El diablo de los números

Sección a cargo de

Javier Fresán

Una aplicación de la gran criba a la teoría de números: un teorema de Gallagher para polinomios palíndromos*

por

Mathieu Da Silva

1. La gran criba

1.1. Un poco de historia

Históricamente, la criba de Eratóstenes es, sin duda, la primera noción de criba utilizada en matemáticas. Sin embargo, se podría decir que la potencia de las técnicas de criba fue subestimada hasta que en el siglo veinte surgieron en teoría de números varias generalizaciones espectaculares. Como en la criba de Eratóstenes, el principio de los métodos de criba modernos consiste en retirar (cribar) de un conjunto finito un cierto número de elementos que satisfacen ciertas condiciones. En el caso de los enteros, esas condiciones se expresan por medio de la pertenencia a ciertas clases de congruencia módulo una cantidad finita de números primos.

Estas técnicas, desarrolladas en primer lugar por Viggo Brun, han servido, por ejemplo, para avanzar en algunos de los problemas más célebres de la teoría de números. Es el caso de la conjetura de los primos gemelos, que afirma que existen infinitos números primos p tales que $p+2$ es también primo (3 y 5, 5 y 7, 17 y 19, 29 y 31,...). Con la ayuda de la criba, Brun demostró hacia 1919 que la serie de los inversos de los números primos gemelos converge, lo cual sabemos que es falso para todos los números primos desde Euler. Después de Brun, los métodos de criba comenzaron a perfeccionarse sobre todo con los trabajos de Selberg [13] y Linnik [9].

En este artículo, nos interesaremos por la gran criba, que tiene la particularidad de ser fácil de utilizar, de aplicarse a conjuntos más generales que los números enteros y de proporcionar buenas cotas a nada que optimicemos cada etapa de su aplicación. La gran criba se debe esencialmente a los trabajos de Selberg. Más recientemente,

*Traducido del francés por Javier Fresán.

Kowalski ha formalizado esta técnica con el objetivo de aplicarla a objetos que no son números enteros [7].

Esbocemos la evolución de la gran criba a lo largo del tiempo. Sea $a = (a_n)_{n\in\mathbb{N}}$ una sucesión de números complejos. Para enteros $M, N \geqslant 0$, consideremos el polinomio trigonométrico S definido, para $t \in \mathbb{R}$, como

$$S_a(t) = \sum_{M<n\leqslant M+N} a_n e^{2i\pi tn}.$$

La forma analítica de la gran criba, tal y como la presentan Davenport y Halberstam [2] por primera vez en 1966, es una desigualdad de la forma

$$\sum_{1\leqslant i\leqslant R} |S_a(t_i)|^2 \leqslant \Delta(N,\delta) \sum_{M<n\leqslant M+N} |a_n|^2 \tag{1}$$

válida para toda R-tupla $(t_1, \ldots, t_R)$ de números reales δ-bien espaciados en el sentido

$$\min_{1\leqslant i<j\leqslant R} |t_j - t_i| \geqslant \delta > 0.$$

El número real $\Delta(N,\delta)$, la llamada *constante de la criba*, es muy difícil de estimar en la práctica. La búsqueda de una cota superior óptima para $\Delta(N,\delta)$ dio lugar a una carrera entre 1965 y 1975. Por ejemplo, Gallagher probó de forma elemental la desigualdad $\Delta(N,\delta) \leqslant 2\pi N + \delta^{-1}$. La demostración de este resultado puede leerse, entre otros sitios, en [7, Thm. 4.1]. Montgomery y Vaughan [12] obtuvieron en 1973 la desigualdad $\Delta(N,\delta) \leqslant N + \delta^{-1}$. La mejor cota conocida de $\Delta(N,\delta)$, no mucho más fuerte que la de Montgomery y Vaughan, se debe a Selberg:

$$\Delta(N,\delta) \leqslant N + \delta^{-1} - 1.$$

El lector encontrará una exposición de la demostración en [11]. La mejora de Selberg no tiene mucha importancia para las aplicaciones, en las que a menudo incluso la cota elemental de Gallagher es suficiente. Añadamos que este tipo de cota se obtiene por medio de argumentos de teoría de Fourier (véase, por ejemplo, [7] o [14]).

La gran criba se convirtió rápidamente en una herramienta muy potente en teoría analítica de números, por las razones que vamos a explicar. La relación entre la desigualdad (1) y los resultados de teoría de números que a uno le gustaría demostrar no está muy clara por el momento; es lo que nos proponemos elucidar. Elijamos los t_i racionales escritos como fracción irreducible k_i/m_i para todo $1 \leqslant i \leqslant R$, con m_i inferior a un cierto entero $L \geqslant 1$. Para $i \neq j$, se tiene entonces

$$|t_j - t_i| \geqslant \frac{1}{L^2},$$

de modo que la desigualdad (1) da

$$\sum_{m\leqslant L} \sum_{\substack{1\leqslant k\leqslant m\\(k,m)=1}} |S_a(k/m)|^2 \leqslant (N - 1 + L^2) \sum_{M<n\leqslant M+N} |a_n|^2.$$

Resulta que la suma interior en el miembro de la izquierda se puede acotar por una función g de m y de $\omega(\ell)$, para ℓ un divisor primo de m, donde $\omega(\ell)$ es el cardinal del conjunto

$$\Omega_\ell = \big\{h \mid 0 \leqslant h < \ell \text{ y } (n \equiv h \text{ mód } \ell \Rightarrow a_n = 0) \text{ para } n \in \{M+1, \dots, M+N\}\big\}$$

dado por las clases módulo ℓ que no contienen ningún índice n en el soporte de $(a_n)_{M<n\leqslant M+N}$. Hemos cribado así el conjunto de los a_n para $M+1 \leqslant n \leqslant M+N$. De hecho, se puede demostrar [14] que la función g está dada por

$$g(m) = \mu(m)^2 \prod_{\ell \mid m} \frac{\omega(\ell)}{\ell - \omega(\ell)},$$

donde μ es la función de Möbius

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ 0 & \text{si } n \text{ posee un factor cuadrado,} \\ (-1)^r & \text{si } n \text{ es producto de } r \text{ primos distintos.} \end{cases}$$

La desigualdad (1) se transforma entonces en

$$\Big| \sum_{M<n\leqslant M+N} a_n \Big|^2 \leqslant \frac{N-1+L^2}{H(L)} \sum_{M<n\leqslant M+N} |a_n|^2 \tag{2}$$

para todo $L \geqslant 1$, donde

$$H(L) = \sum_{m \leqslant L} g(m) = \sum_{m \leqslant L} \mu(m)^2 \prod_{\ell \mid m} \frac{\omega(\ell)}{\ell - \omega(\ell)}.$$

Diremos que la desigualdad (2) es la *forma aritmética de la gran criba*. Sean ahora Ω'_ℓ un conjunto de clases módulo ℓ para cada primo $\ell \leqslant L$, y E el subconjunto de $\{M+1, \dots, M+N\}$ correspondiente a los enteros n que no caen en ninguna de las clases en Ω'_ℓ. Si elegimos $a_n = 1$ si n pertenece a E y $a_n = 0$ si no, entonces los conjuntos Ω_ℓ y Ω'_ℓ coinciden para todo $\ell \leqslant L$, y la desigualdad (2) se reescribe como

$$|E| \leqslant (N - 1 + L^2) H(L)^{-1}. \tag{3}$$

Por tanto, hemos acotado el número de elementos restantes en $\{M+1, \dots, M+N\}$ después de haber cribado respecto a ciertas clases módulo un número finito de números primos ℓ. Observemos que $H(L)$ depende únicamente de las clases módulo ℓ elegidas y de la cota L, mientras que $N-1+L^2$ depende únicamente del número N de términos a_n considerados y de L. Esta «independencia» volverá a aparecer en la versión general de la gran criba que presentaremos en la siguiente sección. Señalemos para terminar que, si bien las cotas superiores de $\Delta(N, \delta)$ son en general suficientes para las aplicaciones, encontrar una cota inferior de $H(L)$ puede resultar bastante complicado y constituye un problema típico en teoría analítica de números.

1.2. Axiomatización de la gran criba

En lo que sigue, si ℓ es un número primo, designaremos por $\mathbb{F}_\ell \simeq \mathbb{Z}/\ell\mathbb{Z}$ el cuerpo finito de ℓ elementos. Para entender mejor la forma abstracta de la criba, reformulemos primero su forma aritmética. Fijamos:

1. Un conjunto finito X de números enteros, por ejemplo,
$$X = \{M+1, \dots, M+N\} \qquad \text{con } M \in \mathbb{Z} \text{ y } N \geqslant 1.$$
2. Un conjunto finito $\mathcal{L}^*$ de números primos (el *soporte primario* de la criba).
3. Una familia $\Omega = (\Omega_\ell)_{\ell \in \mathcal{L}^*}$ con $\Omega_\ell \subset \mathbb{F}_\ell$.

Sea $\rho_\ell \colon \mathbb{Z} \to \mathbb{F}_\ell$ la proyección canónica. El objetivo es dar una cota superior lo más fina posible del cardinal del conjunto

$$S(X, \Omega, \mathcal{L}^*) = \{x \in X \mid \rho_\ell(x) \notin \Omega_\ell \text{ para todo } \ell \in \mathcal{L}^*\}.$$

Como hemos retirado de X los enteros que caen en ciertas clases de congruencias, $S(X, \Omega, \mathcal{L}^*)$ se llama el *conjunto cribado* (corresponde al conjunto E de la introducción). Por ejemplo, para $L \geqslant 2$, tomando $X = \{1, \dots, N\}$, $\mathcal{L}^*$ el conjunto de números primos menores o iguales que L y $\Omega_\ell = \{0 \text{ mód } \ell\}$, se obtiene

$$S(X, \Omega, \mathcal{L}^*) = \{n \in \mathbb{N}^* \mid n \leqslant N \text{ y } \ell \nmid n \text{ para todo } \ell \leq L \text{ primo}\},$$

donde $\mathbb{N}^* = \{1, 2, \dots\}$ designa el conjunto de los números naturales sin el cero. Es la situación de la criba de Eratóstenes.

De forma más general, siguiendo a Kowalski [7], fijamos:

1. Una terna $\mathcal{Y} = (Y, \Lambda, (\rho_\ell)_{\ell \in \Lambda})$ formada por
   a) un conjunto Y,
   b) un conjunto de índices Λ,
   c) una familia $(\rho_\ell)_{\ell \in \Lambda}$ de aplicaciones sobreyectivas $\rho_\ell \colon Y \to Y_\ell$ con valores en un conjunto finito Y_ℓ.
2. Una terna $\mathcal{X} = (X, \mu, F)$ formada por
   a) un espacio medible (X, μ) de medida $\mu(X)$ finita,
   b) una aplicación $F \colon x \in X \mapsto F_x \in Y$ tal que la composición $X \to Y \to Y_\ell$ es medible para todo $\ell \in \Lambda$.
3. Un subconjunto finito $\mathcal{L}^*$ de Λ llamado el soporte primario de la criba.
4. Una familia finita $\Omega = (\Omega_\ell)_{\ell \in \mathcal{L}^*}$ de subconjuntos $\Omega_\ell \subset Y_\ell$.

Teniendo en cuenta que $\rho_\ell \circ F$ es medible, el conjunto cribado

$$\begin{aligned} S(X, \Omega, \mathcal{L}^*) &= \{x \in X \mid \rho_\ell(F_x) \notin \Omega_\ell \text{ para todo } \ell \in \mathcal{L}^*\} \\ &= \bigcap_{\ell \in \mathcal{L}^*} (\rho_\ell \circ F)^{-1}(\mathbb{F}_\ell \setminus \Omega_\ell) \end{aligned}$$

es μ-medible. El objetivo es acotar su medida, que designaremos por

$$|S(X,\Omega,\mathcal{L}^*)| = \mu(S(X,\Omega,\mathcal{L}^*)),$$

de la forma más precisa posible.

Observación. *Esta axiomática generaliza la noción clásica de criba, que se obtiene tomando $Y=\mathbb{Z}$, $\Lambda=\mathcal{P}$ el conjunto de números primos, ρ_ℓ la proyección módulo ℓ primo, $Y_\ell=\mathbb{Z}/\ell\mathbb{Z}$, $X=\{M+1,\dots,M+N\}$, μ la medida de conteo y F la inclusión de X en Y. En este caso, $\mathcal{L}^*$ es un conjunto finito de números primos y los Ω_ℓ forman un número finito de conjuntos de clases de congruencia respecto a las cuales nos gustaría cribar X.*

1.3. La desigualdad de la gran criba

Supongamos que cada Y_ℓ está equipado de una medida de probabilidad ν_ℓ. Se tiene entonces la siguiente generalización de la desigualdad (3):

Teorema 1 (Selberg, Kowalski). *Con la notación anterior, se cumple*

$$|S(X,\Omega,\mathcal{L}^*)| \leqslant \Delta H^{-1} \tag{4}$$

donde

1. *$\Delta=\Delta(X,\mathcal{L}^*)$ es un número real, que seguiremos llamando constante de la criba y que precisaremos más adelante.*
2. *$H=H(\Omega,\mathcal{L}^*)$ está dado por*

$$H=\sum_{\ell\in\mathcal{L}^*}\frac{\nu_\ell(\Omega_\ell)}{1-\nu_\ell(\Omega_\ell)}.$$

El lector encontrará una demostración detallada de este teorema en [7, Chap. 2]. Kowalski considera un marco un poco más general, en el que el soporte de la criba está formado por enteros sin factor cuadrado obtenidos como producto de números primos menores o iguales que L. Recuperamos en este caso una expresión de H que coincide con la de la introducción. Daremos una explicación muy somera de las técnicas que permiten obtener el teorema 1, lo cual nos permitirá definir formalmente Δ y entender un poco mejor la naturaleza de esta desigualdad. La idea es trabajar sobre los espacios de Hilbert $\mathrm{L}^2(Y_\ell\to\mathbb{C},\nu_\ell)$ dotados del producto escalar

$$\langle f,g\rangle_\ell=\sum_{y\in Y_\ell}\nu_\ell(y)f(y)\overline{g(y)}.$$

Podemos entonces considerar una base ortonormal $\mathcal{B}_\ell$ de $\mathrm{L}^2(Y_\ell\to\mathbb{C},\nu_\ell)$ que contenga a χ_{Y_ℓ}, la función constante igual a 1. Escribamos

$$\mathcal{B}_\ell^*=\mathcal{B}_\ell\setminus\{\chi_{Y_\ell}\}.$$

Con esta notación, se demuestra que la desigualdad se cumple para la mejor constante Δ tal que, para todo $\alpha \in \mathrm{L}^2(X,\mu)$, se tiene

$$\sum_{\ell\in\mathcal{L}^*}\sum_{\varphi\in\mathcal{B}_\ell^*}\left|\int_X \alpha(x)\varphi(\rho_\ell(F_x))\,d\mu(x)\right|^2 \leqslant \Delta\int_X |\alpha(x)|^2\,d\mu(x). \tag{5}$$

La desigualdad (5) no es sino una versión más abstracta de (1) que expresa la continuidad de un operador en un espacio de Hilbert. El paso de (5) a (4) es, esencialmente, el mismo que el paso de (1) a (3).

La fuerza del teorema 1 reside, entre otras cosas, en la independencia de las dos constantes Δ y H, que permite «separar» el problema inicial en dos subproblemas independientes: acotar superiormente Δ e inferiormente H.

1.4. Cómo aplicar la gran criba

Dado $Z \subset X$, queremos conocer la medida $\mu(Z)$. Para simplificar,[1] consideremos $\Lambda = \mathcal{P}$, el conjunto de los números primos, y $\mathcal{L}^* = \{1,\dots,L\} \cap \mathcal{P}$ para un entero lo suficientemente grande $L \geqslant 2$, que será especificado al final.

La idea consiste en encontrar un criterio de pertenencia a Z que sea aún válido al reducir módulo ℓ y tomar por Ω_ℓ el conjunto de los $\rho_\ell(x)$, para $x \in X$, que no cumplan este criterio. Se garantiza así la inclusión

$$Z \subset S(X,\Omega,\mathcal{L}^*).$$

Por ejemplo, no es buena idea elegir el conjunto Z formado por los enteros que son suma de dos cuadrados. Aunque la propiedad «ser suma de dos cuadrados» se conserve al reducir módulo ℓ, como todo elemento de $\mathbb{F}_\ell$ es suma de dos cuadrados no hay nada que cribar. En efecto, los cuadrados son las imágenes del morfismo de grupos $x \mapsto x^2$ de $\mathbb{F}_\ell^\times$ en $\mathbb{F}_\ell^\times$. Como $|\ker\varphi| = |\{-1,1\}| = 2$ (para $\ell \geqslant 3$), se deduce que hay exactamente $(\ell-1)/2$ cuadrados no nulos en $\mathbb{F}_\ell$, y por tanto $(\ell+1)/2$ cuadrados en $\mathbb{F}_\ell$. Para $x \in \mathbb{F}_\ell$ fijo, los conjuntos $\{x - y^2 \mid y \in \mathbb{F}_\ell\}$ y $\{z^2 \mid z \in \mathbb{F}_\ell\}$ poseen, por tanto, $(\ell+1)/2 > \ell/2$ elementos. Por el principio del palomar, su intersección es no vacía, es decir, existen $y, z \in \mathbb{F}_\ell$ tales que $x = y^2 + z^2$.

A título de ejemplo, retomemos la criba de Eratóstenes. En este caso, ν_ℓ es la probabilidad uniforme sobre $\mathbb{F}_\ell$, dada por $\nu_\ell(\Omega_\ell) = 1/\ell$. El teorema 1 proporciona[2] la desigualdad

$$\begin{aligned}\big|\{n \in \mathbb{N}^* \mid n \leqslant N \text{ y } \ell \nmid n \text{ para todo } \ell \leqslant L \text{ primo}\}\big| &\leqslant \Delta\Big(\sum_{\ell\leqslant L}\frac{1}{\ell-1}\Big)^{-1}\\ &\leqslant \frac{\Delta}{\log\log L + O(1)},\end{aligned}$$

[1] En ciertos casos, es preferible tomar, por ejemplo, el conjunto de ideales primos de un anillo.

[2] Utilizando una versión débil del teorema de Mertens (véase, por ejemplo, [14]):

$$\sum_{\ell\leqslant L}\frac{1}{\ell} = \log\log L + O(1).$$

donde la suma está tomada sobre todos los primos ℓ menores o iguales que L.

La elección de Ω es crucial para obtener una buena desigualdad al final del proceso. En particular, Ω_ℓ no debe contener demasiados elementos, para que la constante H no sea demasiado grande. Estimar H se reduce entonces a acotar inferiormente $\nu_\ell(\Omega_\ell)$, que suele ser un problema combinatorio, y al cálculo de una suma sobre los números primos (problema típico de la teoría analítica de números).

Falta acotar superiormente la constante de la criba Δ. Ya hemos observado que esta constante depende mucho de X y, por tanto, del problema que intentamos resolver. En el caso unidimensional en el que identificamos X con $\{M, \dots, M+N\}$, vimos en la introducción la desigualdad

$$\Delta \leqslant N + L^2 \leqslant (\sqrt{N} + L)^2.$$

En [6], Huxley demuestra que en el caso $X = \{M, \dots, N+M\}^m$ (con $m \geqslant 2$) y $\mathcal{L}^* = \{1, \dots, L\} \cap \mathcal{P}$ se tiene la siguiente generalización:

$$\Delta \leqslant (\sqrt{N} + L)^{2m}.$$

Una vez estimadas las constantes Δ y H, falta elegir L para optimizar la desigualdad obtenida. Aunque tengamos la impresión de haber optimizado todas las etapas, no hay garantía de que la desigualdad final no sea trivial.

Por ejemplo, con la cota unidimensional de Δ la criba de Eratóstenes da

$$\big|\{n \in \mathbb{N}^* \mid n \leqslant N \text{ y } \ell \nmid n \text{ para todo } \ell \leqslant L \text{ primo}\}\big| \leqslant \frac{(\sqrt{N}+L)^2}{\log\log L + O(1)}.$$

Eligiendo $L = \sqrt{N}$, se obtiene

$$\big|\{n \in \mathbb{N}^* \mid n \leqslant N \text{ y } \ell \nmid n \text{ para todo } \ell \leqslant \sqrt{N} \text{ primo}\}\big| \leqslant \frac{4N}{\log\log N + O(1)}.$$

Llegado este punto, observemos que

$$\begin{aligned}\big|\{n \in \mathbb{N}^* \mid n \leqslant N \text{ y } \ell \nmid n \text{ para todo } \ell \leqslant \sqrt{N} \text{ primo}\}\big| &= \big|\mathcal{P} \cap [\sqrt{N}, N]\big| \\ &= \pi(N) - \pi(\sqrt{N}),\end{aligned}$$

donde $\pi(x)$ designa el número de primos menores o iguales que x. Por tanto, hemos demostrado que $\pi(N) - \pi(\sqrt{N})$ es como mucho del orden de $N/\log\log N$.

Para formalizar la noción de «ser del orden de», introducimos la notación de Vinogradov de uso corriente en teoría analítica de números:

Notación (Vinogradov). *Si $f\colon X \to \mathbb{R}$ y $g\colon X \to \mathbb{R}_+$ son funciones con valores reales sobre un conjunto X, escribimos $f \ll g$ si existe una constante $C \geqslant 0$ tal que $|f(x)| \leqslant Cg(x)$ para todo $x \in X$. Llamaremos constante implícita a toda constante que cumple esta condición. Esta constante puede depender del conjunto X con el que trabajemos, que estará claro según el contexto.*

2. Un teorema de Gallagher para polinomios palíndromos

Sean $\mathbb{K}$ un cuerpo y $P \in \mathbb{K}[T]$ un polinomio. Un *cuerpo de descomposición* de P es una extensión de $\mathbb{K}$ sobre la cual P es producto de factores lineales y que es minimal, en el sentido de que está generada sobre $\mathbb{K}$ por las raíces de P. Se define el grupo de Galois de P como el grupo de $\mathbb{K}$-automorfismos de un cuerpo de descomposición cualquiera de P, siendo todos ellos $\mathbb{K}$-isomorfos. Dado un conjunto E de polinomios, diremos que un elemento de E tiene grupo de Galois maximal si el orden de su grupo de Galois es maximal respecto a los órdenes de los grupos de Galois de los elementos de E. Por ejemplo, si E es el conjunto de todos los polinomios de $\mathbb{K}[T]$ de grado $\leq n$, entonces el grupo de Galois maximal es el grupo simétrico $\mathfrak{S}_n$.

Gracias a la gran criba, Gallagher obtiene en [4] una cota superior para el número de polinomios mónicos de grado $m \geqslant 2$ fijo, grupo de Galois no maximal (es decir, distinto de $\mathfrak{S}_m$) y cuyos coeficientes son números enteros de valor absoluto acotado por $N \geqslant 1$. Una demostración detallada de este resultado figura en [7]. Nuestro objetivo es adaptarla etapa por etapa al caso de polinomios palíndromos. La única referencia para este resultado que conozco es [3], en la que los autores razonan de forma algo distinta (eligiendo otros generadores que los del lema 7).

Se dice que un polinomio P de $\mathbb{Z}[T]$ de grado m es *palíndromo* si es de la forma

$$P = \sum_{k=0}^{m} a_k T^k \text{ con } a_k = a_{m-k} \text{ para todo } 0 \leqslant k \leqslant m.$$

Designaremos por $\mathrm{Pal}_m(N)$ el subconjunto de $\mathbb{Z}[T]$ formado por los polinomios palíndromos de grado $2m$ cuyo grupo de Galois no es maximal y cuyos coeficientes están acotados por N, es decir, cumplen $|a_k| \leq N$ para todo $0 \leq k \leq 2m$.

Observación. *Podemos restringirnos a los polinomios de grado par. En efecto, si el grado de P es impar, como las raíces de un palíndromo van por pares (α, α^{-1}), una raíz debe ser su propia inversa, de modo que se puede factorizar $T - r$ con $r \in \{-1, 1\}$. Se tiene entonces que $P/(T - r)$ es un palíndromo de grado par con coeficientes enteros.*

Nos proponemos demostrar el siguiente resultado:

Teorema 2. *Para todo $N \geqslant 1$ y todo $m \geqslant 2$, se tiene*

$$|\mathrm{Pal}_m(N)| \ll m^3 (2N+1)^{m-1/2} \log N,$$

donde la constante implícita en $\ll$ es absoluta.

Observemos que la cota del teorema es mejor que la cota trivial

$$|\mathrm{Pal}_m(N)| \leqslant (2N+1)^m$$

dada por el número de polinomios mónicos de grado $2m$ con coeficientes enteros en el intervalo $[-N, N]$. La aplicación de la gran criba a este tipo de problemas permite mejorar un poco el exponente de $2N + 1$ en la cota trivial haciendo aparecer un factor logarítmico en N y un factor polinomial en m.

En [3], los autores obtienen el mismo resultado asintótico, pero sin precisar la dependencia en m (el factor m^3). En las páginas siguientes, presentamos una demostración detallada del teorema 2 que nos permitirá revisitar todas las etapas de la demostración del teorema de Gallagher en [7].

2.1. El grupo de Galois maximal de un polinomio palíndromo

La primera pregunta es cuál es el grupo de Galois maximal de un polinomio palíndromo irreducible. Presentamos las principales ideas del cálculo, para cuyos detalles el lector puede consultar [8].

Proposición 3. *Sea G el grupo de Galois maximal de los polinomios palíndromos irreducibles de grado $2m$. Entonces G forma parte de una sucesión exacta*

$$\{0\} \longrightarrow (\mathbb{Z}/2\mathbb{Z})^m \longrightarrow G \longrightarrow \mathfrak{S}_m \longrightarrow \{0\}.$$

Demostración. Como P es irreducible, su grupo de Galois G actúa transitivamente sobre el conjunto $\{\alpha_1, \ldots, \alpha_{2m}\}$ de las raíces de P. Como P es palíndromo, α es raíz de P si y solo si $\alpha \neq 0$ y α^{-1} también es raíz de P de la misma multiplicidad. Podemos, por tanto, hacer actuar G sobre el conjunto de los pares $\{\alpha, \alpha^{-1}\}$ donde α recorre las raíces de P. Como este conjunto es de cardinal m, obtenemos un morfismo $\pi\colon G \to \mathfrak{S}_m$. Para ver que este morfismo es sobreyectivo, primero se demuestra (por recurrencia sobre m) que P se puede escribir como

$$P(T) = T^m Q\left(T + \frac{1}{T}\right),$$

donde Q es un polinomio de grado m con coeficientes enteros. El grupo de Galois de Q es igual a $\pi(G)$, de modo que la única forma de obtener G maximal es que se cumpla la igualdad $\pi(G) = \mathfrak{S}_m$, es decir, que π sea sobreyectivo. El núcleo de π está generado por las m trasposiciones con soportes disjuntos que intercambian cada raíz y su inversa. Es, por tanto, isomorfo a $(\mathbb{Z}/2\mathbb{Z})^m$, como queríamos demostrar. □

Proposición 4. *Sea G el grupo de Galois maximal de los polinomios palíndromos de grado $2m$. Entonces la sucesión exacta*

$$\{0\} \longrightarrow (\mathbb{Z}/2\mathbb{Z})^m \longrightarrow G \longrightarrow \mathfrak{S}_m \longrightarrow \{0\}$$

es escincida. En particular, G es el producto semidirecto

$$G \simeq (\mathbb{Z}/2\mathbb{Z})^m \rtimes \mathfrak{S}_m$$

y todo grupo de Galois de un polinomio palíndromo de grado $2m$ tiene orden $\leq 2^m m!$.

Demostración. Para construir una sección, observemos que $\pi\colon G \to \mathfrak{S}_m$ envía $g \in G$ a la permutación $\rho_g \in \mathfrak{S}_m$ dada por

$$\left\{\alpha_i, \frac{1}{\alpha_i}\right\} \mapsto \left\{g(\alpha_i), g^{-1}(\alpha_i)\right\},$$

y definamos $s\colon \mathfrak{S}_m \to G$ como

$$s(\sigma) = g_\sigma, \quad g_\sigma(\alpha_i) = \alpha_{\sigma(i)}.$$

Esta aplicación es, en efecto, una sección, puesto que

$$g_{\sigma_1\sigma_2}(\alpha_i) = \alpha_{\sigma_1\sigma_2(i)} = g_{\sigma_1}(\alpha_{\sigma_2(i)}) = g_{\sigma_1}g_{\sigma_2}(\alpha_i)$$

y que

$$\pi \circ s(\sigma) = \pi(g_\sigma) = \rho_{g_\sigma} = \left(\left\{\alpha_i, \alpha_i^{-1}\right\} \mapsto \left\{g_\sigma(\alpha_i), g_\sigma^{-1}(\alpha_i)\right\} = \left\{\alpha_{\sigma(i)}, \alpha_{\sigma(i)}^{-1}\right\}\right) = \sigma,$$

lo cual concluye la demostración. □

2.2. El grupo de Galois módulo ℓ

Ahora que hemos precisado el enunciado del teorema 2, es momento de entender por qué es razonable aplicar la gran criba para demostrarlo. Para ello, identificaremos $\mathrm{Pal}_m(N)$ con un subconjunto Z de $X = \{-N, \dots, N\}^m$. La criba (teorema 1) y la cota superior para Δ de Huxley implican la desigualdad

$$|\mathrm{Pal}_m(N)| \leqslant (\sqrt{2N+1} + L)^{2m} H(\Omega, L)^{-1}$$

para todo $L \geqslant 2$. Falta encontrar una cota inferior para H. El hecho de que los grupos de Galois se presten a ser cribados módulo ℓ es una consecuencia de un famoso teorema de Dedekind (véase, por ejemplo, [5, théorème 10.4.4]).

Teorema 5 (Dedekind). *Sean $P \in \mathbb{Z}[T]$ un polinomio mónico irreducible de grado m y ℓ un número primo. Designamos por $\overline{P} \in \mathbb{F}_\ell[T]$ la reducción de P módulo ℓ y por $G_{\mathbb{Q}}(P)$ (resp., $G_{\mathbb{F}_\ell}(\overline{P})$) el grupo de Galois de P (resp., de $\overline{P}$). Si $\overline{P}$ es separable (es decir, tiene raíces simples en una clausura algebraica de $\mathbb{F}_\ell$), entonces:*

1. *Existe una inyección*

$$G_{\mathbb{F}_\ell}(\overline{P}) \hookrightarrow G_{\mathbb{Q}}(P)\,(\hookrightarrow \mathfrak{S}_m)\,.$$

2. *Si, además, $\overline{P} = P_1 \cdots P_m$ es producto de m polinomios $P_1, \dots, P_m$ y, para todo $1 \leqslant i \leqslant m$, el polinomio P_i es producto de $n_i \geqslant 0$ polinomios mónicos irreducibles de grado i, todos ellos distintos, entonces $G_{\mathbb{Q}}(P) \subset \mathfrak{S}_m$ contiene una permutación σ cuya descomposición en ciclos de soporte disjunto posee n_i ciclos de longitud i para todo $1 \leqslant i \leqslant m$.*[3]

Este bello teorema relaciona el grupo de Galois de un polinomio con el de su reducción módulo ℓ, hasta el punto de implicar la existencia de un elemento de $G_{\mathbb{Q}}(P)$ de un cierto tipo cíclico en función de la factorización de $\overline{P}$ en polinomios irreducibles. Observemos que esta factorización está íntimamente ligada al tipo cíclico de una permutación de $\mathfrak{S}_m$, como veremos en el momento de enumerar los polinomios que se factorizan de un cierto modo en $\mathbb{F}_\ell[T]$ (proposición 9).

El teorema de Dedekind se aplica gracias al siguiente resultado:

[3] Diremos entonces que σ tiene tipo cíclico $(n_1, \dots, n_m)$.

Lema 6 (Jordan). *Si $P \in \mathbb{Z}[T]$ es irreducible, su reducción $\overline{P} \in \mathbb{F}_\ell[T]$ es separable para todo ℓ salvo un número finito.*

Demostración. Sean $P \in \mathbb{Z}[T]$ un polinomio irreducible y ℓ un número primo. Designamos por (P, P') el polinomio mónico de mayor grado que divide a P y a su derivada P' en $\mathbb{Z}[T]$. Como P es irreducible en $\mathbb{Z}[T]$ y, por definición, (P, P') divide a P, las únicas dos posibilidades son $(P, P') = P$ o $(P, P') = 1$. Como P' no puede dividir a P, se deduce que P y P' son coprimos en $\mathbb{Z}[T]$. Reduciendo módulo ℓ se obtiene que $\overline{P}$ y $\overline{P'} = \overline{P}'$ son coprimos en $\mathbb{F}_\ell[T]$. Por tanto, si ℓ no divide al grado de P, entonces $\overline{P} \in \mathbb{F}_\ell[T]$ es separable. De ahí se sigue el resultado, puesto que hay solo un número finito de primos ℓ que dividen al grado de P. □

Gracias al teorema de Dedekind, basta con conocer una condición suficiente sobre la descomposición en ciclos de soporte disjunto de los elementos de $K \subset G_{\mathbb{Q}}(P)$ para garantizar la igualdad $K = G_{\mathbb{Q}}(P)$. Podremos entonces cribar estimando el número de polinomios en $\mathbb{F}_\ell[T]$ que poseen la descomposición correspondiente. Es el objetivo del siguiente resultado:

Lema 7. *Para que el grupo de Galois G de un polinomio palíndromo $P \in \mathbb{Z}[T]$ de grado $2m$, mónico e irreducible, sea maximal (es decir, de orden $2^m m!$), basta con que G contenga:*

1. *La composición $\gamma_1 \circ \gamma_2$ de un p-ciclo γ_1, con p primo y $m/2 < p \leqslant m$, y del p-ciclo γ_2 con soporte disjunto de γ_1 únicamente determinado por γ_1.*
2. *La composición $\tau_1 \circ \tau_2$ de una trasposición τ_1 y de la trasposición τ_2 con soporte disjunto de τ_1 únicamente determinada por τ_1.*
3. *Una trasposición τ_0.*

Demostración. Recordemos la igualdad

$$P = T^m Q\left(T + \frac{1}{T}\right),$$

donde $Q \in \mathbb{Z}[T]$ es de grado m. Se sigue que

$$K = \mathbb{Q}\left(\alpha_1 + \frac{1}{\alpha_1}, \ldots, \alpha_m + \frac{1}{\alpha_m}\right)/\mathbb{Q}$$

es un cuerpo de descomposición de Q sobre $\mathbb{Q}$, donde hemos elegido $\alpha_1, \ldots, \alpha_m$ de modo que no existan $1 \leqslant i < j \leqslant m$ tales que $\alpha_i = \alpha_j^{-1}$. El grupo de Galois de Q es, por tanto,

$$H = \mathrm{Gal}\left(\mathbb{Q}\left(\alpha_1 + \frac{1}{\alpha_1}, \ldots, \alpha_m + \frac{1}{\alpha_m}\right)/\mathbb{Q}\right).$$

Como Q es de grado m, se tiene $|H| \leqslant m!$. Por otra parte, $|G|$ está acotado por

$$|G| \leqslant |H|[L : K],$$

donde L es la extensión $L = \mathbb{Q}(\alpha_1, \ldots, \alpha_m)$. Como $L = K(\alpha_1, \ldots, \alpha_m)$, donde $\alpha_i + \alpha_i^{-1} \in L$ para todo $1 \leqslant i \leqslant m$, se cumple $[L : K] \leqslant 2^m$. Teniendo en cuenta la desigualdad $|G| \leqslant 2^m m!$ de la proposición 4, para que G sea maximal basta con tener igualdad en las dos desigualdades $[L : K] \leqslant 2^m$ y $|H| \leqslant m!$.

Empecemos por la igualdad $|H| = m!$. Como P es, por hipótesis, irreducible sobre $\mathbb{Q}$, también lo es el polinomio Q, de modo que H es un subgrupo transitivo de $\mathfrak{S}_m$. En [4], Gallagher demuestra, utilizando la teoría de grafos, que para que un subgrupo transitivo de $\mathfrak{S}_m$ sea maximal, basta con que contenga un p-ciclo γ con p primo tal que $m/2 < p \leqslant m$ y una trasposición τ. Ahora bien, H se inyecta en G «simetrizando», es decir, viendo $\sigma \in H \subset \mathfrak{S}_m$ como el elemento $\sigma' \in \mathfrak{S}_{2m}$ que actúa como σ sobre $\{1, \ldots, m\}$ y sobre $\{m+1, \ldots, 2m\}$ (visto como $\{1, \ldots, m\}$). Este elemento es un producto de dos permutaciones de soporte disjunto con el mismo tipo cíclico que σ. Tomando $\gamma' = \gamma_1 \circ \gamma_2$ y $\tau' = \tau_1 \circ \tau_2$, se obtienen las partes 1 y 2 del enunciado.

Por lo anterior, podemos suponer que $H \simeq \mathfrak{S}_m$ es maximal. Ocupémonos ahora de la igualdad $[L : K] = 2^m$. Para que se cumpla, basta con que G contenga m trasposiciones $\tau^{(1)}, \ldots, \tau^{(m)}$ con soportes disjuntos (lo cual es posible puesto que G es un subgrupo de $\mathfrak{S}_{2m}$) que correspondan a los intercambios $\{\alpha_i, \alpha_i^{-1}\} \leftrightarrow \{\alpha_j, \alpha_j^{-1}\}$ para $i \neq j$. Esta condición es automática en cuanto G contiene una de estas trasposiciones, pongamos τ_0. En efecto, como tenemos una sobreyección de G en $\mathfrak{S}_m$ dada por la acción de G sobre los pares $\{\alpha_i, \alpha_i^{-1}\}$, τ_0 se envía a una trasposición $\widehat{\tau_0} \in \mathfrak{S}_m$. Igual que en la demostración de la proposición 4, sea $\pi \colon G \to \mathfrak{S}_m$. Sabemos que existe $s \colon \mathfrak{S}_m \to G$ tal que $\pi \circ s = \mathrm{id}$. Como todas las trasposiciones de $\mathfrak{S}_m$ son conjugadas entre sí, $\widehat{\tau_0}$ es conjugada a todas las trasposiciones de $\mathfrak{S}_m$. Aplicando s, se obtiene para todo $1 \leqslant i \leqslant m$ un elemento $\sigma_i \in G$ tal que $\tau^{(i)} = \sigma_i \tau_0 \sigma_i^{-1} \in G$. Esto completa la parte 3 del enunciado. □

Observación. *Esta demostración del lema 7 reposa sobre un lema utilizado por Gallagher en la demostración de su teorema. En [3], los autores utilizan un truco para evitar este lema.*

2.3. Una etapa intermedia: el caso de los polinomios reducibles

Todo lo anterior es solo válido cuando el polinomio P es irreducible, puesto que hemos utilizado de manera crucial el hecho de que el grupo de Galois actúa transitivamente sobre el conjunto de raíces. Sea $R_m(N)$ el conjunto de polinomios palíndromos reducibles de grado $2m$ cuyos coeficientes son enteros acotados por un mismo $N \geqslant 1$. Escribamos

$$\mathrm{Pal}_m(N) = R_m(N) \cup I_m(N),$$

donde $I_m(N)$ es el subconjunto de los polinomios irreducibles de grupo de Galois no maximal. Las técnicas de la sección anterior nos permitirán acotar el cardinal de $I_m(N)$. En cuanto a $R_m(N)$, la gran criba nos da el siguiente resultado:

Teorema 8. *Para todo $N \geqslant 1$ y todo $m \geqslant 2$, se tiene*

$$|R_m(N)| \ll m^2 (2N+1)^{m-1/2} \log N,$$

donde la constante implícita en $\ll$ es absoluta.

Demostración. Identifiquemos $R_m(N)$ con un subconjunto Z' de $\{-N,\dots N\}^m$. Si $P \in \mathbb{Z}[T]$ es un polinomio palíndromo mónico reducible de grado $2m$, también lo son todas sus reducciones $\overline{P} \in \mathbb{F}_\ell[T]$ módulo ℓ. Resulta entonces natural tomar por Ω_ℓ el conjunto de los palíndromos de grado $2m$ en $\mathbb{F}_\ell[T]$ que son mónicos e irreducibles. Tomando ν_ℓ la probabilidad uniforme, basta con enumerar los elementos de Ω_ℓ:

$$|\Omega_\ell| = \begin{cases} \frac{1}{2m} \sum\limits_{d|m,\, d \text{ impar}} \ell^{m/d}\mu(d) & \text{si } m \text{ no es una potencia de 2,} \\ \frac{1}{2m}(\ell^m - 1) & \text{si } m \text{ es una potencia de 2,} \end{cases}$$

donde μ designa la función de Möbius. La demostración de este resultado es similar a la de la fórmula para el número de polinomios mónicos irreducibles en $\mathbb{F}_p[T]$, que reposa sobre la factorización de $T^\ell - T$. En el caso de $|\Omega_\ell|$, se utiliza el polinomio $T^{\ell^m+1} - 1$ (véase [10] para los detalles). En particular,

$$|\Omega_\ell| \gg \frac{1}{2m}\ell^m$$

y, por tanto,

$$H(\Omega, L)^{-1} \leqslant \left(\sum_{\ell \leqslant L} \frac{|\Omega_\ell|}{\ell^m}\right)^{-1} \ll \left(\sum_{\ell \leqslant L} \frac{1}{2m}\right)^{-1} = \frac{2m}{\pi(L)}.$$

Combinando esta información con $\pi(L) \gg \frac{L}{\log L}$, se obtiene

$$H(\Omega, L)^{-1} \ll m\frac{\log L}{L},$$

donde la constante implícita en la notación $\ll$ es absoluta. La gran criba da

$$|R_m(N)| \ll \left(\sqrt{2N+1} + L\right)^{2m} \frac{m \log L}{L}. \tag{6}$$

Falta optimizar la elección de L. Buscamos L de la forma $L = m^\beta\sqrt{2N+1}$, para optimizar la cota superior (comparar con el primer factor de (6)), con β por determinar. Sustituyendo L por este valor se obtiene la cota (salvo una constante absoluta)

$$(2N+1)^{m-\frac{1}{2}}(1+m^\beta)^{2m}m^{1-\beta}\left(\beta \log m + \frac{1}{2}\log(2N+1)\right).$$

Debemos elegir β negativo para que el factor $(1+m^\beta)^{2m}m^{1-\beta}$ no explote, pero no «demasiado negativo», pues entonces explotaría el factor $m^{1-\beta}$. Como en el caso del teorema de Gallagher original, parece razonable tomar $\beta = -1$, lo que da

$$|R_m(N)| \ll m^2(2N+1)^{m-1/2}\log N$$

siempre y cuando se cumpla la desigualdad $|\beta \log m| = |\log m| \leqslant \log(2N+1)$. Si $m \leqslant 2N+1$, hemos terminado. Si $m \geqslant 2N+1$, se tiene entonces

$$m^2(2N+1)^{m-1/2}\log N \geqslant (2N+1)^{m+2-1/2}\log N,$$

que es peor que la cota trivial $(2N+1)^m$. En ambos casos se tiene el resultado. □

2.4. Fin de la demostración del teorema

Retomando las notaciones de la sección anterior, nos gustaría acotar el cardinal de $I_m(N)$. Sea

1. E_1 el conjunto de los palíndromos mónicos de grado $2m$ con coeficientes enteros acotados por N cuyo grupo de Galois no contiene ninguna composición $\tau_1 \circ \tau_2$ de dos trasposiciones, con τ_2 determinada por τ_1.
2. E_2 el conjunto de los palíndromos mónicos de grado $2m$ con coeficientes enteros acotados por N cuyo grupo de Galois no contiene ninguna composición $\gamma_1 \circ \gamma_2$ de dos p-ciclos con p primo, $m/2 < p \leqslant m$ y γ_2 determinado por γ_1.
3. E_3 el conjunto de los palíndromos mónicos de grado $2m$ con coeficientes enteros acotados por N cuyo grupo de Galois no contiene ninguna trasposición.

El lema 7 implica la inclusión

$$I_m(N) \subset E_1 \cup E_2 \cup E_3.$$

Usando el teorema de Dedekind (teorema 5), nos bastará con aplicar de nuevo la gran criba. Para ello necesitamos contar los palíndromos en $\mathbb{F}_\ell[T]$ con una factorización en polinomios irreducibles correspondiente a los tipos cíclicos que queremos cribar (los asociados a E_1, E_2 y E_3). Recordemos que $X = \{-N, \dots, N\}^m$.

En el caso de E_1 escribimos

$$E_1 \subset S(X, \Omega^{(1)}, \mathcal{L}^*),$$

tomando como $\Omega_\ell^{(1)}$ el conjunto de los palíndromos de grado $2m$ en $\mathbb{F}_\ell[T]$ cuya factorización en polinomios irreducibles contiene exactamente dos factores de grado 2 que se determinan el uno al otro, y el resto de factores de grado impar.

En el caso de E_2 escribimos

$$E_2 \subset S(X, \Omega^{(2)}, \mathcal{L}^*)$$

tomando como $\Omega_\ell^{(2)}$ el conjunto de los palíndromos de grado $2m$ en $\mathbb{F}_\ell[T]$ cuya factorización en polinomios irreducibles contiene dos factores de grado primo p con $m/2 < p \leqslant m$, que se determinan el uno al otro.

En el caso de E_3 escribimos

$$E_3 \subset S(X, \Omega^{(3)}, \mathcal{L}^*)$$

tomando como $\Omega_\ell^{(3)}$ el conjunto de los palíndromos de grado $2m$ en $\mathbb{F}_\ell[T]$ cuya factorización en polinomios irreducibles contiene exactamente un factor de grado 2 y el resto de factores de grado impar.

Llegado este punto, nos falta estimar el número de polinomios palíndromos mónicos de grado $2m$ en $\mathbb{F}_\ell[T]$ de un tipo cíclico determinado. Como en [10], comencemos observando que el único palíndromo mónico irreducible de grado impar en $\mathbb{F}_\ell[T]$ es $T+1$, y que este factor no aparece en la descomposición de un palíndromo de grado

$2m$ en producto de polinomios irreducibles (según el lema 6, su multiplicidad debería ser 1, lo cual contradice el hecho de que el grado $2m$ sea par). La «partición» de $2m$ asociada a la descomposición de un palíndromo de grado $2m$ como producto de irreducibles es, por tanto, de la forma

$$2m = 2n_1 + 4n_2 + 6n_3 + \cdots + 2mn_m \qquad (n_i \geq 0). \tag{7}$$

Proposición 9. *Sea $\omega_\ell(n_1, \ldots, n_m)$ el número de polinomios palíndromos en $\mathbb{F}_\ell[T]$ de grado $2m$ cuya factorización en irreducibles corresponde al tipo cíclico $(n_1, \ldots, n_m)$. Para ℓ suficientemente grande, se tiene*

$$\frac{\ell^m}{2^{\sum n_k}} \left(\prod_{k=1}^{m} \frac{1}{k^{n_k} n_k!} \right) \left(1 - \frac{3}{\ell}\right)^{\sum n_k} \leqslant \omega_\ell(n_1, \ldots, n_m) \leqslant \frac{\ell^m}{2^{\sum n_k}} \left(\prod_{k=1}^{m} \frac{1}{k^{n_k} n_k!} \right).$$

Observación. *El producto que aparece en esta fórmula es la probabilidad de que un elemento de $\mathfrak{S}_m$ tenga tipo cíclico $(n_1, \ldots, n_m)$.*

Demostración. Es fácil ver que el conjunto de polinomios palíndromos es estable para el producto y que todo palíndromo se factoriza como producto de palíndromos irreducibles. Considerando la igualdad (7), se deduce la expresión

$$\omega_\ell(n_1, \ldots, n_m) = \prod_{k=1}^{m} \binom{j(\ell, k)}{n_k}, \tag{8}$$

donde $j(\ell, k)$ designa el número de palíndromos mónicos irreducibles de grado $2k$ sobre $\mathbb{F}_\ell[T]$. Como sabemos calcular $j(\ell, k)$ explícitamente, podemos acotarlo para ℓ suficientemente grande:

$$\frac{\ell^k}{2k}\left(1 - \frac{1}{\ell}\right) \leqslant j(\ell, k) \leqslant \frac{\ell^k}{2k}.$$

1. La cota superior es evidente a partir de lo anterior.
2. Para obtener la cota inferior, se descompone $k = 2^\alpha q_1^{\beta_1} \cdots q_r^{\beta_r}$ en factores primos. Los divisores de k en los cuales la función de Möbius no se anula son los divisores de $2q_1 \cdots q_r$. Como solo nos interesan los impares, quedan solo los divisores de $q_1 \cdots q_r$, y $k/d = 2^\alpha q_1^{\beta_1 - \varepsilon_1} \cdots q_r^{\beta_r - \varepsilon_r}$ con $\varepsilon_i \in \{0, 1\}$.
   a) O bien $k \geqslant 3$ no es una potencia de 2 y tenemos

$$j(\ell, k) = \frac{1}{2k} \sum_{\substack{d \mid k \\ d \text{ impar}}} \ell^{k/d} \mu(d) = \frac{1}{2k}\ell^k + \frac{1}{2k} \sum_{\substack{d \mid k, d > 1 \\ \text{impar}}} \ell^{k/d} \mu(d),$$

   es decir,

$$j(\ell, k) \geqslant \frac{1}{2k}\ell^k - \frac{1}{2k} \sum \ell^{k/d} \geqslant \frac{\ell^k}{2k}\left(1 - k\left(\frac{1}{\sqrt{\ell}}\right)^k\right)$$

   donde la suma está tomada sobre los divisores $d > 1$ de k impares sin factor cuadrado.

b) O bien $k = 2^\alpha$ y tenemos

$$j(\ell,k) = \frac{\ell^k}{2k}\left(1 - \frac{1}{\ell^k}\right) \geqslant \frac{\ell^k}{2k}\left(1 - \frac{1}{\ell}\right).$$

Observemos que la cota del caso b) es también válida en el caso a) para ℓ suficientemente grande, en vista de la equivalencia

$$k\left(\frac{1}{\sqrt{\ell}}\right)^k \leqslant \frac{1}{\ell} \iff k \leqslant \ell^{k/2-1}.$$

La condición de la derecha se cumple para todo $\ell \geqslant k^{\frac{1}{k/2-1}}$ (en particular, para todo k impar). Para estos ℓ (de los que hay una infinidad), se tiene

$$j(\ell,k) \geqslant \frac{\ell^k}{2k}\left(1 - \frac{1}{\ell}\right).$$

De ello se deduce que también sabemos estimar $\binom{j(\ell,k)}{n_k}$ para ℓ suficientemente grande:

1. La cota superior es inmediata:
$$\binom{j(\ell,k)}{n_k} = \frac{j(\ell,k)(j(\ell,k)-1)\cdots(j(\ell,k)-n_k+1)}{n_k!} \leqslant \frac{\ell^{kn_k}}{2^{n_k}k^{n_k}n_k!}.$$
2. Para obtener la cota inferior, escribimos
$$\begin{aligned}\binom{j(\ell,k)}{n_k} &= \frac{j(\ell,k)(j(\ell,k)-1)\cdots(j(\ell,k)-n_k+1)}{n_k!} \\ &\geqslant \frac{\ell^{kn_k}}{2^{n_k}k^{n_k}n_k!}\prod_{j=0}^{n_k-1}\left(1 - \frac{1}{\ell} - \frac{2kj}{\ell^k}\right).\end{aligned}$$
Como $2jk \leqslant 2k^2 \leqslant 2\ell^{k-2}$, se tiene
$$\binom{j(\ell,k)}{n_k} \geqslant \frac{\ell^{kn_k}}{2^{n_k}k^{n_k}n_k!}\prod_{j=0}^{n_k-1}\left(1 - \frac{1}{\ell} - \frac{2}{\ell^2}\right) \geqslant \frac{\ell^{kn_k}}{2^{n_k}k^{n_k}n_k!}\left(1 - \frac{3}{\ell}\right)^{n_k}.$$

Para concluir utilizamos (8). □

Para estimar los cardinales de $\Omega_\ell^{(1)}$, $\Omega_\ell^{(2)}$ y $\Omega_\ell^{(3)}$, basta simplemente con estimar la densidad en el grupo simétrico $\mathfrak{S}_m$ de los tipos cíclicos asociados.

1. En el caso $\Omega_\ell^{(1)}$, observamos que formalmente se tiene
$$\begin{aligned}&\exp(x)\exp\left(\frac{x^3}{3}\right)\cdots\exp\left(\frac{x^{2(n-1)+1}}{2(n-1)+1}\right)\cdots \\ &\quad= \left(\sum_{i_1\geqslant 0}\frac{x^{i_1}}{i_1!}\right)\left(\sum_{i_2\geqslant 0}\frac{x^{3i_2}}{3^{i_2}i_2!}\right)\cdots\left(\sum_{i_n\geqslant 0}\frac{x^{(2(n-1)+1)i_n}}{(2(n-1)+1)^{i_n}i_n!}\right)\cdots \\ &\quad= \sum_{n,(i_1,\ldots,i_n)}\frac{x^{i_1+3i_2+\cdots+(2(n-1)+1)i_n}}{i_1!\,3^{i_2}i_2!\cdots(2(n-1)+1)^{i_n}i_n!}.\end{aligned}$$

Para la única bitrasposición (resp., trasposición) en el caso de E_1 (resp., de E_3), la densidad buscada vale, por tanto, 1/4 (resp., 1/2), que multiplica al coeficiente de x^{2m-2} en esta serie. Lo calculamos escribiendo

$$\begin{aligned}\exp(x)\exp\left(\frac{x^3}{3}\right)\cdots\exp\left(\frac{x^{2(n-1)+1}}{2(n-1)+1}\right)\cdots &= \exp\left(\sum_{i\geqslant 0}\frac{x^{2i+1}}{2i+1}\right)\\ &= \exp\left(\int_0^x\sum_{i\geqslant 0}t^{2i}\,dt\right) = \exp\left(\int_0^x\frac{1}{1-t^2}\,dt\right)\\ &= \exp\left(\int_0^x\left(\frac{1}{1+t}-\frac{1}{2}\frac{-2t}{1-t^2}\right)dt\right) = \exp\left(\log\left(\frac{1+x}{\sqrt{1-x^2}}\right)\right)\\ &= \frac{1+x}{\sqrt{1-x^2}} = (1+x)\sum_{k\geqslant 0}\frac{(2k)!}{(2^k k!)^2}\,x^{2k}.\end{aligned}$$

Finalmente, se sigue de la fórmula de Stirling que la densidad buscada es equivalente a $1/(4\sqrt{\pi m})$ (resp., a $1/(2\sqrt{2\pi m})$) cuando m tiende a infinito.

2. En el caso de $\Omega_\ell^{(2)}$, usando la subaditividad de las medidas de probabilidad, la densidad buscada es igual a

$$\sum_{m/2<p\leqslant m}\frac{1}{p},$$

y la estimación clásica de Mertens

$$\sum_{p\leqslant x}\frac{1}{p} = \log\log x+\gamma+\sum_p\left(\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right)+O\left(\frac{1}{\log x}\right),$$

implica que esta densidad es $O\left(1/\log m\right)$.

Utilizando la proposición 9 y la criba, se obtienen las estimaciones

$$\begin{aligned}|E_1| &\ll (\sqrt{2N+1}+L)^{2m}\sqrt{m}\,\frac{\log L}{L},\\ |E_2| &\ll (\sqrt{2N+1}+L)^{2m}(\log m)\,\frac{\log L}{L},\\ |E_3| &\ll (\sqrt{2N+1}+L)^{2m}\sqrt{m}\,\frac{\log L}{L}\end{aligned}$$

para $L\geqslant 2$ suficientemente grande.

Fin de la demostración del teorema 2. Juntando todos los resultados anteriores, se obtiene la estimación

$$|\mathrm{Pal}_m(N)| \ll m^2(2N+1)^{m-1/2}\log N+\left(\log m+2\sqrt{m}\right)\left(\sqrt{2N+1}+L\right)^{2m}\frac{\log L}{L}.$$

Tomemos primero L de la forma $f(m)\sqrt{2N+1}$. El segundo sumando en la cota superior es, entonces,

$$\left(\frac{\log m+2\sqrt{m}}{f(m)}\right)(2N+1)^{m-1/2}(1+f(m))^{2m}\log(f(m)\sqrt{2N+1}).$$

Para optimizar, queremos que el factor $(\log m + 2\sqrt{m})/f(m)$ no crezca demasiado rápidamente con m, y que el factor $(1+f(m))^{2m}$ y el factor logarítmico permanezcan acotados. Tomando $f(m) = 1/m$ se obtiene

$$|\mathrm{Pal}_m(N)| \ll m^2(2N+1)^{m-1/2}\log N + \left(m\log m + m^{3/2}\right)(2N+1)^{m-1/2}\log\left(\frac{\sqrt{2N+1}}{m}\right).$$

Ahora bien, para $m \leqslant \sqrt{2N+1}$, el primer sumando posee una cota del orden de $(2N+1)^{m+1/2}$, así que la elección $f(m) = 1/m$ no es la buena. Tomemos más bien $f(m) = 1/m^2$. Si $m^2 \leqslant \sqrt{2N+1}$, el orden de magnitud del primer sumando es el bueno y el factor logarítmico está acotado. Comprobemos que la cota superior sigue siendo válida para $m^2 \geqslant \sqrt{2N+1}$. En este caso, el factor logarítmico crece en valor absoluto con m y, como la cota es peor que la cota trivial, es válida. Así obtenemos, finalmente,

$$\boxed{|\mathrm{Pal}_m(N)| \ll m^3(2N+1)^{m-1/2}\log N},$$

que es lo que queríamos demostrar. □

2.5. Conclusión

Hemos ilustrado el principio de la gran criba por medio de una adaptación del teorema de Gallagher a los polinomios palíndromos. En el caso de los polinomios reducibles, Van der Waerden demuestra en [15] un resultado más preciso que Gallagher sin utilizar la criba: la cota obtenida involucra $(2N+1)^{m-1}$ en lugar de $(2N+1)^{m-1/2}$. El problema de obtener la potencia $m-1$ en el caso de polinomios de grupo de Galois no maximal sigue aún abierto, y ha sido objeto de trabajos recientes en ciertos casos particulares (véase, por ejemplo, [1]). Todo ello plantea la pregunta de hasta qué punto es posible obtener, usando la gran criba, una cota en $(2N+1)^{m-1}$ para todos los polinomios palíndromos.

Referencias

[1] S. Chow y R. Dietmann, Enumerative Galois theory for cubic and quartics, *Adv. Math.* **372** (2020), 107282, 37 pp.

[2] H. Davenport y H. Halberstam, The values of a trigonometrical polynomial at well spaced points, *Mathematika* **13** (1966), 91–96; Corrigendum and Addendum, *Mathematika* **14** (1967), 229–232.

[3] S. Davis, W. Duke y X. Sun, Probabilistic Galois theory of reciprocal polynomials, *Exposition. Math.* **16** (1998), 263–270.

[4] P. X. Gallagher, The large sieve and probabilistic Galois theory, *Analytic number theory* (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, 1972), 91–101. Amer. Math. Soc., Providence, R. I., 1973.

[5] D. Hernández y Y. Laszlo, *Introduction à la théorie de Galois*, Éditions de l'École Polytechnique, 2012.

[6] M. N. Huxley, The large sieve inequality for algebraic number fields, *Mathematika* **15** (1968), no. 2, 178–187.

[7] E. Kowalski, *The large sieve and its applications. Arithmetic geometry, random walks and discrete groups*, Cambridge Tracts in Mathematics **175**, Cambridge University Press, Cambridge, 2008.

[8] P. Lindstrøm, *Galois theory of palindromic polynomials*, MS thesis, University of Oslo, 2015; disponible en `https://www.duo.uio.no/bitstream/handle/10852/45298/PiaLindstromMasteroppgave.pdf`.

[9] Y. V. Linnik, The large sieve, *C. R. (Doklady) Acad. Sci. URSS (N.S.)* **30** (1941), 292–294.

[10] H. Meyn y W. Götz, Self-reciprocal polynomials over finite fields, *Séminaire Lotharingien de Combinatoire* (Oberfranken, 1990), 82–90, *Publ. Inst. Rech. Math. Av.* **413**, Univ. Louis Pasteur, Strasbourg, 1990.

[11] H. L. Montgomery, The analytic principle of the large sieve, *Bull. Amer. Math. Soc.* **84** (1978), no. 4, 547–567.

[12] H. L. Montgomery y R. C. Vaughan, The large sieve, *Mathematika* **20** (1973), no. 2, 119–134.

[13] A. Selberg, On an elementary method in the theory of primes, *Norske Vid. Selsk. Forh., Trondhjem* **19** (1947), no. 18, 64–67.

[14] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, Belin Éducation, 2008.

[15] B. L. van der Waerden, Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt, *Monatsh. Math. Phys.* **43** (1936), no. 1, 133–147.

Mathieu Da Silva, Département de mathématiques, École normale supérieure Paris-Saclay, 4 Avenue des Sciences, 91190 Gif-sur-Yvette, France

Correo electrónico: `mathieu.da_silva@ens-paris-saclay.fr`