
Plazo: Hasta las 23:59 del 21 de noviembre.

Modo de entrega: Subir a Moodle un fichero PDF de a lo más dos caras y menos de 6MB.

Calificación: Resolver correctamente el problema añade un punto a los extras. Se puede conseguir otro 0.25 probando la conjetura de c).

Originalidad: Se permite colaborar para pensar el problema, pero las redacciones de la solución deben ser individuales y distintas. Se te puede requerir que me expliques la solución para conseguir la calificación si tengo indicios de que no la entiendes.

---

1) Para $p > 2$ primo, considera el grupo multiplicativo de matrices

$$\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) = \{M \in \mathcal{M}_{2\times 2}(\mathbb{Z}/p\mathbb{Z}) \,:\, \det M = 1\}.$$

a) [25 %] Calcula el cardinal de $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.

b) [65 %] ¿Cuál es el máximo orden que puede tener una matriz $A \in \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ si satisface que $\mathrm{tr}(A) - 2$ y $\mathrm{tr}(A) + 2$ son o bien ambos residuos cuadráticos o bien ambos no residuos cuadráticos módulo p?

c) [10 %] Enuncia una conjetura para el máximo orden sin imponer condiciones sobre la traza e ilústrala mencionando una matriz para $p = 5$ y otra para $p = 7$ que creas que tienen orden máximo.

Aclaraciones y ayuda:

- Recuerda que $\mathrm{tr}(A)$ significa la traza de A, esto es, $a_{11} + a_{22}$.
- Debes dar una demostración correcta para que la solución de b) sea válida. En realidad el máximo se alcanza siempre cuando ambos son no residuos, pero eso es más difícil.
- Indicación para b): ¿podrías diagonalizar A sobre $\mathbb{Z}/p\mathbb{Z}$?
- Si das una prueba de la conjetura de c) obtendrás 0.25 extra.
- Si deseas usar `sagemath` (`https://sagecell.sagemath.org/`) para hacer cálculos, una manera de hallar el orden módulo `p` de una matriz con elementos `a`, `b`, `c`, `d` es:

```
A = matrix(GF(p),2,2,[a,b,c,d])
B = A
k = 1
while B!=matrix.identity(GF(p), 2):
    k = k+1
    B *= A
print('El orden es:',k)
```

Recuerda sustituir `p`, `a`, `b`, `c` y `d` por los valores que estés considerando. Los comandos para el símbolo de Legendre $\left(\frac{a}{p}\right)$ y la traza $\mathrm{tr}(A)$ son `kronecker_symbol(a, p)` y `A.trace()`.