Pontificia Universidad Católica de Chile
Facultad de Matemáticas

Profesor: Ricardo Menares
Ayudante: José Cuevas Barrientos
Curso: Teoría de Números
Sigla: MAT2814
Fecha: 22 de agosto de 2025

Más sobre DFUs

1. Números de Fermat

1. Sea p un número primo.
   a) Pruebe que, dado un natural $n = n_0 + n_1 p + \cdots + n_d p^d$ en base p, se cumple que
   $$(x+y)^n \equiv (x+y)^{n_0}(x^p+y^p)^{n_1}\cdots\left(x^{p^d}+y^{p^d}\right)^{n_d} \pmod{p}.$$
   b) **Teorema de Lucas:** Sea $m = m_0 + m_1 p + \cdots + m_d p^d \leq n$ otro natural en base p. Pruebe que
   $$\binom{n}{m} \equiv \binom{n_0}{m_0}\binom{n_1}{m_1}\cdots\binom{n_d}{m_d} \pmod{p}.$$
2. Pruebe que si un número de la forma 2^m+1 es primo, entonces necesariamente m es una potencia de dos. Los números de la forma $F_n := 2^{2^n}+1$ se llamarán ***de Fermat***.
3. Pruebe que los números de Fermat son coprimos dos a dos y, con ello, dé una nueva demostración de la infinitud de los primos.
4. Diremos que un dominio íntegro A es ***íntegramente cerrado*** si para todo $\alpha \in \mathrm{Frac}(A)$ tal que existe un polinomio mónico $f(x) \in A[x]$ con $f(\alpha) = 0$, se cumple que $\alpha \in A$. Pruebe que si A es un DIP, entonces es íntegramente cerrado. Con ello concluya que $\mathbb{Z}[n\gamma]$ no es un DFU para $n > 2$ cuando $\gamma \in \mathbb{C} \setminus \mathbb{Q}$ es un entero algebraico.
   Pista: Trate primero de probar que $\mathbb{Z}$ es íntegramente cerrado y generalice. □
5. Sea q una potencia de un primo p, y sea $K := \mathbb{F}_q$.
   a) Pruebe que para un natural $n \in \mathbb{N}$ se cumple que
   $$\sum_{x\in K} x^n = \begin{cases} -1, & q-1 \mid n,\ n \neq 0, \\ 0, & \text{en otro caso.} \end{cases}$$
   b) **Teorema de Chevalley-Warning:** Sean $\{f_\alpha(\boldsymbol{x})\}_\alpha \in K[x_1,\ldots,x_n]$ un conjunto finito de polinomios tales que $\sum_\alpha \deg(f_\alpha) < n$. Sea $V := \mathbf{V}(\{f_\alpha\}) \subseteq K^n$ el conjunto de ceros comunes de los polinomios, entonces pruebe que $|V| \equiv 0 \pmod{p}$.
   Pista: Note que $|V| = \sum_{\boldsymbol{x}\in K^n} \chi_V(\boldsymbol{x})$, donde χ es la función característica. Ahora recupere χ_V mediante polinomios y emplee el inciso anterior. □

Referencias y lecturas adicionales

1. Granville, A. *Number Theory Revealed. A Masterclass* (American Mathematical Society, 2020).
2. Serre, J.-P. *A course in arithmetic* (Springer-Verlag, 1973).

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