Theorem 3.14. Let a and b be positive integers. Then

$$(a, b) = s_n a + t_n b,$$

where s_n and t_n are the nth terms of the sequences defined recursively by

$$s_0 = 1, \quad t_0 = 0,$$
$$s_1 = 0, \quad t_1 = 1,$$

and

$$s_j = s_{j-2} - q_{j-1} s_{j-1}, \quad t_j = t_{j-2} - q_{j-1} t_{j-1}$$

for $j = 2, 3, \ldots, n$, where the q_j are the quotients in the divisions of the Euclidean algorithm when it is used to find (a, b).

Proof. We will prove that

$$r_j = s_j a + t_j b \tag{3.2}$$

for $j = 0, 1, \ldots, n$. Since $(a, b) = r_n$, once we have established (3.2), we will know that

$$(a, b) = s_n a + t_n b.$$

We prove (3.2) using the second principle of mathematical induction. For $j = 0$, we have $a = r_0 = 1 \cdot a + 0 \cdot b = s_0 a + t_0 b$. Hence, (3.2) is valid for $j = 0$. Likewise, $b = r_1 = 0 \cdot a + 1 \cdot b = s_1 a + t_1 b$, so that (3.2) is valid for $j = 1$.

Now, we assume that

$$r_j = s_j a + t_j b$$

for $j = 1, 2, \ldots, k - 1$. Then, from the kth step of the Euclidean algorithm, we have

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

Using the induction hypothesis, we find that

$$\begin{aligned} r_k &= (s_{k-2} a + t_{k-2} b) - (s_{k-1} a + t_{k-1} b) q_{k-1} \\ &= (s_{k-2} - s_{k-1} q_{k-1}) a + (t_{k-2} - t_{k-1} q_{k-1}) b \\ &= s_k a + t_k b. \end{aligned}$$

This finishes the proof. ∎

The following example illustrates the use of this algorithm for expressing (a, b) as a linear combination of a and b.

Example 3.14. We summarize the steps used by the extended Euclidean algorithm to express (252, 198) as a linear combination of 252 and 198 in the following table.

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	252	198	1	54	1	0
1	198	54	3	36	0	1
2	54	36	1	18	1	−1
3	36	18	2	0	−3	4
4					4	−5

The values of s_j and t_j, $j = 0, 1, 2, 3, 4$, are computed as follows:

$$\begin{aligned} s_0 &= 1, & t_0 &= 0, \\ s_1 &= 0, & t_1 &= 1, \\ s_2 &= s_0 - s_1q_1 = 1 - 0 \cdot 1 = 1, & t_2 &= t_0 - t_1q_1 = 0 - 1 \cdot 1 = -1, \\ s_3 &= s_1 - s_2q_2 = 0 - 1 \cdot 3 = -3, & t_3 &= t_1 - t_2q_2 = 1 - (-1)3 = 4, \\ s_4 &= s_2 - s_3q_3 = 1 - (-3) \cdot 1 = 4, & t_4 &= t_2 - t_3q_3 = -1 - 4 \cdot 1 = -5. \end{aligned}$$

Because $r_4 = 18 = (252, 198)$ and $r_4 = s_4a + t_4b$, we have

$$18 = (252, 198) = 4 \cdot 252 - 5 \cdot 198.$$ ◄

Note that the greatest common divisor of two integers may be expressed as a linear combination of these integers in an infinite number of ways. To see this, let $d = (a, b)$ and let $d = sa + tb$ be one way to write d as a linear combination of a and b, guaranteed to exist by the previous discussion. Then for all integers k,

$$d = (s + k(b/d))a + (t - k(a/d))b.$$

Example 3.15. With $a = 252$ and $b = 198$, we have $18 = (252, 198) = (4 + 11k)252 + (-5 - 14k)198$ for any integer k. ◄

3.4 Exercises

1. Use the Euclidean algorithm to find each of the following greatest common divisors.

   a) $(45, 75)$ c) $(666, 1414)$
   b) $(102, 222)$ d) $(20785, 44350)$

2. Use the Euclidean algorithm to find each of the following greatest common divisors.

   a) $(51, 87)$ c) $(981, 1234)$
   b) $(105, 300)$ d) $(34709, 100313)$

3. For each pair of integers in Exercise 1, express the greatest common divisor of the integers as a linear combination of these integers.

4. For each pair of integers in Exercise 2, express the greatest common divisor of the integers as a linear combination of these integers.

5. Find the greatest common divisor of each of the following sets of integers.

   a) 6, 10, 15 b) 70, 98, 105 c) 280, 330, 405, 490