

Matemáticas Discretas

Oscar Bedoya

`oscar.bedoya@correounivalle.edu.co`

- * Aritmética modular
- * Congruencia lineal

Teoría de números

Aritmética modular

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

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

division entera

$$5 \bmod 2 = 1$$

$$5 \div 2 = 2$$

$$5 = 2 \times 2 + R$$

$$R = 5 - 2 \times 2 = 1$$

Teoría de números

Aritmética modular

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

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

Exacta



- $0 \leq a \bmod \textcircled{b} < b$

$10 \bmod 5$ 0, 1, 2, 3, $\textcircled{4}$

$$10 \div 5 = 2$$

$$5 \times 2 + R = 10 \quad R = 0$$

$$9 \bmod 5 \quad 9 \div 5 = 1$$
$$R = 4$$

Teoría de números

- $17 \bmod 5 = 2$

- $9 \bmod 4 = 1$

- $-7 \bmod 3 = 2$

- $2 \bmod 2 = 0$

- $-5 \bmod 2 = 1 \rightarrow 2 \times (-3) + 1 = -5$

$$17 \text{ div } 5 = 3$$

$$9 \text{ div } 4 = 2$$

$$-7 \text{ div } 3 = -3$$

$$17 = \overset{15}{5 \times 3} + R$$

$$9 = 2 \times 4 + \textcircled{R}$$

$$-7 = 3 \times (-3) + R$$

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:

• $-21 \bmod 9 = 6$ ✓

$$9(-3) + R = -21$$

$$-27 + \overset{6}{\textcircled{R}} = -21$$

• $4 \bmod 2 = 0$

• $2 \bmod 4 = 2$

$$2 = 4(0) + R \quad R = 2$$

• $-12 \bmod 5 = 3$

Teoría de números

Calcule los siguientes módulos:

- $-21 \bmod 9 = 6$
- $4 \bmod 2 = 0$
- $2 \bmod 4 = 2$
- $-12 \bmod 5 = 3$

Teoría de números

Calcule los siguientes módulos:

- $-34 \bmod 4 = 2$ $4(-9) + R = -34$ $-36 + 2 = -34$
- $7 \bmod 9 = 7$
- $73 \bmod 8 = 1$
- $-24 \bmod 7 = 4$

Teoría de números

Calcule los siguientes módulos:

- $-34 \bmod 4 = 2$
- $7 \bmod 9 = 7$
- $73 \bmod 8 = 1$
- $-24 \bmod 7 = 4$

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:

$$7 \equiv 2 \pmod{5}$$

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

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

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

Teoría de números

Indique cuáles de las siguientes afirmaciones son ciertas:

- $2 \equiv 20 \pmod{6}$ $2 \pmod{6} = 20 \pmod{6}$ $2=2$ V
- $5 \equiv 16 \pmod{3}$ $5 \pmod{3} = 16 \pmod{3}$ $3 \neq 1$ F

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:

• $-7 \equiv -19 \pmod{4}$

$$\underline{-7} \pmod{4} = \underline{-19} \pmod{4}$$

$$1 = 1 \checkmark$$

• $3 \equiv 38 \pmod{7}$

$$3 \pmod{7} = 38 \pmod{7}$$

$$3 = 3 \checkmark$$

• $-5 \equiv 5 \pmod{5}$

$$5 \pmod{5} = \underline{-5} \pmod{5}$$

$$0 = 0 \checkmark$$

$$m \mid (a - b)$$

$$0 \leq a \pmod{b} < b$$

$$4 \mid (-7 + 19)$$

$$4 \mid 12 \checkmark$$

$$7 \mid (3 - 38)$$

$$7 \mid -35 \checkmark$$

$$5 \mid (-5 - 5)$$

$$5 \mid -10 \checkmark$$

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

Propiedades

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

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

- 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 $a \cdot c = b$

- $a|b$, 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

Propiedades

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

Teoría de números

Propiedades

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

- $2 \equiv 20 \pmod{6}$

$$6 \mid (2 - 20)$$

$$6 \mid -18 \checkmark$$

- $16 \equiv 4 \pmod{12}$

$$12 \mid (16 - 4)$$

$$12 \mid 12 \checkmark$$

- $38 \equiv 3 \pmod{7}$

$$7 \mid (38 - 3)$$

$$7 \mid 35 \checkmark$$

- $-5 \equiv 5 \pmod{5}$

$$5 \mid (-5 - 5)$$

$$5 \mid -10$$

Teoría de números

Indique si se presenta cada una de las siguientes congruencias:

• $-29 \equiv 5 \pmod{17}$

$$17 \nmid (-29 - 5)$$

$$17 \nmid -34 \quad \checkmark$$

• $-122 \equiv 5 \pmod{17}$

$$17 \nmid (-122 - 5)$$

$$17 \nmid -127 \quad \times$$

• $226 \equiv 5 \pmod{17}$

$$17 \nmid (226 - 5)$$

$$17 \nmid 221 \quad \checkmark$$

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 $17 \mid (226-5)$

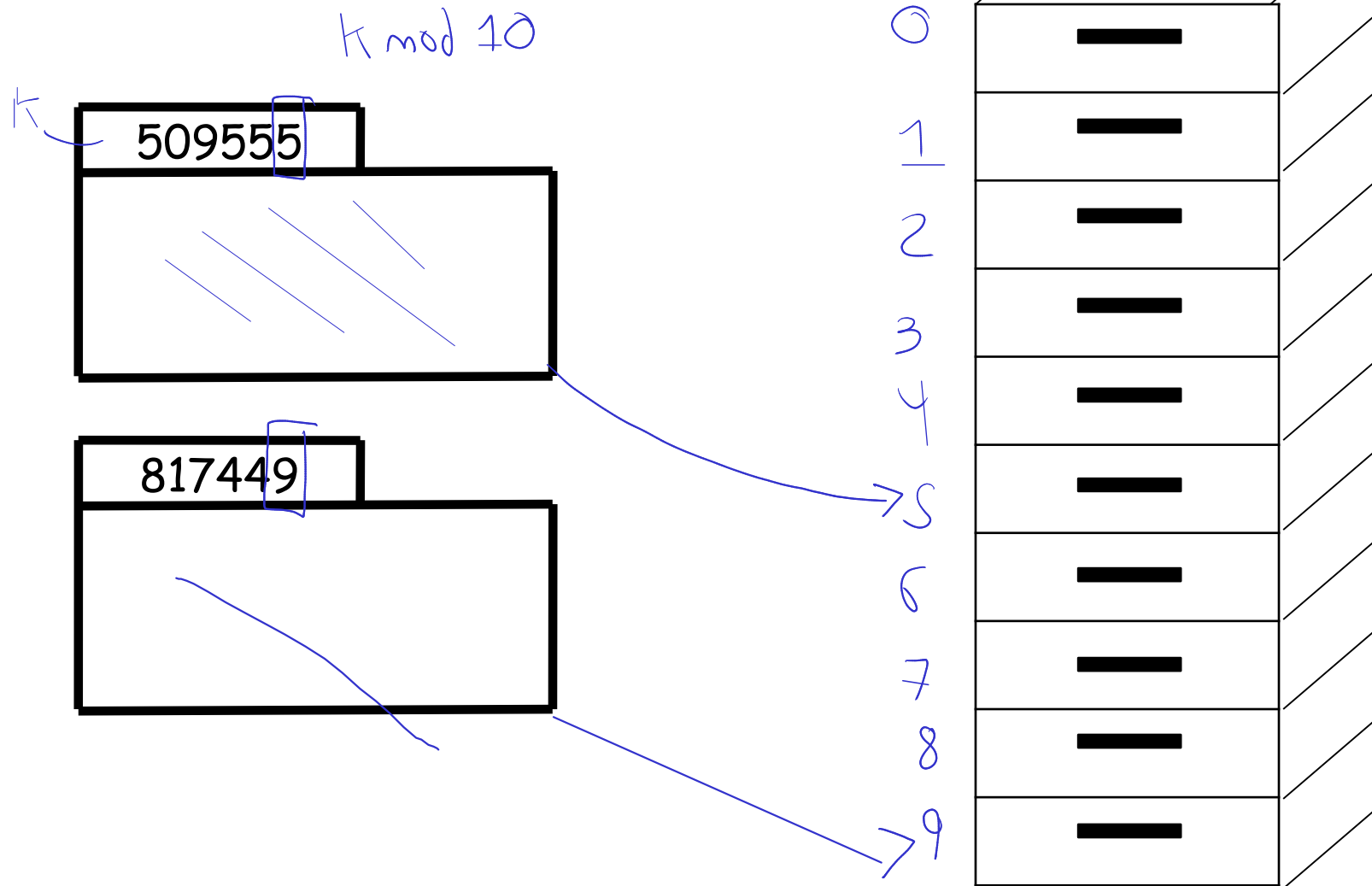
Teoría de números

Aplicación

- Tablas Hash
- Criptología

Teoría de números

Tablas Hash

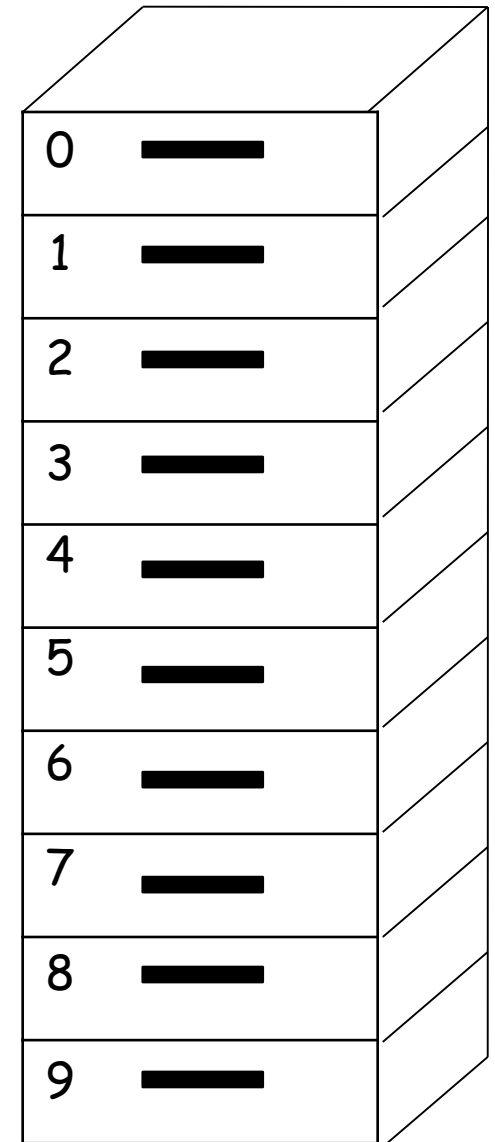


Teoría de números

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:

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

509555

817449

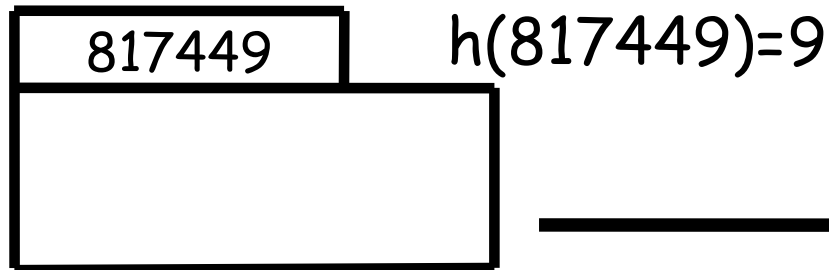
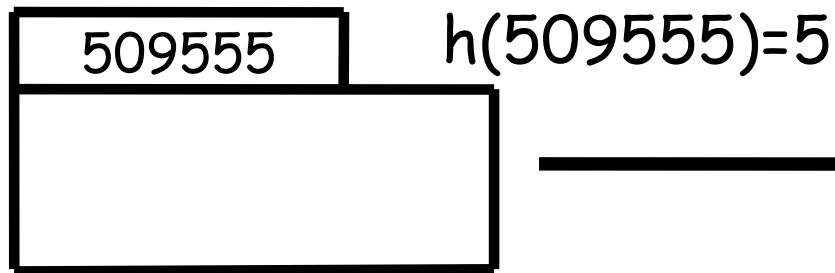
0	_____
1	_____
2	_____
3	_____
4	_____
5	_____
6	_____
7	_____
8	_____
9	_____

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

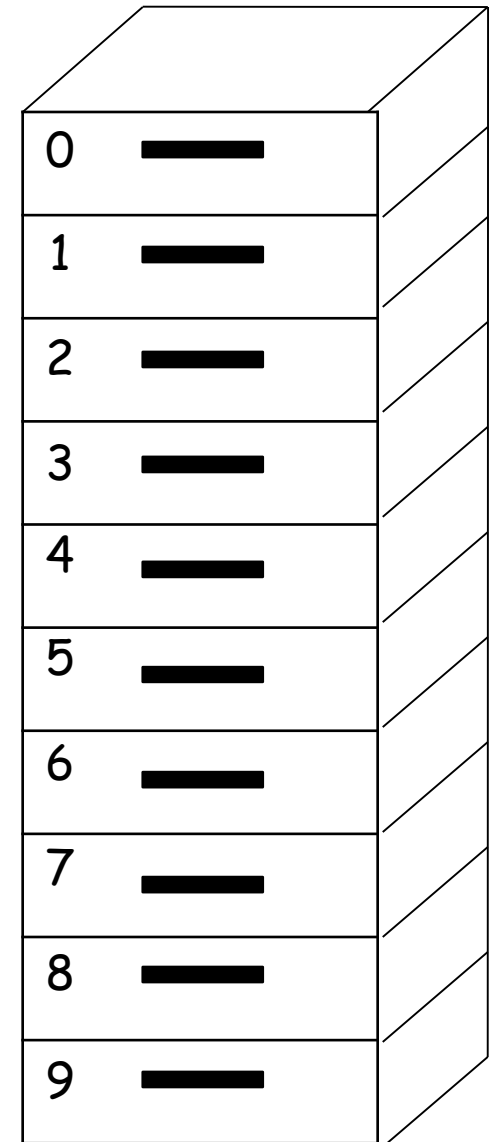
Tablas Hash

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

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

$$h(509555)=5$$

$$h(817449)=9$$



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

Teoría de números

Tablas Hash

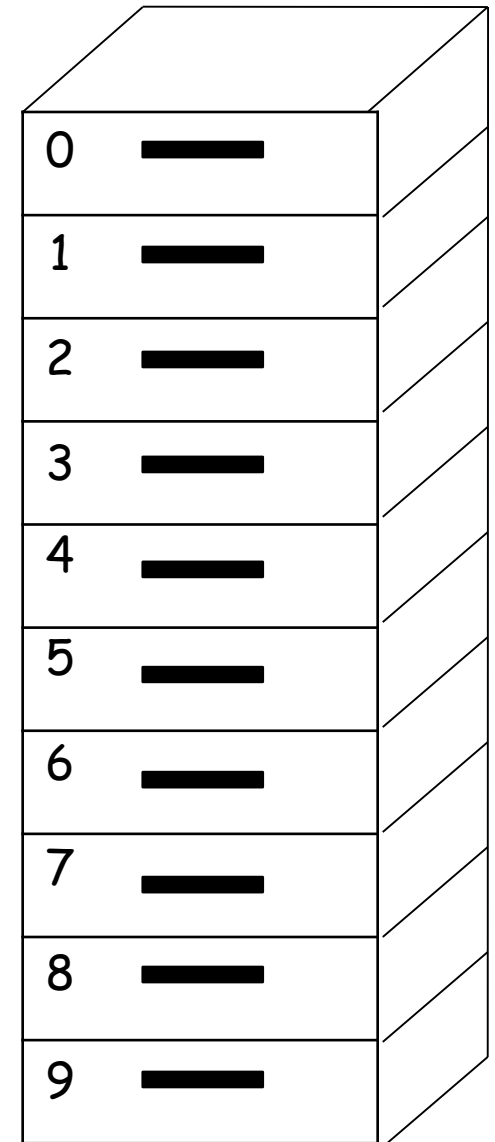
- Dado un **código** k , para conocer el sitio donde se almacena, se utiliza la función:

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

$$h(509555)=5$$

$$h(817449)=9$$

$$h(737459)=?$$



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

Teoría de números

Tablas Hash

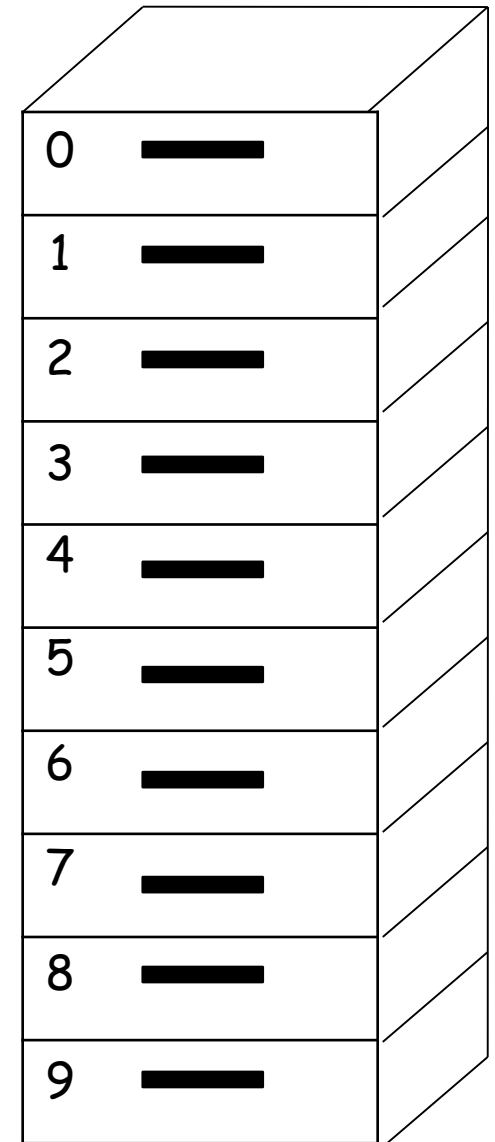
- Dado un **código** k , para conocer el sitio donde se almacena, se utiliza la función:

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

$$h(509555)=5$$

$$h(817449)=9$$

$$h(737459)=9$$



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:

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

$$h(509555)=5$$

$$\left. \begin{array}{l} h(817449)=9 \\ h(737459)=9 \end{array} \right\} \text{Colisión}$$

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:

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

$$h(509555)=5$$

$$h(817449)=9$$

$$h(737459)=9$$

A pesar de las
colisiones la
búsqueda es rápida

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

Teoría de números

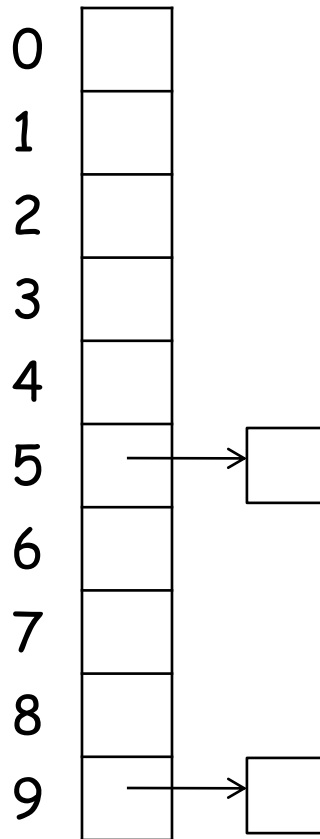
Tablas Hash

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

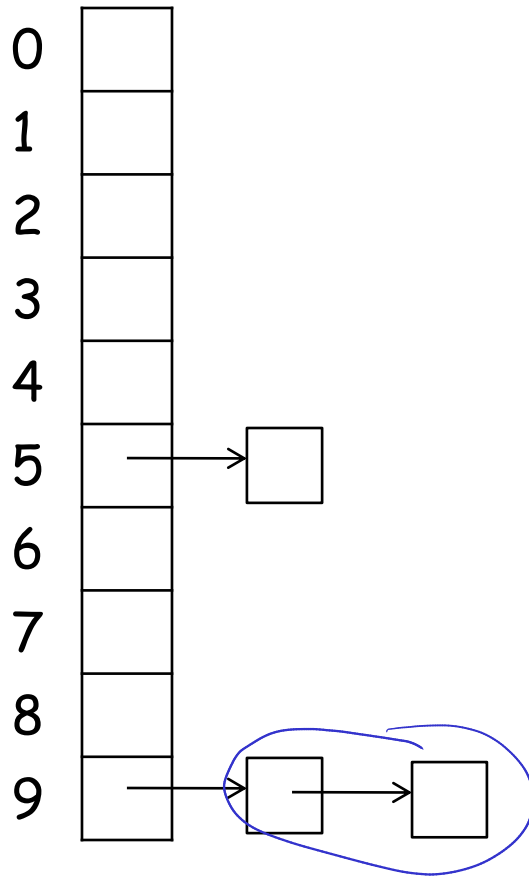
Tablas Hash



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

Teoría de números

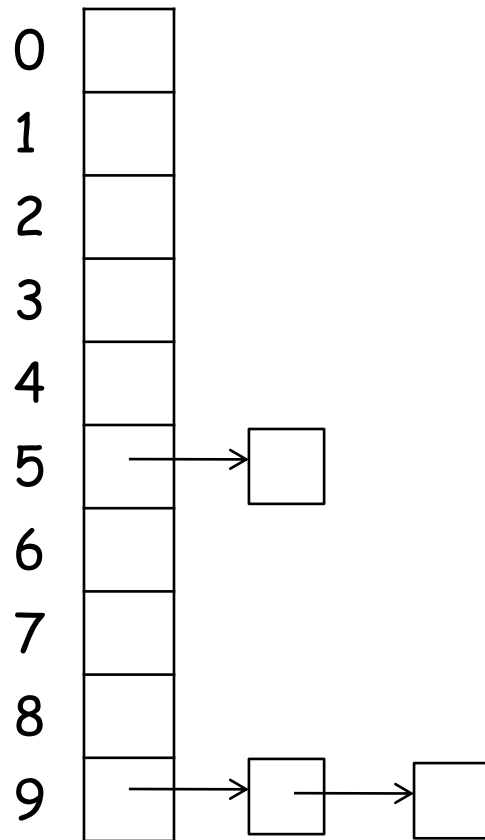
Tablas Hash



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

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



$a \rightarrow b$ $b \rightarrow c$ $z \rightarrow a$

Hola como estas

Gpmb dnp ftubt

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

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



ENRSTDT EIUOSDVCIAREAE BPTAEASRSTDAE

ESTUDIEBASTA
NTEOVAAPERTD
RDISCRETAS

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

ingles $\tilde{n} \rightarrow 27$

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

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

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

$$7 + 3 \bmod 26 \quad 10 \bmod 26 = 10$$

- Encriptar el mensaje "HOLA" K
- 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:
 - $-19 \bmod 7$
 - $-127 \bmod 4$
- Indique si se presenta cada una de las siguientes congruencias. Justifique sus respuestas
 - $52 \equiv 31 \bmod 7$
 - $-31 \equiv 60 \bmod 7$

Resumen

$a \bmod b$ Residuo de la división entre a y $b \rightarrow a/b$

Congruencia $a \equiv b \bmod m$ si $a \bmod m = b \bmod m$

$0 \leq a \bmod b < b$

Si $a \equiv b \bmod m$, que $m \mid (a-b)$

- * Algoritmo de Euclides
- * Combinación lineal
- * Inverso de a mod m

Teoría de números

Algoritmo de Euclides

```
public int mcd(int a, int b){  
    x=a;  
    y=b;  
    int x, r;  
    while (y != 0){  
        r= x mod y;  
        x= y;  
        y= r;  
    }  
    return x;  
}
```


Teoría de números

Aplicar el algoritmo de Euclides para encontrar $\text{mcd}(287, 91)$

Teoría de números

Aplicar el algoritmo de Euclides para encontrar $\text{mcd}(287, 91)$

$$\begin{array}{r|l} 287 & 91 \end{array}$$

Teoría de números

Aplicar el algoritmo de Euclides para encontrar $\text{mcd}(287, 91)$

$$\begin{array}{r|l} 287 & 91 \\ - 273 & 3 \\ \hline 14 & \end{array}$$

Teoría de números

Aplicar el algoritmo de Euclides para encontrar $\text{mcd}(287, 91)$

- $287 = 91 \cdot 3 + 14$

$$287 \bmod 91 = 14$$

$$91 \bmod 14 = 7$$

$$14 \bmod 7 = 0 \quad \text{mcd}(287, 91)$$

Teoría de números

Aplicar el algoritmo de Euclides para encontrar $\text{mcd}(287, 91)$

- $287 = 91 \cdot 3 + 14$

$$\begin{array}{c} \swarrow \quad \nwarrow \\ 91 = 14 \cdot ? + ? \end{array}$$

$\text{mcd } 7$

Teoría de números

Aplicar el algoritmo de Euclides para encontrar $\text{mcd}(287, 91)$

- $287 = 91 \cdot 3 + 14$

$$\begin{array}{c} \swarrow \quad \nwarrow \\ 91 = 14 \cdot 6 + 7 \end{array}$$

Teoría de números

Aplicar el algoritmo de Euclides para encontrar $\text{mcd}(287, 91)$

- $287 = 91 \cdot 3 + 14$

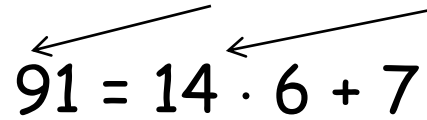
$$91 = 14 \cdot 6 + 7$$

$$14 = 7 \cdot ? + ?$$

Teoría de números

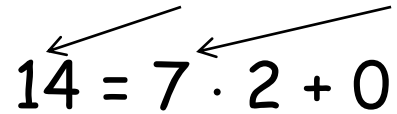
Aplicar el algoritmo de Euclides para encontrar $\text{mcd}(287, 91)$

- $287 = 91 \cdot 3 + 14$



$91 = 14 \cdot 6 + 7$

The diagram shows two arrows pointing from the right side of the first equation to the left side of the second equation. One arrow points from the '14' to the '14' in the second equation. The other arrow points from the '91' to the '14' in the second equation.



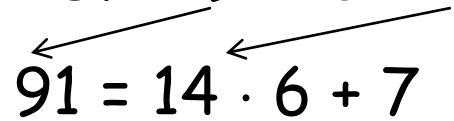
$14 = 7 \cdot 2 + 0$

The diagram shows two arrows pointing from the right side of the second equation to the left side of the third equation. One arrow points from the '7' to the '7' in the third equation. The other arrow points from the '14' to the '14' in the third equation.

Teoría de números

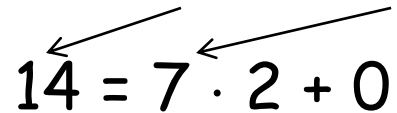
Aplicar el algoritmo de Euclides para encontrar $\text{mcd}(287, 91)$

- $287 = 91 \cdot 3 + 14$



$91 = 14 \cdot 6 + 7$

The diagram shows an arrow pointing from the '14' in the first equation to the '14' in the second equation, and another arrow pointing from the '91' in the first equation to the '91' in the second equation.



$14 = 7 \cdot 2 + 0$

The diagram shows an arrow pointing from the '14' in the second equation to the '14' in the third equation, and another arrow pointing from the '14' in the second equation to the '7' in the third equation.

Se toma el último residuo diferente de 0, en este caso,
 $\text{mcd}(287, 91) = 7$

Teoría de números

Aplicar el algoritmo de Euclides para encontrar $\text{mcd}(91, 287)$

$$91 \bmod 287 = 91$$

↙

$$287 \bmod 91$$

}

$$7$$

Teoría de números

Aplicar el algoritmo de Euclides para encontrar $\text{mcd}(91, 287)$

$$\text{mcd}(\underline{91}, \underline{287}) = 7$$

$$287 \bmod 91$$

- Para aplicar el algoritmo de Euclides se inicia **siempre** dividiendo el mayor (287) entre el menor (91)

$$287 = 91 \cdot 3 + 14$$

$$91 = 14 \cdot 6 + 7$$

$$14 = 7 \cdot 2 + 0$$

Teoría de números

Aplicar el algoritmo de Euclides para encontrar:

- $\text{mcd}(342, 76)$

$$342 \bmod 76 = 38$$

$$76 \bmod 38 = 0$$

$$\text{mcd}(342, 76) = 38$$

Teoría de números

- $\text{mcd}(342, 76)$

$$342 = 76 \cdot 4 + 38$$

$$76 = 38 \cdot 2 + 0$$

- $\text{mcd}(342, 76) = 38$

Teoría de números

Aplicar el algoritmo de Euclides para encontrar:

- $\text{mcd}(48, 512) = 6$

$$512 \bmod 48 = 32$$

$$48 \bmod 32 = 16$$

$$32 \bmod 16 = 0$$

Teoría de números

- $\text{mcd}(48, 512)$

$$512 = 48 \cdot 10 + 32$$

$$48 = 32 \cdot 1 + 16$$

$$32 = 16 \cdot 2 + 0$$

- $\text{mcd}(48, 512) = 16$

Teoría de números

Aplicar el algoritmo de Euclides para encontrar:

- $\text{mcd}(252, 198) = 18$

Handwritten steps of the Euclidean algorithm:

- $252 \bmod 198 = 54$ (198 is circled, 54 is boxed)
- $198 \bmod 54 = 36$ (54 is boxed, 36 is boxed)
- $54 \bmod 36 = 18$ (36 is circled)
- $36 \bmod 18 = 0$

Blue lines connect the circled numbers to the next step: 198 to 54, 54 to 36, and 36 to 18.

Teoría de números

- $\text{mcd}(252, 198)$

$$252 = 198 \cdot 1 + 54$$

$$198 = 54 \cdot 3 + 36$$

$$54 = 36 \cdot 1 + 18$$

$$36 = 18 \cdot 2$$

- **$\text{mcd}(252, 198) = 18$**

$$\text{mod}(345, 155) = 5$$

$$345 \text{ mod } 155 = 35$$

$$155 \text{ mod } 35 = 15$$

$$35 \text{ mod } 15 = 5$$

$$15 \text{ mod } 5 = 0$$

Teoría de números

Teorema: si a y b son enteros positivos, entonces existen enteros s y t tales que $\text{mcd}(a,b)=a \cdot (s) + b \cdot (t)$

Teoría de números

Teorema: si a y b son enteros positivos, entonces existen enteros s y t tales que $\text{mcd}(a,b)=a \cdot (s) + b \cdot (t)$

El $\text{mcd}(a,b)$ se puede expresar como
una combinación lineal de a y b

Teoría de números

$$\text{mcd}(252, 198) = 18$$

Teoría de números

$$\text{mcd}(252,198) = 18 = 252 \cdot x + 198 \cdot y$$

Teoría de números

$$\text{mcd}(252,198) = 18 = 252 \cdot \underline{(4)} + 198 \cdot \underline{(-5)}$$

Teoría de números

- $\text{mcd}(252, 198)$

$$252 = 198 \cdot 1 + 54$$

$$198 = 54 \cdot 3 + 36$$

$$54 = 36 \cdot 1 + 18$$

$$36 = 18 \cdot 2$$

- $\text{mcd}(252, 198) = 18$

$$\text{mcd}(252, 198)$$

$$252 \bmod 198 = 54$$

$$198 \bmod 54 = 36$$

$$54 \bmod 36 = 18$$

$$36 \bmod 18 = 0$$

Teoría de números

- $\text{mcd}(252, 198)$

$$252 = 198 \cdot 1 + 54$$

$$54 = 252 - 198 \cdot 1$$

$$198 = 54 \cdot 3 + 36$$

$$36 = 198 - 54 \cdot 3$$

$$54 = 36 \cdot 1 + 18$$

$$18 = 54 - 36 \cdot 1$$

$$36 = 18 \cdot 2$$

- $\text{mcd}(252, 198) = 18$

Se despejan los residuos

Teoría de números

• $\text{mcd}(252, 198)$

252 = 198 · 1 + 54

54 = 252 - 198 · 1

198 = 54 · 3 + 36

36 = 198 - 54 · 3

54 = 36 · 1 + 18

* 18 = 54 - 36 · 1

36 = 18 · 2

• $\text{mcd}(252, 198) = 18$

Se reemplazan siempre en la ecuación que tiene al mcd

Teoría de números

- $\text{mcd}(252, 198)$

$$252 = 198 \cdot 1 + 54$$

$$54 = 252 - 198 \cdot 1$$

$$198 = 54 \cdot 3 + 36$$

$$54 = 36 \cdot 1 + 18$$

$$18 = 54 - (198 - 54 \cdot 3) \cdot 1$$

$$36 = 18 \cdot 2$$

- **$\text{mcd}(252, 198) = 18$**

Teoría de números

- $\text{mcd}(252, 198)$

$$252 = 198 \cdot 1 + 54$$

$$54 = 252 - 198 \cdot 1$$

$$198 = 54 \cdot 3 + 36$$

$$54 = 36 \cdot 1 + 18$$

$$18 = 54 - 198 \cdot 1 + 54 \cdot 3$$

$$36 = 18 \cdot 2$$

- $\text{mcd}(252, 198) = 18$

Teoría de números

- $\text{mcd}(252, 198)$

$$252 = 198 \cdot 1 + 54$$

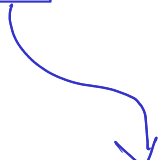
$$198 = 54 \cdot 3 + 36$$

$$54 = 36 \cdot 1 + 18$$

$$36 = 18 \cdot 2$$

- $\text{mcd}(252, 198) = 18$

$$\boxed{54} = 252 - 198 \cdot 1$$


$$18 = 54 \cdot 4 - 198 \cdot 1$$

Teoría de números

- $\text{mcd}(252, 198)$


$$252 = 198 \cdot 1 + 54$$

$$198 = 54 \cdot 3 + 36$$

$$54 = 36 \cdot 1 + 18$$

$$36 = 18 \cdot 2$$

$$54 = 252 - 198 \cdot 1$$


$$18 = 54 \cdot 4 - 198 \cdot 1$$

- $\text{mcd}(252, 198) = 18$

Teoría de números

- $\text{mcd}(252, 198)$

$$252 = 198 \cdot 1 + 54$$

$$198 = 54 \cdot 3 + 36$$

$$54 = 36 \cdot 1 + 18$$

$$18 = (252 - 198 \cdot 1) \cdot 4 - 198 \cdot 1$$

$$36 = 18 \cdot 2$$

- **$\text{mcd}(252, 198) = 18$**

Teoría de números

- $\text{mcd}(252, 198)$

$$252 = 198 \cdot 1 + 54$$

$$198 = 54 \cdot 3 + 36$$

$$54 = 36 \cdot 1 + 18$$

$$36 = 18 \cdot 2$$

$$18 = 252 \cdot 4 - 198 \cdot 4 - 198 \cdot 1$$

- **$\text{mcd}(252, 198) = 18$**

Teoría de números

- $\text{mcd}(252, 198)$

$$252 = 198 \cdot 1 + 54$$

$$198 = 54 \cdot 3 + 36$$

$$54 = 36 \cdot 1 + 18$$

$$18 = 252 \cdot 4 - 198 \cdot 5$$

$$36 = 18 \cdot 2$$

- **$\text{mcd}(252, 198) = 18$**

Teoría de números

- $\text{mcd}(252, 198)$

$$252 = 198 \cdot 1 + 54$$

$$198 = 54 \cdot 3 + 36$$

$$54 = 36 \cdot 1 + 18$$

$$36 = 18 \cdot 2$$

- $\text{mcd}(252, 198) = 18$

$$18 = 252 \cdot (4) + 198 \cdot (-5)$$

Handwritten blue annotations: a '4' with an 'x' above it and a '5' with a '-' sign above it, indicating the coefficients for the linear combination.

Teoría de números

- Exprese el $\text{mcd}(512, 48) = 16$ como una combinación lineal

$$512 = 48 \cdot 10 + 32$$

$$48 = 32 \cdot 1 + 16$$

$$32 = 16 \cdot 2 + 0$$

$$512 \bmod 48 = 32$$

$$48 \bmod 32 = 16$$

$$32 \bmod 16 = 0$$

$$32 = 512 - 48 \times 10$$

$$16 = 48 - \boxed{32} \times 1$$

$$16 = 48 - (512 - 48(10))$$

$$16 = 48 - 512 + 48(10)$$

$$16 = 48(11) + 512(-1)$$

Teoría de números

- Exprese el $\text{mcd}(512, 48) = 16$ como una combinación lineal

$$512 = 48 \cdot 10 + 32 \qquad 32 = 512 - 48 \cdot 10$$

$$48 = 32 \cdot 1 + 16 \qquad 16 = 48 - 32 \cdot 1$$

$$32 = 16 \cdot 2 + 0$$

Teoría de números

- Exprese el $\text{mcd}(512, 48) = 16$ como una combinación lineal

$$512 = 48 \cdot 10 + 32$$

$$48 = 32 \cdot 1 + 16$$

$$32 = 16 \cdot 2 + 0$$

$$16 = 48 - (512 - 48 \cdot 10) \cdot 1$$

$$16 = 48 - 512 \cdot 1 + 48 \cdot 10$$

$$16 = 48 \cdot 11 - 512 \cdot 1$$

$$16 = 48 \cdot (11) + 512 \cdot (-1)$$

Teoría de números

- Exprese el mcd(322, 51)=1 como una combinación lineal

$$322 = 51 \cdot 6 + \boxed{16}$$

$$51 = 16 \cdot 3 + \boxed{3}$$

$$\boxed{16 = 3 \cdot 5 + 1}$$

$$3 = 1 \cdot 3 + 0$$

$$\underline{1} = 322(\overset{\downarrow}{5}) + 51(\overset{\downarrow}{-7})$$

$$1 = 16 - 3 \times 5$$

$$1 = 16 - 5(51 - 16(3))$$

$$1 = 16 - 5(51) + 16(15)$$

$$1 = \boxed{16}(16) - 51(5)$$

$$1 = (76)(322 - 51(6)) - 51(5)$$

$$\underline{1} = (16)322 - 51(96) - 51(5)$$

$$1 = (16)322 + 51(-101)$$

Teoría de números

- Exprese el $\text{mcd}(322, 51) = 1$ como una combinación lineal

$$322 = 51 \cdot 6 + 16 \qquad 16 = 322 - 51 \cdot 6$$

$$51 = 16 \cdot 3 + 3 \qquad 3 = 51 - 16 \cdot 3$$

$$16 = 3 \cdot 5 + 1 \qquad 1 = 16 - 3 \cdot 5$$

$$3 = 1 \cdot 3 + 0$$

Teoría de números

- Exprese el $\text{mcd}(322, 51) = 1$ como una combinación lineal

$$322 = 51 \cdot 6 + 16$$

$$16 = 322 - 51 \cdot 6$$

$$51 = 16 \cdot 3 + 3$$

$$3 = 51 - 16 \cdot 3$$

$$16 = 3 \cdot 5 + 1$$

$$1 = 16 - 3 \cdot 5$$

$$3 = 1 \cdot 3 + 0$$

$$1 = 322 \cdot (16) + 51 \cdot (-101)$$

Teoría de números

- Exprese el $\text{mcd}(235,37)=1$ como una combinación lineal

$$235 = 37 \cdot 6 + 13$$

$$37 = 13 \cdot 2 + 11$$

$$13 = 11 \cdot 1 + 2$$

$$11 = 2 \cdot 5 + 1$$

$$2 = 1 \cdot 2 + 0$$

Teoría de números

- Exprese el $\text{mcd}(235,37)=1$ como una combinación lineal

$$235 = 37 \cdot 6 + 13 \qquad 13 = 235 - 37 \cdot 6$$

$$37 = 13 \cdot 2 + 11 \qquad 11 = 37 - 13 \cdot 2$$

$$13 = 11 \cdot 1 + 2 \qquad 2 = 13 - 11 \cdot 1$$

$$11 = 2 \cdot 5 + 1 \qquad 1 = 11 - 2 \cdot 5$$

$$2 = 1 \cdot 2 + 0$$

Teoría de números

- Exprese el $\text{mcd}(235,37)=1$ como una combinación lineal

$$235 = 37 \cdot 6 + 13 \qquad 13 = 235 - 37 \cdot 6$$

$$37 = 13 \cdot 2 + 11 \qquad 11 = 37 - 13 \cdot 2$$

$$13 = 11 \cdot 1 + 2$$

$$11 = 2 \cdot 5 + 1 \qquad 1 = 11 - 13 \cdot 5 + 11 \cdot 5 = 11 \cdot 6 - 13 \cdot 5$$

$$2 = 1 \cdot 2 + 0$$

Teoría de números

- Exprese el $\text{mcd}(235,37)=1$ como una combinación lineal

$$235 = 37 \cdot 6 + 13 \qquad 13 = 235 - 37 \cdot 6$$

$$37 = 13 \cdot 2 + 11$$

$$13 = 11 \cdot 1 + 2$$

$$11 = 2 \cdot 5 + 1$$

$$1 = 37 \cdot 6 - 13 \cdot 12 - 13 \cdot 5 = 37 \cdot 6 - 13 \cdot 17$$

$$2 = 1 \cdot 2 + 0$$

Teoría de números

- Exprese el $\text{mcd}(235,37)=1$ como una combinación lineal

$$235 = 37 \cdot 6 + 13$$

$$37 = 13 \cdot 2 + 11$$

$$13 = 11 \cdot 1 + 2$$

$$11 = 2 \cdot 5 + 1$$

$$2 = 1 \cdot 2 + 0$$

$$1 = 37 \cdot 6 - (235 - 37 \cdot 6) \cdot 17$$

Teoría de números

- Exprese el $\text{mcd}(235,37)=1$ como una combinación lineal

$$235 = 37 \cdot 6 + 13$$

$$37 = 13 \cdot 2 + 11$$

$$13 = 11 \cdot 1 + 2$$

$$11 = 2 \cdot 5 + 1$$

$$2 = 1 \cdot 2 + 0$$

$$1 = 37 \cdot 6 - 235 \cdot 17 + 37 \cdot 102$$

$$1 = 37 \cdot 108 - 235 \cdot 17$$

$$1 = 37 \cdot (108) + 235 \cdot (-17)$$

Teoría de números

- Exprese el $\text{mcd}(426, 37)$ como una combinación lineal

$$\text{mcd}(426, 37) = \underline{\hspace{1cm}} = 426 \cdot (\underline{\hspace{1cm}}) + 37 \cdot (\underline{\hspace{1cm}})$$

$$426 \bmod 37 = 19$$

$$426 = 37 \times 11 + 19$$

$$37 \bmod 19 = 18$$

$$37 = 19 \times 1 + 18$$

$$19 \bmod 18 = 1$$

$$* 19 = 18 \times 1 + 1$$

$$18 \bmod 1 = 0$$

$$1 = 19 - 18(1)$$

$$1 = 19 - (37 - 19(1))$$

$$1 = (2)19 - 37$$

$$1 = (2)(426 - 37(11)) - 37$$

$$1 = (2)426 + 37(-23)$$

Teoría de números

El inverso de a mod m

- Dado a mod m , su inverso se denota como \overline{a}

Teoría de números

El inverso de a mod m

- Dado a mod m , su inverso se denota como \overline{a}
- Se cumple que $\overline{a} \cdot a \equiv 1 \pmod{m}$

Teoría de números

El inverso de $a \bmod m$

- Dado $a \bmod m$, su inverso se denota como \overline{a}
- Se cumple que $\overline{a} \cdot a \equiv 1 \pmod{m}$

Se tiene $3 \bmod 7$

$$\overline{a} = -2$$

Se puede verificar que:

$$(-2) \cdot 3 \equiv 1 \pmod{7}$$

Teoría de números

El inverso de a mod m

- Solo existe un inverso si $\text{mcd}(a,m)=1$

Teoría de números

El inverso de $a \bmod m$

- Para encontrar \overline{a} , calcule $\text{mcd}(a,m)$, debe ser 1
- Expresa $\text{mcd}(a,m)=1$ como una combinación lineal

$$1 = a \cdot (s) + m \cdot (t)$$

- El coeficiente que acompaña a a , es decir s , es el inverso \overline{a}

Teoría de números

$a \bmod m$

- Encuentre el inverso de **235 mod 37**

1) $\text{mcd}(235, 37) = 1 \quad \checkmark$

2) $1 = 235(s) + 37(t)$

\overline{a}

$$a \times \overline{a} \equiv 1 \bmod m$$

Teoría de números

- Encuentre el inverso de $235 \bmod 37$

$$235 = 37 \cdot 6 + 13$$

$$37 = 13 \cdot 2 + 11$$

$$13 = 11 \cdot 1 + 2$$

$$11 = 2 \cdot 5 + 1$$

$$2 = 1 \cdot 2 + 0$$

$$235 \bmod 37 = 13$$

$$37 \bmod 13 = 11$$

$$13 \bmod 11 = 2$$

$$11 \bmod 2 = 1$$

$$2 \bmod 1 = 0$$

Teoría de números

- Encuentre el inverso de **235 mod 37**

$$235 = 37 \cdot 6 + 13$$

$$37 = 13 \cdot 2 + 11$$

$$13 = 11 \cdot 1 + 2$$

$$11 = 2 \cdot 5 + 1$$

$$2 = 1 \cdot 2 + 0$$

$$1 = 37 \cdot (108) + 235 \cdot (-17)$$

Teoría de números

- Encuentre el inverso de 235 mod 37

$$235 = 37 \cdot 6 + 13$$

$$37 = 13 \cdot 2 + 11$$

$$13 = 11 \cdot 1 + 2$$

$$11 = 2 \cdot 5 + 1$$

$$2 = 1 \cdot 2 + 0$$

$$1 = 37 \cdot (108) + 235 \cdot (-17)$$

El coeficiente que acompaña a 235, es decir -17, es el inverso de 235 mod 37

Teoría de números

- $\text{mcd}(235, 37) = 1$
- $1 = 235 \cdot (-17) + 37 \cdot (108)$
- **-17 es el inverso de 235 mod 37**

Teoría de números

- Se puede verificar que

$$\overline{a} \cdot a \equiv 1 \pmod{m}$$

ya que

$$-17 \cdot 235 \equiv 1 \pmod{37}$$

$$-3995 \equiv 1 \pmod{37}$$

$$-3995 \bmod 37 = 1 \bmod 37$$

$$-3995 = 37(-108) + \boxed{1}$$

$$1 = 37(0) + \boxed{1}$$

Teoría de números

- Encuentre el inverso de 3 mod 7

$$1) \text{ mcd}(3, 7) = 1$$

$$2) 3(s) + 7(t) = 1$$

$\hookrightarrow \bar{a}$

$$3) 3 \times \bar{a} \equiv 1 \pmod{7}$$

$$3 \times (-2) \equiv 1 \pmod{7}$$

$$\rightarrow 6 \equiv 1 \pmod{7}$$

$$7 \pmod{3} = 1 \quad 7 = 3(2) + 1$$
$$3 \pmod{1} = 0$$

$$1 = 7 + 3(-2)$$

$$\boxed{\bar{a} = -2}$$

$$-6 \pmod{7} = 1$$

$$1 \pmod{7} = 1$$

Teoría de números

- Encuentre el inverso de 3 mod 7

$$7 = 3 \cdot 2 + 1$$

$$3 = 1 \cdot 3 + 0$$

Teoría de números

- Encuentre el inverso de 3 mod 7

$$7 = 3 \cdot 2 + 1$$

$$3 = 1 \cdot 3 + 0$$

- Se verifica que $\text{mcd}(7,3)=1$

Teoría de números

- Encuentre el inverso de 3 mod 7

$$7 = 3 \cdot 2 + 1$$

$$3 = 1 \cdot 3 + 0$$

- Se verifica que $\text{mcd}(7,3)=1$. Ahora se expresa como combinación lineal

Teoría de números

- Encuentre el inverso de 3 mod 7

$$7 = 3 \cdot 2 + 1$$

$$3 = 1 \cdot 3 + 0$$

- Se verifica que $\text{mcd}(7,3)=1$. Ahora se expresa como combinación lineal

$$1 = 7 - 3 \cdot 2$$

$$1 = 3 \cdot (-2) + 7 \cdot (1)$$

- El inverso de 3 mod 7 es -2

Teoría de números

- Encuentre el inverso de $7 \bmod 3$

Teoría de números

- Encuentre el inverso de $7 \bmod 3$

$$7 = 3 \cdot 2 + 1$$

$$3 = 1 \cdot 3 + 0$$

- Se verifica que $\text{mcd}(7,3)=1$. Ahora se expresa como combinación lineal

$$1 = 7 - 3 \cdot 2$$

$$1 = 3 \cdot (-2) + 7 \cdot (1)$$

- El inverso de $7 \bmod 3$ es 1

Teoría de números

Encuentre el inverso de:

- $5 \bmod 7$

Teoría de números

- Encuentre el inverso de **5 mod 7**

$$7 = 5 \cdot 1 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 1 \cdot 2 + 0$$

- Se verifica que $\text{mcd}(5,7)=1$. Ahora se expresa como combinación lineal

Teoría de números

- Encuentre el inverso de **5 mod 7**

$$7 = 5 \cdot 1 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 1 \cdot 2 + 0$$

- Se verifica que $\text{mcd}(5,7)=1$. Ahora se expresa como combinación lineal

$$1 = 5 \cdot (3) + 7 \cdot (-2)$$

Teoría de números

- Encuentre el inverso de **5 mod 7**

$$7 = 5 \cdot 1 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 1 \cdot 2 + 0$$

- Se verifica que $\text{mcd}(5,7)=1$. Ahora se expresa como combinación lineal

$$1 = 5 \cdot (3) + 7 \cdot (-2)$$

- El inverso de **5 mod 7** es 3

Teoría de números

Encuentre el inverso de:

- 3 mod 17

$$\gcd(3, 17) = 1$$

$$17 \bmod 3 = 2$$

$$3 \bmod 2 = 1$$

$$2 \bmod 1 = 0$$

$$17 = 3 \times 5 + 2$$

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

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

$$1 = 3 - (17 - 3(5))(1)$$

$$1 = 3(6) - 17$$

$$\overline{a} = 6$$

$$6 \times 3 \equiv 1 \bmod 17$$

$$18 \equiv 1 \bmod 17$$

$$\begin{array}{ccc} 18 \bmod 17 & = & 1 \bmod 17 \\ \downarrow & & \downarrow \\ 1 & & 1 \end{array}$$

Teoría de números

- Encuentre el inverso de 3 mod 17

$$17 = 3 \cdot 5 + 2$$

$$3 = 2 \cdot 1 + 1$$

$$2 = 1 \cdot 2 + 0$$

- Se verifica que $\text{mcd}(3,17)=1$. Ahora se expresa como combinación lineal

Teoría de números

- Encuentre el inverso de 3 mod 17

$$17 = 3 \cdot 5 + 2$$

$$3 = 2 \cdot 1 + 1$$

$$2 = 1 \cdot 2 + 0$$

- Se verifica que $\text{mcd}(3,17)=1$. Ahora se expresa como combinación lineal

$$\underline{1 = 3 \cdot (6) + 17 \cdot (-1)}$$

Teoría de números

- Encuentre el inverso de **3 mod 17**

$$17 = 3 \cdot 5 + 2$$

$$3 = 2 \cdot 1 + 1$$

$$2 = 1 \cdot 2 + 0$$

- Se verifica que $\text{mcd}(3,17)=1$. Ahora se expresa como combinación lineal

$$1 = 3 \cdot (6) + 17 \cdot (-1)$$

- El inverso de **3 mod 17** es 6

Teoría de números

- Encuentre el inverso de $7 \bmod 26$

Teoría de números

- Encuentre el inverso de $7 \bmod 26$

$$26 = 7 \cdot 3 + 5$$

$$7 = 5 \cdot 1 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 1 \cdot 2 + 0$$

- Se verifica que $\text{mcd}(26,7)=1$. Ahora se expresa como combinación lineal

Teoría de números

- Encuentre el inverso de $7 \bmod 26$

$$26 = 7 \cdot 3 + 5 \qquad 5 = 26 - 7 \cdot 3$$

$$7 = 5 \cdot 1 + 2 \qquad 2 = 7 - 5 \cdot 1$$

$$5 = 2 \cdot 2 + 1 \qquad 1 = 5 - 2 \cdot 2$$

$$2 = 1 \cdot 2 + 0$$

Teoría de números

- Encuentre el inverso de $7 \bmod 26$

$$26 = 7 \cdot 3 + 5 \qquad 5 = 26 - 7 \cdot 3$$

$$7 = 5 \cdot 1 + 2$$

$$5 = 2 \cdot 2 + 1 \qquad 1 = 5 - (7 - 5 \cdot 1) \cdot 2 = 5 \cdot 3 - 7 \cdot 2$$

$$2 = 1 \cdot 2 + 0$$

Teoría de números

- Encuentre el inverso de 7 mod 26

$$26 = 7 \cdot 3 + 5$$

$$7 = 5 \cdot 1 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 1 \cdot 2 + 0$$

$$1 = (26 - 7 \cdot 3) \cdot 3 - 7 \cdot 2$$

Teoría de números

- Encuentre el inverso de **7 mod 26**

$$26 = 7 \cdot 3 + 5$$

$$7 = 5 \cdot 1 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 1 \cdot 2 + 0$$

$$1 = 26 \cdot 3 - 7 \cdot 9 - 7 \cdot 2 = 26 \cdot 3 - 7 \cdot 11$$

$$1 = 26 \cdot (3) + 7 \cdot (-11)$$

Teoría de números

- Encuentre el inverso de **7 mod 26**

$$26 = 7 \cdot 3 + 5$$

$$7 = 5 \cdot 1 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$1 = 26 \cdot 3 - 7 \cdot 9 - 7 \cdot 2 = 26 \cdot 3 - 7 \cdot 11$$

$$2 = 1 \cdot 2 + 0$$

$$1 = 26 \cdot (3) + 7 \cdot (-11)$$

- Como $1 = 26 \cdot (3) + 7 \cdot (-11)$, el inverso de **7 mod 26** es **-11**

Teoría de números

> Encuentre el inverso de:

• 9 mod 32

$$\underline{9 \bmod m \equiv 1}$$

$$1) \gcd(9, 32)$$

$$\bullet 32 \bmod 9 = 5$$

$$32 = 9(3) + 5$$

$$\bullet 9 \bmod 5 = 4$$

$$9 = 5(1) + 4$$

$$5 \bmod 4 = 1$$

$$5 = 4(1) + 1$$

$$4 \bmod 1 = 0$$

$$\bar{a} = -7$$

$$1 < -63 \bmod 32 \equiv 1 \bmod 32 > 1$$

$$1) \gcd(9, 32) = 1$$

$$2) 1 = 9(s) + 32(t)$$

$$3) \bar{a} = 5$$

$$4) 9 \times \bar{a} \equiv 1 \bmod 32$$

$$1 = 5 - 4$$

$$1 = 5 - (9 - 5)$$

$$1 = 5(2) - 9$$

$$1 = (32 - 9(3))2 - 9$$

$$1 = 32(2) + 9(-7)$$

$$64 - 63$$

$$9 \times (-7) \equiv 1 \bmod 32$$

Sacar el inverso a mod m

1) mostrar que $\text{mcd}(a, m) = 1$

Metodo es sacar los modulos

Dejar expresadas las ecuaciones

2) Mostrar como un sistema $1 = a(s) + m(t)$ donde s es el inverso $\sim a$

3) Mostrar que $a \cdot \sim a$ congruente $1 \bmod m$