

Ejercicio para entregar N° 2

Instrucciones:

- Elegir **uno** de los dos ejercicios que están abajo y resolverlo detalladamente.
- Se sugiere fuertemente tipear las soluciones en L^AT_EX. Enviar el correspondiente archivo .pdf por mail a msaucedo@dm.uba.ar con asunto **Ejer2**. Excepcionalmente pueden también entregar soluciones escritas a mano llevándolas a clase, pero tienen que estar prolijas y legibles.
- En todos los casos, la fecha límite de entrega es: **Viernes 17 de Noviembre**.

Opción 1. En 1837 Dirichlet probó el siguiente teorema: dados $n > 1$ y $r \in \mathbb{Z}$ coprimo con n , existen infinitos primos p tales que $p \equiv r \pmod{n}$. El objetivo de este ejercicio es probar el caso particular $r = 1$.

Denotamos Φ_n al n -ésimo polinomio ciclotómico (que sabemos que tiene coeficientes en $\mathbb{Z}$).

- a) Sea $a \in \mathbb{Z}$ y sea p un primo que divide a $\Phi_n(a)$. Probar que p no divide a a , y que si p no divide a n entonces necesariamente $p \equiv 1 \pmod{n}$.
- b) Sean $p_1, p_2, \dots, p_k$ números primos distintos. Encontrar un valor de $a \in \mathbb{Z}$ tal que en la factorización en primos de $\Phi_n(a)$ no aparezca ningún p_i ni ningún primo que divida a n .
- c) Probar que el conjunto de los números primos congruentes a 1 módulo n es infinito.

Opción 2. Vimos en clase que un número $\alpha \in \mathbb{R}$ se puede construir con regla y compás si y sólo si existe una torre de cuerpos $\mathbb{Q} = K_0 \subset K_1 \subset \dots \subset K_r \subset \mathbb{R}$ tal que $[K_i : K_{i-1}] = 2$ para $i = 1, \dots, r$ y $\alpha \in K_r$.

- a) Probar que si L es un subcuerpo de $\mathbb{R}$ tal que $L/\mathbb{Q}$ es una extensión **normal** cuyo grado es una potencia de 2, entonces todo $\alpha \in L$ es construible.
- b) Sea $\alpha \in \mathbb{R}$ algebraico sobre $\mathbb{Q}$, sea f su polinomio minimal y sea L un cuerpo de descomposición de f sobre $\mathbb{Q}$. Supongamos que $L \subset \mathbb{R}$ (es decir, que todas las raíces de f son reales). Probar que α es construible si y sólo si $[L : \mathbb{Q}]$ es una potencia de 2.
- c) (Opcional) Pensar cómo se pueden adaptar los resultados anteriores para no tener que suponer $L \subset \mathbb{R}$.