

Segundo parcial de Matemática Discreta II  
3 de julio del 2007

Soluciones.

**Ejercicio 1. (30 puntos)**

a. Ver teórico.

b.  $[2502]$  no es invertible módulo 30771 pues es múltiplo de 3.  
512 es invertible módulo 30771 y su inverso es  $[15686]$ .

c. Hay  $\varphi(30771) = \varphi(9)\varphi(13)\varphi(263) = 6 \cdot 12 \cdot 262 = 18864$  elementos en  $U_{30771}$ .

d. Observemos que como  $3|1500$  tenemos que  $1500^{9432} \equiv 0 \pmod{9}$ , como  $12|9432$  por el pequeño Teorema de Fermat  $1500^{9432} \equiv 1 \pmod{13}$ , como  $262|9432$  por el pequeño Teorema de Fermat  $1500^{9432} \equiv 1 \pmod{263}$ , así que  $1500^{9432}$  es solución del sistema de congruencias:

$$\begin{cases} x \equiv 0 & (\text{mód } 9) \\ x \equiv 1 & (\text{mód } 13) \\ x \equiv 1 & (\text{mód } 263) \end{cases} \Leftrightarrow \begin{cases} x \equiv 0 & (\text{mód } 9) \\ x \equiv 1 & (\text{mód } 3419) \end{cases}$$

De la primer congruencia  $x = 9y$ , sustituyendo en la segunda  $9y \equiv 1 \pmod{3419} \Leftrightarrow y \equiv 380 \pmod{3419} \Leftrightarrow x = 9y \equiv 3420 \pmod{30771}$ . Así que  $1500^{9432} \equiv 3420 \pmod{30771}$ .

**Ejercicio 2. (35 puntos)**

a. Sea  $x \in Z(G)$  y  $f \in \text{Aut}(G)$ , queremos probar que  $f(x) \in Z(G)$ . Si  $g \in G$  tenemos que  $gf(x) = f(f^{-1}(g))f(x) = f(f^{-1}(g)x) = f(xf^{-1}(g)) = f(x)f(f^{-1}(g)) = f(x)g$  así que  $f(x) \in Z(G)$ .

b. Consideramos los automorfismos  $i_g(x) = gxg^{-1}$ , si  $H$  es característico entonces  $gHg^{-1} = i_g(H) \subset H$  para todo  $g \in G$ , por lo tanto  $H \triangleleft G$ .

c.1.  $i_e(x) = exe^{-1} = x$  así que  $id = i_e \in \text{Int}(G)$ .

$$i_a i_b(x) = i_a(bxb^{-1}) = abxb^{-1}a^{-1} = abx(ab)^{-1} = i_{ab} \in \text{Int}(G).$$

$$i_a i_{a^{-1}} = i_{aa^{-1}} = i_e = id \text{ por lo tanto } i_a^{-1} = i_{a^{-1}} \in \text{Int}(G).$$

Si  $f \in \text{Aut}(G)$  tenemos que  $f i_g f^{-1}(x) = f(gf^{-1}(x)g^{-1}) = f(g)x f(g^{-1}) = f(g)x f(g)^{-1} = i_{f(g)}(x)$  así que  $f i_g f^{-1} = i_{f(g)} \in \text{Int}(G)$ .

c.2 Consideramos el morfismo  $f : G \longrightarrow \text{Int}(G)$  tal que  $f(g) = i_g$  (anteriormente probamos que  $i_a i_b = i_{ab}$  lo cual prueba que  $f$  es un morfismo de grupos). Por otra parte, tenemos que  $f(g) = i_g = id \Leftrightarrow i_g(x) = gxg^{-1} =$

$x, \forall x \in G \Leftrightarrow gx = xg, \forall x \in G \Leftrightarrow g \in Z(G)$ . Se concluye aplicando el primer teorema de isomorfismo.

d. 1. Es claro que  $id \in Z(S_n)$ , supongamos que haya alguna permutación  $f \in Z(S_n)$  con  $f \neq id$ , sean  $x, y \in I_n$  con  $f(x) = y, x \neq y$ . Sea  $g = (xy)$ , como  $f \in Z(S_n)$  tenemos que  $fg = gf$ , así que  $f(y) = fg(x) = gf(x) = g(f(x)) = g(y) = x$ . Como  $n \geq 3$ , existe  $z \in I_n$  con  $z \neq x$  y  $z \neq y$ , y consideremos la permutación  $h = (xyz)$ , como  $f \in Z(S_n)$  tenemos que  $fh = hf$ , así que  $f(z) = fh(y) = hf(y) = h(x) = y = f(x)$  lo cual es absurdo pues contradice la inyectividad de  $f$ .

d. 2. Se deduce directamente de d1 y de c2, tomando  $G = S_n$ .

así

### Ejercicio 3. (35 puntos)

a. Ver apuntes teóricos de criptografía.

b. La clave secreta es  $K = 23^{69} = 23^{-1} \pmod{71}$  así que resolvemos  $23x + 71y = 1$  con el Algoritmo de Euclides obteniendo  $34 \cdot 23 - 11 \cdot 71 = 1$ . La clave secreta acordada es  $K = 34$ .

c. Tenemos que  $34 = 3 \cdot 11 + 1$  así que  $E(x) = 3x + 1 \pmod{11}$ .  
 $E(H) = E(4) = 3 \cdot 4 + 1 \pmod{11} = 2 \pmod{11} = L$   
 $E(O) = E(3) = 3 \cdot 3 + 1 \pmod{11} = 10 \pmod{11} = T$   
 $E(L) = E(2) = 3 \cdot 2 + 1 \pmod{11} = 7 \pmod{11} = R$   
 $E(A) = E(0) = 3 \cdot 0 + 1 \pmod{11} = 1 \pmod{11} = C$   
 El mensaje encriptado es LTRC.

d. i) Si  $E(x) = ax + b \pmod{11}$  tenemos que  $E(C) = E$  y  $E(U) = H$  por lo tanto:

$$\begin{cases} a + b \equiv 9 \pmod{11} \\ 5a + b \equiv 4 \pmod{11} \end{cases}$$

Resolviendo este sistema tenemos  $a \equiv 7 \pmod{11}$  y  $b \equiv 2 \pmod{11}$  así que  $E(x) = 7x + 2 \pmod{11}$ .

ii)

$$\begin{aligned} 7x + 2 &\equiv 8 \pmod{11} \Rightarrow x \equiv 4 \pmod{11} \Rightarrow E(4) = 8 = S \\ 7x + 2 &\equiv 2 \pmod{11} \Rightarrow x \equiv 0 \pmod{11} \Rightarrow E(0) = 2 = L \end{aligned}$$

Así que el mensaje original era CHAU.