MATEMÁTICA DISCRETA

Bloque 2

LOS ENTEROS

Transparencias

ESTRUCTURAS ALGEBRAICAS

Grupo

Sea A un conjunto, + una ley de composición.
(A,+) será un Grupo si (IANS)

- \+ es una ley de composición **I**nterna
- \+ es una ley **A**sociativa
- existe un elemento **N**eutro para +
- cada elemento de A tiene un elemento **S**imétrico para la ley +. (opuesto)

(A,+) será un Grupo Conmutativo (o Abeliano 1802-1829) si + es Conmutativa.

Anillo

Sea A un conjunto, + y • dos leyes de composición.
(A,+,•) será un Anillo si

- (A;+) es un Grupo Conmutativo
- • es una ley de composición Interna
- • es una ley Asociativa
- • es distributiva sobre + en ambos lados.

(A,+,•) será un Anillo Conmutativo si • es Conmutativa
(A,+,•) será un Anillo Unitario si existe un elemento Neutro para •
(A,+,•) será un Anillo Íntegro (o Dominio de Integridad) si no existen divisores de cero.

Cuerpo

Sea A un conjunto y +,• dos leyes de composición.
(A,+,•) será un Cuerpo si

- (A,+,•) será un Anillo Conmutativo
- cada elemento de A tiene un elemento Simétrico para la ley •. (Inverso)

MATEMÁTICA DISCRETA

Bloque 2

LOS ENTEROS

Transparencias

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

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

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:

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

con $r_i \in \mathbb{Z}$ / $0 \leq r_i \leq t-1,\ i = 0, 1, 2, \ldots, n$.
Si paramos cuando $q_n = 0$, obtenemos, eliminando los cocientes q_i:

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

Hemos representado x en base t:

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

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 $(109)_{10}$:

$$\begin{aligned}
109 &= 2 \cdot 54 + 1 \\
54 &= 2 \cdot 27 + 0 \\
27 &= 2 \cdot 13 + 1 \\
13 &= 2 \cdot 6 + 1 \\
6 &= 2 \cdot 3 + 0 \\
3 &= 2 \cdot 1 + 1 \\
1 &= 2 \cdot 0 + 1
\end{aligned}$$

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. MÌNIMO 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
mcd(a, b)=mcd($-a, b$)=mcd($a, -b$)=mcd($-a, -b$)

Definición

Los enteros a, b se denominan **primos entre sí**, cuando mcd(a, b)=1.

Corolario

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

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

Teorema (Algoritmo de Euclides)

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

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

Entonces, r_k el último resto distinto de cero es igual al 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 $d =$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 $d =$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

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

Definición
Sean $a, b \in \mathbb{Z}^+$. Diremos que $c \in \mathbb{Z}^+$ es el **mínimo común múltiplo** de a y b y escribiremos $c =$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 $c =$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

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

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 $a \equiv b \ (mod\ n)$ si $a - b = kn$ con $k \in \mathbb{Z}$.

Ejemplo:

$$17 \equiv 2 \ (mod\ 5).$$

$$-7 \equiv -49 \ (mod\ 6).$$

Teorema

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

Teorema

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

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

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

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

donde:

$$\begin{array}{c}
[0] = \{0 + kn \ / \ k \in \mathbb{Z}\} \\
[1] = \{1 + kn \ / \ k \in \mathbb{Z}\} \\
\vdots \\
[n-1] = \{(n-1) + kn \ / \ k \in \mathbb{Z}\},
\end{array}$$

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 $a \equiv r \ (mod \ n)$ 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. mcd(a, n)= 1.

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

El algoritmo de Euclides da lugar a:

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

Por tanto $\mathrm{mcd}(25, 72) = 1$. 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 $\mathbb{Z}_n^*$.

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

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

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

Corolario (Teorema de Fermat)

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

$$y^{p-1} \equiv 1 \ (mod \ p).$$

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

1. Sean $n_1, n_2, \ldots, n_k$ enteros positivos primos entre sí dos a dos.

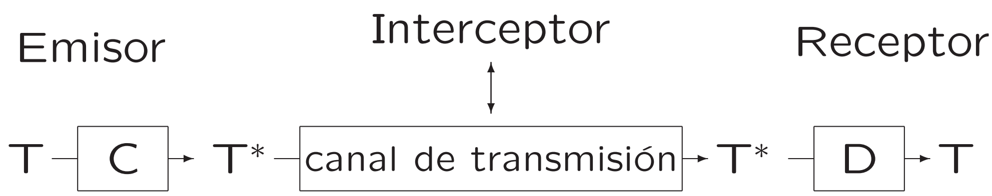
   Si $n = n_1 n_2 \cdots n_k$:

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

2. 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:

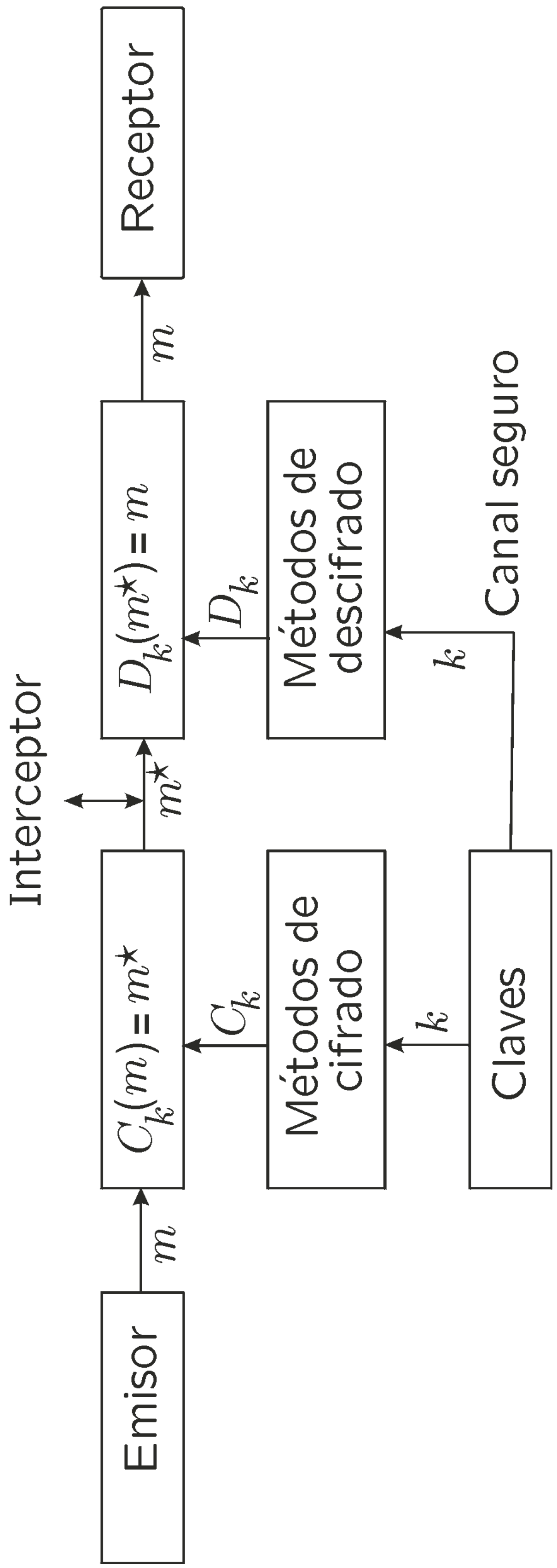
$$C = \{C_k : M \longrightarrow M^*, \ k \in K\};$$

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,

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


Emisor
m
$C_k(m) = m^\star$
C_k
Métodos de cifrado
k
Claves
Interceptor
$m^\star$
$D_k(m^\star) = m$
D_k
Métodos de descifrado
k
Canal seguro
m
Receptor

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:
$M = M^* = \mathbf{Z_{27}}$.
$C_{r,s} : M \longrightarrow M^*$, $r, s \in \mathbb{Z}$, definida por

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

La función de descifrado será

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

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

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

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

$$\text{ROMA} \longrightarrow \text{MGAD}$$

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

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 $M = M^* = \mathbf{Z}_{\mathbf{n}}^*$ y t un entero tal que mcd$(t, \varphi(n)) = 1$.

En estas condiciones existe un entero s tal que

$$ts \equiv 1 \ (mod \ \varphi(n)),$$

esto es,

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

Definimos la función de cifrado por

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

Y la función de descifrado por

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

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

Entonces, escogiendo

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

calculamos el valor de s tal que

$$ts \equiv 1 \ (mod\ 192)$$

y encontramos $s = 35$.

Por tanto:

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

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