Álgebra II
Práctica 0 - Sobre primos, para entrar en calor

Recuerdo de Álgebra I:

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

$$a^{p-1} \equiv 1\ (p).$$

- *(Teorema Chino del Resto)* Sean $a_1, \ldots, a_n \in \mathbb{Z}$, y $m_1, \ldots, m_n \in \mathbb{N}$ tales que $(m_i : m_j) = 1$ para $i \neq j$. Entonces existe $m \in \mathbb{Z}$ tal que $m \equiv a_i\,(m_i), \forall i$, y que m es único módulo $\prod_{i=1}^{n} m_i$.

1. i) Sea $\sigma(a) = \text{mín}\{\ell : a^\ell \equiv 1\,(p)\}$. Probar que si $a^h \equiv 1\,(p)$ 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)* Sea $p \in \mathbb{Z}$. Probar que

$$p \text{ es primo } \Leftrightarrow (p-1)! \equiv -1\ (p).$$

3. Considerando los números de la forma $q = 2 \cdot 3 \cdot 5 \cdots p + 1$ concluir que existen infinitos primos.

4. Sea $p = 4k + 3$, para algún $k \in \mathbb{Z}$, un número primo.

i) Probar que *no* hay una raíz primitiva del unidad de orden 4 módulo p, es decir, no existe un entero a tal que $a^4 \equiv 1(p)$ pero a, a^2, a^3 no son congruentes a 1 módulo p. Concluir que $X^2 \equiv -1\,(p)$ no tiene solución.

ii) Sean $a, b \in \mathbb{Z}$. Probar que si $p \mid a^2 + b^2$ entonces $p \mid a$ y $p \mid b$. Deducir que un primo de la forma $4k + 3$ no es suma de dos cuadrados en $\mathbb{Z}$.

5. Probar que hay infinitos primos de la forma $4k + 1$. *Sugerencia* Considerar los enteros de la forma $(2p_1 \cdots p_r)^2 + 1)$.

6. Probar que hay infinitos primos de la forma $4k + 3$. *Sugerencia* Considerar los enteros de la forma $4p_1 \ldots p_s + 3$, $p_i \neq 3$.

7. Sea $p \in \mathbb{Z}$ primo.

i) Sean $a_i \in \mathbb{Z}$, $0 \leq i \leq n$, con $(a_n : p) = 1$. Probar que la ecuación

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

tiene a lo sumo n soluciones no congruentes módulo p.

ii) Probar que $X^2 - X \equiv 0\ (6)$ tiene 4 soluciones. ¿Contradice esto el ítem anterior?

8. Sean $p \in \mathbb{Z}$ un primo impar y a un entero coprimo con p. Probar 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 $a \equiv x^2\ (p)$ entonces $a^{\frac{p-1}{2}} \equiv 1\,(p)$.

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

iv) Si $a^{\frac{p-1}{2}} \equiv 1\,(p)$ entonces existe $x \in \mathbb{Z}$ tal que $a \equiv x^2\,(p)$. *Sugerencia:* considerar las soluciones de $X^{\frac{p-1}{2}} - 1 \equiv 0\ (p)$.

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

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 item anterior.

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

9. Determinar todas las soluciones no congruentes entre sí de las ecuaciones

i) $X^2 \equiv -1\,(5)$

ii) $X^2 \equiv -1\,(17)$

10. Factorizar módulo 5 el polinomio $p = 6X^4 - 18X^3 + 4X^2 + 9X - 6$.

11. *(Función φ de Euler)* Sea $\varphi : \mathbb{N} \to \mathbb{N}$ la *función totiente de Euler* definida por

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

Probar 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 $\varphi(n) = \frac{n}{2}$.

iii) Para todo m tal que $n \mid m$ vale que $\varphi(n) \mid \varphi(m)$.

iv) Para todo $n \in \mathbb{N}$ vale

$$\sum_{d|n} \varphi(d) = n.$$

v) Para todo $n \geq 2$ vale

$$\sum_{k \leq n, (k:n)=1} k = \frac{n}{2}\varphi(n).$$

vi) Para todo k existen finitas soluciones de $\varphi(n) = k$.

12. *(Teorema de Euler, generalización del Pequeño Teorema de Fermat)* Sean $a, n \in \mathbb{N}$ coprimos. Definimos la función

$$\begin{array}{rccc} r_n : & R_n := \{c \in \mathbb{N} : c \leq n,\ (c:n) = 1\} & \longrightarrow & \mathbb{N} \\ & c & \longmapsto & a \cdot c\ (n). \end{array}$$

i) Probar que r_n es una biyección de R_n en si mismo.

ii) Sean $c_1, c_2, \ldots c_{\varphi(n)}$ los elementos de R_n. Probar que

$$c_1 \cdot c_2 \cdots c_{\varphi(n)} \equiv ac_1 \cdot ac_2 \cdots ac_{\varphi(n)}\,(n).$$

Deducir que $a^{\varphi(n)} \equiv 1\ (n)$. Si n es primo, observar que el Teorema de Euler implica el Pequeño Teorema de Fermat.

iii) Probar que $c_1 \cdot c_2 \cdots c_{\varphi(n)} \equiv -1\ (n)$.

iv) Calcular $r_{20}(2033^{4754})$.

13. *(Conjetura de Carmichael)* Sea $k \in \mathbb{N}$. Probar que si $\varphi(n) = k$ tiene solución, entonces tiene al menos dos soluciones.