Pontificia Universidad Católica de Chile
Facultad de Matemáticas

Profesor: Ricardo Menares | **Ayudante:** José Cuevas Barrientos
Curso: Teoría de Números | **Sigla:** MAT2814
Fecha: 28 de agosto de 2025

Caracteres de Dirichlet

1. Ejercicios

1. Pruebe que las siguientes dos afirmaciones son (elementalmente) equivalentes:
   a) Para cada par de enteros a, n coprimos hay infinitos primos p tales que $p \equiv a \pmod{n}$.
   b) Para cada par de enteros a, n coprimos hay al menos un primo p tal que $p \equiv a \pmod{n}$.
2. Sea $a \in \mathbb{Z}$. Pruebe que si para todo primo $p \nmid a$ se cumple que $(a/p) = 1$, entonces a es un cuadrado perfecto.
3. Pruebe que el grupo de caracteres de Dirichlet módulo n es isomorfo a $(\mathbb{Z}/n\mathbb{Z})^\times$, no canónicamente.
4. Pruebe que para un primo p y un natural $a \in \mathbb{N}_{\geq 2}$ se cumple que
$$(\mathbb{Z}/p^a\mathbb{Z})^\times \cong \begin{cases} C_2, & p = 2,\ a = 2, \\ C_2 \times C_{2^{a-2}}, & p = 2,\ a > 2, \\ C_{p-1} \times C_{p^{a-1}}, & p > 2,\ a \geq 2. \end{cases}$$
   Pista: Para un primo impar p equivale a buscar una raíz primitiva módulo p; para el primo $p = 2$ podemos calcular la 2 y 4-torsión del grupo. □
5. **Un criterio excéntrico de primalidad:** Sea $p = a_d b^d + \cdots + a_1 b + a_0$ un primo $p > b$ en base $b \geq 3$ y sea $f(x) = a_d x^d + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$.
   a) Supongamos que $f(x)$ fuese reducible. Pruebe que existe una raíz $\alpha \in \mathbb{C}$ de f tal que $|b - \alpha| \leq 1$.
   b) Sea α como en el inciso anterior. Pruebe que $\operatorname{Re}(1/\alpha) > 0$, pero que $\operatorname{Re}(1/\alpha^j) < 0$ para algún j.
   c) Pruebe que
$$\operatorname{Re}\left(\frac{f(\alpha)}{\alpha^d}\right) \geq \frac{b-3}{b-2} + a_{d-1}\operatorname{Re}(1/\alpha),$$
   y concluya, por contradicción, que f debía ser irreducible.
   Pista: Dé una cota inferior para $a_{d-n}\operatorname{Re}(1/\alpha^n)$ cuando $n \geq 2$. □
6. Demuestre, empleando el teorema de los números primos en progresión aritmética, que para todo $n \geq 2$ existe un entero algebraico irracional $\gamma \in \mathbb{C} \setminus \mathbb{Q}$ de grado n tal que $\gamma \in \mathbb{Z}[\gamma]$ es irreducible.

Teorema 1.1: Sean a, n un par de enteros coprimos y $\pi(x; a, n)$ la función que cuenta primos $p \leq x$ tales que $p \equiv a \pmod{n}$. Entonces
$$\pi(x; a, n) \sim \frac{1}{\phi(n)} \frac{x}{\log x}, \qquad x \to \infty,$$
donde ϕ es la función de Euler.

Demostración: Vid. [**2**, pág. 361]. □

Referencias y lecturas adicionales

1. Granville, A. *Number Theory Revealed. A Masterclass* (American Mathematical Society, 2020).
2. Tenenbaum, G. *Introduction à la théorie analytique et probabiliste des nombres* 4.ª ed. (Berlin, 2015).

Correo electrónico: josecuevasbtos@uc.cl
URL: https://josecuevas.xyz/teach/2025-2-num/