FUNDAMENTOS MATEMÁTICOS II
Relación 3 2005/2006

1. Sea X el conjunto $\mathbb{R}^2 - \{(0,0)\}$. Se define en X la siguiente relación:

   $x \equiv y$ si y solo si existe una semirrecta que parte del origen y pasa por x e y

   Probar que es una relación de equivalencia, y que el conjunto cociente se identifica de modo natural con una circunferencia centrada en el origen (0,0).

2. Fijado un número natural n, se define en $\mathbb{Z}$ la relación:

   $$m \equiv m' \ (mod\ n) \ si\ y\ solo\ si\ m - m' \ es\ múltiplo\ de\ n$$

   Probar que es de equivalencia, y calcular las clases de equivalencia. El conjunto cociente se denota por $\mathbb{Z}/n$

3. Probar que la relación definida sobre $\mathbb{R}$ por

   $$x \equiv x' \ si\ y\ solo\ si\ x - x' \in \mathbb{Z}$$

   es de equivalencia, y que el conjunto cociente se identifica con la circunferencia.

4. Sea $\mathbb{N} = \{0, 1, 2, \ldots\}$ el conjunto de los números naturales. En el producto directo $\mathbb{N} \times \mathbb{N}$ definimos la relación

   $$(m, n) \equiv (m', n') \Leftrightarrow m + n' = m' + n \ (\equiv \ \ m - n = m' - n')$$

   . Probar que es una relación de equivalencia en $\mathbb{N} \times \mathbb{N}$.

   ¿Quién es el conjunto cociente $\Bigg(\mathbb{N} \times \mathbb{N}\Bigg)/ \equiv$?

5. Sea S el conjunto de los números enteros no nulos. en el producto directo $\mathbb{Z} \times S$ definimos la relación

   $$(a, b) \equiv (b, t) \Leftrightarrow at = bs$$

   Probar que es una relación de equivalencia. ¿Quién es el conjunto cociente $\Bigg(\mathbb{Z} \times S\Bigg)/ \equiv$?

6. Sea X un conjunto en $\wp(X)$ (partes de X. Este conjunto está formado por todos los subconjuntos de X inclido el $\emptyset$ y el total X). En $\wp(X)$ se define la relación.Dados $A, B \subset \wp(X)$ diremos que

   $$A \leq B \Leftrightarrow A \subseteq B$$

   ¿Es $(\wp(X), X)$es un conjunto parcialmente ordenado? ¿Es totalmente ordenado?

7. Sean $a, b, c, m, n \in \mathbb{Z}$. Probar las siguientes afirmaciones:

   a) Si $b|a$ y $c|b \;\Rightarrow\; c|a$

   b) Si $b|a \;\Rightarrow\; bc|ac$

   c) Si $c|a, b \;\Rightarrow\; c|am + bn$ (es decir si b divide a dos enteros, divide a sus combinaciones enteras)

   d) Si $b > 0$ es divisor propio de $a > 0 \;\Rightarrow\; 0 < b < a$

8. Probar que si p es primo y $p|ab$ entonces $p|a$ ó $p|b$ (o a los dos)

9. Probar que existen infinitos primos. (Indicación: Razonar por reducción al absurdo)

10. Calcula por el algoritmo de Euclides el $mcd(247, 9981)$

11. Escribe en pseudocódigo el algoritmo de Euclides.

12. Calcula la factorización de 135 mediante el teorema de descomposición.

13. Sean a, b, c enteros positivos. Supongamos que b divide a c. Demostrar que si a no divide a c entonces a no divide al cociente de c entre b.

14. Probar que todo número entero compuesto a tiene un factor primo, $p \neq 1$ menor o igual que $\sqrt{a}$

    (Indicación.- Razonar por reducción al absurdo)

15. Factorizar 8872.

    (Indicación: Usar el resultado del ejercicio anterior)

16. Calcular las soluciones enteras de

$$3x + 5y = 14$$

17. Encuentra un par de valores $\alpha, \beta \in \mathbb{Z}$ que verifiquen que $433\alpha + 321\beta = 15$

18. Un pueblo se abastece de agua de un canal y de pozos. Del canal se obtienen unidades de $100m^3$ y de los pozos unidades de 5 m^3. las necesidades diarias de agua son de $1500m^3$. ¿Cuántas unidades se pueden obtener del canal y de los pozos para abastecer de agua al pueblo?

19. **Cifrado de César** Vamos a ver un sistema de cifrado clásico. Estos sistemas dependen de las propiedades del alfabeto utilizado. El cifrado de César, se llama así por su relación con Julio César que lo usaba en la Roma antigua. Generalizando, se basa en desplazar el carácter i del alfabeto, j posiciones de modo que toma el valor $(i + j)$ del alfabeto. Por ejemplo,

si contamos con un alfabeto de 26 letras, las funciones de encriptado y desencriptado serían:

$$\begin{aligned} E : \mathbb{Z}/26 &\longrightarrow \mathbb{Z}/26 \\ i &\longrightarrow i+j \\ D : \mathbb{Z}/26 &\longrightarrow \mathbb{Z}/26 \\ i &\longrightarrow i-j \end{aligned}$$

(Observa que las operaciones se realizan módulo 26). Si el alfabeto es A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z, descifrar PXPXKXENVDRV, sabiendo que $X + j = E$ descifra.

20. Sean $a, b, c, d, n \in \mathbb{Z}$ números enteros con $n > 1$ tales que $a \equiv c \ mod \ n$ y $b \equiv d \ mod \ n$. Probar que se verifica:

    a) $a + b \equiv c + d \ mod \ n$;

    b) $ab \equiv cd \ mod \ n$.

21. ¿Cuál es el inverso de $\overline{2}$ en $\mathbb{Z}/5$?

22. Estudiar las operaciones en $\mathbb{Z}/7$ *notación* $\mathbb{Z}_7$ de la suma y el producto de clases.

    Resuelve en $\mathbb{Z}/7 : 2345 + 214 \times 432, \quad 2419 + 987$

23. Resolver la ecuación
$$3x + 3 \equiv 4 \ mod \ 5$$

24. Sean los números $5, 11$. Calcula el inverso de 5 módulo 11.

25. ¿Tiene solución la congruencia:
$$5x + 2 \equiv 5 \ mod \ 7?$$

26. Resolver el sistema:
$$x \equiv 2 \ mod \ 3$$
$$x \equiv 3 \ mod \ 5$$
$$x \equiv 2 \ mod \ 7$$

27. Calcular el resto de dividir 4525^{1000} entre 7.

28. Calcular el resto que resulta de dividir $2^{1982} + 3^{1982}$ entre 10.