DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN E INTELIGENCIA ARTIFICIAL

MATEMÁTICA DISCRETA

Bloque 1

INTRODUCCIÓN A LA TEORÍA DE GRAFOS

Problemas

Lección 1. Grafos: Fundamentos.

1 Plantea dos situaciones reales en las que se vea la utilidad de un grafo dirigido y no dirigido respectivamente. Dibuja tales grafos y estudia los conceptos de incidencia y adyacencia.

2 Da ejemplos, distintos de los vistos en clase, de grafo simple, multigrafo, grafo bipartido, grafo bipartido completo, tanto para el caso dirigido como no dirigido. Calcula para dichos ejemplos el grado de cada vértice y comprueba que se cumple el teorema que aparece en el apartado 3.

3 Da ejemplos de grafos con vértices x, y, z que cumplan las siguientes propiedades:

(1) Hay un ciclo que utiliza los vértices x e y.

(2) Hay un ciclo que utiliza los vértices y y z.

(3) Ningún ciclo utiliza los vértices x y z.

4 Un sistema de carreteras comunica siete pueblos a, b, c, d, e, f, g como sigue:

- a_1 comunica a y c pasando por b.
- a_2 comunica c y d y después pasa por b hasta llegar a f.
- a_3 comunica d y a pasando por e.
- a_4 comunica f y b pasando por g.
- a_5 comunica g y d.

(a) Utilizando vértices para representar los pueblos y arcos, para los tramos de carretera que los unen, dibuja un grafo dirigido que ilustre la situación.

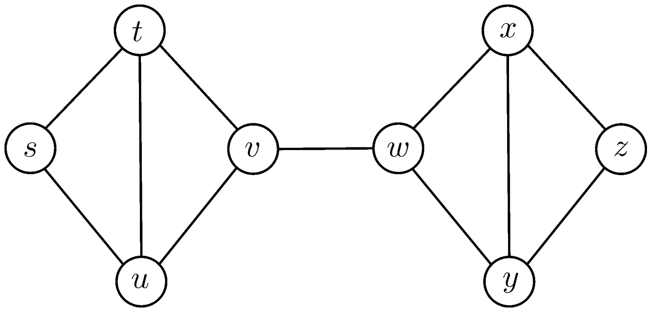
(b) Obtén el grado de entrada y salida de cada vértice.

(c) Lísta los caminos de g a a.

(d) ¿Cuál es el menor número de tramos de carretera que tendrían que cerrarse para interrumpir el paso de b a d?

(e) ¿Es posible salir de c y regresar a él visitando una sóla vez los demás?

5 Considérese el grafo de la figura



(1) ¿Cuáles de las siguientes sucesiones de vértices describen caminos:

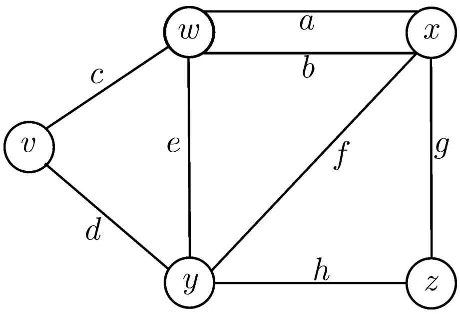
$stuvwxyz$; $tvwzyx$; $stus$; $tuss$; $vwvwvwv$; $wvustvw$.

(2) ¿Cuáles son cadenas cerradas y cuáles ciclos?

(3) Obtén en este grafo los caminos de menor longitud que conecten los siguientes pares de vértices, dando la longitud.

s, v; s, z; u, y; v, w.

6 Considérese el grafo de la figura



(1) Obtén un subgrafo generador. ¿Es único?

(2) Da ejemplos de cadena no simple y que no sea camino.

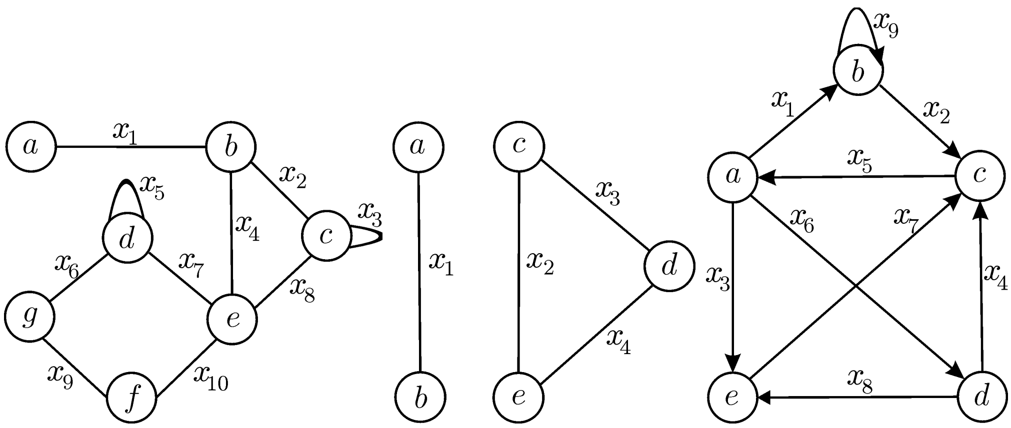
(3) Da ejemplos de cadena simple.

(4) Da ejemplos de cadena cerrada.

(5) Da ejemplos de ciclos.

(6) ¿El grafo es conexo? ¿Por qué?

7 Escribe la matriz de adyacencia, la matriz de incidencia y la tabla de incidencia correspondiente para los siguientes grafos:



8 Responde a las siguientes cuestiones:

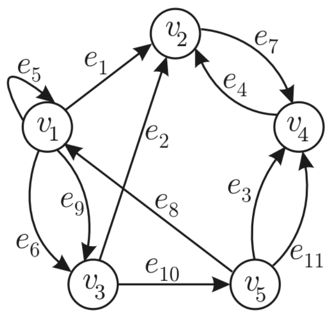
(i) Sea G un grafo con matriz de adyacencia A. Con qué se corresponde el elemento (i, j) de la matriz A^r, $r \geq 1$.

(ii) Sea G un grafo no dirigido. Con qué se corresponde la suma de los elementos de cada fila de la matriz de incidencia.

(iii) Sea G un grafo no dirigido. A qué es igual la suma de los elementos de cada columna de la matriz de incidencia.

(iv) Sea G un grafo dirigido sin bucles. A qué es igual la suma de los elementos de cada columna de la matriz de incidencia.

9 Consideremos el siguiente grafo dirigido G:



- Calcula la matriz de adyacencia del grafo G.
- Calcula la matriz de incidencia del grafo G.
- Dadas las siguientes cadenas en el grafo G, indica, para cada una de ellas su longitud, y si es cadena simple, camino, cadena cerrada o ciclo.

	Longitud	Cadena simple	Camino	Cadena cerrada	Ciclo
C_1: $v_1 e_6 v_3 e_{10} v_5 e_8 v_1 e_9 v_3$					
C_2: $v_3 e_{10} v_5 e_3 v_4 e_4 v_2$					
C_3: $v_5 e_8 v_1 e_9 v_3 e_{10} v_5$					

10 Consideremos un grafo no dirigido $G = (V, A)$ con conjunto de vértices $V = \{v_1, v_2, v_3, v_4, v_5\}$ y cuya matriz de adyacencia tiene como cuarta fila (3 1 1 2 0) y como segunda fila (1 0 2 1 0). Contesta razonadamente a las siguientes cuestiones:

- Indica, razonadamente, cuál es el grado del vértice v_2.
- Calcula, razonadamente, el conjunto $\Gamma(v_4)$.
- Indica, razonadamente, si el grafo es simple.
- Calcula, razonadamente, el número de cadenas de longitud 2 del vértice v_2 al vértice v_4.

11 Sea G un grafo dirigido cuya matriz de incidencia es de orden 4×7 y 3 de sus filas son $F1:\ (0,1,-1,0,0,0,1)$, $F3:\ (-1,0,1,1,0,0,0)$, y $F4:\ (0,0,0,-1,1,2,0)$. Si identificamos los vértices y arcos por su posición en dicha matriz, contesta razonadamente a las siguientes cuestiones:

• ¿El grafo G puede tener bucles? ¿Por qué? En caso afirmativo, razona cuántos bucles tiene.

• Indica cuál es la fila 2 (es decir $F2$) de la matriz de incidencia de G.

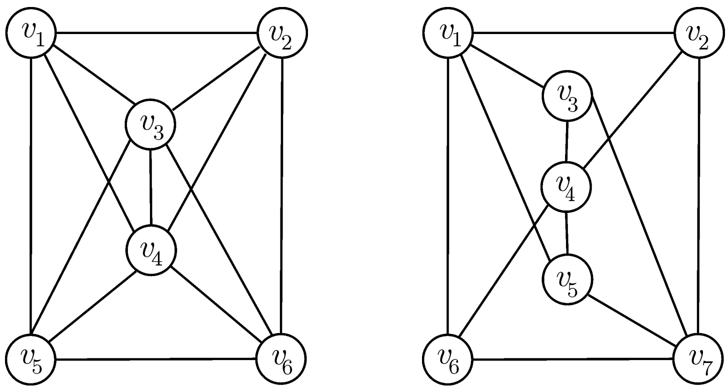
• Si consideramos el subgrafo de G resultante de quitar el arco 6, cuánto suma cada columna de la matriz de incidencia de dicho subgrafo.

Lección 2. Accesibilidad y Conectividad.

12 Calcula las matrices de accesibilidad y acceso del grafo del problema 4. Obtén las componentes conexas mediante los dos métodos conocidos.

13 Obtén las componentes conexas de los grafos del problema 7.

14 Consideremos los siguientes grafos



(a) Describe un camino euleriano para estos grafos o explica por qué no hay uno.

(b) Describe un tour euleriano para estos grafos o explica por qué no hay uno.

15 ¿Es posible para un insecto caminar por las aristas de un cubo, de manera que pase por cada arista exactamente una vez? Explíquese.

16 Construye un grafo con conjunto de vértices $\{0,1\}^3$ y con una arista entre los vértices v y w si v y w difieren en exactamente dos coordenadas.

(a) ¿Cuántas componentes conexas tiene el grafo?

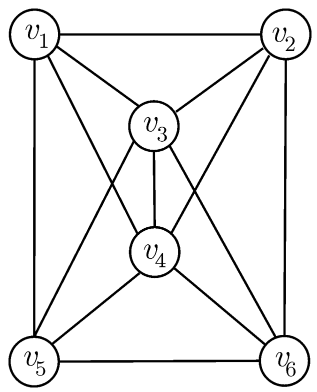
(b) ¿Cuántos vértices de cada grado tiene el grafo?

(c) ¿Tiene el grafo un tour euleriano?

17 Construye un grafo dirigido con más de 10 vértices en el que $d_e(v) = d_s(v)$ para todo vértice v. ¿Es euleriano? Utiliza la modificación del algoritmo de Fleury para localizar un tour euleriano.

18 Construye un grafo dirigido con más de 10 vértices en el que haya dos vértices q y p tales que $d_e(p) = d_s(p) - 1$, $d_e(q) = d_s(q) + 1$ y los restantes vértices verifiquen $d_e(v) = d_s(v)$. ¿Es posible encontrar un camino euleriano? Utiliza la modificación del algoritmo de Fleury para localizarlo.

19 Consideremos el grafo de la figura



(a) ¿Es un grafo hamiltoniano?

(b) ¿Es un grafo completo?

(c) ¿Es bipartido?

(d) ¿Es bipartido completo?

20 **(a)** Definición de tour y camino Euleriano. Enuncia para grafos no dirigidos la caracterización de existencia de un tour Euleriano y de un camino Euleriano.

(b) Dada la siguiente matriz de adyacencia de un grafo no dirigido estudia si existe un tour o camino Euleriano. En caso de que exista, encuéntralo utilizando el algoritmo de Fleury y explica dicho algoritmo.

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

21 Definición de ciclo Hamiltoniano. Explica qué es un código de Gray y da su interpretación y solución en términos de teoría de grafos.

22 Construye un código de Gray de longitud 4.

23 Sea G un grafo dirigido cuya matriz de adyacencia es

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

(a) Explica los dos métodos vistos en clase para el cálculo de las componentes conexas en un grafo dirigido.

(b) Obtén por los dos métodos anteriores las distintas componentes conexas de G.

24 Consideremos un grafo dirigido cuya matriz de adyacencia es

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Calcula la matriz de accesibilidad siguiendo el algoritmo de Warshall. Calcula las componentes conexas asociadas al grafo mediante los dos métodos conocidos, explicando los algoritmos que utilices para esta última pregunta.

25 Consideremos un grafo bipartido completo simple con bipartición $\{X, Y\}$, tal que $card(X) \leq card(Y)$. Si el grafo tiene 16 aristas, determínese razonadamente y enunciando los resultados teóricos que se utilicen:

(a) $card(X)$ y $card(Y)$ para que el grafo posea un tour euleriano pero no un ciclo hamiltoniano.

(b) $card(X)$ y $card(Y)$ para que el grafo posea un tour euleriano y un ciclo hamiltoniano.

26 Consideremos un grafo con 5 vértices. Sea la matriz R_3 resultante de la iteración 3 del algoritmo de Warshall:

$$R_3 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Calcula la matriz de accesibilidad siguiendo el algoritmo mencionado y las componentes conexas asociadas al grafo detallando el algoritmo que utilices para esta última pregunta.

27 Consideremos un grafo con 6 vértices. Sea R_4 la matriz resultante de la iteración 4 del algoritmo de Warshall:

$$R_4 = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Calcula la matriz de accesibilidad siguiendo el algoritmo mencionado. ¿Desde qué vértice es accesible el vértice 2? ¿Y el vértice 3? ¿Por qué? Calcula las componentes conexas asociadas al grafo detallando el algoritmo que utilices para esta última pregunta.

28 Consideremos un grafo con 6 vértices. Sea R_4 la matriz resultante de la iteración 4 del algoritmo de Warshall.

$$R_4 = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Calcula la matriz de accesibilidad siguiendo el algoritmo mencionado. A partir de dicha matriz explica qué vértices son accesibles desde el 3 y qué vértices alcanzan al 3. Calcula las componentes conexas asociadas al grafo detallando el algoritmo que utilices.

29 Dado el grafo cuya matriz de adyacencia es la siguiente:

$$A = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

(a) Calcula la matriz de accesibilidad $R = [r_{ij}]_{1 \leq i,j \leq 5}$, utilizando el algoritmo de Warshall.

(b) Calcula las componentes conexas.

(c) Calcula, utilizando las matrices A y R, el menor entero positivo ℓ, tal que para todo par de vértices $v_i, v_j,\ i \neq j$ que cumplen $r_{ij} \neq 0$, existe un camino de v_i a v_j de longitud menor o igual que ℓ.

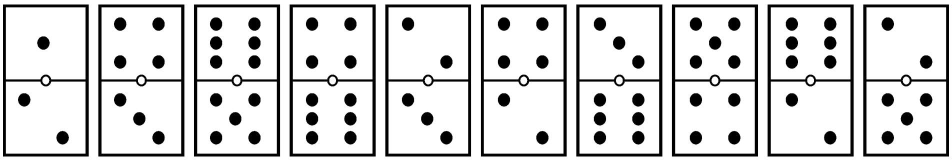
30 Consideremos un grafo con 6 vértices. Sea R_4 la matriz resultante de la iteración 4 del algoritmo de Warshall.

$$R_4 = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Calcula la matriz de accesibilidad siguiendo el algoritmo mencionado. A partir de dicha matriz explica razonadamente qué vértices son accesibles desde el 1 y qué vértices alcanzan al 1. Calcula las componentes conexas asociadas al grafo detallando el algoritmo que utilices.

31 Demuestra que en el juego del dominó hay partidas que emplean todas las fichas (Sugerencia: construye un grafo con las fichas del dominó de manera que los vértices sean los valores que aparecen en las fichas, $V = \{0, 1, 2, 3, 4, 5, 6\}$, y las aristas cada una de las fichas).

Estudia si en una partida de dominó las diez fichas siguientes pueden aparecer las primeras.



32 Consideremos un grafo representado por la matriz de adyacencia adjunta y con conjunto de vértices $\{v_1, v_2, v_3, v_4, v_5\}$.

(a) Aplica el algoritmo de Warshall a dicho grafo.

(b) ¿Cómo se llama la matriz que obtiene este algoritmo y qué representa? Indica concretamente el significado de la fila 5 de la matriz que obtiene el algoritmo de Warshall.

(c) Calcula las componentes conexas asociadas al grafo.

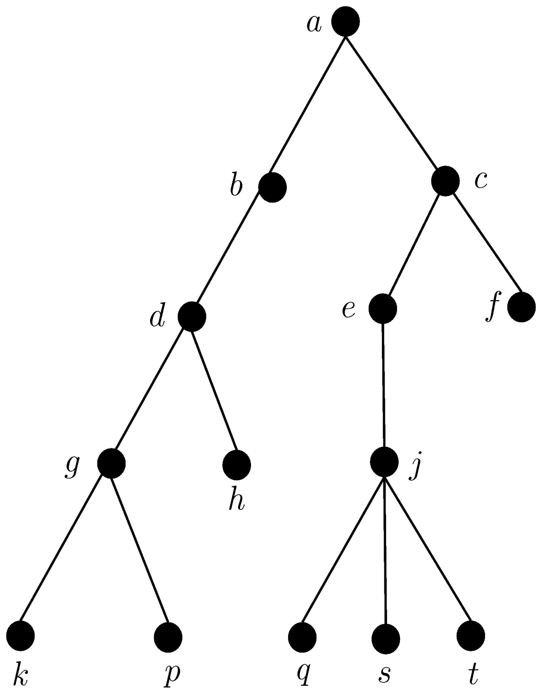
$$A = \begin{bmatrix} 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 3 & 0 \end{bmatrix}$$

Lección 3. Árboles

33 Esquematiza todos los árboles con raíz distintos, salvo isomorfismos, con seis vértices.

34 Da ejemplos de árboles que se usen para especificar relaciones de jerarquía (organización administrativa de cierto organismo, organización política, registro de libros, ...).

35 Responde a las siguientes preguntas sobre el árbol de la figura:



(a) ¿Qué vértice es la raíz?

(b) ¿Qué vértice es el padre de g?

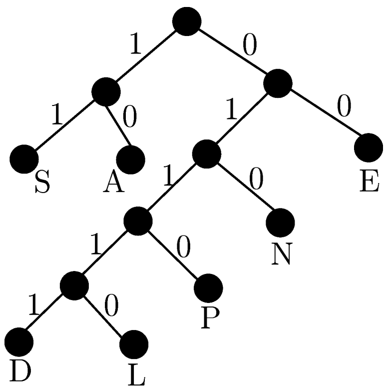
(c) ¿Qué vértices son los descendientes de c?

(d) ¿Qué vértices son los hermanos de s?

(e) ¿Qué vértices se encuentran en el nivel 4?

(f) ¿Cuál es la altura del árbol?

36 Descifra o decodifica cada uno de los siguientes arreglos utilizando el código de Huffman presentado a continuación.



(a) 011000010

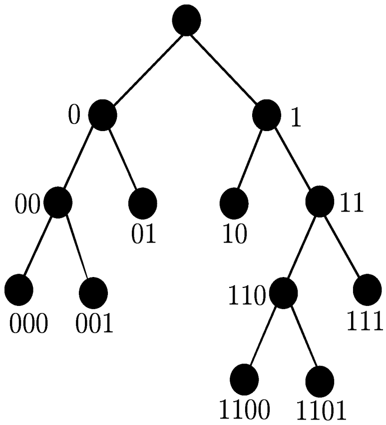
(b) 01110100110

(c) 01111001001110

Codifica ahora las palabras SALEN, PENA, LANA, PALAS.

37 Coloca las palabras de las siguientes frases en un árbol binario de búsqueda con altura mínima. ¿Cuántos pasos se requerirán en el peor de los casos para buscar una palabra?
Hace ochenta y siete años nuestros antepasados procrearon.
Nunca conocí a un hombre que no me simpatizara.

38 Utiliza los algoritmos PREORDEN, POSTORDEN e INORDEN para listar los vértices del árbol:



39 Calcula las siguientes expresiones dadas en notación polaca inversa.

(a) $3\;3\;4\;5\;1\; -\; \star\; +\; +$

(b) $3\;3\; +\; 4\; +\; 5\; \star\; 1\; -$

(c) $3\;3\;4\; +\; 5\; \star\; 1\; -\; +$

(d) $6\;3\;/\;3\; +\; 7\;3\; -\; \star$

(e) $3\;2\; \uparrow\; 4\;2\; \uparrow\; +\;5\;/\;2\;\star$

40 Calcula las siguientes expresiones dadas en notación polaca directa.

(a) $-\; \star\; 3\; \uparrow\; 5\;2\;2$

(b) $-\; \uparrow\; \star\;3\;5\;2\;2$

(c) $\star\; +\; /\;6\;3\;3\; -\; 7\;3$

(d) $\uparrow\; \star\;3\;5\; -\; 2\;2$

(e) $/\; \star\; 2\; +\; 2\;5\; \uparrow\; +\;3\;4\;2$

41 Escribe las siguientes expresiones en notación polaca inversa y directa.

(a) $(3x-4)^2$

(b) $(a+2b)/(a-2b)$

(c) $x-x^2+x^3-x^4$

42 Dada la expresión en notación polaca directa:

$$\backslash - a \uparrow b\; 2 + c * 3\; d$$

Calcula la expresión original y escríbela también en notación polaca inversa.

43 Calcula razonadamente y enunciando los teoremas utilizados el número de vértices de grado uno que tiene un árbol con dos vértices de grado cuatro y tres vértices de grado tres.

44 Demuestra que en un árbol el número de aristas es igual al número de vértices menos uno.

45 Determina razonadamente y paso a paso, la expresión algebraica correspondiente a la siguiente expresión en notación polaca inversa: $x\; y\; +\; 2\; \uparrow\; x\; y\; -\; 2\; \uparrow\; -\; x\; y\; \star\; /$. Da también, explicando los pasos seguidos, la correspondiente expresión en notación polaca directa.

46 Determina razonadamente y paso a paso, la expresión algebraica correspondiente a la siguiente expresión en notación polaca directa: $\uparrow\; +\; \star\; 2\; a\; 3\; -\; b\; 5$. Da también, explicando los pasos seguidos, la correspondiente expresión en notación polaca inversa.

47 **(a)** Calcula razonadamente y enunciando los teoremas utilizados, el número de vértices de grado uno que tiene un árbol con tres vértices de grado cuatro, dos vértices de grado tres y cinco vértices de grado dos.

(b) Demuestra que en un árbol el número de aristas es igual al número de vértices menos uno.

48 Determina razonadamente y paso a paso, la expresión algebraica correspondiente a la siguiente expresión en notación polaca inversa o postfija: $1\ 3\ x\ \uparrow\ -\ 2\ 5\ y\ \uparrow\ -\ /$. Construye el árbol binario que representa a esta operación y da también, explicando los pasos seguidos, la correspondiente expresión en notación polaca directa o prefija.

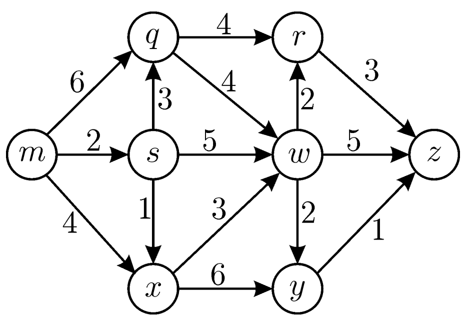
49 Calcula razonadamente y enunciando los teoremas utilizados el número de vértice de grado 3 que tiene un árbol con 3 vértices de grado 4, 3 vértices de grado 2 y 13 vértices de grado 1. se supone que el árbol no tiene otro tipo de vértices salvo los indicados. Enuncia los teoremas que utilices para calcularlo.

50 Calcula razonadamente y enunciando los teoremas utilizados el número de vértice de grado 4 que tiene un árbol con 4 vértices de grado 3, 3 vértices de grado 2 y 14 vértices de grado 1. Se supone que el árbol sólo tiene vértices de grado $1, 2, 3$ y 4.

51 **(a)** Calcula razonadamente y enunciando los teoremas utilizados, el número de vértice de grado 3 que tiene un árbol con 3 vértices de grado 4, 7 vértices de grado 2 y 12 vértices de grado 1. No tiene otro tipo de vértices salvo los indicados.
(b) Determina razonadamente y paso a paso, la expresión algebraica correspondiente a la siguiente expresión en notación polaca directa o prefija: $/\ -\ 1\ \uparrow\ 3\ x\ -\ 2\ \uparrow\ 5\ y$. Construye el árbol binario que representa a esta operación y da también, explicando los pasos seguidos, la correspondiente expresión en notación polaca inversa o postfija.

Lección 4. Grafos Ponderados

52 Consideremos el siguiente grafo

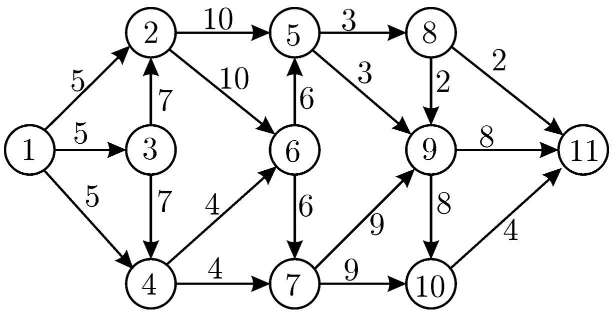


(a) Obtén la matriz de peso del grafo.

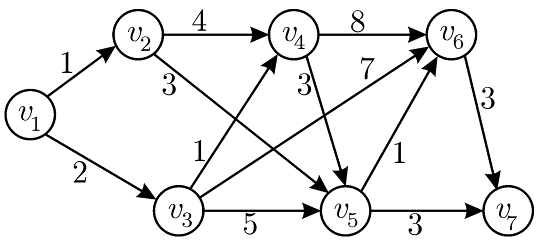
(b) Obtén el camino crítico de m a z utilizando las ecuaciones de Bellman.

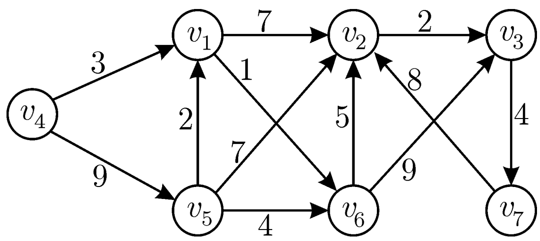
(c) En caso de que sea posible el retraso de algunas actividades no críticas sin retrasar la duración del proyecto total, averigua cuánto se pueden retrasar individualmente.

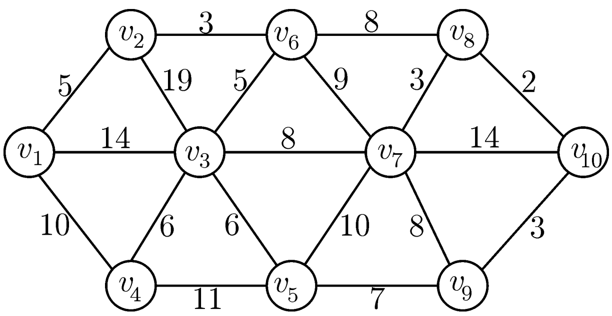
53 Considera el diagrama PERT de la figura. Encuentra los caminos críticos y calcula el máximo retraso admisible de la actividad 5, que no produzca, por sí sólo un retraso en el proyecto final.

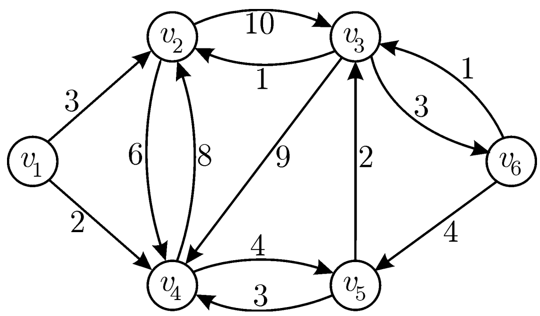


54 Utilizando el algoritmo de Dijkstra, calcula los caminos más cortos del vértice v_1 al resto de los vértices para los grafos:









55 Considerando la siguiente matriz de peso, obtén, aplicando el método de Foyd-Warshall, las longitudes de los caminos más cortos entre todos los pares de vértices y cuáles son dichos caminos.

$$W = \begin{bmatrix} \infty & 11 & 9 & \infty & 2 \\ \infty & \infty & \infty & \infty & \infty \\ \infty & 1 & \infty & \infty & \infty \\ \infty & \infty & 2 & \infty & \infty \\ \infty & \infty & 6 & 3 & \infty \end{bmatrix}$$

56 La siguiente tabla informa de la distancia en millas entre cada dos ciudades del estado de Indiana, Estados Unidos.

	Bloomington	Evansville	Fort Wayne	Gary	Indianapolis	South Bend
Evansville	119	-	-	-	-	-
Fort Wayne	174	290	-	-	-	-
Gary	198	277	132	-	-	-
Indianapolis	51	168	121	153	-	-
South Bend	198	303	79	58	140	-
Terre Haute	58	113	201	164	71	196

Se va a construir un sistema de carreteras que comunique estas siete ciudades. Determínese qué carreteras deberán construirse para que el coste de construcción sea mínimo. Supóngase que el coste de construcción de una milla de carretera es el mismo entre dos ciudades cualesquiera. Resuélvase el problema mediante los dos algoritmos conocidos.

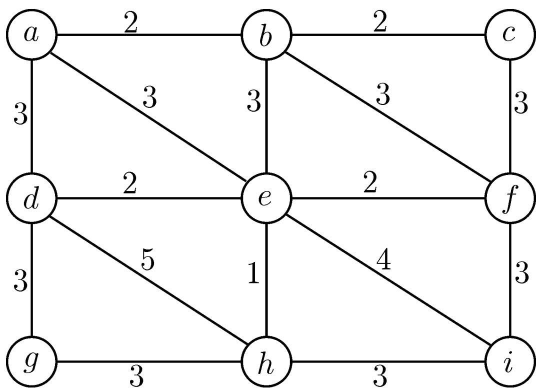
57 Modifica el algoritmo de Kruskal para determinar un árbol generador de máximo peso y aplícalo al grafo del ejercicio anterior.

58 **(a)** Responde al ejercicio 56 con la condición adicional de que el sistema incluya una carretera que una de forma directa Evansville e Indianapolis.

(b) Si debe haber una comunicación directa también entre Fort Wayne y Gary, halla el menor número de millas de carretera que debe construirse y cuáles.

59 Modifica el algoritmo de Kruskal para hallar un árbol generador de peso mínimo que incluya una o más aristas prescritas.

60 Aplica los algoritmos de Kruskal y Prim para determinar los árboles generadores de mínimo peso del grafo dado.



61 Consideremos un grafo ponderado con conjunto de vértices $V = \{A, B, C, D, E, F\}$, y cuya matriz de pesos es:

$$\begin{bmatrix} \infty & 2 & \infty & 5 & 8 & \infty \\ \infty & \infty & 1 & 2 & 6 & \infty \\ 1 & \infty & \infty & 3 & \infty & \infty \\ \infty & \infty & \infty & \infty & 3 & \infty \\ 1 & \infty & 7 & \infty & \infty & 4 \\ 3 & \infty & \infty & \infty & \infty & \infty \end{bmatrix}$$

Calcula el camino más corto de A a E y su peso, con la condición de que no contenga los vértices C y F como internos. El algoritmo que utilices debe aplicarse sobre la totalidad del grafo, es decir, no se permite eliminar vértices.

62 Consideremos un grafo no dirigido ponderado con 7 vértices. En una cierta etapa del algoritmo de Prim obtenemos:

$$\begin{array}{r|l} T = \{a_1, a_2, \{2,5\}\} & L(4) = \omega_{14} = 5 \\ U = \{1,2,3,5\} & L(6) = \omega_{56} = 3 \\ & L(7) = \omega_{57} = 2 \end{array}$$

Continua el algoritmo escribiendo explícitamente entre qué valores se calcula el mínimo para actualizar cada $L(u)$ y cómo va modificándose T y U. ¿Qué representa la solución de este algoritmo?

DATOS: a_1, a_2 aristas que forman parte de T y que no es necesario conocer. $\omega_{37} = 4, \omega_{67} = 5, \omega_{47} = 4$ y $\omega_{46} = 7$.

63 Consideremos un grafo dirigido ponderado con vértices $\{1,2,3,4,5,6\}$ y definido por la siguiente matriz de pesos:

$$\begin{bmatrix} \infty & \infty & \infty & \infty & \infty & 2 \\ \infty & \infty & \infty & \infty & \infty & 3 \\ 2 & \infty & \infty & \infty & \infty & 3 \\ \infty & 5 & 1 & \infty & 2 & \infty \\ \infty & 2 & \infty & \infty & \infty & 6 \\ \infty & \infty & \infty & \infty & \infty & \infty \end{bmatrix}$$

Aplica el algoritmo de Floyd-Warshall para calcular el peso del camino más corto entre los vértices 4 y 6, con la condición de que el camino no contenga los vértices 1 y 3. Explica la modificación que debe realizarse para que el algoritmo funcione. Esta modificación **no debe** consistir en eliminar vértices, es decir el algoritmo debe aplicarse con los 6 vértices. Identifica dicho camino con ayuda del propio algoritmo e indica cómo lo obtienes.

64 La tabla siguiente es una lista de las actividades $a_1, a_2, \ldots, a_8$ de un proyecto y para cada una de ellas, el tiempo en días necesario y las actividades que deben completarse antes de poder iniciarse.

Actividad	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
Tiempo necesario	4	3	7	4	6	5	2	5
Prerrequisitos	–	–	a_1	a_1	a_2	a_4, a_5	a_3, a_6	a_4, a_5

Calcula el mínimo número de días en que puede completarse el proyecto. Identifica el camino crítico, explicando su significado. Explica razonadamente cuántos días se puede retrasar la actividad a_8 sin afectar la duración total del proyecto.

65 La tabla siguiente es una lista de las actividades $A, B, C, D, E, F, G, H, I$ de un proyecto y para cada una de ellas, el tiempo en días necesario y las actividades que deben completarse antes de poder iniciarse.

Actividad	A	B	C	D	E	F	G	H	I
Tiempo necesario	3	6	8	7	5	11	3	3	2
Prerrequisitos	–	–	A, B	C, E	B	E	D	F, G	B

Calcula el mínimo número de días en que puede completarse el proyecto. Identifica el camino crítico, explicando su significado. Explica razonadamente cuántos días se puede retrasar la actividad E sin afectar la duración total del proyecto.

66 Consideremos un grafo ponderado con conjunto de vértices $V = \{1, 2, 3, 4, 5\}$, y matriz de pesos:

$$\begin{bmatrix} \infty & 4 & 1 & \infty & 9 \\ \infty & \infty & \infty & \infty & \infty \\ \infty & 2 & \infty & 3 & \infty \\ \infty & \infty & \infty & \infty & 4 \\ 5 & \infty & 5 & \infty & \infty \end{bmatrix}$$

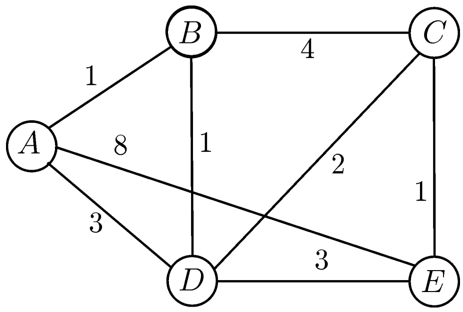
Calcula el peso del camino más corto entre cada par de vértices. Identifica el camino más corto del vértice 1 al 5. ¿Cuál es el camino más corto del vértice 4 al 2 con la condición de que no contenga como interno el vértice 3?

67 La tabla siguiente es una lista de las actividades $a_1, a_2, \ldots, a_{11}$ de un proyecto y para cada una de ellas, el tiempo en días necesario y las actividades que deben completarse antes de poder iniciarse.

Actividad	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}
Tiempo necesario	6	2	10	1	4	2	4	7	9	2	4
Prerrequisitos	–	–	a_1	a_1	a_1	a_5 a_{10}	a_2 a_4	a_3 a_6	a_2 a_4	a_7	a_8 a_{10}

Calcula el mínimo número de días en que puede completarse el proyecto. Identifica el camino crítico, explicando su significado. Explica razonadamente cuántos días se puede retrasar la actividad a_{10} sin afectar la duración total del proyecto.

68 Una red informática conecta 5 puntos A, B, C, D y E tal y como indica el siguiente grafo, en donde los pesos asignados a las aristas representan el tiempo en milisegundos que se tarda en transmitir una palabra de un punto a otro.



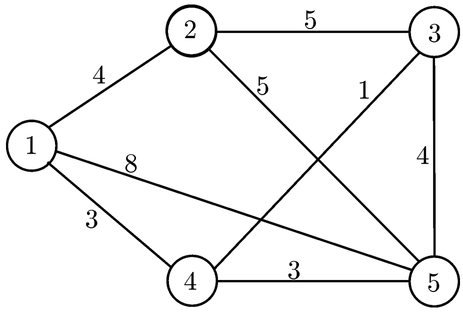
Si puede establecerse una comunicación entre todos los pares de puntos, se desea establecer qué ruta deben seguir los mensajes para que el tiempo de transmisión sea mínimo. Por otro lado, se sabe que los enlaces en los puntos B y D fallan en ocasiones, es decir, cuando este fallo se produce un mensaje no puede pasar por los puntos B y D; deseamos conocer una ruta alternativa para utilizarla en caso de que este fallo se produzca. Además de expresar la solución general en forma matricial, da la ruta inicial y la alternativa para la conexión de A a C.

69 Consideremos un grafo dirigido ponderado con 5 vértices, cuya matriz de pesos es:

$$W = \begin{bmatrix} \infty & 2 & 6 & \infty & 4 \\ 3 & \infty & 3 & \infty & \infty \\ \infty & \infty & \infty & \infty & \infty \\ 4 & \infty & 3 & \infty & \infty \\ \infty & 2 & \infty & 1 & \infty \end{bmatrix}$$

Calcula los caminos más cortos y sus pesos entre cada par de vértices. Identifica explícitamente, el camino más corto y su peso entre el vértice 5 y el vértice 3. Calcula el camino más corto y su peso del vértice 5 al 3 con la condición de que no contenga como interno el vértice 4.

70 Se desea establecer una red informática que conecte 5 puntos a_1, a_2, a_3, a_4 y a_5. Las posibilidades de conexión vienen dadas en el siguiente grafo, en donde los pesos asignados a las aristas representan el coste de construcción de la línea directa correspondiente.



Usa el algoritmo de Prim para determinar qué líneas deben construirse para que el coste total sea mínimo. Por otro lado se prevé que el trafico entre los puntos a_3 y a_5 sea muy intenso, por lo que se desea saber qué líneas deben construise de manera que exista una comunicación directa entre a_3 y a_5 y con coste mínimo. Modifica el algoritmo anterior (explicando dicha modificación) y aplícalo para resolver esta cuestión.

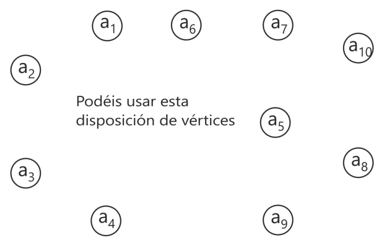
71 Consideremos un grafo dirigido ponderado dado por su matriz de pesos Ω y con conjunto de vértices $V = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}$.

En dicho grafo los vértices representan nodos de una red de telecomunicaciones, los arcos representan las distintas conexiones, y el peso de cada arco representa el tiempo de comunicación de la correspondiente conexión. Se desea conocer cuál es la ruta que debe seguir un mensaje desde el nodo v_2 al resto de manera que el tiempo de comunicación sea mínimo. Indica también cuál es el tiempo mínimo de comunicación desde el nodo v_2 al resto.

$$\Omega = \begin{bmatrix} \infty & 2 & \infty & 3 & \infty & \infty & \infty \\ \infty & \infty & 7 & 2 & \infty & 4 & \infty \\ \infty & \infty & \infty & \infty & \infty & \infty & 8 \\ \infty & \infty & \infty & \infty & 9 & 1 & \infty \\ \infty & \infty & \infty & \infty & \infty & \infty & 4 \\ \infty & \infty & 3 & \infty & 5 & \infty & 10 \\ \infty & \infty & \infty & \infty & \infty & \infty & \infty \end{bmatrix}$$

72 La tabla siguiente es una lista de las actividades $a_1, a_2, \ldots, a_{10}$ de un proyecto. Para cada una de ellas, se indica el tiempo en días necesario y las actividades que deben completarse antes de poder iniciarse. Calcula el mínimo número de días en que puede completarse el proyecto. Identifica el camino crítico, explicando su significado. Explica cuántos días se puede retrasar la actividad a_4 sin afectar la duración total del proyecto.

Activ.	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}
Tiempo	6	3	2	5	4	3	1	4	3	8
Prer.	a_2 a_3	–	–	a_3	a_4 a_6 a_7	a_1 a_4	a_6	a_9	a_4 a_5	a_5 a_7

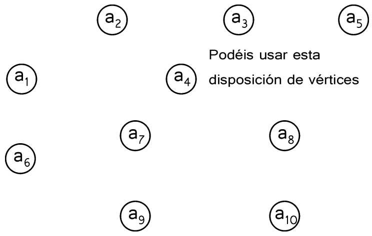


73 Se dispone de seis de ordenadores A, B, C, D, E y F que queremos conectar en red. El coste de conexión de cada par de ordenadores viene reflejado en la siguiente tabla. Si no se especifica un valor en la tabla, esto indica que la conexión correspondiente no es factible. Calcula qué conexiones deben incorporarse de manera que todo el sistema esté conectado y el coste sea mínimo. Hazlo utilizando los dos algoritmos que conozcas para resolver este problema.

	A	B	C	D	E	F
A	–	2	–	4	9	–
B	2	–	3	–	8	6
C	–	3	–	–	5	7
D	4	–	–	–	–	7
E	9	8	5	–	–	–
F	–	6	7	7	–	–

74 La tabla siguiente es una lista de las actividades $a_1, a_2, \ldots, a_{10}$ de un proyecto. Para cada una de ellas, se indica el tiempo en días necesario y las actividades que deben completarse antes de poder iniciarse. Calcula el mínimo número de días en que puede completarse el proyecto. Identifica el camino crítico, explicando su significado. Explica cuántos días se puede retrasar la actividad a_9 sin afectar la duración total del proyecto.

Activ.	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}
Tiempo	4	2	5	1	6	3	6	1	5	8
Prer.	–	a_1	a_2 a_4	a_2	a_3 a_8	–	a_1 a_6	a_7 a_9	a_6	a_9



75 Una red informática conecta 5 puntos A, B, C, D y E a través de una serie de conexiones que pueden ser representadas en un grafo ponderado no dirigido, en donde los pesos asignados a las aristas representan el tiempo en milisegundos que se tarda en transmitir una palabra de un punto a otro. Necesitamos conocer las rutas que deberían seguir los mensajes entre cada par de puntos de manera que el tiempo de transmisión sea mínimo. Además de expresar la solución general en forma matricial para cualquier par de puntos, calcula en particular y razonadamente, la ruta para la conexión de A a C y el tiempo necesario para dicha conexión.

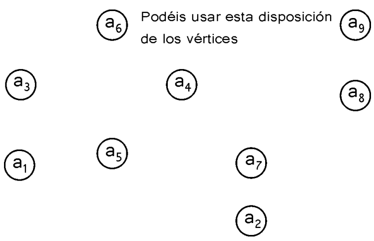
Por otro lado, se sabe que los enlaces en el punto B fallan en ocasiones, es decir, cuando este fallo se produce un mensaje no puede pasar por el punto B; calcula en forma matricial las rutas alternativas para utilizarlas en caso de que este fallo se produzca. Indica expresamente cuál sería la conexión de A a C y su tiempo de transmisión, de manera que éste sea mínimo.

$\Omega \equiv$

	A	B	C	D	E
A	∞	1	∞	3	8
B	1	∞	∞	2	1
C	∞	∞	∞	4	2
D	3	2	4	∞	∞
E	8	1	2	∞	∞

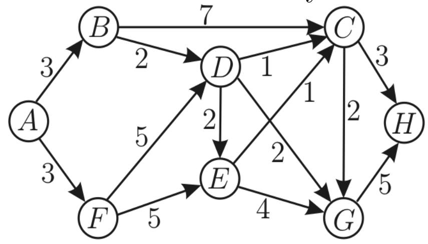
76 La tabla siguiente es una lista de las actividades $a_1, a_2, \ldots, a_9$ de un proyecto. Para cada una de ellas, se indica el tiempo en días necesario y las actividades que deben completarse antes de poder iniciarse. Calcula el mínimo número de días en que puede completarse el proyecto. Identifica el camino crítico, explicando su significado. Explica cuántos días se puede retrasar la actividad a_6 sin afectar la duración total del proyecto.

Activ.	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9
Tiempo	6	1	4	2	4	5	6	7	3
Prer.	–	a_1	–	a_1 a_5 a_6	a_1	a_3	a_4 a_5	a_4	a_7 a_6



77 El siguiente grafo representa un proyecto de secuenciación de actividades en donde el peso asociado a los arcos representa el tiempo en días necesario entre una actividad y otra.

Calcula el mínimo número de días en que puede completarse el proyecto. Identifica el camino crítico, explicando su significado. Explica razonadamente cuántos días se puede retrasar la actividad B sin afectar a la duración total del proyecto.



78 Una red informática conecta 5 puntos A, B, C, D y E a través de una serie de conexiones que pueden ser representadas en un grafo ponderado no dirigido, en donde los pesos asignados a las aristas representan el tiempo en milisegundos que se tarda en transmitir una palabra de un punto a otro. Necesitamos conocer las rutas que deberían seguir los mensajes entre cada par de puntos de manera que el tiempo de transmisión sea mínimo. Además de expresar la solución general en forma matricial para cualquier par de puntos, calcula, razonadamente, la ruta para la conexión de A a C y el tiempo necesario para dicha conexión. Por otro lado, se sabe que los enlaces en el punto D fallan en ocasiones, es decir, cuando este fallo se produce un mensaje no puede pasar por el punto D; calcula, razonadamente, la ruta alternativa para la conexión de A a C y su tiempo de transmisión, de manera que éste sea mínimo, para utilizarla en caso de que este fallo se produzca.

Como dato para realizar este ejercicio se da la matriz de pesos y la matriz de caminos de la penúltima iteración del algoritmo de Floyd-Warshall. No se permite modificar el grafo.

$$\Omega^{(5)} \equiv \begin{array}{c||ccccc||} & E & A & C & B & D \\ \hline E & 2 & 6 & 1 & 5 & 3 \\ A & 6 & 2 & 5 & 1 & 2 \\ C & 1 & 5 & 2 & 4 & 2 \\ B & 5 & 1 & 4 & 2 & 1 \\ D & 3 & 2 & 2 & 1 & 2 \\ \hline \end{array}, \quad \Theta^{(5)} \equiv \begin{array}{c||ccccc||} & E & A & C & B & D \\ \hline E & C & B & E & C & E \\ A & C & B & B & A & B \\ C & C & B & E & C & C \\ B & C & B & B & A & B \\ D & D & B & D & D & B \\ \hline \end{array}.$$

MATEMÁTICA DISCRETA

Bloque 2

ENTEROS

Problemas

Lección 1. Los números enteros

79 En los siguientes casos escribe $a = bq + r$, donde $0 \leq r < |b|$.
$a = 20, b = 3$; $a = 3, b = 22$; $a = 8, b = -3$.

80 Encuentra cuáles de los siguientes números son primos:

$$22, 47, 527, 1180, 29, 81, 247, 1201.$$

81 Escribe cada entero de los siguientes como un producto de primos y sus potencias:

$$60, 858, 1125, 350, 1666, 210.$$

82 Encuentra en los siguientes casos el $mcd(a, b)$, y obtén la mínima combinación lineal de a y b que produce un entero positivo.

$$32, 27; 40, 88; 34, 58; 45, 33; 60, 100; 77, 128.$$

83 Obtén el mcm de los siguientes pares de números.

$$72, 108; 150, 70; 175, 245; 32, 27.$$

84 Sean a, b dos enteros. Si p es primo tal que $p|ab$ demostrar que $p|a$ o $p|b$. (Sugerencia: supón que p no divide a a, entonces $1 = mcd(a, p)$ y podremos escribir $1 = sa + tp$.

85 Escribe los siguientes enteros en base 2, 4 y 8:

$$137, 6243, 12345.$$

86 Escribe un programa de ordenador para convertir un número dado en base 10 a base b para b entre 2 y 9, ambos incluidos.

87 Definición de ecuación diofántica. Da condiciones que garanticen la existencia de solución en esta ecuación. Resuelve las ecuaciónes diofánticas,

$$30x - 21y = 9$$

$$10x + 47y = 3$$

$$45x + 9y = 4$$

88 Determínese aquellos valores de $c \in \mathbf{Z}^+$, $10 < c < 20$ para los que no tiene solución entera la ecuación diofántica $84x + 990y = c$.

Determínese las soluciones para los valores restantes de c.

89 Definimos en $\mathbf{Z}^+$ la siguiente relación:

$$aRb \text{ sii } mcd(a, b) = 1.$$

Estudia que propiedades verifica.

90 Un ejecutivo gastó 2490 euros en juguetes para los hijos de sus empleados. Los juguetes regalados a las niñas costaron 33 euros unidad y los de los niños 29. Obtén cuántos juguetes compró de cada tipo.

91 Resuelve la ecuación diofántica $50x - 3y = 50$, siguiendo el algoritmo visto en clase.

92 Determina la cantidad de ordenadores que se pueden comprar de cada uno de los precios 2900 euros y 1700 euros si se dispone de un presupuesto de 78000 euros.

93 Se dispone de 2 tipos de piezas circulares. El diámetro de una pieza del tipo A es de 37 milímetros, y el de una pieza tipo B es de 23 milímetros. ¿De cuántas maneras puede obtenerse la longitud de 1 metro, alineando piezas del tipo A y B?

94 Disponemos de dos tipos A y B de piezas de 9 cm. y 15 cm. de largo, respectivamente. ¿Con cuántas piezas del tipo A y B podemos obtener la longitud de 6 metros alineando dichas piezas? ¿Y si se quieren colocar al menos 33 piezas del tipo A y 17 piezas del tipo B?

95 En el departamento de informática de una empresa se desea hacer un pedido de infraestructura para comprar ordenadores personales. Disponen de 29500 euros que se desea gastar en su totalidad. El precio de un ordenador Tipo A es de 1500 euros y el de un ordenador tipo B es de 2500 euros. ¿Cuántos ordenadores de cada tipo se pueden comprar si como mínimo se desea comprar 8 del tipo A?

96 Calcula las soluciones enteras de la ecuación $x + 1001y = 9998$.

97 **(a)** Dados $n, i \in Z,\ n \geq 1,\ i \geq 0$, calcula las soluciones enteras no negativas de la ecuación $x + (n+1)y = i$.

(b) Calcula el coeficiente que acompaña a s^{9998} en $(1 + s + s^2 + \ldots + s^{1000})^{1000}$.

98 En el departamento de informática de una empresa se desea hacer un pedido de infraestructura para comprar dispositivos portátiles. Disponen de 60000€ que se desea gastar en su totalidad. El precio de un netbook es de 620€ y el de un tablet es de 460€. ¿Cuántos dispositivos de cada tipo se pueden comprar si como mínimo se desea comprar 50 de cada tipo?

99 Calcula las distintas formas de gastar exactamente un presupuesto de 50.600€ comprando tablets de 10" y de 7" de precios respectivos 638€ y 418€. ¿Cuál sería la cantidad de cada tipo de tablets si se pusiera la condición de comprar al menos 35 de cada tipo?

100 Una empresa de ordenadores personales ha fabricado entre 500 y 600 ordenadores. Determina el número exacto de ellos sabiendo que al empaquetarlos en cajas con una capacidad para 13 unidades sobraron 7 unidades, pero cuando usamos cajas con una capacidad de 11 unidades, nos sobraron 10.

Lección 2. Congruencias en los enteros. Aritmética modular

101 En Z_{27}, expresa $[1598]$, $[-2300]$, $[42]$, $[-13]$ como clases de equivalencia, en las que el representante de clase esté comprendido entre 0 y 26.

102 Determina si es cierto o falso:
$9 \equiv 3(mod\ 7)$, $5 \equiv 5(mod\ 19)$,
$6 \equiv -15(mod\ 7)$, $-2 \equiv 162(mod\ 24)$

103 Demuestra las propiedades de la suma y el producto en Z_n dadas en clase.

104 Opera y expresa como $[a]$ en Z_n, $0 \leq a < n$:
$[256] + [34]$, $n = 11$;
$[14] - [38]$, $n = 5$;
$[32][17]$, $n = 34$;
$[15][31]$, $n = 15$.

105 Lístense cuatro elementos de las siguientes clases de equivalencia:
$[1]$ en Z_7, $[2]$ en Z_{11}, $[10]$ en Z_{17}.

106 Calcula $\varphi(n)$ para $n = 2, \ldots, 25$.

107 Verifica las siguientes operaciones:
$1234 \times 4735 = 5843980$
$147 \times 23 = 3381$
$12 \times 1993 = 23916$
$895 \times 496 = 443910$
$\frac{123456}{24} = 5134$

108 Determina los enteros que verifiquen:

(1) $x \equiv 7(mod\ 11)$, $x \equiv 4(mod\ 19)$

(2) $x \equiv 2(mod\ 17)$, $x \equiv 9(mod\ 31)$

(3) $x \equiv 2(mod\ 14)$, $x \equiv 4(mod\ 28)$

109 Resuelve las congruencias siguientes:

(1) $3x \equiv 7(mod\ 16)$

(2) $4x \equiv 9(mod\ 13)$

(3) $5x + 7 \equiv 6(mod\ 23)$

(4) $2x + 8 \equiv 5(mod\ 33)$

(5) $4x + 3 \equiv 7x + 12(mod\ 11)$

(6) $3x + 9 \equiv 8x + 61(mod\ 64)$

110 Halla $[a]^{-1}$ en Z_{1009} para $a = 17,\ 100,\ 777$

111 Calcula el número de elementos inversibles que hay en Z_{17}, Z_{117}, Z_{1117}.

112 Si $p = 29,\ q = 31,\ t = 17$, codifica los siguientes mensajes según el código RSA:
El gato y el perro son animales domésticos.
Dime qué hora es.
Estoy estudiando Informática.
El correo se recibirá a las tres.
Razona si es posible tomar $t = 2$.
Una vez codificados los mensajes, comprueba con la decodificación que se codificaron bien.

113 Usando el código clásico, dado en clase, y tomando $r = 5$, $s = 4$ codifica los mensajes anteriores. Razona si es posible tomar $r = 9$. Comprueba mediante la decodificación, si la codificación fue correcta.

114 Resuelve en Z_7 el siguiente sistema. Expresa la solución con representantes de clase entre 0 y 6.

$$\left.\begin{array}{rcrcl} x & + & [5]y & = & [2] \\ [2]x & - & y & = & [3] \end{array}\right\}$$

115 **(a)** Resuelve el siguiente sistema de ecuaciones lineales en Z_7.

$$\left.\begin{array}{rcrcl} x & + & [2]y & = & [4] \\ [4]x & + & [3]y & = & [4] \end{array}\right\}$$

Expresa el resultado mediante representantes de clase entre 0 y 6. ¿Existe alguna solución en Z_5?

(b) Usar el Teorema de Fermat para calcular el resto de dividir 3^{47} entre 23.

116 Consideremos un código RSA con $p = 11,\ q = 3$ y $t = 7$. Calcula la función de decodificación. Decodificar el mensaje recibido dado por $[10],\ [5]$.

117 Estudia las soluciones positivas de la congruencia $3x \equiv 7(\text{mod } 16)$

118 Calcula el inverso de $[33]$ en Z_{50}. Expresar el resultado con el representante de clase entre 0 y 49.

119 Sean $a, b, m \in Z$. Demuestra la siguiente equivalencia

$$\exists x_0 \in Z \ / \ a \cdot x_0 \equiv b \ (\text{mod } m) \Longleftrightarrow \exists k_0 \in Z \ / \ b = k_0 \cdot \text{mcd}(a, m)$$

120 En el criptosistema de clave privada con $r = 4$ y $s = 5$, codifica el mensaje `MANO` y decodifica el mensaje `ALV`.

121 Resuelve en Z_5 el siguiente sistema. Expresa la solución con representantes de clase entre 0 y 4.

$$\left.\begin{array}{rcrcl} [2]x & + & [3]y & = & [1] \\ [3]x & - & [4]y & = & [2] \end{array}\right\}$$

122 Estudia las soluciones positivas de la congruencia $3x \equiv 7(\text{mod } 16)$

123 Resuelve la siguiente ecuación cuadrática en Z_{11}.

$$x^2 + [3]x + [4] = 0, \quad x \in Z_{11}.$$

Expresa el resultado mediante representantes de clase entre 0 y 10.

124 Usar el Teorema de Fermat para calcular el resto de dividir $3^{25} \cdot 7^{68}$ entre 23.

125 Determina los enteros que verifiquen: $\{x \equiv 7 \pmod{11},\ x \equiv 4 \pmod{17}\}$.

126 Un reloj digital se pone en hora a las 12 en punto del mediodia de un día determinado. ¿Qué hora sería después de transcurridas 5^{100} horas exactas, si no se para nunca y es totalmente preciso?

127 Un reloj digital se pone en hora a las 13 horas en punto de un día determinado. ¿Qué hora sería después de transcurridas $3^{25} \cdot 7^{73}$ horas exactas, si no se para nunca y es totalmente preciso?

128 Calcula razonadamente cuál es el conjunto de enteros que son divisibles por 5 pero queda resto 1 al dividirlos por 3? Expresa el resultado como una clase de equivalencia.

129 **(a)** Usa el Teorema de Euler para responder a la siguiente cuestión. Se sabe que un determinado planeta tarda en completar su órbita alrededor de una cierta estrella 35 años. Si actualmente se encuentra en la posición A y transcurren 27^{99} años, ¿cuántos años más deben transcurrir para que vuelva a encontrarse en la misma posición A?

(b) Resuelve en Z_8 el siguiente sistema. Expresa la solución con representantes de clase entre 0 y 7.

$$\left.\begin{array}{rcrcl} x & + & [2]y & = & [2] \\ [5]x & + & [4]y & = & [4] \end{array}\right\}$$

130 **(a)** Resuelve en Z_{17} el siguiente sistema. Expresa la solución con representantes de clase entre 0 y 16.

$$\left.\begin{array}{rcrcl} [2]x & - & [3]y & = & [5] \\ [3]x & + & y & = & [7] \end{array}\right\}$$

(b) Un mensaje oculto está almacenado en los números 39^{162} y 39^{201}. El mensaje oculto está formado por las dos últimas cifras de la representación decimal de cada uno de los anteriores números, en el orden correspondiente (es decir, cuatro cifras en total, primero las dos últimas cifras de 39^{162} y después las dos últimas cifras de 39^{201}). Teniendo en cuenta la asignación siguiente:

número	0	1	2	3	4	5	6	7	8	9
letra	m	i	b	e	c	f	s	p	a	n

Utiliza el Teorema de Euler para identificar el mensaje oculto.

131 Utilizando el Teorema de Fermat, indica cuál es la última cifra de la representación en base 10 de 7^{93}.

132 **(a)** Se ha cifrado un mensaje mediante el criptosistema de clave privada visto en clase (cifrado afín) e identificando las letras mayúsculas del alfabeto con los enteros módulo 28 (incluyendo el espacio en blanco). El mensaje cifrado ha resultado ser MQTF. Si la función de codificación es $C_{3,5}([m]) = [3][m] + [5]$, obtén la función de decodificación y calcula el mensaje original. La asignación de letras con los enteros congruentes módulo 28 es:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

(b) Un mensaje oculto está almacenado en los números 67^{842} y 67^{1323}. El mensaje oculto está formado por las dos últimas cifras de la representación decimal de cada uno de los anteriores números, en el orden correspondiente (es decir, cuatro cifras en total, primero las dos últimas cifras de 67^{842} y después las dos últimas cifras de 67^{1323}). Teniendo en cuenta la asignación siguiente:

número	0	1	2	3	4	5	6	7	8	9
letra	m	a	s	n	c	f	e	p	b	i

Utiliza el Teorema de Euler para identificar el mensaje oculto.

133 Una empresa ha fabricado recientemente entre 1000 y 1500 unidades SSD. Determina el número exacto de ellas sabiendo que se cumplen las dos condiciones siguientes:
(a) El número buscado debe ser congruente con 7 módulo 17.
(b) Si dividimos este número entre 23 nos da como resto 11.

134 Encuentra todos los enteros comprendidos entre 4000 y 5000 que verifiquen simultáneamente las siguientes dos condiciones:
- El número buscado debe ser congruente con 7 módulo 13.
- Si dividimos este número por 17 nos da como resto 3.

135 **(a)** Utilizando el Teorema de Euler, calcula las dos últimas cifras de la representación decimal de 21^{1642}.
(b) Sin realizar la siguiente operación, ¿puedes afirmar sin ninguna duda que está incorrectamente efectuada? $4587113 * 321195642 = 1473360704962546$. Explica cómo deduces tu contestación. Enuncia el resultado teórico que utilices para responder esta pregunta.
(c) Explica teóricamente cómo se construyen las funciones de codificación y descodificación del sistema RSA, mostrando que son funciones una inversa de la otra. En particular, en un sistema RSA de parámetros $n = 91$ y $t = 7$ calcula la función de decodificación.

136 **(a)** Un mensaje oculto está almacenado en el número 39^{1164}. El mensaje oculto está formado por las dos últimas cifras de la representación decimal del número anterior, en el orden correspondiente. Teniendo en cuenta la asignación siguiente:

número	0	1	2	3	4	5	6	7	8	9
letra	m	k	b	e	o	f	s	p	a	n

Utiliza el Teorema de Euler para identificar el mensaje oculto. Sugerencia: las dos últimas cifras se pueden obtener trabajando en Z_{100}.
(b) Teniendo en cuenta que identificamos las letras del alfabeto con el conjunto de los enteros congruentes módulo 27, es decir, Z_{27}, explica teóricamente cómo se construyen las funciones de codificación y descodificación del sistema de clave privada visto en clase (cifrado afín), mostrando que son funciones una inversa de la otra.

137 **(a)** Calcula un entero a, tal que $43797689 \equiv a \pmod{23}$, $0 \leq a \leq 22$.
(b) Calcula los enteros x que verifican simultáneamente las siguientes condiciones: (i) $x \equiv 7 \pmod{23}$, (ii) si dividimos el número x por 16 nos da como residuo 11, y (iii) $6000 \leq x \leq 6999$.

138 Consideremos la siguiente asignación de letras a los enteros de 0 a 22:

T	R	W	A	G	M	Y	F	P	D	X	B	N	J	Z	S	Q	V	H	L	C	K	E
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22

Teniendo en cuenta esta asignación, y sabiendo que la letra del NIF correspondiente a un número de DNI se calcula a partir del único entero a tal que $\text{DNI} \equiv a \pmod{23}$, $0 \leq a \leq 22$, contesta razonadamente a las siguientes cuestiones:
(a) ¿Cuál es la letra del NIF correspondiente al DNI número 41236754?
(b) Consideremos el NIF: 73146[redacted] -F, en el que aparecen borrosos los tres últimos dígitos del DNI. Es decir, sabemos que la letra del NIF correspondiente al número de DNI 73146[redacted] es F. Además sabemos que si dividimos este número por 16 nos da como resto 11. Calcula razonadamente cuántos números del DNI cumplen esta condición y cuáles son.

139 Se ha cifrado un mensaje mediante el criptosistema de clave privada visto en clase (cifrado afín) e identificando las letras mayúsculas del alfabeto con los enteros módulo 28 (incluyendo el espacio en blanco). El mensaje cifrado ha resultado ser MQTF. Si la función de codificación es $C_{3,5}([m]) = [3][m] + [5]$, obtén la función de decodificación y calcula el mensaje original. La asignación de letras con los enteros congruentes módulo 28 es:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27