Universidad Carlos III de Madrid

COSEC LAB· Dpto. Informática

TEMA 1. FUNDAMENTOS MATEMÁTICOS

José Soler

Criptografía y seguridad informática
Seguridad en las tecnologías de la información
@ COSEC LAB

Curso 2016-2017

ÍNDICE

Conceptos básicos

- Sea **Z** conjunto de números enteros, con a, b, c $\in$ **Z**
  - **Z** forma estructura de Grupo (**Z**, +) si: cumple las propiedades:

$a + b \in \mathbf{Z}$	cierre : si se opera sigue perteneciendo
$a + (b + c) = (a + b) + c$	asociativa
$a + 0 = a$	identidad
$a + (-a) = 0$	inverso

FUNDAMENTOS MATEMÁTICOS

- **Z** forma estructura de Grupo Conmutativo o Abeliano si:

$a + b = b + a$	conmutativa

- **Z** forma estructura de Anillo (**Z**, +, ·) si **Z** es Grupo Abeliano y:

las sigu. prop. para la mult.:

$a \cdot b \in \mathbf{Z}$	cierre
$a \cdot (b \cdot c) = (a \cdot b) \cdot c$	asociativa
$a \cdot 1 = a$	identidad
$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$	· es distributiva respecto +

(**Z**, ·) es Semigrupo

FUNDAMENTOS MATEMÁTICOS

- **Z** forma estructura de Anillo Conmutativo si **Z** Anillo y:

$$\boxed{a \cdot b = b \cdot a}$$ conmutativa

- Anillo de División:

$$\boxed{a \cdot a^{-1} = 1}$$ inverso (·)

- **Cuerpo**: Anillo de División Conmutativo

ÍNDICE

- 1. FUNDAMENTOS MATEMÁTICOS
  - Conceptos básicos
    - **Congruencias**
    - Reducción módulo n
    - Conjunto $\mathbf{Z}_n$
  - Cálculo de inversos
    - Teorema de Fermat
    - Indicador de Euler y conjunto $\mathbf{Z}_n^*$
    - 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

FUNDAMENTOS MATEMÁTICOS

Congruencias

$18 \equiv 6 \bmod 12$ (Horas)
La diferencia entre ambos es un múltiplo del mod
$18-6=12=12\cdot 1$

1. Sean a, b, $n \in \mathbf{Z}$ con $n \neq 0$
2. a y b son congruentes módulo n ($a \equiv b$ (mód. n)) si

$$a \equiv b \ (\text{mód.}n) \quad \Leftrightarrow \quad a - b = k \cdot n \text{ para algún entero } k$$

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"

$a = 23, b = 3, n_1 = 10, n_2 = 11$
$a \equiv b$ (mód.n_1) pero $a \not\equiv b$ (mód.n_2)
$23 - 3 = 20 = 2 \cdot 10$ pero $\nexists \; k \in Z \;|\; 20 = k \cdot 11$

Congruencias

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

↳ van desde a y sumando el n y restando.
a-2n ; a-n , a+n ; a+2n

La clase de congruencia [3] módulo 10 =

$[3]_{10}$ = { …, -27, -17, -7, 3, 13, 23, 33, …} =
{ …, 3 **– 3** ·10, 3 **– 2** ·10, 3 **– 1** ·10, 3 **– 0** ·10, 3 **+ 1** ·10, 3 **+ 2** ·10, 3 **+ 3** ·10,…}
$-27 \equiv -17 \equiv -7 \equiv 3 \equiv 13 \equiv 23 \equiv 33$ (mód.10)

La clase de congruencia [7] módulo 11 =

$[7]_{11}$ = { …, -26, -15, -4, 7, 18, 29, 40, …} =
{ …, 7 **– 3** ·11, 7 **– 2** ·11, 7 **– 1** ·11, 7 **– 0** ·11, 7 **+ 1** ·11, 7 **+ 2** ·11, 7 **+ 3** ·11,…}
$-26 \equiv -15 \equiv -4 \equiv 7 \equiv 18 \equiv 29 \equiv 40$ (mód.11)

ÍNDICE

- 1. FUNDAMENTOS MATEMÁTICOS
  - Conceptos básicos
    - Congruencias
    - **Reducción módulo n**
    - Conjunto $\mathbf{Z}_n$
  - Cálculo de inversos
    - Teorema de Fermat
    - Indicador de Euler y conjunto $\mathbf{Z}_n^*$
    - 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

FUNDAMENTOS MATEMÁTICOS

- **Reducción módulo n**
  - Restar el valor mod, y quedarse con el positivo + bajo.
  - Dividir entre mod, y es el resto

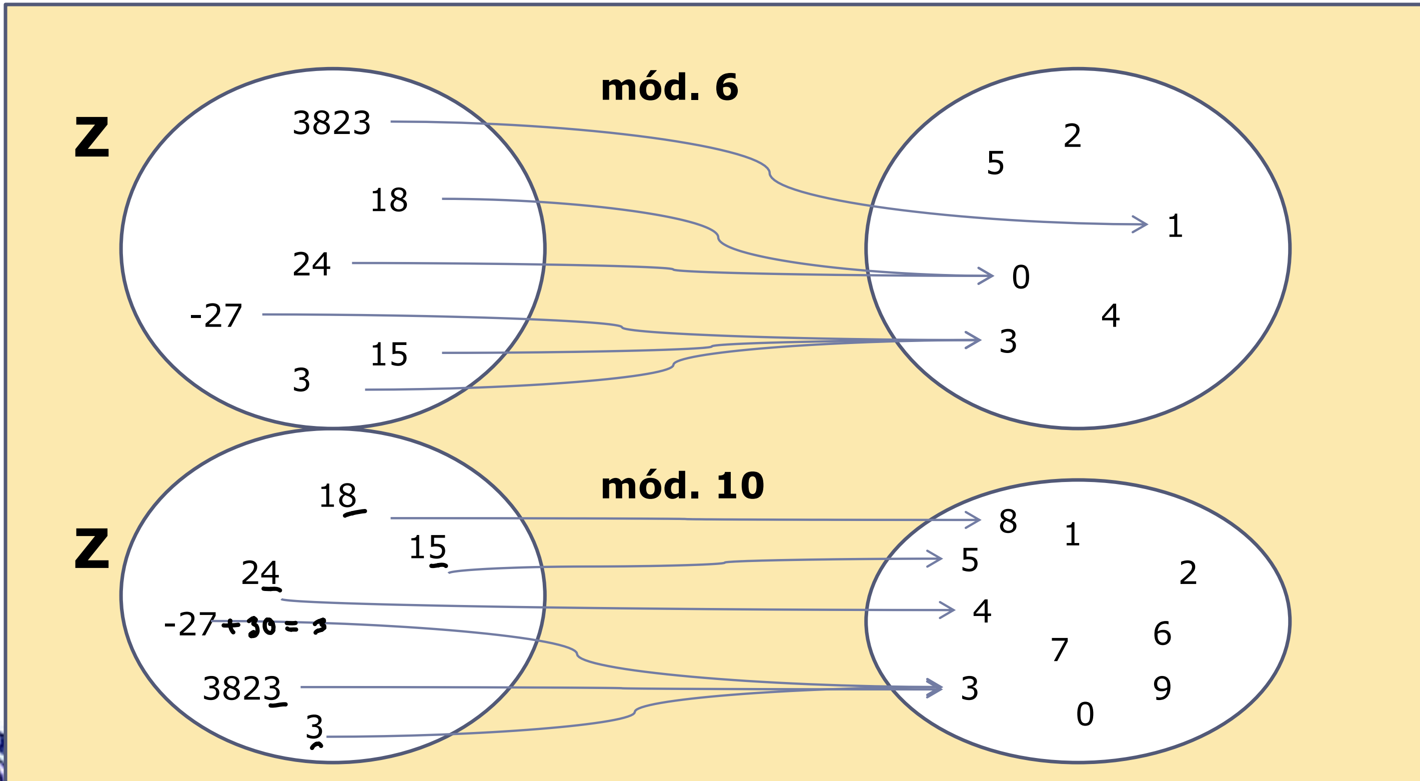
  Sean a, n ∈ **Z** (n ≠ 0). Se llama reducción módulo n (o módulo n) a la función (representada por (mód. n)) que aplicada a a, obtiene un $r \in \mathbf{Z}^{+} + \{0\}$ / $r \in \{0,1,\ldots n-1\}$ y $a \equiv r$ (mód. n)

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

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

26 (mód. 5) = 5 · 5 + 1 (mód. 5) = 1	(1<5-1)	p.t.	26 ≡ 1 (mód. 5)
30 (mód. 7) = 4 · 7 + 2 (mód. 7) = 2	(2<7-1)	p.t.	30 ≡ 2 (mód. 7)
11 (mód. 33) = 11	(11<33-1)		
256 (mód. 8) = 32 ·8+0 (mód. 8) = 0	(0<8-1)	p.t.	256 ≡ 0 (mód. 8)
-17 (mód. 12) ≡ -17 + 2 · 12 = 7	(7<12-1)	p.t.	-17 ≡ 7 (mód. 12)

Reducción módulo n



ÍNDICE

- 1. FUNDAMENTOS MATEMÁTICOS
  - Conceptos básicos
    - Congruencias
    - Reducción módulo n
    - **Conjunto Z_n**
  - Cálculo de inversos
    - Teorema de Fermat
    - Indicador de Euler y conjunto $\mathbf{Z_n}$*
    - 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

FUNDAMENTOS MATEMÁTICOS

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

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

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

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

> $Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$
>
> $Z_{31} = \{0, 1, 2, 3, 4, 5, 6, 7, \ldots, 26, 27, 28, 29, 30\}$

FUNDAMENTOS MATEMÁTICOS

- **Conjunto Z_n**
- **Operaciones ($+_n$, $\cdot_n$)**
  - Se define la suma y la multiplicación para $\mathbf{Z_n}$

Para $[a], [b], [c] \in Z_n$ $\quad +_n : [a] +_n [b] = [a+b]$ mod n $\quad \cdot_n : [a] \cdot_n [b] = [a \cdot b]$ mod n

Z_8 :

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

Z_{31} :

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

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

Para $n \neq 0$, Z_n es un anillo conmutativo respecto ($+_n$, $\cdot_n$)

$[a] +_n [b] \in \mathbf{Z}_n$	cierre	$[a] \cdot_n [b] \in \mathbf{Z}_n$
$[a] +_n ([b] +_n [c]) = ([a] +_n [b]) +_n [c]$	$[a] \cdot_n ([b] \cdot_n [c]) = ([a] \cdot_n [b]) \cdot_n [c]$
$[a] +_n 0 = [a]$	$[a] \cdot_n 1 = [a]$
$[a] +_n (-[a]) = 0$	$[a] \cdot_n ([b] +_n [c]) = ([a] \cdot_n [b]) +_n ([a] \cdot_n [c])$
$[a] +_n [b] = [b] +_n [a]$	$[a] \cdot_n [b] = [b] \cdot_n [a]$

- **Conjunto Z_n**
- **Relación de homomorfismo con el anillo de los enteros Z**
- La función de "reducción módulo n (mód. n)" es un homomorfismo entre Z (el anillo de los enteros) y $\mathbf{Z_n}$ (el anillo de los enteros módulo n) <-> Se cumple que:

Dados a, b $\in Z$, f(a),f(b) $\in Z_n$, con $f: Z \dashrightarrow Z_n$ (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) (mód. n)** = a (mód. n) $+_n$ b (mód. n) = (a(mód. n) + b(mód. n))(mód. n)

    $[\,(a+b)\,] = [a] +_n [b] = [\,[a]+[b]\,]$
  - **(a·b) (mód. n)** = a (mód. n) $\cdot_n$ b (mód. n) = (a (mód. n) · b (mód. n)) (mód. n)

    $[\,(a \cdot b)\,] = [a] \cdot_n [b] = [\,[a] \cdot [b]\,]$
  - **(a·(b+c)) (mód. n)** = ((a (mód. n) $\cdot_n$ b (mód. n)) $+_n$ (a (mód. n) $\cdot_n$ c (mód. n)) =

    = ((a·b) (mód. n)+(a·c) (mód. n)) (mód. n)

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

(3+8) mod 10

(3 mod 10 + 8 mod 10) mod 10

ejemplos

FUNDAMENTOS MATEMÁTICOS

(a + b)(mód. n) = a (mód. n) $+_n$ b (mód. n) = (a(mód. n) + b(mód. n))(mód. n)

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

Ejemplo:

(3 + 8) (mód. 5) = 3 (mód. 5) $+_n$ 8 (mód. 5) =

= (3 (mód. 5) + 8 (mód. 5)) mód. 5 =

= (3 + 3) mód. 5 = 6 mód. 5 = **1**

(3 + 8) (mód. 5) = 11 (mód. 5) = 1

FUNDAMENTOS MATEMÁTICOS

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

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

Ejemplo:

$\mathbf{(3 \cdot 8)\ (mód.\ 5)} = 3\ (mód.\ 5) \cdot_n 8\ (mód.\ 5) = (\ 3\ (mód.\ 5) \cdot 8\ (mód.\ 5)\ )\ mód.\ 5 =$

$= (\ 3 \cdot 3\ )\ mód.\ 5 = 9\ mód.\ 5 =$ **4**

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

$\mathbf{7^4\ (mód.\ 5)} = (7 \cdot 7 \cdot 7 \cdot 7)\ (mód.\ 5) =$

$= (\ 7\ (mód.\ 5) \cdot 7\ (mód.\ 5) \cdot 7\ (mód.\ 5) \cdot 7\ (mód.\ 5)\ )\ mód.\ 5 \Rightarrow >$

$= (\ 2 \cdot 2 \cdot 2 \cdot 2)\ mód.\ 5 = 2^4\ (mód.\ 5) = 16\ mód.\ 5 =$ **1**

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

FUNDAMENTOS MATEMÁTICOS

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

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

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

Ejemplo:

$$\mathbf{(3 \cdot (8+4))(\text{\textbf{mód.} } 5)} = ((3(\text{mód. } 5) \cdot_n 8(\text{mód. } 5)) +_n (3(\text{mód. } 5) \cdot_n 4(\text{mód. } 5)) =$$

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

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

$$= (9\ (\text{mód. } 5) + 12\ (\text{mód. } 5))\ (\text{mód. } 5) = (4 + 2)\ (\text{mód. } 5) =$$

$$= 6 \text{ mód. } 5 = 1$$

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

FUNDAMENTOS MATEMÁTICOS

Otros ejemplos:

$(23 + 4)(\text{mód. } 5) = 2$ $\quad 27 \bmod 5 = 2$ (−25)

$2^9\ (\text{mód. } 5) = 2$ $\quad (\underbrace{2^3}_{8})^3 \bmod 5 = (3)^3 \bmod 5 = 27 \bmod 5 = 2$

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

$(\underbrace{41 + 1001}_{1042}) \cdot \underbrace{999}_{4}\ (\text{mód. } 5) = 3$

$2 \cdot 4 \bmod 5 = 8 \bmod 5 = 3$

ÍNDICE

- 1. FUNDAMENTOS MATEMÁTICOS
  - Conceptos básicos
    - Congruencias
    - Reducción módulo n
    - Conjunto $\mathbf{Z}_n$
  - **Cálculo de inversos**
    - Teorema de Fermat
    - Indicador de Euler y conjunto $\mathbf{Z}_n^*$
    - 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

Cálculo de Inversos

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

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

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

$\frac{ax}{a} = \frac{1}{a} \bmod n \Rightarrow x = a^{-1} \bmod n$

- Este valor se representa por:

$$x = a^{-1} \quad (\text{mód. } n)$$

FUNDAMENTOS MATEMÁTICOS

- **Cálculo de Inversos**

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

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

ÍNDICE

- 1. FUNDAMENTOS MATEMÁTICOS
  - Conceptos básicos
    - Congruencias
    - Reducción módulo n
    - Conjunto $\mathbf{Z}_n$
  - Cálculo de inversos
    - **Teorema de Fermat**
    - Indicador de Euler y conjunto $\mathbf{Z}_n$*
    - 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

- **Teorema de Fermat**

coprimos

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

↳ Comprobar siempre.

$$\boxed{a^{p-1} \text{ mód. } p = 1}$$

De lo que se deduce:

Para el inverso:

$$a \cdot a^{p-2} \text{ mód. } p = 1 \rightarrow a^{-1} = a^{p-2} \text{ mód. } p = 1$$

FUNDAMENTOS MATEMÁTICOS

- Resolver: $2x$ mod.7 = 1 7 y 2 coprimos mcd(7,2) = 1

  Solución: 2^{-1} mod 7 = 1 2^5 mod 7 = $2^3 \cdot 2^2$ mod 7 = 1 · 4 mod 7 = 4 mod 7

  $\boxed{x = 4 \text{ mod } 7}$

  a=2, p=7 primo, m.c.d.(2,7)=1, aplicando Fermat:

  $x = 2^{p-2}$ mod.7 ⇨ $x = 2^{7-2}$ mod.7 ⇨ $x = 2^5$ mod.7 ⇨

  $x = 2^3\ 2^2$ mod.7 ⇨ x= 4 mod.7

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

  Solución

  a=35, p=3 primo, m.c.d.(35,3)=1,

  35x mod 3= (35 mod 3) (x mod 3) mod 3 = 2 x mod 3 = 1

  Aplicando Fermat: $x = 2^{p-2}$ mod.3 ⇨ $x = 2^{3-2}$ mod.3 ⇨ x= 2 mód.3

ÍNDICE

- 1. FUNDAMENTOS MATEMÁTICOS
  - Conceptos básicos
    - Congruencias
    - Reducción módulo n
    - Conjunto $\mathbf{Z}_n$
  - Cálculo de inversos
    - Teorema de Fermat
    - **Indicador de Euler y conjunto $\mathbf{Z}_n$****
    - 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

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 m.c.d. (a, n)=1) $Z^*_{12} = \underbrace{1, 5, 7, 11}_{\phi(12) = 4}$
  - Todos los elementos de Z_n* tienen inverso multiplicativo
- **Indicador de Euler: Φ(n)**

  Al número de elementos de Z_n* se le llama <u>indicador de Euler de n</u> (y se representa por Φ(n))

- **Conjunto reducido de restos Z_n***

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

$Z_8^* = \{1, 3, 5, 7\}$

$\Phi(8) = 4$

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

$Z_7^* = \{1, 2, 3, 4, 5, 6\}$

$\Phi(7) = 6$

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

- Si n es un número primo, p:

$$\boxed{\Phi(p) = p-1}$$

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

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

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

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

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

  - Si p y q son primos entre si:

$$\boxed{\Phi(p \cdot q) = \Phi(p) \cdot \Phi(q)}$$

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

$\phi(27) = \phi(3^3) = 2 \cdot 3^2 = 18$

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

$$\boxed{\Phi(n) = \prod p_i^{\,ki-1}\,(p_i - 1)}$$

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

ÍNDICE

FUNDAMENTOS MATEMÁTICOS

- **Teorema de Euler**

maximo comun divisor

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

↳ Pero n no tiene porque ser primo

$$\boxed{\mathbf{a^{\Phi(n)} \ \text{mód}\ n = 1}}$$

de lo que se deduce:

Simplificar cuando se pueda el valor de an

$\boxed{a \cdot a^{\Phi(n)-1} \ \text{mód}\ n = 1}$ y por tanto $\boxed{\mathbf{a^{-1} = a^{\Phi(n)-1} \ \text{mód}\ n}}$

✓ Se ve que Fermat también funciona

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

$\boxed{a^{-1} = a^{p-2} \ \text{mód}\ p}$ ← Fermat!

- Ejemplos de cálculo de inversos con Euler:

3 y 10 coprimos y 10 no primo

$x = 3^{-1} \bmod 10$ $\quad$ $x = 3^{\varphi(10)} \bmod 10$

$x = 3^{1 \cdot 4 - 1} \bmod 10$ $\quad$ $x = 3^3 \bmod 10$

$27 \bmod 10 = 7 \bmod 10$

  - 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**

- (Ejer. 2) Resuelva: 17x mod.12 =1

Solución

a=17, n=12, m.c.d.(17,12)=1, 5x mod 12 = 1

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

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

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

$\Rightarrow$ x = 5

FUNDAMENTOS MATEMÁTICOS

- (Ejer. 7) Resuelva: 37x mod.10 =1 { Coprimo

  ↳ primo ↳ no primo

  $37 - 10 \cdot 3 = 7$

  Solución $x = 7^{-1} \bmod 10 = 7^{\phi(10)-1} \bmod 10 = 7^3 \bmod 10$

  $7^2 \cdot 7$ ó $7 \cdot 7 \cdot 7 \Rightarrow 49 \cdot 7$ ó $-3 \cdot -3 \cdot -3 \Rightarrow 9 \cdot 7$ ó $-3^3 \Rightarrow 63$ ó -27; 3 ó $+30 \to 3$ } 3 mod 10

  a=37, n=10, m.c.d.(37,10)=1, 7x mod 10 =1

  metodos: Descomponer; Si es alto en su Z_n quitarle el n a cada uno

  Aplicando Euler: $x = 7^{\Phi(10)\,-1}$ mod.10

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

  $x = 7^{4-1}$ mod.10 ⇨ $x = 7^3$ mod.10 ⇨ $x = (-1) \cdot 7$ mod.10 ⇨

  $x = -7$ mod.10 ⇨ x = 3 mod.10 =3

FUNDAMENTOS MATEMÁTICOS

- Resuelva: 37x mod 41 =1

Solución

a=37, n=41, m.c.d.(37,41)=1,

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

Podemos aplicar Euclides

… $41 = 37 \cdot 1 + 4$

… $37 = 4 \cdot 9 + 1$ mcd

… $4 = 1 \cdot 4 + 0$

$1 = 37 - 4 \cdot 9$

$1 = 37 - 9(41 - 37)$

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

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

mod 41 … mod 41 = 0

$1 = (10 \cdot 37) \bmod 41 - \underbrace{9 \cdot 41 \bmod 41}_{0}$

$1 = 10 \cdot 37 \bmod 41 - 0$

$37^{-1} = 10 \bmod 41$

…

…

…

ÍNDICE

- 1. FUNDAMENTOS MATEMÁTICOS
  - Conceptos básicos
    - Congruencias
    - Reducción módulo n
    - Conjunto $\mathbf{Z}_n$
  - Cálculo de inversos
    - Teorema de Fermat
    - Indicador de Euler y conjunto $\mathbf{Z}_n^*$
    - 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

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

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

→ cuando es 1 son coprimos y podemos aplicar Euclides para hallar el inverso.

→ El último resto es el máximo común divisor

- **Cálculo del inverso con Euclides Modificado**

	c_1	c_2	…	…	…	c_n	c_{n+1}
n	a	r_1	r_2	…	…	r_{n-1}	1
r_1	r_2	r_3	…	…	**1**	**0**	

$n = c_1 \cdot a + r_1$

$a = c_2 \cdot r_1 + r_2$

$r_1 = c_3 \cdot r_2 + r_3$

…

…

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

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

- **Cálculo del inverso con Euclides Modificado**

el ultimo resto tiene que ser 1 (nunca que de 0) (1 = 0)

Despejamos los restos:

Vamos despejando dejando el 1 fuera vamos volviendo hacia atras y finalmente el que acompañaba a la x, el valor que multiplica sera el inverso.

$$n - c_1 \cdot a = r_1$$
$$a - c_2 \cdot r_1 = r_2$$
$$r_1 - c_3 \cdot r_2 = r_3$$
$$\ldots$$
$$\ldots$$
$$\color{red}{r_{n-2} - c_n \cdot r_{n-1} = 1}$$
$$r_{n-1} - c_{n+1} \cdot 1 = 0$$

- **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: $1 = k_1 \cdot a \ (\text{mód. } n)$

Por lo que $\boxed{\mathbf{a^{-1}\ (mód.\ n) = k_1}}$

FUNDAMENTOS MATEMÁTICOS

- Cálculo de inverso con Euclides modificado
- Resuelva 37x mod 41 =1

	1	9	4
41	37	4	1
4	**1**	**0**	

$n = c_1 \cdot a + r_1$ ⇨

$41 = 1 \cdot 37 + 4$

$37 = 9 \cdot 4 + \mathbf{1}$

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

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

$1 = 37 \cdot 10 \text{ mod } 41$

x = 10 mod. 41

- Cálculo de inverso con Euclides modificado
- Resuelva 23x mod 25 =1

$25 = \underline{23}\cdot 1 + \underline{2}$

$23 = 2\cdot 11 + 1$ $\begin{cases} 23 = \underline{2}\cdot 10 + \underline{3} \\ 2 = \underline{3}\cdot 0 + \underline{2} \end{cases}$

$3 = \underline{2}\cdot 1 + \underline{1}$ mcd( )=1

$2 = 1\cdot 2 + 0$

$1 = 3 - 2$

$1 = 3 - 2$

$1 = (23 - 2\cdot 10) - 2 = 23 - 2\cdot 11$

$1 = 23 - 11\cdot(25 - 23)$

$1 = \underline{12}\cdot 23 - 11\cdot 25$

25	23		

$n = c_1 \cdot a + r_1$ ⇨

25 = ? · 23 + ?

23 = ? · ? + ?

$1 = (12\cdot 23) \bmod 25 - \underbrace{(11\cdot 25) \bmod 25}_{0}$

$1 = 12\cdot 23 \bmod 25$

x = 12

$\boxed{23^{-1} = 12 \bmod 25}$

ÍNDICE

$ax = 1 \bmod b \; ; \; x = a^{-1} \bmod b$

FUNDAMENTOS MATEMÁTICOS

- **Resolución de ecuaciones de congruencia lineales**

$$\boxed{a \cdot x \equiv b \text{ mód. } n} \quad \Rightarrow \quad \boxed{\text{Existe un k entero tal que } \quad a \cdot x + n \cdot k = b}$$

$a \cdot x - b = nk \Rightarrow ax - \underbrace{n}_{+}k = b$

Tres casos:

- Si m.c.d.(a, n) = 1, la ecuación tiene solución y es única
- Si m.c.d.(a, n) = m ≠ 1, y m | b, ∃ m soluciones ~ tantas como mcd
  - b Lm
  - m | b == "m" divide a "b" → Existe c tal que b = c · m
- Caso contrario, no existe solución a la ecuación

FUNDAMENTOS MATEMÁTICOS

Resolución de ecuaciones de congruencia lineales

- Si m.c.d.(a, n)=1, la ecuación tiene solución y es única

Calcular el inverso y multiplicar por el correspondiente b

$$\mathbf{x = b \cdot \underbrace{y}_{a^{-1}} \ (mód.\ n)}$$

donde "y" se halla como:

$$a \cdot y = 1 \ (\text{mód. } n) \qquad \{\text{e.d., } y = a^{-1} \ (\text{mód. } n)\}$$

- Si m.c.d.(a, n) = m ≠ 1, m | b, ∃ m soluciones

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

donde "y" se halla como: inverso de z

o este método o el que sea

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

FUNDAMENTOS MATEMÁTICOS

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

$$\begin{array}{r|l} 14 & 2 \\ 7 & 7 \end{array}$$

$\varnothing(14) = \varnothing(2)\varnothing(7) = 1 \cdot 6 = 6$

mcd(3,14)=1 Solución única
14 no primo ⇒ Por Euler.

$x = 3 \cdot 3^{-1} \bmod 14 = 1 \bmod 14$

$3^{-1} = 3^{\varnothing(14)-1} \bmod 14 = 3^5 \bmod 14$

$3^{-1} = 3^3 \cdot 3^2 \bmod 14 = 13 \cdot (-5) \bmod 14$

$3^{-1} = 5 \bmod 14$

$15 - 14 = 1$

$x = 3 \cdot 5 \bmod 14$

$x = 1 \bmod 14$

$\phi(9) = \phi(3^2) = 3^1(2) = 6$

$15 \mid 3$, $5 \mid 5$, 1 1 — $9 \mid 3$, $3 \mid 3$, 1 1

FUNDAMENTOS MATEMÁTICOS

mcd(15, 9) = 3 $\quad 3 \mid 6 \quad 6 \mid 3$, $0 \; 2$

- (Ejer. 6) Resuelva 15 ·x = 6 mód. 9
  - Ecuación tipo a ·x = b mód. n
  - Se puede reducir → 6 · x = 6 mód. 9 → a=6, b=6, n=9
  - m = m.c.d(a, n) = m.c.d(6, 9) = 3 ≠ 1
    - ¿existe c | b=c ·m? Sí: 6=2 ·3 → c=2 → Existen m=3 soluciones
  - **x = (b/m) ·y + j ·(n/m) mod n j∈{0,m-1}**
  - x = (6/3) ·y + j ·(9/3) mód. 9 = 2 ·y + j ·3 mód. 9, j∈{0,2}

$5x = 2 \bmod 3 \quad x = 2 \cdot 5^{-1} \bmod 3$

$5^{-1} = 5^{\phi(3)-1} \bmod 3 = (5^2)^3 \bmod 3 = 1 \bmod 3$

$\boxed{x = 2 \bmod 3 \Rightarrow x = 2 \bmod 9 \;/\; x = 5 \bmod 9 \;/\; x = 8 \bmod 9}$

FUNDAMENTOS MATEMÁTICOS

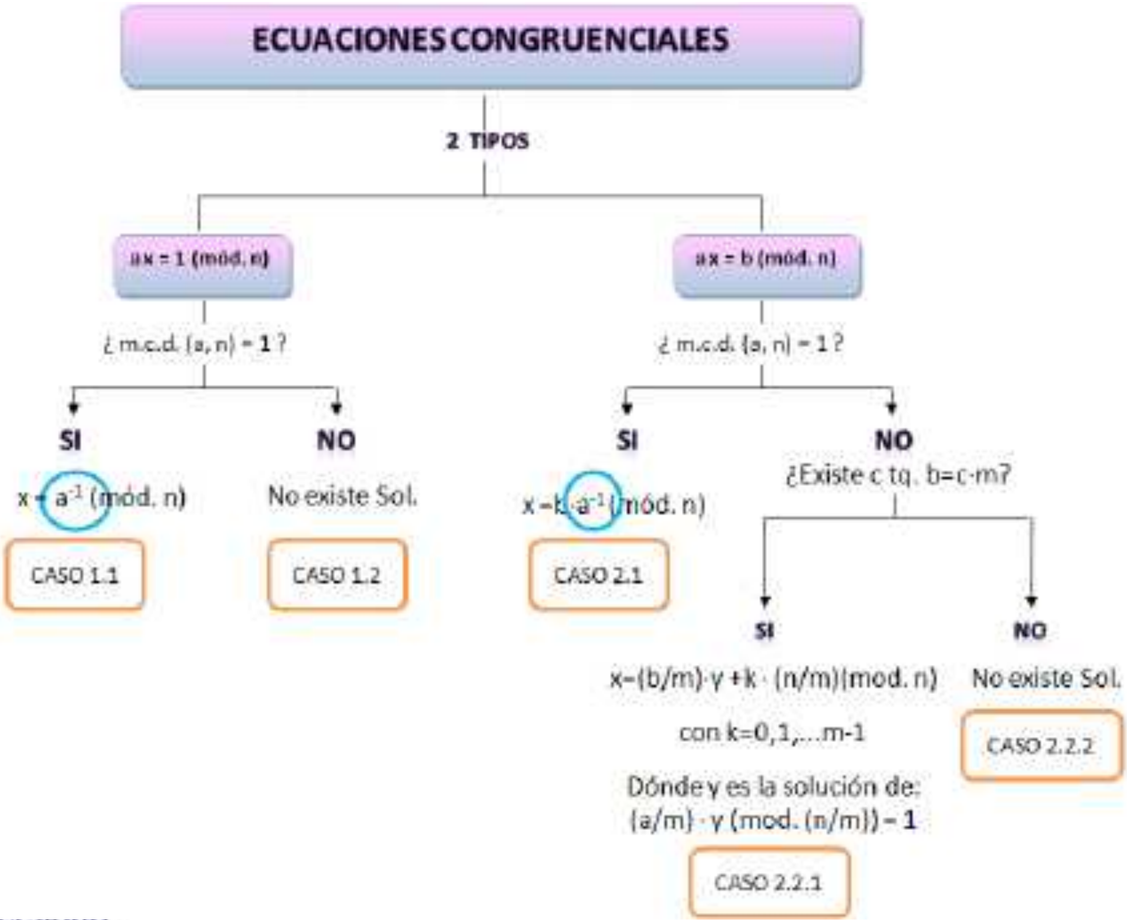
- (Ejer. 6) Resuelva $15 \cdot x = 6$ mód. 9 (cont.)

  - **$y = (a/m)^{-1}$ (mód. (n/m))** $= (6/3)^{-1}$ (mód.$(9/3)$) $= 2^{-1}$ mód.3
    - Aplicando Fermat/Euler: 2^{-1} mód. 3 = $2^{\Phi(3)-1}$ mód. 3
    - $\Phi(3) = (3-1) = 2$
    - $y = 2^{-1}$ mód. 3 = $2^{\Phi(3)-1}$ mód. 3 = 2^{1} mód. 3 = 2

  - $x = 2 \cdot y + j \cdot 3$ mód. 9 = $2 \cdot 2 + j \cdot 3$ mód. 9 = $4 + 3 \cdot j$ mód. 9, $j \in \{0,1,2\}$
    - $j=0 \rightarrow x_1 =$ **4**
    - $j = 1 \rightarrow x_2 = 4 + 3$ mód. 9 = **7**
    - $j = 2 \rightarrow x_3 = 4 + 6$ mód. 9 = **1**

FUNDAMENTOS MATEMÁTICOS

Teoría para test



ÍNDICE

- 1. FUNDAMENTOS MATEMÁTICOS
  - Conceptos básicos
    - Congruencias
    - Reducción módulo n
    - Conjunto $\mathbf{Z}_n$
  - Cálculo de inversos
    - Teorema de Fermat
    - Indicador de Euler y conjunto $\mathbf{Z}_n$*
    - 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

- **Restos potenciales**
- = Potencias de un entero módulo n
  - Dado **a** la base ∈ **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 mód. n
    - a^1 mód. n
    - a^2 mód. n
    - …
    - a^g mód. n
    - …

- **Restos potenciales**
  - n = 19

Son periodicas hasta el 1.

$= 3^4 \bmod 19$

bases

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

$19^2 \bmod 19$

- **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 $\Phi(n)$

↳ Hay tantos como múltiplos de $\phi(n)$ pero los hay menores

El menor es el gaussiano

- **Gaussiano w (orden de a respecto a n)**

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

Si $a^w = 1$ (mód. n) y w es el menor de los exponentes que satisface esta propiedad,

w = orden(a, n)

a^0 (mód.n)=1, a^1 (mód.n), a^2 (mód.n),…,a^{w-1} (mód.n) son todos distintos
y
a^w (mód.n) = 1 $\Rightarrow$ $a^{w+1} = a$ (mód.n), $a^{w+2} = a^2$ (mód.n) , …

FUNDAMENTOS MATEMÁTICOS

- **Gaussiano w (orden de a respecto a n)** → Es un divisor de $\phi(n)$ $w \mid \phi(n)$
  ↳ El menor exponente de la base (a) que da 1 haciendo mod n
- El gaussiano de a respecto n divide al número de elementos de $\mathbf{Z_n}^*$ (e.d., divide a $\Phi(n)$):

  Se busca el exponente más bajo que $a^w \bmod n = 1$

  - Si w = orden(a,n) → $w \mid \Phi(n)$ {e.d., existe c / $\Phi(n) = c \cdot w$ }
    {e.d., w es divisor de $\Phi(n)$}

    Probar con los exponentes divisores 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 $\mathbf{Z}_n$
  - Cálculo de inversos
    - Teorema de Fermat
    - Indicador de Euler y conjunto $\mathbf{Z}_n^*$
    - 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

- **Raíces primitivas - generador** Genera Z_n^*

↳ Si el gaussiano (orden) de a con n es igual que $\phi(n)$

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

Si w = orden(a, n) = Φ(n) → a es raíz primitiva de n

↳ Si es el gaussiano es $\phi(n)$

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

↳ los coprimos con n

FUNDAMENTOS MATEMÁTICOS

- **Raíces primitivas – generador**

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

- E.g., 3 es una raíz primitiva (generador) de 19 ~ El menor gaussiano es $\phi(19) = 18$ $\Rightarrow$ 3 es generador de 19
  - orden (3, 19) = 18 = $\Phi(19)$ → 3 es raíz primitiva de 19
  - $\{3^0$ mód. 19, 3^1 mód. 19, 3^2 mód. 19, ..., 3^{18-1} mód. 19$\} = \mathbf{Z}_{19}{}^*$

- No todos los enteros n tienen raíces primitivas, solo aquellos que cumplen $n \in \{2, 4, p^\alpha, 2 \cdot p^\alpha\}$ con p un primo impar (p>2) y α entero positivo

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

Probar con exp. divisores de $\phi(7)=6$

orden(2,7) = 3 Que no es $\phi(7)=6$

orden(3,7) = 6 = $\phi(7)$ coincide con el Euler de n Generador

exponente 1, 2, 3, 4, 5, 6

$\cancel{2^0} \equiv 1,\ 2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 1$ orden (2, 7) = w = 3 ≠ Φ(7)

$\cancel{3^0} \equiv 1,\ 3^1 \equiv 3,\ 3^2 \equiv 2,\ 3^3 \equiv 6,\ \cancel{3^4 \equiv 4},\ \cancel{3^5 \equiv 5},\ 3^6 \equiv 1$ orden (3, 7) = **w = 6 = Φ(7)**

$\cancel{4^0} \equiv 1,\ 4^1 \equiv 4,\ 4^2 \equiv 2,\ 4^3 \equiv 1$ orden(4,7) = 3 ≠ $\phi(7)$ no es generador orden (4, 7) = w = 3 ≠ Φ(7)

$\cancel{5^0} \equiv 1,\ 5^1 \equiv 5,\ 5^2 \equiv 4,\ 5^3 \equiv 6,\ \cancel{5^4 \equiv 2},\ \cancel{5^5 \equiv 3},\ 5^6 \equiv 1$ orden (5, 7) = **w = 6 = Φ(7)**

$\cancel{6^0} \equiv 1,\ 6^1 \equiv 6,\ 6^2 \equiv 1$ orden (6, 7) = w = 2 ≠ Φ(7)

orden(6,7) = 2 No es generador

orden(5,7) = 6 coincide con $\phi(7)$ Generador

- Solución: los generadores de Z_7* son g_1 = **3** y g_2 = **5**

FUNDAMENTOS MATEMÁTICOS

- **Raíces primitivas – generador**
- Calcule las raíces primitivas de n=13
  - n es primo, $\Phi(n) = n-1 = 13 - 1 = 12 = 3 \cdot 2^2$
  - $\mathbf{Z_n}$= {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12}
  - $\mathbf{Z_n}$*= {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 Como exponente
    - Analizaremos, para todos los a $\in \mathbf{Z_n}$***,** si a elevado a los divisores de $\Phi(13)$ es 1:
      - En este caso: a^2 mód. 13, a^3 mód. 13, a^4 mód. 13, a^6 mód. 13, y a^{12} mód. 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 orden(a,13)=$\Phi(13)$ =12}

FUNDAMENTOS MATEMÁTICOS

a	a^2	a^3	a^4	a^6	a^{12}	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
$4 = 2^2$	$3 = 2^4$	?	?	$1 = 2^{12}$		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	?	?	$1 = 2^{12}$	---	---	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	?	?	?	$1 = (3^3)^2 \cdot 4^6$	---	w=6	No

ÍNDICE

- 1. FUNDAMENTOS MATEMÁTICOS
  - Conceptos básicos
    - Congruencias
    - Reducción módulo n
    - Conjunto $\mathbf{Z}_n$
  - Cálculo de inversos
    - Teorema de Fermat
    - Indicador de Euler y conjunto $\mathbf{Z}_n$*
    - 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**

Logaritmos discretos

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

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

x se expresa como: $\log_a \cancel{a^x} = \log_a b$ $\underline{\text{mód. } n}$

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

↳ la base

Ir mirando los modulos de las potencias de a y buscar las que dan b.

todas no hay truco

¡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 porqué 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

→ buscar el mod19 que da 7 ⇒ que es 3^6;

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