Hoja 1 Criptografía 2024–2025

Plazo y modo de entrega: Hasta las 23:59 del 27 de marzo. Se debe subir a Moodle un solo fichero PDF de a lo más ocho páginas y 6MB[1].

Calificación: A pesar de que los ejercicios tienen diferente dificultad y extensión, cada uno se puntuará sobre 20, de modo que la calificación máxima es 100. Se valorará la elegancia y la concisión de las soluciones.

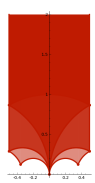
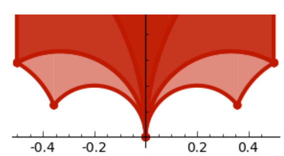
---

1) Para p primo y $\alpha \in \mathbb{Z}^+$, demuestra que $\left|\mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z})\right| = p^{3\alpha} - p^{3\alpha-2}$. Utiliza el teorema chino del resto para concluir $\left|\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\right| = N^3 \prod_{p|N} \left(1 - p^{-2}\right)$ para $N > 1$, que se dio por supuesto en una de las clases.

2) Considera el cifrado de Hill con $p = 11$ y $n = 3$. Halla la clave sabiendo que los vectores $(5,1,0)$, $(7,2,0)$ y $(0,0,2)$ se encriptan, respectivamente, como $(1,2,1)$, $(0,1,0)$ y $(3,1,1)$. Calcula también cómo se encriptaría $(1,2,3)$.

3) Explica por qué los únicos puntos de $\overline{\mathcal{F}}$ que permanecen fijos por elementos elípticos del grupo modular $\mathrm{SL}_2(\mathbb{Z})$ son i, $e^{\pi i/3}$ y $e^{2\pi i/3}$.

4) Prueba que el grupo $\Gamma_0(5)$ admite un dominio fundamental del tipo

$\mathcal{D} =$  Detalle de la parte inferior: 

Halla explícitamente los 5 vértices de este polígono (excluyendo $i\infty$). Nota: Los diferentes tonos de rojo son solo una pequeña ayuda.

5) Demuestra que $j(i) = 1728$.

---

[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/`.