Cálculo del número exacto de primos menores o iguales que x: Método de Lehmer

Hong Christian Lin Jiang

Trabajo de Fin de Grado de Matemáticas
Universidad de Zaragoza

Directores del TFG: Julio Bernués Pardo
Ángel R. Francés Román

Summary

In this document our goal is to find how to evaluate the $\pi(x)$ function, which tells us the number of prime numbers less or equal to x. We divide it into two chapters.

In the first chapter we introduce some mathematical tools, such as the convolution between two functions and Euler's summation formula, to show some results about prime numbers at the end. For example, we deduce that sums like these

$$\sum_{p\leq x}\frac{\log(p)}{p} \text{ and } \sum_{p\leq x}\frac{1}{p}, \text{ with } p \text{ prime}$$

can be approximated by a sort of function of x for large values of x with a margin of error bounded above by an another function.

We begin recalling the usual convolution from Real Analysis course and the Cauchy product of two series, where a kind of convolution is involved. Then we present our main operator: the Dirichlet convolution of two arithmetic functions (functions with domain in the natural numbers) and its generalized version, both applied on $(\mathbb{R}^+, d\mu, \cdot)$, where $\mathbb{R}^+ \equiv (0,\infty)$ is the main domain with the counting measure and usual multiplication.

We also show some arithmetic functions useful in Analytic Number Theory related to prime numbers (Möbius' μ, Mangoldt's Λ and Euler's totient function φ among others). We deduce some special properties of this convolution (the neutral function and the Dirichlet inverse of a function) ending this section with the generalized inversion formula. Throught this process we state some equalities that involve arithmetic functions in as examples of applying the proven results.

Apart from that, Euler's summation formula transforms expressions with finite sums into others with some integrals, showing some examples using that formula and how useful is to analyze the asymptotic behaviour of a function. Also, we prove a connection between partial sums of arithmetic functions with partial sum of its convolution applying convolution properties. From that, we obtain another results for our aim purpose in this chapter.

Finally, we need the Chebyshev's ψ and ϑ functions and the Shapiro's theorem combining with tools previously described to prove results about prime numbers (such as bounds for $\pi(x)$). We will notice, as a consequence, there is an alternative way to prove the existence of infinity primes different from the classical Euclid's proof. We also state about Abel's summation formula, a general version of Euler's one, that we will use that in a proof.

Next chapter, we show a way to calculate $\pi(x)$, based on sieving interval methods and we analize the computational complexity of Lehmer's algorithm. We introduce the counting sieve function $\phi(x,a)$, which counts the numbers n less or equal to x such that n is not divisible by the first a primes. We obtain a formula for that using the Principle of Inclusion-Exclusion. This formula will be helpful to present Legendre's $\pi(x)$ formula. After that, we find some ways to compute that ϕ function, mainly with a recursive formula and deducing some other properties.

Also, we present the k-th partial sieve function $P_k(x,a)$ (related to $\phi(x,a)$) and we express $\pi(x)$ in terms of $\phi(x,a)$ and $P_k(x,a)$ varying the k parameter up to a certain number, depending on which value of a we choose. This obtained formula of $\pi(x)$ contains the Legendre's formula, taking $a=\pi(x^{1/2})$. Meissel improved the way to compute $\pi(x)$ with $a=\pi(x^{1/3})$. Later, Lehmer chose $a=\pi(x^{1/4})$, having this formula

$$\pi(x) = \phi(x, a) + a - 1 - P_2(x, a) - P_3(x, a)$$

Then, we deduce a recursive expression for these $P_k(x, a)$ functions and the explicit formulas for the cases $k = 2$ and $k = 3$, used in Lehmer's formula. After done that, we construct an algorithm based on those obtained results and formulas and we review the classic Erathostenes sieve during the process. Finally, we study the computational cost by time (number of operations) and storage room (memory space) of Lehmer's method. We also comment about some improvements that can be implemented in the algorithm to reduce time and storage room.

Índice general

Capítulo 1

Sobre resultados matemáticos de los números primos

En este capítulo el objetivo es demostrar estimaciones sobre números primos como esta:

$$\sum_{p\leq x}\frac{\log(p)}{p}=\log(x)+O(1)$$

Para ello, necesitamos estas dos herramientas fundamentales:

- Convolución de funciones aritméticas y generalizada: se basan en la convolución de funciones integrables (respecto a la medida de contar) para operar funciones aritméticas.
- Fórmula de sumación de Euler: Esta fórmula transforma expresiones que involucran sumas en otras con integrales.

1.1. Convolución de funciones: Dirichlet y generalizada

Ejemplo 1. *1. En Análisis Matemático vimos la convolución en $(\mathbb{R},dx,+)$, con la suma usual y la medida de Lebesgue (que cumple que $m(x+E)=m(E)$, siendo $x\in\mathbb{R}$ y $E\in\mathscr{B}(\mathbb{R})$ un boreliano). Esta convolución está dada para funciones integrables.*

$$(f\star g)(x)\coloneqq\int_{\mathbb{R}}f(y)g(x-y)dy$$

2. También en $(l_1(\mathbb{Z}),\mathbb{Z},d\mu,+)$, con la suma usual y la medida de contar, se tiene que dadas las sucesiones $a=(a_i)$ y $b=(b_j)$; el producto de Cauchy de las series $\sum_i a(i)$ y $\sum_j b(j)$ está dado en función de una convolución.

$$\left(\sum_i a(i)\right)\left(\sum_j b(j)\right)=\sum_n(a\star b)(n)\ ,\ \text{donde}\ (a\star b)(n)=\sum_k a_{n-k}b_k$$

3. En este trabajo veremos el caso sobre $(\mathbb{R}^+,d\mu,\cdot)$, donde $\mathbb{R}^+\equiv(0,\infty)$ con la multiplicación usual y la medida de contar. En tal caso la convolución está dada por

$$(f\star g)(x)\coloneqq\int_{\mathbb{R}^+}f(y)g\left(\frac{x}{y}\right)d\mu(y)$$

Para que $f:\mathbb{R}^+\to\mathbb{R}$ sea integrable respecto a la medida de contar, f debe cumplir "buenas"propiedades.

a) *Por ejemplo (ver 4), si* $f = 0$ *en* $\mathbb{R}^+ \setminus N$ *(es decir,* f *toma valores no nulos solamente en* $\mathbb{N}$ *y a esto se la llamaremos* función aritmética*), la convolución toma la forma*

$$(f \star g)(n) = \int_{\mathbb{R}^+} f(y) g\left(\frac{n}{y}\right) d\mu(y) = \int_{\mathbb{N}} f(l) g\left(\frac{n}{l}\right) d\mu(l) = \sum_{l|n} f(l) g\left(\frac{n}{l}\right)$$

b) *Si* α *es una función aritmética, pero permitimos a* $F : \mathbb{R}^+ \to \mathbb{R}$ *con* $F((0,1)) = \{0\}$ *(ver 11), entonces es de la forma*

$$(\alpha \star F)(x) = \int_{\mathbb{R}^+} \alpha(y) F\left(\frac{x}{y}\right) d\mu(y) = \int_{\mathbb{N}} \alpha(n) F\left(\frac{x}{n}\right) d\mu(n) = \sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right)$$

Nota 2. En general, la herramienta de convolución sirve para una terna $(G, \mathrm{M}, \cdot)$, en donde $(G, \cdot)$ es un grupo abeliano y M es una medida invariante por G.

Ejemplo 3 (Algunas funciones aritméticas)**.** (1) *La función unidad* u*, dada por* $u(n) = 1$ *en* $\mathbb{N}$

(2) *La función autoasignación* $N(n) = n$ *en* $\mathbb{N}$

(3) *La función identidad* I*, dada por*

$$I(n) = \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{en otro caso} \end{cases}$$

(4) *La función* μ *de Möbius, dada por* $\mu(1) = 1$ *y si* $n > 1$*, con su factorización por primos* p_i

$$n = \prod_{1 \leq i \leq k} {p_i}^{a_i} \text{ donde } p_1 < p_2 < \cdots < p_k \text{ y } a_i \neq 0,$$

$$\mu(n) = \begin{cases} (-1)^k & \text{si } a_i = 1 \ \forall i \\ 0 & \text{en otro caso} \end{cases}$$

(5) *La función* φ *de Euler, dada por* $\varphi(n) = |\{\, m \in \mathbb{N} \text{ con } m \leq n \mid mcd(m,n) = 1 \,\}|$*. Esta función cumple las propiedades siguientes, conocidas en teoría de números:*

a) $\varphi(p) = p - 1$ *si* p *es primo*
b) $\varphi(mn) = \varphi(m)\varphi(n)$ *si* $mcd(m,n) = 1$
c) $\varphi(p^a) = p^{a-1}(p-1)$ *si* p *es primo*

(6) *La función* Λ *de Mangoldt, dada por*

$$\Lambda(n) = \begin{cases} \log(p) & \text{si } n = p^m, \text{ con } p \text{ primo y } m \geq 1 \\ 0 & \text{en otro caso} \end{cases}$$

Definición 4 (Convolución de Dirichlet)**.** *Sean* $f,\ g : \mathbb{N} \to \mathbb{R}$ *funciones aritméticas. La* convolución de Dirichlet *entre* f *y* g *está dada por*

$$(f \star g)(n) \coloneqq \sum_{d|n} f(d) g\left(\frac{n}{d}\right) \text{ para } n \in \mathbb{N}$$

Nota 5. De igual manera a como se prueban las propiedades algebraicas de la convolución en $(L_1(\mathbb{R}), dx, +)$ ó $(l_1(\mathbb{Z}), \mathbb{Z}, d\mu, +)$, la convolución de Dirichlet de funciones aritméticas es conmutativa, asociativa y distributiva respecto de la suma de funciones.

Teorema 6 (Elemento Neutro e Inverso de Dirichlet)**.** (1) *$f \star I = f = I \star f$, $\forall f$ función aritmética con I la identidad (*neutro de Dirichlet*)*

(2) *Sea f una función aritmética con $f(1) \neq 0$. Entonces existe una única función aritmética f^{-1} llamada* inverso de Dirichlet *tal que $f \star f^{-1} = I = f^{-1} \star f$, dada por*

$$f^{-1}(n) = \begin{cases} \frac{1}{f(1)} & si\ n = 1 \\ \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) & si\ n > 1 \end{cases}$$

(3) *Sean f, g funciones aritméticas tales que $f(1), g(1) \neq 0$. Entonces existe $(f \star g)^{-1}$, con $(f \star g)^{-1} = f^{-1} \star g^{-1}$*

Demostración. (1) Tenemos que

$$(f \star I)(n) = \sum_{d|n} f(d) I\left(\frac{n}{d}\right) = f(n)$$

, ya que $\lfloor d/n \rfloor = 0$ si $d < n$.

(2) Hallamos f^{-1} tal que $f \star f^{-1} = I$ en $\mathbb{N}$. Para $n = 1$, $f(1)f^{-1}(1) = 1$ tiene solución única si $f(1) \neq 0$. Para $n > 1$, tenemos que

$$f(1)f^{-1}(n) + \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) = 0$$

, que tiene solución única porque está determinado por los $f^{-1}(d)$ del sumatorio hallados previamente con esta recursión.

(3) Existe $(f \star g)^{-1}$, porque $(f \star g)(1) = f(1)g(1) \neq 0$. Aplicando la propiedad asociativa y del inverso, se tiene que $I = (f \star g) \star (f \star g)^{-1} = f \star (g \star (f \star g)^{-1})$. Luego, convolucionando con f^{-1} a ambos miembros, llegamos a

$$f^{-1} \star I = f^{-1} = (f^{-1} \star f) \star (g \star (f \star g)^{-1}) = I \star (g \star (f \star g)^{-1}) = g \star (f \star g)^{-1}$$

Finalmente, convolucionando con g^{-1} a ambos miembros y aplicando la propiedad conmutativa,

$$g^{-1} \star f^{-1} = (g^{-1} \star g) \star (f \star g)^{-1} = (f \star g)^{-1}$$

□

Ejemplo 7. *Veamos que $\sum_{d|n} \mu(d) = I(n)$ para $n \geq 1$. Si $n = 1$, es trivial. Dado un $n > 1$, tomamos su factorización por primos de (4). En este caso, vemos que solo los divisores libres de cuadrados contribuyen a la suma $\sum_{d|n} \mu(d)$, teniendo*

$$\sum_{d|n} \mu(d) = \mu(1) + \sum_{1 \leq i \leq k} \mu(p_i) + \sum_{1 \leq i < j \leq k} \mu(p_i p_j) + \cdots + \mu\left(\prod_{1 \leq i \leq k} p_i\right) =$$

$$= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k = (1-1)^k = 0$$

Hemos demostrado que

$$\mu \star u = I,\ o\ equivalentemente,\ \mu = u^{-1} (ó\ u = \mu^{-1})$$

Teorema 8 (Fórmula de inversión de Möbius)**.** *Sean f, g funciones aritméticas. Entonces*

$$f(n) = \sum_{d|n} g(d) \Leftrightarrow g(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right)$$

Demostración. En términos de convolución de Dirichlet, $f = g \star u \Rightarrow f \star \mu = (g \star u) \star \mu = g \star (u \star \mu) = g \star I = g$. De forma análoga, $g = f \star \mu \Rightarrow g \star u = f$. □

Ejemplo 9. *Podemos expresar la función φ en términos de μ, obteniendo*

$$\varphi(n) = \sum_{1\leq k\leq n} \left\lfloor \frac{1}{mcd(n,k)} \right\rfloor = \sum_{1\leq k\leq n} \sum_{d|mcd(n,k)} \mu(d) = \sum_{1\leq k\leq n} \sum_{\substack{d|n \\ d|k}} \mu(d)$$

Intercambiando el orden de los sumatorios con una variable q tal que $k = qd$, tenemos que

$$\varphi(n) = \sum_{d|n} \sum_{1\leq q\leq \frac{n}{d}} \mu(d) = \sum_{d|n} \mu(d)\frac{n}{d},\ \forall n \geq 1$$

Luego, hemos probado que

$$\varphi = \mu \star N \text{ con } N \text{ de } (2)$$

Aplicando la fórmula de inversión de Möbius, se tiene que

$$N = \varphi \star u \text{ (es decir } \sum_{d|n} \varphi(d) = n \text{)}$$

Ejemplo 10. *Veamos la suma $\sum_{d|n} \Lambda(d)$. Sea $n > 1$, con su factorización por primos de (4). Tomando logaritmos a ambos miembros, tenemos que*

$$\log(n) = \sum_{1\leq k\leq r} a_k \log(p_k)$$

Luego,

$$\sum_{d|n} \Lambda(d) = \sum_{1\leq k\leq r} \sum_{1\leq m\leq a_k} \Lambda(p_k^m) = \sum_{1\leq k\leq r} \sum_{1\leq m\leq a_k} \log(p_k) = \sum_{1\leq k\leq r} a_k \log(p_k) = \log(n)$$

Esta igualdad se cumple también para $n = 1$ (trivial). Por tanto, $\Lambda \star u = \log$. Luego,

$$\Lambda = \mu \star \log = -(\mu \log) \star u$$

por la fórmula de inversión de Möbius y por

$$\Lambda(n) = \log(n) \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d)\log(d) = \log(n)I(n) - \sum_{d|n} \mu(d)\log(d)$$

Notar que $I \log = 0$ función nula.

Definición 11 (Convolución generalizada)**.** *Sea $\alpha : \mathbb{N} \to \mathbb{R}$ una función aritmética y sea $F : \mathbb{R}^+ \to \mathbb{R}$ tal que $F((0,1)) = \{0\}$. La* convolución generalizada *entre α y F está dada por*

$$(\alpha \circ F)(x) \coloneqq \sum_{n\leq x} \alpha(n) F\left(\frac{x}{n}\right) \text{ para } x \in \mathbb{R}$$

Nota 12. Notar que si denotamos $G \equiv \alpha \circ F$, $G((0,1)) = \{0\}$. La convolución de Dirichlet y la convolución generalizada parten de un mismo tipo de convolución (de la terna de 3).

Teorema 13 (Propiedad asociativa alternativa entre $\star$ y $\circ$)**.** *Sean α, β funciones aritméticas y sea $F : \mathbb{R}^+ \to \mathbb{R}$ tal que $F((0,1)) = \{0\}$. Entonces $\alpha \circ (\beta \circ F) = (\alpha \star \beta) \circ F$*

Demostración. Para $x > 0$,

$$(\alpha \circ (\beta \circ F))(x) = \sum_{n \leq x} \alpha(n) \sum_{m \leq x/n} \beta(m) F\left(\frac{x}{mn}\right) = \sum_{mn \leq x} \alpha(n)\beta(m) F\left(\frac{x}{mn}\right) =$$

$$= \sum_{k \leq x} \left(\sum_{n|k} \alpha(n) \beta\left(\frac{k}{n}\right) \right) F\left(\frac{x}{k}\right) = \sum_{k \leq x} (\alpha \star \beta)(k) F\left(\frac{x}{k}\right) = ((\alpha \star \beta) \circ F)(x)$$

□

Teorema 14 (Fórmula de inversión generalizada)**.** *Sea α una función aritmética tal que exista inversa de Dirichlet α^{-1} y sean F, G con $F((0,1)) = G((0,1)) = \{0\}$. Entonces*

$$G(x) = \sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right) \Leftrightarrow F(x) = \sum_{n \leq x} \alpha^{-1}(n) G\left(\frac{x}{n}\right)$$

Demostración. Notar que la función identidad I (neutro de Dirichlet) es el neutro a izquierda para la convolución generalizada, ya que $I \circ F = F$. Sabiendo esto y aplicando la propiedad asociativa alternativa, $G = \alpha \circ F \Rightarrow \alpha^{-1} \circ G = \alpha^{-1} \circ (\alpha \circ F) = (\alpha^{-1} \star \alpha) \circ F = I \circ F = F$. Análogamente, obtenemos también que $F = \alpha^{-1} \circ G \Rightarrow \alpha \circ F = G$. □

1.2. Fórmula de sumación de Euler

En esta sección vamos a estudiar el comportamiento asintótico de sumas parciales transformando la expresión en una aproximación integral, incluyendo términos de error (acotados por una cierta función). Para ello introducimos la siguiente fórmula de Euler, útil para llegar a nuestro objetivo.

Teorema 15 (Fórmula de sumación de Euler)**.** *Sea una función $f \in \mathscr{C}^1([y,x])$, con $y > 0$. Entonces*

$$\sum_{y < n \leq x} f(n) = \int_y^x f(t)dt + \int_y^x (t - \lfloor t \rfloor) f'(t)dt + (f(t)(\lfloor t \rfloor - t))|_{t=y}^{t=x}$$

Demostración. Si n, $n-1 \in \mathbb{N} \cap [y,x]$, se tiene que

$$\int_{n-1}^n \lfloor t \rfloor f'(t)dt = (n-1) \int_{n-1}^n f'(t)dt =$$

$$= (n-1)(f(n) - f(n-1)) = nf(n) - (n-1)f(n-1) - f(n)$$

Integrando en $[\lfloor y \rfloor + 1, \lfloor x \rfloor]$,

$$\int_{\lfloor y \rfloor + 1}^{\lfloor x \rfloor} \lfloor t \rfloor f'(t)dt = \sum_{n = \lfloor y \rfloor + 2}^{\lfloor x \rfloor} \int_{n-1}^n \lfloor t \rfloor f'(t)dt =$$

$$= \sum_{n = \lfloor y \rfloor + 2}^{\lfloor x \rfloor} (nf(n) - (n-1)f(n-1)) - \sum_{n = \lfloor y \rfloor + 2}^{\lfloor x \rfloor} f(n) =$$

$$= (tf(t))|_{t = \lfloor y \rfloor + 1}^{t = \lfloor x \rfloor} - \sum_{y+1 < n \leq x} f(n)$$

$$\int_{\lfloor y\rfloor+1}^{\lfloor x\rfloor} \lfloor t\rfloor f'(t)dt = \lfloor x\rfloor f(\lfloor x\rfloor) - \lfloor y\rfloor f(\lfloor y\rfloor+1) - \sum_{y<n\leq x} f(n) \tag{1.1}$$

Por un lado, se tienen estas igualdades:

$$\int_{y}^{\lfloor y\rfloor+1} \lfloor t\rfloor f'(t)dt = \lfloor y\rfloor(f(\lfloor y\rfloor+1) - f(y)) \tag{1.2}$$

$$\int_{\lfloor x\rfloor}^{x} \lfloor t\rfloor f'(t)dt = \lfloor x\rfloor(f(x) - f(\lfloor x\rfloor)) \tag{1.3}$$

Despejando $\sum_{y<n\leq x} f(n)$ de la igualdad (1.1); y sumando y restanto términos de (1.2) y (1.3), obtenemos

$$\sum_{y<n\leq x} f(n) = -\int_{y}^{\lfloor y\rfloor+1} \lfloor t\rfloor f'(t)dt - \int_{\lfloor y\rfloor+1}^{\lfloor x\rfloor} \lfloor t\rfloor f'(t)dt - \int_{\lfloor x\rfloor}^{x} \lfloor t\rfloor f'(t)dt +$$

$$+\lfloor x\rfloor f(\lfloor x\rfloor) - \lfloor y\rfloor f(\lfloor y\rfloor+1) + \lfloor x\rfloor(f(x) - f(\lfloor x\rfloor)) + \lfloor y\rfloor(f(\lfloor y\rfloor+1) - f(y))$$

$$\sum_{y<n\leq x} f(n) = -\int_{y}^{x} \lfloor t\rfloor f'(t)dt + (\lfloor t\rfloor f(\lfloor t\rfloor))|_{t=y}^{t=x} \tag{1.4}$$

Por otro lado, integrando f por partes tenemos que

$$\int_{y}^{x} f(t)dt = (tf(t))|_{t=y}^{t=x} - \int_{y}^{x} tf'(t)dt \tag{1.5}$$

Combinando (1.4) y (1.5), se llega al resultado.

$$\sum_{y<n\leq x} f(n) - \int_{y}^{x} f(t)dt = \int_{y}^{x} (t - \lfloor t\rfloor)f'(t)dt + (f(t)(\lfloor t\rfloor - t))|_{t=y}^{t=x}$$

□

Teorema 16 (Ejemplos: fórmulas elementales asintóticas)**.** *Para todo $x \geq 1$,*

(1)
$$\sum_{n\leq x} \frac{1}{n} = \log(x) + \gamma + O\left(\frac{1}{x}\right), \text{ donde } \gamma \text{ es una constante real}$$

(2)
$$\sum_{n\leq x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} + \zeta(s) + O(x^{-s}), \text{ si } s > 0 \text{ y } s \neq 1$$

(3)
$$\sum_{n>x} \frac{1}{n^s} = O(x^{1-s}), \text{ si } s > 1$$

(4)
$$\sum_{n\leq x} n^{\alpha} = \frac{x^{\alpha+1}}{\alpha+1} + O(x^{\alpha}), \text{ si } \alpha \geq 0$$

donde ζ es la función zeta de Riemann, definida como

$$\zeta(s) = \begin{cases} \sum_{n\geq 1} n^{-s} & si\ \ s > 1 \\ \lim_{x\to+\infty} \left(\sum_{n\leq x} n^{-s} - (x^{1-s})(1-s)^{-1}\right) & si\ \ s \in (0,1) \end{cases}$$

Demostración. Todas estas fórmulas resultan de una aplicación de la fórmula de sumación de Euler.

1. Tomando $f(t) = t^{-1}$, tenemos

$$\sum_{n\leq x}\frac{1}{n} = 1 + \sum_{1<n\leq x}\frac{1}{n} = \int_1^x \frac{dt}{t} - \int_1^x \frac{t-\lfloor t\rfloor}{t^2}dt + 1 - \frac{x-\lfloor x\rfloor}{x} =$$

$$= \log(x) + 1 - \int_1^\infty \frac{t-\lfloor t\rfloor}{t^2}dt + \int_x^\infty \frac{t-\lfloor t\rfloor}{t^2}dt + O\left(\frac{1}{x}\right)$$

   Para todo $x \geq 1$, la integral $\int_x^\infty (t-\lfloor t\rfloor)t^{-2}dt$ es convergente porque

$$0 \leq \int_x^\infty \frac{t-\lfloor t\rfloor}{t^2}dt \leq \int_x^\infty \frac{1}{t^2}dt = \frac{1}{x}$$

   Luego,

$$\sum_{n\leq x}\frac{1}{n} = \log(x) + \gamma + O\left(\frac{1}{x}\right) \text{ , donde } \gamma = 1 - \int_1^\infty \frac{t-\lfloor t\rfloor}{t^2}dt$$

2. Tomando $f(t) = t^{-s}$, con si $s > 0$ y $s \neq 1$,

$$\sum_{n\leq x}\frac{1}{n^s} = 1 + \sum_{1<n\leq x}\frac{1}{n^s} = \int_1^x \frac{dt}{t^s} - s\int_1^x \frac{t-\lfloor t\rfloor}{t^{s+1}}dt + 1 - \frac{x-\lfloor x\rfloor}{x^s}$$

$$\sum_{n\leq x}\frac{1}{n^s} = \frac{x^{1-s}}{1-s} + C(s) + O(x^{-s}) \tag{1.6}$$

   , donde

$$C(s) = 1 - \frac{1}{1-s} - s\int_1^x \frac{t-\lfloor t\rfloor}{t^{s+1}}dt$$

   Queda ver que $C(s) = \zeta(s)$ para $s > 0$. Si $s > 1$, al tomar límites cuando $x \to \infty$ en la igualdad (1.6), $\zeta(s) = 0 + C(s) + 0 = C(s)$. Análogamente, si $0 < s < 1$, obtenemos que

$$\zeta(s) = \lim_{x\to\infty}\left(\sum_{n\leq x}\frac{1}{n^s} - \frac{x^{1-s}}{1-s}\right) = C(s) + 0 = C(s)$$

3. Aplicando (2) para $s > 1$,

$$\sum_{n>x}\frac{1}{n^s} = \zeta(s) - \sum_{n\leq x}\frac{1}{n^s} = \frac{x^{1-s}}{1-s} + O(x^{-s}) = O(x^{1-s})$$

   , ya que $x^{-s} \leq x^{1-s}$

4. Tomando $f(t) = t^\alpha$,

$$\sum_{n\leq x} n^\alpha = 1 + \sum_{1<n\leq x} n^\alpha = \int_1^x t^\alpha dt + \alpha\int_1^x t^{\alpha-1}(t-\lfloor t\rfloor)dt + 1 - (x-\lfloor x\rfloor)x^\alpha =$$

$$= \frac{x^{\alpha+1}}{\alpha+1} - \frac{1}{\alpha+1} + O\left(\alpha\int_1^x t^{\alpha-1}dt\right) + O(x^\alpha) = \frac{x^{\alpha+1}}{\alpha+1} + O(x^\alpha)$$

□

Teorema 17. *Sean f, g funciones aritméticas y sea $h = f \star g$. Definimos las sumas parciales $F(x) = \sum_{n\leq x} f(n)$, $G(x) = \sum_{n\leq x} g(n)$ y $H(x) = \sum_{n\leq x} h(n)$. Entonces se cumple que*

$$H(x) = \sum_{n\leq x} f(n)G\left(\frac{x}{n}\right) = \sum_{n\leq x} g(n)F\left(\frac{x}{n}\right)$$

Demostración. Definimos $U : \mathbb{R}^+ \to \mathbb{R}$ la función indicatriz $U(x) = \mathbb{1}_{\{x\geq 1\}}(x)$. Notar que $F = f \circ U$ y $G = g \circ U$. Aplicando la propiedad asociativa alternativa entre $\star$ y $\circ$, se tiene $f \circ G = f \circ (g \circ U) = (f \star g) \circ U = h \circ U = H$ y de forma análoga, $g \circ F = H$. □

Corolario 18. *Sea f una función aritmética, con $F(x) = \sum_{n\leq x} f(n)$. Entonces*

$$\sum_{n\leq x}\sum_{d|n} f(d) = \sum_{n\leq x} f(n)\left\lfloor\frac{x}{n}\right\rfloor = \sum_{n\leq x} F\left(\frac{x}{n}\right)$$

Demostración. Aplicando el teorema anterior con $g = u$ la función unidad, $G(x) = \lfloor x\rfloor$ y se tiene el resultado. □

Teorema 19. *Si $x \geq 1$, se cumple que*

$$\sum_{n\leq x} \mu(n)\left\lfloor\frac{x}{n}\right\rfloor = 1$$

$$\sum_{n\leq x} \Lambda(n)\left\lfloor\frac{x}{n}\right\rfloor = \log(\lfloor x\rfloor!) \tag{1.7}$$

Demostración. Aplicando el corolario anterior; por un lado, tomo $f = \mu$ de Möbius y obtengo

$$\sum_{n\leq x} \mu(n)\left\lfloor\frac{x}{n}\right\rfloor = \sum_{n\leq x}\sum_{d|n} \mu(d) = \sum_{n\leq x}\left\lfloor\frac{1}{n}\right\rfloor = 1$$

Por otro lado, tomando $f = \Lambda$ de Mangoldt, llegamos a

$$\sum_{n\leq x} \Lambda(n)\left\lfloor\frac{x}{n}\right\rfloor = \sum_{n\leq x}\sum_{d|n} \Lambda(d) = \sum_{n\leq x} \log(n) = \log(\lfloor x\rfloor!)$$

□

Teorema 20 (Identidad de Legendre)**.** *Si $x \geq 1$, se tiene la siguiente factorización en primos.*

$$\lfloor x\rfloor! = \prod_{p\leq x} p^{\alpha(p)}, \text{ con } \alpha(p) = \sum_{m\geq 1}\left\lfloor\frac{x}{p^m}\right\rfloor$$

Notar que $\alpha(p)$ tiene un número finito de términos porque $\lfloor x/p^m\rfloor = 0$ para un primo $p > x$.

Demostración. Yendo a la fórmula 1.7 del teorema anterior y aplicando la definición de Λ de Mangoldt, llegamos a

$$\log(\lfloor x\rfloor!) = \sum_{n\leq x} \Lambda(n)\left\lfloor\frac{x}{n}\right\rfloor = \sum_{p\leq x}\sum_{m\geq 1}\left\lfloor\frac{x}{p^m}\right\rfloor \log(p) = \sum_{p\leq x} \alpha(p)\log(p)$$

Tomando exponenciales exp en esta última expresión, se tiene el resultado. □

Ejemplo 21. *Dado $x \in \mathbb{N}$, la identidad de Legendre nos ayuda a factorizar en primos $x!$ sin tener que factorizar por separado los números $n \leq x$ y combinarlo después. Como ejemplo, vamos a factorizar $15!$. El conjunto de primos menores o iguales que 15 es $\{2,3,5,7,11,13\}$. Estos primos aparecen en dicha factorización. Hallamos la mayor potencia de cada primo del conjunto que divide a $15!$. Empezando con el primo 2, obtenemos que*

$$\alpha(2) = \sum_{m\geq 1} \left\lfloor \frac{15}{2^m} \right\rfloor = \sum_{1\leq m\leq 3} \left\lfloor \frac{15}{2^m} \right\rfloor = \left\lfloor \frac{15}{2} \right\rfloor + \left\lfloor \frac{15}{4} \right\rfloor + \left\lfloor \frac{15}{8} \right\rfloor = 7+3+1 = 11$$

Análogamente con el resto de los primos, tenemos que $\alpha(3) = 5+1 = 6$, $\alpha(5) = 3$, $\alpha(7) = 2$ y $\alpha(11) = \alpha(13) = 1$. Por tanto, $15! = 2^{11} \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13$.

Teorema 22. *Para todo $x \geq 2$,*

$$\log(\lfloor x \rfloor !) = x\log(x) - x + O(\log(x))$$

Luego,

$$\sum_{n\leq x} \Lambda(n) \left\lfloor \frac{x}{n} \right\rfloor = x\log(x) - x + O(\log(x))$$

Demostración. Aplicando la fórmula de sumación de Euler con $f(t) = \log(t)$, tenemos que

$$\sum_{n\leq x} \log(n) = \int_1^x \log(t)dt + \int_1^x \frac{t - \lfloor t \rfloor}{t} dt - (x - \lfloor x \rfloor)\log(x) =$$

$$= x\log(x) - x + 1 + \int_1^x \frac{t - \lfloor t \rfloor}{t} dt + O(\log(x))$$

Como

$$\int_1^x \frac{t - \lfloor t \rfloor}{t} dt = O\left(\int_1^x \frac{dt}{t} \right) = O(\log(x))$$

, el resultado queda demostrado. □

Teorema 23. *Si $x \geq 2$, entonces*

$$\sum_{p\leq x} \left\lfloor \frac{x}{p} \right\rfloor \log(p) = x\log(x) + O(x)$$

, con el sumatorio aplicado a los primos $p \leq x$.

Demostración. Por definición de Λ de Mangoldt,

$$\sum_{n\leq x} \left\lfloor \frac{x}{n} \right\rfloor \Lambda(n) = \sum_p \sum_{\substack{m\geq 1 \\ p^m \leq x}} \left\lfloor \frac{x}{p^m} \right\rfloor \Lambda(p^m) =$$

Como la suma afecta a los primos tales que $p^m \leq x$ en este caso, basta con $p \leq x$ porque $\lfloor x/p^m \rfloor = 0$ si $p > x$.

$$= \sum_{p\leq x} \sum_{m\geq 1} \left\lfloor \frac{x}{p^m} \right\rfloor \log(p) = \sum_{p\leq x} \left\lfloor \frac{x}{p} \right\rfloor \log(p) + \sum_{p\leq x} \sum_{m\geq 2} \left\lfloor \frac{x}{p^m} \right\rfloor \log(p)$$

Queda ver que el segundo sumando de la igualdad es $O(x)$.

$$\sum_{p\leq x} \sum_{m\geq 2} \left\lfloor \frac{x}{p^m} \right\rfloor \log(p) \leq x \sum_{p\leq x} \log(x) \sum_{m\geq 2} \frac{1}{p^m} = x \sum_{p\leq x} \frac{\log(p)}{p(p-1)} \leq x \sum_{n\geq 2} \frac{\log(n)}{n(n-1)} = Kx$$

, con $K > 0$ constante. La serie que acota la suma en esta desigualdad converge. Puede comprobarse mediante el criterio de comparación por paso al límite con $\sum_{n\geq 2} 1/n^{3/2}$.

□

1.3. Teorema de Shapiro y números primos

Definición 24 (Funciones ψ y ϑ de Chebyshev)**.** *Para $x > 0$; estas funciones están dadas por $\psi(x) = \sum_{n\leq x} \Lambda(n)$, con Λ de Mangoldt; y $\vartheta(x) = \sum_{p\leq x} \log(p)$, donde la suma se aplica a los primos $p \leq x$.*

Nota 25. Podemos relacionar estas dos funciones. Por definición de Λ,

$$\psi(x) = \sum_{m\geq 1} \sum_{\substack{p \\ p^m\leq x}} \Lambda(p^m) = \sum_{m\geq 1} \sum_{p\leq x^{\frac{1}{m}}} \log(p) = \sum_{m\leq \log_2(x)} \sum_{p\leq x^{\frac{1}{m}}} \log(p) = \sum_{m\leq \log_2(x)} \vartheta(x^{\frac{1}{m}})$$

Luego, $\psi(x) = \sum_{m\leq \log_2(x)} \vartheta(x^{1/m})$

Teorema 26 (Teorema de Shapiro)**.** *Sea una sucesión $\{a(n)\}_{n\geq 1}$ de términos no negativos tal que*

$$\sum_{n\leq x} a(n) \left\lfloor \frac{x}{n} \right\rfloor = x\log(x) + O(x),\ \forall x \geq 1$$

Entonces

(a)
$$\exists B > 0 \text{ tal que } \sum_{n\leq x} a(n) \leq Bx,\ \forall x \geq 1$$

(b)
$$\sum_{n\leq x} \frac{a(n)}{n} = \log(x) + O(1),\ \forall x \geq 1$$

Demostración. Como notación, definimos $S(x) \equiv \sum_{n\leq x} a(n)$ y $T(x) \equiv \sum_{n\leq x} a(n) \lfloor \frac{x}{n} \rfloor$. Luego, con dicha notación, tenemos que

$$T(x) - 2T\left(\frac{x}{2}\right) = \sum_{n\leq x} \left\lfloor \frac{x}{n} \right\rfloor a(n) - 2 \sum_{n\leq x/2} \left\lfloor \frac{x}{2n} \right\rfloor a(n) =$$

$$= \sum_{n\leq x/2} \left(\left\lfloor \frac{x}{n} \right\rfloor - 2 \left\lfloor \frac{x}{2n} \right\rfloor \right) a(n) + \sum_{x/2<n\leq x} \left\lfloor \frac{x}{n} \right\rfloor a(n)$$

Como $\lfloor 2t \rfloor - 2\lfloor t \rfloor \in \{0, 1\}$ para $t \in \mathbb{R}^+$ (porque si $\lfloor t \rfloor = m \in \mathbb{N} \cup \{0\}$, entonces $m \leq t \leq m+1 \Leftrightarrow 2m \leq 2t \leq 2m+2$ y eso implica que $\lfloor 2t \rfloor \in \{2m, 2m+1\}$), obtenemos esta desigualdad

$$T(x) - 2T\left(\frac{x}{2}\right) \geq \sum_{x/2<n\leq x} \left\lfloor \frac{x}{n} \right\rfloor a(n) =$$

$$= \sum_{x/2<n\leq x} a(n) = S(x) - S\left(\frac{x}{2}\right)$$

Por hipótesis,

$$T(x) - 2T\left(\frac{x}{2}\right) = x\log(x) + O(x) - 2\left(\frac{x}{2}\log\left(\frac{x}{2}\right) + O(x)\right) = O(x)$$

Por tanto; $S(x) - S(x/2) = O(x)$, es decir, que

$$\exists K > 0 \text{ tal que } S(x) - S\left(\frac{x}{2}\right) \leq Kx,\ \forall x \geq 1$$

Podemos obtener; a partir de esta última desigualdad; otras similares, sustituyendo la x por $x/2^k$ variando $k \in \mathbb{N}$. Sumando todas estas desigualdades, llegamos a

$$\sum_{k\geq 0}\left(S\left(\frac{x}{2^k}\right) - S\left(\frac{x}{2^{k+1}}\right)\right) \leq \left(\sum_{k\geq 0}\frac{1}{2^k}\right)Kx = 2Kx$$

Tomando $B = 2K$, se tiene el resultado.

Notar que $\lfloor x/n \rfloor = (x/n) + O(1)$. Reemplazando esto último en $T(x)$, obtenemos que

$$T(x) = x\sum_{n\leq x}\frac{a(n)}{n} + O\left(\sum_{n\leq x}a(n)\right) = x\sum_{n\leq x}\frac{a(n)}{n} + O(x)$$

debido a (a). Despejando $\sum_{n\leq x} a(n)/n$ y aplicando la hipótesis, se tiene lo demostrado.

$$\sum_{n\leq x}\frac{a(n)}{n} = \frac{1}{x}T(x) + O(1) = \log(x) + O(1)$$

□

Corolario 27. *Para $x \geq 1$, se tiene que*

$$\sum_{n\leq x}\frac{\Lambda(n)}{n} = \log(x) + O(1)$$

Además, $\psi(x) = O(x)$.

Demostración. Aplicando el teorema de Shapiro con $a(n) = \Lambda(n)$ de Mangoldt, se tiene el resultado por $\Lambda \geq 0$ y el teorema 22. □

Teorema 28. *Para $x \geq 1$,*

$$\sum_{p\leq x}\frac{\log(p)}{p} = \log(x) + O(1)$$

Además, $\vartheta(x) = O(x)$.

Demostración. Recordemos que por el teorema 23,

$$\sum_{p\leq x}\left\lfloor\frac{x}{p}\right\rfloor\log(p) = x\log(x) + O(x)$$

Definamos la función aritmética $\Lambda_1(n) = \mathbb{1}_{\{n\in\mathbb{P}\}}(n)\log(n)$, con $\mathbb{P}$ el conjunto de números primos. Notar que $\Lambda_1 \geq 0$. Reesbribiendo lo probado,

$$\sum_{n\leq x}\Lambda_1(n)\left\lfloor\frac{x}{n}\right\rfloor = x\log(x) + O(x)$$

Como se cumplen las hipótesis necesarias, aplicando el Teorema de Shapiro con $a(n) = \Lambda_1(n)$, se tiene el resultado. □

Como consecuencia de 28, se puede dar una demostración alternativa a la de Euclides sobre la existencia de infinitos números primos. Tomando límites cuando $x \to \infty$ obtenemos que

$$\lim_{x\to\infty}\left(\sum_{p\leq x}\frac{\log(p)}{p}\right) = +\infty$$

debido a que $\log(x) \to \infty$. Como cada término $\log(p)/p$ de la suma es finito; para que dicho límite se cumpla, tiene que haber infinitos términos en la suma. Por tanto; existen infinitos números primos.

Corolario 29. *Existen $c_1, c_2 \in \mathbb{R}$ tales que para $x \geq 2$, se cumple que*

$$\frac{c_1 x}{\log(x)} \leq \pi(x) \leq \frac{c_2 x}{\log(x)},$$

donde $\pi(x) = |\{\, p \leq x \mid p \in \mathbb{P} \,\}|$

Demostración. Podemos acotar ϑ del siguiente modo: $\vartheta(x) = \sum_{p \leq x} \log(p) \leq \pi(x)\log(x)$. Despejando de esta desigualdad, obtenemos que

$$\pi(x) \geq \frac{\vartheta(x)}{\log(x)} \geq \frac{c_1 x}{\log(x)}$$

debido a que $\vartheta(x) = O(x)$ Por otro lado,

$$\vartheta(x) \geq \sum_{\sqrt{x} \leq p \leq x} \log(p) \geq (\pi(x) - \pi(\sqrt{x}))\log(x) \geq (\pi(x) - \sqrt{x})\log(x)$$

porque $\pi(\sqrt{x}) \leq \sqrt{x}$. Como $\vartheta(x) = O(x)$ (de nuevo), despejando se llega a

$$\frac{kx}{\log(x)} \geq \pi(x) - \sqrt{x} \text{ para algún } k \in \mathbb{R}$$

$$\pi(x) \leq \frac{kx}{\log(x)} + \sqrt{x} \leq \frac{c_2 x}{\log(x)}$$

□

Podemos aplicar el resultado 18, con ψ y ϑ de Chebyshev (por definición de suma parcial), para reescribir de otro modo estos resultados probados anteriormente.

Teorema 30. *Para $x \geq 1$,*

$$\sum_{n \leq x} \psi\left(\frac{x}{n}\right) = x\log(x) - x + O(\log(x)) \; y \; \sum_{n \leq x} \vartheta\left(\frac{x}{n}\right) = x\log(x) + O(x)$$

A continuación, solo enunciamos la fórmula de sumación de Abel, cuya demostración es similar a la de Euler y puede verse en [1, pág. 77–78].

Teorema 31 (Fórmula de sumación de Abel)**.** *Sea una función aritmética $a(n)$ y consideramos su suma parcial $A(x) = \sum_{n \leq x} a(n)$. Sea una función $f \in \mathscr{C}^1([y, x])$, con $y > 0$. Entonces*

$$\sum_{y < n \leq x} a(n)f(n) = (A(t)f(t))|_{t=y}^{t=x} - \int_y^x A(t)f'(t)dt$$

Teorema 32. *Para $x \geq 2$,*

$$\sum_{p \leq x} \frac{1}{p} = \log(\log(x)) + A + O\left(\frac{1}{\log(x)}\right),$$

donde $A \in \mathbb{R}$ es una constante.

Demostración. Definimos $a(n) = \mathbb{1}_{\{n \in \mathbb{P}\}}(n)$ y sea $A(x) = \sum_{p \leq x} \log(p)/p$. Notar que

$$\sum_{p \leq x} \frac{1}{p} = \sum_{n \leq x} \frac{a(n)}{n} \text{ y } A(x) = \sum_{n \leq x} \frac{a(n)}{n}\log(n)$$

Aplicando la fórmula de sumación de Abel con $f(t) = 1/\log(t)$ y nuestro $A(x)$, y como $A(t) = 0$ si $t < 2$, se tiene que

$$\sum_{p\leq x}\frac{1}{p} = \sum_{n\leq x}\frac{a(n)\log(n)}{n}\frac{1}{\log(n)} = \frac{A(x)}{\log(x)} + \int_2^x \frac{A(t)}{t\log^2(t)}dt$$

Como $A(x) = \log(x) + O(1)$ (visto en 28), llegamos a que

$$\sum_{p\leq x}\frac{1}{p} = 1 + O\left(\frac{1}{\log(x)}\right) + \int_2^x \frac{dt}{t\log(t)} + \int_2^x \frac{O(1)}{t\log^2(t)}dt =$$

$$= 1 + O\left(\frac{1}{\log(x)}\right) + \log(\log(x)) - \log(\log(2)) + \int_2^\infty \frac{O(1)}{t\log^2(t)}dt - \int_x^\infty \frac{O(1)}{t\log^2(t)}dt$$

Esta última integral converge porque

$$\int_x^\infty \frac{O(1)}{t\log^2(t)}dt = O\left(\int_x^\infty \frac{1}{t\log^2(t)}dt\right) = O\left(\frac{1}{\log(x)}\right)$$

Por tanto; se tiene probado el resultado, donde

$$A = 1 - \log(\log(2)) + \int_2^\infty \frac{O(1)}{t\log^2(t)}dt$$

□

Capítulo 2

Hallando $\pi(x)$: Método de Lehmer

2.1. Función de cribado parcial $\phi(x,a)$: Fórmula de Legendre

Dado un número $x \in \mathbb{N}$, nos interesa saber cuántos números menores o iguales que x son primos. Para ello, definimos la función $\pi(x) = |\{\, p \leq x \mid p \in \mathbb{P} \,\}|$. Hallar $\pi(x)$ no es tarea fácil. El primer método fue la criba de Eratóstenes, que requería hallar todos los primos menores o iguales que x.

Legendre dedujo que bastaba hallar todos los primos menores o iguales que $\sqrt{x}$ para averiguar $\pi(x)$ aplicando el principio de inclusión-exclusión que indicamos a continuación.

Teorema 33 (Principio de Inclusión-Exclusión)**.** *Sean $S_1, S_2, \cdots, S_a$ conjuntos finitos. Entonces*

$$\left| \bigcup_{1\leq i\leq a} S_i \right| = \sum_{1\leq i\leq a} |S_i| - \sum_{1\leq i<j\leq a} |S_i \cap S_j| + \sum_{1\leq i<j<k\leq a} |S_i \cap S_j \cap S_k| + \cdots + (-1)^{a+1} \left| \bigcap_{1\leq i\leq a} S_i \right|$$

En el resto del trabajo denotaremos por p_i el i-ésimo primo; es decir, que $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ...

Definición 34 (Función de cribado parcial $\phi(x,a)$)**.** *Dado $a \in \mathbb{N}$ arbitrario, para cada $x \in \mathbb{N}$ se define $\phi(x,a)$ como la cantidad de números menores o iguales que x que no son divisibles por los primeros a primos; es decir, $\phi(x,a) = |\{\, n \leq x \mid$ si $p \mid n$ con $p \in \mathbb{P} \Rightarrow p > p_a \,\}|$.*

Nota 35. Obsérvese que $\phi(x,a)$ define una familia infinita de funciones aritméticas de parámetro a. Para $a = 0$, podemos extender la definición de forma consistente, estableciendo $\phi(x,0) = x$, ya que el conjunto formado por ningún primo es vacío. Si $a = 1$, la función cuenta los impares menores o iguales que x; y si $x < p_{a+1}$, $\phi(x,a) = 1$. No debe confundirse esta función $\phi(x,a)$ con la $\varphi(x)$ de Euler, aunque más adelante veremos que están relacionadas de algún modo.

Teorema 36. *Sean $x, a \in \mathbb{N}$. Entonces*

$$\phi(x,a) = \lfloor x \rfloor - \sum_{p_i \leq p_a} \left\lfloor \frac{x}{p_i} \right\rfloor + \sum_{p_i < p_j \leq p_a} \left\lfloor \frac{x}{p_i p_j} \right\rfloor - \sum_{p_i < p_j < p_k \leq p_a} \left\lfloor \frac{x}{p_i p_j p_k} \right\rfloor + \cdots + (-1)^a \left\lfloor \frac{x}{p_1 p_2 \cdots p_a} \right\rfloor \tag{2.1}$$

Demostración. Sean el conjunto $S = \{\, n \leq x \mid n \in \mathbb{N} \,\}$ y los subconjuntos $S_i = \{\, n \leq x \mid$ con $p_i \mid n \,\}$ para $1 \leq i \leq a$. Entonces $|S| = x$ y $|S_i| = \lfloor x/p_i \rfloor$ para $1 \leq i \leq a$. Tener en cuenta que

$$\bigcap_{1\leq j\leq k} S_{i_j} = \{\, n \leq x \mid (p_{i_1} p_{i_2} \cdots p_{i_k}) \mid n \,\}, \text{ luego } \left| \bigcap_{1\leq j\leq k} S_{i_j} \right| = \left\lfloor \frac{x}{p_{i_1} p_{i_2} \cdots p_{i_k}} \right\rfloor$$

Por la definición de $\phi(x,a)$, se tiene que

$$\phi(x,a) = \left| S - \bigcup_{1\leq i\leq a} S_i \right| = |S| - \left| \bigcup_{1\leq i\leq a} S_i \right|.$$

Entonces el resultado se sigue aplicando el Principio de Inclusión-Exclusión a los conjuntos S, $S_1, \cdots, S_a$. □

Nota 37. Relacionando con el capítulo anterior, la fórmula de $\phi(x,a)$ se puede expresar también como

$$\phi(x,a) = \sum_{\substack{q=\prod p_i \\ p_i\leq p_a}} \mu(q)\left\lfloor \frac{x}{q}\right\rfloor = \sum_{n\leq x} \mu_a(n)\left\lfloor \frac{x}{n}\right\rfloor;$$

en donde si $n>1$ y $n=\prod_{1\leq j\leq k} {p_{i_j}}^{a_{i_j}}$, con $p_{i_1}<p_{i_2}<\ \ldots\ <p_{i_k}$ y $a_{i_j}\neq 0$ es su factorización por primos, definimos μ_a como

$$\mu_a(n) = \begin{cases} \mu(n) & \text{si } n=1 \text{ , ó } p_{i_j}\leq p_a \forall j \\ 0 & \text{en otro caso} \end{cases},$$

donde μ es la función de Möbius.

Teorema 38 (Fórmula de Legendre)**.** *Dado un $x>0$, se tiene que $\pi(x)=\pi(x^{1/2})-1+\phi(x,\pi(x^{1/2}))$. Es decir,*

$$\pi(x) = \pi(x^{1/2}) - 1 + \lfloor x\rfloor - \sum_{p_i\leq x^{1/2}} \left\lfloor \frac{x}{p_i}\right\rfloor + \sum_{p_i<p_j\leq x^{1/2}} \left\lfloor \frac{x}{p_ip_j}\right\rfloor - \sum_{p_i<p_j<p_k\leq x^{1/2}} \left\lfloor \frac{x}{p_ip_jp_k}\right\rfloor + \cdots \quad (2.2)$$

Demostración. Por la siguiente Obs. 39,

$$\phi(x,\pi(x^{1/2})) = |\{\, p\in\mathbb{P} \mid x^{1/2}<p\leq x\,\}\cup\{1\}| = 1+|\{\, p\in\mathbb{P}\mid x^{1/2}<p\leq x\,\}|$$

Luego, $\pi(x)=\pi(x^{1/2})+|\{\, p\in\mathbb{P}\mid x^{1/2}<p\leq x\,\}| = \pi(x^{1/2})-1+\phi(x,\pi(x^{1/2}))$ □

Observación 39. Obsérvese que si $n\leq x$ no tiene divisores propios menores o iguales que $\sqrt{x}$, entonces $n\in\mathbb{P}$ o bien es la unidad. En efecto, si $n=pq$ es compuesto con divisores propios $p,q>\sqrt{x}$, entonces $n>x$.

El siguiente resultado nos ofrece algunas herramientas alternativas para hallar $\phi(x,a)$.

Proposición 40. (a) *La función $\phi(x,a)$ sigue esta recurrencia:*

$$\phi(x,a) = \phi(x,a-1) - \phi\left(\frac{x}{p_a}, a-1\right)$$

(b) *Sea $m_k=\prod_{1\leq j\leq k} p_j$ el producto de los primeros k números primos. Entonces se tiene que $\phi(m_k,k)=\prod_{1\leq j\leq k}(p_j-1)=\varphi(m_k)$*

(c) *$\phi(m_k-1,k)=\phi(m_k,k)=\varphi(m_k)$. En general si x es par, $\phi(x,k)=\phi(x-1,k)$ para $k\geq 1$.*

(d) *$\phi(sm_k+t,k)=s\varphi(m_k)+\phi(t,k)$, con $0\leq t<m_k$*

(e) *$\phi(t,k)=\varphi(m_k)-\phi(m_k-t-1,k)$, si $m_k/2<t<m_k$*

Demostración. (a) Por definición, $\phi(x,a-1)$ cuenta los números menores o iguales que x no divisibles por los primeros $a-1$ primos. Este conjunto es la unión disjunta de dos subconjuntos: el de los menores o iguales que x no divisibles por los primeros a primos y el de los menores o iguales que x tales que $n=mp_a$ con $m\leq x/p_a$ no divisible por los primeros $a-1$ primos. Tomando cardinales de los subconjuntos y sumándolos, la recurrencia está demostrada.

(b) Como m_k es producto de los primeros k primos, el hecho de que $n \leq m_k$ no sea divisible por los primeros k primos equivale a que $mcd(m_k, n) = 1$. Tomando cardinales de estos conjuntos iguales y aplicando propiedades de la φ de Euler, se tiene que $\phi(m_k, k) = \varphi(m_k) = \prod_{1 \leq j \leq k}(p_j - 1)$

(c) Inmediato.

(d) Notar que $p_i \mid n \Leftrightarrow p_i \mid sm_k + n$, $\forall s \in \mathbb{N}$, $1 \leq i \leq k$. Entonces se sigue que $\phi(sm_k, k) = \phi((s-1)m_k, k) + \phi(m_k, k)$ ya que $(s-1)m_k < (s-1)m_k + n \leq sm_k$ divisible por algún p_i equivale a que $p_i \mid n$. Por inducción, se llega a $\phi(sm_k, k) = s\phi(m_k, k)$ y análogamente, $\phi(sm_k + t, k) = \phi(sm_k, k) + \phi(t, k)$. Combinando estas dos últimas igualdades y aplicando (b), se tiene el resultado.

(e) Notar que $p_i \mid n \Leftrightarrow p_i \mid m_k - n$ para $1 \leq i \leq k$. En general, para $1 \leq t < m_k$, se cumple que $\phi(m_k, k) = \phi(m_k - t - 1, k) + \phi(t, k)$ ya que $m_k - t \leq n < m_k$ divisible por algún p_i equivale a que $p_i \mid (m_k - n)$ con $m_k - n \leq t$. Despejando $\phi(t, k)$ de la igualdad obtenida y aplicando (b), llegamos al resultado.

□

2.2. Funciones k-ésimas de cribado parcial $P_k(x, a)$: Método de Lehmer

En la fórmula de Legendre (ver 2.2) vimos que se necesita hallar $\phi(x, a_0)$ para calcular $\pi(x)$, donde $a_0 = \pi(x^{1/2})$. Viendo la recurrencia de la Prop. 40 (a), se propone elegir un $a < a_0$ para evaluar un $\phi(x, a)$ con más facilidad. Esto nos motiva a introducir la siguiente familia de funciones aritméticas, relacionada con $\phi(x, a)$.

Definición 41 (Función k-ésima de cribado parcial $P_k(x, a)$)**.** *Sean $x, a \in \mathbb{N}$ y fijado un $k \in \mathbb{N}$, definimos $P_k(x, a) = \left|\left\{ n \leq x \mid n = \prod_{1 \leq j \leq k} p_{m_j} \text{ con } p_{m_j} \in \mathbb{P},\ m_j > a \right\}\right|$; esto es, la cantidad de números menores o iguales que x que son el producto de exactamente k primos, posiblemente repetidos, y todos ellos mayores que p_a.*

Nota 42. La definición anterior se puede extender considerando que $P_0(x, a) = 1$ porque el 1 no es primo ni tiene factores primos.

Es inmediato que $\phi(x, a) = \sum_{k \geq 0} P_k(x, a) = 1 + \sum_{k \geq 1} P_k(x, a)$. Entonces, dado que $P_1(x, a) = \pi(x) - a$, esto es, $P_1(x, a)$ cuenta los primos p tales que $p_a < p \leq x$,

$$\pi(x) = \phi(x, a) + a - 1 - \sum_{k \geq 2} P_k(x, a) \tag{2.3}$$

La siguiente proposición nos indica que esta suma tiene una cantidad finita de términos no nulos realmente.

Proposición 43. *Si a es tal que $x^{1/r} < p_{a+1}$ para un cierto $r \geq 2$ natural, en particular si $a = \pi(x^{1/r})$, entonces $P_k(x, a) = 0$ para $k \geq r$.*

Demostración. Notar que, por definición, $P_k(x, a)$ cuenta los naturales $n = p_{i_1} p_{i_2} \cdots p_{i_k} \leq x$ con $a + 1 \leq i_1 \leq i_2 \leq \cdots \leq i_k$. Si $k \geq r$, entonces $n > (x^{1/r})^r = x$ y por tanto, $P_k(x, a) = 0$. □

Obsérvese que si $a = \pi(x^{1/2})$, entonces (2.3) es la fórmula de Legendre (ver (2.2)), donde los $P_k(x, a)$ son todos nulos para $k \geq 2$. Meissel utilizó $a = \pi(x^{1/3})$. Lehmer tomó $a = \pi(x^{1/4})$ para hallar $\pi(x)$, obteniendo que

$$\pi(x) = \phi(x, a) + a - 1 - P_2(x, a) - P_3(x, a) \tag{2.4}$$

Para calcular $\pi(x)$ por el método de Lehmer con la fórmula (2.4), necesitamos una forma de calcular explícitamente $P_2(x, a)$ y $P_3(x, a)$.

Proposición 44. *Sea $x > 0$ y $a \in \mathbb{N}$. Entonces, para todo $k \in \mathbb{N}$, se tiene la siguiente recurrencia.*

$$P_k(x,a) = \sum_{i>a} P_{k-1}\left(\frac{x}{p_i}, i-1\right)$$

Demostración. Sabemos que $P_k(x,a) = \left|\left\{ n \leq x \mid n = \prod_{1\leq j\leq k} p_{i_j} \text{ con } p_{i_j} \in \mathbb{P},\, i_j > a \right\}\right|$. Separando este conjunto en subconjuntos disjuntos donde en cada uno de ellos se fija el primero de los factores primos, p_{i_1}, con $p_{i_1} > p_a$, obtenemos que

$$P_k(x,a) = \sum_{i_1>a} \left|\left\{ n \leq x \mid n = p_{i_1} \prod_{2\leq j\leq k} p_{i_j} \text{ con } p_{i_j} \in \mathbb{P},\, i_1 \leq i_2 \leq \cdots \leq i_k \right\}\right|$$

donde el cardinal del subconjunto correspondiente al fijado primo p_{i_1} en el sumatorio anterior es $P_{k-1}(x/p_{i_1}, i_1 - 1)$. Por tanto, tenemos la recurrencia. □

Nota 45. Notar que en la recurrencia de Prop. 44 el sumatorio tiene realmente una cantidad finita de términos no nulos; ya que si $i > \pi(x^{1/k})$, entonces

$$x^{1/k} < p_i \Leftrightarrow x < p_i^k \Leftrightarrow \left(\frac{x}{p_i}\right)^{1/(k-1)} < p_i = p_{(i-1)+1}$$

y, por Prop. 43, $P_{k-1}(x/p_i, i-1) = 0$.

Proposición 46. (a) *Sea $x > 0$ y $a \in \mathbb{N}$ tal que $a < \pi(x^{1/2}) \equiv b$, entonces se tiene que*

$$P_2(x,a) = -\frac{(b-a)(b+a-1)}{2} + \sum_{a+1\leq i\leq b} \pi\left(\frac{x}{p_i}\right) = -\frac{(b-a)(b+a-1)}{2} + \sum_{p_a<p\leq x^{1/2}} \pi\left(\frac{x}{p}\right)$$

(b) *Sea $x > 0$ y $a \in \mathbb{N}$ tal que $a < \pi(x^{1/3}) \equiv c$, entonces se tiene que*

$$P_3(x,a) = \sum_{a+1\leq i\leq c} P_2\left(\frac{x}{p_i}, i-1\right) = \sum_{a+1\leq i\leq c} \sum_{i\leq j\leq b_i} \left(\pi\left(\frac{x}{p_i p_j}\right) - (j-1)\right),$$

donde $b_i = \pi(\sqrt{x/p_i})$.

Demostración. Basta aplicar la recurrencia de Prop. 44 para llegar a las fórmulas.

(a)

$$P_2(x,a) = \sum_{a+1\leq i\leq b} P_1\left(\frac{x}{p_i}, i-1\right) = \sum_{a+1\leq i\leq b} \left[\pi\left(\frac{x}{p_i}\right) - (i-1)\right] = \sum_{p_a<p\leq x^{1/2}} \pi\left(\frac{x}{p}\right) - \sum_{a\leq i\leq b-1} i$$

Realizando la suma de una progresión aritmética, se tiene el resultado.

(b) Se obtiene de forma análoga.

□

Observación 47. (a) Si $p_a < p \leq x^{1/2}$, entonces $x^{1/2} \leq x/p < x/p_a$. Esta desigualdad nos indica que para hallar $P_2(x,a)$, basta calcular los primos hasta x/p_a.

(b) Si $p_a < p_i \leq x^{1/3}$, se tiene que $x^{1/3} \leq \sqrt{x/p_i} < \sqrt{x/p_a}$. Más aún, si $p_i \leq p_j \leq \sqrt{x/p_i}$, tenemos que

$$p_a < p_i \leq p_j \leq \sqrt{\frac{x}{p_i}} < \sqrt{\frac{x}{p_a}}$$

$$\sqrt{\frac{p_a}{x}} < \sqrt{\frac{p_i}{x}} \leq \frac{1}{p_j} \leq \frac{1}{p_i} < \frac{1}{p_a}$$

Aprovechando estas desigualdades, podemos obtener la siguiente cadena de desigualdades.

$$x^{1/3} \leq \sqrt{\frac{x}{p_i}} \leq \frac{x}{p_i p_j} < \frac{x}{p_a p_i} < \frac{x}{p_a^2}$$

Esto nos indica que para hallar $P_3(x, a)$, basta calcular los primos hasta x/p_a^2.

(c) En particular, si $a = \pi(x^{1/4})$, necesitamos una lista de primos hasta $x^{3/4}$ para calcular $P_2(x, a)$ y hasta $x^{1/2}$ para calcular $P_3(x, a)$.

2.3. Algoritmos y coste computacional

El cálculo de $\pi(x)$ a partir de la igualdad de Lehmer (Ec. (2.4)) necesita algoritmos que resuelvan las tareas siguientes:

1. Calcular $a = \pi(x^{1/4})$ y, al menos, la lista de los a primeros primos.
2. Calcular $\phi(x, a)$, utilizando la lista de los a primeros primos como dato de entrada adicional.
3. Calcular $P_2(x, a)$ y $P_3(x, a)$.

Para la primera tarea; utilizamos el método de la *Criba de Eratóstenes*, donde calculamos todos los primos menores o iguales que x. Dicho método usa una $(x-1)$-tupla v de enteros cuyas componentes están indexadas con $2 \leq p \leq x$. Finalizado el proceso, $v[p] = 0 \Leftrightarrow p \in \mathbb{P}$. Al principio, todas las componentes de v tienen valor 0 y se le asigna el valor 2 al índice p (línea 2). Se cambian a 1 todas las componentes cuyos índices son múltiplos propios de p menores o iguales que x. Para ello, por la Obs. 39, basta recorrer secuencialmente los índices $p^2 + kp \leq x$, con $k \in \mathbb{N} \cup \{0\}$ (líneas 5–7). Una vez recorrido los índices pares; a p se le asigna el valor del primer índice cuya componente es 0, que debe ser primo por Obs. 39, y se criba de forma análoga con dicho p. Es decir; que el proceso se repite con el siguiente primo (esto es, el menor índice $q > p$ tal que $v[q] = 0$) hasta alcanzar uno mayor que $\sqrt{x}$ (líneas 8–11). Los números primos se obtienen extrayendo de la tupla los índices p tales que $v[p] = 0$ y con ello, podemos hallar $\pi(x)$ contando dichos primos.

Teorema 48. *El algoritmo de la criba de Eratóstenes (Alg. (1)) tiene un coste en tiempo $T(x) \in O(x \log\log(x))$ y en memoria $M(x) \in O(x)$, donde x es el dato de entrada del algoritmo.*

Demostración. La sentencia crítica de este algoritmo, la operación que más veces se ejcuta, se encuentra en la línea 6: el cribado de los múltiplos de los primos menores o iguales que $\sqrt{x}$ que son menores o iguales que x. Dado un p, el número de éstos es exactamente $\lfloor x/p \rfloor$, por lo que una cota superior para el coste en tiempo es

$$\sum_{p \leq \sqrt{x}} \frac{x}{p} = x \sum_{p \leq \sqrt{x}} \frac{1}{p} = O(x \log\log(\sqrt{x})) = O(x \log\log(x))$$

Como el algoritmo utiliza un array de x componentes, entonces $M(x) \in O(x)$. □

Algorithm 1 Criba de Eratóstenes

Entradas: $x \in \mathbb{N}$ tal que $x \geq 2$.

Salidas:

- L, la lista ordenada de primos de $\{\, p \leq x \mid p \in \mathbb{P} \,\}$.
- πx, la longitud de L.

```
1:  procedure ERATÓSTENES(x ∈ ℕ tal que x ≥ 2)
2:      v[2..x] ← 0; p ← 2; sqr2x ← ⌊√x⌋
3:      while p ≤ sqr2x do
4:          j ← p^2
5:          while j ≤ x do
6:              v[j] ← 1; j ← j + p
7:          end while
8:          p ← p + 1
9:          while v[p] = 1 do
10:             p ← p + 1
11:         end while
12:     end while
13:
14:     πx ← 0; L ← ∅;
15:     j ← 2
16:     while j ≤ x do
17:         if v[j] = 0 then
18:             πx ← πx + 1; L ← L ∪ [j]
19:         end if
20:         j ← j + 1
21:     end while
22:     return L, πx
23: end procedure
```

Nota 49. Podemos reducir el espacio utilizado en la criba de Eratóstenes. En lugar de una x-tupla, podemos usar una $(x/2)$-tupla porque los pares son múltiplos de 2 (el primer primo). En esta $(x/2)$-tupla sus componentes se corresponden a los números impares mayores o iguales que 3 hasta x y el cribado empieza con los múltiplos propios impares de 3. Aún así, el coste en memoria sigue siendo de $M(x) \in O(x)$. Se puede mejorar el algoritmo cribando $[1, x]$ por subintervalos de longitud $\lfloor\sqrt{x}\rfloor$, de la forma $[(k-1)\lfloor\sqrt{x}\rfloor + 1, k\lfloor\sqrt{x}\rfloor]$ con $1 \leq k \leq \lfloor\sqrt{x}\rfloor + 1$. Se criba totalmente $[1, \lfloor\sqrt{x}\rfloor]$ para hallar los primos menores o iguales que $\sqrt{x}$ y se criba "parcialmente" los otros subintervalos para obtener el resto de los primos. Se puede ver que $M(x) \in O(máx\{\sqrt{x}, \pi(x)\})$.

A partir de la recurrencia de Prop. 40 (a), vamos a calcular $\phi(x, a)$ utilizando la lista de los a primeros primos. La recurrencia genera un árbol binario formado por nodos de la forma $\phi(y, b)$, donde $y = \lfloor x/\prod_j p_{i_j}\rfloor$ con $p_{i_j} > p_b$. Las hojas del árbol cumplen $y \leq p[b]$ o bien $b = 0$ (ver Obs. 35). Así, cada nodo $\phi(x/n, b)$ tiene asociado de forma única el par ordenado (n, b) donde $n = \prod_j p_{i_j}$, esto es, un producto de primos distintos.

Algorithm 2 Cálculo de $\phi(x, a)$

Entradas:

- $x \in \mathbb{N}$, $a \in \mathbb{N} \cup \{0\}$.
- $P = [p[j]]_{j\geq 1}$, la lista ordenada de los primeros (al menos a) primos.

Salidas: El valor de $\phi(x, a)$.

```
1: procedure PHI(x ∈ ℕ, a ∈ ℕ, P)
2:     if a = 0 then
3:         return x
4:     else if x ≤ p[a] then
5:         return 1
6:     else
7:         return PHI(x, a − 1, P) − PHI(⌊x/p[a]⌋, a − 1, P)
8:     end if
9: end procedure
```

Teorema 50. *El algoritmo del cálculo de $\phi(x, a)$ (Alg. (2)) tiene un coste en tiempo $T(x, a) \in O(x)$ y en memoria $M(x, a) \in O(a)$.*

Demostración. Puesto que cada nodo $\phi(x/n, b)$ está asociado a un par ordenado (n, b), donde $n \leq x$ es un producto de primos distintos, dicho número de nodos debe ser menor o igual que x; esto es, $O(x)$ es una cota superior del coste en tiempo para calcular $\phi(x, a)$.

Para hallar $\phi(x, a)$, por Alg. (2), tenemos que hacer dos llamadas recursivas (línea 7). Sin embargo, la segunda llamada no empezará a evaluarse hasta que la primera esté evaluada. Luego, realizamos a llamadas recursivas simultáneas a lo sumo por la altura del árbol generado. Por tanto, una cota superior del coste en memoria es $O(a)$.

□

Teorema 51. *Si tomamos $a = \pi(x^{1/r})$ y cumple que $a \geq r$, con $r \geq 2$ natural, entonces el coste en tiempo para calcular $\phi(x, a)$ está acotado inferiormente por*

$$T(x, a) \in \Omega\left(\frac{x}{\log^r(x)}\right)$$

Demostración. Primero, teniendo que

$$a \geq r = \frac{r(r-1)}{r-1} = \frac{r^2 - r}{r-1},$$

se llega fácilmente a la siguiente desigualdad.

$$a - r + 1 \geq \frac{a}{r} \tag{2.5}$$

Como $\phi(x, a)$ está formado por términos de la forma $\lfloor x/n \rfloor$ (ver 2.1), con $n = \prod_{p_{i_j} \leq p_a \leq x^{1/r}} p_{i_j}$, entonces $n = p_{i_1} p_{i_2} \cdots p_{i_r} \leq (x^{1/r})^r = x$ para primos $p_{i_j} \leq p_a \leq x^{1/r}$. Luego, $\phi(x, a)$ tiene al menos $\binom{a}{r}$ términos. Dicho número de términos se puede acotar inferiormente aplicando la desigualdad obtenida en 2.5.

$$\binom{a}{r} = \frac{a(a-1)(a-2)\cdots(a-r+1)}{r!} \geq \frac{(a-r+1)^r}{r!} \geq \frac{a^r}{r^r}\frac{1}{r!}$$

Sabiendo que $a = \pi(x^{1/r})$, por 29, existe un $c > 0$ constante tal que

$$a \geq \frac{crx^{1/r}}{\log(x)}$$

Finalmente, llegamos a que

$$\binom{a}{r} \geq \frac{\frac{(cr)^r x}{\log^r(x)}}{r! r^r} = \frac{c^r}{r!}\frac{x}{\log^r(x)} \tag{2.6}$$

□

Observación 52. En el método de Lehmer, dado que $a = \pi(x^{1/4})$, la desigualdad 2.6 se cumple para $x \geq p_a^4 \geq p_4^4 = 7^4 = 2401$, ya que $a \geq 4$.

Nota 53. Para el cálculo de $\phi(x, a)$; podemos añadir $a = 1$ (ver 35) y $a = 2$ a los casos base de la recurrencia de Alg. (2), cuyas fórmulas son las siguientes (por el teorema 36).

$$\phi(x, 1) = x - \lfloor (x/2) \rfloor$$

$$\phi(x, 2) = x - \lfloor (x/2) \rfloor - \lfloor (x/3) \rfloor + \lfloor (x/6) \rfloor$$

Así, las llamadas recursivas se detendrán a lo sumo hasta $a_0 = 2$ si $a > a_0$. Luego, la altura de este árbol es de $a - 2$.

También podemos implementar en el algoritmo las propiedades de Prop. 40, necesitando de una tabla que tenga calculados los valores de $\phi(x, a_1)$ para los x menores o iguales que $m_{a_1}/2$, con m_{a_1} el producto de los primero a_1 primos y fijando un $a_1 \leq a$. Así, las llamadas recursivas se detendrán como máximo hasta a_1 si $a > a_1$. Luego, la nueva altura del árbol es de $a - a_1$.

Para hallar $P_2(x, a)$ y $P_3(x, a)$, vamos a utilizar las fórmulas de la Prop. 46 y necesitamos una lista ordenada P de primos hasta un cierto K (ver Obs. 47). Supongamos que tenemos disponible una función $smallpi(x, P)$ que nos devuelve el valor de $\pi(x)$ si $x \leq K$. Dicha función puede ser implementada utilizando una búsqueda binaria.

Teorema 54. *El algoritmo presentado para el cálculo de $P_2(x, a)$ (Alg. (3)) tiene un coste en tiempo*

$$T(x, a) \in O\left(\frac{x^{1/2}}{\log(x)} \log\left(\frac{x/p_a}{\log(x/p_a)}\right)\right)$$

y en memoria

$$M(x, a) \in O\left(\frac{x/p_a}{\log(x/p_a)}\right)$$

Algorithm 3 Cálculo de $P_2(x, a)$

Entradas:

- $x \in \mathbb{N}$, $a \in \mathbb{N}$.
- $P = [p[j]]_{j \geq 1}$, la lista ordenada de los primeros (al menos $a+1$) primos y hasta x/p_a.

Salidas: El valor de $P_2(x, a)$.

```
1: procedure P2(x ∈ ℕ, a ∈ ℕ, P)
2:     Q ← √x
3:     if Q < p[a + 1] then
4:         return 0
5:     else
6:         b ← smallpi(Q, P); S ← 0; i ← a + 1
7:         while i ≤ b do
8:             S ← S + smallpi(x/p[i], P); i ← i + 1
9:         end while
10:        return S + (a − b)(a + b − 1)/2
11:    end if
12: end procedure
```

Demostración. Primero, veamos el coste en tiempo. Sabemos que realizar una búsqueda binaria de un elemento en una lista ordenada de m elementos tiene un coste $O(\log(m))$. Como vemos en Alg. (3), se hace una primera búsqueda binaria en la lista P que contiene del orden de $(x/p_a)/\log(x/p_a)$ primos (por 29) para hallar $b = \pi(x^{1/2})$, con coste $O(L(x, a))$ donde $L(x, a) = \log\left(\frac{x/p_a}{\log(x/p_a)}\right)$. Teniendo en cuenta que la operación más repetitiva (línea 8) es hacer las $b - a$ búsquedas binarias en P, siendo $b \in O(x^{1/2}/\log(x))$ (por 29), en total se han hecho $b - a + 1$ búsquedas binarias en el algoritmo. Luego, el coste total es de $O((b - a + 1)L(x, a))$ y debido a que $a < \pi(x^{1/2})$, se tiene que

$$O((b - a + 1)L(x, a)) \subseteq O\left(\frac{x^{1/2}}{\log(x)} L(x, a)\right).$$

El algoritmo almacena principalmente la lista P, por lo que el coste en memoria es de $O((x/p_a)/\log(x/p_a))$. □

Nota 55. En particular, tomando $a = \pi(x^{1/4})$ (Lehmer), necesitamos la lista de primos hasta $x^{3/4}$ y los costes obtenidos para $P_2(x, a)$ se pueden acotar superiormente por

$$T(x) \in O\left(\frac{x^{1/2}}{\log(x)} \log\left(\frac{x^{3/4}}{\log(x)}\right)\right) \subseteq O(x^{1/2})$$

$$M(x) \in O\left(\frac{x^{3/4}}{\log(x)}\right)$$

Teorema 56. *El algoritmo presentado para el cálculo de $P_3(x, a)$ (Alg. (4)) tiene un coste en tiempo*

$$T(x, a) \in O\left(\frac{x^{1/3}\sqrt{x/p_a}}{\log^2(x)} \log\left(\frac{x/p_a^2}{\log(x)}\right)\right)$$

Algorithm 4 Cálculo de $P_3(x,a)$

Entradas:

- $x \in \mathbb{N}$, $a \in \mathbb{N}$.
- $P = [p[j]]_{j\geq 1}$, la lista ordenada de los primeros (al menos $a+1$) primos y hasta x/p_a^2.

Salidas: El valor de $P_3(x,a)$.

```
1: procedure P3(x ∈ ℕ, a ∈ ℕ, P)
2:     CB ← x^{1/3}
3:     if CB < p[a+1] then
4:         return 0
5:     else
6:         c ← smallpi(CB, P); S ← 0; i ← a+1
7:         while i ≤ c do
8:             S ← S + P2(⌊x/p[i]⌋, i−1, P); i ← i+1
9:         end while
10:        return S
11:    end if
12: end procedure
```

y en memoria

$$M(x,a) \in O\left(\frac{x/p_a^2}{\log(x/p_a^2)}\right)$$

Demostración. Primero, veamos el coste en tiempo. Como vemos en Alg. (4), se hace una primera búsqueda binaria en la lista P que contiene del orden de $(x/p_a^2)/\log(x/p_a^2)$ primos (por 29) para hallar $c = \pi(x^{1/3})$, con coste $O(N(x,a))$ donde $N(x,a) = \log\left(\frac{x/p_a^2}{\log(x/p_a^2)}\right)$.

Teniendo en cuenta que la sentencia más repetitiva (línea 8) es el cálculo de los P_2, entonces una cota superior para su coste en tiempo es de

$$\sum_{a+1\leq i\leq c} \frac{\sqrt{x/p_i}}{\log(x/p_i)} \log\left(\frac{x/(p_i p_{i-1})}{\log(x/(p_i p_{i-1}))}\right) \leq (c-a)\frac{\sqrt{x/p_a}}{\log(x^{2/3})} \log\left(\frac{x/p_a^2}{\log(x^{1/3})}\right);$$

siendo $c \in O(x^{1/3}/\log(x))$ (por 29).

Sumando todos los costes y simplificando; debido a que $a < \pi(x^{1/3})$; se tiene que

$$O(N(x,a)) + O\left((c-a)\frac{\sqrt{x/p_a}}{\log(x^{2/3})} \log\left(\frac{x/p_a^2}{\log(x^{1/3})}\right)\right) = O\left(\frac{x^{1/3}\sqrt{x/p_a}}{\log^2(x)} \log\left(\frac{x/p_a^2}{\log(x)}\right)\right)$$

El algoritmo almacena principalmente la lista P, por lo que el coste en memoria es de $O((x/p_a^2)/\log(x/p_a^2))$. □

Nota 57. En particular, tomando $a = \pi(x^{1/4})$ (Lehmer), necesitamos la lista de primos hasta $x^{1/2}$ y los costes obtenidos para $P_3(x,a)$ se pueden acotar superiormente por

$$T(x) \in O\left(\frac{x^{1/3}x^{3/8}}{\log^2(x)} \log\left(\frac{x^{1/2}}{\log(x)}\right)\right) = O\left(\frac{x^{17/24}}{\log^2(x)} \log\left(\frac{x^{1/2}}{\log(x)}\right)\right) \subseteq O\left(\frac{x^{17/24}}{\log(x)}\right)$$

$$M(x) \in O\left(\frac{x^{1/2}}{\log(x)}\right)$$

Algorithm 5 Cálculo de $\pi(x)$ por el método de Lehmer

Entradas: $x \in \mathbb{N}$ con $x \geq 2$.
Salidas: El valor de $\pi(x)$.

```
1: procedure LEHMER(x ∈ ℕ)
2:     R ← x^{1/4}
3:     [P, z] ← ERATÓSTENES(R^3); a ← smallpi(R, P)
4:     return PHI(x, a, P) + a − 1 − P2(x, a, P) − P3(x, a, P)
5: end procedure
```

Teorema 58. *El método de Lehmer visto en Alg. (5) para calcular $\pi(x)$ tiene un coste en tiempo $T(x) \in O(x)$ y en memoria $M(x) \in O\left(\frac{x^{3/4}}{\log(x)}\right)$.*

Demostración. Como dicho método requiere realizar los cálculos mencionados en 2.3, entonces el coste en tiempo se obtiene tomando el máximo de los costes en tiempo del cálculo de $\phi(x, a)$, $P_2(x, a)$ y $P_3(x, a)$ (ver 50, 55, 57). Luego, $T(x) \in O(x)$. Análogamente, obtenemos también el coste en memoria. □

Nota 59. Podemos optimizar el coste del método de Lehmer realizando cribas parciales de los subintervalos de longitud $\lfloor x^{1/4} \rfloor$, de la forma $[(k-1)\lfloor x^{1/4} \rfloor + 1, k\lfloor x^{1/4} \rfloor]$ con $1 \leq k \leq \lfloor \sqrt{x} \rfloor + 1$ en lugar de cribar directamente $[1, x^{3/4}]$.

Una pregunta que nos podemos plantear es si el coste de calcular $\pi(x)$ se reduce tomando $a = \pi(x^{1/r})$, con $r \geq 5$ natural. Para ello; necesitamos la lista de primos hasta $x^{(r-1)/r}$ y calcular unos $P_k(x, a)$ de más hasta $k = r - 1$, cribando parcialmente subintervalos longitud $\lfloor x^{1/r} \rfloor$, de la forma $[(k-1)\lfloor x^{1/r} \rfloor + 1, k\lfloor x^{1/r} \rfloor]$ con $1 \leq k \leq \lfloor x^{(r-2)/r} \rfloor + 1$. A medida que aumentamos el valor de r, nos damos cuenta que cribamos gran parte del intervalo $[1, x]$ y que para calcular los $P_k(x, a)$, necesitamos realizar bastantes llamadas recursivas.

Bibliografía

[1] Tom M. Apostol. *Introduction to analytic number theory.* Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976.

[2] Hans Riesel. *Prime numbers and computer methods for factorization.* Modern Birkhäuser Classics. Reprint of the second (1994) edition. Birkhäuser/Springer, New York, 2012.

[3] D. H. Lehmer. "On the exact number of primes less than a given limit". En: *Illinois J. Math.* 3 (1959), págs. 381-388.

[4] J. C. Lagarias, V. S. Miller y A. M. Odlyzko. "Computing $\pi(x)$: the Meissel-Lehmer method". En: *Math. Comp.* 44.170 (1985), págs. 537-560.