\binom{2n}{n} = \underbrace{\frac{2n}{n}}_{\geq 2} \cdot \underbrace{\frac{2n-1}{n-1}}_{\geq 2} \cdots \underbrace{\frac{n+1}{1}}_{\geq 2} \geq 2^n.$$

Entonces, $\pi(2n) \geq \dfrac{\log \binom{2n}{n}}{\log 2n} \geq \dfrac{n \log 2}{\log 2n}$.

De ahí que

$$\pi(x) \geq \frac{x \log 2}{2 \log x},$$

para todo x par, lo que implica la misma ecuación para todo x entero, pues $\pi(2k-1) = \pi(2k)$, para $k \geq 2$. $\square$

Corolario

Sea p_n el n-ésimo número primo. Existen constantes $0 < c' < C'$ tales que

$$c' n \log n < p_n < C' n \log n.$$

<u>Prueba</u>: Si $\limsup_{n\to\infty} \frac{p_n}{n \log n} > C'$, entonces vale

$$\begin{aligned} \liminf_{x\to\infty} \frac{\pi(x)}{x/\log x} &\leq \liminf_{n\to\infty} \frac{\pi(p_n)}{p_n/\log p_n} \\ &\leq \liminf_{n\to\infty} \frac{n(\log n + \log n + \log\log n)}{C' n \log n} = \frac{1}{C'}, \end{aligned}$$

ya que $\frac{x}{\log x}$ es creciente para $x \geq 3$. Así, como $\liminf_{x\to\infty} \frac{\pi(x)}{x/\log x} > 0$, por el Teorema de Chebyshev tenemos que existe $C' > 0$ tal que $p_n < C' n \log n$, para todo $n \geq 2$. De forma similar se prueba la existencia de la constante c'. $\square$

Corolario

a) *Las funciones* p_n *y* $n \log n$ *tienen el mismo orden de magnitud, esto es* $p_n \asymp n \log n$.

b) *Las funciones* $\pi(x)$ *y* $\frac{x}{\log x}$ *tienen el mismo orden de magnitud, esto es* $\pi(x) \asymp \dfrac{x}{\log x}$.

Prueba: (a) Se deduce inmediatamente del corolario previo $c'\, n \log n < p_n < C'\, n \log n$.
(b) Se deduce inmediatamente del Teorema de Chebyshev $c\, \frac{x}{\log x} < \pi(x) < C\, \frac{x}{\log x}$. $\square$

Corolario

Sea $f : \mathbb{N} \to [0, \infty)$ *una función decreciente. La serie*

$$\sum_{p \text{ primo}} f(p) \text{ converge} \qquad \Longleftrightarrow \qquad \sum_{n=2}^{\infty} \frac{f(n)}{\log n} \text{ converge}.$$

En particular, $\sum_p \frac{1}{p}$ *converge.* $\square$

Postulado de Bertrand

Sabemos que existen secuencias arbitrariamente grandes de números consecutivos que no contienen primos. Por ejemplo

$$k! + 2, k! + 3, k! + 4, \ldots k! + k.$$

Nuestro próximo resultado afirma que los primos no son tan ralos, sino que siguen cierta "densidad". Este teorema también se debe a CHEBYSHEV.

Comenzamos con un lema:

Lema

Para todo $n \geq 2$, tenemos $\prod_{p \leq n} p \leq 4^n$.

Prueba: Por inducción sobre n.
Es fácil verificar que el resultado vale para $n = 2, 3y4$.

Suponga que el resultado vale para $n = 2m + 1$, entonces vale también para $n = 2m + 2$, pues no agregamos nuevos primos al producto al pasar de $2m + 1$ a $2m + 2$.

UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

Postulado de Bertrand

Basta entonces mostrar la desigualdad para un número impar $2m+1$. Para un primo p tal que $m+1 < p \leq 2m+1$, se tiene que $p \mid (2m+1)!$ pero $p \nmid m!$ y $p \nmid (m+1)!$, entonces

$$\prod_{m+1<p\leq 2m+1} p \leq \binom{2m+1}{m+1} = \binom{2m}{m+1} + \binom{2m}{m} < (1+1)^{2m} = 2^{2m} = 4^m.$$

De la hipótesis inductiva, se tiene que

$$\prod_{p\leq 2m+1} p = \prod_{p\leq m+1} p \prod_{m+1<p\leq 2m+1} p < 4^{m+1}4^m = 4^{2m+1}. \square$$

Teorema (Postulado de Bertrand)

Sea $n \in \mathbb{Z}^+$ un entero positivo. Entonces, siempre existe un número primo p tal que $n \leq p \leq 2n$.

Prueba: Supongamos que el resultado es falso para algún valor de n. Vamos a mostrar que n no puede ser muy grande.

Sea p_k el k-ésimo primo y sea α_k el mayor valor tal que $p_k^{\alpha_k} \mid \binom{2n}{n}$. Como estamos suponiendo que no hay primos entre n y $2n$, y como ningún primo entre $\frac{2}{3}n$ y n divide a $\binom{2n}{n}$, por el lema al inicio del aula tenemos que $p_k^{\alpha_k} \leq 2n$, y $\alpha_j \leq 1$, para $p_j > \sqrt{2n}$. Luego

$$\binom{2n}{n} \leq \prod_{p_k \leq \sqrt{2n}} p_k^{\alpha_k} \prod_{\sqrt{2n} < p_j \leq \frac{2n}{3}} p_j \leq \prod_{p_k \leq \sqrt{2n}} 2n \prod_{p_j \leq \frac{2n}{3}} p_j.$$

Ahora, del lema anterior, y suponiendo que n es suficientemente grande, de modo que el número de primos entre 1 y $\sqrt{2n}$ es menor que $\sqrt{n/2} - 1$ ($n = 100$ es suficiente, pues ya a partir de este número la mitad de los valores en este intervalo son pares), tenemos

$$\binom{2n}{n} < (2n)^{\sqrt{n/2} - 1} \cdot 4^{2n/3}.$$

Postulado de Bertrand

Por otro lado, $n\binom{2n}{n} = n\binom{2n-1}{n} + n\binom{2n-1}{n-1} > (1+1)^{2n-1} = 2^{2n-1}$. y así, la desigualdad anterior implica que

$$\frac{2^{2n-1}}{n} < (2n)^{\sqrt{n/2}-1} \cdot 4^{2n/3} \qquad \Longrightarrow \qquad 2^{2n/3} < (2n)^{\sqrt{n/2}}.$$

Tomando logaritmo base 2, obtenemos la desigualdad $\frac{2\sqrt{2}}{3} < \log_2 n + 1$, que es falsa para todo $n > 50$. Así, de existir un contra-ejemplo al postulado de Bertrand, éste debe ser menor a 100. Para concluir el resultado, basta mostrar un primo que cumple las condiciones del teorema para todo $n < 100$:

$p = 2$ para $1 \leq n \leq 2$,
$p = 5$ para $3 \leq n \leq 5$,
$p = 11$ para $6 \leq n \leq 11$,
$p = 23$ para $12 \leq n \leq 23$,
$p = 47$ para $24 \leq n \leq 47$,
$p = 79$ para $48 \leq n \leq 79$,
$p = 101$ para $80 \leq n \leq 100$. $\square$