

MATEMÁTICA DISCRETA
Transparencias curso 2009/2010
Contenido

Bloque 1. Introducción a la teoría de grafos.

Lección 1. Grafos: fundamentos.

Lección 2. Accesibilidad y Conectividad.

Lección 3. Árboles.

Lección 4. Grafos Ponderados.

Bloque 2. Los Enteros.

Lección 1. Los números enteros.

Lección 2. Congruencias. Aritmética modular.

MATEMÁTICA DISCRETA

Bloque 1

INTRODUCCIÓN A LA TEORÍA DE GRAFOS

Transparencias

- Lección 1. Grafos: fundamentos.
- Lección 2. Accesibilidad y Conectividad.
- Lección 3. Árboles.
- Lección 4. Grafos Ponderados.

Lección 1.

GRAFOS: FUNDAMENTOS

1. Definición y conceptos básicos.
2. Tipos particulares de grafos.
3. Grado de un vértice.
4. Caminos y conexión.
5. Representación matricial.

1. DEFINICION Y CONCEPTOS BASICOS

Definiciones:

1. Un **grafo no dirigido** G es un par (V, A) , en el que V es un conjunto cuyos elementos llamaremos **vértices**, y A una familia de pares no ordenados de vértices, que llamaremos **aristas**.

2. Un **grafo dirigido** G es un par (V, A) , en el que V es un conjunto cuyos elementos llamaremos **vértices**, y A una familia de pares ordenados de vértices, que llamaremos **arcos**.

3. Llamamos **grafo no dirigido asociado** a un grafo dirigido, a un grafo con el mismo conjunto de vértices y en el que se han ignorado las direcciones de los arcos.

4. Un **grafo mixto** es aquel que contiene tanto arcos como aristas.

5. Los extremos de una arista (arco) se dice que son **incidentes** con la arista (arco).

6. Dos vértices incidentes con una misma arista (arco) se dicen **adyacentes**.

7. Un **bucle** es una arista (o arco) cuyos extremos son el mismo vértice.

2. TIPOS PARTICULARES DE GRAFOS.

Definiciones:

1. Un grafo **simple** es un grafo sin bucles en el que no hay dos aristas que unan el mismo par de vértices. Si el grafo es dirigido diremos que es simple si no tiene bucles y no hay dos arcos uniendo el mismo par de vértices y con la misma dirección. Si un grafo no es simple se llama **multigrafo**.

2. Un grafo no dirigido (dirigido) se dice que es **completo** si hay al menos una arista (arco) uniendo cada par de vértices distintos. Denominaremos por K_n al grafo completo no dirigido y simple.

3. Un grafo no dirigido diremos que es **bipartido** si existe una partición $\{X, Y\}$ del conjunto de vértices de forma que toda arista tiene un extremo en X y otro en Y . Un grafo dirigido es bipartido si lo es su grafo no dirigido asociado.

4. Diremos que un **grafo bipartido es completo** si cada vértice de X está unido con cada vértice de Y .

5. Sean $G = (V, A)$ y $H = (V', A')$ dos grafos. H es **subgrafo** de G si $V' \subseteq V$ y $A' \subseteq A$.

6. Diremos que un subgrafo H de un grafo G es **generador** si sus conjuntos de vértices son iguales.

3. GRADO DE UN VÉRTICE

Definiciones:

1. Llamamos **grado de un vértice** v en un grafo no dirigido G al número de aristas incidentes con él. Cada bucle se cuenta dos veces. Se denotará por $d_G(v)$.

Designamos por $\Gamma(v)$ al conjunto de vértices adyacentes a v .

2. Sea G un grafo dirigido. Llamaremos **grado de salida** de un vértice v y lo denotaremos por $d_s(v)$ al número de arcos salientes de v . Llamaremos **grado de entrada** de un vértice v y lo denotaremos por $d_e(v)$ al número de arcos entrantes en v . Se llamará **grado de un vértice** a la suma de estos dos grados.

Análogamente se puede definir $\Gamma(v)$ y $\Gamma^{-1}(v)$.

Teorema

1. Sea $G = (V, A)$ un grafo, entonces

$$\sum_{v \in V} d_G(v) = 2 \text{card}(A)$$

2. Sea $G = (V, A)$ un grafo dirigido, entonces:

$$\sum_{v \in V} d_s(v) = \sum_{v \in V} d_e(v) = \text{card}(A)$$

Corolario

El número de vértices de grado impar de un grafo es par.

4. CAMINOS Y CONEXION

Definiciones: Sea G un grafo no dirigido:

1. Una **cadena** es una sucesión finita $W = v_0 e_1 v_1 \dots e_k v_k$ cuyos términos son alternativamente vértices y aristas.
2. La **longitud** de una cadena es el número de aristas que contiene.
3. Una **cadena simple** es una cadena con todas sus aristas distintas.
4. Un **camino** es una cadena con todos sus vértices distintos.
5. Una **cadena cerrada** es una cadena de longitud no nula en donde el vértice inicial y final coinciden.
6. Un **ciclo** es una cadena simple cerrada con todos sus vértices distintos.

Estos conceptos son los mismos para grafos dirigidos salvo que las direcciones de los arcos deben concordar con la dirección del camino o cadena. En el caso dirigido el ciclo recibe el nombre de **circuito**.

7. Diremos que dos vértices u y v están **conectados** si existe un camino de u a v y viceversa.

8. Un grafo es **conexo** si todo par de vértices están conectados.

9. Un grafo dirigido es **débilmente conexo** si su grafo no dirigido asociado es conexo.

Teorema

La relación de conexión es de equivalencia y por tanto determina una partición en el conjunto de vértices. A los elementos de dicha partición se les denomina **componentes** conexas del grafo

Teorema

Un grafo es conexo si y sólo si el número de componentes conexas es 1.

Teorema (Para grafos no dirigidos)

Un grafo es bipartido si y sólo si no contiene ningún ciclo impar.

5. REPRESENTACION MATRICIAL

Definición

Sea G un grafo con n vértices $\{v_i\}_{i=1}^n$. Llamamos **matriz de adyacencia** a la matriz de orden $n \times n$, $A = [a_{ij}]$ tal que a_{ij} es igual al número de aristas (arcos) del vértice v_i al v_j .

Propiedades de la matriz de adyacencia:

1. Sea G un grafo no dirigido con matriz de adyacencia A . Entonces, la suma de los elementos de la fila i (o columna i) es igual al grado del vértice v_i .
2. Sea G un grafo dirigido con matriz de adyacencia A . Entonces, la suma de los elementos de la fila i es igual al grado de salida del vértice v_i y la suma de los elementos de la columna j es igual al grado de entrada del vértice v_j .
3. Sea G un grafo con matriz de adyacencia A . Entonces, el elemento (i, j) de la matriz A^r , $r \geq 1$, es igual al número de cadenas de v_i a v_j de longitud r .

Definición

Sea $G = (V, A)$ un grafo no dirigido con n vértices y m aristas siendo $V = \{v_i\}_{i=1}^n$ y $A = \{a_i\}_{i=1}^m$. Llamamos **matriz de incidencia** de G a la matriz de orden $n \times m$

$$M = [m_{ij}] / m_{ij} = \begin{cases} 0 & \text{si } v_i \text{ no es incidente con } a_j \\ 1 & \text{si } v_i \text{ es incidente con } a_j \\ 2 & \text{si } a_j \text{ es un bucle en } v_i \end{cases}$$

Sea $G = (V, A)$ un grafo dirigido con n vértices y m arcos siendo $V = \{v_i\}_{i=1}^n$ y $A = \{a_i\}_{i=1}^m$. Llamamos **matriz de incidencia** de G a la matriz de orden $n \times m$

$$B = [b_{ij}] / b_{ij} = \begin{cases} 0 & \text{si } v_i \text{ no es incidente con } a_j \\ 1 & \text{si } v_i \text{ es vértice inicial de } a_j \\ -1 & \text{si } v_i \text{ es vértice final de } a_j \\ 2 & \text{si } a_j \text{ es un bucle en } v_i \end{cases}$$

Propiedades de la matriz de incidencia:

1. Sea G un grafo no dirigido. La suma de los elementos de cada fila de la matriz de incidencia es igual al grado del correspondiente vértice.
2. Sea G un grafo no dirigido. La suma de los elementos de cada columna de la matriz de incidencia es igual a 2.
3. Sea G un grafo dirigido sin bucles. La suma de los elementos de cada columna de la matriz de incidencia es igual a 0.

Definiciones:

1. Sea G un grafo no dirigido. Llamaremos **tabla de aristas incidentes** del grafo G a una tabla que lista, para cada vértice v , todas las aristas incidentes con v .
2. Sea G un grafo dirigido. Llamaremos **tabla de arcos salientes** del grafo G a una tabla que lista, para cada vértice v , todos los arcos salientes de v . Llamaremos **tabla de arcos entrantes** del grafo G a una tabla que lista, para cada vértice v , todos los arcos entrantes en v .

Lección 2.

ACCESIBILIDAD Y CONECTIVIDAD

1. Accesibilidad.
2. Cálculo de componentes conexas.
3. Problemas de recorrido de aristas.
4. Problemas de recorridos de vértices.

1. ACCESIBILIDAD

Sea $G = (V, A)$ un grafo dirigido.

Definiciones:

1. Sean $x_i, x_j \in V$, diremos que x_j es **alcanzable** desde x_i o que x_i **alcanza** a x_j si existe un camino dirigido de x_i a x_j .

2. Sea $V = \{x_i\}_{i=1}^n$. Llamaremos **matriz de accesibilidad** asociada al grafo G a la matriz cuadrada de orden n definida por

$$R = [r_{ij}] / r_{ij} = \begin{cases} 1 & \text{si } x_i \text{ alcanza a } x_j \\ 0 & \text{en otro caso} \end{cases}$$

3. Sea $V = \{x_i\}_{i=1}^n$. Llamaremos **matriz de acceso** asociada al grafo G a la matriz cuadrada de orden n definida por

$$Q = [q_{ij}] / q_{ij} = \begin{cases} 1 & \text{si } x_i \text{ es alcanzable desde } x_j \\ 0 & \text{en otro caso} \end{cases}$$

Proposición $Q = R^T$.

2. CÁLCULO DE COMPONENTES CONEXAS.

Sea $G = (V, A)$ un grafo dirigido.

MÉTODO 1.

Etapa 1. Inicializar $i \leftarrow 1$, $V^{(1)} = V$.

Etapa 2. Tomar $v_i \in V^{(i)}$.

Etapa 3. Calcular $R(v_i) \cap Q(v_i)$.

Hacer $V^{(i+1)} = V^{(i)} \sim R(v_i) \cap Q(v_i)$.

Hacer $i \leftarrow i + 1$.

Etapa 4. Si $V^{(i)} = \emptyset$, entonces STOP.

En otro caso, volver a Etapa 2.

MÉTODO 2.

Otra forma de calcular las componentes conexas es calcular $R \otimes Q$. La componente conexa de x_i se calcula viendo qué columnas tienen un 1 en la fila i .

Observación: En el caso no dirigido es obvio que la componente conexa asociada a un vértice x_i puede ser calculada obteniendo el conjunto

$$x_i \cup \Gamma(x_i) \cup \dots \cup \Gamma^p(x_i)$$

3. PROBLEMAS DE RECORRIDOS DE ARISTAS.

Definiciones: Sea G un grafo conexo y en general no simple.

1. Llamaremos **tour** de G a una cadena cerrada que atraviesa cada arista de G al menos una vez.
2. Llamaremos **tour euleriano** de G a un tour de G que atraviesa cada arista exactamente una vez.
3. Llamaremos **grafo euleriano** a aquel en el que podemos encontrar un tour euleriano.
4. Llamaremos **camino euleriano** a una cadena (simple) que atraviesa cada arista exactamente una vez.

Teorema

Sea G un grafo no dirigido y conexo.

(a) G es euleriano si y sólo si no tiene vértices de grado impar.

(b) G contiene un camino euleriano si y sólo si tiene exactamente dos vértices de grado impar.

Teorema

Sea $G = (V, A)$ un grafo dirigido y débilmente conexo.

(a) G es euleriano si y sólo si, para todo vértice v , $d_e(v) = d_s(v)$.

(b) G contiene un camino euleriano si y sólo si

$$d_e(v) = d_s(v), \quad \forall v \neq p, q$$

$$d_e(p) = d_s(p) - 1, \quad d_e(q) = d_s(q) + 1.$$

Siendo p y q los vértices inicial y final respectivamente del camino.

ALGORITMO DE FLEURY

El siguiente algoritmo encuentra un tour o camino euleriano en un grafo no dirigido.

- (1)** Si el grafo es euleriano, a partir de un vértice cualquiera de G , construiremos una cadena simple de forma que no se repitan aristas y no se elijan aristas de corte a no ser que no haya otra alternativa. Al finalizar este proceso, es decir, cuando hayamos agotado todas las aristas, habremos obtenido un tour euleriano.

- (2)** Si el grafo contiene un camino euleriano comenzaremos con un vértice de grado impar siguiendo el proceso descrito.

MODIFICACIÓN PARA GRAFOS DIRIGIDOS

- (1) Si el grafo es euleriano, a partir de un vértice cualquiera de G construimos una cadena simple de forma que no se repitan arcos y no se elija nunca un arco si al eliminarlo aumenta el número de componentes conexas del grafo no dirigido asociado, a no ser que no tengamos otra alternativa.

- (2) Si el grafo contiene un camino euleriano, comenzamos con un vértice p tal que $d_e(p) = d_s(p) - 1$, siguiendo el proceso descrito.

5. PROBLEMAS DE RECORRIDO DE VÉRTICES

Definiciones:

1. Un **camino Hamiltoniano** en un grafo G es un camino que atraviesa cada vértice del grafo exactamente una vez.
2. Un **ciclo Hamiltoniano** en un grafo G es un ciclo que atraviesa cada vértice del grafo exactamente una vez.
3. Un grafo es **Hamiltoniano** si contiene un ciclo Hamiltoniano.

REGLAS BÁSICAS PARA CONSTRUIR CAMINOS Y CICLOS HAMILTONIANOS

Regla 1. Si G no es conexo, no posee ciclos Hamiltonianos.

Regla 2. Si G es un grafo con n vértices, entonces un camino Hamiltoniano debe tener exactamente $n - 1$ aristas, y un ciclo Hamiltoniano n aristas.

Regla 3. Si v es un vértice del grafo, entonces un camino Hamiltoniano debe tener al menos una arista incidente con v y como mucho dos.

Regla 4. Si G es Hamiltoniano, entonces $d_G(v) \geq 2$, $\forall v \in V$.

Regla 5. Si $v \in V$ tiene grado 2, entonces las dos aristas incidentes con v deben aparecer en cualquier ciclo Hamiltoniano de G .

Regla 6. Si $v \in V$ tiene grado mayor que 2, entonces cuando se intenta construir un ciclo Hamiltoniano, una vez que se pase por v , las aristas no utilizadas incidentes se dejan de tener en cuenta.

Regla 7. Al construir un ciclo o camino Hamiltoniano para G , no se puede dar el caso de obtener un ciclo para un subgrafo de G a menos que contenga todos los vértices de G .

Teorema

Sea G un grafo bipartido con partición $\{X, Y\}$.

(1) Si G tiene un ciclo Hamiltoniano, entonces $\text{card}(X) = \text{card}(Y)$.

(2) Si G tiene un camino Hamiltoniano, entonces $\text{card}(X)$ y $\text{card}(Y)$ difieren a lo sumo en 1.

El recíproco es cierto para grafos bipartidos completos con más de 2 vértices.

Teorema Teorema de Dirac

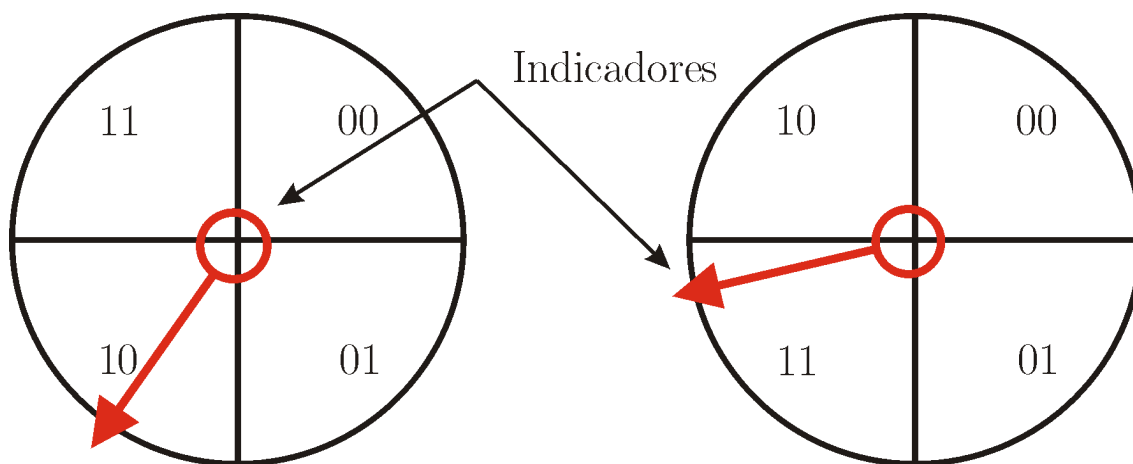
Todo grafo simple con n vértices, $n \geq 3$, en el que todo vértice tiene grado por lo menos $\frac{n}{2}$, tiene un ciclo Hamiltoniano.

Corolario

Si G es un grafo completo simple con n vértices, $n \geq 3$, entonces G tiene un ciclo Hamiltoniano.

APLICACIÓN: CODIGOS DE GRAY

Una manera de convertir la posición angular de un indicador rotativo a forma digital es dividir el círculo en 2^n sectores iguales, etiquetar los segmentos con números binarios de 0 a $2^n - 1$ y registrar el número de segmento que señala el indicador mediante algún sistema digital.



Para leer la etiqueta mediante el uso de sensores podemos colocar n anillos concéntricos segmentados, de manera que el indicador haga contacto con el anillo i si y sólo si el i -ésimo dígito de la etiqueta es un 1.

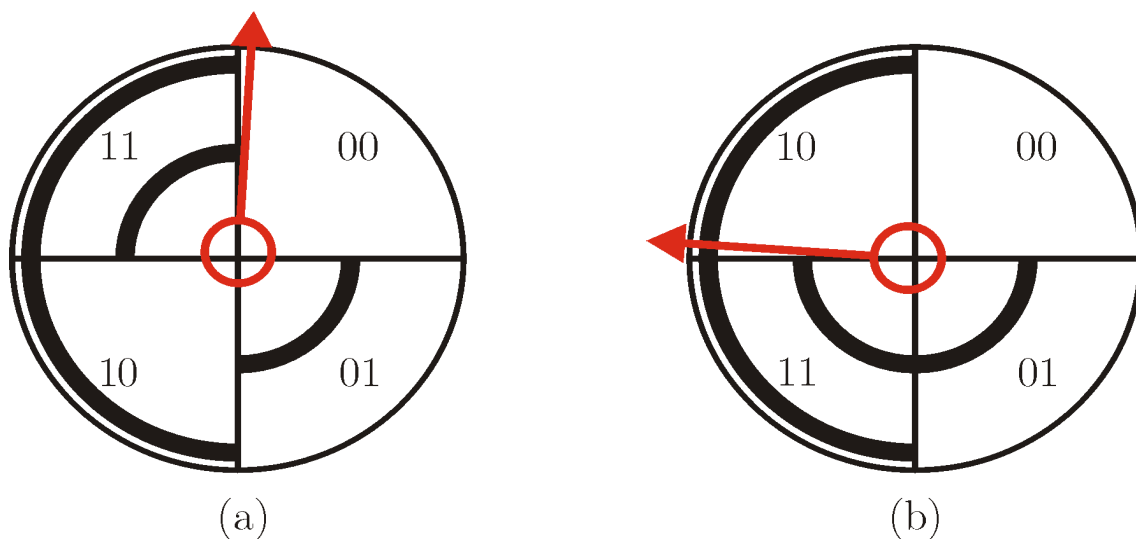
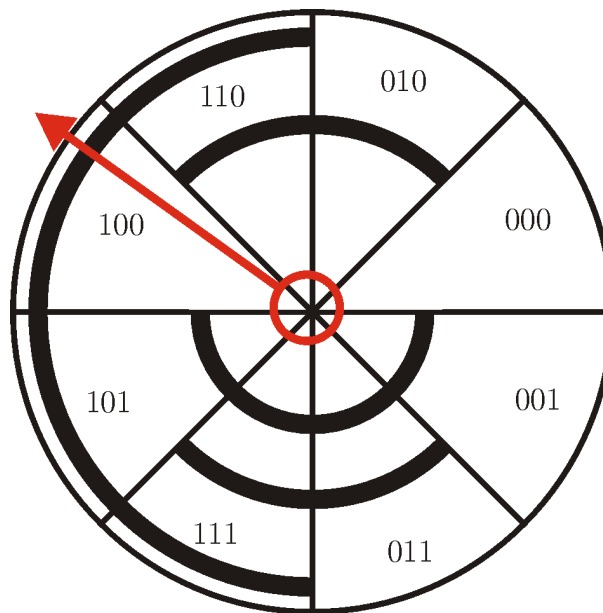


Figura (a): Si el indicador está en 00 pero cerca de la frontera entre 00 y 11, una pequeña irregularidad en el contacto puede hacer que se lea 01 (sector adyacente lejano), o 11 (sector adyacente), o 10 (sector opuesto). Errores en los dos dígitos.

Figura (b): Sólo se pueden producir errores en un sólo dígito y caso de producirse el error nos lleva siempre al sector más adyacente.

Definición

Un código de Gray de longitud n es una asignación de etiquetas a los 2^n sectores iguales del círculo con expresiones binarias de longitud n , de manera que las etiquetas de sectores adyacentes difieran en exactamente en un dígito.



Podemos ver la construcción de un código de Gray como un problema de grafos:

Consideremos como conjunto de vértices

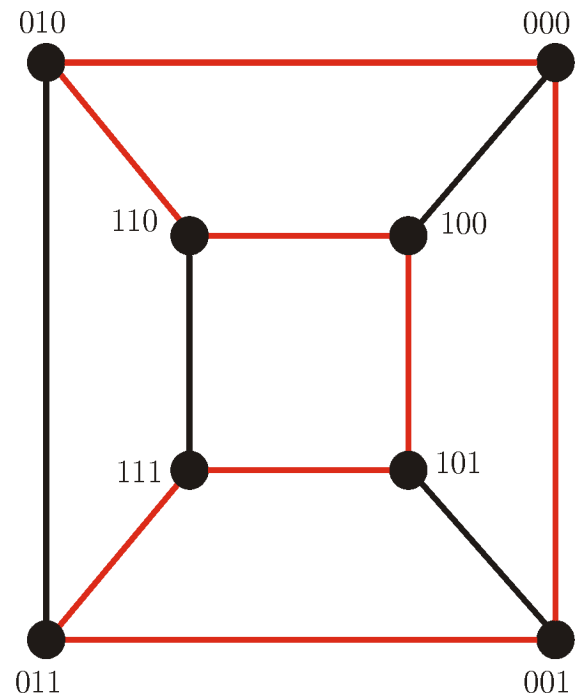
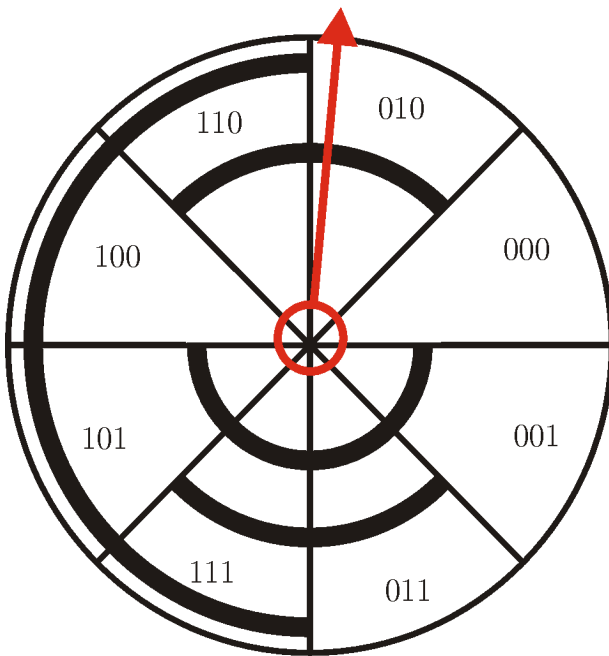
$$V = \{0, 1\}^n,$$

es decir, números binarios de longitud n , y unamos dos vértices $u, v \in V$ con una arista si u y v difieren en exactamente un dígito. Se puede demostrar por inducción que este grafo es Hamiltoniano para $n \geq 2$; recibe el nombre de n -cubo y se representa por Q_n .

Es evidente que un código de Gray corresponde a un ciclo Hamiltoniano en Q_n .

Ejemplo:

Hay 12 códigos de Gray de longitud 3. Uno de ellos queda representado aquí.



Lección 3.

ÁRBOLES

1. Definiciones. Propiedades y ejemplos.
2. Árboles con raíz o enraizados.
3. Algoritmos de búsqueda de primera profundidad.

1. DEFINICIONES. PROPIEDADES Y EJEMPLOS.

Sea G un grafo no dirigido.

Definiciones:

1. Diremos que G es un **árbol** si G es conexo y acíclico.
2. Diremos que T es un **árbol generador** de un grafo G si T es árbol y subgrafo generador de G .

Teorema

1. En un árbol dos vértices cualesquiera están unidos por un único camino.
2. Un grafo G es conexo si y sólo si tiene un árbol generador.
3. Si G es un árbol, entonces el número de aristas es igual al número de vértices menos uno.
4. Todo árbol T no trivial (más de 1 vértice) tiene al menos dos vértices de grado 1.

2. ÁRBOLES CON RAIZ O ENRAIZADOS.

Definiciones:

1. Sea T un árbol. Eligiendo un vértice r_0 de T que llamamos **raíz**, al ser el árbol conexo, todo otro vértice estará conectado con r_0 . Podemos entonces definir un grafo dirigido $T(r_0)$ donde todos los arcos sean extremos finales de un camino que se inicia en r_0 . A este árbol lo llamaremos **árbol enraizado en r_0** .

2. Sea T un árbol enraizado y u un vértice de T . Llamamos **nivel** del vértice u a la longitud del camino que va de la raíz a dicho vértice. La **altura** de un árbol es el valor del nivel máximo.

Definición Sea T un árbol con raíz r_0 . Supongamos que x, y, z son vértices de T y que $v_0v_1 \dots v_{n-1}v_n$ es un camino en T . Entonces:

- v_{n-1} es el **padre** de v_n .
- v_0, \dots, v_{n-1} son los **antepasados** de v_n .
- v_n es el **hijo** de v_{n-1} .
- Si x es un antepasado de y , entonces y es un **descendiente** de x .
- Si x e y son hijos de z , entonces x e y son **hermanos**.
- Si x no tiene hijos diremos que es un vértice **terminal**.
- Si x no es un vértice terminal diremos que es **interno**.
- El subgrafo de T que consiste en x y todos sus descendientes, con x como raíz se llama **subárbol** de T que tiene a x como raíz.

Definiciones:

1. Un **árbol binario** es un árbol enraizado en el cual cada vértice tiene un hijo a la derecha, o un hijo a la izquierda, o un hijo a la derecha y un hijo a la izquierda, o bien ningún hijo.
2. Un árbol binario **completo** es un árbol binario en el que cada vértice tiene un hijo a la derecha y otro a la izquierda o bien ningún hijo.

Teorema

1. Si T es un árbol binario completo con i vértices internos, entonces T tiene $i + 1$ vértices terminales y $2i + 1$ vértices en total.
2. Sea T un árbol binario de altura h y con t vértices terminales, entonces $t \leq 2^h$.

Definición

Un árbol binario de búsqueda es un árbol binario T en donde se han asociado datos a los vértices. Los datos se disponen de manera que para cualquier vértice v en T , cada dato en el subárbol a la izquierda (derecha, respectivamente) de v es menor que (mayor que, respectivamente) el dato correspondiente a v .

ALGORITMO DE BÚSQUEDA

Sea T un árbol binario de búsqueda con raíz RAIZ. Si v es un vértice:

- $IZQUIERDA(v)$ es el hijo a la izquierda de v .
- $DERECHA(v)$ es el hijo a la derecha de v .
- Si v no tiene hijos a la izquierda haremos $IZQUIERDA(v) = \lambda$.
- Si v no tiene hijos a la derecha haremos $DERECHA(v) = \lambda$.
- $VALOR(v)$ proporciona el dato asociado al vértice v .

Paso 1. $P := \text{RAIZ}$

Paso 2. Si $P = \lambda$, STOP.

En otro caso si $\text{VALOR}(P) = W$, STOP
(P es el vértice que contiene el dato W .)

Paso 3. Si $W > \text{VALOR}(P)$, tómesese

$P := \text{DERECHA}(P)$, e ir a 2.

En otro caso, tómesese

$P := \text{IZQUIERDA}(P)$, e ir a 2.

3. ALGORITMOS DE BÚSQUEDA DE PRIMERA PROFUNDIDAD.

Definición

Un **árbol enraizado ordenado** es un árbol enraizado tal que el conjunto de hijos de cada padre está ordenado linealmente de izquierda a derecha.

ALGORITMO PREORDEN(v)

Paso 1. Listar los subárboles con los hijos de v como raíz [Utilizar $\text{PREORDEN}(w)$ para listar T para cada hijo w de v].

Paso 2. Listar T_v poniendo en sucesión v seguido por las listas del paso 1 en el orden de izquierda a derecha.

Si v no tiene hijos, la lista de T_v es solamente v .

ALGORITMO POSTORDEN(v)

Paso 1. Listar los subárboles con los hijos de v como raíz [Utilizar $\text{POSTORDEN}(w)$ para listar T para cada hijo w de v].

Paso 2. Listar T_v poniendo en sucesión las listas del paso 1 en el orden de izquierda a derecha seguidas por v .

Si v no tiene hijos, la lista de T_v es solamente v .

ALGORITMO INORDEN(v)

Paso 1. Listar el subárbol de la izquierda [Utilizar INORDEN(w) para el hijo w a la izquierda de v].

Paso 2. Listar el subárbol de la derecha [Utilizar INORDEN(w) para el hijo w a la derecha de v].

Paso 3. Listar T_v poniendo en una sucesión las listas del paso 1, después v y luego el resultado del paso 2.

Si v no tiene hijos, la lista de T_v es solamente v .

Lección 4.

GRAFOS PONDERADOS

1. Definición y ejemplos.
2. Caminos más cortos.
3. Grafos acíclicos. Método del camino crítico.
4. Algoritmo de Dijkstra.
5. Caminos más cortos entre todos los pares de vértices. Método de Floyd-Warshall.
6. Árboles generadores de mínimo peso.

1. DEFINICION Y EJEMPLOS

Definiciones:

1. Un grafo simple $G = (V, A)$ (grafo simple dirigido, respectivamente) diremos que es un grafo **ponderado** si tiene asociado una función $W : A \longrightarrow \mathbf{R}$ llamada **función de ponderación**.

La imagen de cada arista (arco, respectivamente) determinada por los vértices v_i y v_j la llamaremos **peso** de la arista (arco) y lo denotaremos por w_{ij} .

2. Sea $G = (V, A)$ un grafo ponderado finito tal que $V = \{v_1, \dots, v_n\}$. Llamaremos **matriz de peso** del grafo G a la siguiente matriz de orden $n \times n$

$$W = [a_{ij}] / a_{ij} = \begin{cases} w_{ij} & \text{si } (v_i, v_j) \in A \\ \infty & \text{si } (v_i, v_j) \notin A \end{cases}$$

3. En un grafo ponderado llamamos **peso de un camino** a la suma de los pesos de las aristas (arcos respectivamente) que lo forman.

4. En un grafo ponderado llamamos **camino más corto** entre dos vértices dados al camino de peso mínimo entre dichos vértices.

5. En un grafo ponderado llamaremos **camino más largo o camino crítico** entre dos vértices dados al camino de peso máximo entre dichos vértices.

2. CAMINOS MAS CORTOS.

Supondremos que los pesos asociados a los arcos son todos no negativos y que el grafo es dirigido. Supondremos además que los vértices del grafo están numerados de 1 a n , de forma que w_{ij} representa el peso del arco (i, j) y que el vértice 1 es el origen del camino. Además u_j denotará el peso del c.m.c. de 1 a j .

Teorema

Sea $1, \dots, k, \dots, j$ un c.m.c. entre los vértices 1 y j de un grafo ponderado G . Entonces las secciones de este camino $1, \dots, k$ y k, \dots, j son los caminos más cortos entre los vértices respectivos.

Corolario

Supongamos que en un grafo ponderado tenemos un camino más corto entre los vértices 1 y j . Sea k el vértice inmediatamente anterior a j en este camino. Entonces la sección de este camino desde 1 a k es el camino más corto entre estos dos vértices. Además

$$u_j = u_k + w_{kj}$$

Ecuaciones de Bellman

$$u_1 = 0$$

$$u_j = \min_{k \neq j} \{u_k + w_{kj}\} \quad j = 2, \dots, n$$

3. GRAFOS ACÍCLICOS. MÉTODO DEL CAMINO CRÍTICO

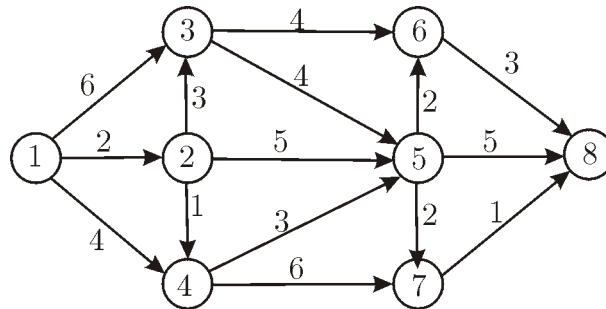
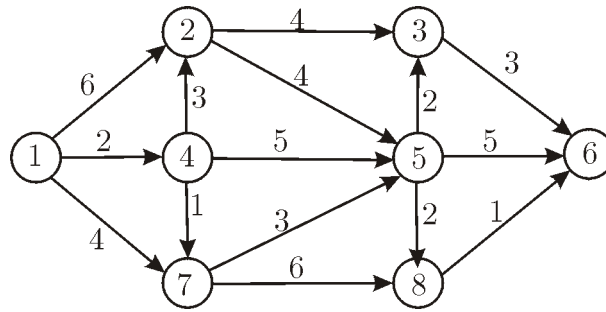
Teorema

Un grafo dirigido no tiene circuitos si y sólo si existe una numeración de los vértices para la que se cumple que si (i, j) es un arco del grafo entonces $i < j$.

Con esta numeración, las ecuaciones de Bellman pueden ser reemplazadas por

$$u_1 = 0$$

$$u_j = \min_{k < j} \{u_k + w_{kj}\} \quad j = 2, \dots, n$$



$$u_1 = 0$$

$$u_2 = u_1 + w_{12} = 2$$

$$u_3 = \min \{u_1 + w_{13}, \overline{u_2 + w_{23}}\}$$

$$= \min \{6, 2 + 3\} = 5$$

$$u_4 = \min \{u_1 + w_{14}, \overline{u_2 + w_{24}}\}$$

$$= \min \{4, 2 + 1\} = 3$$

$$u_5 = \min \{u_2 + w_{25}, u_3 + w_{35}, \overline{u_4 + w_{45}}\}$$

$$= \min \{2 + 5, 5 + 4, 3 + 3\} = 6$$

$$u_6 = \min \{u_3 + w_{36}, \overline{u_5 + w_{56}}\}$$

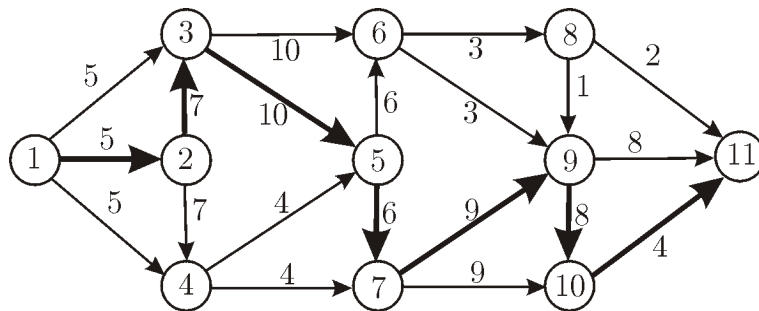
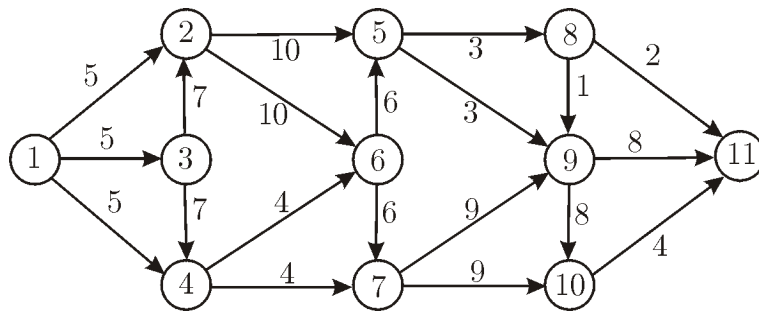
$$= \min \{5 + 4, 6 + 2\} = 8$$

$$u_7 = \min \{u_4 + w_{47}, \overline{u_5 + w_{57}}\}$$

$$= \min \{3 + 6, 6 + 2\} = 8$$

$$u_8 = \min \{u_5 + w_{58}, u_6 + w_{68}, \overline{u_7 + w_{78}}\}$$

$$= \min \{6 + 5, 8 + 3, 8 + 1\} = 9$$

EJEMPLO: PERT

EJEMPLO: PERT (Continuación)

$$u_1 = 0$$

$$u_2 = \text{máx} \{u_1 + w_{12}\} = 5$$

$$\begin{aligned} u_3 &= \text{máx} \{u_1 + w_{13}, \overline{u_2 + w_{23}}\} \\ &= \text{máx} \{5, 5 + 7\} = 12 \end{aligned}$$

$$\begin{aligned} u_4 &= \text{máx} \{u_1 + w_{14}, \overline{u_2 + w_{24}}\} \\ &= \text{máx} \{5, 5 + 7\} = 12 \end{aligned}$$

$$\begin{aligned} u_5 &= \text{máx} \{\overline{u_3 + w_{35}}, u_4 + w_{45}\} \\ &= \text{máx} \{12 + 10, 12 + 4\} = 22 \end{aligned}$$

$$\begin{aligned} u_6 &= \text{máx} \{u_3 + w_{36}, \overline{u_5 + w_{56}}\} \\ &= \text{máx} \{12 + 10, 22 + 6\} = 28 \end{aligned}$$

$$\begin{aligned} u_7 &= \text{máx} \{u_4 + w_{47}, \overline{u_5 + w_{57}}\} \\ &= \text{máx} \{12 + 4, 22 + 6\} = 28 \end{aligned}$$

$$u_8 = \text{máx} \{u_6 + w_{68}\} = 28 + 3 = 31$$

$$\begin{aligned} u_9 &= \text{máx} \{u_6 + w_{69}, \overline{u_7 + w_{79}}, u_8 + w_{89}\} \\ &= \text{máx} \{28 + 3, 28 + 9, 31 + 1\} = 37 \end{aligned}$$

$$\begin{aligned} u_{10} &= \text{máx} \{u_7 + w_{7,10}, \overline{u_9 + w_{9,10}}\} \\ &= \text{máx} \{28 + 9, 37 + 8\} = 45 \end{aligned}$$

$$\begin{aligned} u_{11} &= \text{máx} \{u_8 + w_{8,11}, u_9 + w_{9,11}, \overline{u_{10} + w_{10,11}}\} \\ &= \text{máx} \{31 + 2, 37 + 8, 45 + 4\} = 49 \end{aligned}$$

4. ALGORITMO DE DIJKSTRA

Sea un grafo ponderado tal que $w_{ij} \geq 0$. Este algoritmo encuentra los caminos más cortos y sus pesos desde el vértice 1 al resto.

Se asignan varias etiquetas a los vértices del grafo. En algún momento algunos vértices podrán tener etiquetas variables y el resto etiquetas fijas.

Denotaremos al conjunto de vértices con etiqueta fija por P y al conjunto de vértices con etiqueta variable por T .

EJEMPLO DIJKSTRA

Paso 1. Inicialización.

$$\begin{aligned}P &= \{1\} & T &= \{2, 3, \dots, n\} \\u_1 &= 0 \\u_j &= w_{1j} & j &\in \Gamma(1) \\u_j &= \infty & j &\notin \Gamma(1)\end{aligned}$$

Paso 2. Designación de etiqueta variable como fija.

Determinar $k \in T / u_k = \min_{j \in T} \{u_j\}$

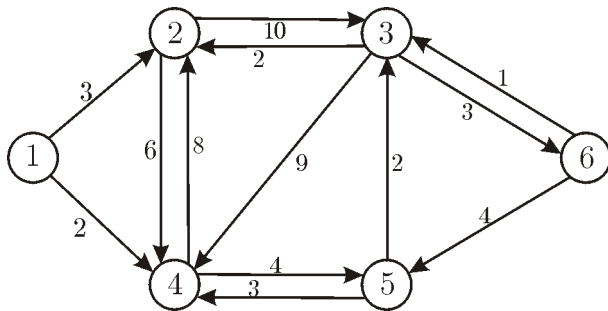
Hacer $T := T \sim \{k\}$ y $P := P \cup \{k\}$

Si $T = \emptyset$, STOP; u_j es el peso del camino más corto de 1 a j , $j = 2, 3, \dots, n$

Paso 3. Actualización.

$$\forall j \in \Gamma(k) \cap T, \quad u_j := \min\{u_j, u_k + w_{kj}\}$$

Ir al Paso 2.



Inicialización
Iteración 1
$T = \{2, 3, 4, 5, 6\}$
$P = \{1\},$
$u_1 = 0$
$u_2 = w_{12} = 3$
$u_3 = \infty$
$u_4 = w_{14} = 2$
$u_5 = \infty$
$u_6 = \infty$

Iteración 2
$T = \{2, 3, 5, 6\}$ $P = \{1, 4\}, \Gamma(4) \cap T = \{2, 5\}$ $u_2 = \min\{u_2, u_4 + w_{42}\} = \min\{3, 2 + 8\} = 3$ $u_3 = \infty$ $u_5 = \min\{u_5, u_4 + w_{45}\} = \min\{\infty, 2 + 4\} = 6$ $u_6 = \infty$
Iteración 3
$T = \{3, 5, 6\}$ $P = \{1, 4, 2\}, \Gamma(2) \cap T = \{3\}$ $u_3 = \min\{u_3, u_2 + w_{23}\} = \min\{\infty, 3 + 10\} = 13$ $u_5 = 6$ $u_6 = \infty$
Iteración 4
$T = \{3, 6\}$ $P = \{1, 4, 2, 5\}, \Gamma(5) \cap T = \{3\}$ $u_3 = \min\{u_3, u_5 + w_{53}\} = \min\{13, 6 + 2\} = 8$ $u_6 = \infty$
Iteración 5
$T = \{6\}$ $P = \{1, 4, 2, 5, 3\}, \Gamma(3) \cap T = \{6\}$ $u_6 = \min\{u_6, u_3 + w_{36}\} = \min\{\infty, 8 + 3\} = 11$
Iteración 6
$T = \emptyset$ $P = \{1, 4, 2, 5, 3, 6\}, \text{ STOP}$

5. CAMINOS MÁS CORTOS ENTRE TODOS LOS PARES DE VÉRTICES. MÉTODO DE FLOYD-WARSHALL

Llamaremos u_{ij} al peso del camino más corto de i a j . Utilizaremos las variables:

$u_{ij}^{(m)} \equiv$ peso del camino más corto del vértice i al j con la restricción de que no contenga a los vértices $m, m + 1, \dots, n$ (exceptuando a los extremos i y j en su caso).

Estas variables pueden calcularse recursivamente utilizando las ecuaciones:

$$u_{ij}^{(1)} = w_{ij} \quad \forall i, j$$

$$u_{ij}^{(m+1)} = \min \left\{ u_{ij}^{(m)}, u_{im}^{(m)} + u_{mj}^{(m)} \right\} \quad \forall i, j,$$

$$m = 1, 2, \dots, n$$

Y es posible ver que:

$$u_{ij} = u_{ij}^{(n+1)}$$

con lo que tendremos los pesos de los caminos más cortos entre todos los pares de vértices.

Para facilitar la construcción de los caminos más cortos una vez calculados sus pesos, se puede utilizar otra matriz

$$\Theta^{(m)} = [\theta_{ij}^{(m)}]$$

donde $\theta_{ij}^{(m)}$ representa el vértice anterior al j en el camino más corto de i a j en la iteración m .

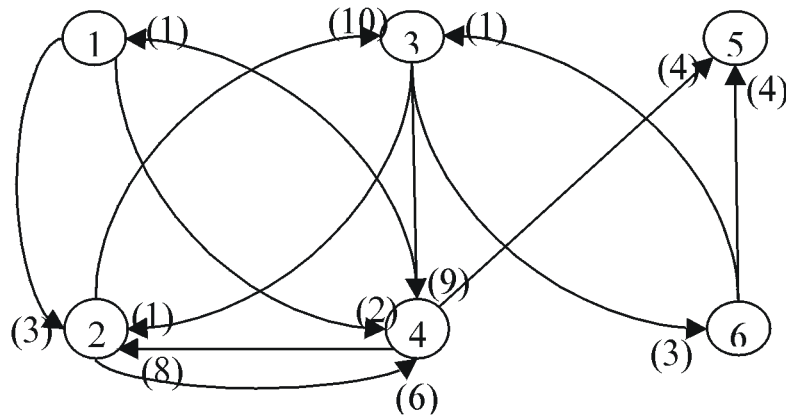
Inicialmente $\theta_{ij}^{(1)} = i$ si $u_{ij}^{(1)} < +\infty$, y

$$\theta_{ij}^{(m+1)} = \begin{cases} \theta_{ij}^{(m)} & \text{si } u_{ij}^{(m+1)} = u_{ij}^{(m)} \\ \theta_{mj}^{(m)} & \text{si } u_{ij}^{(m+1)} < u_{ij}^{(m)} \end{cases}$$

EJEMPLO

Matrices:

		$[u_{ij}^{(m)}]$						$[\theta_{ij}^{(m)}]$					
		1	2	3	4	5	6	1	2	3	4	5	6
(m=1)	1	∞	3	∞	2	∞	∞	1	1		1		
	2	∞	∞	10	6	∞	∞	2		2	2		
	3	∞	1	∞	9	∞	3	3		3			3
	4	1	8	∞	∞	4	∞	4	4			4	
	5	∞	∞	∞	∞	∞	∞	5					
	6	∞	∞	1	∞	4	∞	6		6		6	
(m=2)	1	∞	3	∞	2	∞	∞	1	1		1		
	2	∞	∞	10	6	∞	∞	2		2	2		
	3	∞	1	∞	9	∞	3	3		3			3
	4	1	[4]	∞	[3]	4	∞	4	4	[1]	[1]	4	
	5	∞	∞	∞	∞	∞	∞	5					
	6	∞	∞	1	∞	4	∞	6		6		6	
(m=3)	1	∞	3	[13]	2	∞	∞	1	1	[2]	1		
	2	∞	∞	10	6	∞	∞	2		2	2		
	3	∞	1	[11]	[7]	∞	3	3		[2]	[2]		3
	4	1	4	[14]	3	4	∞	4	4	1	[2]	1	4
	5	∞	∞	∞	∞	∞	∞	5					
	6	∞	∞	1	∞	4	∞	6		6		6	



(m=4)

	1	2	3	4	5	6
1	∞	3	13	2	∞	[16]
2	∞	[11]	10	6	∞	[13]
3	∞	1	11	7	∞	3
4	1	4	14	3	4	[17]
5	∞	∞	∞	∞	∞	∞
6	∞	[2]	1	[8]	4	[4]

	1	2	3	4	5	6
1		1	2	1		[3]
2		[3]	2	2		[3]
3		3	2	2		3
4	4	1	2	1	4	[3]
5						
6		[3]	6	[2]	6	[3]

(m=5)

	1	2	3	4	5	6
1	[3]	3	13	2	[6]	16
2	[7]	[10]	10	6	[10]	13
3	[8]	1	11	7	[11]	3
4	1	4	14	3	4	17
5	∞	∞	∞	∞	∞	∞
6	[9]	2	1	8	4	4

	1	2	3	4	5	6
1	[4]	1	2	1	[4]	3
2	[4]	[1]	2	2	[4]	3
3	[4]	3	2	2	[4]	3
4	4	1	2	1	4	3
5						
6	[4]	3	6	2	6	3

(m=6)

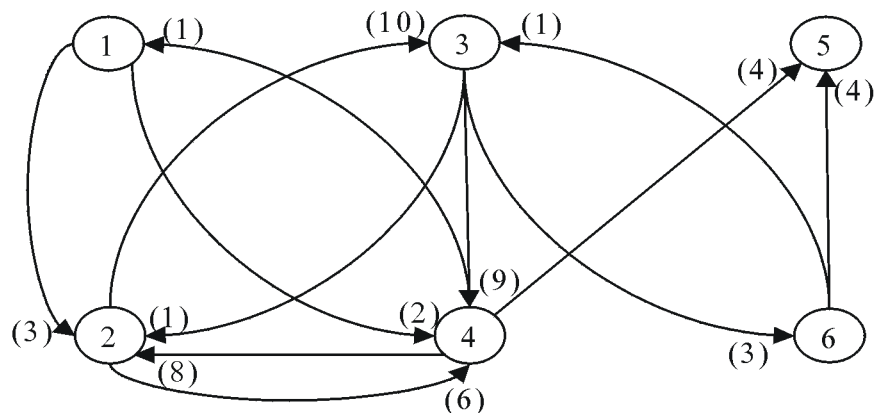
	1	2	3	4	5	6
1	3	3	13	2	6	16
2	7	10	10	6	10	13
3	8	1	11	7	11	3
4	1	4	14	3	4	17
5	∞	∞	∞	∞	∞	∞
6	9	2	1	8	4	4

	1	2	3	4	5	6
1	4	1	2	1	4	3
2	4	1	2	2	4	3
3	4	3	2	2	4	3
4	4	1	2	1	4	3
5						
6	4	3	6	2	6	3

(m=7)

	1	2	3	4	5	6
1	3	3	13	2	6	16
2	7	10	10	6	10	13
3	8	1	[4]	7	[7]	3
4	1	4	14	3	4	17
5	∞	∞	∞	∞	∞	∞
6	9	2	1	8	4	4

	1	2	3	4	5	6
1	4	1	2	1	4	3
2	4	1	2	2	4	3
3	4	3	[6]	2	[6]	3
4	4	1	2	1	4	3
5						
6	4	3	6	2	6	3



6. ÁRBOLES GENERADORES DE MÍNIMO PESO

Definición

Sea G un grafo ponderado y no dirigido. Diremos que T es un **árbol generador de mínimo peso** si T es un árbol generador tal que la suma de los pesos asociados a sus aristas es mínima.

ALGORITMO DE KRUSKAL

Sea $G = (V, A)$ un grafo no dirigido y con pesos w_i asociados a cada arista $e_i \in A$, $i = 1, 2, \dots, m$ y con n vértices.

Paso 1. $T = \emptyset$

Paso 2. Ordenar en orden creciente las aristas de G , es decir,

$$e_1, e_2, \dots, e_m / w_1 \leq w_2 \leq \dots \leq w_m$$

Paso 3. Añadir aristas en T de forma ordenada siempre que no se formen ciclos hasta tener en T $n - 1$ aristas.

ALGORITMO DE PRIM

Sea G un grafo no dirigido ponderado con n vértices.

Paso 1. $T = \emptyset$, $U = \{v^*\}$ $v^* \in V(G)$

$$L(u) = w(u, v^*) \quad (\infty \text{ si } \nexists \text{ arista}) \quad \forall u \in V(G)$$

Paso 2. Encontrar $u^* \in V(G)$ tal que

$$L(u^*) = \min_{u \notin U} \{L(u)\}$$

Paso 3. Añadir u^* a U , es decir, $U := U \cup \{u^*\}$

Añadir la arista e incidente con u^* con peso $L(u^*)$ a T , es decir, $T := T \cup \{e\}$

Paso 4. Si $\text{card}(U) = n$, STOP.

Si $\text{card}(U) < n$, hacer

$$L(u) := \min \{L(u), w(u^*, u)\} \quad \forall u \notin U$$

e ir al Paso 2.

MATEMÁTICA DISCRETA

Bloque 2

LOS ENTEROS

Transparencias



Lección 1. Los números enteros.

Lección 2. Congruencias. Aritmética modular.

Lección 1.

LOS NUMEROS ENTEROS

1. Los enteros. Principio de la buena ordenación.
2. Divisibilidad.
3. Máximo común divisor y mínimo común múltiplo.
4. Números primos. Factorización.

1. LOS ENTEROS. PRINCIPIO DE LA BUENA ORDENACION.

Definición El conjunto \mathbb{Z} verifica los siguientes axiomas:

A1 Hay definidas dos operaciones binarias $+$ y \cdot .

A2 Son conmutativas

A3 Son asociativas

A4 Existe elemento neutro para cada una de ellas

A5 \cdot es distributiva respecto de $+$

A6 $\forall a \in \mathbb{Z} \exists!(-a) \in \mathbb{Z} / a + (-a) = 0$

A7 Si $a \neq 0$ y $a \cdot b = a \cdot c$, entonces $b = c$

Existe en \mathbb{Z} una relación \leq que verifica:

A8 Es reflexiva

A9 Es antisimétrica

A10 Es transitiva

A11 Si $a \leq b$, entonces $a + c \leq b + c$

A12 Si $a \leq b$ y $0 \leq c$, entonces $a \cdot c \leq b \cdot c$

A13 Si X es un subconjunto no vacío y acotado inferiormente, entonces X posee mínimo.

2. DIVISIBILIDAD

Teorema (Algoritmo de la división)

Sean a, b dos enteros. Si b no es nulo, existen dos únicos enteros q, r verificando

$$a = b \cdot q + r \text{ y } 0 \leq r \leq |b|.$$

Definición

El cálculo de q y r en el teorema anterior se llama **división euclídea** de a por b ; el número q es el **cociente** de la división, y r es el **resto**.

APLICACIÓN: REPRESENTACIÓN EN BASE t DE UN ENTERO

Sea $t \geq 2$ un entero (**base para el cálculo**).

Para cualquier $x \in \mathbb{Z}$, por aplicación reiterada del algoritmo de la división, tenemos:

$$\begin{aligned} x &= t \cdot q_0 + r_0 \\ q_0 &= t \cdot q_1 + r_1 \\ q_1 &= t \cdot q_2 + r_2 \\ &\dots \\ &\dots \\ q_{n-2} &= t \cdot q_{n-1} + r_{n-1} \\ q_{n-1} &= t \cdot q_n + r_n \end{aligned}$$

con $r_i \in \mathbb{Z} / 0 \leq r_i \leq t - 1$, $i = 0, 1, 2, \dots, n$.

Si paramos cuando $q_n = 0$, obtenemos, eliminando los cocientes q_i :

$$x = r_n \cdot t^n + r_{n-1} \cdot t^{n-1} + \dots + r_1 \cdot t + r_0.$$

Hemos representado x en base t :

$$x = (r_n r_{n-1} \dots r_1 r_0)_t.$$

Convencionalmente $t = 10$ es la base usual y generalmente omitimos de dicha representación el subíndice $t = 10$. Por ejemplo

$$1432 = 1 \cdot 10^3 + 4 \cdot 10^2 + 3 \cdot 10^1 + 2 \cdot 10^0.$$

Veamos cuál es la representación en base 2 de $(109)_{10}$:

$$109 = 2 \cdot 54 + 1$$

$$54 = 2 \cdot 27 + 0$$

$$27 = 2 \cdot 13 + 1$$

$$13 = 2 \cdot 6 + 1$$

$$6 = 2 \cdot 3 + 0$$

$$3 = 2 \cdot 1 + 1$$

$$1 = 2 \cdot 0 + 1$$

Así

$$109 = 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1.$$

Y su representación en base 2 es:

$$(1101101)_2$$

Definición

Sean $a, b \in \mathbb{Z}$, con $b \neq 0$. Se dice que b **divide a** a , b es un **divisor de** a , o que a es un **múltiplo de** b y lo representamos por b/a , si existe un entero q tal que $a = b \cdot q$.

Proposición Sean $a, b, c \in \mathbb{Z}$.

1. $1/a, a/0, a/a$
2. Si a/b y b/a , entonces $a = \pm b$
3. Si a/b y b/c , entonces a/c
4. Si a/b , entonces $a/bx, \forall x \in \mathbb{Z}$
5. Si a/b y a/c , entonces $a/(bx + cy), \forall x, y \in \mathbb{Z}$

3. MÁXIMO COMÚN DIVISOR. MÍNIMO COMÚN MULTIPLO

Definición

Sean $a, b \in \mathbb{Z}$, donde al menos uno de ellos es no nulo. Entonces, $c \in \mathbb{Z}$ se denomina **máximo común divisor** (mcd) de a, b si

1. c/a y c/b
2. Si d/a y d/b entonces d/c

Teorema

Para cualesquiera $a, b \in \mathbb{Z}^+$, existe un $c \in \mathbb{Z}^+$ único, que es el máximo común divisor de a y b .

Observación

$$\text{mcd}(a, b) = \text{mcd}(-a, b) = \text{mcd}(a, -b) = \text{mcd}(-a, -b)$$

Definición

Los enteros a, b se denominan **primos entre sí**, cuando $\text{mcd}(a, b) = 1$.

Corolario

Sean $a, b \in \mathbb{Z}$ y $d = \text{mcd}(a, b)$. Entonces

$$\exists s, t \in \mathbb{Z} / d = as + bt.$$

Teorema (Algoritmo de Euclides)

Si $a, b \in \mathbb{Z}$ y se aplica el algoritmo de la división:

$$\begin{aligned} a &= q_1 b + r_1 & 0 < r_1 < b \\ b &= q_2 r_1 + r_2 & 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 & 0 < r_3 < r_2 \\ &\dots \\ r_i &= q_{i+2} r_{i+1} + r_{i+2} & 0 < r_{i+2} < r_{i+1} \\ &\dots \\ r_{k-2} &= q_k r_{k-1} + r_k & 0 < r_k < r_{k-1} \\ r_{k-1} &= q_{k+1} r_k \end{aligned}$$

Entonces, r_k el último resto distinto de cero es igual al $\text{mcd}(a, b)$.

Definición

Sean $a, b \in \mathbb{Z}$ y $c \in \mathbb{Z}^+$. Se denomina **ecuación diofántica** a la ecuación

$$ax + by = c,$$

donde $x, y \in \mathbb{Z}$ son incógnitas.

Teorema

Sean $a, b \in \mathbb{Z}$, $c \in \mathbb{Z}^+$ y $d = \text{mcd}(a, b)$. La ecuación diofántica $ax + by = c$ tiene solución entera si y sólo si d/c , es decir, si $c = kd$, $k \in \mathbb{Z}$.

Observación

Es obvio que obtenida una solución entera que verifique la identidad de Bezout $ax + by = d$ ($x = x_0, y = y_0$) tendremos también una solución entera de la anterior ecuación sin más que considerar $x = kx_0, y = ky_0$.

Teorema

Sean $a, b \in \mathbb{Z}^+$ y $d = \text{mcd}(a, b)$.

Sean $\alpha, \beta \in \mathbb{Z}^+$ / $a = \alpha d$, $b = \beta d$ y

$x_0, y_0 \in \mathbb{Z}$ una solución de la ecuación diofántica

$$ax + by = dn.$$

Entonces, $x, y \in \mathbb{Z}$ es solución de la anterior ecuación si y sólo si

$$\left. \begin{array}{l} x = x_0 + k\beta \\ y = y_0 - k\alpha \end{array} \right\} k \in \mathbb{Z}.$$

Definición

Sean $a, b \in \mathbb{Z}^+$. Diremos que $c \in \mathbb{Z}^+$ es el **mínimo común múltiplo** de a y b y escribiremos $c = \text{mcm}(a, b)$, si c es el menor de los enteros positivos que son múltiplos comunes de a y b .

Teorema

Sean $a, b \in \mathbb{Z}^+$ y $c = \text{mcm}(a, b)$.

Si $\exists d \in \mathbb{Z}^+$ tal que a/d y b/d , entonces c/d .

4. NUMEROS PRIMOS. FACTORIZACION

Definición

Diremos que $p \in \mathbb{Z}^+$ es **primo** si tiene exactamente dos divisores positivos distintos.

Teorema

Si a es un entero estrictamente mayor que 1, su menor divisor estrictamente mayor que 1 es un número primo.

Teorema

Todo elemento de \mathbb{Z}^+ mayor o igual que 2, es un número primo o es un producto de números primos. Esta descomposición es única salvo el orden.

Definición

El cálculo de los números primos cuyo producto vale un número entero dado n , se llama **descomposición en factores primos de n** .

Teorema

Sean $a, b \in \mathbb{Z}^+$ y

$$a = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}, \quad b = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t},$$

con cada p_i primo y $e_i, r_i \geq 0$, $1 \leq i \leq t$.

Entonces, si

$$a_i = \min\{e_i, r_i\}, \quad b_i = \max\{e_i, r_i\}, \quad 1 \leq i \leq t,$$

se obtiene que

$$\text{mcd}(a, b) = \prod_{i=1}^t p_i^{a_i}, \quad \text{mcm}(a, b) = \prod_{i=1}^t p_i^{b_i}$$

Teorema

Sean $a, b \in \mathbb{Z}^+$, entonces

$$a \cdot b = \text{mcd}(a, b) \cdot \text{mcm}(a, b).$$

Lección 2.

CONGRUENCIAS. ARITMETICA MODULAR

1. Congruencias.
2. Los enteros módulo n . Aritmética en \mathbb{Z}_n .
3. Elementos inversibles en \mathbb{Z}_n .
Función de Euler.
4. Aplicación a la criptografía.

1. CONGRUENCIAS

Definición

Sea n un entero mayor que 1. Dados a y $b \in \mathbb{Z}$, diremos que a es **congruente con b módulo n** y escribiremos $a \equiv b \pmod{n}$ si $a - b = kn$ con $k \in \mathbb{Z}$.

Ejemplo:

$$17 \equiv 2 \pmod{5}.$$

$$-7 \equiv -49 \pmod{6}.$$

Teorema

La relación de congruencia módulo n ($n > 1$) es una relación de equivalencia.

Teorema

Si $(x_n x_{n-1} \dots x_1 x_0)_{10}$ es la representación en base 10 de un entero positivo x , entonces

$$x \equiv (x_0 + x_1 + \dots + x_{n-1} + x_n) \pmod{9}.$$

2. LOS ENTEROS MÓDULO n . ARITMÉTICA EN \mathbb{Z}_n

$$\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\},$$

donde:

$$\begin{aligned} [0] &= \{0 + kn \mid k \in \mathbb{Z}\} \\ [1] &= \{1 + kn \mid k \in \mathbb{Z}\} \\ &\vdots \\ [n-1] &= \{(n-1) + kn \mid k \in \mathbb{Z}\}, \end{aligned}$$

Ya que, para todo $a \in \mathbb{Z} \exists! q, r \in \mathbb{Z}$ tal que

$$a = qn + r, \quad 0 \leq r < |n|,$$

de modo que $a \equiv r \pmod{n}$ y por tanto

$$[a] = [r], \quad 0 \leq r \leq n-1.$$

Teorema

\mathbb{Z}_n es un anillo conmutativo con unidad con las operaciones inducidas:

$$[x] + [y] = [x + y], \quad [x] \cdot [y] = [xy], \quad \forall x, y \in \mathbb{Z}.$$

3. ELEMENTOS INVERSIBLES EN \mathbb{Z}_n . FUNCION DE EULER

Teorema

Sea \mathbb{Z}_n^* el conjunto de los elementos inversibles de \mathbb{Z}_n , para el producto. Son equivalentes:

1. $[a] \in \mathbb{Z}_n^*$.
2. $\exists [b] \in \mathbb{Z}_n$ tal que $[a][b] = [1]$.
3. $\exists b, k \in \mathbb{Z}$ tal que $ab - kn = 1$.
4. $\text{mcd}(a, n) = 1$.

Ejemplo: Hállese $[25]^{-1}$ en \mathbb{Z}_{72} .

El algoritmo de Euclides da lugar a:

$$\begin{aligned}72 &= 2(25) + 22, & 0 < 22 < 25 \\25 &= 1(22) + 3, & 0 < 3 < 22 \\22 &= 7(3) + 1, & 0 < 1 < 3 \\3 &= 3(1) + 0.\end{aligned}$$

Por tanto $\text{mcd}(25, 72) = 1$. Además:

$$\begin{aligned}1 &= 22 - 7(3) = 22 - 7(25 - 22) = \\&= (-7)(25) + (8)(22) = \\&= (-7)(25) + 8(72 - 2(25)) = \\&= 8(72) - 23(25).\end{aligned}$$

Luego $[25]^{-1} = [-23] = [49 - 72] = [49]$.

Definición

Sea $n \geq 1$. Llamamos **función de Euler** sobre n y la denotamos por $\varphi(n)$ al cardinal de \mathbb{Z}_n^* .

$$\varphi(n) = \text{card}\{x \in \mathbb{Z}^+ / x \leq n \text{ y } \text{mcd}(x, n) = 1\}.$$

Claramente si p es primo, $\varphi(p) = p - 1$.

Teorema (Teorema de Euler)

Si $[y] \in \mathbb{Z}_n^*$, entonces $[y]^{\varphi(n)} = [1]$.

Teorema (Teorema de Euler)

Sean $y, n \in \mathbb{Z}^+ / \text{mcd}(y, n) = 1$, entonces

$$y^{\varphi(n)} \equiv 1 \pmod{n}.$$

Corolario (Teorema de Fermat)

Sea $y \in \mathbb{Z}^+$ y p primo. Si p no divide a y , entonces

$$y^{p-1} \equiv 1 \pmod{p}.$$

Proposición

Si $p \in \mathbb{Z}^+$ es un número primo y $u \in \mathbb{Z}^+$, entonces

$$\varphi(p^u) = p^{u-1}(p - 1).$$

Teorema

- Sean n_1, n_2, \dots, n_k enteros positivos primos entre sí dos a dos.

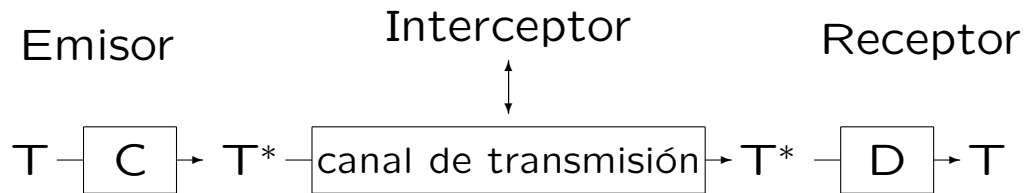
Si $n = n_1 n_2 \cdots n_k$:

$$\varphi(n) = \varphi(n_1) \varphi(n_2) \cdots \varphi(n_k).$$

- Si $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ es la descomposición en factores primos de un entero positivo n ,

$$\begin{aligned} \varphi(n) &= \\ &= p_1^{r_1-1} (p_1 - 1) p_2^{r_2-1} (p_2 - 1) \cdots p_k^{r_k-1} (p_k - 1) \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right). \end{aligned}$$

APLICACION A LA CRIPTOGRAFIA



T: Texto llano (en lenguaje natural o bien reducido a una sucesión de dígitos de transcripción inmediata).

T*: Criptograma, o texto cifrado (ilegible para quien no conozca D).

C: Función de cifrado o de codificación, conocida por el emisor.

D: Función de descifrado o de decodificación, conocida por el receptor.

C y D son funciones inversas una de otra.

Definición

Un **sistema criptográfico** o **criptosistema** consiste en cinco componentes: M, M^*, K, C y D .

M es el conjunto de todos los mensajes a transmitir;

M^* el de todos los mensajes cifrados;

K el conjunto de claves a utilizar, es decir los parámetros que controlan los procesos de cifrado y descifrado;

C el conjunto de todos los métodos de cifrado:

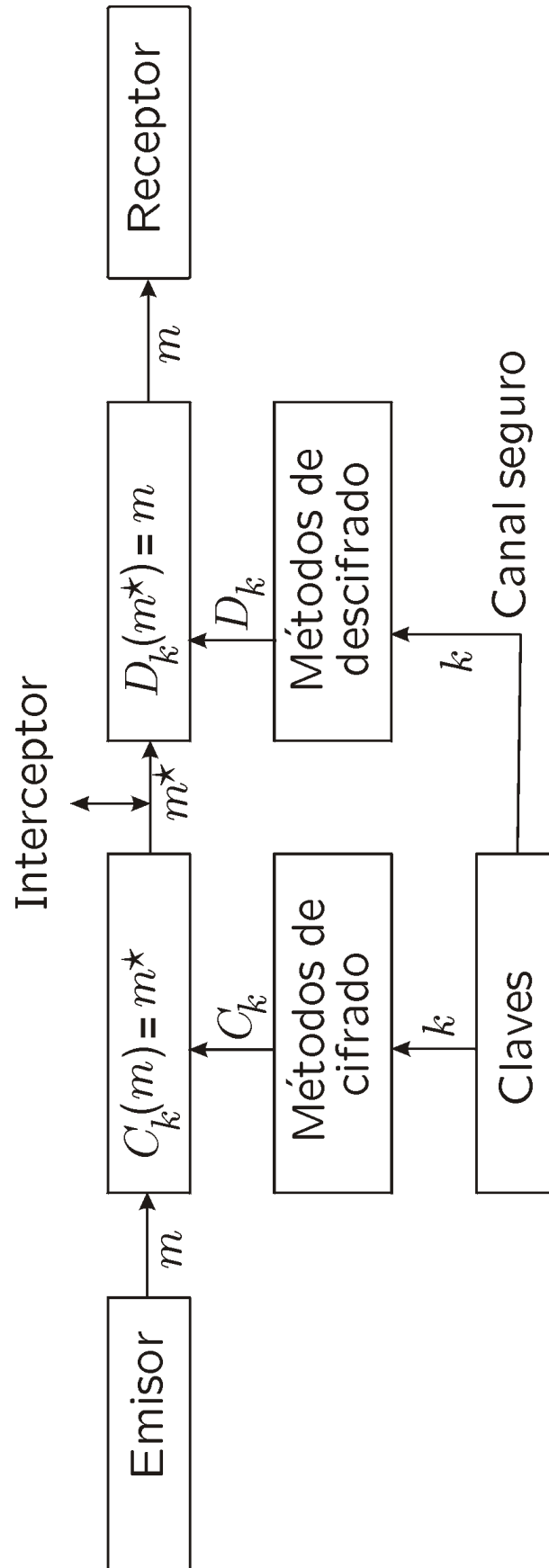
$$C = \{C_k : M \longrightarrow M^*, k \in K\};$$

D el de todos los métodos de descifrado:

$$D = \{D_k : M^* \longrightarrow M, k \in K\}.$$

Para una clave dada k , la transformación D_k es la inversa de C_k ; es decir,

$$D_k(C_k(m)) = m, \quad \forall m \in M.$$



CRIPTOSISTEMA DE CLAVE PRIVADA.

Un criptosistema de clave privada basa su técnica en un valor secreto llamado clave. El emisor y el receptor establecen de mutuo acuerdo el sistema criptográfico, y la clave concreta que utilizarán en sus comunicaciones. Este tipo de criptosistemas permite, conociendo la función de cifrado, obtener la de descifrado, y viceversa.

Ejemplo: Identificando las letras del alfabeto con los enteros módulo 27:

$$M = M^* = \mathbb{Z}_{27}.$$

$C_{r,s} : M \longrightarrow M^*$, $r, s \in \mathbb{Z}$, definida por

$$C_{r,s}([m]) = [r][m] + [s], \quad \text{con } \text{mcd}(r, 27) = 1.$$

La función de descifrado será

$$D_{r,s} : M^* \longrightarrow M \quad / \quad D_{r,s}([m^*]) = [r]^{-1}([m^*] - [s]).$$

Tomando como caso particular $r = 2$ y $s = 3$:

$$C_{2,3}([m]) = [2][m] + [3], \quad \text{con } \text{mcd}(2, 27) = 1.$$

$$D_{2,3}([m^*]) = [2]^{-1} ([m^*] - [3]).$$

ROMA \longrightarrow MGAD

$$[18], [15], [12], [0] \xrightarrow{C_{2,3}} [12], [6], [0], [3]$$

Si aplicáramos ahora el algoritmo de descifrado, obteniendo previamente $[2]^{-1} = [14]$, volveríamos a obtener el texto original.

CRIPTOSISTEMA DE CLAVE PUBLICA.

Ejemplo: Sistema Rivest-Shamir-Adleman
(Sistema RSA).

Sean p y q dos números primos, y $n = pq$. Consideremos $M = M^* = \mathbf{Z}_n^*$ y t un entero tal que $\text{mcd}(t, \varphi(n)) = 1$.

En estas condiciones existe un entero s tal que

$$ts \equiv 1 \pmod{\varphi(n)},$$

esto es,

$$ts = k\varphi(n) + 1 \quad \text{para algún } k \in \mathbf{Z}.$$

Definimos la función de cifrado por

$$C : M \longrightarrow M^* / C([m]_n) = [m]_n^t.$$

Y la función de descifrado por

$$D : M^* \longrightarrow M / D([m^*]_n) = [m^*]_n^s.$$

La semiclave que se publica es el par (n, t) .

Deben mantenerse en secreto $p, q, \varphi(n)$ y s .

Supongamos el caso concreto donde $p = 13$ y $q = 17$. Entonces,

$$n = 13 \times 17 = 221 \text{ y}$$

$$\varphi(n) = 12 \times 16 = 192.$$

Por tanto $M = M^* = \mathbf{Z}_{221}^*$.

Entonces, escogiendo

$$t = 11 \text{ (ya que, } \text{mcd}(11, 192) = 1)$$

calculamos el valor de s tal que

$$ts \equiv 1 \pmod{192}$$

y encontramos $s = 35$.

Por tanto:

$$C([m]_{221}) = [m]_{221}^{11}.$$

$$D([m^*]_{221}) = [m^*]_{221}^{35}.$$