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

Reciprocidad cuadrática y otros temas

1. Ejercicios

1. Pruebe que un primo p es suma de dos cuadrados syss $p = 2$ o $p \equiv 1 \pmod 4$.
2. **Criterio de Pépin:** Mediante reciprocidad cuadrática pruebe que si el número de Fermat $F_n := 2^{2^n} + 1$ (con $n > 0$) es primo syss $3^{\frac{1}{2}(F_n - 1)} \equiv -1 \pmod{F_n}$.
3. Diremos que un dominio íntegro A es ***íntegramente cerrado*** si para todo $\alpha \in \operatorname{Frac}(A)$ 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 DFU, 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. □
4. Sea q una potencia de un primo p, y sea $K := \mathbb{F}_q$.
   a) Pruebe que $K^\times$ es un grupo cíclico.
   b) Pruebe que para un natural $n \in \mathbb{N}$ se cumple que
   $$\sum_{x \in K} x^n = \begin{cases} -1, & q - 1 \mid n,\ n \neq 0, \\ 0, & \text{en otro caso.} \end{cases}$$
   c) **Teorema de Chevalley-Warning:** Sean $\{f_\alpha(\boldsymbol{x})\}_\alpha \in K[x_1, \dots, x_n]$ 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. □
5. 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
   $$\binom{n}{m} \equiv \binom{n_0}{m_0} \binom{n_1}{m_1} \cdots \binom{n_d}{m_d} \pmod p.$$

A. Ejercicios adicionales

1. 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***.
2. Pruebe que los números de Fermat son coprimos dos a dos y, con ello, dé una nueva demostración de la infinitud de los primos.

B. Comentarios adicionales

Una de las consecuencias del teorema de Chevalley-Warning (y parte del interés detrás de esta proposición) está en que muestra que los cuerpos finitos son *cuasialgebraicamente cerrados*. En lenguaje de geometría algebraica, un cuerpo es algebraicamente cerrado si toda variedad algebraica no vacía tiene puntos racionales. Piense el lector en la curva dada por los ceros del polinomio $x^2 + y^2 = 1$, es un círculo y eligiendo un punto base como $(1, 0)$ vemos que tras trazar una recta de pendiente p (con el convenio de que la vertical corresponde a $p = \infty$), vemos que hay una biyección con los puntos de ésta y los de la recta proyectiva $\mathbb{P}^1$.

La curva $x^2 + y^2 = -1$ tiene la misma suerte si nos paramos en el punto $(\sqrt{-1}, 0)$ que es «racional» sobre $\mathbb{C}$, de modo que vemos que toda cónica no degenerada es isomorfa a la recta proyectiva. Pero sobre $\mathbb{Q}$, ésta curva no tiene puntos racionales, de modo que no es una recta proyectiva, pese a que la razón tiene solo que ver con el cuerpo base, no con la «geometría interna» de la curva. Esta clase de variedades se llaman ***de Brauer-Severi***; mediante el teorema de Chevalley-Warning uno puede probar que sobre un cuerpo finito no hay variedades de Brauer-Severi salvo por los espacios proyectivos $\mathbb{P}^n$.

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/`