Álgebra II

Primer Cuatrimestre - 2025

Práctica 0

Sobre primos, para entrar en calor

Comencemos con algunos recuerdos de Álgebra I:

Teorema 1 (Pequeño Teorema de Fermat)**.** *Sea p un primo y $a \in \mathbb{Z}$ coprimo con p. Entonces*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Teorema 2 (Teorema Chino del Resto)**.** *Sean $a_1, \ldots, a_n \in \mathbb{Z}$, y $m_1, \ldots, m_n \in \mathbb{N}$ coprimos dos a dos. Existe $m \in \mathbb{Z}$ tal que para todo $1 \leq i \leq n$*

$$m \equiv a_i \pmod{m_i},$$

y m resulta único módulo $\prod_{i=1}^{n} m_i$.

1. Sean $a \in \mathbb{Z}$, $h \in \mathbb{N}$ y p un número primo.

(I) Sea $\sigma(a) = \min\{\ell : a^\ell \equiv 1 \pmod{p}\}$. Demostrar que si $a^h \equiv 1 \pmod{p}$ entonces $\sigma(a) \mid h$.

(II) Sean p y q primos impares. Si $p \mid 2^q - 1$, entonces $p > q$. Deducir que existen infinitos primos.

2 (Teorema de Wilson)**.** Demostrar que un entero p es primo si y solo si $(p-1)! \equiv -1 \pmod{p}$.

3. Demostrar que:

(I) existen infinitos números primos, considerando los números de la forma $(p_1 \cdots p_n) + 1$ donde $p_1, \ldots, p_n$ son primos distintos.

(II) existen infinitos números primos congruentes a 3 módulo 4, considerando los números de la forma $4(p_1 \cdots p_n) + 3$ donde $p_1, \ldots, p_n$ son primos distintos.

4. Sean p un número primo, m un número entero coprimo con p y r un número natural. Demostrar que p *no* divide a $\binom{p^r m}{p^r}$. Es decir,

$$p \nmid \binom{p^r m}{p^r}.$$

5. Sea $p \in \mathbb{Z}$ un número primo.

(I) Sean $n \in \mathbb{N}_0$ y $a_0, ..., a_n$ enteros tales que a_n es coprimo con p. Demostrar que la ecuación

$$a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 \equiv 0 \pmod{p}$$

tiene a lo sumo n soluciones no congruentes módulo p.

(II) Demostrar que $X^2 - X \equiv 0\ (6)$ tiene 4 soluciones. ¿Contradice esto al ítem anterior?

6. Sea $\varphi : \mathbb{N} \to \mathbb{N}$ la *función totiente de Euler* definida por

$$\varphi(n) = \#\{k \in \mathbb{N} : k \leq n,\ (k : n) = 1\}.$$

Demostrar las siguientes afirmaciones:

(I) Para todo $n > 2$, $\varphi(n)$ es par.

(II) Existe $k \geq 1$ tal que $n = 2^k$ si y sólo si $\varphi(n) = \frac{n}{2}$.

7. Sea p un número primo congruente a 3 módulo 4.

(I) Demostrar que *no* hay una raíz primitiva de la unidad de orden 4 módulo p. Es decir, no existe un entero a tal que $a^4 \equiv 1 \pmod{p}$ con a, a^2, a^3 no congruentes a 1 módulo p. Concluir que $X^2 \equiv -1 \pmod{p}$ no tiene solución.

(II) Sean $a, b \in \mathbb{Z}$. Demostrar que si $p \mid a^2 + b^2$ entonces $p \mid a$ y $p \mid b$. Deducir que un primo congruente a 3 módulo no es suma de dos cuadrados en $\mathbb{Z}$.

8. ($\star$) Sean $p \in \mathbb{Z}$ un primo impar y a un entero coprimo con p. Demostrar las siguientes afirmaciones:

(I) El entero $a^{\frac{p-1}{2}}$ es congruente a 1 o -1 módulo p.

(II) Si existe $x \in \mathbb{Z}$ tal que $a \equiv x^2 \pmod{p}$ entonces $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

(III) Los enteros $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ no son congruentes entre sí módulo p.

(IV) Si $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ entonces existe $x \in \mathbb{Z}$ tal que $a \equiv x^2 \pmod{p}$.

Sugerencia: considerar las soluciones de $X^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$.

(V) El entero a no es un cuadrado módulo p si y sólo si $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

(VI) Si p es de la forma $4k + 1$ para algún $k \in \mathbb{Z}$, entonces -1 es un cuadrado módulo p. Deducir que -1 es un cuadrado módulo p si y sólo si es de la forma $4k + 1$.

Sugerencia: observar que $\frac{p-1}{2} = 2k$ y usar el ítem anterior.

(VII) Si $k \in \mathbb{N}$ y $p = 4k + 1$ entonces $(2k)!$ es solución de $X^2 \equiv -1 \pmod{p}$.