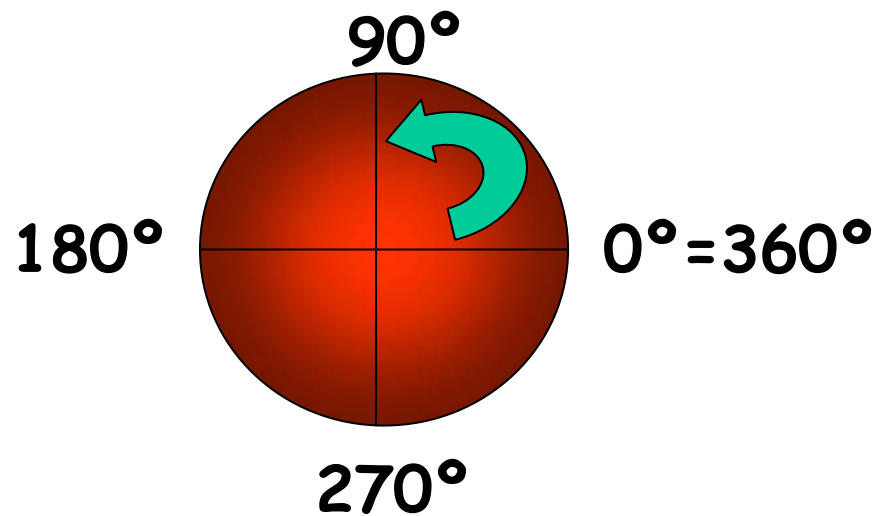


# Códigos para tratamiento de errores

- Códigos polinómicos o de redundancia cíclica
  - Conceptos previos
    - Es natural contar de forma cíclica
      - LOS GRADOS: Supongamos que contamos un número de grados entero.  
El orden es:  
 $0, 1, 2, \dots, 45, \dots, 180, \dots, 357, 358, 359, 360=0, 1, \text{etc.}$



# Códigos para tratamiento de errores

- Códigos polinómicos o de redundancia cíclica
  - Conceptos previos
    - LOS GRADOS:  
Es fácil operar
      - » El siguiente a 359 es 0
      - » El anterior a 0 es 359
      - » Tres más que 358 es 1
      - » Cinco menos que 2 es 357



# Códigos para tratamiento de errores

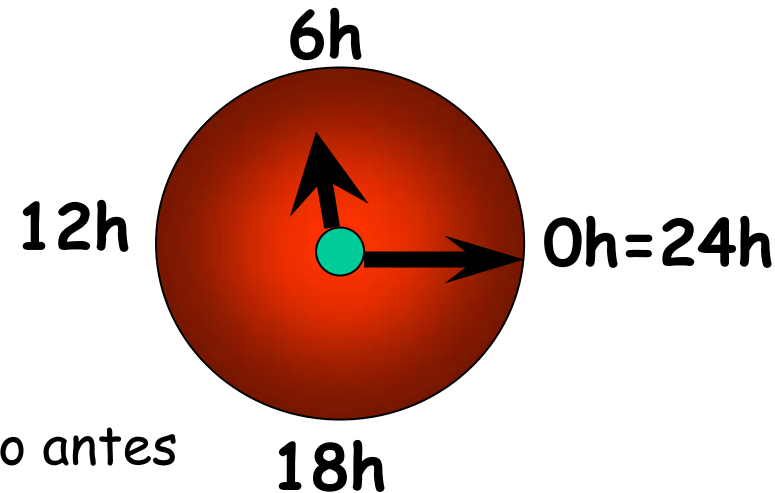
- Códigos polinómicos o de redundancia cíclica

- Conceptos previos

- LAS HORAS DEL DÍA

El orden es

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18,  
19, 20, 21, 22, 23, 0, 1, ...



Y operar es como antes



Escuela Politécnica Superior

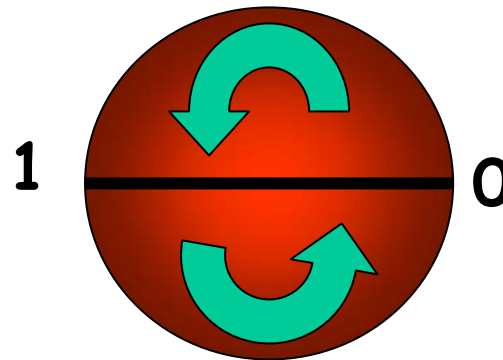
# Códigos para tratamiento de errores

- Códigos polinómicos o de redundancia cíclica
  - Conceptos previos

- El conjunto de los enteros módulo 2

-  $\{0, 1\}$

- Su orden cíclico



- Las operaciones pueden representarse con tablas

$$\begin{aligned} 1+1 &= 0 \\ 0-1 &= 1 \end{aligned}$$

+	0	1
0	0	1
1	1	0

-	0	1
0	0	1
1	1	0

*	0	1
0	0	0
1	0	1

# Códigos para tratamiento de errores

- Códigos polinómicos o de redundancia cíclica

- Conceptos previos

- Observaciones sobre los polinomios  $Q[x]$

- División de polinomios con coeficientes racionales (Q)

Ejemplo:  $D = 6x^4 + 9x^3 + 5x + 2$  y  $d = 2x^2 - 1$

$$\begin{array}{r} 6x^4 + 9x^3 + 0x^2 + 5x + 2 \quad | \quad 2x^2 + 0x - 1 \\ \underline{6x^4 + 0x^3 - 3x^2} \phantom{+ 5x + 2} \\ 0x^4 + 9x^3 + 3x^2 + 5x \phantom{+ 2} \quad | \quad 3x^2 + (9/2)x + (3/2) \\ \phantom{0x^4 + } \underline{+ 9x^3 + 0x^2 - (9/2)x} \phantom{+ 2} \\ \phantom{0x^4 + } 0x^3 + 3x^2 + (19/2)x + 2 \phantom{+ 2} \\ \phantom{0x^4 + } \phantom{0x^3 + } \underline{+ 3x^2 + 0x - (3/2)} \\ \phantom{0x^4 + } \phantom{0x^3 + } 0x^2 + (19/2)x + (7/2) \end{array}$$

Se obtiene:  $q = 3x^2 + (9/2)x + (3/2)$  y  $r = (19/2)x + (7/2)$



# Códigos para tratamiento de errores

- Códigos polinómicos o de redundancia cíclica
  - Conceptos previos

- Observaciones sobre los polinomios  $Q[x]$

Ejemplo:

Se puede representar abreviadamente:

6	9	0	5	2	2	0	-1
6	0	-3			3	9/2	3/2
0	9	+3	5				
	9	0	-(9/2)				
	0	3	+(19/2)	2			
		3	0	-(3/2)			
		0	(19/2)	+(7/2)			



# Códigos para tratamiento de errores

- Códigos polinómicos o de redundancia cíclica

- Conceptos previos

- Polinomios con coeficientes enteros módulo 2

- Se puede demostrar (no objeto de este curso) que esta división también es posible cuando los coeficientes son enteros módulo 2 siempre que las operaciones (resta, productos, etc.) sean definidas en ese conjunto

- Ejemplo:  $D = x^{13} + x^{12} + x^{10} + x^8 + x^7 + x^5 + x^4$  y  $d = x^4 + x + 1$

$$\begin{array}{r}
 \textcolor{red}{1} \textcolor{red}{1} \textcolor{red}{0} \textcolor{red}{1} \textcolor{red}{0} \textcolor{red}{1} \textcolor{red}{1} \textcolor{red}{0} \textcolor{red}{1} \textcolor{red}{1} \textcolor{red}{0} \textcolor{red}{0} \textcolor{red}{0} \textcolor{red}{0} \textcolor{red}{0} \quad \overline{) \quad 1 \textcolor{blue}{0} \textcolor{blue}{0} \textcolor{blue}{1} \textcolor{blue}{1}} \\
 \underline{1 \textcolor{blue}{0} \textcolor{blue}{0} \textcolor{blue}{1} \textcolor{blue}{1}} \phantom{0000000000000} \\
 0 \textcolor{blue}{1} \textcolor{blue}{0} \textcolor{blue}{0} \textcolor{blue}{1} \textcolor{blue}{1} \phantom{000000000000} \\
 \underline{1 \textcolor{blue}{0} \textcolor{blue}{0} \textcolor{blue}{1} \textcolor{blue}{1}} \phantom{000000000000} \\
 0 \textcolor{green}{0} \textcolor{green}{0} \textcolor{green}{0} \textcolor{green}{0} \textcolor{green}{0} \textcolor{magenta}{1} \textcolor{magenta}{0} \textcolor{magenta}{1} \textcolor{magenta}{1} \textcolor{magenta}{0} \phantom{000000} \\
 \phantom{000000} \underline{1 \textcolor{magenta}{0} \textcolor{magenta}{0} \textcolor{magenta}{1} \textcolor{magenta}{1}} \phantom{000000} \\
 00 \textcolor{green}{1} \textcolor{green}{0} \textcolor{green}{1} \textcolor{green}{0} \textcolor{green}{0} \phantom{000000} \\
 \phantom{000000} \underline{1 \textcolor{green}{0} \textcolor{green}{0} \textcolor{green}{1} \textcolor{green}{1}} \phantom{000000} \\
 00 \textcolor{green}{1} \textcolor{green}{1} \textcolor{green}{1} \textcolor{green}{0} \phantom{000000}
 \end{array}$$

**Resultado:**  $q = x^9 + x^8 + x^3 + x$  y  $r = x^3 + x^2 + x$



# Códigos para tratamiento de errores

- Códigos polinómicos o de redundancia cíclica

- Presentación de la técnica

- Se interpretan las cadenas de 1's y 0's como coeficientes enteros módulo 2 de polinomios
    - Los k bits de cada mensaje se tratan como si fueran los coeficientes de un polinomio  $M(x)$ , de orden  $k-1$ , en el que las operaciones se hacen en módulo 2

- Si el mensaje fuese: 10010110

el polinomio considerado sería:

$$\begin{aligned} M(x) &= 1 \cdot x^7 + 0 \cdot x^6 + 0 \cdot x^5 + 1 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x^1 + 0 \cdot x^0 = \\ &= x^7 + x^4 + x^2 + x \end{aligned}$$

- Se utiliza un polinomio generador  $G(x)$  de grado  $r$ . Este polinomio está predeterminado, y es el mismo en el emisor y el receptor





# Códigos para tratamiento de errores

- Códigos polinómicos o de redundancia cíclica
  - Presentación de la técnica
    - Operaciones en módulo 2:

$$\begin{aligned}0 + 0 &= 0 \\0 + 1 &= 1 \\1 + 0 &= 1 \\1 + 1 &= 0 \text{ (sin acarreo)}\end{aligned}$$

$$\begin{aligned}0 - 0 &= 0 \\0 - 1 &= 1 \text{ (sin acarreo)} \\1 - 0 &= 1 \\1 - 1 &= 0\end{aligned}$$



# Códigos para tratamiento de errores

- Códigos polinómicos o de redundancia cíclica

- Presentación de la técnica

- Objetivo del procedimiento: Añadir  $r$  bits al mensaje de  $k$  bits, de forma tal que el polinomio resultante,  $T(x)$ , correspondiente a los  $k+r$  bits, sea divisible por  $G(x)$
    - El receptor verifica si  $T(x)$  es divisible por  $G(x)$ , y si no lo es hay un error en la transmisión



# Códigos para tratamiento de errores

- Códigos polinómicos o de redundancia cíclica

- Uso de la técnica

- Emisor (algoritmo a seguir):

- Añadir  $r$  bits 0 al extremo de menor orden del mensaje. El polinomio correspondiente será  $x^r \cdot M(x)$

- Dividir (módulo 2)  $x^r \cdot M(x)$  entre  $G(x)$ : 
$$\frac{x^r \cdot M(x)}{G(x)} = C(x) + \frac{R(x)}{G(x)}$$

$C(x)$  es el cociente y  $R(x)$  el resto

- Restar a  $x^r \cdot M(x)$  el valor del resto  $R(x)$  (esto es equivalente a añadir al mensaje original  $M(x)$  el resto  $R(x)$ )

$$T(x) = x^r \cdot M(x) - R(x)$$

- Se obtiene así  $T(x)$ , cuyos coeficientes (unos o ceros) sustituyen el mensaje a transmitir.  $T(x)$  es siempre divisible por  $G(x)$



# Códigos para tratamiento de errores

- Códigos polinómicos o de redundancia cíclica
  - Uso de la técnica
    - Receptor:
      - Recibe el mensaje  $T'(x)$  del emisor
      - Divide  $T'(x)$  entre  $G(x)$
      - Si el resto es cero, el mensaje ha llegado correctamente ( $T'(x) = T(x)$ )
      - Si el resto no es cero, el mensaje ha llegado con error y hay que pedir una retransmisión ( $T'(x) \neq T(x)$ )



# Códigos para tratamiento de errores

- Códigos polinómicos o de redundancia cíclica
  - **Ejemplo:** Se requiere transmitir 10011011. Polinomio generador  $G(x) = x^3 + 1$ 
    - Mensaje: 10011011
    - Polinomio generador: 1001 ( $r=3$ )
    - Se añaden 3 bits 0 al final del mensaje: 10011011000
    - Se divide  $x^3 \cdot M(x)$  entre  $G(x)$ :

1 0 0 1 1 0 1 1 0 0 0

1 0 0 1

0 0 0 0 1 0 1 1  
1 0 0 1

0 0 1 0 0 0

1 0 0 1

0 0 0 1 0

1 0 0 1

1 0 0 0 1 0 1 0

- Se transmite 10011011010 ( $4DA_{16}$ )



# Códigos para tratamiento de errores

- Códigos polinómicos o de redundancia cíclica

- El polinomio generador

- La selección del polinomio generador es esencial si queremos detectar la mayoría de los errores que ocurran
    - Se puede demostrar (no objeto de este curso) que los polinomios generadores son más potentes con el primer y último bits a 1
    - Ejemplos de polinomios generadores (estándares internacionales):

- CRC-12:  $x^{12} + x^{11} + x^3 + x^2 + x + 1$

- CRC-16:  $x^{16} + x^{15} + x^2 + 1$

- CRC-CCITT:  $x^{16} + x^{12} + x^5 + 1$

- » 100% errores simples

- » 100% errores dobles

- » 100% errores en un número impar de bits

- » 100% errores en ráfagas de igual a o menos de 16 bits

- » 99.997% errores de ráfagas de 17 bits

- » 99.998% de errores en ráfagas de 18 o más bits



# Códigos para tratamiento de errores

- Códigos polinómicos o de redundancia cíclica
  - **Ejercicio:** Utilizando el polinomio generador  $G = x^3 + 1$ , determinar los valores hexadecimales que se transmitirán para mandar el mensaje binario 10110110

(Solución:  $5B2_{16}$ )

