Álgebra II
Segundo Cuatrimestre — 2007
Práctica 0

1. *a*) (Pequeño Teorema de Fermat) Sea p un primo, $(a, p) = 1$. Entonces
$$a^{p-1} \equiv 1(p).$$
b) Sea $\sigma(a) = \text{mín}\{l / a^l \equiv 1(p)\}$. Probar que $a^h \equiv 1(p) \Rightarrow \sigma(a) \mid h$.
c) Sean p y q primos impares. Si $p \mid 2^q - 1$, 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
$$p \text{ es primo } \iff (p-1)! \equiv -1(p)$$

2. *a*) Sea p primo. Consideremos
$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \equiv 0(p)$$
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)?

3. Sea p un primo impar. Probar que
a) $(a, p) = 1 \Rightarrow a^{\frac{p-1}{2}} \equiv 1$ ó $-1 \bmod p$.
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 $p \iff a^{\frac{p-1}{2}} \equiv -1(p)$.
f) Si p es un primo de la forma $4k + 1$, entonces -1 es un cuadrado módulo p. Deducir que $x^2 \equiv -1(p) \iff p = 4k + 1$.
g) Probar que $(2k)!$ es solución de $X^2 \equiv -1(p)$ si $p = 4k + 1$.

4. *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, $p(X) = 6X^4 - 18X^3 + 4X^2 + 9X - 6$.

5. (Función ϕ de Euler) Definimos $\phi(n)$ como la cantidad de números naturales $\leq n$ coprimos con n. Probar que:

   a) $\phi(p) = p - 1$ y $\phi(p^k) = (p-1)p^{k-1}$, para p primo.

   b) $\phi(n.m) = \phi(n).\phi(m)$ si $(n, m) = 1$.

   c) $\phi(n)$ es par, $\forall n > 2$.

   d) $\phi(n) = \frac{n}{2} \iff n = 2^k$ con $k \geq 1$.

   e) $\sum_{d/n} \phi(d) = n$ para todo $n \in \mathbb{N}$.

   f) $\sum_{k \leq n,(k,n)=1} k = \frac{1}{2} n\phi(n)$ para todo $n \geq 2$.

   g) Para todo k existen a lo sumo finitas soluciones de $\phi(n) = k$.

6. (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 $c_1, c_2, \ldots, c_{\phi(n)}$ esos restos. Probar que:

   $$c_1.c_2 \ldots c_{\phi(n)} \equiv ac_1.ac_2 \ldots ac_{\phi(n)}(n).$$

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

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

7. (Raíces de la unidad) Sea $n \in \mathbb{N}$ y sea $G_n = \{z \in \mathbb{C} / z^n = 1\}$. Probar que

   a) G_n tiene n elementos.

   b) $z, w \in G_n \Rightarrow z.w \in G_n$

   c) $w \in G_n \Rightarrow w^{-1} \in G_n$

8. Sean $n, m \in \mathbb{N}$. Probar que

   a) $G_n \cap G_m = G_{(n:m)}$

   b) $G_n \subset G_m \iff n \mid m$

Definición: Sea $n \in \mathbb{N}$ y sea $w \in \mathbb{C}$. Diremos que w es una *raíz n-ésima primitiva de la unidad* si $w \in G_n$ y para todo $z \in G_n$ existe $r \in \mathbb{N}$ tal que $z = w^r$.

9. *a*) Sea $n \in \mathbb{N}$, $w \in \mathbb{C}$ una raíz n-ésima primitiva de la unidad y $k \in \mathbb{N}$. Probar que w^k es una raíz n-ésima primitiva de la unidad si y sólo si $(n : k) = 1$.

   b) Deducir que la cantidad de raíces n-ésimas primitivas de la unidad es $\phi(n)$.