

Algoritmo extendido de Euclides

Método de la tabla

Daniel Felipe Triviño

Asistente graduado · Fundamentos Matemáticos para la Computación · Universidad de los Andes

Algoritmo extendido de Euclides

Método de la tabla

$$a \cdot s + b \cdot t = \text{mcd}(a, b)$$

Daniel Felipe Triviño

Asistente graduado · Fundamentos Matemáticos para la Computación · Universidad de los Andes

Ejemplo 1

$$a = 77, \quad b = 5$$

1. Algoritmo de Euclides

$$\text{mcd}(77, 5) = ?$$

$$\text{dividendo} = \text{divisor} \times \text{cociente} + \text{residuo}$$

1. Algoritmo de Euclides

$$\text{mcd}(77, 5) = ?$$

$$\text{dividendo} = \text{divisor} \times \text{cociente} + \text{residuo}$$

$$77 = 5 \times 15 + 2$$

Dividimos el número mayor entre el menor.

1. Algoritmo de Euclides

$$\text{mcd}(77, 5) = ?$$

$$\text{dividendo} = \text{divisor} \times \text{cociente} + \text{residuo}$$

$$77 = 5 \times 15 + 2$$

$$5 = 2 \times 2 + 1$$


El divisor pasa a ser el dividendo; el residuo, el nuevo divisor.

1. Algoritmo de Euclides

$$\text{mcd}(77, 5) = ?$$

$$\text{dividendo} = \text{divisor} \times \text{cociente} + \text{residuo}$$

$$77 = 5 \times 15 + 2$$

$$5 = 2 \times 2 + 1$$

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

Cuando el residuo es 0, terminamos.

1. Algoritmo de Euclides

$$\text{mcd}(77, 5) = 1$$

$$\text{dividendo} = \text{divisor} \times \text{cociente} + \text{residuo}$$

$$77 = 5 \times 15 + 2$$

$$5 = 2 \times 2 + 1$$

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

El último residuo distinto de cero es el máximo común divisor.

2. De las divisiones a la tabla

$$77 = 5 \times 15 + 2$$

$$5 = 2 \times 2 + 1$$

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

i	r_i	q_i	s_i	t_i

Los mismos números se reorganizan en una tabla: **residuos** r_i y **cocientes** q_i .

2. De las divisiones a la tabla

$$77 = 5 \times 15 + 2$$

$$5 = 2 \times 2 + 1$$

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

i	r_i	q_i	s_i	t_i
1	77	—		

La primera fila es el número mayor; todavía no hay cociente.

2. De las divisiones a la tabla

$$77 = \boxed{5 \times 15} + 2$$

$$5 = 2 \times 2 + 1$$

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

i	r_i	q_i	s_i	t_i
1	77	—		
2	5	15		

Cada pareja divisor $\times$ cociente ocupa una fila.

2. De las divisiones a la tabla

$$77 = 5 \times 15 + 2$$

$$5 = \boxed{2 \times 2} + 1$$

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

i	r_i	q_i	s_i	t_i
1	77	—		
2	5	15		
3	2	2		

Cada pareja divisor $\times$ cociente ocupa una fila.

2. De las divisiones a la tabla

$$77 = 5 \times 15 + 2$$

$$5 = 2 \times 2 + 1$$

$$2 = \boxed{1 \times 2} + 0$$

i	r_i	q_i	s_i	t_i
1	77	—		
2	5	15		
3	2	2		
4	1	2		

Cada pareja divisor $\times$ cociente ocupa una fila.

2. De las divisiones a la tabla

$$77 = 5 \times 15 + 2$$

$$5 = 2 \times 2 + 1$$

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

i	r_i	q_i	s_i	t_i
1	77	—		
2	5	15		
3	2	2		
4	1	2		

El residuo 0 no se anota: la tabla termina en el mcd.

3. Arranque: la matriz identidad

Matriz identidad 2×2

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

i	r_i	q_i	s_i	t_i
1	77	—		
2	5	15		
3	2	2		
4	1	2		

Las columnas s_i y t_i siempre arrancan con la matriz identidad.

3. Arranque: la matriz identidad

Matriz identidad 2×2

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

i	r_i	q_i	s_i	t_i
1	77	—	1	0
2	5	15	0	1
3	2	2		
4	1	2		

Las columnas s_i y t_i siempre arrancan con la matriz identidad.

3. Arranque: la matriz identidad

$$77 = 77 \cdot 1 + 5 \cdot 0$$

$$5 = 77 \cdot 0 + 5 \cdot 1$$

i	r_i	q_i	s_i	t_i
1	77	—	1	0
2	5	15	0	1
3	2	2		
4	1	2		

¿Por qué? Cada fila escribe su residuo como combinación de 77 y 5.

3. Arranque: la matriz identidad

$$77 = 77 \cdot 1 + 5 \cdot 0$$

$$5 = 77 \cdot 0 + 5 \cdot 1$$

$$r_i = 77 \cdot s_i + 5 \cdot t_i$$

i	r_i	q_i	s_i	t_i
1	77	—	1	0
2	5	15	0	1
3	2	2		
4	1	2		

Esa regla se va a cumplir en todas las filas de la tabla.

4. Calcular s_i y t_i

$$s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$$

$$t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}$$

i	r_i	q_i	s_i	t_i
1	77	—	1	0
2	5	15	0	1
3	2	2		
4	1	2		

Cada valor nuevo se calcula con las dos filas anteriores.

4. Calcular s_i y t_i

$$s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$$

$$t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}$$

i	r_i	q_i	s_i	t_i
1	77	—	1	0
2	5	15	0	1
3	2	2		
4	1	2		

...y le restamos el cociente por el valor de la fila anterior.

4. Calcular s_i y t_i

$$s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$$

$$t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}$$

$$1 - 15 \cdot 0 = 1$$

i	r_i	q_i	s_i	t_i
1	77	—	1	0
2	5	15	0	1
3	2	2	1	
4	1	2		

...y le restamos el cociente por el valor de la fila anterior.

4. Calcular s_i y t_i

$$s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$$

$$t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}$$

$$0 - 15 \cdot 1 = -15$$

i	r_i	q_i	s_i	t_i
1	77	—	1	0
2	5	15	0	1
3	2	2	1	-15
4	1	2		

Para t_i es el mismo patrón, una columna a la derecha.

4. Calcular s_i y t_i

$$s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$$

$$t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}$$

$$2 = 77 \cdot 1 + 5 \cdot (-15) \quad \checkmark$$

i	r_i	q_i	s_i	t_i
1	77	—	1	0
2	5	15	0	1
3	2	2	1	-15
4	1	2		

Comprobación: la fila 3 también cumple $r_i = 77 \cdot s_i + 5 \cdot t_i$.

4. Calcular s_i y t_i

$$s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$$

$$t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}$$

$$0 - 2 \cdot 1 = -2$$

i	r_i	q_i	s_i	t_i
1	77	—	1	0
2	5	15	0	1
3	2	2	1	-15
4	1	2	-2	

Bajamos una fila y repetimos.

4. Calcular s_i y t_i

$$s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$$

$$t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}$$

$$1 - 2 \cdot (-15) = 31$$

i	r_i	q_i	s_i	t_i
1	77	—	1	0
2	5	15	0	1
3	2	2	1	-15
4	1	2	-2	31

Bajamos una fila y repetimos.

5. Identidad de Bézout

i	r_i	q_i	s_i	t_i
1	77	—	1	0
2	5	15	0	1
3	2	2	1	-15
4	1	2	-2	31

La última fila tiene el mcd y los coeficientes que buscábamos.

5. Identidad de Bézout

Identidad de Bézout

$$a \cdot s + b \cdot t = \text{mcd}(a, b)$$

$$77 \times (-2) + 5 \times 31 = 1$$

i	r_i	q_i	s_i	t_i
1	77	—	1	0
2	5	15	0	1
3	2	2	1	-15
4	1	2	-2	31

La última fila tiene el mcd y los coeficientes que buscábamos.

5. Identidad de Bézout

Identidad de Bézout

$$a \cdot s + b \cdot t = \text{mcd}(a, b)$$

$$77 \times (-2) + 5 \times 31 = 1$$

$$-154 + 155 = 1 \quad \checkmark$$

i	r_i	q_i	s_i	t_i
1	77	—	1	0
2	5	15	0	1
3	2	2	1	-15
4	1	2	-2	31

Así se escribe el mcd como combinación de 77 y 5.

Ejemplo 2: un caso más largo

$$a = 779, \quad b = 17$$

1. Algoritmo de Euclides

$$\text{mcd}(779, 17) = ?$$

$$\text{dividendo} = \text{divisor} \times \text{cociente} + \text{residuo}$$

1. Algoritmo de Euclides

$$\text{mcd}(779, 17) = ?$$

$$\text{dividendo} = \text{divisor} \times \text{cociente} + \text{residuo}$$

$$779 = 17 \times 45 + 14$$

1. Algoritmo de Euclides

$$\text{mcd}(779, 17) = ?$$

$$\text{dividendo} = \text{divisor} \times \text{cociente} + \text{residuo}$$

$$779 = 17 \times 45 + 14$$

$$17 = 14 \times 1 + 3$$


El divisor pasa a ser el dividendo; el residuo, el nuevo divisor.

1. Algoritmo de Euclides

$$\text{mcd}(779, 17) = ?$$

$$\text{dividendo} = \text{divisor} \times \text{cociente} + \text{residuo}$$

$$779 = 17 \times 45 + 14$$

$$17 = 14 \times 1 + 3$$

$$14 = 3 \times 4 + 2$$

El divisor pasa a ser el dividendo; el residuo, el nuevo divisor.

1. Algoritmo de Euclides

$$\text{mcd}(779, 17) = ?$$

dividendo = divisor $\times$ cociente + residuo

$$779 = 17 \times 45 + 14$$

$$17 = 14 \times 1 + 3$$

$$14 = 3 \times 4 + 2$$

$$3 = 2 \times 1 + 1$$

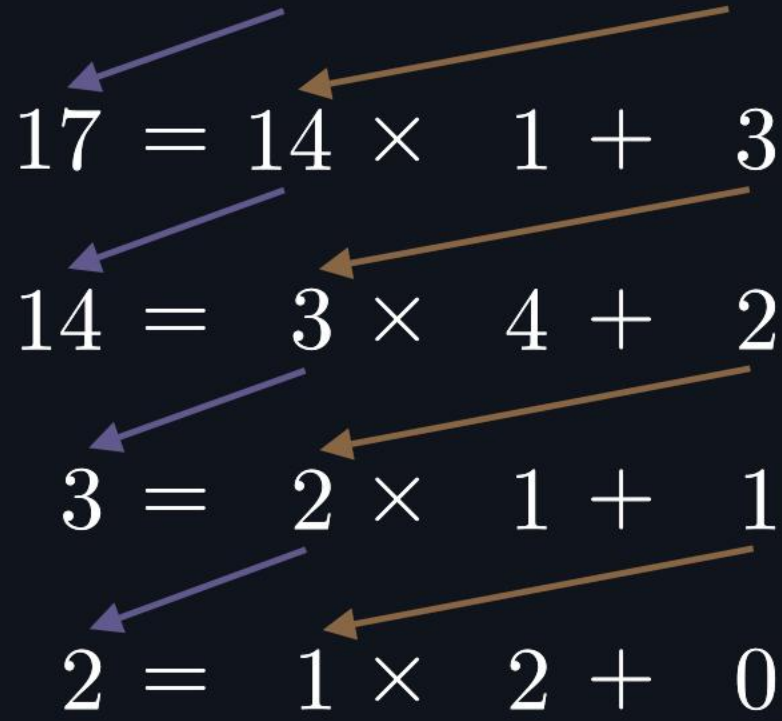
El divisor pasa a ser el dividendo; el residuo, el nuevo divisor.

1. Algoritmo de Euclides

$$\text{mcd}(779, 17) = ?$$

dividendo = divisor $\times$ cociente + residuo

$$779 = 17 \times 45 + 14$$


$$17 = 14 \times 1 + 3$$

$$14 = 3 \times 4 + 2$$

$$3 = 2 \times 1 + 1$$

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

Cuando el residuo es 0, terminamos.

1. Algoritmo de Euclides

$$\text{mcd}(779, 17) = 1$$

dividendo = divisor $\times$ cociente + residuo

$$779 = 17 \times 45 + 14$$

$$17 = 14 \times 1 + 3$$

$$14 = 3 \times 4 + 2$$

$$3 = 2 \times 1 + \boxed{1}$$

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

El último residuo distinto de cero es el máximo común divisor.

2. De las divisiones a la tabla

$$779 = 17 \times 45 + 14$$

$$17 = 14 \times 1 + 3$$

$$14 = 3 \times 4 + 2$$

$$3 = 2 \times 1 + 1$$

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

i	r_i	q_i	s_i	t_i

Los mismos números se reorganizan en una tabla: residuos r_i y cocientes q_i .

2. De las divisiones a la tabla

$$779 = 17 \times 45 + 14$$

$$17 = 14 \times 1 + 3$$

$$14 = 3 \times 4 + 2$$

$$3 = 2 \times 1 + 1$$

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

i	r_i	q_i	s_i	t_i
1	779	—		

La primera fila es el número mayor; todavía no hay cociente.

2. De las divisiones a la tabla

$$779 = 17 \times 45 + 14$$

$$17 = 14 \times 1 + 3$$

$$14 = 3 \times 4 + 2$$

$$3 = 2 \times 1 + 1$$

$$2 = \boxed{1 \times 2} + 0$$

i	r_i	q_i	s_i	t_i
1	779	—		
2	17	45		
3	14	1		
4	3	4		
5	2	1		
6	1	2		

Cada pareja divisor $\times$ cociente ocupa una fila.

2. De las divisiones a la tabla

$$779 = 17 \times 45 + 14$$

$$17 = 14 \times 1 + 3$$

$$14 = 3 \times 4 + 2$$

$$3 = 2 \times 1 + 1$$

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

i	r_i	q_i	s_i	t_i
1	779	—		
2	17	45		
3	14	1		
4	3	4		
5	2	1		
6	1	2		

El residuo 0 no se anota: la tabla termina en el mcd.

3. Arranque: la matriz identidad

Matriz identidad 2×2

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

i	r_i	q_i	s_i	t_i
1	779	—	1	0
2	17	45	0	1
3	14	1		
4	3	4		
5	2	1		
6	1	2		

Las columnas s_i y t_i siempre arrancan con la matriz identidad.

4. Calcular s_i y t_i

$$s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$$

$$t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}$$

i	r_i	q_i	s_i	t_i
1	779	—	1	0
2	17	45	0	1
3	14	1		
4	3	4		
5	2	1		
6	1	2		

El mismo patrón de tres celdas, fila por fila.

4. Calcular s_i y t_i

$$s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$$

$$t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}$$

$$1 - 45 \cdot 0 = 1$$

i	r_i	q_i	s_i	t_i
1	779	—	1	0
2	17	45	0	1
3	14	1	1	
4	3	4		
5	2	1		
6	1	2		

El mismo patrón de tres celdas, fila por fila.

4. Calcular s_i y t_i

$$s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$$

$$t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}$$

$$0 - 45 \cdot 1 = -45$$

i	r_i	q_i	s_i	t_i
1	779	—	1	0
2	17	45	0	1
3	14	1	1	-45
4	3	4		
5	2	1		
6	1	2		

El mismo patrón de tres celdas, fila por fila.

4. Calcular s_i y t_i

$$s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$$

$$t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}$$

$$0 - 1 \cdot 1 = -1$$

i	r_i	q_i	s_i	t_i
1	779	—	1	0
2	17	45	0	1
3	14	1	1	-45
4	3	4	-1	
5	2	1		
6	1	2		

El mismo patrón de tres celdas, fila por fila.

4. Calcular s_i y t_i

$$s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$$

$$t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}$$

$$1 - 1 \cdot (-45) = 46$$

i	r_i	q_i	s_i	t_i
1	779	—	1	0
2	17	45	0	1
3	14	1	1	-45
4	3	4	-1	46
5	2	1		
6	1	2		

El mismo patrón de tres celdas, fila por fila.

4. Calcular s_i y t_i

$$s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$$

$$t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}$$

$$1 - 4 \cdot (-1) = 5$$

i	r_i	q_i	s_i	t_i
1	779	—	1	0
2	17	45	0	1
3	14	1	1	-45
4	3	4	-1	46
5	2	1	5	
6	1	2		

El mismo patrón de tres celdas, fila por fila.

4. Calcular s_i y t_i

$$s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$$

$$t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}$$

$$-45 - 4 \cdot 46 = -229$$

i	r_i	q_i	s_i	t_i
1	779	—	1	0
2	17	45	0	1
3	14	1	1	-45
4	3	4	-1	46
5	2	1	5	-229
6	1	2		

El mismo patrón de tres celdas, fila por fila.

4. Calcular s_i y t_i

$$s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$$

$$t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}$$

$$-1 - 1 \cdot 5 = -6$$

i	r_i	q_i	s_i	t_i
1	779	—	1	0
2	17	45	0	1
3	14	1	1	−45
4	3	4	−1	46
5	2	1	5	−229
6	1	2	−6	

El mismo patrón de tres celdas, fila por fila.

4. Calcular s_i y t_i

$$s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$$

$$t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}$$

$$46 - 1 \cdot (-229) = 275$$

i	r_i	q_i	s_i	t_i
1	779	—	1	0
2	17	45	0	1
3	14	1	1	-45
4	3	4	-1	46
5	2	1	5	-229
6	1	2	-6	275

El mismo patrón de tres celdas, fila por fila.

5. Identidad de Bézout

i	r_i	q_i	s_i	t_i
1	779	—	1	0
2	17	45	0	1
3	14	1	1	−45
4	3	4	−1	46
5	2	1	5	−229
6	1	2	−6	275

La última fila tiene el mcd y los coeficientes que buscábamos.

5. Identidad de Bézout

Identidad de Bézout

$$a \cdot s + b \cdot t = \text{mcd}(a, b)$$

$$779 \times (-6) + 17 \times 275 = 1$$

i	r_i	q_i	s_i	t_i
1	779	—	1	0
2	17	45	0	1
3	14	1	1	−45
4	3	4	−1	46
5	2	1	5	−229
6	1	2	−6	275

La última fila tiene el mcd y los coeficientes que buscábamos.

5. Identidad de Bézout

Identidad de Bézout

$$a \cdot s + b \cdot t = \text{mcd}(a, b)$$

$$779 \times (-6) + 17 \times 275 = 1$$

$$-4674 + 4675 = 1 \quad \checkmark$$

i	r_i	q_i	s_i	t_i
1	779	—	1	0
2	17	45	0	1
3	14	1	1	-45
4	3	4	-1	46
5	2	1	5	-229
6	1	2	-6	275

Así se escribe el mcd como combinación de 779 y 17.

Dos caminos, la misma identidad

Sustitución hacia atrás

$$2 = 77 - 5 \times 15$$

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

$$1 = 5 - (77 - 5 \times 15) \times 2$$

$$1 = 5 \times 31 - 77 \times 2$$

$$77 \times (-2) + 5 \times 31 = 1$$

Sustitución hacia atrás: del mcd hacia los dos números.

Dos caminos, la misma identidad

Sustitución hacia atrás

$$2 = 77 - 5 \times 15$$

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

$$1 = 5 - (77 - 5 \times 15) \times 2$$

$$1 = 5 \times 31 - 77 \times 2$$

$$77 \times (-2) + 5 \times 31 = 1$$

Tabla

i	r_i	q_i	s_i	t_i
1	77	—	1	0
2	5	15	0	1
3	2	2	1	−15
4	1	2	−2	31

$$77 \times (-2) + 5 \times 31 = 1$$

Los dos métodos dan los mismos s y t .

Dos caminos, la misma identidad

Sustitución hacia atrás

$2 = 77 - 5 \times 15$

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

$$1 = 5 - (77 - 5 \times 15) \times 2$$

$$1 = 5 \times 31 - 77 \times 2$$

Tabla

i	r_i	q_i	s_i	t_i
1	77	—	1	0
2	5	15	0	1
3	2	2	1	-15
4	1	2	-2	31

$$2 = 77 \times 1 + 5 \times (-15)$$

Las filas de la tabla son los mismos despejes.

Dos caminos, la misma identidad

Sustitución hacia atrás

$$2 = 77 - 5 \times 15$$

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

$$1 = 5 - (77 - 5 \times 15) \times 2$$

$$1 = 5 \times 31 - 77 \times 2$$

Tabla

i	r_i	q_i	s_i	t_i
1	77	—	1	0
2	5	15	0	1
3	2	2	1	−15
4	1	2	−2	31

Fila 4 = fila 2 − cociente × fila 3.

Dos caminos, la misma identidad

Sustitución hacia atrás


$$2 = 77 - 5 \times 15$$

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

$$1 = 5 - (77 - 5 \times 15) \times 2$$

$$1 = 5 \times 31 - 77 \times 2$$

Tabla



i	r_i	q_i	s_i	t_i
1	77	—	1	0
2	5	15	0	1
3	2	2	1	-15
4	1	2	-2	31

Hacia atrás: del mcd a los números. Tabla: de los números al mcd.

Dos caminos, la misma identidad

Sustitución hacia atrás


$$2 = 77 - 5 \times 15$$

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

$$1 = 5 - (77 - 5 \times 15) \times 2$$

$$1 = 5 \times 31 - 77 \times 2$$

$$77 \times (-2) + 5 \times 31 = 1$$

Tabla



i	r_i	q_i	s_i	t_i
1	77	—	1	0
2	5	15	0	1
3	2	2	1	-15
4	1	2	-2	31

$$77 \times (-2) + 5 \times 31 = 1$$

Hacia atrás: del mcd a los números. Tabla: de los números al mcd.

En resumen

En resumen

1. Euclides: dividir hasta llegar al residuo 0.

En resumen

1. Euclides: dividir hasta llegar al residuo 0.
2. Tabla: residuos r_i , cocientes q_i y la identidad en s_i, t_i .

En resumen

1. Euclides: dividir hasta llegar al residuo 0.
2. Tabla: residuos r_i , cocientes q_i y la identidad en s_i, t_i .
3. $s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}, \quad t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}.$

En resumen

1. Euclides: dividir hasta llegar al residuo 0.
2. Tabla: residuos r_i , cocientes q_i y la identidad en s_i, t_i .
3. $s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$, $t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}$.
4. Última fila: $a \cdot s + b \cdot t = \text{mcd}(a, b)$.