The Euclidean Algorithm

THEOREM 1 (Euclidean Algorithm): Let a and b be integers with $a \geq b > 0$. Then there is an algorithm that finds (a, b).

LEMMA: If a, b, q, r are integers and $a = bq + r$, then $(a, b) = (b, r)$.

Proof: We have

$$(a, b) = (bq + r, b)$$

which is equal to (b, r) by Theorem 1 (ii) from Section 3.3. ■

Proof of the Theorem: The idea is to keep repeating the division algorithm. Put $r_0 = a$ and $r_1 = b$. We have:

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2, & 0 \leq r_2 < r_1, &\implies & (r_0, r_1) &= (r_1, r_2) \\
r_1 &= r_2 q_2 + r_3, & 0 \leq r_3 < r_2, &\implies & (r_1, r_2) &= (r_2, r_3) \\
r_2 &= r_3 q_3 + r_4, & 0 \leq r_4 < r_3, &\implies & (r_2, r_3) &= (r_3, r_4) \\
&\dots & & & & \\
r_{n-3} &= r_{n-2} q_{n-2} + r_{n-1}, & 0 \leq r_{n-1} < r_{n-2}, &\implies & (r_{n-3}, r_{n-2}) &= (r_{n-2}, r_{n-1}) \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n, & 0 \leq r_n < r_{n-1}, &\implies & (r_{n-2}, r_{n-1}) &= (r_{n-1}, r_n) \\
r_{n-1} &= r_n q_n, & & \implies & (r_{n-1}, r_n) &= r_n
\end{aligned}$$

therefore

$$(a, b) = (r_0, r_1) = (r_1, r_2) = (r_2, r_3) = (r_3, r_4) = \ldots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = r_n$$

■

REMARK: One can show that if the Euclidean Algorithm requires N steps for the pair $a \geq b > 0$, then $N \leq 5 \log_{10} b$. Thus, the Euclidean Algorithm always needs less than $O(h)$ divisions, where h is the number of digits in the smaller number b.

EXAMPLE: Find

(a) $(252, 198)$ (b) $(326, 78)$ (c) $(4361, 42371)$

Solution: By the Euclidean Algorithm, we have

$$\begin{aligned}
252 &= 198 \cdot 1 + 54 \\
198 &= 54 \cdot 3 + 36 \\
54 &= 36 \cdot 1 + 18 \\
36 &= 18 \cdot 2
\end{aligned}
\qquad
\begin{aligned}
326 &= 78 \cdot 4 + 14 \\
78 &= 14 \cdot 5 + 8 \\
14 &= 8 \cdot 1 + 6 \\
8 &= 6 \cdot 1 + 2 \\
6 &= 2 \cdot 3
\end{aligned}
\qquad
\begin{aligned}
42371 &= 9 \cdot 4361 + 3122 \\
4361 &= 1 \cdot 3122 + 1239 \\
3122 &= 2 \cdot 1239 + 644 \\
1239 &= 1 \cdot 644 + 595 \\
644 &= 1 \cdot 595 + 49 \\
595 &= 12 \cdot 49 + 7 \\
49 &= 7 \cdot 7 + 0
\end{aligned}$$

therefore

$$(252, 198) = 18 \qquad (326, 78) = 2 \qquad (4361, 42371) = 7$$

THEOREM 2: 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

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

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

$$r_j = s_j a + t_j b \tag{2}$$

for $j = 0, 1, \ldots, n$. Because $(a, b) = r_n$, once we have established (2), we will know that

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

We prove (2) by induction.

STEP 1: For $j = 0$ (2) is true, since

$$r_0 = a = 1 \cdot a + 0 \cdot b = s_0 a + t_0 b$$

Similarly, (2) is true for $j = 1$, since

$$r_1 = b = 0 \cdot a + 1 \cdot b = s_1 a + t_1 b$$

STEP 2: Suppose (2) is true for some $j = k - 2$ and $j = k - 1$, $k \geq 2$, that is

$$r_{k-2} = s_{k-2}a + t_{k-2}b \qquad \text{and} \qquad r_{k-1} = s_{k-1}a + t_{k-1}b$$

STEP 3: We prove that (2) is true for $j = k$, that is

$$r_k \stackrel{?}{=} s_k a + t_k b$$

By the kth step of the Euclidean algorithm, we have

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

therefore

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

■

EXAMPLE: Express the greatest common divisor of 252 and 198 as a linear combination of these integers.

Solution 1: 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:

$$\begin{aligned} &s_0 = 1, && t_0 = 0 \\ &s_1 = 0, && t_1 = 1 \\ &s_2 = s_0 - s_1 q_1 = 1 - 0 \cdot 1 = 1, && t_2 = t_0 - t_1 q_1 = 0 - 1 \cdot 1 = -1 \\ &s_3 = s_1 - s_2 q_2 = 0 - 1 \cdot 3 = -3, && t_3 = t_1 - t_2 q_2 = 1 - (-1) \cdot 3 = 4 \\ &s_4 = s_2 - s_3 q_3 = 1 - (-3) \cdot 1 = 4, && t_4 = t_2 - t_3 q_3 = -1 - 4 \cdot 1 = -5 \end{aligned}$$

Because

$$r_4 = 18 = (252, 198) \qquad \text{and} \qquad r_4 = s_4 a + t_4 b$$

we have

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

Moreover,

$$\begin{aligned} 18 = (252, 198) &= \left(4 + \frac{198}{18}k\right) 252 + \left(-5 - \frac{252}{18}k\right) 198 \\ &= (4 + 11k)\, 252 + (-5 - 14k)\, 198 \end{aligned}$$

for any integer k.

Solution 2: By the Euclidean Algorithm, we have

$$\begin{aligned} 252 &= 198 \cdot 1 + 54 \\ 198 &= 54 \cdot 3 + 36 \\ 54 &= 36 \cdot 1 + 18 \\ 36 &= 18 \cdot 2 \end{aligned}$$

From the third equation it follows that

$$18 = 54 - 36 \cdot 1 \tag{3}$$

By the preceding step, it follows that

$$36 = 198 - 54 \cdot 3 \tag{4}$$

Plugging in (4) into (3), we get

$$18 = 54 - 36 \cdot 1 = 54 - (198 - 54 \cdot 3) \cdot 1 = 54 \cdot 4 - 198 \cdot 1 \tag{5}$$

Likewise, by the first step, we have

$$54 = 252 - 198 \cdot 1 \tag{6}$$

Plugging in (6) into (5), we get

$$18 = 54 \cdot 4 - 198 \cdot 1 = (252 - 198 \cdot 1) \cdot 4 - 198 \cdot 1 = 252 \cdot 4 - 198 \cdot 5$$

This last equation exhibits $18 = (252, 198)$ as a linear combination of 252 and 198.

Solution 3: We have

$$\begin{aligned}\frac{252}{198} = 1 + \frac{54}{198} = 1 + \frac{1}{198/54} = 1 + \frac{1}{3 + \frac{36}{54}} = 1 + \frac{1}{3 + \frac{1}{54/36}} \\ = 1 + \frac{1}{3 + \frac{1}{1 + \frac{18}{36}}} \\ = 1 + \frac{1}{3 + \frac{1}{1 + \frac{1}{2}}}\end{aligned}$$

Then

$$-\frac{t_4}{s_4} = 1 + \frac{1}{3 + \frac{1}{1+0}} = 1 + \frac{1}{3+1} = 1 + \frac{1}{4} = \frac{5}{4}$$

EXAMPLE: Express 1 as a linear combination of 5 and 8.

Solution: We have

$$\frac{8}{5} = 1 + \frac{3}{5} = 1 + \frac{1}{5/3} = 1 + \frac{1}{1 + \frac{2}{3}} = 1 + \frac{1}{1 + \frac{1}{3/2}} = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}$$

Then

$$-\frac{t_4}{s_4} = 1 + \frac{1}{1 + \frac{1}{1+0}} = 1 + \frac{1}{1+1} = 1 + \frac{1}{2} = \frac{3}{2}$$

Therefore

$$1 = 8 \cdot 2 - 5 \cdot 3$$

EXAMPLE: Express 1 as a linear combination of 21 and 34.

Solution: We have

$$\frac{34}{21} = 1 + \frac{13}{21} = 1 + \frac{1}{21/13} = 1 + \frac{1}{1 + \frac{8}{13}} = 1 + \frac{1}{1 + \frac{1}{13/8}}$$

$$= 1 + \frac{1}{1 + \frac{1}{1 + \frac{5}{8}}}$$

$$= 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{8/5}}}$$

$$= 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{3}{5}}}}$$

$$= 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{5/3}}}}$$

$$= 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{2}{3}}}}}$$

$$= 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{3/2}}}}}$$

$$= 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}}}}$$

Then

$$-\frac{t_7}{s_7} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1+0}}}}} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1+\frac{1}{2}}}} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3/2}}}$$

$$= 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{2}{3}}}$$

$$= 1 + \cfrac{1}{1 + \cfrac{1}{5/3}}$$

$$= 1 + \cfrac{1}{1 + \cfrac{3}{5}}$$

$$= 1 + \cfrac{1}{8/5}$$

$$= 1 + \frac{5}{8}$$

$$= \frac{13}{8}$$

Therefore

$$1 = 21 \cdot 13 - 34 \cdot 8$$