

Algebra II - Práctica 0.

Segundo cuatrimestre de 2003.

1. (a) (Pequeño Teorema de Fermat) Sea p un primo, $(a, p) = 1$. Entonces

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

- (b) Sea $\sigma(a) = \min \{ \ell / a^\ell \equiv 1 \pmod{p} \}$. Probar que $a^h \equiv 1 \pmod{p} \Rightarrow \sigma(a) / h$.

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

- (d) (Teorema Chino del Resto) Sean $a_1, \dots, a_n \in \mathbb{Z}$, $m_1, \dots, m_n \in \mathbb{N}$ tales que $(m_i, m_j) = 1$ para $i \neq j$.

Probar que entonces existe $M \in \mathbb{Z}$ tal que $M \equiv a_i \pmod{m_i}, \forall i$ y que M es único módulo

$$\prod_{i=1}^n m_i.$$

- (e) (Teorema de Wilson) Probar que

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

2. (a) Probar que existen infinitos primos (otra forma). Considerar $q = (2 \cdot 3 \cdot 5 \dots p) + 1$.

- (b) Probar que si p es un primo de la forma $4k + 3$, entonces $X^2 \equiv -1 \pmod{p}$ NO tiene solución (o sea, -1 no es un cuadrado módulo p).

- (c) Probar que si p es un primo de la forma $4k + 3$ tal que $p/a^2 + b^2$ entonces p/a y p/b . Deducir que un primo de la forma $4k + 3$ no es suma de dos cuadrados en \mathbb{Z} .

- (d) Probar que hay infinitos primos de la forma $4k+1$. (Considerar $(2p_1 \dots p_r)^2 + 1$).

- (e) Probar que hay infinitos primos de la forma $4k + 3$. (Considerar $4p_1 \dots p_s + 3$, $p_i \neq 3$).

3. (a) Sea p primo. Consideremos

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

donde $a_i \in \mathbb{Z}$ y $(a_n, p) = 1$.

Probar que esta ecuación tiene, a lo sumo, n soluciones no congruentes módulo p .

- (b) $X^2 - X \equiv 0 \pmod{6}$ tiene 4 soluciones. ¿ Contradice esto i)?

4. Sea p un primo impar. Probar que

- (a) $(a, p) = 1 \Rightarrow a^{\frac{p-1}{2}} \equiv 1 \text{ ó } -1 \pmod{p}$.

- (b) Existe x tal que $a \equiv x^2 \pmod{p} \Rightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

- (c) $1^2, 2^2, \dots, (\frac{p-1}{2})^2$ son todos no congruentes módulo p .

- (d) $a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \Rightarrow \exists x/a \equiv x^2 \pmod{p}$.

- (e) a no es un cuadrado módulo $p \Leftrightarrow a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.
- (f) Si p es un primo de la forma $4k + 1$, entonces -1 es un cuadrado módulo p .
Deducir que $x^2 \equiv -1 \pmod{p} \Leftrightarrow p = 4k + 1$.
- (g) Probar que $(2k)!$ es solución de $X^2 \equiv -1 \pmod{p}$ si $p = 4k + 1$.

5. (a) Resolver completamente (encontrar todas las soluciones no congruentes módulo p)

$$X^2 \equiv -1 \pmod{5}; \quad X^2 \equiv -1 \pmod{17}; \quad X^2 \equiv 8 \pmod{17}$$

- (b) Factorizar módulo 5, $p(X) = 6X^4 - 18X^3 + 4X^2 + 9X - 6$.

6. (Función φ de Euler) Probar que:

- (a) $\varphi(n)$ es par, $\forall n > 2$.
- (b) $\varphi(n) = \frac{n}{2} \Leftrightarrow n = 2^k$ con $k \geq 1$.
- (c) $n/m \Rightarrow \varphi(n)/\varphi(m)$.
- (d) $\sum_{d|n} \varphi(d) = n$ para todo $n \in \mathbb{N}$.
- (e) $\sum_{k \leq n, (k,n)=1} k = \frac{1}{2}n\varphi(n)$ para todo $n \geq 2$.
- (f) Para todo k existen a lo sumo finitas soluciones de $\varphi(n) = k$.

7. (Teorema de Euler, generalización del Pequeño Teorema de Fermat)

- (a) Sea $(a, n) = 1$. Para todo $c \leq n$ tal que $(c, n) = 1$, se define una aplicación $c \rightarrow r_n(a.c)$. Probar que esta aplicación es una biyección del conjunto de restos coprimos con n en él mismo.
- (b) Sean $c_1, c_2, \dots, c_{\varphi(n)}$ esos restos. Probar que:

$$c_1 \cdot c_2 \dots c_{\varphi(n)} \equiv a c_1 a c_2 \dots a c_{\varphi(n)} \pmod{n}.$$

Deducir que $a^{\varphi(n)} \equiv 1 \pmod{n}$ (teorema de Euler). En particular, si $n = p$ es primo, deducir el Pequeño

Teorema de Fermat.

- (c) Probar que $c_1 c_2 \dots c_{\varphi(n)} \equiv -1 \pmod{n}$.
- (d) Calcular $r_{20}(2033^{4754})$.