Universidad de la República
Facultad de Ingeniería.

Examen de Matemática Discreta II

......de febrero de 2014

Número de Examen	Cédula	Nombre y Apellido

1. (*aa* **puntos)**

   a) Sean a, b, n enteros tales que $d = \text{mcd}(a, n)$, con $d \neq 1$ y $d \mid b$
   Demostrar que existen x_1 y x_2 soluciones de $ax = b$ mód (n) tales que $x_1 \neq x_2$ mód (n).
   (o bien preguntar) Hallar todas las soluciones de $ax = b$ mód (n). ¿Cuántas soluciones hay entre 1 y n?

   b) Resolver la ecuación diofántica $2x \equiv 14$ mód(80).

   c) Sea n el mayor natural que es solución de la ecuación de la parte anterior. Determinar cuántas raíces primitivas tiene $U(n)$, y hallar la menor de todas.

2. (*bb* **puntos)**

   a) Sea $\sigma \in S_n$ y $\sigma = c_1 \dots c_n$ producto de ciclos disjuntos.

      1) Escribir $o(\sigma)$ en función de $o(c_1), \dots, o(c_n)$

      2) Probar el resultado enunciado en 1).

   b) Considerar $\mathbb{Z}_{30}$. Exhibir elementos $a, b \in \mathbb{Z}_{30}$ tales que $o(a + b) <$mcm$(o(a), o(b))$.

   c) Dado $(G, \cdot)$ grupo finito y $x, y \in G$ con $xy = yx$ entonces, si $a = o(x)$, $b = o(y)$, $m =$mcm(a, b) y $d =$mcd(a, b), demostrar que $\frac{m}{d}|o(xy)$ y que $o(xy)|m$.

3. (*cc* **puntos)**

   a) Sean p,a b naturales tales que p es primo, $b \equiv 0$ mód$(p - 1)$, mcd$(a, p) = 1$
   Encontrar en función de p el menor natural n que verifica: $a^b x^3 + 8x \equiv 5x^2 + 4$ mód(p), con $x \neq 1$ mód(p).
   Solución: $n = p + 2$ (atención, yo creo que hay un pequeño error acá, revisar con cuidado)

   b) Sea n en natural hallado en la parte anterior, encontrar todas las soluciones del sistema:

$$\begin{cases} x \equiv 1 \text{ mód}(n - p) \\ x \equiv 2 \text{ mód}(5) \\ x \equiv -3 \text{ mód}(10) \end{cases}$$

   c) Sea m el menor natural que satisface el sistema de la parte b). Calcular $(n - p)^{10325}$ mód$(5m)$

   Solución: $10325 = 24 \times 430 + 5$ y $\varphi(5m) = \varphi(57) = \varphi(5)\varphi(7) = 24$.

4. (*dd* **puntos)**
   Ejercicio de Criptografía.