

Corrección primer parcial Matemática Discreta 2

07 de mayo de 2005

Ejercicio 1. (Total: 9 puntos).

1. **(4 puntos).** Demostrar que existen infinitos valores enteros de x y encontrarlos todos, que resuelven el sistema siguiente:
$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{4} \\ x \equiv 3 \pmod{5} \end{cases}$$

SOLUCIÓN: por el Teorema Chino del resto $x \equiv 2M_1b_1 + 3M_2b_2 + 3M_3b_3 \pmod{60}$ siendo $M_1 = 20, M_2 = 15, M_3 = 12$ y:

$$20b_1 \equiv 1 \pmod{3}, \quad 15b_2 \equiv 1 \pmod{4}, \quad 12b_3 \equiv 1 \pmod{5}$$

$$\Rightarrow -b_1 \equiv 1 \pmod{3}, \quad -b_2 \equiv 1 \pmod{4}, \quad 2b_3 \equiv 1 \pmod{5}$$

$$\Rightarrow b_1 \equiv -1 \pmod{3}, \quad b_2 \equiv -1 \pmod{4}, \quad b_3 \equiv 3 \pmod{5}$$

Luego $x \equiv -40 + (-45) + 108 \equiv 23 \pmod{60}$, o sea el conjunto de soluciones del sistema es

$$\{23 + 60k, k \in \mathbb{Z}\}.$$

2. **(3 puntos).** Demostrar que las soluciones del sistema siguiente son las mismas que las del sistema de la parte 1):
$$\begin{cases} x \equiv 8 \pmod{15} \\ x \equiv 11 \pmod{12} \end{cases}$$

$$\text{SOLUCIÓN: } \begin{cases} x \equiv 8 \pmod{15} \\ x \equiv 11 \pmod{12} \end{cases} \Leftrightarrow \begin{cases} x \equiv 8 \pmod{5} \\ x \equiv 8 \pmod{3} \\ x \equiv 11 \pmod{4} \\ x \equiv 11 \pmod{3} \end{cases} \Leftrightarrow \begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{4} \\ x \equiv 2 \pmod{3} \end{cases} \Leftrightarrow \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{4} \\ x \equiv 3 \pmod{5} \end{cases}$$

3. **(2 puntos).** Demostrar que no existen valores enteros de x que resuelven el sistema siguiente:
$$\begin{cases} x \equiv 9 \pmod{15} \\ x \equiv 11 \pmod{12} \end{cases}$$

$$\text{SOLUCIÓN: } x \equiv 9 \pmod{15} \Leftrightarrow \begin{cases} x \equiv 9 \pmod{5} \\ x \equiv 9 \pmod{3} \end{cases} \Leftrightarrow \begin{cases} x \equiv -1 \pmod{5} \\ x \equiv 0 \pmod{3} \end{cases}$$

$$x \equiv 11 \pmod{12} \Leftrightarrow \begin{cases} x \equiv 11 \pmod{4} \\ x \equiv 11 \pmod{3} \end{cases} \Leftrightarrow \begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 2 \pmod{3} \end{cases}$$

$$\text{Por lo cual el sistema dado es equivalente a } \begin{cases} x \equiv -1 \pmod{5} \\ x \equiv 0 \pmod{3} \\ x \equiv 3 \pmod{4} \\ x \equiv 2 \pmod{3} \end{cases} \text{ y es incompatible ya que ningún entero puede}$$

ser congruente módulo 3 con 0 y 2.

Ejercicio 2. (Total: 7 puntos). Hallar todas las parejas de enteros positivos (a, b) tales que

$$\text{mcm}(a, b) = 155 \text{mcd}(a, b), \quad a + b = 432 \text{ y } a < b.$$

SOLUCIÓN: podemos escribir $a = a' \times \text{mcd}(a, b)$ y $b = b' \times \text{mcd}(a, b)$ con $\text{mcd}(a', b') = 1$. Por ser $a < b$ entonces $a' < b'$.

Como $ab = \text{mcm}(a, b)\text{mcd}(a, b) = 155\text{mcd}(a, b)^2$ entonces $ab = a'b'\text{mcd}(a, b)^2 = 155\text{mcd}(a, b)^2$ es decir que

$$a'b' = 155 = 31 \times 5. \text{ Esto implica que } \begin{cases} a' = 1, & b' = 155 \\ \text{o} \\ a' = 5 & b' = 31 \end{cases}$$

En el primer caso $a' = 1, b' = 155$, tendríamos $432 = a + b = a'mcd(a, b) + b'mcd(a, b) = (a' + b')mcd(a, b) = 156mcd(a, b)$ lo cual es absurdo pues 156 no divide a 432.

En el segundo caso $a' = 5, b' = 31$, tenemos $432 = a + b = a'mcd(a, b) + b'mcd(a, b) = (a' + b')mcd(a, b) = 36mcd(a, b)$, luego $mcd(a, b) = 12$, lo cual implica que $a = 5 \times 12 = 60$ y $b = 31 \times 12 = 372$.

Ejercicio 3. (Total: 10 puntos).

Sea p un número primo y consideramos $\mathbb{Z}_p = \{0, 1, \dots, p-1\}$ el conjunto de los enteros modulo p .

1. **(3 puntos).** Probar que si $a, b \in \mathbb{Z}_p$ y verifican $ab = 0$ entonces $a = 0$ o $b = 0$.

Sug: Usar que $ab = 0$ es equivalente en escribir $ab \equiv 0 \pmod{p}$, es decir $ab = kp$ para algún $k \in \mathbb{Z}$.

SOLUCIÓN: $ab = 0$ en $\mathbb{Z}_p \Leftrightarrow ab \equiv 0 \pmod{p} \Leftrightarrow p \mid ab$, con p primo, por lo cual p divide a a o p divide a b , es decir $a \equiv 0 \pmod{p}$ o $b \equiv 0 \pmod{p}$ lo cual es equivalente con $a = 0$ o $b = 0$ en \mathbb{Z}_p .

2. **(3 puntos).** Probar que si $x^2 \equiv 1 \pmod{p}$ entonces $x \equiv 1 \pmod{p}$ o $x \equiv -1 \pmod{p}$.

SOLUCIÓN: $x^2 \equiv 1 \pmod{p} \Leftrightarrow x^2 - 1 \equiv 0 \pmod{p} \Leftrightarrow (x-1)(x+1) \equiv 0 \pmod{p}$. Por la parte anterior esto implica que $x-1 \equiv 0 \pmod{p}$ o $x+1 \equiv 0 \pmod{p}$, lo cual significa que $x \equiv 1 \pmod{p}$ o $x \equiv -1 \pmod{p}$.

3. **(4 puntos).** Probar el teorema de Wilson: $(p-1)! \equiv -1 \pmod{p}$.

Sug.: Recordar que $(\mathbb{Z}^p \setminus \{0\}, \cdot)$ es grupo y usar la parte anterior.

SOLUCIÓN: $(p-1)! = (p-1) \times (p-2) \times \dots \times 2 \times 1$. $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ es un grupo por lo cual los elementos $p-1, p-2, \dots, 2, 1$ tienen inversos en $\{1, 2, \dots, p-1\}$. Por la parte anterior, solamente $p-1$ y 1 son inversos de si mismo ya que verifican la ecuación $x^2 \equiv 1 \pmod{p}$ (observar que $p-1 \equiv -1 \pmod{p}$). Luego reagrupando adecuadamente (cancelando cada elemento multiplicando por su inverso) en el desarrollo de $(p-1)!$ obtenemos que

$$(p-1)! = (p-1) \times (p-2) \times \dots \times 2 \times 1 \equiv p-1 \equiv -1 \pmod{p}.$$

Ejercicio 4. (Total: 14 puntos).

Sea G un grupo. Entenderemos por *automorfismo* del grupo G a un isomorfismo de G sobre si mismo (es un morfismo biyectivo sobre G).

Un subgrupo H de un grupo G se dice *invariante en G* si $\varphi(H) \subset H$ para todos los automorfismos φ de G .

1. **(3 puntos).** Si H es invariante en G probar que H es un subgrupo normal de G .

SOLUCIÓN: recordamos que, si $a \in G$ entonces $\varphi_a : G \rightarrow G / \varphi_a(g) = aga^{-1}$ es un automorfismo de G . Como H es invariante en G entonces $\varphi(H) \subset H \forall \varphi$ automorfismo de G , en particular $\varphi_a(H) \subset H, \forall a \in G$, es decir $aHa^{-1} \subset H, \forall a \in G$ lo cuál significa que H es normal en G .

2. **(3 puntos).** Sean H y K subgrupos invariantes en G . Probar que $HK = \{hk : h \in H, k \in K\}$ es un subgrupo de G y que además es invariante en G .

Sug.: Recordar que HK es un subgrupo si y solamente si $HK = KH$.

SOLUCIÓN: HK es un subgrupo si y solamente si $HK = KH$ es decir si y solamente $\forall h \in H, k \in K, \exists \tilde{h} \in H, \tilde{k} \in K$ tales que $hk = \tilde{k}\tilde{h}$. Como H y K son invariantes en G entonces, por la parte anterior, H y K son normales en G . Entonces si $h \in H$ tenemos $hkh^{-1} \in K$, o sea $hkh^{-1} = \tilde{k}$, es decir $hk = \tilde{k}h \in HK$, o sea $HK \subset KH$. Análogamente, usando que H es normal, se prueba que $KH \subset HK$, lo cual termina de probar que HK es un subgrupo de G .

Si φ es un automorfismo de G y hk es un elemento de HK entonces $\varphi(hk) = \varphi(h)\varphi(k) \in HK$ pues H y K son invariantes en G . Luego HK es invariante en G .

3. **(3 puntos).** Probar que el centro de un grupo G , $Z(G)$, es un subgrupo invariante en G .

SOLUCIÓN: sea φ un automorfismo de G . Queremos probar que $\varphi(Z(G)) \subset Z(G)$.

Sea $a \in Z(G)$. Veamos que $\varphi(a) \in Z(G)$. Tenemos que probar que $\varphi(a)g = g\varphi(a)$, $\forall g \in G$. Para cada $g \in G$, como φ es biyectiva, existe $\tilde{g} \in G$ tal que $\varphi(\tilde{g}) = g$. Entonces:

$$\varphi(a)g = \varphi(a)\varphi(\tilde{g}) = \varphi(a\tilde{g}) = \varphi(\tilde{g}a) = \varphi(\tilde{g})\varphi(a) = g\varphi(a).$$

Lo cual prueba que $Z(G)$ es invariante en G .

4. **(5 puntos)**. Supongamos que $|G| = pm$ donde $p > m$, p es primo y m es natural. Si H es un subgrupo de orden p , probar que H es invariante en G .

Sug.: Recordar el resultado del ejercicio 2 del práctico 5: si H y K son subgrupos de un grupo G entonces

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

SOLUCIÓN: Sea H un subgrupo de orden p y φ un automorfismo de G . Entonces $\varphi(H)$ es un subgrupo de G también de orden p . Esto último es porque φ es isomorfismo y al ser H de orden primo p , $\varphi(H)$ también es de orden p . Luego:

$$|H\varphi(H)| = \frac{|H||\varphi(H)|}{|H \cap \varphi(H)|} = \frac{p^2}{|H \cap \varphi(H)|}.$$

$H \cap \varphi(H)$ es un subgrupo de H luego su orden divide a p . Como p es primo entonces $|H \cap \varphi(H)| = 1$ ó p . Si $|H \cap \varphi(H)| = p$ entonces necesariamente $H \cap \varphi(H) = H$ luego $\varphi(H) = H$ y por lo tanto H es invariante en G .

Si $|H \cap \varphi(H)| = 1$ entonces $|H\varphi(H)| = p^2$. Como $|G| \geq |H\varphi(H)|$ (observar que es una desigualdad entre cantidad de elementos de subconjuntos) esto se traduce en $pm \geq p^2$ lo cual implicaría que $m \geq p$ lo cual no puede ser por la hipótesis.