Algebra Lineal 1, agsto-dic, 2003.

Tarea num. 6
(Para el 19 sept, 2003)

Definiciones:

- Dados $d, n \in \mathbb{Z}$, $d \neq 0$, d divide a n si existe un $k \in \mathbb{Z}$ tal que $n = dk$. Notación: $d|k$.
- Un $p \in \mathbb{Z}$ es primo si (i) $p > 1$, (ii) p no tiene divisores positivos mas que 1 y p.
- El máximo comun divisor de dos enteros $a, b \in \mathbb{Z}$, $a, b \neq 0$, es el entero máximal d que divide a ambos a y b. Notación: $d = (a, b)$. Por ejemplo: $1 = (6, 7) = (7, 6) = (-6, 7)$, $4 = (8, 12)$.
- Se define una estructura de anillo en $\mathbb{Z}/n\mathbb{Z}$ por $[x] + [y] := [x + y]$, $[x][y] := [xy]$, con elementos nuetros para la suma y el producto $[0]$ y $[1]$ (resp).

Problemas

1. (a) Demuestra que el conjunto de números primos es infinito.

   Sugerencia: mirar las notas, pág. 29.

   (b) El ejercicio de la página 30 de las notas.

   (c) (Opcional) Demostrar que hay infinidad de primos de la forma $4k + 3$.

2. (a) (Ejercisio de la pág 32 de las notas) Sean $p_1, p_2, \ldots, p_k$ primos distintos, $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$, $N = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Encuentra el número de divisores positivos de N.

   (b) ¿Cuántos divisores positivos tiene 1000?

3. Sea p un primo. Demuestra que para todo $a \in \mathbb{Z}$, $a^p \equiv a \mod p$.

   Sugerencia: usar el "principio de casillas" como en la clase de 11 sept; ver la pág. 45 de las notas.

4. Sean a, b dos enteros, $b > 0$.

   (a) Demuestra que existen $q, r \in \mathbb{Z}$ tal que $a = bq + r$, $0 \leq r < b$. ¿Son únicos estos q, r?

   Sugerencia: Toma q como la parte entera de a/b, o sea $q := \max\{x \in \mathbb{Z} \mid x \leq a/b\}$.

   Terminología: r se llama el residuo de la división de a entre b.

   (b) Demuestra que si $a = bq + r$, $0 \leq r < b \Rightarrow (a, b) = (b, r)$.

   Terminología: La aplicación sucesiva de este inciso a un par de enteros a, b, $b > 0$, se llama el algoritmo de Euclides para el máximo común divisor de a y b: se divide primero el a entre b con residuo r_1, $0 \leq r_1 < b$. Si $r_1 = 0$ terminamos, ya que $b|a$ y $(a, b) = b$; si no, tenemos $(a, b) = (b, r_1)$ y volvemos a dividir la b entre r_1 con residuo r_2, $0 \leq r_2 < r_1$. Si $r_2 = 0$ terminamos, ya que $(a, b) = (b, r_1) = r_1$; si no, seguimos ... obteniendo una sucesión descreciente de residuos $r_1 > r_2 > r_3 \ldots$. En algun momento tenemos que obtener un residuo 0 y el algoritmo se termina, (a, b) siendo el último residuo positivo.

   (c) Encuentra $(1804, 328)$.

   Sugerencia: Aplica el algoritmo de euclides.

   (d) (Opcional) Escribe 2003 en base 7.

   (e) Demuestra que existen $x, y \in \mathbb{Z}$ tal que $(a, b) = ax + yb$.

   Sugerencia: es una consecuencia del algoritmo de Euclides; ver la pág 53 de las notas.

   (f) Encuentra x, y del u'ltimo inciso para $a = 1804$, $b = 328$.

   (g) Concluye que si $(a, n) = 1$, $n > 1$, entonces $[a] \in \mathbb{Z}_n$ tiene inversa multiplicativa.

   Sugerencia: $(a, n) = 1 \Rightarrow \exists x, y \in \mathbb{Z}$ tal que $1 = ax + ny \Rightarrow ax \equiv 1 \mod n$.

   (h) Concluye que $\mathbb{Z}_p$ es un campo si p es un primo.

   (i) Encontrar todas las inversas multiplicativas en $\mathbb{Z}_{31}$. Por ejemplo: $[2]^{-1} = [16]$.