*$2^{do}$ cuatrimestre 2004*

# Álgebra II

## Práctica 0

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

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

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

   *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 $a_1, \ldots, a_n \in \mathbb{Z}$, $m_1, \ldots, m_n \in \mathbb{N}$ tales que $(m_i, m_j) = 1$ para $i \neq j$.

   Probar que entonces existe $M \in \mathbb{Z}$ tal que $M \equiv a_i\,(m_i), \forall i$ y que $M$ es único módulo $\prod_{i=1}^{n} m_i$.

   *e*) (Teorema de Wilson) Probar que

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

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

   *b*) Probar que si $p$ es un primo de la forma $4k+3$, entonces $X^2 \equiv -1 \ (p)$ 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 $(2p_1 \ldots p_r)^2 + 1$).

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

3. *a*) Sea $p$ primo. Consideremos

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

   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*) $X^2 - X \equiv 0 \ (6)$ tiene $4$ soluciones. ¿ Contradice esto a)?

4. Sea $p$ un primo impar. Probar que

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

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

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

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

e) $a$ no es un cuadrado módulo $p \Leftrightarrow a^{\frac{p-1}{2}} \equiv -1\ (p)$.

f) Si $p$ es un primo de la forma $4k+1$, entonces $-1$ es un cuadrado módulo $p$. Deducir que $x^2 \equiv -1\ (p) \Leftrightarrow p = 4k+1$.

g) Probar que $(2k)!$ es solución de $X^2 \equiv -1\ (p)$ si $p = 4k+1$.

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

$$X^2 \equiv -1\ (5)\ ;\ X^2 \equiv -1\ (17)\ ;\ X^2 \equiv 8\ (17)$$

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

6. (Función $\varphi$ 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 $c \to r_n(a.c)$. Probar que esta aplicación es una biyección del conjunto de restos coprimos con $n$ en él mismo.

b) Sean $c_1, c_2, \ldots c_{\varphi(n)}$ esos restos. Probar que:

$$c_1.c_2 \ldots c_{\varphi(n)} \equiv ac_1ac_2 \ldots ac_{\varphi(n)}\ (n).$$

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

Teorema de Fermat.

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