

Identidad de Bézout

Por sustitución hacia atrás

Daniel Felipe Triviño

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

Identidad de Bézout

Por sustitución hacia atrás

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

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

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

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

$$\begin{array}{rcl} 77 & = & 5 \times 15 + 2 \\ & \swarrow & \nwarrow \\ 5 & = & 2 \times 2 + 1 \end{array}$$

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. Despejar los residuos

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

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

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

Meta: escribir el mcd como combinación de 77 y 5.

2. Despejar los residuos

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

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

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

De cada división despejamos el residuo.

2. Despejar los residuos

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

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

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

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

De cada división despejamos el residuo.

2. Despejar los residuos

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

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

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

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

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

De cada división despejamos el residuo.

2. Despejar los residuos

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

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

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

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

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

De cada división despejamos el residuo.

3. Sustituir hacia atrás

Despejes

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

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

Sustitución hacia atrás

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

Se empieza por el último despeje: el del mcd.

3. Sustituir hacia atrás

Despejes

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

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

Sustitución hacia atrás

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

Cada residuo intermedio se reemplaza por su despeje.

3. Sustituir hacia atrás

Despejes

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

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

Sustitución hacia atrás

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

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

Cada residuo intermedio se reemplaza por su despeje.

3. Sustituir hacia atrás

Despejes

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

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

Sustitución hacia atrás

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

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

No se multiplican los residuos: solo se cuentan.

3. Sustituir hacia atrás

Despejes

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

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

Sustitución hacia atrás

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

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

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

No se multiplican los residuos: solo se cuentan.

4. Identidad de Bézout

Despejes

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

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

Sustitución hacia atrás

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

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

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

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

Solo quedan 77 y 5.

4. Identidad de Bézout

Despejes

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

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

Sustitución hacia atrás

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

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

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

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

Comprobación: $-154 + 155 = 1$.

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

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

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

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

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

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

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

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. Despejar los residuos

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

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

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

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

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

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

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

$$1 = 3 - 2 \times 1$$

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

De cada división despejamos el residuo.

3. Sustituir hacia atrás

Despejes

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

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

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

$$1 = 3 - 2 \times 1$$

Sustitución hacia atrás

$$1 = 3 - 2 \times 1$$

Se empieza por el último despeje: el del mcd.

3. Sustituir hacia atrás

Despejes

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

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

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

$$1 = 3 - 2 \times 1$$

Sustitución hacia atrás

$$1 = 3 - 2 \times 1$$

$$1 = 3 - (14 - 3 \times 4) \times 1$$

$$1 = 3 \times 5 - 14 \times 1$$

Cada residuo intermedio se reemplaza por su despeje.

3. Sustituir hacia atrás

Despejes

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

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

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

$$1 = 3 - 2 \times 1$$

Sustitución hacia atrás

$$1 = 3 - 2 \times 1$$

$$1 = 3 - (14 - 3 \times 4) \times 1$$

$$1 = 3 \times 5 - 14 \times 1$$

$$1 = (17 - 14 \times 1) \times 5 - 14 \times 1$$

$$1 = 17 \times 5 - 14 \times 6$$

Cada residuo intermedio se reemplaza por su despeje.

3. Sustituir hacia atrás

Despejes

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

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

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

$$1 = 3 - 2 \times 1$$

Sustitución hacia atrás

$$1 = 3 - 2 \times 1$$

$$1 = 3 - (14 - 3 \times 4) \times 1$$

$$1 = 3 \times 5 - 14 \times 1$$

$$1 = (17 - 14 \times 1) \times 5 - 14 \times 1$$

$$1 = 17 \times 5 - 14 \times 6$$

$$1 = 17 \times 5 - (779 - 17 \times 45) \times 6$$

$$1 = 17 \times 275 - 779 \times 6$$

Cada residuo intermedio se reemplaza por su despeje.

4. Identidad de Bézout

Despejes

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

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

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

$$1 = 3 - 2 \times 1$$

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

Sustitución hacia atrás

$$1 = 3 - 2 \times 1$$

$$1 = 3 - (14 - 3 \times 4) \times 1$$

$$1 = 3 \times 5 - 14 \times 1$$

$$1 = (17 - 14 \times 1) \times 5 - 14 \times 1$$

$$1 = 17 \times 5 - 14 \times 6$$

$$1 = 17 \times 5 - (779 - 17 \times 45) \times 6$$

$$1 = 17 \times 275 - 779 \times 6$$

Solo quedan 779 y 17.

En resumen

En resumen

1. Euclides: dividir hasta llegar al residuo 0.

En resumen

1. Euclides: dividir hasta llegar al residuo 0.
2. Despejar el residuo de cada división.

En resumen

1. Euclides: dividir hasta llegar al residuo 0.
2. Despejar el residuo de cada división.
3. Desde el último despeje, reemplazar residuos y agrupar.

En resumen

1. Euclides: dividir hasta llegar al residuo 0.
2. Despejar el residuo de cada división.
3. Desde el último despeje, reemplazar residuos y agrupar.
4. Al llegar a a y b : $a \cdot s + b \cdot t = \text{mcd}(a, b)$.

En resumen

1. Euclides: dividir hasta llegar al residuo 0.
2. Despejar el residuo de cada división.
3. Desde el último despeje, reemplazar residuos y agrupar.
4. Al llegar a a y b : $a \cdot s + b \cdot t = \text{mcd}(a, b)$.

Siguiente video: el método de la tabla.