Algoritmo extendido de Euclides (cálculo de los coeficientes de Bézout)

1. Ejemplo. Calcular el máximo común divisor d de los números 141 y 96. Encontrar números u y v tales que $141u + 96v = d$. Hacer comprobaciones.

Solución. Primero apliquemos el algoritmo de Euclides:

$$\begin{aligned} 141 &= 96 \cdot 1 + 45; \\ 96 &= 45 \cdot 2 + 6; \\ 45 &= 6 \cdot 7 + 3; \\ 6 &= 3 \cdot 2 + 0. \end{aligned}$$

De aquí concluimos que $d = 3$. Comprobamos que 3 es un divisor común de 141 y 96:

$$141 = 3 \cdot 47, \quad \checkmark \qquad\qquad 96 = 3 \cdot 32. \quad \checkmark$$

Ahora calculemos u y v. Vamos a representar cada uno de los residuos del algoritmo de Euclides como una combinación lineal entera de 141 y 96. Empezamos con 141 y 96:

$$\begin{aligned} 141 &= 141 \cdot 1 + 96 \cdot 0; \\ 96 &= 141 \cdot 0 + 96 \cdot 1. \end{aligned}$$

Luego usamos las igualdades del algoritmo de Euclides para expresar cada residuo a través de dos anteriores y representarlo como una combinación lineal entera de 141 y 96:

$$\begin{aligned} 45 &= 141 - 96 = (141 \cdot 1 + 96 \cdot 0) - (141 \cdot 0 + 96 \cdot 1) = 141 \cdot 1 + 96 \cdot (-1); \\ 6 &= 96 - 45 \cdot 2 = (141 \cdot 0 + 96 \cdot 1) - (141 \cdot 1 + 96 \cdot (-1)) \cdot 2 = 141 \cdot (-2) + 96 \cdot 3; \\ 3 &= 45 - 6 \cdot 7 = (141 \cdot 1 + 96 \cdot (-1)) - (141 \cdot (-2) + 96 \cdot 3) \cdot 7 = 141 \cdot 15 + 96 \cdot (-22). \end{aligned}$$

Hemos encontrado u y v:

$$u = 15, \qquad v = -22.$$

Comprobemos que $141u + 96v = d$:

$$141 \cdot 15 + 96 \cdot (-22) = 2115 - 2112 = 3. \quad \checkmark$$

□

2. Fórmulas recursivas para los coeficientes de Bézout. Analicemos cómo escribir los cálculos de la segunda parte de manera más eficiente. Denotando a por r_{-1} y b por r_0, uno puede escribir el algoritmo de Euclides de la siguiente manera:

$$\begin{aligned} r_{-1} &= r_0 q_1 + r_1, \\ r_0 &= r_1 q_2 + r_2, \\ r_1 &= r_2 q_3 + r_3, \\ &\dots \\ r_{n-2} &= r_{n-1} q_n + r_n. \end{aligned}$$

En el k-ésimo paso

$$r_{k-2} = r_{k-1} q_k + r_k,$$

esto es,

$$r_k = r_{k-2} - q_k r_{k-1}.$$

Suponiendo que r_{k-2} y r_{k-1} ya están escritos como combinaciones enteras de a y b:

$$r_{k-2} = a u_{k-2} + b v_{k-2}, \qquad r_{k-1} = a u_{k-1} + b v_{k-1},$$

obtenemos

$$r_k = r_{k-2} - r_{k-1} q_k = a(u_{k-2} - q_k u_{k-1}) + b(v_{k-2} - q_k v_{k-1}).$$

Esto significa que u_k y v_k se pueden calcular por las fórmulas:

$$u_k = u_{k-2} - q_k u_{k-1}, \qquad v_k = v_{k-2} - q_k v_{k-1}. \tag{1}$$

Regresando al Ejemplo 1, escribamos los cálculos de la segunda parte de manera más breve, usando fórmulas recursivas:

		$q_1 = 1$	$q_2 = 2$	$q_3 = 7$
$u_{-1} = 1$	$u_0 = 0$	$u_1 = 1$	$u_2 = -2$	$u_3 = 15$
$v_{-1} = 0$	$v_0 = 1$	$v_1 = -1$	$v_2 = 3$	$v_3 = -22$
$r_{-1} = 141$	$r_0 = 96$	$r_1 = 45$	$r_2 = 6$	$r_3 = 3$

El renglón con $r_{-1}, r_0, r_1, r_2, r_3$ no es necesario y solamente ayuda a entender el sentido de los números u_k y v_k. En cada paso tenemos $r_k = 141 u_k + 96 v_k$. Por ejemplo,

$$141 u_2 + 96 v_2 = 141 \cdot (-2) + 96 \cdot 3 = -282 + 288 = 6 = r_2.$$

3. Ejemplo. Calcular el máximo común divisor d de los números 356 y 260. Encontrar números u y v tales que $356u + 260v = d$. Hacer comprobaciones.

Solución. Primero apliquemos el algoritmo de Euclides:

$$\begin{aligned} 356 &= 260 \cdot 1 + 96; \\ 260 &= 96 \cdot 2 + 68; \\ 96 &= 68 \cdot 1 + 28; \\ 68 &= 28 \cdot 2 + 12; \\ 28 &= 12 \cdot 2 + 4; \\ 12 &= 4 \cdot 3 + 0. \end{aligned}$$

De aquí concluimos que $d = 4$. Comprobamos que 4 es un divisor común de 356 y 260:

$$356 = 4 \cdot 89, \quad \checkmark \qquad\qquad 260 = 65. \quad \checkmark$$

Ahora calculemos u y v usando las fórmulas recursivas (1).

		$q_1 = 1$	$q_2 = 2$	$q_3 = 1$	$q_4 = 2$	$q_5 = 2$
$u_{-1} = 1$	$u_0 = 0$	$u_1 = 1$	$u_2 = -2$	$u_3 = 3$	$u_4 = -8$	$u_5 = 19$
$v_{-1} = 0$	$v_0 = 1$	$v_1 = -1$	$v_2 = 3$	$v_3 = -4$	$v_4 = 11$	$v_5 = -26$

Hemos encontrado u y v:

$$u = 19, \qquad v = -26.$$

Comprobación:

$$19 \cdot 356 - 26 \cdot 260 = 6764 - 6760 = 4. \quad \checkmark$$

□