

Matemáticas Discretas

Oscar Bedoya

`oscar.bedoya@correounivalle.edu.co`

`http://eisc.univalle.edu.co/~oscarbed/MD/`

PARTE 2.

- * TEORÍA DE NÚMEROS
- * TÉCNICAS DE DEMOSTRACIÓN
- * RELACIONES

- * Notación $a|b$
- * Números primos
- * Aritmética modular
- * Congruencia lineal
- * Aplicaciones

Teoría de números

División

- Sean a y b dos enteros, $a \neq 0$, se dice que **a divide a b** de forma exacta si existe un entero c tal que $a \cdot c = b$

Teoría de números

División

- $a|b$, si y solo si, existe un c tal que $a \cdot c = b$

$3|6$ porque $3 \cdot 2 = 6$

$4|28$ porque $4 \cdot 7 = 28$

$2 \nmid 5$ porque no existe c

Teoría de números

Determine si las siguientes expresiones son falsas o verdaderas:

• $3|12$ ✓ $12 = 3 \times 4$

• $12|4$ No

• $1|1$ $1 = 1 \times 1$

• $4|15$ No

• $0|23$ No

• $4|4$ $4 = 4 \times 1$

• $7|13$ No

• $2|3$ No

Teoría de números

Determine si las siguientes expresiones son falsas o verdaderas:

- $3|12$, **verdadero** porque $3 \cdot 4 = 12$
- $12|4$, **falso** porque no existe un entero c tal que $12 \cdot c = 4$
- $1|1$, **verdadero** porque $1 \cdot 1 = 1$
- $4|15$, **falso** porque no existe un entero c tal que $4 \cdot c = 15$
- $0|23$, **falso** porque no está definida la división entre 0
- $4|4$, **verdadero** porque $4 \cdot 1 = 4$
- $7|13$, **falso** porque no existe un entero c tal que $7 \cdot c = 13$
- $2|3$, **falso** porque no existe un entero c tal que $2 \cdot c = 3$

Teoría de números

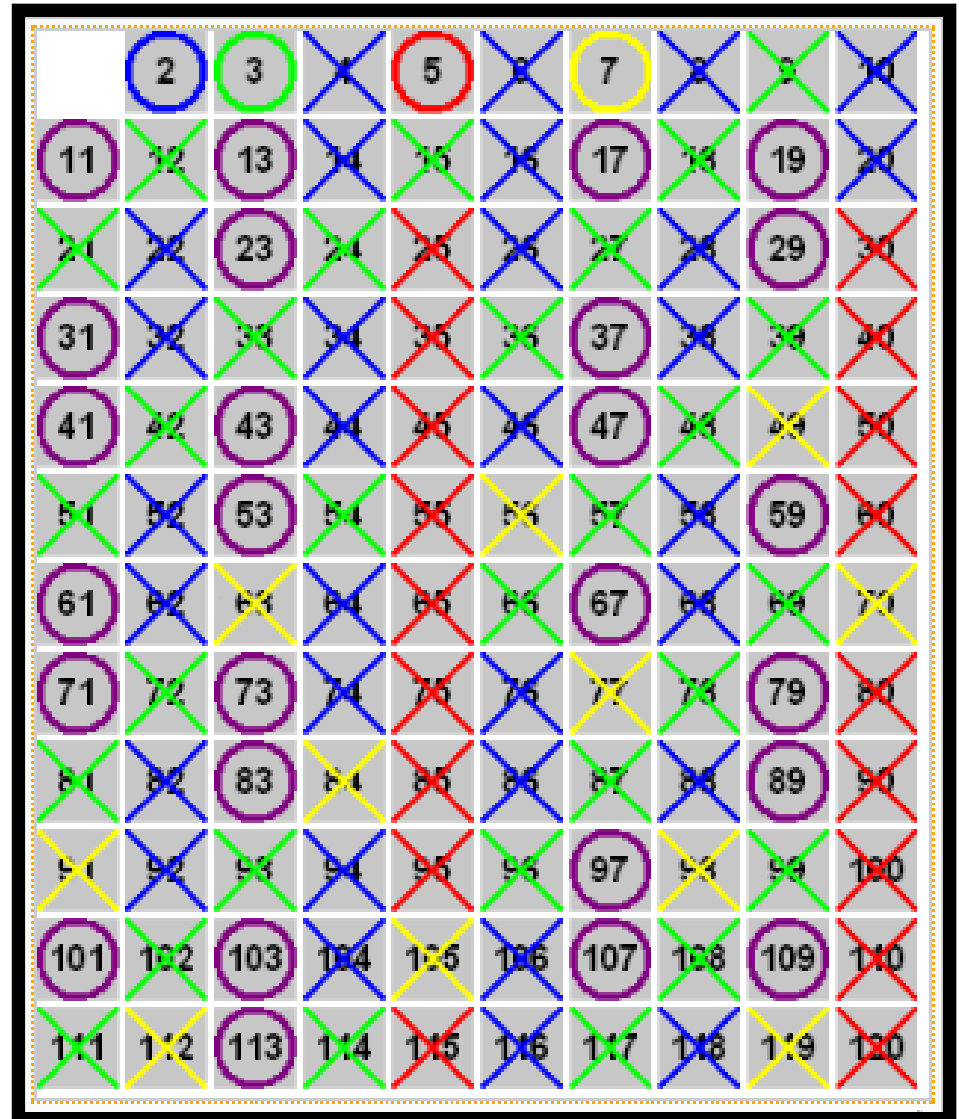
Números primos

- Un entero positivo p mayor que 1 se llama **primo** si los únicos divisores de p son 1 y p
- Un entero positivo mayor que 1 que no es primo se denomina **compuesto**

Teoría de números

Criba de Eratóstenes

Es un método para hallar todos los números primos menores que un natural N dado



Teoría de números

Algoritmo Criba de Eratóstenes (Complejidad

$O(n \log^2(n) \log \log n)$)

Entrada: Un número natural n

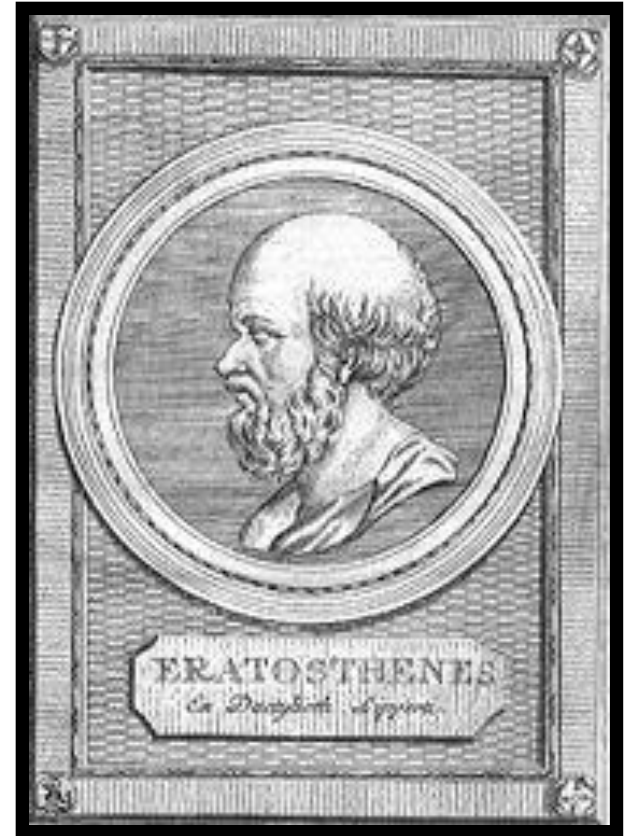
Salida: El conjunto de números primos anteriores a n
(incluyendo n)

1. Escriba todos los números naturales desde 2 hasta n
2. **Para** i desde 2 hasta $\lfloor \sqrt{n} \rfloor$ **haga lo siguiente:**
 1. **Si** i no ha sido marcado **entonces:**
 1. **Para** j desde i hasta $n \div i$ **haga lo siguiente:**
 1. Ponga una marca en $i \times j$
3. **El resultado es:** Todos los números sin marca

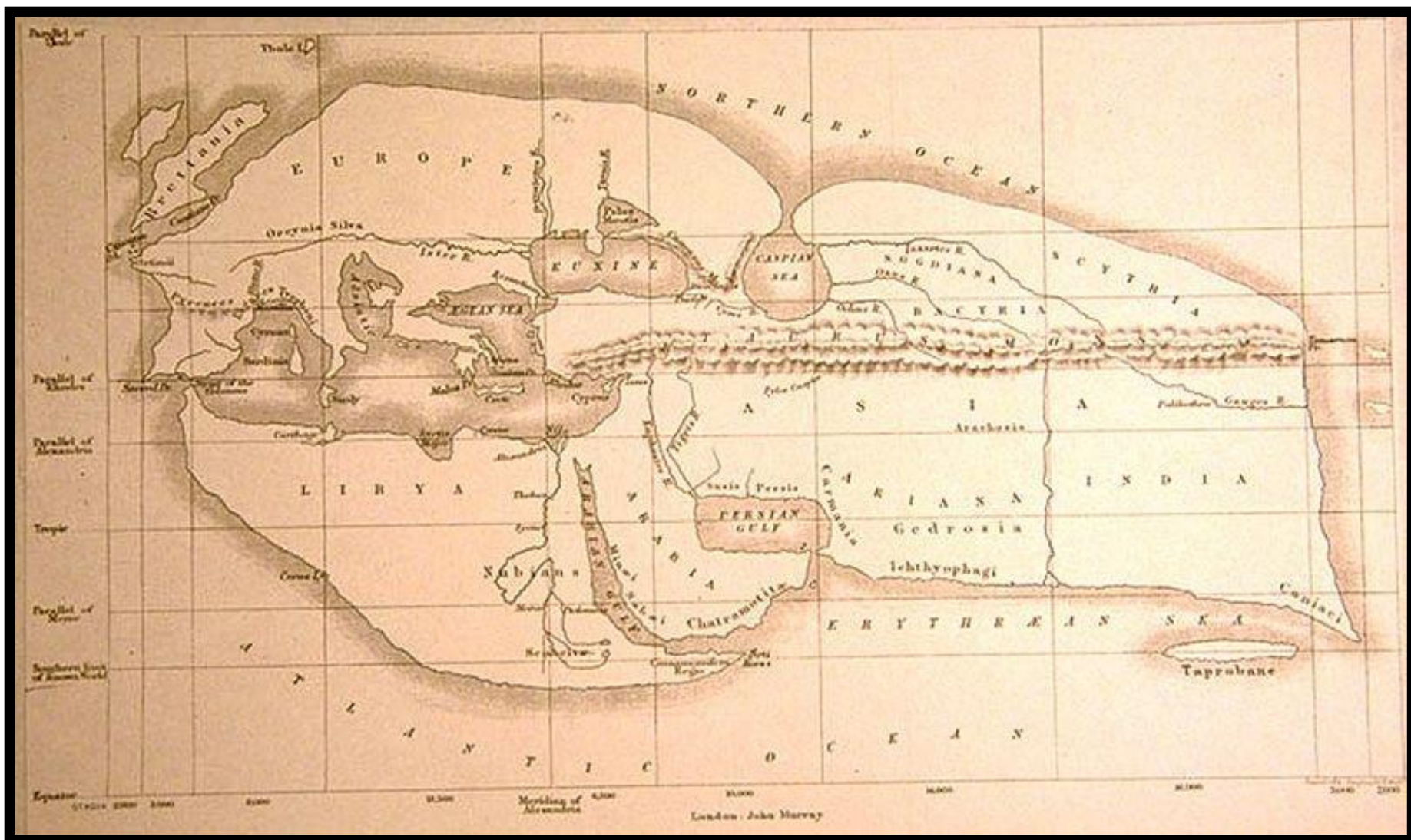
Teoría de números

Eratóstenes

- Matemático, astrónomo y geógrafo griego
- Hizo contribuciones acerca de las dimensiones de la tierra
- Compañero de Arquímedes



(276a.c - 194a.c)



Teoría de números

#	n	Fecha del descubrimiento	Descubridor
1	2	<i>antigüedad</i>	<i>desconocido</i>
2	3	<i>antigüedad</i>	<i>desconocido</i>
3	5	<i>antigüedad</i>	<i>desconocido</i>
4	7	<i>antigüedad</i>	<i>desconocido</i>
5	13	1456	anónimo
6	17	1588	Cataldi
7	19	1588	Cataldi
8	31	1772	Euler
9	61	1883	Pervushin
10	89	1911	Powers
11	107	1914	Powers
12	127	1876	Lucas
13	521	30-01-1952	Robinson
14	607	30-01-1952	Robinson
15	1.279	25-06-1952	Robinson
16	2.203	07-10-1952	Robinson

Teoría de números

Número primo	Fecha de descubrimiento
$2^{42643801}-1$	2009
$2^{37156667}-1$	2008
$2^{32582657}-1$	2006
$2^{30402457}-1$	2005

$2^{82589933}-1$ 2018.

$$4GB = 2^{32}$$

32 bits

82589933 bits \rightarrow 80MB

Teoría de números

Teorema: si n es un número compuesto, entonces tiene un divisor primo menor o igual a \sqrt{n}

Teoría de números

Teorema: si n es un número compuesto, entonces tiene un divisor primo menor o igual a \sqrt{n}

$$642 = 12$$

- Muestre que 101 es primo

$$101 \quad \sqrt{101} = 10$$

$$11 \nmid 101 \quad \text{No}$$

$$7 \nmid 101 \quad \text{No}$$

$$8 \nmid 101 \quad \text{No}$$

$$3 \nmid 101$$

$$2 \nmid 101 \quad \text{No}$$

Teoría de números

Teorema: si n es un número compuesto, entonces tiene un divisor primo menor o igual a \sqrt{n}

- $\sqrt{101} = 10.04$

Primos menores que 100				
2	3	5	7	11
13	17	19	23	29
31	37	41	43	47
53	59	61	67	71
73	79	83	89	97

Teoría de números

Teorema: si n es un número compuesto, entonces tiene un divisor primo menor o igual a \sqrt{n}

- $\sqrt{101} = 10.04$, se evalúa si 2,3,5,7 son divisores de 101

Primos menores que 100				
2	3	5	7	11
13	17	19	23	29
31	37	41	43	47
53	59	61	67	71
73	79	83	89	97

Teoría de números

Teorema: si n es un número compuesto, entonces tiene un divisor primo menor o igual a \sqrt{n}

- $\sqrt{101} = 10.04$, se evalúa si 2,3,5,7 son divisores de 101. Como no lo son, se puede asegurar que 101 es primo

Teoría de números

Teorema: si n es un número compuesto, entonces tiene un divisor primo menor o igual a \sqrt{n}

- Muestre que 133 no es primo

2 3 5 7 11 13 17

$\sqrt{133} = 11.83 \approx 12$ 11 | 133 7 | 133 ^{Sr}

Computato $7 \times 9 = 133$ $5 \mid 133$ X $3 \mid 133$ X
 $2 \mid 133$ X

Teoría de números

Teorema: si n es un número compuesto, entonces tiene un divisor primo menor o igual a \sqrt{n}

- $\sqrt{133} = 11.53$, se evalúa si 2,3,5,7,11 son divisores de 133

Primos menores que 100				
2	3	5	7	11
13	17	19	23	29
31	37	41	43	47
53	59	61	67	71
73	79	83	89	97

Teoría de números

Teorema: si n es un número compuesto, entonces tiene un divisor primo menor o igual a \sqrt{n}

- $\sqrt{133} = 11.53$, se evalúa si 2,3,5,7,11 son divisores de 133
Como $7|133$, se puede asegurar que 133 no es primo

Teoría de números

Clasifique los siguientes números como primos o compuestos:

• 123

$\lceil \sqrt{n} \rceil$, No 3 | 123

• 719

23, 19, 17, 13, 11, 7, 5, 3, 2

Primos menores que 100				
2	3	5	7	11
13	17	19	23	29
31	37	41	43	47
53	59	61	67	71
73	79	83	89	97

Teoría de números

Clasifique los siguientes números como primos o compuestos:

- $\sqrt{123} = 11.09$, dados 2,3,5,7,11. $3|123$. 123 es **compuesto**
- $\sqrt{719} = 26.81$, dados 2,3,5,7,11,13,17,19,23. Ninguno divide a 719, por lo tanto es primo

Primos menores que 100				
2	3	5	7	11
13	17	19	23	29
31	37	41	43	47
53	59	61	67	71
73	79	83	89	97

Teoría de números

Números primos de Mersenne

• Encontrar primos de la forma $2^p - 1$ donde p es un número primo

- $2^2 - 1 = 3$ es primo
- $2^3 - 1 = 7$ es primo
- $2^5 - 1 = 31$ es primo

$$1 \text{ --- } 2^{10^9}$$

$2^{10^2} \text{ --- } 2^{10^4}$

Teoría de números

Números primos de Mersenne

- Encontrar primos de la forma $2^p - 1$ donde p es un número primo
 - $2^2 - 1 = 3$ es primo
 - $2^3 - 1 = 7$ es primo
 - $2^5 - 1 = 31$ es primo
- No funciona en todos los casos
 - $2^{11} - 1 = 2047$ no es primo puesto que $23 \mid 2047$

Teoría de números

GIMPS



<http://mersenne.org/prime.html>

Claves publicas

Claves privadas

Teoría de números

Marin Mesenne

- Conoció a Descartes y le recomendó no publicar algunos de sus escritos
- Filósofo, matemático, músico y teólogo francés



(1588 – 1648)

Teoría de números

Aritmética modular

Se basa en la operación residuo o módulo definida a continuación:

$a \bmod b$ es el residuo de $a \div b$

Teoría de números

Aritmética modular

Se basa en la operación residuo o módulo definida a continuación:

$a \bmod b$ es el residuo de $a \div b$

- $0 \leq a \bmod b < b$

Teoría de números

$$\bullet 17 \bmod 5 = 2$$

$$17 = 5 \times 3 + \textcircled{2} \quad \text{residuo}$$

$$\bullet 9 \bmod 4 = 1$$

$$9 = 4 \times 2 + \textcircled{1} \quad \text{residuo}$$

$$\bullet -7 \bmod 3 = 2$$

$$-7 = 3(-3) + 2$$

$$\bullet 2 \bmod 2 = 0$$

$$2 = 2 \times 1 + 0$$

$$\bullet -5 \bmod 2 = 1$$

$$-5 = 2(-3) + 1$$

Teoría de números

- $17 \bmod 5 = 2$
- $9 \bmod 4 = 1$
- $-7 \bmod 3 = 2$
- $2 \bmod 2 = 0$
- $-5 \bmod 2 = 1$

Teoría de números

Calcule los siguientes módulos:

- $-133 \bmod 9$

$$-133 = 9 \times (-15) + 2$$

- $4 \bmod 2$

$$4 = 2 \times 2 + 0$$

- $2 \bmod 4$

$$2 = 4 \times 0 + 2$$

- $-12 \bmod 5$

$$-12 = 5 \times (-3) + 3$$

Teoría de números

Calcule los siguientes módulos:

- $-133 \bmod 9 = 2$
- $4 \bmod 2 = 0$
- $2 \bmod 4 = 2$
- $-12 \bmod 5 = 3$

Teoría de números

Calcule los siguientes módulos:

- $-57 \bmod 4 = 3$ $-57 = 4(-15) + 3$
- $7 \bmod 9 = 7$ $7 = 9 \times 0 + 7$
- $73 \bmod 8 = 1$ $73 = 8 \times 9 + 1$
- $-24 \bmod 7 = 4$ $-24 = 7(-4) + 4$

Teoría de números

Calcule los siguientes módulos:

- $-57 \bmod 4 = 3$
- $7 \bmod 9 =$ ~~0~~ 7
- $73 \bmod 8 = 1$
- $-24 \bmod 7 = 4$

Teoría de números

Calcule y compare los siguientes pares de valores:

- $7 \bmod 5, 2 \bmod 5$ 2, 2
- $4 \bmod 3, 13 \bmod 3$ 1, 1
- $11 \bmod 5, 21 \bmod 5$ 1, 1
- $22 \bmod 4, 38 \bmod 4$ 2, 2

Teoría de números

Calcule y compare los siguientes pares de valores:

- $7 \bmod 5 = 2 \bmod 5 = 2$
- $4 \bmod 3 = 13 \bmod 3 = 1$
- $11 \bmod 5 = 21 \bmod 5 = 1$
- $22 \bmod 4 = 38 \bmod 4 = 2$

Teoría de números

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

- Se dice que a es congruente con b módulo m , si y solo si,
$$a \bmod m = b \bmod m$$

Teoría de números

$a \equiv b \pmod{m}$

- Se dice que a es congruente con b módulo m , si y solo si,
 $a \bmod m = b \bmod m$

- Para los casos anteriores se tiene que:

$$7 \equiv 2 \pmod{5} \quad 7 \bmod 5 = 2 \bmod 5$$

$$4 \equiv 13 \pmod{3}$$

$$11 \equiv 21 \pmod{5}$$

$$22 \equiv 38 \pmod{4}$$

Teoría de números

Indique cuáles de las siguientes afirmaciones son ciertas:

- $2 \equiv 20 \pmod{6}$ $2 \pmod{6} = 20 \pmod{6} \Rightarrow 2 = 2$
- $5 \equiv 16 \pmod{3}$ $5 \pmod{3} = 16 \pmod{3} \Rightarrow \textcircled{2 = 1} \text{ No }$

Teoría de números

Indique cuáles de las siguientes afirmaciones son ciertas:

- $2 \equiv 20 \pmod{6}$. **si**, $2 \bmod 6 = 20 \bmod 6 = 2$
- $5 \equiv 16 \pmod{3}$. **no**, $5 \bmod 3 = 2$ y $16 \bmod 3 = 1$

Teoría de números

Indique cuáles de las siguientes afirmaciones son ciertas:

SI • $-7 \equiv -19 \pmod{4}$ $-7 \pmod{4} = 1, -19 \pmod{4} = 1 \Rightarrow 1 \equiv 1 \pmod{4}$ $\text{mod } m \text{ si } a \pmod{m} = b \pmod{m}$

SI • $3 \equiv 38 \pmod{7}$ $3 \pmod{7} = 3, 38 \pmod{7} = 3 \Rightarrow 3 \equiv 3 \pmod{7}$ $3 = 7 \times 0 + 3$ $38 \pmod{7} = 3$ SI

• $-5 \equiv 5 \pmod{5} \equiv 0$ $-5 \pmod{5} = 0, 5 \pmod{5} = 0 \Rightarrow 0 \equiv 0 \pmod{5}$ SI

Teoría de números

Indique cuáles de las siguientes afirmaciones son ciertas:

- $-7 \equiv -19 \pmod{4}$. si, $-7 \bmod 4 = -19 \bmod 4 = 1$
- $3 \equiv 38 \pmod{7}$. si, $3 \bmod 7 = 38 \bmod 7 = 3$
- $-5 \equiv 5 \pmod{5}$. si, $-5 \bmod 5 = 5 \bmod 5 = 0$

Teoría de números

Liste cinco enteros que sean congruentes con $4 \pmod{12}$

Teoría de números

Liste cinco enteros que sean congruentes con 4 mod 12

- $16 \equiv 4 \pmod{12}$
- $28 \equiv 4 \pmod{12}$
- $40 \equiv 4 \pmod{12}$
- $52 \equiv 4 \pmod{12}$
- $64 \equiv 4 \pmod{12}$

Teoría de números

Propiedades

- $a \equiv b \pmod{m}$, si y solo si, $m \mid (a-b)$

Teoría de números

Indique si se presenta cada una de las siguientes congruencias:

- $-29 \equiv 5 \pmod{17}$ *Sí*
- $-122 \equiv 5 \pmod{17}$ *No*
- $226 \equiv 5 \pmod{17}$ *Sí*

$$m | (a - b)$$

$$17 | (-29 - 5) \quad \boxed{17 | -34}$$

$$17 | (-122 - 5) -$$
$$17 | -127$$

$$17 | 226 - 5$$

$$17 | 221$$

Teoría de números

Indique si se presenta cada una de las siguientes congruencias:

- $-29 \equiv 5 \pmod{17}$. **si** porque $17 \mid (-29-5)$
- $-122 \equiv 5 \pmod{17}$. **no** porque $17 \nmid (-122-5)$
- $226 \equiv 5 \pmod{17}$. **si** porque $17 \mid (226-5)$

Teoría de números

Aplicaciones

- Tablas Hash
- Criptología

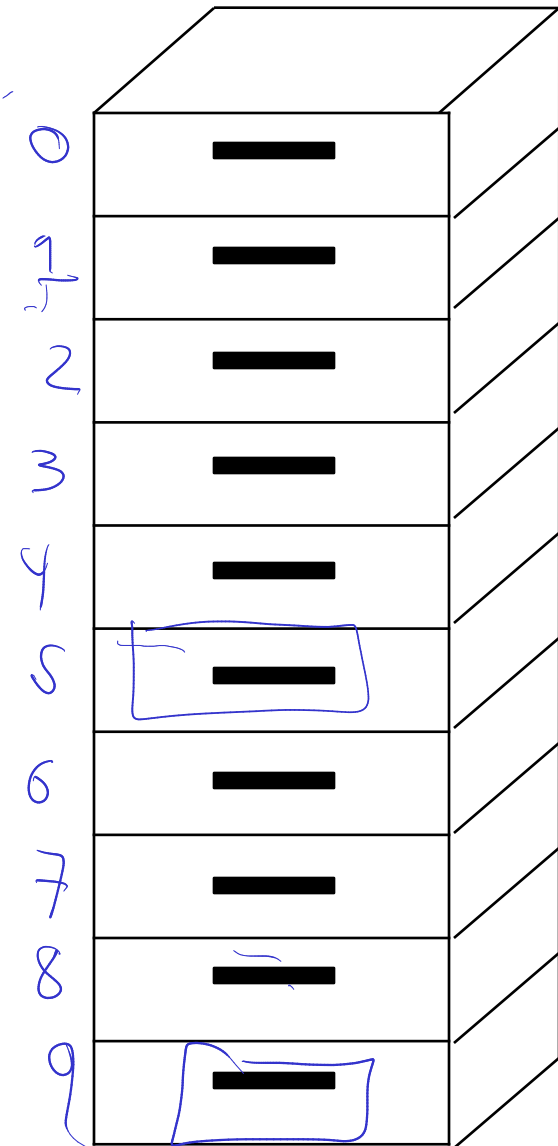
Teoría de números

Tablas Hash

0509555

0817449

$$0509555 \bmod 10 = 5$$
$$50955 \times 10 + 5$$

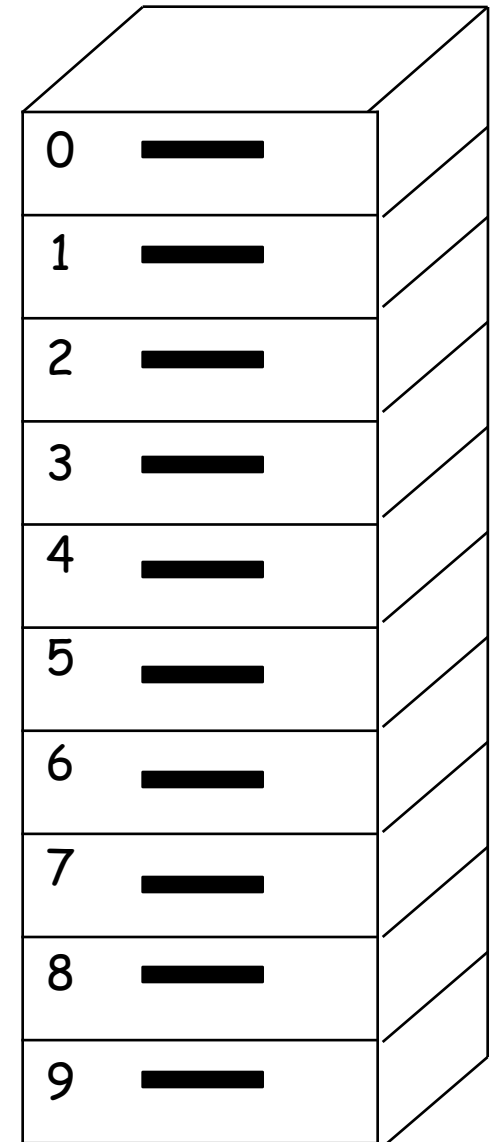


Teoría de números

Tablas Hash

- Dado un **código** k , para conocer el sitio donde se almacena, se utiliza la función:

$$h(k) = k \bmod 10$$



0	█
1	█
2	█
3	█
4	█
5	█
6	█
7	█
8	█
9	█

Teoría de números

Tablas Hash

- Dado un **código** k , para conocer el sitio donde se almacena, se utiliza la función:

$$h(k) = k \bmod 10$$

0509555

0817449

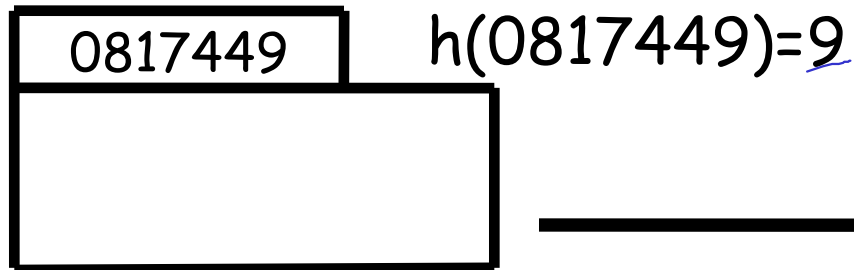
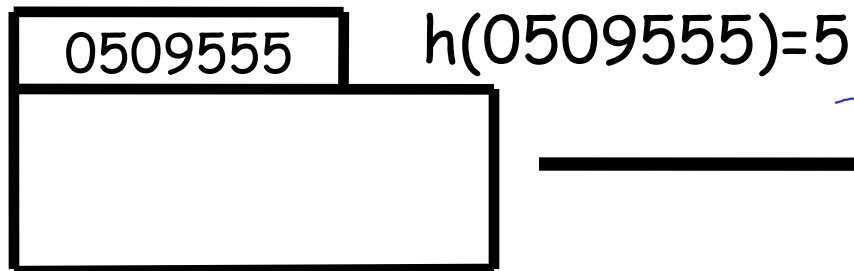
0	_____
1	_____
2	_____
3	_____
4	_____
5	_____
6	_____
7	_____
8	_____
9	_____

Teoría de números

Tablas Hash

- Dado un **código** k , para conocer el sitio donde se almacena, se utiliza la función:

$$h(k) = k \bmod 10$$



0	—
1	—
2	—
3	—
4	—
5	—
6	—
7	—
8	—
9	—

Teoría de números

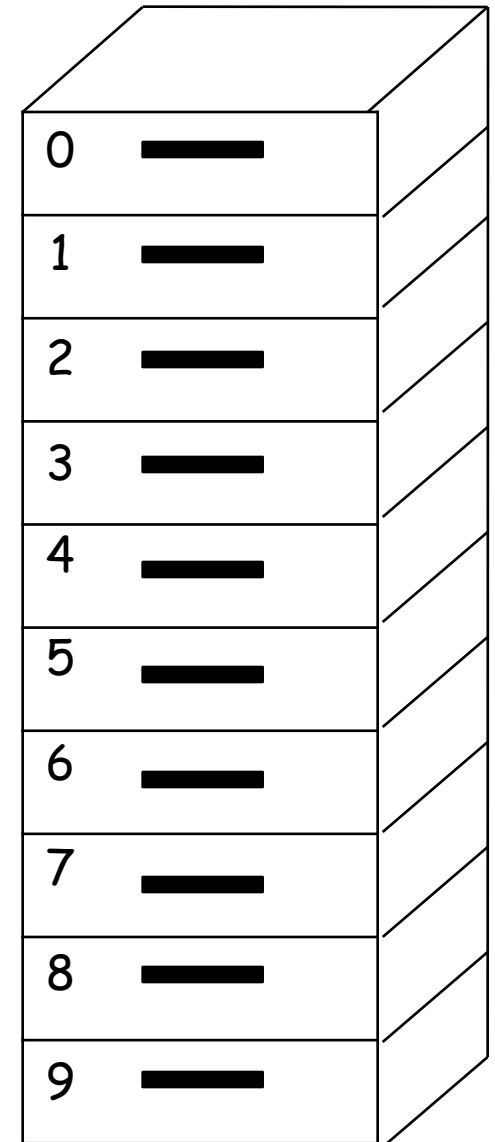
Tablas Hash

- Dado un **código** k , para conocer el sitio donde se almacena, se utiliza la función:

$$h(k) = k \bmod 10$$

$$h(0509555)=5$$

$$h(0817449)=9$$



0	█
1	█
2	█
3	█
4	█
5	█
6	█
7	█
8	█
9	█

Teoría de números

Tablas Hash

- Dado un **código** k , para conocer el sitio donde se almacena, se utiliza la función:

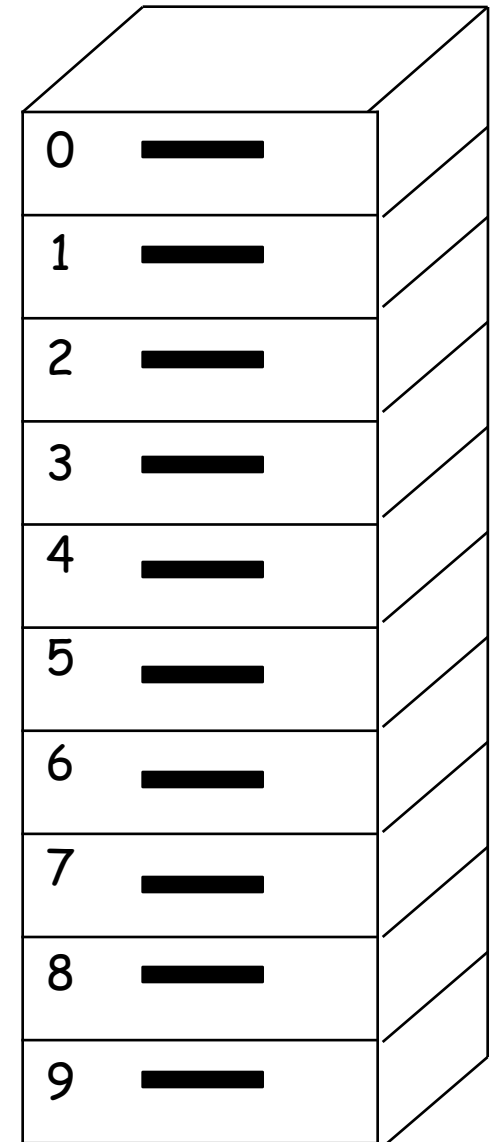
$$h(k) = k \bmod 10$$

$$h(0509555)=5$$

$$h(0817449)=9$$

$$h(0737459)=?$$

9



0	█
1	█
2	█
3	█
4	█
5	█
6	█
7	█
8	█
9	█

Teoría de números

Tablas Hash

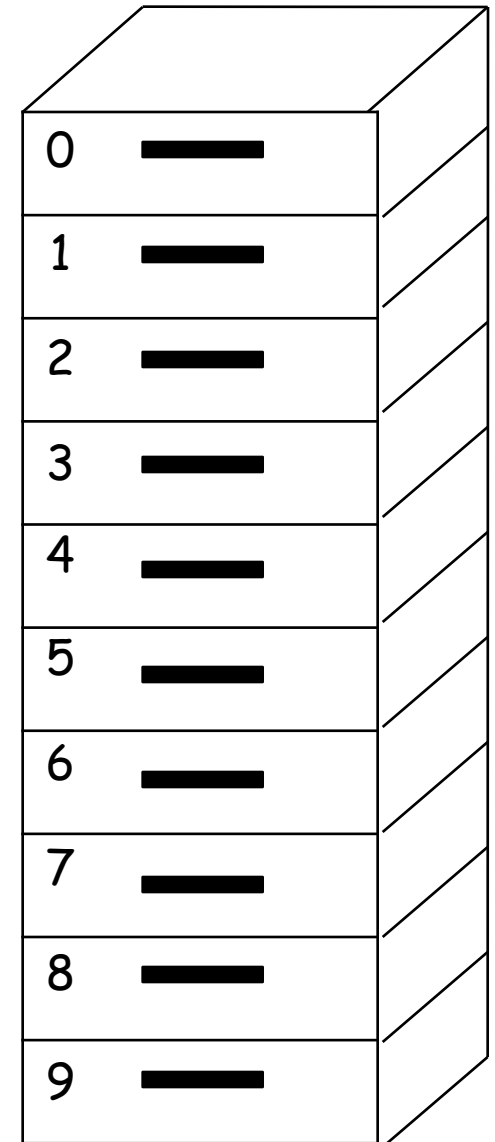
- Dado un **código** k , para conocer el sitio donde se almacena, se utiliza la función:

$$h(k) = k \bmod 10$$

$$h(0509555)=5$$

$$h(0817449)=9$$

$$h(0737459)=9$$



0	█
1	█
2	█
3	█
4	█
5	█
6	█
7	█
8	█
9	█

Teoría de números

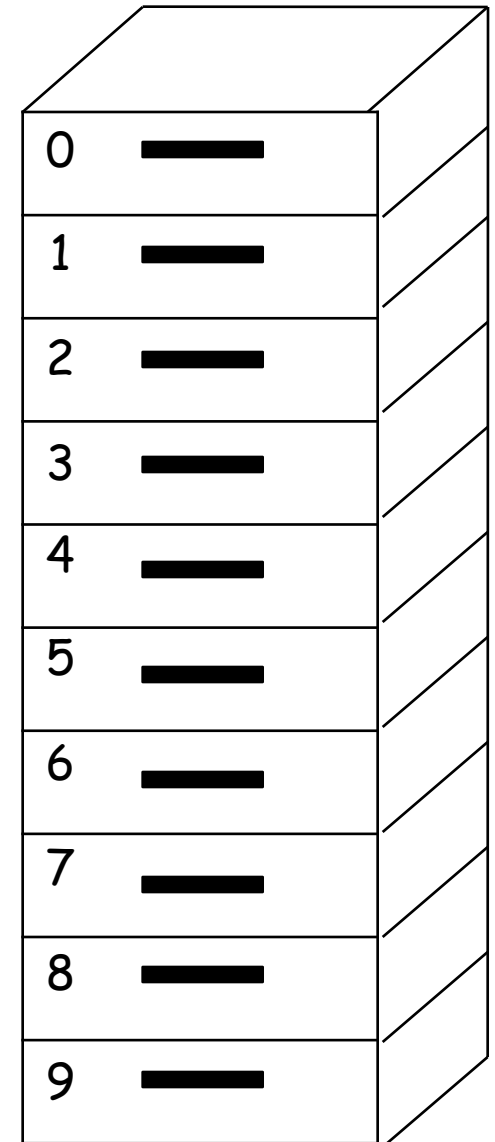
Tablas Hash

- Dado un **código** k , para conocer el sitio donde se almacena, se utiliza la función:

$$h(k) = k \bmod 10$$

$$h(0509555)=5$$

$$\left. \begin{array}{l} h(0817449)=9 \\ h(0737459)=9 \end{array} \right\} \text{Colisión}$$



0	█
1	█
2	█
3	█
4	█
5	█
6	█
7	█
8	█
9	█

Teoría de números

Tablas Hash

- Dado un **código** k , para conocer el sitio donde se almacena, se utiliza la función:

$$h(k) = k \bmod 10$$

$$h(0509555)=5$$

$$h(0817449)=9$$

$$h(0737459)=9$$

A pesar de las colisiones la búsqueda es rápida

0	_____
1	_____
2	_____
3	_____
4	_____
5	_____
6	_____
7	_____
8	_____
9	_____

Teoría de números

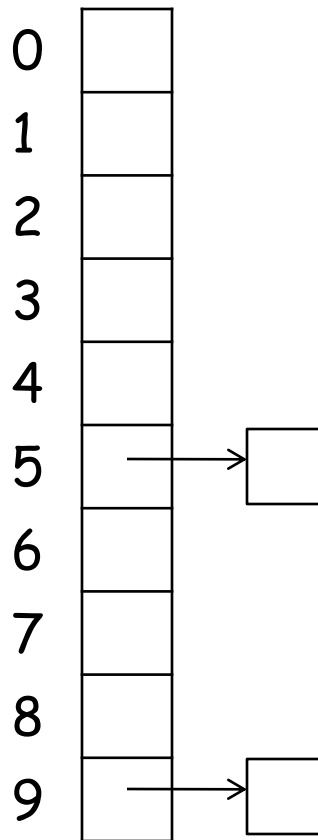
Tablas Hash

0	
1	
2	
3	
4	
5	
6	
7	
8	
9	

La función $h(k)=k \bmod 10$ indica en cuál espacio del arreglo colocar el dato k

Teoría de números

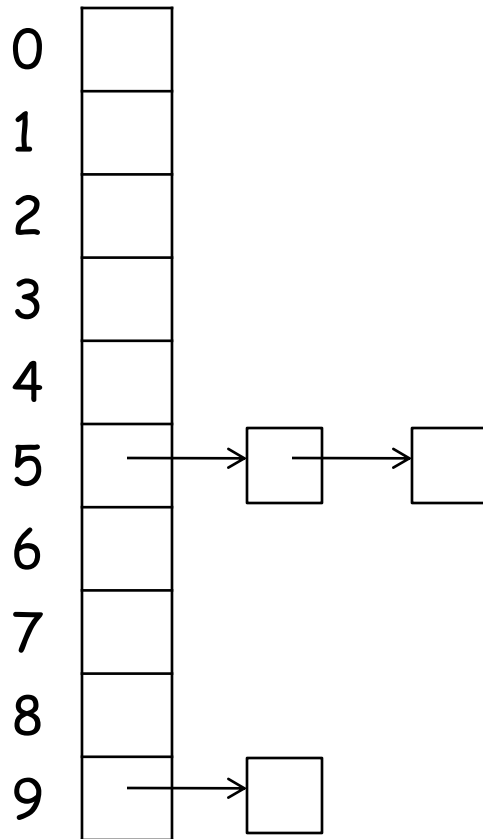
Tablas Hash



La función $h(k)=k \bmod 10$ indica en cuál espacio del arreglo colocar el dato k

Teoría de números

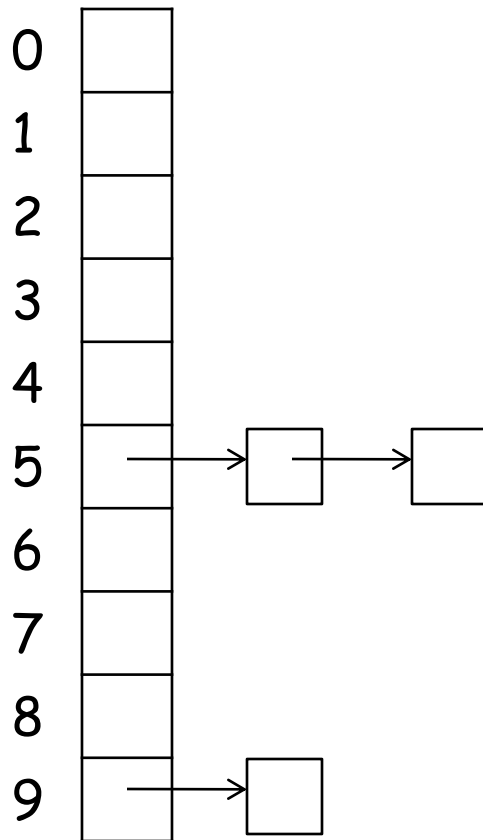
Tablas Hash



Para **resolver** la **colisión** se utiliza una lista en cada espacio del arreglo

Teoría de números

Tablas Hash



Una **tabla hash** permite ordenar los datos de tal forma que la recuperación sea rápida

Teoría de números

Criptología

Teoría de números

Julio Cesar

- Uno de los más destacados líderes militares y políticos romanos
- Sus conquistas extendieron el dominio romano sobre los territorios que hoy integran Francia, Bélgica, Holanda y parte de Alemania



(100a.c - 44a.c)

Teoría de números

Escitala Espartana

- Usada en la antigua Grecia en el año 400a.c
- Se enrolla una cinta sobre un vara
- El ancho con el cual fue escrito el mensaje corresponde con la vara adecuada para descifrar el mensaje



E
N
R
S
T
D
T
E
I
U
O
S
D
V
C
I
A
R
E
A
E
B
P
T
A
E
A
S
R
S
T
D
A
E



E
N
R
S
T
D
T
E
I
U
O
S
D
V
C
I
A
R
E
A
E
B
P
T
A
E
A
S
R
S
T
D
A
E

E R T T I O D C A E E P A A R T A
N S D E U S V I R A B T E S S D E

ENRSTUEIUOSDVCIAREAEPTAEASRSSTDAE



E
N
R
S
T
D
T
E
I
U
O
S
D
V
C
I
A
R
E
A
E
B
P
T
A
E
A
S
R
S
T
D
A
E

E S T U D I E B A S T A
N T E O V A A P E R D E
R D I S C R E T A S

Teoría de números

Criptología

- Es el estudio de técnicas que permitan **transformar** un mensaje en otro, que oculta el significado del original

Teoría de números

Método de Julio Cesar

1. Transforme cada letra a un número, para ello, utilice la posición relativa en el alfabeto. A es 0, B es 1, C es 2 ...
2. Aplique la función $f(p) = (p+3) \bmod 26$ para cada número
3. Transforme cada número a letra y envíe el mensaje

q - 6
6 → 0

q = Z
6 = X
c = 0

El profesor es muy bueno
ca usxgc ct buqu

Teoría de números

Método de Julio Cesar

1. Transforme cada letra a un número, para ello, utilice la posición relativa en el alfabeto. A es 0, B es 1, C es 2 ...
2. Aplique la función $f(p) = (p+3) \bmod 26$ para cada número
3. Transforme cada número a letra y envíe el mensaje

Para **decodificar** el mensaje

1. Transforme cada letra a número
2. Utilice la función $f^{-1}(p) = (p-3) \bmod 26$

Teoría de números

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

Teoría de números

- Encriptar el mensaje "HOLA"
- Encriptar el mensaje "MUERTE"
- Desencriptar el mensaje "HVWXGLHRYDDSHUGHU"

Teoría de números

- Encriptar el mensaje "HOLA"

$$f(p) = (p+3) \bmod 26$$

$$f(7) = 10 \bmod 26 = 10$$

$$f(14) = 17 \bmod 26 = 17$$

$$f(11) = 14 \bmod 26 = 14$$

$$f(0) = 3 \bmod 26 = 3$$

- El mensaje encriptado es "KROD"

Teoría de números

- Desencriptar el mensaje "HVWXGLHRYDDSHUGHU"

	H	V	W	X	G	L	H	R	Y	D	D	S	H	U	G	H	U
p	7	21	22	23	6	11	7	17	24	3	3	18	7	20	6	7	20
$f^{-1}(p)$	4	18	19	20	3	8	4	14	21	0	0	15	4	17	3	4	17
	E	S	T	U	D	I	E	O	V	A	A	P	E	R	D	E	R

Teoría de números

- Calcule los siguientes módulos:

• $-19 \bmod 7 \leftarrow 2$

• $-127 \bmod 4 \leftarrow 1$

- Indique si se presenta cada una de las siguientes congruencias. Justifique sus respuestas

• $52 \equiv 31 \bmod 7$

$52 \bmod 7 = 31 \bmod 7$
 $3 = 3$

$7 \mid (52 - 31) \checkmark$
 21

• $-31 \equiv 60 \bmod 7$

$-31 \bmod 7 = 60 \bmod 7$
 $4 = 4$

$7 \mid (-31 - 60) \checkmark$
 -91