# REPASO MADI

## ◦ ARITMÉTICA MODULAR

### INVERSO MODULAR

Un inverso modular DEBE SER PRIMO CON EL MÓDULO.

$E_i$: inversos de 6: $\{1,5\}$
NO inversos de 6: $\{2,3,4,0\}$

### CRITERIOS DIVISIBILIDAD

**2,5**: Si $a_0$ es divisible por $N$.
**4**: Si $a_1a_0$ es divisible por 4.
**8**: Si $a_2a_1a_0$ es divisible por 8.
**3,9**: Si $a_n + a_{n-1} \dots + a_1 + a_0$ es divisible por $N$.
**11**: Si $(-1)^n \cdot a_n + \dots + a_2 - a_1 + a_0$ es divisible por 11.
**7,13**: Si $a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 \dots$ es divisible por $N$.

### TEOREMA CHINO DE LOS RESTOS

$$x \equiv a_1 \bmod m_1$$
$$x \equiv a_2 \bmod m_2$$
$$x \equiv a_3 \bmod m_3$$

$$x = a_1 \left(\frac{m_1 \cdot m_2 \cdots m_k}{m_1}\right)\left(\frac{m_1 \cdot m_2 \cdot m_k}{m_1}\right)^{-1} \bmod m_1 + \dots + a_k \left(\frac{m_1 \cdot m_2 \cdots m_k}{m_k}\right)\left(\frac{m_1 m_2 \cdots m_k}{m_k}\right)^{-1} \bmod m_k.$$

## ◦ RECURRENCIA

$$a_n = \underbrace{4 \cdot a_{n-1} - 4a_{n-2}}_{\text{P. HOMOGÉNEA}} \underbrace{+3}_{\text{P. HET.}}, \quad n \geq 2$$

iniciales:
$a_0 = 6 \qquad a_1 = 8$

Ecuación característica:

$$x^2 - 4x + 4 = 0 \longrightarrow x_1 = 2, \; x_2 = 2$$

$a_n = k_1 \cdot 2^n + k_2 \cdot n \cdot 2^n$ // Si las raíces fueran distintas:

// $a_n = k_1 \cdot x_1^n + k_2 \cdot x_2^n$

$$\left.\begin{aligned} 6 &= k_1 + k_2 \\ 8 &= 2^n k_1 + n\,2^n k_2 \end{aligned}\right\} \qquad \left.\begin{aligned} 6 &= k_1 + k_2 \\ 8 &= 2^2 k_1 + 2 \cdot 2^2 k_2 \end{aligned}\right\}$$

$$\left.\begin{aligned} 6 &= k_1 + k_2 \\ 8 &= 4k_1 + 8k_2 \end{aligned}\right\} \begin{aligned} k_1 &= 2 \\ k_2 &= 4 \end{aligned}$$

$a_n = 2 \cdot 2^2 + 4 \cdot 2 \cdot 2^2 + (\text{S.HET}) =$

$= 8 + 16 + (\text{S.HET}) = 8 + 16 + \frac{3}{4} = 24 + \frac{3}{4} = \frac{99}{4}$

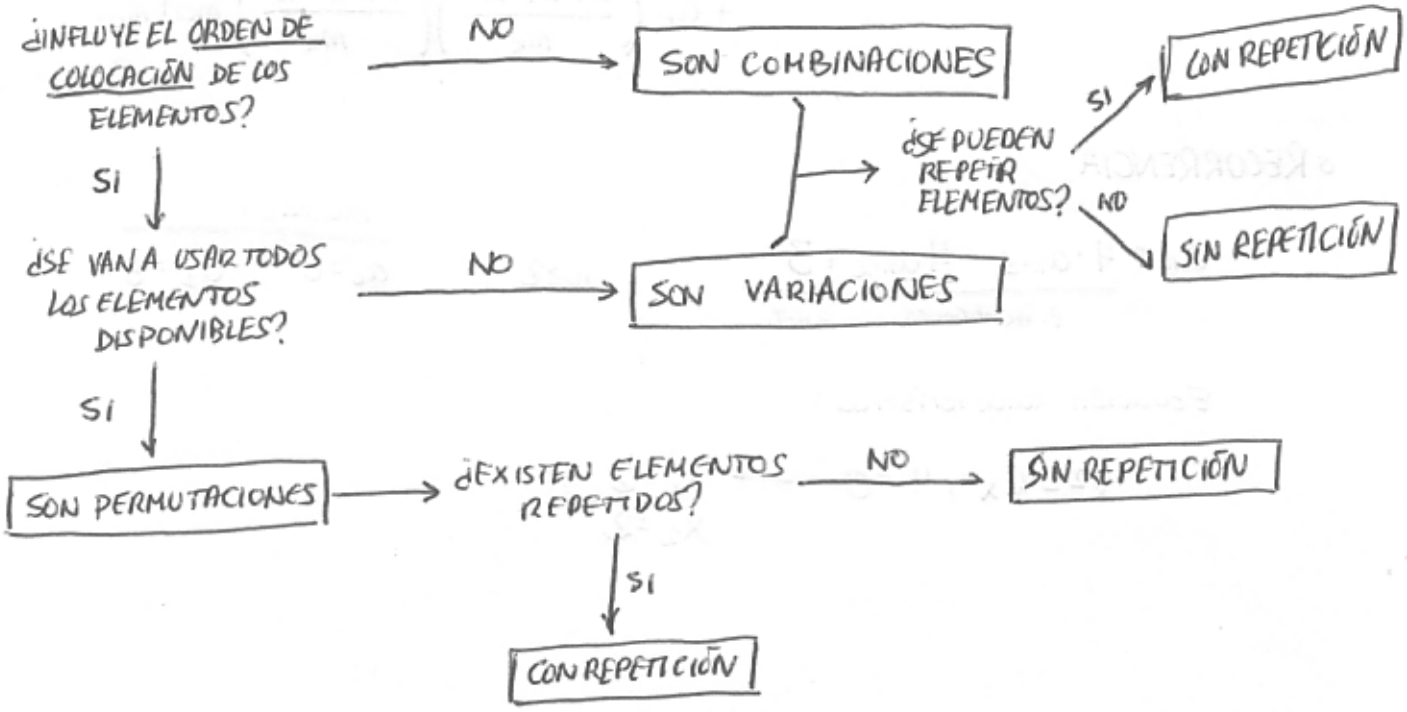
S.HET → $a_n = 4a_{n-1} + 4a_{n-2} + 3$

$4A + 4 + 1 = 0$

$4A = 3$

$A = \frac{3}{4}$ ← S.HET.

- COMBINATORIA.



| | SIN REPETICIÓN | CON REPETICIÓN |
|---|---|---|
| VARIACIONES | $V_n^p = \frac{n!}{(n-p)!}$ | $VR_n^p = n^p$ |
| PERMUTACIONES | $P_n = n!$ | $PR_n^{a,b,c} = \frac{n!}{a!\,b!\,c!}$ |
| COMBINACIONES | $C_n^p = \binom{n}{p}$ | $CR_n^p = \binom{n+p-1}{p}$. |

$$\binom{n}{p} = \frac{n!}{p!\,(n-p)!}$$

- ALGORITMOS de ARITMÉTICA MODULAR

LETRA NIF

```
a=numero Dni MOD 23 ; letras:=[T,R,W,A,G,M,Y,F,P,D,X,B,N,J,Z,S,Q,V,H,L,C,K,E]
letras[a];
```

MASTERCARD

```
im:=sum(impares*2); pa:=Sum(pares)
param(impares[>9], impares-9 & re++);
digito:=(pa+im+re) MOD 10;
```

ISBN

```
for i=1; i≤9; i++;
   k:k+(v[i]×i);
nom:k mod 11;
```

RSA

```
p,q; n:=p*q; phi(n):=23088; 1/e MOD phi(n);
CLAVE PÚBLICA:(n,e)
CLAVE PRIVADA:(1/e MOD phi(n)),(=d)

convert(convert(mensaje,bytes),base,256,n); // cambiar base

EE:=x→Power(x,e) mod n;
DD:=x→Power(x,d) mod n;

CIFRAR:→ map(EE,mensaje);
DESCIFRAR:→ map(DD,mensaje);
```

# FIRMA DIGITAL

p1, q1  p2, q2  // primos grandes

na := p1 · q1;  nb := p2 · q2;

ea := aleatorio;  da := 1/e_a MOD (p1-1)*(q1-1)  // si e_a existe
eb := aleatorio;  db := 1/e_b MOD (p2-1)*(q2-1)  // si e_b existe

d_a CLAVE PRIVADA  e_a CLAVE PÚBLICA

(nb > ea) → CODIFICAR CON eb da
(ea > nb) → CODIFICAR CON da eb

convert ( convert ( texto, bytes), base, 256, na );

Ea := x → Power (x, ea) MOD na;
Eb := x → Power (x, eb) MOD nb;

Da := x → Power (x, da) MOD na;
Db := x → Power (x, db) MOD nb;

CIFRAR: map (Da@Eb, texto);
DESCIFRAR: map (Ea@Db, texto);