

Universidad Católica San Pablo
Programa de Ciencia de la Computación

ALGEBRA ABSTRACTA

Ana Maria Cuadros Valdivia

OBJETIVO

- Conocer las técnicas y métodos de encriptación de datos aplicando conceptos de teoría de números y álgebra abstracta.

Criptografía

UNIDAD 1

Definición

Criptografía

- Cryptography :
 - Kryptos: Ocultar
 - Gráphien: Escribir
- Estudio de métodos para enviar y recibir mensajes por medio de un algoritmo, usando una o más claves.
 - Cifrar: Transformar un texto plano en texto cifrado.
 - Descifrar: Operación inversa, transformar un texto cifrado en un texto plano.

Proceso de Cifrado y Descifrado

Criptografía

Intruso



Emisor



CIFRADO

**MENSAJE
ORIGINAL**

L

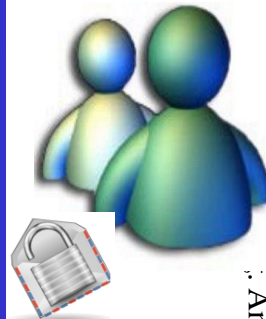
Canal Inseguro

DESCIFRADO

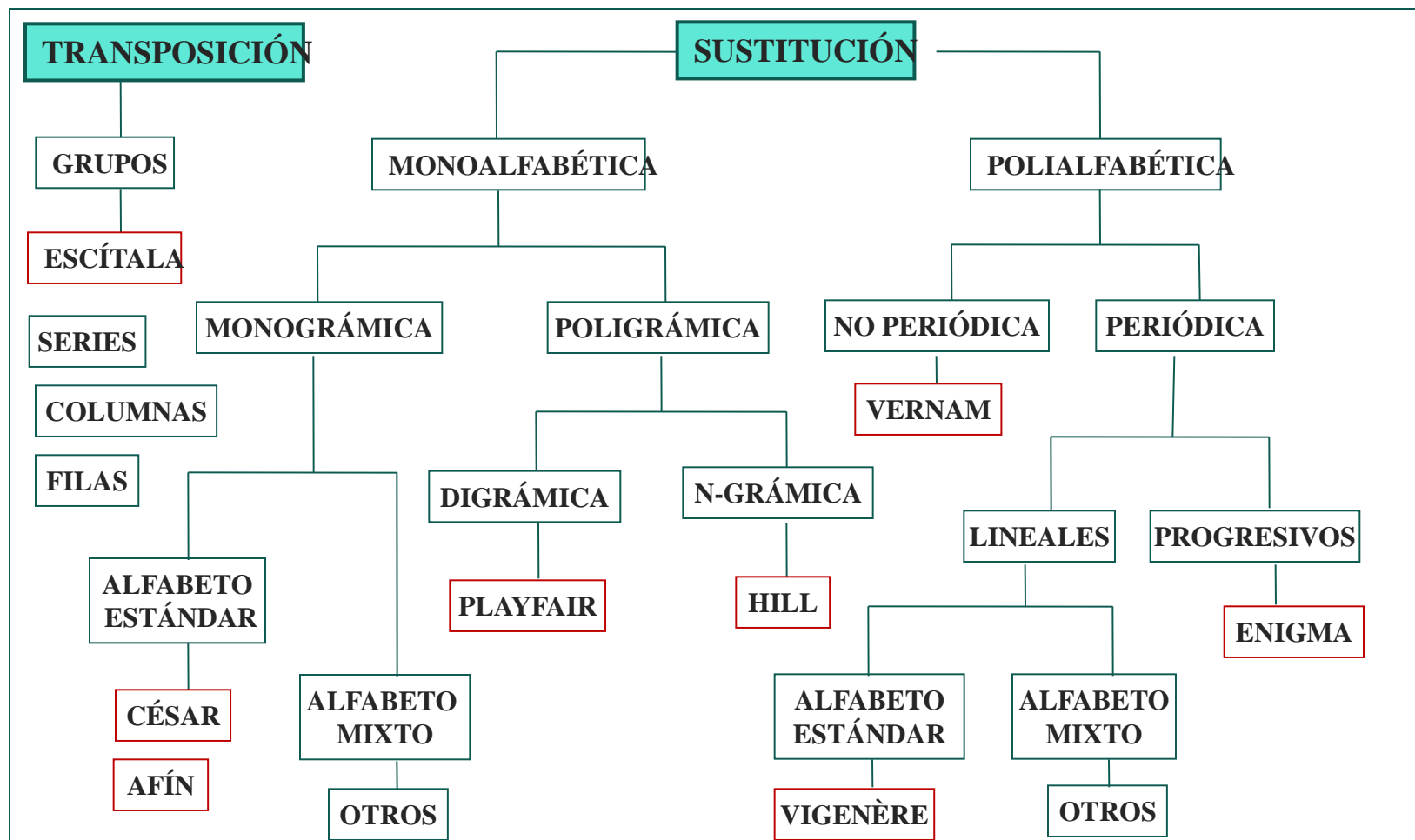
**MENSAJE
ORIGINAL**

L

Receptor



Criptografía Tradicional



Cifrado de César

- Sustituye una letra del alfabeto por otra: **clave 3**

plaintext:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
ciphertext:	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Caesar cipher with a shift of 3.

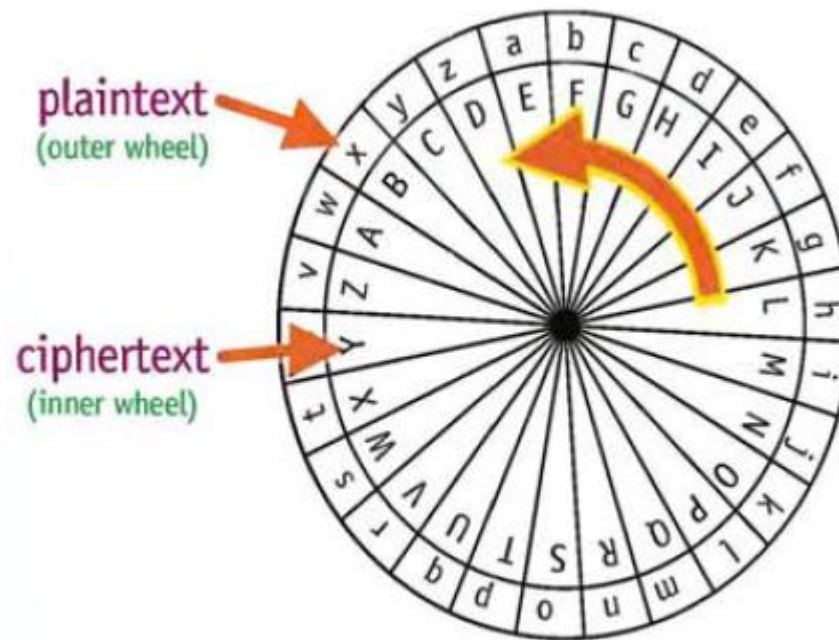
- Mensaje : **hola**

- Mensaje encriptado:

- Mensaje : **paz** **clave 4**

- Mensaje encriptado:

Cifrado de César



A cipher wheel with a shift of 4.

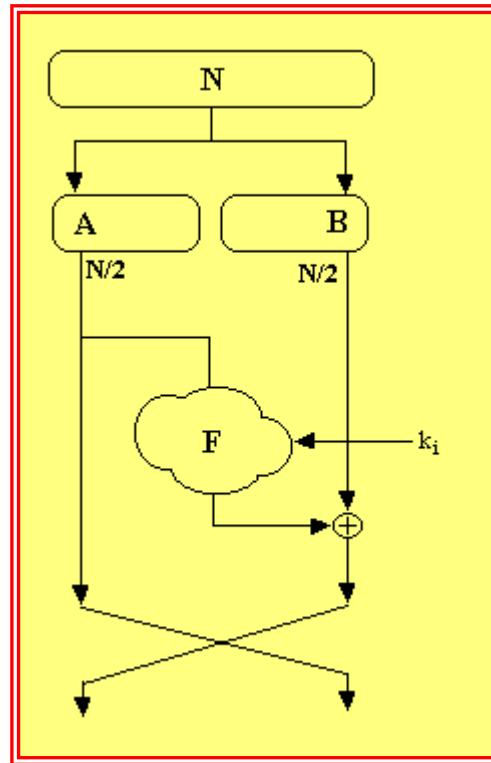
-
- Mensaje : **paz** **clave 4**
 - Mensaje encriptado:

Cifrado de César

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

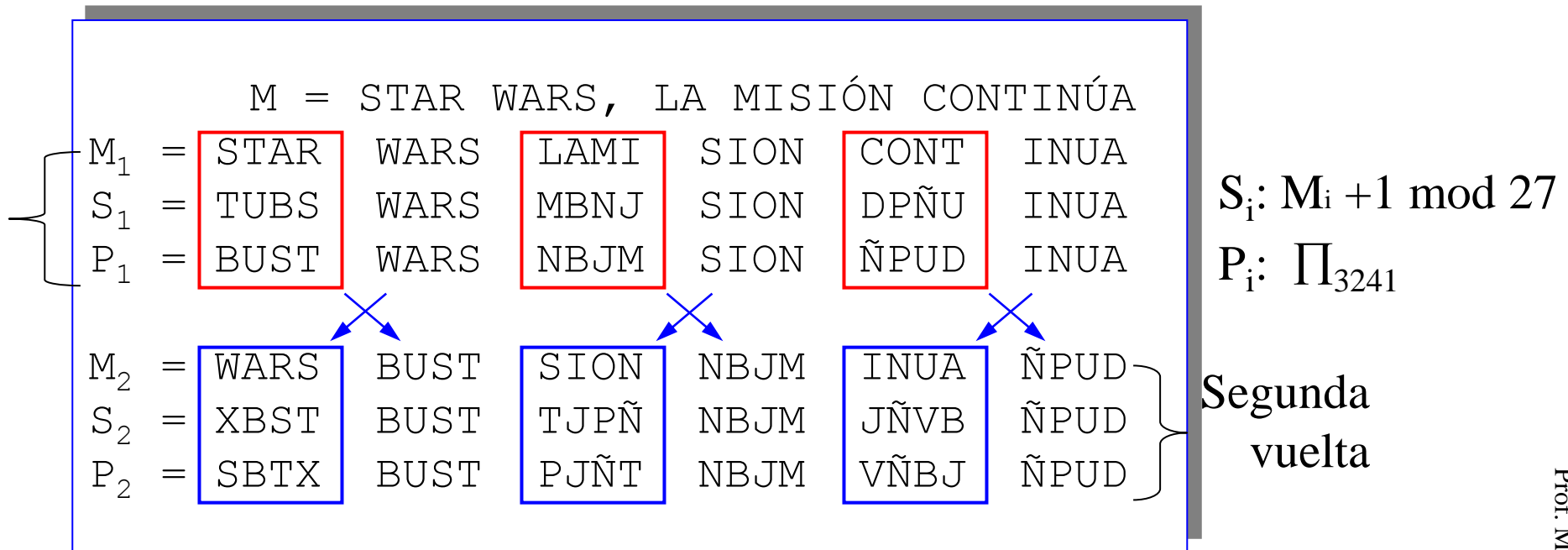
- Mensaje : Paz
- Clave : 5
- Mensaje encriptado: uigwz

Cifrado por Bloques



Cifrado de Feistel

Mensaje: $M = \text{STAR WARS, LA MISIÓN CONTINÚA}$



$C = \text{SBTX BUST PJÑT NBJM VÑBJ ÑPUD}$

Cifrados de clave pública

- Criptografía RSA
 - Escoger dos números primos distintos p y q , y multiplicarlos obteniendo un número n .
 - 77
 - 24152531111715249931151329153211
- “Fácil de hacer, difícil de deshacer”
 - Multiplicar 2 números primos.
 - Factorizar N y encontrar los primos

Referencias bibliográficas

- Handbook of Applied Cryptography, Alfred Menezes, Paul van Oorschot, Scott Vantone, CRC Press, 1996.

Teoría de Números

UNIDAD 2

Cryptography and Network Security (Behrouz Forouzan)
Mathematics of Cryptography

Part I: Modular Arithmetic, Congruence,
and Matrices

Introducción

TEORIA DE NUMEROS

- Criptografía moderna construida por: algebra y teoría de números.
 - RSA:
 - ¿cómo encontrar números primos y cómo factorizarlos?
 - ¿cómo calcular el m.c.d. de dos números?
 - Potencia de enteros
- La teoría de números es una rama de las matemáticas que se ocupa del estudio de los números enteros y sus propiedades.

Introducción

Conjunto de enteros

$$\mathbf{Z} = \{ \dots, -2, -1, 0, 1, 2, \dots \}$$

- Los enteros: suma, resta, multiplicación (leyes conmutativa, asociativa, distributiva).
- \mathbf{Z} bajo la suma y multiplicación : **ANILLOS**

Introducción

OPERACIONES BINARIAS

- **Definición:**

- Una **operación binaria $*$ en un conjunto**, es una regla que asigna a cada par ordenado de elementos de un conjunto, algún elemento del conjunto

- **Ejemplo:**

- a) Defínase en \mathbb{Z}^+ una operación binaria $*$ por $a*b$ que es igual al mínimo entre a y b o al valor común si $a=b$.
- b) Defínase en \mathbb{Z}^+ una operación binaria $*$ por $a*b = a$
- c) Defínase en \mathbb{Z}^+ una operación binaria $*$ mediante $a*b = (a*b) + 2$ donde $*$ está definida por el ejemplo a)

Introducción

OPERACIONES BINARIAS

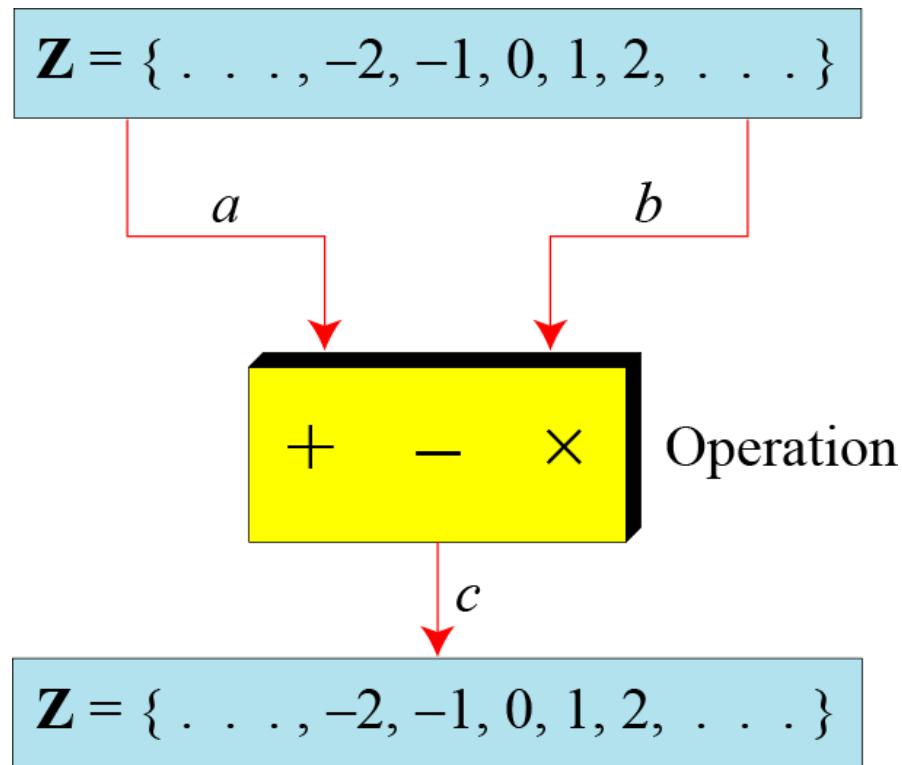
- **Definición:**

- Una **operación binaria $*$** en un conjunto S es conmutativa si y solo si $a*b=b*a$ para todo $a,b \in S$. La operación $*$ es asociativa si y solo si $(a*b) * c=a*(b*c)$ para todo $a,b,c \in S$

Introducción

OPERACIONES BINARIAS

- Operaciones binarias: dos entradas, una salida
- Criptografía: suma, resta y multiplicación



Introducción

OPERACIONES BINARIAS

Add:	$5 + 9 = 14$	$(-5) + 9 = 4$	$5 + (-9) = -4$	$(-5) + (-9) = -14$
Subtract:	$5 - 9 = -4$	$(-5) - 9 = -14$	$5 - (-9) = 14$	$(-5) - (-9) = +4$
Multiply:	$5 \times 9 = 45$	$(-5) \times 9 = -45$	$5 \times (-9) = -45$	$(-5) \times (-9) = 45$

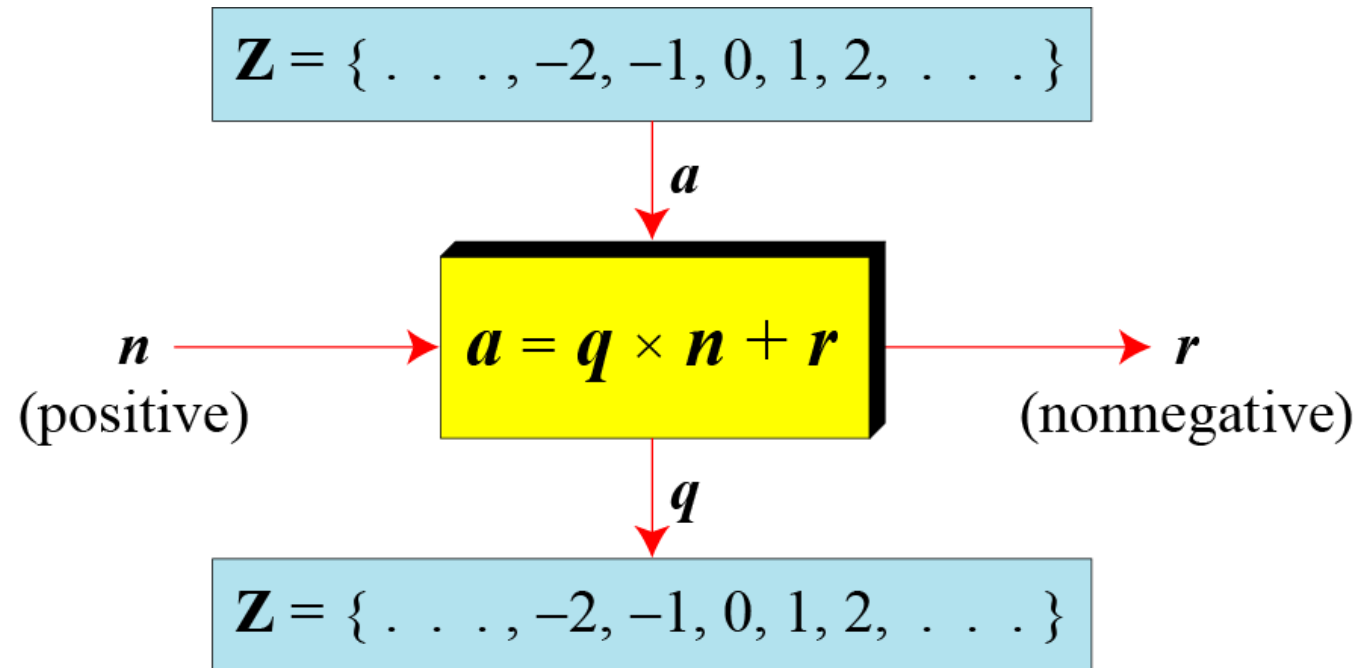
División de Enteros

- Si dividimos a por n , obtenemos q y r .

$$a = q \times n + r$$

- Ejemplo:
 - $a = 255$
 - $n = 11$
 - $q = 23$
 - $r = 2$

Dos restricciones



Ejemplo

$$a = q \times n + r$$

- $a = -255$
- $n = 11$

Ejemplo

$$a = q \times n + r$$

- $a = -255$
- $n = 11$

$$-255 = (-\mathbf{23} \times 11) + (-\mathbf{2}) \quad \Leftrightarrow \quad -255 = (-\mathbf{24} \times 11) + \mathbf{9}$$

Función módulo: $a = q \cdot n + r$

- Para convertir el módulo a positivo:
 - Decrementar el valor de q en uno.
 - Adicionar el valor de n a r para convertirlo a positivo

1. CONCEPTO DE DIVISIBILIDAD

Definiciones:

RELACION DE DIVISIBILIDAD EN \mathbb{Z}

$$a = q \times n$$

- Observación: si “n” divide “a” también decimos que:
 - n es un divisor de a
 - a es un múltiplo de n
 - n es un factor de a
 - a es divisible por n
- Notación: $n|a$ “n divide a a” si el resto es cero de lo contrario $a \nmid b$

Ejemplo :

DIVISIBILIDAD: $a = b.n$

- El entero 4 divide al entero 32 porque $32 = 4 \times 8$

$$4 \mid 32$$

- El número 8 no divide al número 42 porque $42 = 8 \times 5 + 2$. Hay un resto.

$$8 \nmid 42$$

- $13 \mid 78$, $7 \mid 98$, $-6 \mid 24$, $4 \mid 44$ y $11 \mid (-33)$
- $13 \nmid 27$, $7 \nmid 50$, $-6 \nmid 23$, $4 \nmid 41$ y $11 \nmid (-32)$

Ejemplos :

DIVISIBILIDAD: $a = b.n$

- $21 = 3.7$

3 divide a 21 $\Rightarrow 3|21$.

El cociente “n” es 7

3 es un divisor o factor de 21.

- $-3|18$

$$18 = (-3)(-6)$$

- $a|0$

$$0 = (a)(0)$$

Propiedades

DIVISIBILIDAD

- Para todo $a, b, c, \in \mathbf{Z}$, se cumple lo siguiente:

Propiedad 1: if $a|1$, then $a = \pm 1$.

Propiedad 2: if $a|b$ and $b|a$, then $a = \pm b$.

Propiedad 3: if $a|b$ and $b|c$, then $a|c$.

Propiedad 4: if $a|b$ and $a|c$, then
 $a|(m \times b + n \times c)$, donde m
y n son enteros arbitrarios.

Propiedades DIVISIBILIDAD

- a. Desde que $3 \mid 15$ y $15 \mid 45 \rightarrow$
- b. Desde que $3 \mid 15$ y $3 \mid 9 \rightarrow$

Propiedades DIVISIBILIDAD

- a. Desde que $3|15$ y $15|45 \rightarrow 3|45$ (iii prop).
- b. Desde que $3|15$ y $3|9$ (iv prop)
 $3|(15 \times 2 + 9 \times 4)$, que significa $3|66$

Propiedades

DIVISIBILIDAD

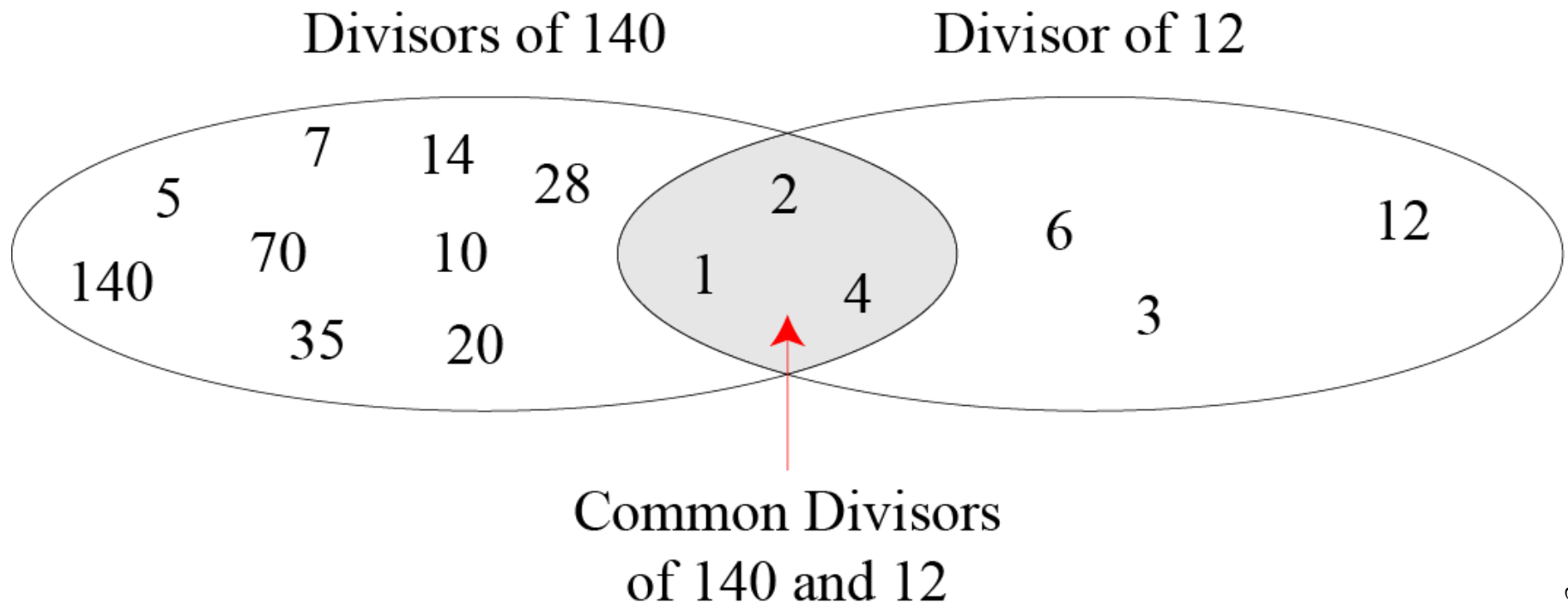
Hecho 1: El entero 1 tiene un solo divisor, el mismo

Hecho 2: Cualquier entero positivo tiene al menos 2 divisores, 1 y el mismo (puede tener más).

- 32 tiene 6 divisores: 1, 2, 4, 8, 16 y 32

2. MÁXIMO COMÚN DIVISOR

DIVISORES COMUNES DE DOS ENTEROS



Definiciones:

DIVISOR COMÚN

- Para $a, b \in \mathbb{Z}$, un entero positivo c es un divisor común de a y b si $c|a$ y $c|b$.
- Los divisores comunes de 42 y 70 son: 1, 2, 7 y 14.

Definiciones:

MÁXIMO COMÚN DIVISOR $\text{mcd}(a,b)=d$

- Se dice que un entero positivo ***d*** es el máximo común divisor de los enteros *a* y *b*,
 - *d* es divisor común de *a* y *b*;
 - El entero más grande *d* tal que $d|a$ y $d|b$
- Ejemplo:
Los divisores comunes de 12 y 18 son {1,2,3,6} y
 $\text{mcd}(12,18) = 6$

ALGORITMO DE EUCLIDES

- Basado en los siguientes hechos:

Hecho 1 : $\text{mcd}(a, 0) = a$

Hecho 2: $\text{mcd}(a, b) = \text{mcd}(b, r)$, donde r es el resto de dividir a por b

- Ejemplo: $\text{mcd}(36, 10)$

Definiciones:

ALGORITMO DE EUCLIDES

- Si $a, b \in \mathbb{Z}^+$ aplicamos el algoritmo de la división como sigue:

$$a = q_1 b + r_1, \quad 0 < r_1 < b$$

$$b = q_2 r_1 + r_2, \quad 0 < r_2 < r_1$$

$$r_1 = q_3 r_2 + r_3, \quad 0 < r_3 < r_2$$

...

$$r_i = q_{i+2} r_{i+1} + r_{i+2}, \quad 0 < r_{i+2} < r_{i+1}$$

....

$$r_{k-2} = q_k r_{k-1} + r_k, \quad 0 < r_k < r_{k-1}$$

$$r_{k-1} = q_{k+1} r_k$$

Entonces, r_k , el último resto distinto de cero, es igual a $\text{mcd}(a, b)$

Si $a, b \in \mathbb{Z}^+$ con $a > b$, entonces el $\text{mcd}(a, b) = \text{mcd}(b, a \bmod b)$

Ejemplo:

ALGORITMO DE EUCLIDES

- Determinar el m.c.d. de 250 y 111, expresado como combinación lineal de los enteros.

$$a = q \cdot b + r$$

$$250 = 2 \cdot (111) + 28 \quad 0 < 28 < 111$$

$$111 = 3 \cdot (28) + 27 \quad 0 < 27 < 111$$

$$28 = 1 \cdot (27) + 1 \quad 0 < 1 < 27$$

$$27 = 27 \cdot (1) + 0$$

$$\text{mcd}(250, 111) = 1$$

Ejemplo:

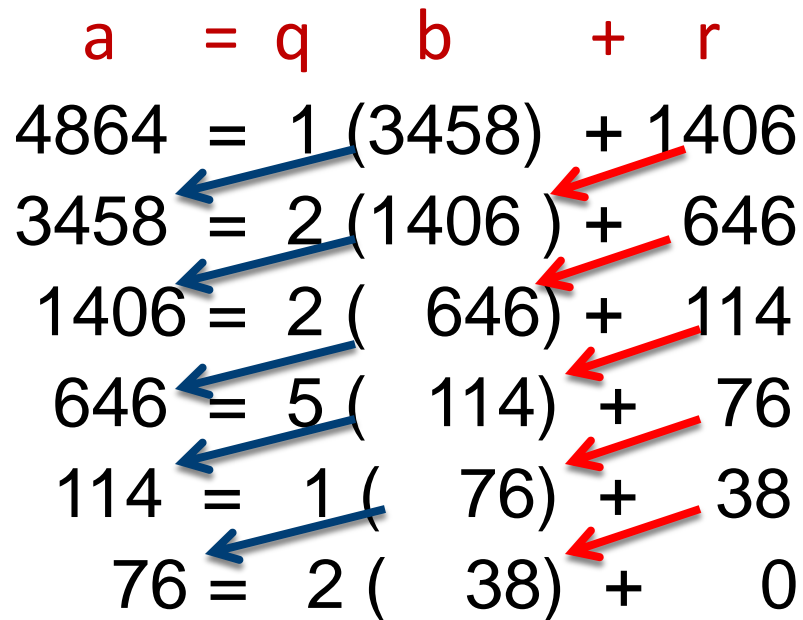
ALGORITMO DE EUCLIDES

- $\text{mcd}(4864, 3458)$

Ejemplo:

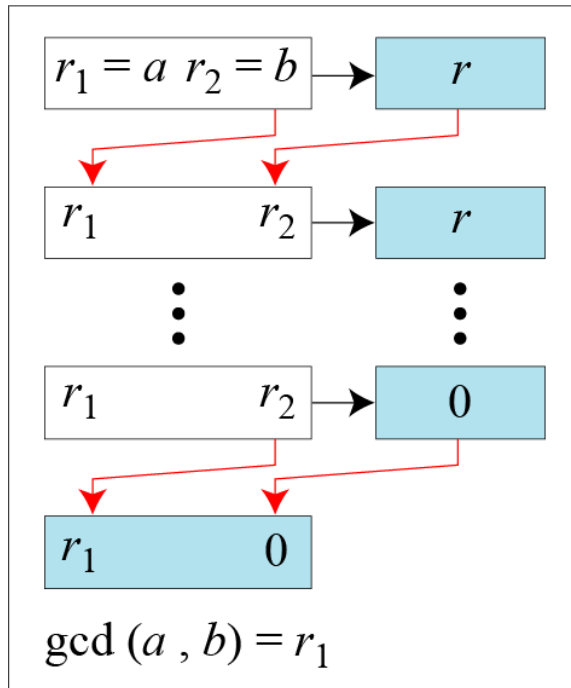
ALGORITMO DE EUCLIDES

- $\text{mcd}(4864, 3458)$

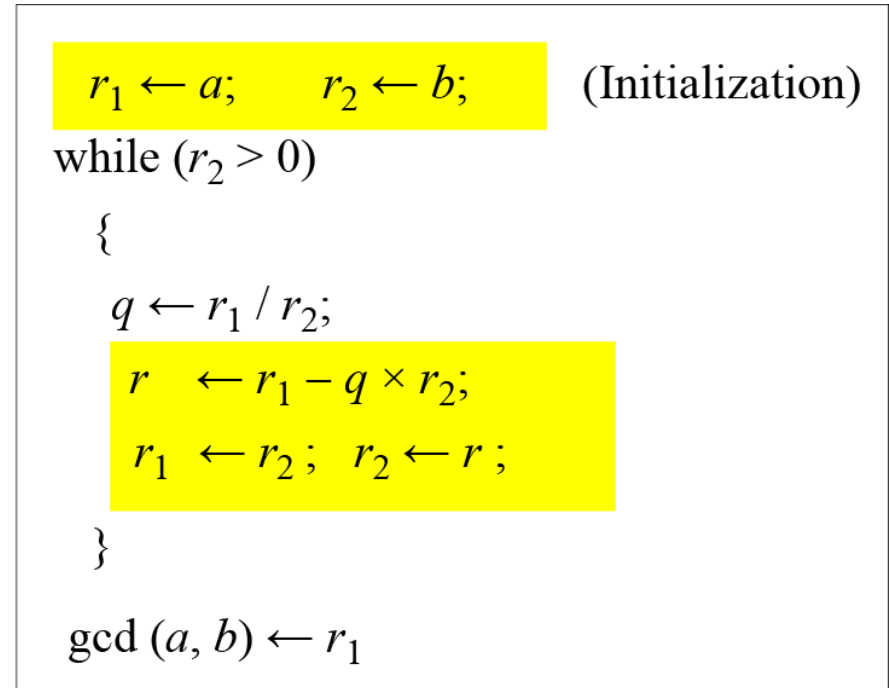
$$\begin{array}{rclcl} a & = & q & b & + & r \\ 4864 & = & 1 & (3458) & + & 1406 \\ 3458 & = & 2 & (1406) & + & 646 \\ 1406 & = & 2 & (646) & + & 114 \\ 646 & = & 5 & (114) & + & 76 \\ 114 & = & 1 & (76) & + & 38 \\ 76 & = & 2 & (38) & + & 0 \end{array}$$


$$\text{mcd}(4864, 3458) = 38$$

ALGORITMO DE EUCLIDES



a. Process



b. Algorithm

ALGORITMO DE EUCLIDES

- Encontrar el mcd de 2740 y 1760
- Encontrar el mcd de 25 y 60

ALGORITMO DE EUCLIDES

- Encontrar el mcd de 2740 y 1760

q	r_1	r_2	r
1	2740	1760	980
1	1760	980	780
1	980	780	200
3	780	200	180
1	200	180	20
9	180	20	0
	20	0	

- $\text{Mcd}(2740, 1760) = 20$

ALGORITMO DE EUCLIDES

- Encontrar el mcd de 25 y 60

q	r_1	r_2	r
0	25	60	25
2	60	25	10
2	25	10	5
2	10	5	0
	5	0	

- $\text{Mcd}(25, 60) = 5$

ALGORITMO DE EUCLIDES

Cuando $\text{mcd}(a, b) = 1$, decimos que a y b son relativamente primos.

Definiciones:

ALGORITMO EXTENDIDO DE EUCLIDES

- El algoritmo extendido de Euclides puede ser fácilmente extendido para que aunado a la obtención del m.c.d.(a,b) = d, encuentre además la solución:

$$a x + b y = d$$

como una combinación lineal de a y b

Ejemplo:

ALGORITMO EXTENDIDO DE EUCLIDES

Mcd(250,111)

$$250 = 2(111) + 28$$

$$111 = 3(28) + 27$$

$$28 = 1(27) + 1$$

$$27 = 27(1) + 0$$

$$\text{mcd}(250,111) = 1$$

$$1 = 28 - 1(27)$$

$$1 = 28 - 1(111 - 3(28))$$

$$1 = -1(111) + 4(28)$$

$$1 = -1(111) + 4(250 - 2(111))$$

$$1 = -1(111) + 4(250) - 8(111)$$

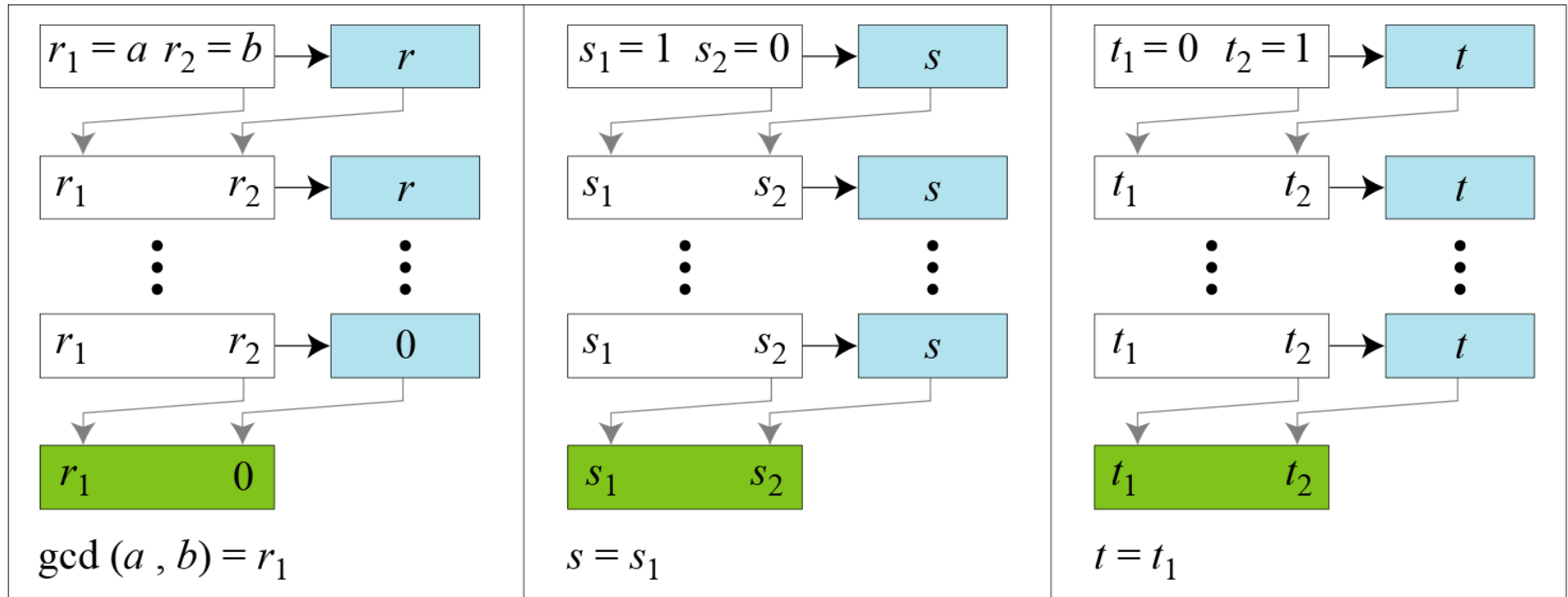
$$1 = -9(111) + 4(250)$$

$$ax + by = d$$

- $250(4) + 111(-9) = 1$

ALGORITMO EXTENDIDO DE EUCLIDES

$$s \times a + t \times b = \gcd(a, b)$$



a. Process

ALGORITMO EXTENDIDO DE EUCLIDES

```
 $r_1 \leftarrow a; \quad r_2 \leftarrow b;$   
 $s_1 \leftarrow 1; \quad s_2 \leftarrow 0;$   
 $t_1 \leftarrow 0; \quad t_2 \leftarrow 1;$ 
```

(Initialization)

```
while ( $r_2 > 0$ )
```

```
{
```

```
   $q \leftarrow r_1 / r_2;$ 
```

```
     $r \leftarrow r_1 - q \times r_2;$ 
```

```
     $r_1 \leftarrow r_2; \quad r_2 \leftarrow r;$ 
```

(Updating r 's)

```
     $s \leftarrow s_1 - q \times s_2;$ 
```

```
     $s_1 \leftarrow s_2; \quad s_2 \leftarrow s;$ 
```

(Updating s 's)

```
     $t \leftarrow t_1 - q \times t_2;$ 
```

```
     $t_1 \leftarrow t_2; \quad t_2 \leftarrow t;$ 
```

(Updating t 's)

```
}
```

```
gcd( $a, b$ )  $\leftarrow r_1; \quad s \leftarrow s_1; \quad t \leftarrow t_1$ 
```

b. Algorithm

ALGORITMO EXTENDIDO DE EUCLIDES

- Dados a y b , encontrar el $\text{mcd}(a,b)$ y los valores de x , y
 - $a=161$ y $b=28$
 - $a=17$ y $b=0$
 - $a=0$ y $b=45$

ALGORITMO EXTENDIDO DE EUCLIDES

- Dados $a=161$ y $b=28$, encontrar el $\text{mcd}(a,b)$ y los valores de x, y
- $\text{Mcd}(161,28)=7$, $x=-1$, $y=6$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
5	161	28	21	1	0	1	0	1	-5
1	28	21	7	0	1	-1	1	-5	6
3	21	7	0	1	-1	4	-5	6	-23
	7	0		-1	4		6	-23	

$a = 17$ and $b = 0$,

Solución

$\text{mcd}(17, 0) = 17$, $s = 1$, and $t = 0$.

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
	17	0		1	0		0	1	

$a = 0$ and $b = 45$

Solución

$\text{mcd}(0, 45) = 45, s = 0, t = 1.$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
0	0	45	0	1	0	1	0	1	0
	45	0		0	1		1	0	

3. ECUACIONES DIOFANTICAS

Ecuación Linear Diofántica

- Objetivo: Encontrar x , y que satisfagan la ecuación

Una ecuación diofántica tiene dos variables
 $ax + by = c$.

- Puede tener:
 - ninguna solución : si $d \nmid c$
 - o infinitas soluciones : si $d \mid c$

Ecuación Linear Diofántica

$$a x + b y = c$$

Solución Particular:

$$x_0 = (c/d) * x \quad y \quad y_0 = (c/d) * y$$

Solución General :

$$x = x_0 + k (b/d) \quad e \quad y = y_0 - k(a/d)$$

donde k is un entero

Pasos:

Ecuación Linear Diofántica

$$a x + b y = c$$

- Calcular $d = \text{mcd}(a, b)$ por el algoritmo de Euclides.
- Comprobar si $d \mid c$,
 - si no divide, no existen soluciones enteras, termina.
 - De lo contrario :
 - Reducir la ec. dividiendo ambos lados de la ec. por d .
 - Encontrar x, y usando el alg. Extendido de Euclides
 - $e = c/d$
 - Encontrar el par $x_0, y_0 = (x_e, y_e)$ es una solución particular
- Se usa la solución general.

Ejemplo:

Ec. Diafónica

- Encontrar la solución particular y general de

$$21x + 14y = 35$$

a) $\text{mcd}(21,14)$

b) $21x + 14y = 35$

c) $x_0 = (c/d) * x$ $y_0 = (c/d) * y$

d) $x = x_0 + k (b/d)$ $y = y_0 - k(a/d)$

Ejemplo:

Ec. Diofántica

- Encontrar la solución particular y general de
 $21x + 14y = 35$

Particular: $x_0 = 5 \times 1 = 5$ and $y_0 = 5 \times (-1) = -5$

General: $x = 5 + k \times 2$ and $y = -5 - k \times 3$

Ejemplo:

Ec. Diafónica

- Consideremos la ecuación

$$1492x + 1066y = -4$$

Ejemplo:

Ec. Diafónica

- Al ayudar a los estudiantes en sus cursos de programación, Juan observa que en promedio puede ayudar a un estudiante a depurar un programa en Pascal en 6 minutos, pero tarda 10 minutos en depurar un programa escrito en C++. Si trabajó en forma continua durante 104 minutos y no desperdició tiempo, ¿Cuántos programas depuró en cada lenguaje?