Hoja 3 CRIPTOGRAFÍA 2024–2025

Plazo y modo de entrega: Hasta las 23:59 del 25 de mayo. Se debe subir a Moodle un solo fichero PDF de a lo más ocho páginas y 6MB[1].

Calificación: El ejercicio 3 se puntuará sobre 40, el resto sobre 20, de modo que la calificación máxima es 100. Se valorará la elegancia y la concisión de las soluciones.

Observaciones:

- En el ejercicio 1 solo se pide la existencia de la base $\{f_j\}_{j=1}^d$, no hay que hallarla explícitamente.
- En el ejercicio 2 aparecen números grandes, necesitarás una calculadora u ordenador. Recuerda que $\tau(1) = 1$, $\tau(2) = -24$ y $\tau(3) = 252$.
- Se dice que $\alpha \in \mathbb{C}$ es un *entero algebraico* de grado n si $P(\alpha) = 0$ para $P \in \mathbb{Z}[x]$ mónico irreducible.
- Se puede dar por conocido que $e^{-\pi x^2}$ es su propia transformada de Fourier, pero ninguna transformada explícita más.

1) Sea $d = \dim S_k > 0$ y usemos el convenio $E_0 = 1$. Demuestra que $\left\{\Delta^j E_4^{3(d-j)} E_{k-12d}\right\}_{j=1}^d$ es una base de S_k con coeficientes de Fourier enteros. A partir de ello, demuestra también que existe una base $\{f_j\}_{j=1}^d$ tal que $f_j(z) = e^{2\pi ijz} + \sum_{n=d+1}^\infty a_n^{(j)} e^{2\pi inz}$ con $a_n^{(j)} \in \mathbb{Z}$.

2) Según la teoría, $\mathcal{B} = \{E_4^3\Delta, E_6^2\Delta\}$ es una base de $\mathcal{S}_{24}$. Halla la matriz de T_2 en dicha base, diagonalízala y utiliza el resultado para hallar una base de formas de Hecke.

3) Explica por qué T_n tiene una matriz con coeficientes enteros en la base $\{f_j\}_{j=1}^d$ del primer ejercicio y demuestra que toda forma de Hecke en $\mathcal{S}_k$ tiene coeficientes de Fourier que son enteros algebraicos de grado a lo más $k/12$.

4) Para $A \in \mathrm{SL}_d(\mathbb{R})$ con d múltiplo de 8 definimos

$$f_A(z) = \sum_{\vec{n}\in\mathbb{Z}^d} e^{\pi iz\|A\vec{n}\|^2} \qquad \text{con} \quad z \in \mathbb{H}.$$

Sea B es la matriz formada por los cofactores de A (a veces también llamada matriz adjunta). Comprueba que $B \in \mathrm{SL}_d(\mathbb{R})$ y, aplicando la fórmula de sumación de Poisson en dimensión d, demuestra la identidad $f_A(z) = z^{-d/2} f_B(-1/z)$.

---

[1] Si tienes problemas con el tamaño del fichero o para pasar tu documento a PDF, usa por ejemplo la aplicación gratuita *online* `https://www.ilovepdf.com/`.