

# Fundamentos matemáticos

## CURSO CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

Ana I. González-Tablas Ferreres

José María de Fuentes García-Romero de Tejada

Lorena González Manzano

Pablo Martín González

**uc3m** | Universidad **Carlos III** de Madrid

COSEC



# ÍNDICE

- 1. FUNDAMENTOS MATEMÁTICOS
  - **Conceptos básicos**
    - Congruencias
    - Reducción módulo  $n$
    - Conjunto  $\mathbb{Z}_n$
  - Cálculo de inversos
    - Teorema de Fermat
    - Indicador de Euler y conjunto  $\mathbb{Z}_n^*$
    - Teorema de Euler
    - Cálculo de inversos mediante Euclides Modificado
  - Resolución de ecuaciones congruenciales
  - Exponenciación y logaritmo discreto
    - Restos potenciales y gaussiano
    - Raíces primitivas o generador
    - Logaritmos discretos
  - Cuerpos de Galois

# FUNDAMENTOS MATEMÁTICOS

- Conceptos básicos

- Sea  $\mathbf{Z}$  conjunto de números enteros, con  $a, b, c \in \mathbf{Z}$

- $\mathbf{Z}$  forma estructura de Grupo  $(\mathbf{Z}, +)$  si:

$$a + b \in \mathbf{Z}$$

cierre

$$a + (b + c) = (a + b) + c$$

asociativa

$$a + 0 = a$$

identidad

$$a + (-a) = 0$$

inverso

# FUNDAMENTOS MATEMÁTICOS

- $\mathbf{Z}$  forma estructura de Grupo Conmutativo o Abeliانو si:

$$a + b = b + a$$

conmutativa

- $\mathbf{Z}$  forma estructura de Anillo  $(\mathbf{Z}, +, \cdot)$  si  $\mathbf{Z}$  es Grupo Abeliانو y:

$$a \cdot b \in \mathbf{Z}$$

cierre

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

asociativa

$$a \cdot 1 = a$$

identidad

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

$\cdot$  es distributiva respecto  $+$

$(\mathbf{Z}, \cdot)$  es  
semigrupo

# FUNDAMENTOS MATEMÁTICOS

- $\mathbb{Z}$  forma estructura de Anillo Conmutativo si  $\mathbb{Z}$  Anillo y:

$$a \cdot b = b \cdot a$$

conmutativa

- Anillo de División:

$$a \cdot a^{-1} = 1$$

inverso ( $\cdot$ )

- **Cuerpo:** Anillo de División Conmutativo

# ÍNDICE

- 1. FUNDAMENTOS MATEMÁTICOS
  - Conceptos básicos
    - **Congruencias**
      - Reducción módulo  $n$
      - Conjunto  $\mathbb{Z}_n$
  - Cálculo de inversos
    - Teorema de Fermat
    - Indicador de Euler y conjunto  $\mathbb{Z}_n^*$
    - Teorema de Euler
    - Cálculo de inversos mediante Euclides Modificado
  - Resolución de ecuaciones congruenciales
  - Exponenciación y logaritmo discreto
    - Restos potenciales y gaussiano
    - Raíces primitivas o generador
    - Logaritmos discretos
  - Cuerpos de Galois

# FUNDAMENTOS MATEMÁTICOS

- **Congruencias**

1. Sean  $a, b, n \in \mathbf{Z}$  con  $n \neq 0$

2.  $a$  y  $b$  son congruentes módulo  $n$  ( $a \equiv b \pmod{n}$ ) si

$$a \equiv b \pmod{n} \quad \Leftrightarrow \quad a - b = k \cdot n \text{ para algún entero } k$$

3. Al número  $b$  se le denomina “resto de  $a$  módulo  $n$ ” y recíprocamente,  $a$  es el “resto de  $b$  módulo  $n$ ”

*“ $a$  y  $b$  son congruentes módulo  $n$  si ambos dejan el mismo resto si los dividimos por  $n$ , o, equivalentemente, si  $a - b$  es un múltiplo de  $n$ ”*

$$a = 23, b = 3, n_1 = 10, n_2 = 11$$

$$a \equiv b \pmod{n_1} \quad \text{pero } a \not\equiv b \pmod{n_2}$$

$$23 - 3 = 20 = 2 \cdot 10 \quad \text{pero } \nexists k \in \mathbf{Z} \mid 20 = k \cdot 11$$

# FUNDAMENTOS MATEMÁTICOS

- **Congruencias**

4. Denotaremos con  $[a]$  el conjunto  $\{..., a-2n, a-n, a, a+n, a+2n, ...\}$ , que es la clase de congruencias de  $a$  módulo  $n$  (e.d., para todo  $x, y \in [a]$  respecto de  $n$ ,  $x \equiv y \pmod{n}$  y  $a \in \{0, 1, \dots, n-1\}$ )

La clase de congruencia  $[3]$  módulo 10 =

$$\begin{aligned} [3]_{10} &= \{ ..., -27, -17, -7, 3, 13, 23, 33, ... \} = \\ &\{ ..., 3 - 3 \cdot 10, 3 - 2 \cdot 10, 3 - 1 \cdot 10, 3 - 0 \cdot 10, 3 + 1 \cdot 10, 3 + 2 \cdot 10, 3 + 3 \cdot 10, ... \} \\ -27 &\equiv -17 \equiv -7 \equiv 3 \equiv 13 \equiv 23 \equiv 33 \pmod{10} \end{aligned}$$

La clase de congruencia  $[7]$  módulo 11 =

$$\begin{aligned} [7]_{11} &= \{ ..., -26, -15, -4, 7, 18, 29, 40, ... \} = \\ &\{ ..., 7 - 3 \cdot 11, 7 - 2 \cdot 11, 7 - 1 \cdot 11, 7 - 0 \cdot 11, 7 + 1 \cdot 11, 7 + 2 \cdot 11, 7 + 3 \cdot 11, ... \} \\ -26 &\equiv -15 \equiv -4 \equiv 7 \equiv 18 \equiv 29 \equiv 40 \pmod{11} \end{aligned}$$

# ÍNDICE

- 1. FUNDAMENTOS MATEMÁTICOS
  - Conceptos básicos
    - Congruencias
    - **Reducción módulo  $n$**
    - Conjunto  $\mathbb{Z}_n$
  - Cálculo de inversos
    - Teorema de Fermat
    - Indicador de Euler y conjunto  $\mathbb{Z}_n^*$
    - Teorema de Euler
    - Cálculo de inversos mediante Euclides Modificado
  - Resolución de ecuaciones congruenciales
  - Exponenciación y logaritmo discreto
    - Restos potenciales y gaussiano
    - Raíces primitivas o generador
    - Logaritmos discretos
  - Cuerpos de Galois

# FUNDAMENTOS MATEMÁTICOS

- **Reducción módulo  $n$**

Sean  $a, n \in \mathbf{Z}$  ( $n \neq 0$ ). Se llama reducción módulo  $n$  (o módulo  $n$ ) a la función (representada por (mód.  $n$ )) que aplicada a  $a$ , obtiene un  $r \in \mathbf{Z}^+ + \{0\} / r \in \{0, 1, \dots, n-1\}$  y  $a \equiv r \text{ (mód. } n)$

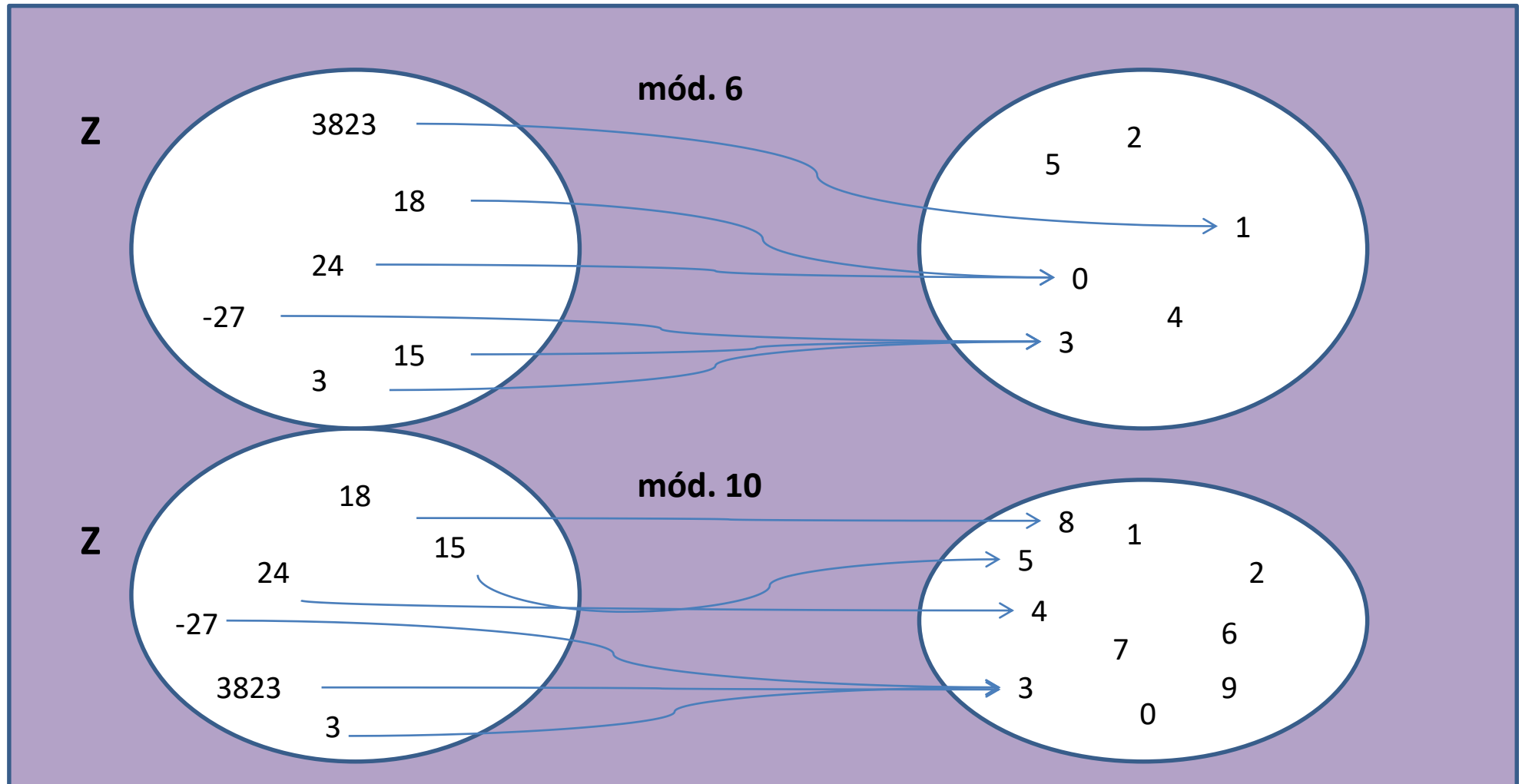
$$a \text{ (mód. } n) = r \Rightarrow a \equiv r \text{ (mód. } n) \text{ y } r \in \{0, 1, \dots, n-1\}$$

Nota: “ $r$  es el resto de la división entera de  $a$  entre  $n$  (para  $a > 0$ )”

$$\begin{array}{llll} 26 \text{ (mód. } 5) = 5 \cdot 5 + 1 \text{ (mód. } 5) = 1 & (1 < 5-1) & \text{p.t.} & 26 \equiv 1 \text{ (mód. } 5) \\ 30 \text{ (mód. } 7) = 4 \cdot 7 + 2 \text{ (mód. } 7) = 2 & (2 < 7-1) & \text{p.t.} & 30 \equiv 2 \text{ (mód. } 7) \\ 11 \text{ (mód. } 33) = 11 & (11 < 33-1) & & \\ 256 \text{ (mód. } 8) = 32 \cdot 8 + 0 \text{ (mód. } 8) = 0 & (0 < 8-1) & \text{p.t.} & 256 \equiv 0 \text{ (mód. } 8) \\ -17 \text{ (mód. } 12) \equiv -17 + 2 \cdot 12 = 7 & (7 < 12-1) & \text{p.t.} & -17 \equiv 7 \text{ (mód. } 12) \end{array}$$

# FUNDAMENTOS MATEMÁTICOS

- Reducción módulo  $n$



# ÍNDICE

- 1. FUNDAMENTOS MATEMÁTICOS
  - Conceptos básicos
    - Congruencias
    - Reducción módulo  $n$
    - **Conjunto  $\mathbb{Z}_n$**
  - Cálculo de inversos
    - Teorema de Fermat
    - Indicador de Euler y conjunto  $\mathbb{Z}_n^*$
    - Teorema de Euler
    - Cálculo de inversos mediante Euclides Modificado
  - Resolución de ecuaciones congruenciales
  - Exponenciación y logaritmo discreto
    - Restos potenciales y gaussiano
    - Raíces primitivas o generador
    - Logaritmos discretos
  - Cuerpos de Galois

# FUNDAMENTOS MATEMÁTICOS

- Conjunto  $Z_n$
- $Z_n = \{ [a] / a \in \mathbb{Z} \}$

$Z_n$  es el conjunto de clases de congruencia respecto a un módulo  $n$

Si  $n \neq 0$ ,  $Z_n = \{ [0], [1], \dots, [n-1] \}$  o simplificando

$Z_n = \{ 0, 1, \dots, n-1 \}$  (“**anillo de enteros módulo  $n$** ”)

$$Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$$

$$Z_{31} = \{0, 1, 2, 3, 4, 5, 6, 7, \dots, 26, 27, 28, 29, 30\}$$

# FUNDAMENTOS MATEMÁTICOS

## — Conjunto $\mathbb{Z}_n$

### • Operaciones ( $+_n, \cdot_n$ )

— Se define la suma y la multiplicación para  $\mathbb{Z}_n$

Para  $[a], [b], [c] \in \mathbb{Z}_n$        $+_n : [a] +_n [b] = [a+b]$        $\cdot_n : [a] \cdot_n [b] = [a \cdot b]$

$\mathbb{Z}_8 :$

$$[6] +_8 [7] = (6 + 7) \text{ mód. } 8 = 13 \text{ mód. } 8 = [5]$$

$\mathbb{Z}_{31} :$

$$[3] \cdot_{31} [11] = (3 \cdot 11) \text{ mód. } 31 = 33 \text{ mód. } 31 = [2]$$

# FUNDAMENTOS MATEMÁTICOS

- Conjunto  $\mathbf{Z}_n$
- $\mathbf{Z}_n$  - propiedades respecto  $(+_n, \cdot_n)$

Para  $n \neq 0$ ,  $\mathbf{Z}_n$  es un anillo conmutativo respecto  $(+_n, \cdot_n)$

$$[a] +_n [b] \in \mathbf{Z}_n$$

$$[a] \cdot_n [b] \in \mathbf{Z}_n$$

$$[a] +_n ([b] +_n [c]) = ([a] +_n [b]) +_n [c]$$

$$[a] \cdot_n ([b] \cdot_n [c]) = ([a] \cdot_n [b]) \cdot_n [c]$$

$$[a] +_n 0 = [a]$$

$$[a] \cdot_n 1 = [a]$$

$$[a] +_n (-[a]) = 0$$

$$[a] \cdot_n ([b] +_n [c]) = ([a] \cdot_n [b]) +_n ([a] \cdot_n [c])$$

$$[a] +_n [b] = [b] +_n [a]$$

$$[a] \cdot_n [b] = [b] \cdot_n [a]$$

# FUNDAMENTOS MATEMÁTICOS

## ► Conjunto $\mathbb{Z}_n$

### ► Relación de homomorfismo con el anillo de los enteros $\mathbb{Z}$

- La función de “reducción módulo  $n$  (mód.  $n$ )” es un homomorfismo entre  $\mathbb{Z}$  (el anillo de los enteros) y  $\mathbb{Z}_n$  (el anillo de los enteros módulo  $n$ )  $\leftrightarrow$  Se cumple que:

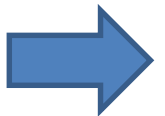
Dados  $a, b \in \mathbb{Z}$ ,  $f(a), f(b) \in \mathbb{Z}_n$ , con  $f: \mathbb{Z} \rightarrow \mathbb{Z}_n$  ( $f$  = reducción módulo  $n$ )

$$f(a + b) = f(a) +_n f(b) \quad ; \quad f(a \cdot b) = f(a) \cdot_n f(b)$$

### ► “Consecuencias” (Principios fundamentales de la Aritmética Modular):

- $(a + b) \text{ (mód. } n) = a \text{ (mód. } n) +_n b \text{ (mód. } n) = (a \text{ (mód. } n) + b \text{ (mód. } n)) \text{ (mód. } n)$   
 $[ (a + b) ] = [a] +_n [b] = [ [a] + [b] ]$
- $(a \cdot b) \text{ (mód. } n) = a \text{ (mód. } n) \cdot_n b \text{ (mód. } n) = (a \text{ (mód. } n) \cdot b \text{ (mód. } n)) \text{ (mód. } n)$   
 $[ (a \cdot b) ] = [a] \cdot_n [b] = [ [a] \cdot [b] ]$
- $(a \cdot (b+c)) \text{ (mód. } n) = ((a \text{ (mód. } n) \cdot_n b \text{ (mód. } n)) +_n (a \text{ (mód. } n) \cdot_n c \text{ (mód. } n))) \text{ (mód. } n)$   
 $= ((a \cdot b) \text{ (mód. } n) + (a \cdot c) \text{ (mód. } n)) \text{ (mód. } n)$   
 $[ (a \cdot (b + c)) ] = [a] \cdot_n ([b] +_n [c]) = [ [a] \cdot ([b] + [c]) ]$

ejemplos



# FUNDAMENTOS MATEMÁTICOS

$$(a + b)(\text{mód. } n) = a (\text{mód. } n) +_n b (\text{mód. } n) = (a(\text{mód. } n) + b(\text{mód. } n))(\text{mód. } n)$$

$$[ (a + b) ] = [a] +_n [b] = [ [a] + [b] ]$$

Ejemplo:

$$\begin{aligned}(3 + 8) (\text{mód. } 5) &= 3 (\text{mód. } 5) +_n 8 (\text{mód. } 5) = \\ &= (3 (\text{mód. } 5) + 8 (\text{mód. } 5)) \text{mód. } 5 = \\ &= (3 + 3) \text{mód. } 5 = 6 \text{mód. } 5 = \mathbf{1}\end{aligned}$$

$$(3 + 8) (\text{mód. } 5) = 11 (\text{mód. } 5) = 1$$

# FUNDAMENTOS MATEMÁTICOS

$$(a \cdot b)(\text{mód. } n) = a(\text{mód. } n) \cdot_n b(\text{mód. } n) = (a(\text{mód. } n) \cdot b(\text{mód. } n))(\text{mód. } n)$$

$$[ (a \cdot b) ] = [a] \cdot_n [b] = [ [a] \cdot [b] ]$$

Ejemplo:

$$\begin{aligned}(3 \cdot 8)(\text{mód. } 5) &= 3(\text{mód. } 5) \cdot_n 8(\text{mód. } 5) = (3(\text{mód. } 5) \cdot 8(\text{mód. } 5)) \text{mód. } 5 = \\ &= (3 \cdot 3) \text{mód. } 5 = 9 \text{mód. } 5 = \mathbf{4}\end{aligned}$$

$$(3 \cdot 8)(\text{mód. } 5) = 24(\text{mód. } 5) = 4$$

$$\begin{aligned}7^4(\text{mód. } 5) &= (7 \cdot 7 \cdot 7 \cdot 7)(\text{mód. } 5) = \\ &= (7(\text{mód. } 5) \cdot 7(\text{mód. } 5) \cdot 7(\text{mód. } 5) \cdot 7(\text{mód. } 5)) \text{mód. } 5 \Rightarrow \\ &= (2 \cdot 2 \cdot 2 \cdot 2) \text{mód. } 5 = 2^4(\text{mód. } 5) = 16 \text{mód. } 5 = \mathbf{1}\end{aligned}$$

$$7^4(\text{mód. } 5) = 2401(\text{mód. } 5) = 1$$

# FUNDAMENTOS MATEMÁTICOS

$$(a \cdot (b+c))(\text{mód. } n) = ((a(\text{mód. } n) \cdot_n b(\text{mód. } n)) +_n (a(\text{mód. } n) \cdot_n c(\text{mód. } n))) = \\ = ((a \cdot b)(\text{mód. } n) + (a \cdot c)(\text{mód. } n))(\text{mód. } n)$$

$$[ (a \cdot (b + c)) ] = [a] \cdot_n ( [b] +_n [c] ) = [ [a] \cdot ( [b] + [c] ) ]$$

Ejemplo:

$$(3 \cdot (8+4))(\text{mód. } 5) = ((3(\text{mód. } 5) \cdot_n 8(\text{mód. } 5)) +_n (3(\text{mód. } 5) \cdot_n 4(\text{mód. } 5))) = \\ = ((3 \cdot 8)(\text{mód. } 5) + (3 \cdot 4)(\text{mód. } 5))(\text{mód. } 5) = \\ = ((3 \cdot 3)(\text{mód. } 5) + (3 \cdot 4)(\text{mód. } 5))(\text{mód. } 5) = \\ = (9 (\text{mód. } 5) + 12 (\text{mód. } 5)) (\text{mód. } 5) = (4 + 2) (\text{mód. } 5) = \\ = 6 \text{ mód. } 5 = \mathbf{1}$$

$$(3 \cdot (8+4))(\text{mód. } 5) = 36 (\text{mód. } 5) = 1$$

# FUNDAMENTOS MATEMÁTICOS

Otros ejemplos:

$$(23 + 4)(\text{mód. } 5) = 2$$

$$2^9 (\text{mód. } 5) = 2$$

$$(3 + 8) \cdot 5 (\text{mód. } 5) = 0$$

$$(41 + 1001) \cdot 999 (\text{mód. } 5) = 3$$

# ÍNDICE

- 1. FUNDAMENTOS MATEMÁTICOS
  - Conceptos básicos
    - Congruencias
    - Reducción módulo  $n$
    - Conjunto  $\mathbb{Z}_n$
  - **Cálculo de inversos**
    - Teorema de Fermat
    - Indicador de Euler y conjunto  $\mathbb{Z}_n^*$
    - Teorema de Euler
    - Cálculo de inversos mediante Euclides Modificado
  - Resolución de ecuaciones congruenciales
  - Exponenciación y logaritmo discreto
    - Restos potenciales y gaussiano
    - Raíces primitivas o generador
    - Logaritmos discretos
  - Cuerpos de Galois

# FUNDAMENTOS MATEMÁTICOS

- **Cálculo de Inversos**

- Si  $a \in \mathbb{Z}_n$  / **m.c.d.  $(a, n) = 1$  (coprimos)**, existe un único  $x \in \mathbb{Z}_n - \{0\}$  /

$$a \cdot x = 1 \quad (\text{mód. } n)$$

- Este valor se representa por:

$$x = a^{-1} \quad (\text{mód. } n)$$

# FUNDAMENTOS MATEMÁTICOS

- Cálculo de Inversos

$\mathbb{Z}_8$

| w | -w | w <sup>-1</sup> |
|---|----|-----------------|
| 0 | 0  | ---             |
| 1 | 7  | 1               |
| 2 | 6  | ---             |
| 3 | 5  | 3               |
| 4 | 4  | ---             |
| 5 | 3  | 5               |
| 6 | 2  | ---             |
| 7 | 1  | 7               |

$\mathbb{Z}_7$

| w | -w | w <sup>-1</sup> |
|---|----|-----------------|
| 0 | 0  | ---             |
| 1 | 6  | 1               |
| 2 | 5  | 4               |
| 3 | 4  | 5               |
| 4 | 3  | 2               |
| 5 | 2  | 3               |
| 6 | 1  | 6               |

# ÍNDICE

- 1. FUNDAMENTOS MATEMÁTICOS
  - Conceptos básicos
    - Congruencias
    - Reducción módulo  $n$
    - Conjunto  $\mathbb{Z}_n$
  - Cálculo de inversos
    - **Teorema de Fermat**
    - Indicador de Euler y conjunto  $\mathbb{Z}_n^*$
    - Teorema de Euler
    - Cálculo de inversos mediante Euclides Modificado
  - Resolución de ecuaciones congruenciales
  - Exponenciación y logaritmo discreto
    - Restos potenciales y gaussiano
    - Raíces primitivas o generador
    - Logaritmos discretos
  - Cuerpos de Galois

# FUNDAMENTOS MATEMÁTICOS

- **Teorema de Fermat**

Si  $p$  es primo,  $\forall a \in \mathbf{Z}$ , m.c.d.  $(a, p) = 1$ , se cumple:

coprimos

$$a^{p-1} \pmod{p} = 1$$

De lo que se deduce:

$$a \cdot a^{p-2} \pmod{p} = 1 \rightarrow a^{-1} = a^{p-2} \pmod{p}$$

# FUNDAMENTOS MATEMÁTICOS

- Resolver:  $2x \bmod 7 = 1$

**Solución:**

$a=2$ ,  $p=7$  primo,  $\text{m.c.d.}(2,7)=1$ , aplicando Fermat:

$$x = 2^{p-2} \bmod 7 \Rightarrow x = 2^{7-2} \bmod 7 \Rightarrow x = 2^5 \bmod 7 \Rightarrow$$

$$x = 2^3 2^2 \bmod 7 \Rightarrow x = 4 \bmod 7$$

- (Ejer. 1) Resolver:  $35x \bmod 3 = 1$

**Solución**

$a=35$ ,  $p=3$  primo,  $\text{m.c.d.}(35,3)=1$ ,

$$35x \bmod 3 = (35 \bmod 3)(x \bmod 3) \bmod 3 = 2x \bmod 3 = 1$$

$$\text{Aplicando Fermat: } x = 2^{p-2} \bmod 3 \Rightarrow x = 2^{3-2} \bmod 3 \Rightarrow x = 2 \bmod 3$$

# ÍNDICE

- 1. FUNDAMENTOS MATEMÁTICOS
  - Conceptos básicos
    - Congruencias
    - Reducción módulo  $n$
    - Conjunto  $\mathbb{Z}_n$
  - Cálculo de inversos
    - Teorema de Fermat
    - **Indicador de Euler y conjunto  $\mathbb{Z}_n^*$**
    - Teorema de Euler
    - Cálculo de inversos mediante Euclides Modificado
  - Resolución de ecuaciones congruenciales
  - Exponenciación y logaritmo discreto
    - Restos potenciales y gaussiano
    - Raíces primitivas o generador
    - Logaritmos discretos
  - Cuerpos de Galois

# FUNDAMENTOS MATEMÁTICOS

- **Conjunto reducido de restos  $Z_n^*$** 
  - Es el conjunto de números de  $Z_n$  que son coprimos con  $n$  (conjunto de enteros positivos,  $a$ , tales que  $0 < a < n$  y  $\text{m.c.d.}(a, n) = 1$ )
  - Todos los elementos de  $Z_n^*$  tienen inverso multiplicativo
- **Indicador de Euler:  $\Phi(n)$** 

Al número de elementos de  $Z_n^*$  se le llama indicador de Euler de  $n$  (y se representa por  $\Phi(n)$ )

# FUNDAMENTOS MATEMÁTICOS

- Conjunto reducido de restos  $\mathbb{Z}_n^*$

$\mathbb{Z}_8$

| w | -w | $w^{-1}$ |
|---|----|----------|
| 0 | 0  | ---      |
| 1 | 7  | 1        |
| 2 | 6  | ---      |
| 3 | 5  | 3        |
| 4 | 4  | ---      |
| 5 | 3  | 5        |
| 6 | 2  | ---      |
| 7 | 1  | 7        |

$$\mathbb{Z}_8^* = \{1, 3, 5, 7\}$$

$$\Phi(8) = 4$$

$\mathbb{Z}_7$

| w | -w | $w^{-1}$ |
|---|----|----------|
| 0 | 0  | ---      |
| 1 | 6  | 1        |
| 2 | 5  | 4        |
| 3 | 4  | 5        |
| 4 | 3  | 2        |
| 5 | 2  | 3        |
| 6 | 1  | 6        |

$$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$$

$$\Phi(7) = 6$$

# FUNDAMENTOS MATEMÁTICOS

- **Cálculo del indicador de Euler:  $\Phi(n)$**

- Si  $n$  es un número primo,  $p$ :

$$\Phi(p) = p-1$$

- $\Phi(13) = 13-1 = 12$

- Si  $p$  es primo y  $k \in \mathbf{Z}^+$ :

$$\Phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$$

- $\Phi(9) = \Phi(3^2) = 3^{2-1} \cdot (3-1) = 3 \cdot 2 = 6$

# FUNDAMENTOS MATEMÁTICOS

- **Cálculo del indicador de Euler:  $\Phi(n)$**

- Si  $p$  y  $q$  son primos entre sí:

$$\Phi(p \cdot q) = \Phi(p) \cdot \Phi(q)$$

- $\Phi(10) = \Phi(5 \cdot 2) = \Phi(5) \cdot \Phi(2) = 4 \cdot 1 = 4$

- Si  $n = \prod p_i^{k_i} / \forall i \ p_i$  es primo,  $k_i \in \mathbf{Z}^+$ :

$$\Phi(n) = \prod p_i^{k_i-1} (p_i - 1)$$

- $\Phi(28) = \Phi(7 \cdot 4) = (7^0 \cdot 6) \cdot (2^1 \cdot 1) = 12$

# ÍNDICE

- 1. FUNDAMENTOS MATEMÁTICOS
  - Conceptos básicos
    - Congruencias
    - Reducción módulo  $n$
    - Conjunto  $\mathbb{Z}_n$
  - Cálculo de inversos
    - Teorema de Fermat
    - Indicador de Euler y conjunto  $\mathbb{Z}_n^*$
    - **Teorema de Euler**
    - Cálculo de inversos mediante Euclides Modificado
  - Resolución de ecuaciones congruenciales
  - Exponenciación y logaritmo discreto
    - Restos potenciales y gaussiano
    - Raíces primitivas o generador
    - Logaritmos discretos
  - Cuerpos de Galois

# FUNDAMENTOS MATEMÁTICOS

- Teorema de Euler

$\forall a, n \in \mathbf{Z} (n \neq 0) / \text{m.c.d.}(a, n) = 1:$  ← coprimos

$$a^{\Phi(n)} \pmod{n} = 1$$

de lo que se deduce:

$$a \cdot a^{\Phi(n)-1} \pmod{n} = 1$$

y por tanto

$$a^{-1} = a^{\Phi(n)-1} \pmod{n}$$

- Por lo ya visto, si  $n$  es primo (representado por  $p$ ) resulta:

$$a^{-1} = a^{p-2} \pmod{p}$$

← ¡Fermat!

# FUNDAMENTOS MATEMÁTICOS

- Ejemplos de cálculo de inversos con Euler:
  - Resolver  $3x \bmod 10 = 1$   
 $a=3; n=10; \Phi(10)=4;$   
 $x = 3^{4-1} \bmod 10 = 3^3 \bmod 10 = 3 \cdot 3^2 \bmod 10$   
 $= 3 \cdot (-1) \bmod 10 = -3 \bmod 10 = 7$
  - Resolver  $2x \bmod 11 = 1$   
 $a=2; n=11; \Phi(11)=10;$   
 $x = 2^{10-1} \bmod 11 = (2^3)^3 \bmod 11 = (-3)^3 \bmod 11 =$   
 $= (-2) \cdot (-3) \bmod 11 = 6$

# FUNDAMENTOS MATEMÁTICOS

- (Ejer. 2) Resuelva:  $17x \bmod 12 = 1$

## Solución

$$a=17, n=12, \text{m.c.d.}(17,12)=1, 5x \bmod 12 = 1$$

$$\text{Aplicando Euler: } x = 5^{\Phi(12)-1} \bmod 12$$

$$12 = 2^2 \cdot 3, \Phi(12) = \Phi(2^2) \cdot \Phi(3) = 2^{2-1} \cdot (2-1) \cdot 2 = 4$$

$$x = 5^{4-1} \bmod 12 \Leftrightarrow x = 5^3 \bmod 12 \Leftrightarrow x = 13 \cdot 5 \bmod 12$$

$$\Leftrightarrow x = 5$$

# FUNDAMENTOS MATEMÁTICOS

- (Ejer. 7) Resuelva:  $37x \bmod 10 = 1$

## Solución

$$a=37, n=10, \text{m.c.d.}(37,10)=1, 7x \bmod 10 = 1$$

$$\text{Aplicando Euler: } x = 7^{\Phi(10)-1} \bmod 10$$

$$10 = 2 \cdot 5, \Phi(10) = \Phi(2) \cdot \Phi(5) = 1 \cdot 4 = 4$$

$$x = 7^{4-1} \bmod 10 \Leftrightarrow x = 7^3 \bmod 10 \Leftrightarrow x = (-1) \cdot 7 \bmod 10 \Leftrightarrow$$

$$x = -7 \bmod 10 \Leftrightarrow x = 3 \bmod 10 = 3$$

# FUNDAMENTOS MATEMÁTICOS

- Resuelva:  $37x \bmod 41 = 1$

## Solución

$a=37$ ,  $n=41$ ,  $\text{m.c.d.}(37,41)=1$ ,

Aplicando Euler:  $x = 37^{\Phi(41) - 1} \bmod 41$

...

...

...

...

...

...

...

# ÍNDICE

- 1. FUNDAMENTOS MATEMÁTICOS
  - Conceptos básicos
    - Congruencias
    - Reducción módulo  $n$
    - Conjunto  $\mathbb{Z}_n$
  - Cálculo de inversos
    - Teorema de Fermat
    - Indicador de Euler y conjunto  $\mathbb{Z}_n^*$
    - Teorema de Euler
    - **Cálculo de inversos mediante Euclides Modificado**
  - Resolución de ecuaciones congruenciales
  - Exponenciación y logaritmo discreto
    - Restos potenciales y gaussiano
    - Raíces primitivas o generador
    - Logaritmos discretos
  - Cuerpos de Galois

# FUNDAMENTOS MATEMÁTICOS

- **Algoritmo de Euclides**

- Permite hallar el m.c.d. de dos números enteros positivos
- No requiere la factorización de los números
- El algoritmo ligeramente modificado (Euclides extendido) permite calcular el inverso de un número respecto al otro (el módulo) cuando el m.c.d. de ambos es 1 (coprimos)

# FUNDAMENTOS MATEMÁTICOS

- Ejemplo de cálculo de m.c.d. con Euclides
- Calcule el m.c.d. entre 1547 y 560

|           |      |     |     |     |    |    |   |
|-----------|------|-----|-----|-----|----|----|---|
| cocientes |      | 2   | 1   | 3   | 4  | 1  | 3 |
|           | 1547 | 560 | 427 | 133 | 28 | 21 | 7 |
| restos    | 427  | 133 | 28  | 21  | 7  | 0  |   |

# FUNDAMENTOS MATEMÁTICOS

- $1547 = 2 \cdot 560 + 427$
- $560 = 1 \cdot 427 + 133$
- $427 = 3 \cdot 133 + 28$
- $133 = 4 \cdot 28 + 21$
- $28 = 1 \cdot 21 + 7$
- $21 = 3 \cdot 7 + 0$
- **$\text{m.c.d.}(1547, 560) = 7$**

# FUNDAMENTOS MATEMÁTICOS

- Cálculo del inverso con Euclides Modificado

|       |       |       |       |     |          |           |           |
|-------|-------|-------|-------|-----|----------|-----------|-----------|
|       | $c_1$ | $c_2$ | ...   | ... | ...      | $c_n$     | $c_{n+1}$ |
| $n$   | $a$   | $r_1$ | $r_2$ | ... | ...      | $r_{n-1}$ | <b>1</b>  |
| $r_1$ | $r_2$ | $r_3$ | ...   | ... | <b>1</b> | <b>0</b>  |           |

$$n = c_1 \cdot a + r_1$$

$$a = c_2 \cdot r_1 + r_2$$

$$r_1 = c_3 \cdot r_2 + r_3$$

...

$$r_{n-2} = c_n \cdot r_{n-1} + 1$$

$$r_{n-1} = c_{n+1} \cdot 1 + 0$$

# FUNDAMENTOS MATEMÁTICOS

- **Cálculo del inverso con Euclides Modificado**

Despejamos los restos:

$$n - c_1 \cdot a = r_1$$

$$a - c_2 \cdot r_1 = r_2$$

$$r_1 - c_3 \cdot r_2 = r_3$$

...

$$r_{n-2} - c_n \cdot r_{n-1} = 1$$

$$r_{n-1} - c_{n+1} \cdot 1 = 0$$

# FUNDAMENTOS MATEMÁTICOS

- **Cálculo del inverso con Euclides Modificado**

Partimos de la expresión:  $1 = r_{n-2} - c_n \cdot r_{n-1}$

Sustituimos los restos de la expresión usando las expresiones anteriores (sin operar con “a” ni “n”) hasta llegar a una expresión del tipo:

$$1 = k_1 \cdot a + k_2 \cdot n$$

Reduciendo módulo n queda:  $1 = k_1 \cdot a \pmod{n}$

Por lo que

$$a^{-1} \pmod{n} = k_1$$

# FUNDAMENTOS MATEMÁTICOS

- **Cálculo del inverso con Euclides Modificado**
- Resuelva  $37x \bmod 41 = 1$

|    |    |   |   |
|----|----|---|---|
|    | 1  | 9 | 4 |
| 41 | 37 | 4 | 1 |
| 4  | 1  | 0 |   |

$$n = c_1 \cdot a + r_1 \Rightarrow$$

$$41 = 1 \cdot 37 + 4$$

$$37 = 9 \cdot 4 + 1$$

$$1 = 37 - 9 \cdot 4 = 37 - 9(41 - 37)$$

$$1 = 37 - 9 \cdot 41 + 9 \cdot 37 = 37 \cdot 10 - 9 \cdot 41$$

$$1 = 37 \cdot 10 \bmod 41$$

$$\mathbf{x = 10 \bmod. 41}$$

# FUNDAMENTOS MATEMÁTICOS

- **Cálculo del inverso con Euclides Modificado**
- Resuelva  $23x \bmod 25 = 1$

|    |    |  |  |
|----|----|--|--|
|    |    |  |  |
| 25 | 23 |  |  |
|    |    |  |  |

$$\begin{aligned}n &= c_1 \cdot a + r_1 \Rightarrow \\25 &= ? \cdot 23 + ? \\23 &= ? \cdot ? + ?\end{aligned}$$

$$x = 12$$

# ÍNDICE

- 1. FUNDAMENTOS MATEMÁTICOS
  - Conceptos básicos
    - Congruencias
    - Reducción módulo  $n$
    - Conjunto  $\mathbb{Z}_n$
  - Cálculo de inversos
    - Teorema de Fermat
    - Indicador de Euler y conjunto  $\mathbb{Z}_n^*$
    - Teorema de Euler
    - Cálculo de inversos mediante Euclides Modificado
  - **Resolución de ecuaciones congruenciales**
  - Exponenciación y logaritmo discreto
    - Restos potenciales y gaussiano
    - Raíces primitivas o generador
    - Logaritmos discretos
  - Cuerpos de Galois

# FUNDAMENTOS MATEMÁTICOS

- Resolución de ecuaciones de congruencia lineales

$$a \cdot x \equiv b \text{ mód. } n$$

$\Rightarrow$

Existe un  $k$  entero tal que

$$a \cdot x + n \cdot k = b$$

Tres casos:

- Si  $\text{m.c.d.}(a, n) = 1$ , la ecuación tiene solución y es única
- Si  $\text{m.c.d.}(a, n) = m \neq 1$ , y  $m \mid b$ ,  $\exists m$  soluciones
  - $m \mid b \iff$  “ $m$ ” divide a “ $b$ ”  $\rightarrow \exists c$  tal que  $b = c \cdot m$
- Caso contrario, no existe solución a la ecuación

# FUNDAMENTOS MATEMÁTICOS

- **Resolución de ecuaciones de congruencia lineales**
- Si  $\text{m.c.d.}(a, n)=1$ , la ecuación tiene solución y es única

$$x = b \cdot y \pmod{n}$$

donde “y” se halla como:

$$a \cdot y = 1 \pmod{n} \quad \{\text{e.d., } y = a^{-1} \pmod{n}\}$$

- Si  $\text{m.c.d.}(a, n) = m \neq 1$ ,  $m \mid b$ ,  $\exists m$  soluciones

$$x = (b/m) \cdot y + j \cdot (n/m) \pmod{n} \quad j \in \{0, m-1\}$$

donde “y” se halla como:

$$(a/m) \cdot y \pmod{(n/m)} = 1 \quad \{\text{e.d., } y = (a/m)^{-1} \pmod{(n/m)}\}$$

# FUNDAMENTOS MATEMÁTICOS

- (Ejer. 4) Resuelva  $3x = 3 \pmod{14}$ 
  - Ecuación tipo  $a \cdot x = b \pmod{n} \rightarrow a=3, b=3, n=14$
  - $\text{m.c.d}(a, n) = \text{m.c.d}(3, 14) = 1 \rightarrow$  Existe solución y es única
  - $x = b \cdot a^{-1} \pmod{n} = 3 \cdot 3^{-1} \pmod{14}$
  - Hallemos  $3^{-1} \pmod{14}$ 
    - Aplicando Euler:  $3^{-1} \pmod{14} = 3^{\Phi(14)-1} \pmod{14}$
    - $\Phi(14) = \Phi(2 \cdot 7) = \Phi(2) \cdot \Phi(7) = (2-1) \cdot (7-1) = 6$
    - $3^{-1} \pmod{14} = 3^{\Phi(14)-1} \pmod{14} = 3^5 \pmod{14} = 243 \pmod{14} = 5$
  - $x = 3 \cdot 3^{-1} \pmod{14} = 3 \cdot 5 \pmod{14} = \mathbf{1}$

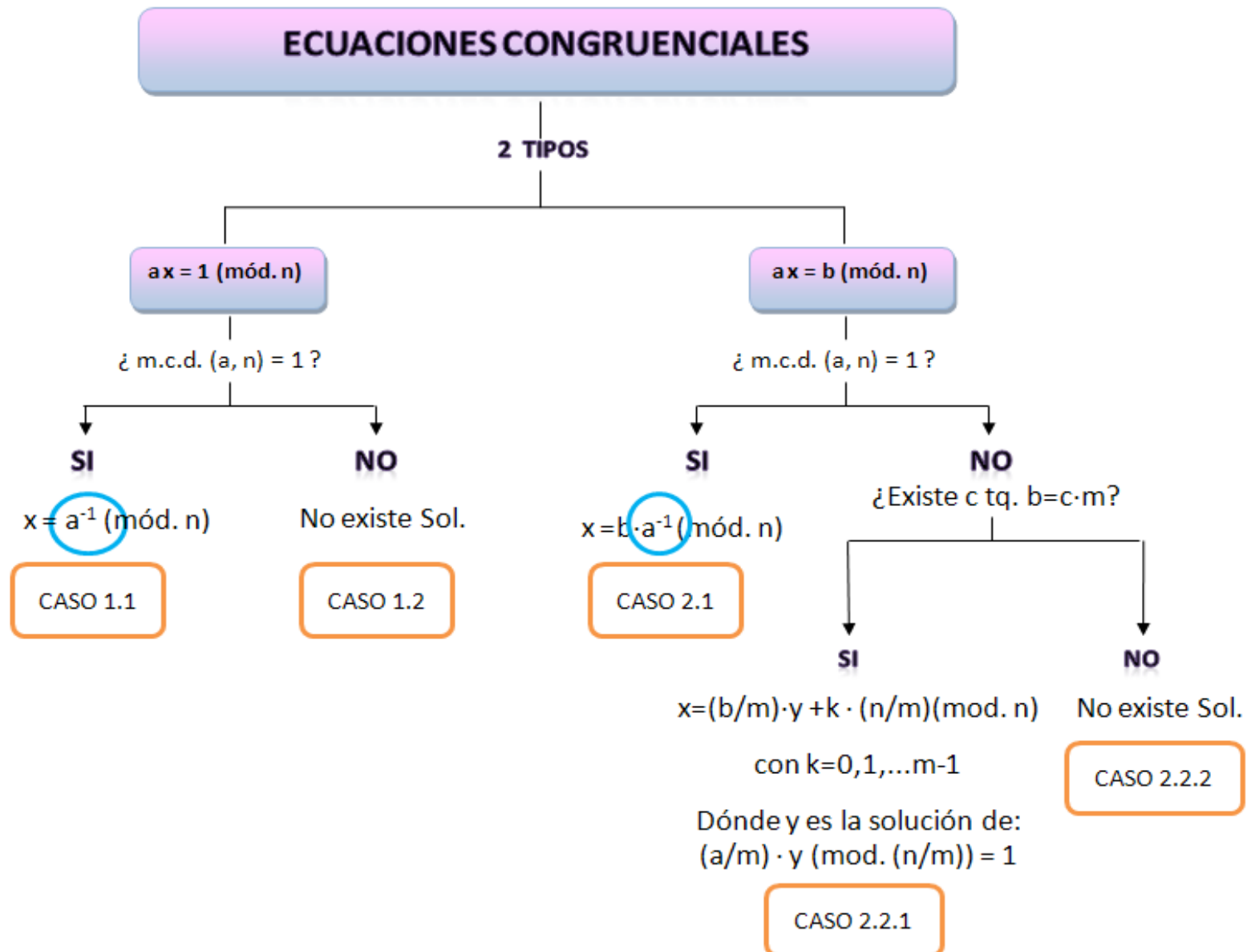
# FUNDAMENTOS MATEMÁTICOS

- (Ejer. 6) Resuelva  $15x = 6 \pmod{9}$ 
  - Ecuación tipo  $a \cdot x = b \pmod{n}$
  - Se puede reducir  $\rightarrow 6 \cdot x = 6 \pmod{9} \rightarrow a=6, b=6, n=9$
  - $m = \text{m.c.d.}(a, n) = \text{m.c.d.}(6, 9) = 3 \neq 1$ 
    - ¿ $\exists c \mid b=c \cdot m$ ? Sí:  $6=2 \cdot 3 \rightarrow c=2 \rightarrow$  Existen  $m=3$  soluciones
  - **$x = (b/m) \cdot y + j \cdot (n/m) \pmod{n} \quad j \in \{0, m-1\}$**
  - $x = (6/3) \cdot y + j \cdot (9/3) \pmod{9} = 2 \cdot y + j \cdot 3 \pmod{9}, \quad j \in \{0, 2\}$

# FUNDAMENTOS MATEMÁTICOS

- (Ejer. 6) Resuelva  $15 \cdot x = 6 \pmod{9}$  (cont.)
  - $y = (a/m)^{-1} \pmod{(n/m)} = (6/3)^{-1} \pmod{(9/3)} = 2^{-1} \pmod{3}$ 
    - Aplicando Fermat/Euler:  $2^{-1} \pmod{3} = 2^{\Phi(3)-1} \pmod{3}$
    - $\Phi(3) = (3-1) = 2$
    - $y = 2^{-1} \pmod{3} = 2^{\Phi(3)-1} \pmod{3} = 2^1 \pmod{3} = 2$
  - $x = 2 \cdot y + j \cdot 3 \pmod{9} = 2 \cdot 2 + j \cdot 3 \pmod{9} = 4 + 3 \cdot j \pmod{9}, j \in \{0,1,2\}$ 
    - $j=0 \rightarrow x_1 = \mathbf{4}$
    - $j=1 \rightarrow x_2 = 4 + 3 \pmod{9} = \mathbf{7}$
    - $j=2 \rightarrow x_3 = 4 + 6 \pmod{9} = \mathbf{1}$

# FUNDAMENTOS MATEMÁTICOS



# ÍNDICE

- 1. FUNDAMENTOS MATEMÁTICOS
  - Conceptos básicos
    - Congruencias
    - Reducción módulo  $n$
    - Conjunto  $\mathbb{Z}_n$
  - Cálculo de inversos
    - Teorema de Fermat
    - Indicador de Euler y conjunto  $\mathbb{Z}_n^*$
    - Teorema de Euler
    - Cálculo de inversos mediante Euclides Modificado
  - Resolución de ecuaciones congruenciales
  - Exponenciación y logaritmo discreto
    - **Restos potenciales y gaussiano**
    - Raíces primitivas o generador
    - Logaritmos discretos
  - Cuerpos de Galois

# FUNDAMENTOS MATEMÁTICOS

- **Restos potenciales**
- = Potencias de un entero módulo  $n$ 
  - Dado  $a \in \mathbf{Z}$ , se llaman restos potenciales de  $a$  respecto al módulo  $n$ , a los restos de las potencias sucesivas de  $a$  respecto de ese mismo módulo:
    - $a^0 \text{ mód. } n$
    - $a^1 \text{ mód. } n$
    - $a^2 \text{ mód. } n$
    - ...
    - $a^g \text{ mód. } n$
    - ...

# FUNDAMENTOS MATEMÁTICOS

- Restos potenciales

–  $n = 19$

| $a$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ | $a^6$ | $a^7$ | $a^8$ | $a^9$ | $a^{10}$ | $a^{11}$ | $a^{12}$ | $a^{13}$ | $a^{14}$ | $a^{15}$ | $a^{16}$ | $a^{17}$ | $a^{18}$ |
|-----|-------|-------|-------|-------|-------|-------|-------|-------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| 3   | 9     | 8     | 5     | 15    | 7     | 2     | 6     | 18    | 16       | 10       | 11       | 14       | 4        | 12       | 17       | 13       | 1        |
| 4   | 16    | 7     | 9     | 17    | 11    | 6     | 5     | 1     | 4        | 16       | 7        | 9        | 17       | 11       | 6        | 5        | 1        |
| 7   | 11    | 1     | 7     | 11    | 1     | 7     | 11    | 1     | 7        | 11       | 1        | 7        | 11       | 1        | 7        | 11       | 1        |
| 19  | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0        | 0        | 0        | 0        | 0        | 0        | 0        | 0        | 0        |

# FUNDAMENTOS MATEMÁTICOS

## ► Gaussiano $w$ (orden de $a$ respecto a $n$ )

- Si m.c.d.  $(a, n) = 1$ , por Euler:

Existe al menos un  $m$  tal que  $a^m = 1 \pmod{n}$

$$a^{\Phi(n)} = 1 \pmod{n} \rightarrow m = \Phi(n)$$

- Hemos visto que hay más exponentes que lo cumplen,
  - e.g.:  $m = k \cdot \Phi(n)$ , y, a veces, otros números menores que  $\Phi(n)$

# FUNDAMENTOS MATEMÁTICOS

## ► Gaussiano $w$ (orden de $a$ respecto a $n$ )

- El menor exponente  $w$  que cumple  $a^w = 1 \pmod{n}$  se denomina **gaussiano (orden) de  $a$  respecto del módulo  $n$**

Si  $a^w = 1 \pmod{n}$  y  $w$  es el menor de los exponentes que satisface esta propiedad,

$$w = \text{orden}(a, n)$$

$a^0 \pmod{n} = 1, a^1 \pmod{n}, a^2 \pmod{n}, \dots, a^{w-1} \pmod{n}$  son todos distintos  
y  
 $a^w \pmod{n} = 1 \Rightarrow a^{w+1} = a \pmod{n}, a^{w+2} = a^2 \pmod{n}, \dots$

# FUNDAMENTOS MATEMÁTICOS

► **Gaussiano  $w$  (orden de  $\alpha$  respecto a  $n$ )**

- El gaussiano de  $a$  respecto  $n$  divide al número de elementos de  $\mathbf{Z}_n^*$  (e.d., divide a  $\Phi(n)$ ):
  - Si  $w = \text{orden}(a,n) \rightarrow w \mid \Phi(n)$       { e.d., existe  $c / \Phi(n) = c \cdot w$  }  
                                                                { e.d.,  $w$  es divisor de  $\Phi(n)$  }
  - Por tanto, **solo pueden ser gaussianos de  $a$  respecto  $n$  los divisores de  $\Phi(n)$**

# ÍNDICE

- 1. FUNDAMENTOS MATEMÁTICOS
  - Conceptos básicos
    - Congruencias
    - Reducción módulo  $n$
    - Conjunto  $\mathbb{Z}_n$
  - Cálculo de inversos
    - Teorema de Fermat
    - Indicador de Euler y conjunto  $\mathbb{Z}_n^*$
    - Teorema de Euler
    - Cálculo de inversos mediante Euclides Modificado
  - Resolución de ecuaciones congruenciales
  - Exponenciación y logaritmo discreto
    - Restos potenciales y gaussiano
    - **Raíces primitivas o generador**
    - Logaritmos discretos
  - Cuerpos de Galois

# FUNDAMENTOS MATEMÁTICOS

- **Raíces primitivas - generador**

- Cuando el gaussiano (orden) de  $a$  respecto de  $n$  es igual al indicador de Euler  $\Phi(n)$ , se dice que  $a$  es una raíz primitiva o generador de  $n$

**Si  $w = \text{orden}(a, n) = \Phi(n) \rightarrow a$  es raíz primitiva de  $n$**

- Los restos potenciales de las raíces primitivas generan todo el conjunto reducido de restos  $\mathbf{Z}_n^*$  (elementos con inverso multiplicativo de  $\mathbf{Z}_n$ )

# FUNDAMENTOS MATEMÁTICOS

- Raíces primitivas – generador**

| a | a <sup>2</sup> | a <sup>3</sup> | a <sup>4</sup> | a <sup>5</sup> | a <sup>6</sup> | a <sup>7</sup> | a <sup>8</sup> | a <sup>9</sup> | a <sup>10</sup> | a <sup>11</sup> | a <sup>12</sup> | a <sup>13</sup> | a <sup>14</sup> | a <sup>15</sup> | a <sup>16</sup> | a <sup>17</sup> | a <sup>18</sup> |
|---|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|
| 3 | 9              | 8              | 5              | 15             | 7              | 2              | 6              | 18             | 16              | 10              | 11              | 14              | 4               | 12              | 17              | 13              | 1               |
| 4 | 16             | 7              | 9              | 17             | 11             | 6              | 5              | 1              | 4               | 16              | 7               | 9               | 17              | 11              | 6               | 5               | 1               |
| 7 | 11             | 1              | 7              | 11             | 1              | 7              | 11             | 1              | 7               | 11              | 1               | 7               | 11              | 1               | 7               | 11              | 1               |

- E.g., 3 es una raíz primitiva (generador) de 19
  - orden (3, 19) = 18 =  $\Phi(19)$   $\rightarrow$  3 es raíz primitiva de 19
  - $\{3^0 \bmod 19, 3^1 \bmod 19, 3^2 \bmod 19, \dots, 3^{18-1} \bmod 19\} = \mathbb{Z}_{19}^*$
- No todos los enteros n tienen raíces primitivas, solo aquellos que cumplen  $n \in \{2, 4, p^k, 2 \cdot p^k\}$  con p un primo impar ( $p > 2$ ) y k entero positivo

# FUNDAMENTOS MATEMÁTICOS

- Calcule las raíces primitivas o generadores de  $n=7$  ( $Z_7^*$ )
  - $\Phi(7) = 6$

|                                                                                                             |                                                 |
|-------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| $2^0 \equiv 1, 2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv \mathbf{1}$                                           | $\text{orden}(2, 7) = w = 3 \neq \Phi(7)$       |
| $3^0 \equiv 1, 3^1 \equiv 3, 3^2 \equiv 2, 3^3 \equiv 6, 3^4 \equiv 4, 3^5 \equiv 5, 3^6 \equiv \mathbf{1}$ | $\text{orden}(3, 7) = \mathbf{w = 6 = \Phi(7)}$ |
| $4^0 \equiv 1, 4^1 \equiv 4, 4^2 \equiv 2, 4^3 \equiv \mathbf{1}$                                           | $\text{orden}(4, 7) = w = 3 \neq \Phi(7)$       |
| $5^0 \equiv 1, 5^1 \equiv 5, 5^2 \equiv 4, 5^3 \equiv 6, 5^4 \equiv 2, 5^5 \equiv 3, 5^6 \equiv \mathbf{1}$ | $\text{orden}(5, 7) = \mathbf{w = 6 = \Phi(7)}$ |
| $6^0 \equiv 1, 6^1 \equiv 6, 6^2 \equiv \mathbf{1}$                                                         | $\text{orden}(6, 7) = w = 2 \neq \Phi(7)$       |

- Solución: los generadores de  $Z_7^*$  son  $g_1 = \mathbf{3}$  y  $g_2 = \mathbf{5}$

# FUNDAMENTOS MATEMÁTICOS

- **Raíces primitivas – generador**
- Calcule las raíces primitivas de  $n=13$ 
  - $n$  es primo,  $\Phi(n) = n-1 = 13 - 1 = 12 = 3 \cdot 2^2$
  - $\mathbb{Z}_n = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$
  - $\mathbb{Z}_n^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$
  - Los divisores de  $\Phi(13)$  son  $= \{1, 2, 3, 4, 6, 12\}$ , por tanto solo estos números pueden ser los gaussianos de  $a$  respecto 13
    - Analizaremos, para todos los  $a \in \mathbb{Z}_n^*$ , si  $a$  elevado a los divisores de  $\Phi(13)$  es 1:
      - En este caso:  $a^2 \bmod 13$ ,  $a^3 \bmod 13$ ,  $a^4 \bmod 13$ ,  $a^6 \bmod 13$ , y  $a^{12} \bmod 13$  (esto permite hallar el orden o gaussiano de  $a$  respecto  $n$ )
    - Si, para cierto ' $a$ ',  $w$ , la primera potencia cuyo resto potencial es igual a 1 corresponde a la potencia 12 ( $=\Phi(13)$ ), ' $a$ ' será una raíz primitiva de  $n$  ( $n=13$ ) {e.d., si el  $\text{orden}(a,13)=\Phi(13)=12$ }

# FUNDAMENTOS MATEMÁTICOS

| a                  | a <sup>2</sup>     | a <sup>3</sup> | a <sup>4</sup>      | a <sup>6</sup>                                      | a <sup>12</sup> | Gaussiano de a respecto n | ¿Es a raíz primitiva de n=13? |
|--------------------|--------------------|----------------|---------------------|-----------------------------------------------------|-----------------|---------------------------|-------------------------------|
| 1                  | 1                  | ---            | ---                 | ---                                                 | ---             | ---                       | ---                           |
| 2                  | 4                  | 8              | 3                   | 12                                                  | 1               | w=12                      | Sí                            |
| 3                  | 9                  | 1              | ---                 | ---                                                 | ---             | w=3                       | No                            |
| 4 = 2 <sup>2</sup> | 3 = 2 <sup>4</sup> | ?              | ?                   | 1 = 2 <sup>12</sup>                                 |                 | w=6                       | No                            |
| 5                  | 12                 | 8              | 1                   | ---                                                 | ---             | w=4                       | No                            |
| 6                  | 10                 | 8              | 9                   | 12                                                  | 1               | w=12                      | Sí                            |
| 7                  | 10                 | 5              | 9                   | 12                                                  | 1               | w=12                      | Sí                            |
| 8                  | ?                  | ?              | 1 = 2 <sup>12</sup> | ---                                                 | ---             | w=4                       | No                            |
| 9                  | 3                  | 1              | ---                 | ---                                                 | ---             | w=3                       | No                            |
| 10                 | 9                  | 12             | 1                   | ---                                                 | ---             | w=6                       | No                            |
| 11                 | 4                  | 5              | 3                   | 12                                                  | 1               | w=12                      | Sí                            |
| 12                 | ?                  | ?              | ?                   | 1 = (3 <sup>3</sup> ) <sup>2</sup> · 4 <sup>6</sup> | ---             | w=6                       | No                            |

# ÍNDICE

- 1. FUNDAMENTOS MATEMÁTICOS
  - Conceptos básicos
    - Congruencias
    - Reducción módulo  $n$
    - Conjunto  $\mathbb{Z}_n$
  - Cálculo de inversos
    - Teorema de Fermat
    - Indicador de Euler y conjunto  $\mathbb{Z}_n^*$
    - Teorema de Euler
    - Cálculo de inversos mediante Euclides Modificado
  - Resolución de ecuaciones congruenciales
  - Exponenciación y logaritmo discreto
    - Restos potenciales y gaussiano
    - Raíces primitivas o generador
    - **Logaritmos discretos**
  - Cuerpos de Galois

# FUNDAMENTOS MATEMÁTICOS

- **Logaritmos discretos**

- El cálculo inverso a la exponenciación en la aritmética modular se denomina logaritmo discreto. Consiste en obtener un  $x$  tal que:

$$a^x = b \pmod{n}$$

$x$  se expresa como:

$$x = \log_a b \pmod{n}$$

*¡Se calcula probando las sucesivas potencias de  $a$ !*

# FUNDAMENTOS MATEMÁTICOS

- Si  $a$  es una raíz primitiva de  $n$ , el logaritmo siempre existe
- Si  $a$  no es raíz primitiva, no tiene por qué existir, y si existe será múltiple

| $a$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ | $a^6$ | $a^7$ | $a^8$ | $a^9$ | $a^{10}$ | $a^{11}$ | $a^{12}$ | $a^{13}$ | $a^{14}$ | $a^{15}$ | $a^{16}$ | $a^{17}$ | $a^{18}$ |
|-----|-------|-------|-------|-------|-------|-------|-------|-------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| 3   | 9     | 8     | 5     | 15    | 7     | 2     | 6     | 18    | 16       | 10       | 11       | 14       | 4        | 12       | 17       | 13       | 1        |
| 4   | 16    | 7     | 9     | 17    | 11    | 6     | 5     | 1     | 4        | 16       | 7        | 9        | 17       | 11       | 6        | 5        | 1        |
| 7   | 11    | 1     | 7     | 11    | 1     | 7     | 11    | 1     | 7        | 11       | 1        | 7        | 11       | 1        | 7        | 11       | 1        |

- $x = \log_3 7 \pmod{19} = 6$  (3 es raíz primitiva de 19)
- $x = \log_4 3 \pmod{19}$  no tiene solución, 4 no es raíz primitiva de 19 ( $4^{ix} = 3 \pmod{19}$ ) pero
- $x = \log_4 9 \pmod{19}$  tiene solución pero no es única  $x = \{4, 13\}$

# CURSO CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

COSEC

**uc3m** | Universidad **Carlos III** de Madrid

