

Solución  
Examen de Matemática Discreta II  
27 de febrero de 2008

1. (30 puntos)

a) (20 puntos)

Sea  $s$  el número de salas y  $c$  el número de cajas de 50 baldosas ( $19 \leq c \leq 39$ ). Entonces  $50c + 42 = 32s + 20$ . Luego  $25c \equiv -11 \pmod{16}$ , o sea  $9c \equiv -11 \pmod{16}$ . Como 9 es inverso de sí mismo en  $\mathbb{Z}_{16}$ , se obtiene que  $c \equiv 13 \pmod{16}$ . **O sea  $c = 29$  y el hospital precisa de 1492 baldosas.**

b) (10 puntos)

Sea  $n = 1492 = 2^2 \times 373$ . Entonces  $\varphi(n) = 2 \times 372$ . Sea  $m = 1119 = 3 \times 373$ . Luego  $\varphi(m) = \varphi(n)$ .

2. (35 puntos)

a) (4 puntos)

Los restos cuadráticos en  $\mathbb{Z}_7^*$  son:  $\{1, 2, 4\}$ .

b) (8 puntos)

$\phi$  es morfismo:

$\phi(x.y) = (x.y)^2 = x^2.y^2 = \phi(x).\phi(y)$  (el grupo es abeliano).

Núcleo:

$\phi(x) = 1 \Leftrightarrow [x]^2 \equiv 1 \pmod{p} \Leftrightarrow (x-1)(x+1) \equiv 0 \pmod{p}$ . Podemos tomar  $1 \leq x \leq p-1$ , con lo cual las soluciones son:  $x = 1$  o  $x = p-1$ . O sea:  $N(\phi) = \{\pm 1\}$ .

c) (12 puntos)

Como  $H = \text{Im}(\phi)$  del punto anterior, entonces  $H < G$  y luego  $H = \text{Im}(\phi) \cong \frac{G}{N(\phi)} = \frac{\mathbb{Z}_p^*}{\{\pm 1\}}$ .

d) (6 puntos)

Como el grupo es abeliano todo subgrupo es normal. Como  $\frac{\mathbb{Z}_p^*}{H}$  tiene dos elementos entonces es isomorfo a  $\mathbb{Z}_2$ . La tabla se deduce a partir de lo anterior.

e) (5 puntos)

Consecuencia directa del punto anterior.

3. (35 puntos)

a) (7 puntos)

Ver teórico del año.

b) i. (14 puntos)

Tenemos  $x_1 = y_1^{c_1} \cdot (y_2^{c_2})^{-1} \pmod{n} = x^{e_1 \cdot c_1 - e_2 \cdot c_2} \pmod{n}$ . Esto último es  $x \pmod{n}$ .

ii. (14 puntos)

Primero calculamos  $c_1$  y  $c_2$ . Tenemos que  $c_1 = 27^{-1} \pmod{29} = 14 \pmod{29}$ , y  $c_2 = \frac{14 \cdot 27 - 1}{29} = 13$ .  
Por la parte anterior,  $x_1 = y_1^{c_1} (y_2^{c_2})^{-1} \pmod{n} = 9983^{14} \cdot (4026^{13})^{-1} \pmod{16123}$ .

Calculemos primero  $4026^{13} \pmod{16123}$  utilizando el algoritmo de exponenciación rápida.  $4026^{13} = 4026^{2^3 + 2^2 + 1}$   
 $4026^2 = 5061 \pmod{16123}$

$4026^{2^2} = (4026^2)^2 \pmod{16123} = 5061^2 \pmod{16123} = 10397 \pmod{16123}$

$4026^{2^3} = (4026^{2^2})^2 \pmod{16123} = 10397^2 \pmod{16123} = 9017 \pmod{16123}$

Entonces,  $4026^{13} \pmod{16123} = 4026^{2^3 + 2^2 + 1} \pmod{16123} = 9017 \cdot 10397 \cdot 4026 \pmod{16123} = 9983 \pmod{16123}$ .

Observemos entonces que  $x_1 = 9983^{14} \cdot (9983)^{-1} \pmod{16123} = 9983^{13} \pmod{16123}$

Calculemos  $9983^{13} \pmod{16123} = 9983^{2^3 + 2^2 + 1}$ .

$9983^2 = 4026 \pmod{16123}$

$$9983^{2^2} = 4026^2 = 5061 \bmod(16123)$$

$$9983^{2^3} = 4026^{2^2} = 10397 \bmod(16123)$$

$$\text{Entonces, } 9983^{13} \bmod(16123) = 9983^{2^3+2^2+1} \bmod(16123) = 10397 \cdot 5061 \cdot 9983 \bmod(16123) = 714 \bmod(16123).$$

Por lo tanto,  $x = 714 \bmod(16123)$ .