Soluciones del Examen de MD2
24 de Febrero de 2010

Solución al ejercicio 1.

a) Si $a_1, a_2, \ldots, a_n$ son enteros cualquiera y $m_1, m_2, \ldots, m_n$ son enteros coprimos 2 a 2 entonces el sistema de congruencias $X \equiv a_i \pmod{m_i}, \forall i = 1, 2, \ldots, n$ tiene solución. Si $A \in \mathbb{Z}$ es una solución particular entonces las soluciones del sistema viene dada por aquellos $x \in \mathbb{Z}$ que verifican $x \equiv A \pmod{M}$ donde $M = m_1 m_2 \ldots m_n$.

b) i) Observese que para que un número sea A-coherente, debe verificar el sistema de congruencias:

$$\begin{cases} n \equiv -a_0 & (\text{mód } a_1) \\ n \equiv -a_1 & (\text{mód } a_2) \\ \vdots & \\ n \equiv -a_9 & (\text{mód } a_{10}) \end{cases}$$

Como los módulos son coprimos dos a dos, por el Teorema del Resto Chino, la solución del sistema es de la forma $n \equiv A \pmod{M}$ donde $M = a_1 a_2 \ldots a_{10}$ y A una solución particular del sistema. Como $a_i < 10^2$ para $i = 1, 2, \ldots, 10$ entonces $M < (10^2)^{10} = 10^{20}$, por lo tanto existe alguna solución del sistema menor que 10^{20}.

ii) Cada intervalo de la forma $[10^{20}, 2 \cdot 10^{20}), [2 \cdot 10^{20}, 3 \cdot 10^{20}), \ldots, [9 \cdot 10^{20}, 10^{21})$ tiene longitud $10^{20} - 1 \geq M$, luego, en virtud del Teorema del Resto Chino en cada uno de esos intervalos habrá alguna solución al sistema y cada una de esas soluciones tendrá exactamente 21 dígitos (por estar entre 10^{20} y $10^{21} - 1$).

Ejercicio 2.

a) Por Bezout existen $\alpha, \beta \in \mathbb{Z}$ tales que $d = \alpha m + \beta m$, sea $x \in G$ y fijado x llamemos $y = x^\beta$. Observemos que $x^d = (x^\alpha)^m (x^\beta)^n = y^n$ (pues $x^\alpha \in G$ y $m = |G|$). Así que tenemos:

$$\varphi(x^d) = \varphi(y^n) = \varphi(y)^n = e_H$$

donde en la última igualdad se usa que $\varphi(y) \in H$ y $n = |H|$. Por lo tanto $x^d \in ker(\varphi)$ como queríamos probar.

b) Sean m_1 y m_2 los órdenes de G_1 y G_2 respectivamente, y denotemos por e_1 y e_2 al neutro de G_1 y G_2 respectivamente . Por ser $Im(\varphi_1)$ e $Im(\varphi_2)$ subgrupos de H se tiene que $e_H \in Im(\varphi_1) \cap Im(\varphi_2)$. Por otra parte, si $x \in Im(\varphi_1) \cap Im(\varphi_2)$ entonces para $i = 1, 2$ existe $g_i \in Im(\varphi_i)$ tales que $x = \varphi_i(g_i)$. Se tiene que $x^{m_i} = \varphi_i(g_i)^{m_i} = \varphi_i(g_i^{m_i}) = \varphi_i(e_i) = e_H$ para $i = 1, 2$. Como m_1 y m_2 son coprimos, usando nuevamente Bezout tenemos que $1 = \alpha m_1 + \beta m_2$ para ciertos enteros α y β, por lo tanto $x = x^1 = (x^{m_1})^\alpha (x^{m_2})^\beta = e_H \cdot e_H = e_H$.

Ejercicio 3.

i) Dos interlocutores A y B se ponen de acuerdo en un primo n y una raiz primitiva módulo n que llamaremos g (obs. tanto n como g son públicos). El interlocutor A elige en secreto un número a mientras que B hace lo propio eligiendo un número b (obs. solo A conoce a y solo B conoce b). El interlocutor A calcula $x = g^a \pmod n$ y se lo envia a B, el interlocutor B calcula $y = g^b \pmod n$ y se lo envia a A (obs. tanto x como y serán de dominio público). La clave común acordada será $k = g^{ab} \pmod n$ (A puede calcular k efectivamente como $y^a \pmod n$ mientras B la puede calcular efectivamente como $x^b \pmod n$).

ii) En este caso tenemos $a = 4$ e $y = 15$ (donde A soy yo y B mi interlocutor), así que puedo calcular la clave como $k = 15^4 \pmod{61}$, simplemente calculamos:

$$15^4 = (15^2)^2 \equiv 42^2 \equiv 56 \pmod{61}$$

por lo tanto la clave común es $k = 56$.

iii) Descomponemos $56 = 2 \cdot 2 \cdot 2 \cdot 7$ que corresponde la palabra CCCH (ver tabla).

iv) El mensaje desencriptado es "MAS VALE PAJARO EN MANO QUE CIEN VOLANDO".

v) El mensaje encriptado es: UCDOCUBWCNCITCU.