1. Recordando

Criba combinatoria:

Hallar $\mathcal{D}^-, \mathcal{D}^+ \subset [1, D]$ tales que

$$\sum_{\substack{d|P(z)\\ d\in\mathcal{D}^-}} \mu(d)|A_d| \leq S(A,z) \leq \sum_{\substack{d|P(z)\\ d\in\mathcal{D}^+}} \mu(d)|A_d|.$$

$XV^-(z) + R^- \leq S(A,z) \leq XV^+(z) + R^+$

Identidad de Buchstab:

$$|A| = S(A,z) + \sum_{p<z} S(A_p, p)$$

todos — sin factores $< z$ — menor factor $= p$

$$1 = V(z) + \sum_{p<z} \frac{\rho(p)}{p} V(p)$$

Prob no factor $p < z$ — Prob menor factor $= p$

2. Pidiendo

$z = X^{\text{algo}}, \quad D = X^{\text{algo mayor}}$

Notación: $s = \frac{\log D}{\log z} > 1, \quad z^s = D$

Esperamos:

$$f(s)XV(z) - E \leq S(A,z) \leq F(s)XV(z) + E$$

Digamos que

$$V(z) \sim \frac{\text{Cte}}{\log^{\kappa} z} \qquad \text{supongamos } \kappa = 1 \text{ (criba lineal)}$$

Queremos que el error no engulla al término principal:

$$E = \sum_{\substack{d|P(z) \\ d \leq D}} |r_d| \ll \frac{X}{\log^2 X}$$

$$z = p, \ A_p \ \Rightarrow \ s_p = \frac{\log D/p}{\log p} = \frac{\log D}{\log p} - 1$$

3. Soñando

$$\left.\begin{array}{l} V(z) = \mathrm{Cte}/\log z \\ 1 = V(z) + \sum_{p<z} \frac{\rho(p)}{p} V(p) \end{array}\right\} \Rightarrow -\frac{\rho(t)}{t} V(t) = \Delta\big(\frac{\mathrm{Cte}}{\log t}\big)$$

$$S(A,z) = X - \sum_{p<z} S(A_p, p)$$

$$\lesssim X - \sum_{p<z} f\big(\frac{\log D/p}{\log p}\big) X \frac{\rho(p)}{p} V(p)$$

$$= XV(z)\left(1 + \frac{1}{V(z)} \sum_{p<z} \big(1 - f(\frac{\log D}{\log t} - 1)\big) \frac{\rho(p)V(p)}{V(z)}\right)$$

$$\approx XV(z)\left(1 + \frac{1}{V(z)} \int_1^z \big(1 - f(\frac{\log D}{\log t} - 1)\big)\ d\big(\frac{\mathrm{Cte}}{\log t}\big)\right)$$

$$= XV(z)\left(1 + \frac{1}{s} \int_s^\infty \big(1 - f(t-1)\big)\ dt\right)$$

f cota inferior $\Rightarrow F(s) = 1 + \frac{1}{s}\int_s^\infty \ldots$ cota superior
$(sF(s))' = f(s-1)$.

Problema de ecuaciones diferenciales en diferencias

$$\left.\begin{array}{ll} (sF(s))' = f(s-1) & s > \beta + 1 \\ (sf(s))' = F(s-1) & s > \beta \\ F(\infty) = f(\infty) = 1 & \\ 0 \leq f \leq F & \\ f(s) = 0 \Leftrightarrow s \leq \beta & \\ F(s) = A/s & s \leq \beta + 1 \end{array}\right\} \Rightarrow \begin{array}{l} A = 2e^{\gamma} \\ \quad = 3'56\ldots \\ \beta = 2 \end{array}$$

β=límite de criba (sieving limit)

Problema bueno

$$\text{(B)} \left\{\begin{array}{ll} (sF(s))' = f(s-1) & s > 3 \\ (sf(s))' = F(s-1) & s > 2 \\ f(s) = 0 \text{ si } s \leq 2 & \\ F(s) = 2e^{\gamma}/s \text{ si } s \leq 3 & \end{array}\right.$$

Dado un s se puede hallar fácilmente $f(s)$ y $F(s)$ iterando a partir de las condiciones iniciales.

4. Cribando

Para no acumular errores, tratamos de no sumar términos triviales, que suponemos que aparecen si $s > \beta = 2$.

$$S(A,z) = |A| - \sum_{p<z} S(A_p, p)$$

$$S(A_p,p) \gtrsim f(s_p)\frac{X\rho(p)}{p}V(p), \quad s_p > 2 \Rightarrow D/p > p^2$$

Por tanto, escribimos:

$$S(A,z) \leq |A| - \sum_{\substack{p<z \\ p^3<D}} S(A_p,p).$$

En la segunda iteración de Buchstab no podemos eliminar términos sin perder la desigualdad,

$$S(A,z) \leq |A| - \sum_{\substack{p_1<z \\ p_1^3<D}} |A_{p_1}| + \sum_{\substack{p_2<p_1<z \\ p_1^3<D}} S(A_{p_1p_2}, p_2).$$

Pero sí en la tercera:

$$S(A,z) \leq |A| - \sum_{\substack{p_1<z \\ p_1^3<D}} |A_{p_1}| + \sum_{\substack{p_2<p_1<z \\ p_1^3<D}} |A_{p_1p_2}| - \sum_{\substack{p_3<p_2<p_1<z \\ p_1^3<D,\ p_3^3p_2p_1<D}} S(A_{p_1p_2p_3}, p_3).$$

Iterando, probamos que

$$\begin{aligned}\mathcal{D}^+ &= \{p_1p_2\cdots p_m \ : \ p_m < p_{m-1} < \ldots < p_1, \\ &\quad p_{2r+1}^3 p_{2r}\cdots p_2p_1 < D \text{ para todo } 2r+1 \leq m\} \\ \mathcal{D}^- &= \{p_1p_2\cdots p_m \ : \ p_m < p_{m-1} < \ldots < p_1, \\ &\quad p_{2r}^3 p_{2r-1}\cdots p_2p_1 < D \text{ para todo } 2r \leq m\}\end{aligned}$$

definen una criba.

Gran problema:

Demostrar

$$\sum_{\substack{d|P(z) \\ d\in\mathcal{D}^-}} \mu(d)|A_d| \approx f(s)XV(z)$$

y

$$\sum_{\substack{d|P(z) \\ d\in\mathcal{D}^+}} \mu(d)|A_d| \approx F(s)XV(z)$$

El teorema

Una vez superado este obstáculo, el teorema fundamental sería:

Teorema 1 (Jurkat-Richter) *Supongamos* $\kappa = 1$ *y* f *y* F *soluciones de* (B)*, entonces:*

$$(f(s)-\epsilon)XV(z)-E \leq S(A,z) \leq (F(s)+\epsilon)XV(z)+E$$

donde ϵ *tiende a cero si* D *crece.*

Obs. 1: ϵ decae algo más lento que $(\log\log D)^{-1}$, con constantes que dependen de las de la definición de dimensión.

Obs. 2: El teorema se generaliza a todas las dimensiones $\kappa > 1/2$ cambiando el problema (B) por

$$\begin{cases} (s^\kappa F(s))' = \kappa s^{\kappa-1} f(s-1) \\ (s^\kappa f(s))' = \kappa s^{\kappa-1} F(s-1) \end{cases}$$

con ciertas condiciones iniciales y límite de criba β que dependen de κ (de una forma muy complicada).

Ideas en la prueba

• V_m "trozo" de $V(z)$ tal que la condición que define $\mathcal{D}^+$ y $\mathcal{D}^-$ falla para el m-ésimo mayor primo:

$$\sum_{\substack{d|P(z)\\ d\in\mathcal{D}^-}} \mu(d)\frac{\rho(d)}{d} = V(z) - \sum_{2|m} V_m(z)$$

y

$$\sum_{\substack{d|P(z)\\ d\in\mathcal{D}^+}} \mu(d)\frac{\rho(d)}{d} = V(z) + \sum_{2\not|m} V_m(z)$$

con

$$V_m(z) = \sum_{(p_1,p_2,\ldots,p_m)\in\mathcal{N}_m} \frac{\rho(p_1p_2\cdots p_m)}{p_1p_2\cdots p_m} V(p_m)$$

donde

$$\begin{aligned}\mathcal{N}_m \;=\; \big\{&(p_1,p_2,\ldots,p_m) \;:\; p_m<\ldots<p_1<z,\\ &p_m^3p_{m-1}\cdots p_1 \geq D,\\ &p_n^3p_{n-1}\cdots p_1 < D \text{ si } m-n=\text{par}>0\big\}\end{aligned}$$

• Sumación por partes (usando la definición de dimensión, $K\approx 1$) $\Rightarrow V_m(z)/V(z)\approx f_m(s) =$

$$\frac{1}{s}\int_{\substack{t_1+\cdots+t_{n-1}+3t_n<1 \text{ si } m-n=\text{par}>0\\ t_1+\cdots+t_{m-1}+3t_m\geq 1}} \quad t_1^{-1}\cdots t_{m-1}^{-1}t_m^{-2}\,dt_1\ldots\,dt_m$$

• Relaciones de recurrencia para V_m y $f_m \Rightarrow$

$$\sum_{\substack{m \leq M \\ m \equiv M \ (2)}} V_m(z) < V(z) \sum_{\substack{m \leq M \\ m \equiv M \ (2)}} f_m(s) + \texttt{Error}$$

`Error` es muy malo, crece exponencialmente en la constante K de la definición de criba.

• Podemos aproximar K a 1 a voluntad si sólo se consideran los primos grandes. Se dividen los primos entre los que cumplen $p \leq w$ y $p > w$ y se hace una composición de cribas. En los primeros primos la criba vendrá de aplicar el lema fundamental, y en los segundos se utilizará la fórmula anterior.

Los parámetros son:

- Truncación: $w = D^{-\epsilon/\log \epsilon}$
- Criba pequeña: nivel $= D^{\epsilon}$
- Criba grande: nivel $= D$

5. Practicando

$f(s) = 2e^{\gamma} s^{-1} \log(s-1)$ en $(2,4] \Rightarrow$ Cota inferior (no trivial siempre que $s > \beta$)

1) ¿Hay infinitos primos de la forma n^2+1?

$$A = \{n^2 + 1 \ : \ n \leq X\}$$

$$|A_p| = \{n^2 \equiv -1 \ (p) \ : \ n \leq X\} = X\frac{\rho(p)}{p} + r_p$$

$$\rho(p) = \begin{cases} 2 & \text{si } p \equiv 1 \ (4) \\ 0 & \text{si } p \equiv 3 \ (4) \\ 1 & \text{si } p = 2 \end{cases} \qquad V(z) \sim \frac{\text{Cte}}{\log z}$$

$D \ll X/\log^3 X \ \Rightarrow$ Error despreciable

$$s > 2 \qquad \Rightarrow \qquad S(A,z) \gg \frac{X}{\log X} \quad \text{con } z = X^{0'49}$$

Como $(X^{0'49})^5 > X^2 + 1$

Hay infinitos números de la forma n^2+1 con a lo más cuatro factores primos.

2) Detectando primos

$$A = \{1, 2, 3, \ldots, X\}$$

$S(A, x^{1/2+\epsilon}) \asymp X/\log X$ pero no podemos tratar el caso $\epsilon = 0$ que daría una cota inferior para $\pi(x)$.

3) Problema de paridad

$$\begin{aligned} A^0 &= \{n \leq 2X \ : \ 2 | \text{num. factores primos de } n\} \\ A^1 &= \{n \leq 2X \ : \ 2 \not| \text{num. factores primos de } n\} \end{aligned}$$

Selberg: $\quad z = x^{1/s} \quad (D \ll X)$

$$\begin{aligned} S(A^0, z) &= f(s)XV(z) + O(X/\log^2 X) \\ S(A^1, z) &= F(s)XV(z) + O(X/\log^2 X) \end{aligned}$$

¡El teorema es óptimo! A^0 y A^1 son indistinguibles desde el punto de vista de la criba. ($\rho^0(d)$ y $\rho^1(d)$ iguales con errores r_d^0, r_d^0 comparables) *Fenómeno de paridad*. Sin embargo son bien diferentes y A_0 ni siquiera contiene primos.

Entonces...¿no se puede ir más allá? ¿guardamos en el almacén los libros de criba? No se pierda las próximas *xerrades*.

Seminario de Criba. Barcelona 2005

1. Cribas combinatorias

La fórmula exacta de la criba de Eratóstenes-Legendre (inclusión-exlusión),

$$S(A,z) = \sum_{d|P(z)} \mu(d)|A_d|, \tag{1}$$

tiene una serie deficiencia, y es que el número de sumandos crece exponencialmente con z y por tanto en las aproximaciones $|A_d| = X\rho(d)/d + r(A,d)$ la acumulación de los términos de error $r(A,d)$ arruina el término principal excepto para z excesivamente pequeño.

Supongamos que sólo tenemos un control adecuado de los términos de error cuando $d < D$ con $D = z^s$, para algún $s > 1$; típicamente una cota de la forma

$$\sum_{\substack{d|P(z)\\ d<D}} |r(A,d)| \ll \frac{X}{\log^C X} \tag{2}$$

para $C > 0$ suficientemente grande, una vez establecida una cota para D en función de X.

La criba combinatoria consiste en despreciar en (1) los sumandos correspondientes a los valores de d que estén fuera de cierto subconjunto de $[1,D]$ (a D se le llama nivel de criba). Con ello perderemos la igualdad pero procediendo adecuadamente todavía podremos conseguir desigualdades.

Concretamente, dados dos subconjuntos $\mathcal{D}^+, \mathcal{D}^- \subset [1,D]$ para los que se verifique

$$\sum_{\substack{d|n\\ d\in\mathcal{D}^-}} \mu(d) \le \sum_{d|n} \mu(d) \le \sum_{\substack{d|n\\ d\in\mathcal{D}^+}} \mu(d)$$

se obtiene

$$\sum_{\substack{d|P(z)\\ d\in\mathcal{D}^-}} \mu(d)|A_d| \le S(A,z) \le \sum_{\substack{d|P(z)\\ d\in\mathcal{D}^+}} \mu(d)|A_d|. \tag{3}$$

La aproximación $A_d \approx X\rho(d)/d$ lleva comúnmente a términos principales comparables a $XV(z)$, salvo constantes dependiendo de s, y se siguen desigualdades del tipo

$$f(s)XV(z) + \texttt{error} \le S(A,z) \le F(s)XV(z) + \texttt{error}, \tag{4}$$

donde, como antes, $s = \log D/\log z$ (esto es, $D = z^s$), $s \ge 1$, y el error viene de (2).

2. La criba de Brun

La criba de Brun se basa en las desigualdades

$$\sum_{\substack{d|n\\ \omega(d)\leq 2k+1}} \mu(d) \leq \sum_{d|n} \mu(d) \leq \sum_{\substack{d|n\\ \omega(d)\leq 2k}} \mu(d) \qquad \text{con } \omega(d) = \text{n}^{\text{o}} \text{ de factores primos de } d,$$

De forma que $\mathcal{D}^-$ y $\mathcal{D}^+$ son subconjuntos de enteros con un número impar y par de factores primos, respectivamente.

Brun perfeccionó esta elección y probó algunos resultados notables (el más conocido es que la suma de los inversos de los primos gemelos converge). Como es de esperar, cuando $s \to \infty$, es decir cuando la restricción dada por el tamaño de D no se hace sentir, los términos principales en (4) se acercan al término esperado desde el punto de vista probabilista: $XV(z)$. A la cuantificación de esta propiedad se le suele llamar *lema fundamental*. Explícitamente, si K y κ son como en la definición de dimensión de criba:

$$\prod_{w\leq p<z} \big(1-\rho(p)/p\big)^{-1} \leq K(\log z/\log w)^{\kappa}, \tag{5}$$

una forma del lema fundamental afirma que para s suficientemente grande en comparación con κ, se cumple que $f(s)$ y $F(s)$ son $1+O\big(K^{10}e^{9\kappa-s}\big)$ con una constante O absoluta.

3. Las iteraciones de Buchstab

Buchstab introdujo la fórmula

$$S(A,z) = |A| - \sum_{p<z} S(A_p,p), \tag{6}$$

cuya demostración se reduce a notar que los elementos cribados están en alguno de los conjuntos contados por los $S(A_p,p)$ y que éstos son disjuntos. Una de las virtudes de esta fórmula es que permite transformar cotas inferiores en cotas superiores y viceversa. Pero sobre todo, permite en algunas ocasiones mejorar resultados de criba.

Procediendo sin rigor, se pueden anticipar los resultados de la criba β aplicando sucesivamente (6), éstas son las iteraciones de Buchstab. Antes de ilustrar este punto, nótese la fórmula

$$V(z) = 1 - \sum_{p<z} \frac{\rho(p)}{p} V(p) \tag{7}$$

que, aunque inmediata, podría considerarse una consecuencia de (6).

Supongamos que en (4) despreciamos el error (lo que indicamos empleando $\lesssim$ en lugar de $\leq$). Por (6)

$$S(A,z) \lesssim X - \sum_{p<z} f(s_p)\frac{X}{p}V(p)$$

donde $s_p = \log(D/p)/\log p = \log D/\log p - 1$. Empleando (7) esto se puede reescribir como

$$S(A,z) \lesssim XV(z)\left(1 + \sum_{p<z} \big(1 - f\big(\frac{\log D}{\log p} - 1\big)\big)\frac{\rho(p)}{p}\frac{V(p)}{V(z)}\right).$$

Si pudiéramos aplicar la definición de dimensión (5) con $K = 1$ e igualdad, por (7) se tendría que $-\rho(t)V(t)/t$ es el incremento de $\log^{-\kappa} t$ y $V(z)$ es como $\log^{-\kappa} z$ de modo que el paréntesis exterior se debería aproximar por

$$1 + \int_0^z \big(1 - f\big(\frac{\log D}{\log t} - 1\big)\big)\frac{d(\log^{-\kappa} t)}{\log^{-\kappa} z} = 1 + \kappa s^{-\kappa}\int_s^\infty (1 - f(t-1))t^{\kappa-1}\,dt$$

(esta igualdad se sigue del cambio $\log D/\log t \mapsto t$).

Lo mismo se aplica con la cota inferior. Si este proceso fuera "contractivo" en el límite se obtendría (4) con funciones f y F cumpliendo

$$F(s) = 1 + \kappa s^{-\kappa}\int_s^\infty (1 - f(t-1))t^{\kappa-1}\,dt, \quad f(s) = 1 + \kappa s^{-\kappa}\int_s^\infty (1 - F(t-1))t^{\kappa-1}\,dt,$$

o lo que es lo mismo

$$\begin{cases} (s^\kappa f(s))' = \kappa s^{\kappa-1}F(s-1) \\ (s^\kappa F(s))' = \kappa s^{\kappa-1}f(s-1) \end{cases} \tag{8}$$

Si todo este proceso se pudiera justificar, y supiéramos resolver las ecuaciones (8) con $f(\infty) = F(\infty) = 1$, tendríamos un candidato para desigualdad de criba óptima. Sin embargo, la acumulación de términos de error y las simplificaciones incorrectas, hacen de ello una tarea poco realista. En su lugar, veremos una criba combinatoria que permite alcanzar el límite de las iteraciones de Buchstab.

4. La criba β

Ciertamente no parece útil contemplar en las iteraciones de Buchstab rangos en los que las desigualdades de criba (4) sean triviales. Supongamos que existe un $\beta > 1$ a partir del cual la cota inferior en (4) deja de ser trivial, esto es, $f(\beta) = 0$ y $f(s) > 0$ para $s > \beta$. A este valor se le llama límite de criba (*sieving limit*).

El s correspondiente a $S(A_p, p)$ es $s_p = \log(D/p)/\log p$, y lo anterior sugiere desconsiderar en (6) los términos con $\beta \geq s_p$, obteniéndose

$$S(A,z) \leq |A| - \sum_{\substack{p<z \\ p^{\beta+1}<D}} S(A_p, p).$$

En la segunda iteración de Buchstab no podemos eliminar términos sin perder la desigualdad, por tanto tenemos simplemente

$$S(A,z) \leq |A| - \sum_{\substack{p_1<z \\ p_1^{\beta+1}<D}} |A_{p_1}| + \sum_{\substack{p_2<p_1<z \\ p_1^{\beta+1}<D}} S(A_{p_1p_2}, p_2).$$

Pero en la tercera iteración podemos eliminar los términos con $\beta \geq s_{p_1p_2p_3}$, donde $s_{p_1p_2p_3} = \log(D/p_1p_2p_3)/\log p_3$, y se tiene

$$S(A,z) \leq |A| - \sum_{\substack{p_1<z \\ p_1^{\beta+1}<D}} |A_{p_1}| + \sum_{\substack{p_2<p_1<z \\ p_1^{\beta+1}<D}} |A_{p_1p_2}| - \sum_{\substack{p_3<p_2<p_1<z \\ p_1^{\beta+1}<D,\ p_3^{\beta+1}p_2p_1<D}} S(A_{p_1p_2p_3}, p_3).$$

Razonamientos análogos dan lugar a cotas inferiores. Con ello hemos creado una criba combinatoria determinada por

$$\begin{aligned} \mathcal{D}^+ &= \{p_1p_2\cdots p_m \ : \ p_m < p_{m-1} < \ldots < p_1 \text{ y } p_{2r+1}^{\beta+1}p_{2r}\cdots p_2p_1 < D \text{ para } 2r+1 \leq m\} \\ \mathcal{D}^- &= \{p_1p_2\cdots p_m \ : \ p_m < p_{m-1} < \ldots < p_1 \text{ y } p_{2r}^{\beta+1}p_{2r-1}\cdots p_2p_1 < D \text{ para } 2r \leq m\} \end{aligned}$$

Ésta es la criba β (desarrollada por H. Iwaniec).

Al ser una criba combinatoria, se pueden controlar los términos de error bajo la condición (2) y se obtienen cotas del tipo

$$X \sum_{\substack{d|P(z) \\ d\in\mathcal{D}^-}} \mu(d)\frac{\rho(d)}{d} + \texttt{error} \leq S(A,z) \leq X \sum_{\substack{d|P(z) \\ d\in\mathcal{D}^+}} \mu(d)\frac{\rho(d)}{d} + \texttt{error}.$$

Ahora esperamos extraer de estos sumandos un factor $V(z)$ y acumular las cantidades sobrantes en las funciones f y F. Con tal fin escribimos cada sumatorio como $V(z)$ quitando los productos correspondientes a los elementos que no estén en $\mathcal{D}^-$ o en $\mathcal{D}^+$, y estos productos eliminados los clasificamos en diferentes sumatorios V_m, donde m indica que el m-ésimo mayor primo es el primero para el que falla la condición que define $\mathcal{D}^-$ y $\mathcal{D}^+$. Concretamente:

$$\sum_{\substack{d|P(z) \\ d\in\mathcal{D}^-}} \mu(d)\frac{\rho(d)}{d} = V(z) - \sum_{2|m} V_m(z) \quad \text{y} \quad \sum_{\substack{d|P(z) \\ d\in\mathcal{D}^+}} \mu(d)\frac{\rho(d)}{d} = V(z) + \sum_{2\not|m} V_m(z)$$

con

$$V_m(z) = \sum_{(p_1,p_2,\ldots,p_m)\in\mathcal{N}_m} \frac{\rho(p_1p_2\cdots p_m)}{p_1p_2\cdots p_m} V(p_m)$$

donde

$$\begin{aligned} \mathcal{N}_m = \big\{(p_1,p_2,\ldots,p_m) \ : \quad & p_m < \ldots < p_1 < z,\ p_m^{\beta+1}p_{m-1}\cdots p_1 \geq D, \\ & p_n^{\beta+1}p_{n-1}\cdots p_1 < D \text{ si } m-n = \text{par} > 0\big\} \end{aligned}$$

Como habíamos visto, la definición de dimensión de criba (5), suponiendo $K \approx 1$ y (7), sugiere que $-\rho(t)V(t)/t$ se comporta como el incremento de $\log^{-\kappa} t$, $V(z)$ como $\log^{-\kappa} z$ y $\rho(t)/t$ como el incremento de $\kappa \log\log t$. Así que una conjetura plausible es que

$$\frac{V_m(z)}{V(z)} \approx \log^{\kappa} z \int_{(t_1,\ldots,t_m)\in\mathcal{N}_m} \frac{\kappa\, dt_1}{t_1\log t_1} \cdot \frac{\kappa\, dt_2}{t_2\log t_2} \cdots \frac{\kappa\, dt_{m-1}}{t_{m-1}\log t_{m-1}}\, d(-\log^{-\kappa} t_m).$$

Con el cambio $\log t_j/\log D \mapsto u_j$ se sigue $V_m(z)/V(z) \approx f_m(s)$ donde

$$f_m(s) = \kappa^m s^{-\kappa} \int_{\substack{0<t_m<\ldots<t_1<1/s \\ t_1+\cdots+t_{n-1}+(\beta+1)t_n<1 \text{ si } m-n=\text{par}>0 \\ t_1+\cdots+t_{m-1}+(\beta+1)t_m\geq 1}} t_1^{-1}t_2^{-1}\cdots t_{m-1}^{-1}t_m^{-\kappa-1}\, dt_1\, dt_2 \ldots\, dt_m.$$

En definitiva, cabe esperar que se cumplan las desigualdades de criba (4) con

$$f(s) = 1 - \sum_{2|m} f_m(s) \qquad \text{y} \qquad F(s) = 1 + \sum_{2\not| m} f_m(s) \tag{9}$$

para $s > \beta$ con β el "último cero" de f.

5. El teorema de criba

Transformar las ideas del apartado anterior en un teorema es una tarea ardua.

Un punto básico es cuantificar la precisión de la aproximación de $V_m(z)/V(z)$ por $f_m(s)$ lo que lleva al problema aparentemente irresoluble de que el error acumulado tiende exponencialmente a infinito con el número de términos. En concreto, se puede probar que para $M \in \mathbb{Z}^+$

$$\sum_{\substack{m\leq M \\ m\equiv M\ (2)}} V_m(z) < V(z)\Bigg(\sum_{\substack{m\leq M \\ m\equiv M\ (2)}} f_m(s) + (K-1)M^2K^M\big(\frac{\beta+M}{\beta-1}\big)^{\kappa M}\Bigg) \tag{10}$$

donde K es como en (5).

La forma de llegar a (10) pasa por notar primero que escribiendo $z_m = D^{1/(\beta+m)}$ e $y_m = \text{mín}\left(z, D^{1/(\beta+\delta_m)}\right)$ con $\delta_m = (1-(-1)^m)/2$, se tiene

$$V_m(z) = \sum_{z_m\leq p<y_m} \frac{\rho(p)}{p} V_{m-1}(D/p, p) \qquad \text{si } \beta-\delta_m \leq s < \beta+m,$$

donde $V_{m-1}(D/p,p)$ es $V_{m-1}(p)$ cambiando D por D/p. Análogamente definiendo $s_m = \text{máx}(s, \beta+\delta_m)$ se tiene

$$s^\kappa f_m(s) = \kappa \int_{s_m}^{\beta+m} f_{m-1}(t-1)t^{\kappa-1}\, dt \qquad \text{si } \beta-\delta_m \leq s < \beta+m. \tag{11}$$

Evidentemente $V_m(z) = f_m(s) = 0$ si $s \geq \beta+m$. Para demostrar (10) se aplican estas fórmulas de recurrencia y sumación por partes completándose un proceso de inducción.

Incluso olvidando el crecimiento del error en (10), hay un problema de naturaleza más técnica pero en absoluto trivial, y es la convergencia de las series (9). Una vez supuesta para $s > \beta$, derivando (11) (nótese que $s_m = s$ para $s_m \geq \beta+\delta_m$) se puede deducir que las funciones (9) verifican (8). De hecho la convergencia se prueba definiendo unas soluciones de ecuaciones de este tipo que actúan como mayorantes. La determinación de β en función de κ, el único parámetro del que depende (11) y por tanto f y F, no es fácil.

Para $\kappa = 1$ (criba lineal) se tiene $\beta = 2$ y $\beta \approx 1 + 3'591\kappa$ para κ grande. De la segunda ecuación (8) se sigue $F(s) = A/s^\kappa$ donde la constante A también está determinada por κ (debido a la homogeneidad de (8) y la condición $F(\infty) = f(\infty) = 1$). De nuevo, no hay una fórmula sencilla para A pero se puede probar que para $\kappa = 1$ se tiene $A = 2e^\gamma = 3'562\ldots$ y $A \approx 2'556(\beta-1)^\kappa$ para κ grande. Una vez hallados $\beta = \beta(\kappa)$ y $A = A(\kappa)$, es fácil calcular numéricamente $f(s)$ y $F(s)$ para cualquier valor de s recursivamente por medio de:

$$\begin{cases} (s^\kappa f(s))' = \kappa s^{\kappa-1} F(s-1) & \text{si } s > \beta \\ (s^\kappa F(s))' = \kappa s^{\kappa-1} f(s-1) & \text{si } s > \beta+1 \\ f(s) = 0 & \text{si } s \le \beta \\ F(s) = A/s^\kappa & \text{si } s \le \beta+1 \end{cases} \tag{12}$$

Para compensar el crecimiento exponencial en M del último término de (10), debería ser K muy próximo a 1 pero en (5) esto no va a ser posible si w es pequeño. Típicamente se tiene $K = 1 + L/\log w$ con L una constante. Repitiendo la construcción de $\mathcal{D}^-$ y $\mathcal{D}^+$ pero ahora añadiendo la condición de que todos los factores sean mayores que w, podríamos escribir en (10) $L/\log w$ en lugar de $K-1$. Por otra parte, $p_j > w$ implica $v_m(z) = 0$ para $m + \beta \ge \log D/\log w$ de modo que podemos fijar en el término de error $M = \log D/\log w - \beta$ mientras que M continúa siendo arbitrario en los sumatorios. Eligiendo $w = D^{-\epsilon/\log\epsilon}$ (w "poco mayor" que D^ϵ), $\log D > L$ y $\log\log D > \epsilon^{-1}\log^2\epsilon$, se consigue que el término de error sea comparable a ϵL con ϵ tan pequeño como se desee. En definitiva

$$\sum_{\substack{d|P(z)\\ d\in\mathcal{D}_*^-}} \mu(d)\frac{\rho(d)}{d} = V(z)\big(f(s)+O(\epsilon L)\big) \quad \text{y} \quad \sum_{\substack{d|P(z)\\ d\in\mathcal{D}_*^+}} \mu(d)\frac{\rho(d)}{d} = V(z)\big(F(s)+O(\epsilon L)\big)$$

donde $\mathcal{D}_*^-$ y $\mathcal{D}_*^+$ son como $\mathcal{D}^-$ y $\mathcal{D}^+$ pero con la condición de que los factores primos sean mayores que $w = D^{-\epsilon/\log\epsilon}$.

Evidentemente esto no es directamente aplicable, porque a la hora de cribar hemos descartado simplemente los primos $p_j \le w$. Pero el lema fundamental asegura que podemos construir una criba de nivel $\widetilde{D} = D^\epsilon$ y $\widetilde{z} = D^{-\epsilon/\log\epsilon}$ para cribar los primos $p_j \le \widetilde{z} = w$ en la que se cumpla (4) con $f(s)$ y $F(s)$ iguales a $1 + O(\epsilon L^{10})$.

Finalmente, componiendo ambas cribas se tendría una criba de nivel $D^{1+\epsilon}$ y $F(s)$ y $f(s)$ vendrían dadas por las series (9), que a su vez son soluciones de (12) (una vez determinados β y A), salvo un error $(1+O(\epsilon L))(1+O(\epsilon L^{10})) = 1 + O(\epsilon L^{11})$.

Con algunos cambios, por ejemplo renombrar $D^{1+\epsilon}$ como D y elegir un ϵ adecuado, se tiene el teorema de criba:

Teorema 2 *Si L es una constante tal que* (5) *es válido con $K = 1 + L/\log w$. Para $\log D > 2L$ y suponiendo* (2)*, se tiene para $s > \beta = \beta(\kappa)$*

$$\big(f(s)+O(\Delta)\big)XV(z) + O(E) \le S(A,z) \le \big(F(s)+O(\Delta)\big)XV(z) + O(E)$$

donde $E = X/\log^C X$, $\Delta = L^{11}(\log\log\log D)^3/\log\log D$ y $f(s)$ y $F(s)$ son las soluciones de (12)*.*

6. El caso lineal. Ejemplos

Como hemos mencionado antes, para $\kappa = 1$ (criba lineal) se tiene $\beta = 2$ y $A = 2e^\gamma$. Gracias a (12), en el intervalo $[2, 3]$

$$f(s) = \frac{2e^\gamma}{s}\log(s-1) \qquad \text{y} \qquad F(s) = \frac{2e^\gamma}{s}.$$

Iterando se puede extender este rango de definición (con fórmulas cada vez más complejas).

Como ejemplo ilustrativo cribemos en el conjunto

$$A = \{n^2 + 1 \ : \ n \leq X\}.$$

De la fórmula $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, se tiene para $p \neq 2$

$$|A_p| = |\{n \leq X \ : \ p|n^2+1\}| = \begin{cases} 2X/p + O(1) & \text{si } p \equiv 1 \ (4) \\ 0 & \text{si } p \equiv 3 \ (4) \end{cases}$$

Por tanto $\rho(p) = 2$ si $p \equiv 1$ (4), y $\rho(p) = 0$ si $p \equiv 3$ (4). La criba es consecuentemente lineal.

En general se tiene por el teorema chino de resto

$$|A_{p_1 p_2 \cdots p_r}| = \frac{\rho(p_1 p_2 \cdots p_r)X}{p_1 p_2 \cdots p_r} + O(2^r).$$

Así que siempre que $D \leq X/\log^{C+1} X$ se tiene asegurado (2).

La condición $s > 2$ que se necesita para tener una cota inferior no trivial lleva a que el mayor z aceptable es $X^{1/2-\epsilon}$ con ϵ arbitrariamente pequeño. Con esta elección se tiene

$$S(A, z) \geq C_\epsilon \frac{X}{\log X} \qquad \text{para } X \text{ grande y cierta } C_\epsilon > 0.$$

Los elementos de A están acotados por X^2+1 y como para $\epsilon < 0'1$ se tiene $5(1/2-\epsilon) > 2$, en estas condiciones, los elementos que subsisten tras la criba tienen menos de 5 factores primos. Es decir, hemos probado:

Hay infinitos números de la forma $n^2 + 1$ con a lo más cuatro factores primos.

Veamos un ejemplo doble de Selberg que tiene gran interés teórico. Consideremos

$$A^{\text{par}} = \{n \leq 2X \ : \ \lambda(n) = 1\} \qquad \text{y} \qquad A^{\text{impar}} = \{n \leq 2X \ : \ \lambda(n) = -1\}$$

donde λ es la función de Liouville que vale 1 si el número de factores primos (contando multiplicidades) es par y -1 si es impar.

Se tiene

$$|A_d^{\text{par}}| = |\{n \leq 2X/d \ : \ \lambda(d)\lambda(n) = 1\}| = \frac{1}{2} \sum_{n \leq 2X/d} (1 + \lambda(d)\lambda(n)).$$

Se conoce por métodos de teoría analítica de números que $\sum_{n \leq N} \lambda(n) = O(N/\log^C N)$ para cualquier $C > 0$, por tanto $\rho(d) = 1$ con un error admisible y se tiene que la criba es lineal. Lo mismo se aplica a A^{impar}.

Según el teorema, salvo términos de error, $S(A^{\text{par}}, z)$ y $S(A^{\text{impar}}, z)$ están entre $f(s)XV(z)$ y $F(s)XV(z)$. Pero por otra parte, aplicando las iteraciones de Buchstab directamente a $S(A^{\text{par}}, z)$ y $S(A^{\text{impar}}, z)$, desarrollando un proceso iterativo, se puede probar que para $D = X$ y cada $s > 1$ se tiene

$$S(A^{\text{par}}, z) = f(s)XV(z) + O\big(\frac{X}{\log^2 X}\big) \quad \text{y} \quad S(A^{\text{impar}}, z) = F(s)XV(z) + O\big(\frac{X}{\log^2 X}\big).$$

De aquí se pueden deducir dos consecuencias importantes:

- Si $\kappa = 1$, el teorema de criba es óptimo en el sentido de que los términos principales no se pueden mejorar, ya que para A^{par} y A^{impar} se alcanzan.
- Los conjuntos A^{par} y A^{impar} son indistinguibles desde el punto de vista de la criba (ya que $|A_d^{\text{par}}|$ y $|A_d^{\text{impar}}|$ son similares), y sin embargo son bien distintos y $S(A^{\text{par}}, z)$ y $S(A^{\text{impar}}, z)$ tienen diferente asintótica. Hay un límite teórico para separar con métodos de criba números con una cantidad par o impar de factores (fenómeno de paridad).