**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.

## 2. Más sobre DFUs

4. **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 $\alpha$ 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 $n \geq 2$. □
5. Diremos que un número algebraico $\gamma \in \mathbb{C}$ es un ***entero algebraico*** si su polinomio minimal tiene coeficientes en $\mathbb{Z}$. Demuestre, empleando el postulado de Bertrand, 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 2.1 (postulado de Bertrand):** Para todo entero $n \geq 2$ existe un primo $p$ tal que $n/2 < p \leq n$.

6. Sea $\gamma \in \mathbb{C} \setminus \mathbb{Q}$ un entero algebraico cuadrático. Pruebe que existen infinitos $n \in \mathbb{Z}$ tales que $n\gamma \in \mathbb{Z}[n\gamma]$ es irreducible y...

## Referencias y lecturas adicionales

1. Granville, A. *Number Theory Revealed. A Masterclass* (American Mathematical Society, 2020).

*Correo electrónico*: josecuevasbtos@uc.cl