CONGRUENCIAS:

David González Sánchez

José Núñez Sánchez

ÍNDICE:

ÍNDICE:

1. DIVISIBILIDAD: algoritmo de la división.

$$D = d * c + r$$

1. DIVISIBILIDAD: algoritmo de la división.

$$D = d * c + r$$

1. DIVISIBILIDAD: criterios de divisibilidad.

UN Nº ES DIVISIBLE ENTRE…	UN Nº TIENE RESTO 0 AL DIVIDIRLO ENTRE…
2 sii su última cifra es par.	**2**
3 sii la suma de cifras es divisible entre 3.	**3**
5 sii su última cifra es 5.	**5**
10 sii su última cifra es 0.	**10**
9 sii la suma de cifras es divisible entre 9.	**9**

1. DIVISIBILIDAD: criterios de divisibilidad.

- **Criterio del 7:**

  Restar el doble de la cifra de las unidades al número sin la última cifra.

Ejemplo: 161 → 16 – 2*1 = 14 → 161 es divisible entre 7.

Ejemplo: 374 → 37 – 2*4 = 29 → 274 no es múltiplo de 7.

- **Criterio del 11:**

  Restar la suma de las cifras en posición impar a la suma de las cifras en posición par.

Ejemplo: **161** → (1+1) – (6) = – 4 → 161 no es divisible entre 11.

Ejemplo: **374** → (3+4) – (7) = 0 → 274 es múltiplo de 11.

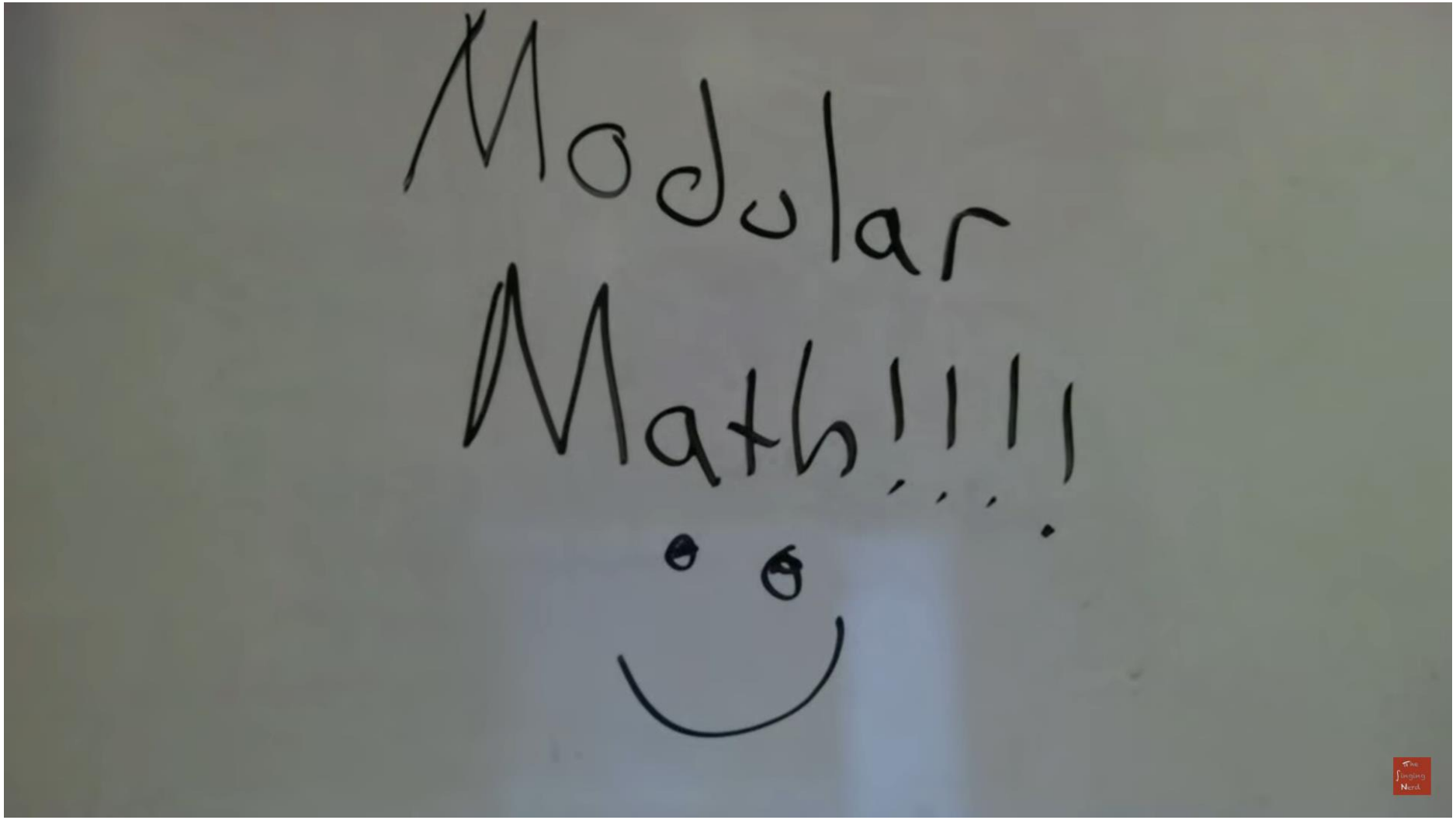
EJERCICIO 1: calcular cifras.

¿Qué cifras faltan en la igualdad

$14! = 87178\_\_12\_\_?$

ÍNDICE:

2. CONGRUENCIAS: definición.



2. CONGRUENCIAS: definición.

$$D = d * c + r$$

$$a = n*k + b$$

2. CONGRUENCIAS: definición.

$$D = d * c + r$$

$$a = n * k + b$$

2. CONGRUENCIAS: definición.

$$D = d * c + r$$

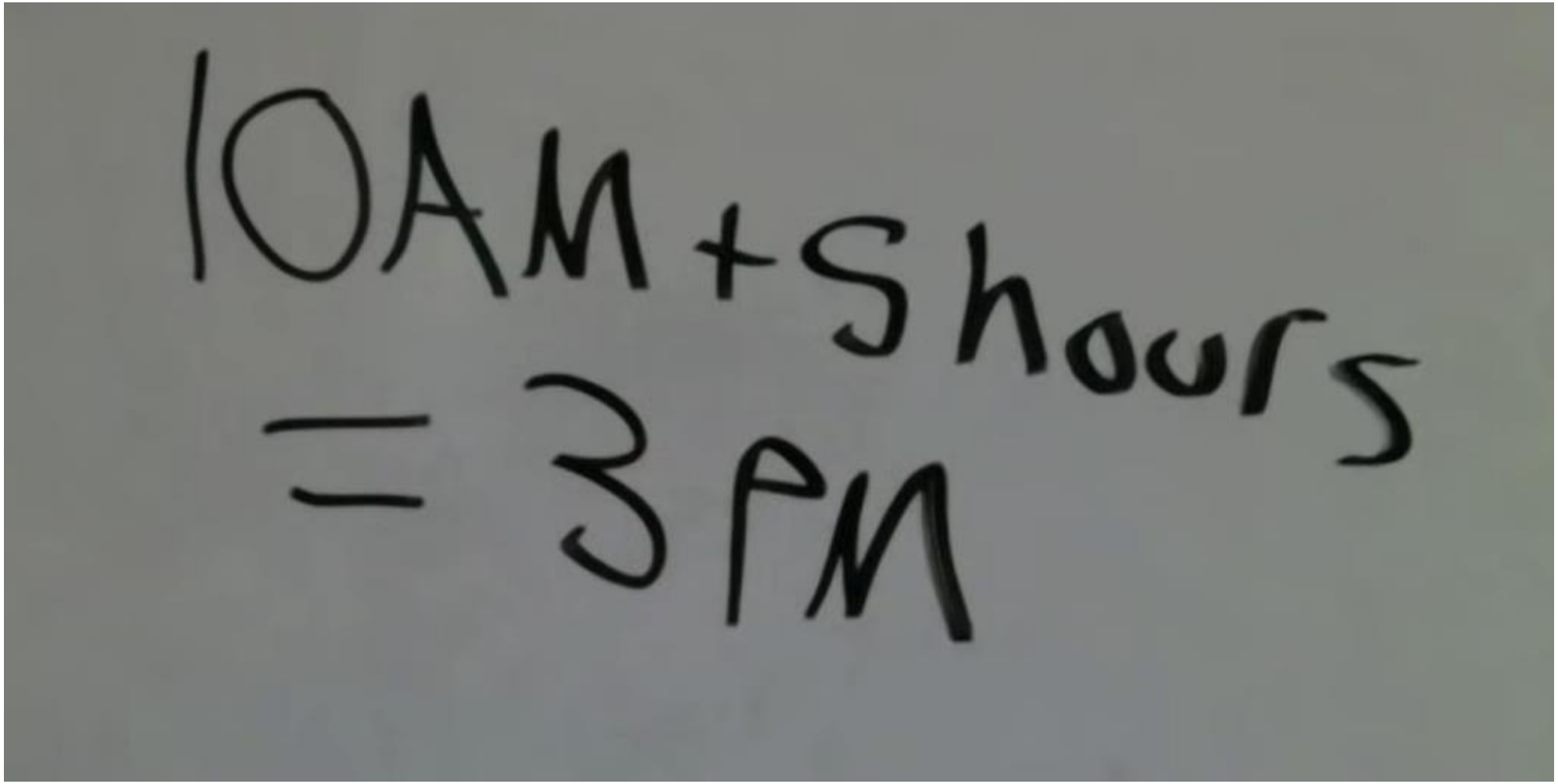
$$a \equiv b \pmod{n}$$

2. CONGRUENCIAS: definición.

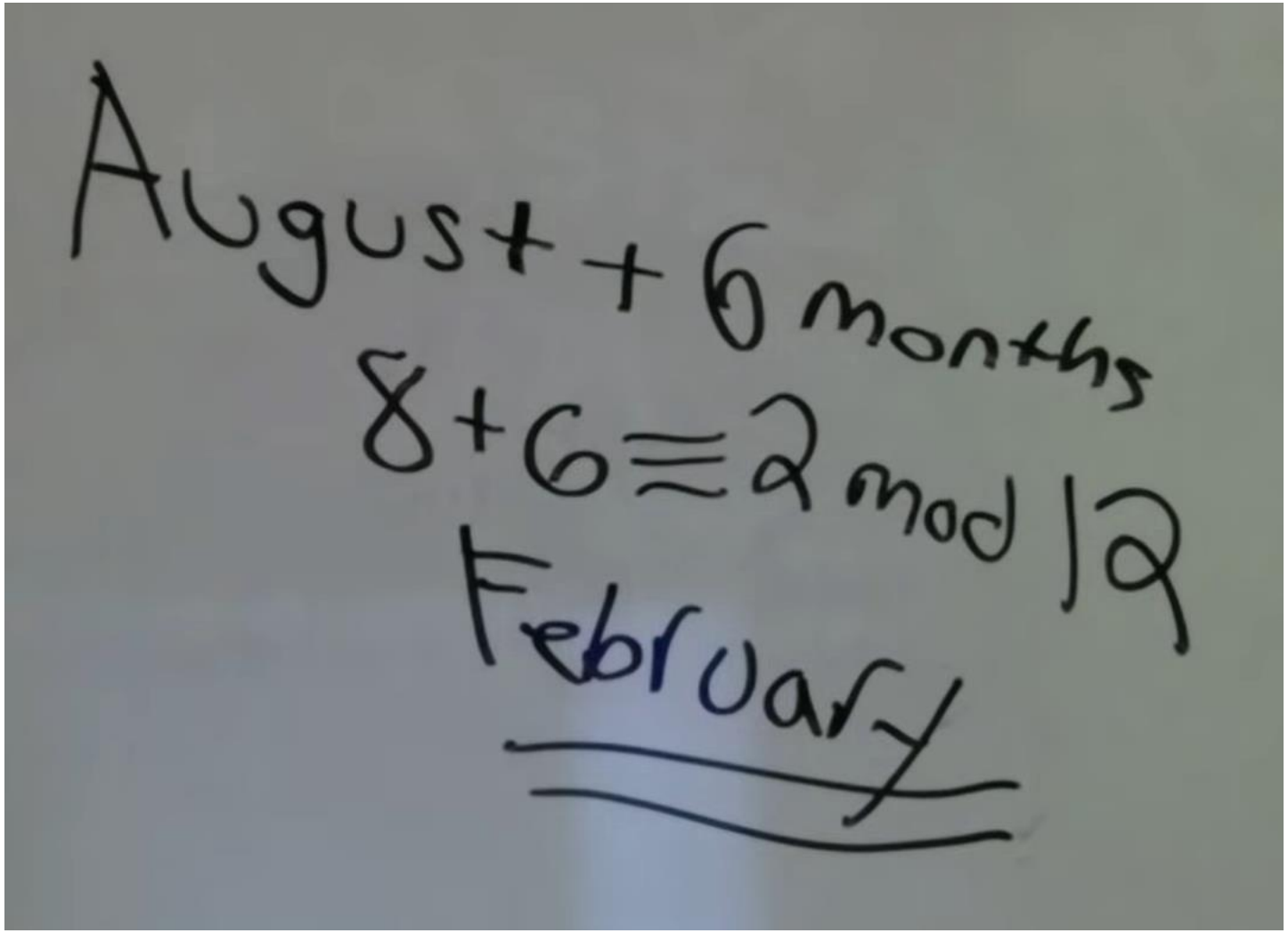
$$a = n*k + b$$

$$a \equiv b \pmod{n}$$

2. CONGRUENCIAS: definición.



2. CONGRUENCIAS: definición.



EJERCICIO 2: calcular restos.

$3 + 5 \equiv \quad \pmod{12}$

$7 + 6 \equiv \quad \pmod{12}$

$11 + 7 \equiv \quad \pmod{12}$

$7 + 13 \equiv \quad \pmod{12}$

$9 + 14 \equiv \quad \pmod{12}$

EJERCICIO 2: calcular restos.

$3 + 5 \equiv \mathbf{8} \pmod{12}$

$7 + 6 \equiv \mathbf{1} \pmod{12}$

$11 + 7 \equiv \mathbf{6} \pmod{12}$

$7 + 13 \equiv \mathbf{8} \pmod{12}$

$9 + 14 \equiv \mathbf{9} \pmod{12}$

ÍNDICE:

3. OPERACIONES: la suma.

$$a \equiv b_{(mod.n)} \longrightarrow a+c \equiv b+c_{(mod.n)}$$

3. OPERACIONES: la suma.

$$a \equiv b_{(mod.n)}$$
$$c \equiv d_{(mod.n)}$$

$$\Rightarrow$$

$$a+c \equiv b+d_{(mod.n)}$$
$$a+d \equiv b+c_{(mod.n)}$$

EJERCICIO 3: tabla de la suma en mód. 5

+	0	1	2	3	4
0					
1					
2					
3					
4					

EJERCICIO 3: tabla de la suma en mód. 5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

3. OPERACIONES: la multiplicación.

$$a \equiv b_{(mod.n)} \longrightarrow a \cdot c \equiv b \cdot c_{(mod.n)}$$

3. OPERACIONES: la multiplicación.

$$a \equiv b_{(mod.n)}$$
$$c \equiv d_{(mod.n)}$$

$$a \cdot c \equiv b \cdot d_{(mod.n)}$$
$$a \cdot d \equiv b \cdot c_{(mod.n)}$$

EJERCICIO 4: tabla de la multiplicación en mód. 5

·	0	1	2	3	4
0					
1					
2					
3					
4					

EJERCICIO 3: tabla de la suma en mód. 5

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

PRÁCTICA 1: las próximas Navidades.

- El año pasado, el día de Navidad (25 de diciembre) cayó en domingo, ¿en qué día de la semana celebraremos esta Navidad? ¿Y la del año que viene?

- El 1 de enero del año 2100 es viernes, ¿en qué día de la semana celebraremos la Navidad en el año 2100?

PRÁCTICA 2: verificación de DNI.

- Si os inventáis un DNI falso, en más del 95% de los casos lo puedo detectar con una calculadora.

- ¿Soy adivino? ¿Tengo acceso a una base de datos con todos los DNI de España?

- No, pero sé congruencias.

PRÁCTICA 2: verificación de DNI.

0	1	2	3	4	5	6	7	8	9	10	11
T	R	W	A	G	M	Y	F	P	D	X	B

12	13	14	15	16	17	18	19	20	21	22	
N	J	Z	S	Q	V	H	L	C	K	E	

3. OPERACIONES: la división.

3. OPERACIONES : la división.

- **SOLO** podemos “dividir” entre un número si es coprimo con el módulo.
- Aunque lo escribamos como división, estamos multiplicando por otro número al que llamamos EL INVERSO.
- Cuando el módulo es un número primo, cualquier número con resto no nulo tiene un inverso (y es único).

3. OPERACIONES: la potencia.

$$a \equiv b_{(mod.n)} \longrightarrow a^c \equiv b^c \ (mod.n)$$

El pequeño teorema de Fermat

Si p es un número primo que no divide al entero a, entonces

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

3. OPERACIONES: la raíz.

3. OPERACIONES: la raíz.

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

3. OPERACIONES: la raíz.

·	0	1	2	3	4	5	6	7
0								
1								
2								
3								
4								
5								
6								
7								

3. OPERACIONES: la raíz.

·	0	1	2	3	4	5	6	7
0	**0**							
1		**1**						
2			**4**					
3				**1**				
4					**0**			
5						**1**		
6							**4**	
7								**1**

$x^2 \equiv 0 \pmod{8} \Leftrightarrow x = 0, 4$

$x^2 \equiv 1 \pmod{8} \Leftrightarrow x = 1, 3, 5, 7$

$x^2 \equiv 4 \pmod{8} \Leftrightarrow x = 2, 6$

$x^2 \equiv 2 \pmod{8} \Leftrightarrow$ NO HAY SOL

$x^2 \equiv 3 \pmod{8} \Leftrightarrow$ NO HAY SOL

$x^2 \equiv 5 \pmod{8} \Leftrightarrow$ NO HAY SOL

$x^2 \equiv 6 \pmod{8} \Leftrightarrow$ NO HAY SOL

$x^2 \equiv 7 \pmod{8} \Leftrightarrow$ NO HAY SOL

PRÁCTICA 3.1: códigos ISBN.

El número ISBN es el que nos ayuda a identificar los libros. Hasta el 1 de enero de 2007, un número ISBN constaba de 10 dígitos divididos en 4 partes de longitud variable: identificador de grupo (país, área geográfica o área lingüística), de editor, de título y un dígito de control.

Una vez determinados los 9 primeros dígitos, por ejemplo 0 8536 1072, se calcula el número x entre 0 y 10 que verifique

$$(0 \times 1) + (8 \times 2) + (5 \times 3) + (3 \times 4) + (6 \times 5) + (1 \times 6) + (0 \times 7) + (7 \times 8) +$$

$$+ (2 \times 9) \equiv x \ (\text{mód } 11)$$

Si x no es 10, entonces el último dígito del ISBN es x. Si, por el contrario, x es 10, en lugar de un último dígito se añade una letra X.

PRÁCTICA 3.2: códigos ISBN.

Sin embargo, desde 2007 se cambió el formato y se pasó a un código de 13 cifras. Las 12 primeras corresponden a datos de control mientras que la decimotercera sirve como control y se calcula con la siguiente fórmula:

$$x_{13} \equiv -\sum_{i=1}^{6}(x_{2i-1} + 3x_{2i}) \quad (\text{mód } 10).$$

PRÁCTICA 4: encriptación y RSA.

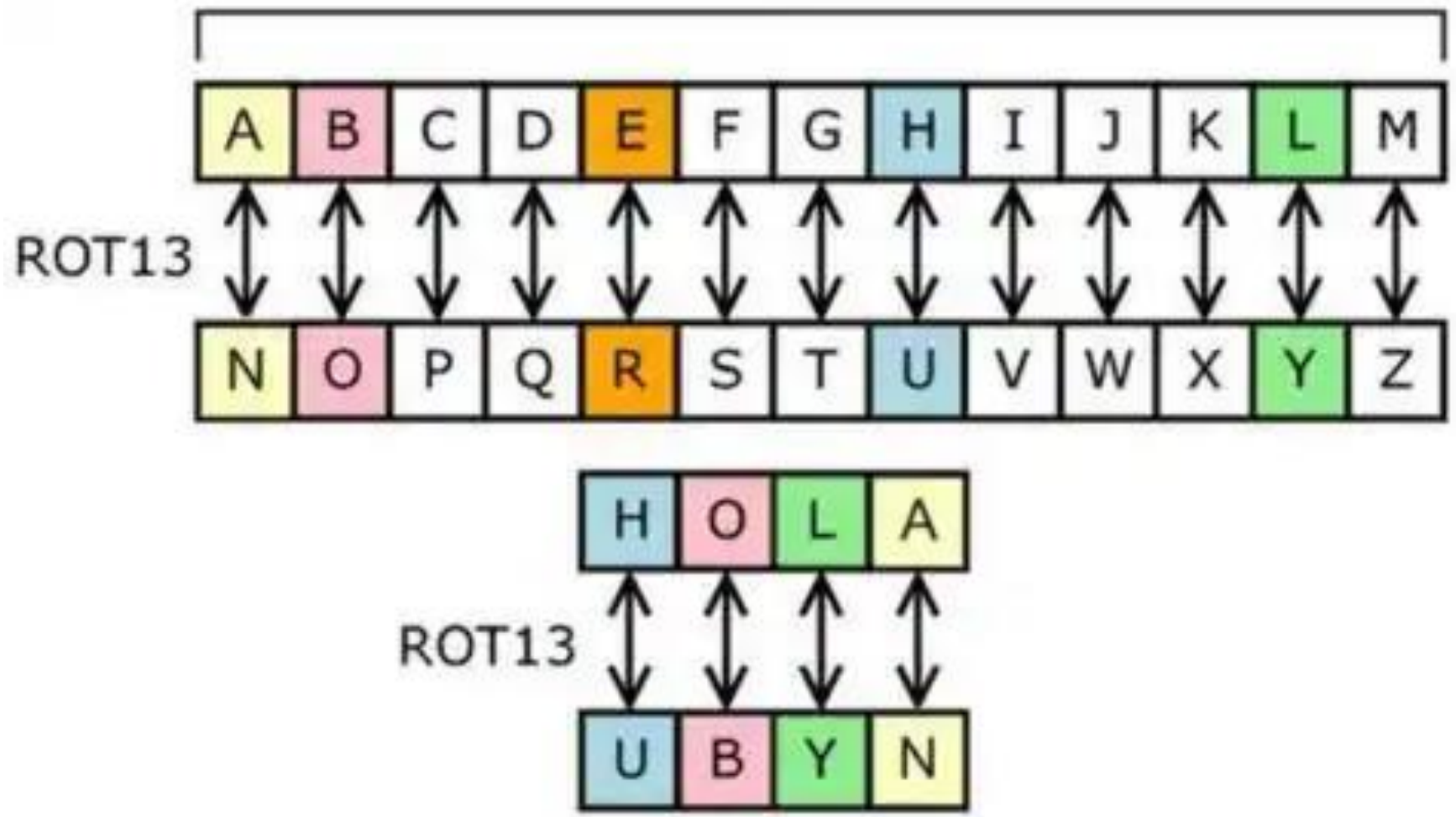
Congruencias → criptografía (ej: RSA)

Vamos a trabajar con una versión simplificada del RSA:

1. Pasemos las letras a números. Como tenemos 27 caracteres, trabajaremos en módulo 27.

A	B	C	D	E	F	G	H	I	J	K	L	M	
1	2	3	4	5	6	7	8	9	10	11	12	13	
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	_
14	15	16	17	18	19	20	21	22	23	24	25	26	0

PRÁCTICA 4: encriptación y RSA.



PRÁCTICA 4: encriptación y RSA.

2. Elegimos dos enteros (a, b) de forma que b esté entre 0 y 26 (por simplicidad) y a tenga inverso mód.27. Por tanto, a no podrá ser múltiplo de **…**

A	B	C	D	E	F	G	H	I	J	K	L	M	
1	2	3	4	5	6	7	8	9	10	11	12	13	
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	_
14	15	16	17	18	19	20	21	22	23	24	25	26	0

PRÁCTICA 4: encriptación y RSA.

2. Elegimos dos enteros (a, b) de forma que b esté entre 0 y 26 (por simplicidad) y a tenga inverso mód.27. Por tanto, a no podrá ser múltiplo de **3** .

3. Evaluamos cada número en la función f(x)= a·x + b

4. Reescribimos el mensaje con nuestras nuevas letras.

A	B	C	D	E	F	G	H	I	J	K	L	M	
1	2	3	4	5	6	7	8	9	10	11	12	13	
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	_
14	15	16	17	18	19	20	21	22	23	24	25	26	0

PRÁCTICA 4: encriptación y RSA.

5. Para desencriptar, pasamos las letras a números y evaluamos en la función inversa de f [nota: existe porque a tiene inverso en mód.27].

$f(x) = ax+b \Leftrightarrow f(x)-b = ax \Leftrightarrow (f(x)-b)\cdot a^{-1} = x$

6. Pasamos los nuevos números a letras.

A	B	C	D	E	F	G	H	I	J	K	L	M	
1	2	3	4	5	6	7	8	9	10	11	12	13	
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	_
14	15	16	17	18	19	20	21	22	23	24	25	26	0