The Euclidean Algorithm

Lemma : (1.3)

If $a = bq + r$, then $(a, b) = (b, r)$.

Proof. Let $d = (a, b)$, that is $d \mid a$ and $d \mid b$. From the equation $a = bq + r$, it follows that $d \mid r$. Thus, d is a common divisor of b and r.

Suppose c is any common divisor of b and r. We know that $c \mid b$ and $c \mid r$, so it follows from $a = bq + r$ that $c \mid a$. Thus, c is a common divisor of a and b, and hence $c \leq d$. Therefore, by definition, d is the greatest common divisor of b and r.

So, we have that $(a, b) = d = (b, r)$ as desired. □

Example

Find the greatest common divisor of 70 and 21.

By the Division Algorithm, we have that:

$$70 = 3 \cdot 21 + 7$$

Therefore, by Lemma 1.3,

$$(70, 21) = (21, 7) = 7$$

Theorem : The Euclidean Algorithm

If a and b are positive integers, $b \neq 0$ and

$$\begin{aligned} a &= bq + r, & 0 \leq r < b \\ b &= rq_1 + r_1, & 0 \leq r_1 < r \\ r &= r_1 q_2 + r_2 & 0 \leq r_2 < r_1 \\ &\vdots \end{aligned}$$

Then for k large enough, say $k = t$, we have that $r_{t-1} = r_t q_{t+1}$ and $(a, b) = r_t$.

Proof. The sequence of non-negative integers must end

$$b > r > r_1 > r_2 > \cdots \geq 0$$

Eventually, one of the remainders will be zero, suppose it is r_{t+1}. Then we have that $r_{t-1} = r_t q_{t+1}$. Applying Lemma 1.3 repeatedly, we have

$$(a, b) = (b, r) = (r, r_1) = (r_1, r_2) = \cdots = (r_{t-1}, r_t) = r_t$$

If either a or b is negative, we can use that

$$(a, b) = (-a, b) = (a, -b) = (-a, -b)$$

□

Example

Apply the Euclidean Algorithm to calculate $(662, 414)$.

By applying the Division Algorithm, we have that

$$\begin{aligned} 662 &= 1 \cdot 414 + 248 \\ 414 &= 1 \cdot 248 + 166 \\ 248 &= 1 \cdot 166 + 82 \\ 166 &= 2 \cdot 82 + 2 \\ 82 &= 41 \cdot 2 \end{aligned}$$

Thus, by the Euclidean Algorithm, we have that $(662, 414) = 2$.

Example

Apply the Euclidean Algorithm to calculate $(343, 280)$.

By applying the Division Algorithm, we have that

$$\begin{aligned} 343 &= 1 \cdot 280 + 63 \\ 280 &= 4 \cdot 63 + 28 \\ 63 &= 2 \cdot 28 + 7 \\ 28 &= 4 \cdot 7 \end{aligned}$$

Thus, by the Euclidean Algorithm, we have that $(343, 280) = 7$.

Theorem : (1.4)

If $(a, b) = d$, then there are integers x and y such that

$$ax + by = d$$

Example

Find integers x and y such that $343x + 280y = 7$.

By working the Euclidean Algorithm backwards, we have that

$$\begin{aligned} 7 &= 63 - 2 \cdot 28 \\ 7 &= 63 - 2 \cdot (280 - 4 \cdot 63) \\ 7 &= 9 \cdot 63 - 2 \cdot 280 \\ 7 &= 9 \cdot (343 - 1 \cdot 280) - 2 \cdot 280 \\ 7 &= 9 \cdot 343 - 11 \cdot 280 \end{aligned}$$

Therefore, the integers are $x = 9$, and $y = -11$.

Corollary : (1.1)

If $d \mid (ab)$ and $(d, a) = 1$, then $d \mid b$.

Proof. From Theorem 1.4, we have that there are integers x and y such that

$$dx + ay = 1$$

$$d\,(bx) + (ab)\,y = b$$

Since $d \mid (bx)$ and since $d \mid (ab)$ by assumption, we have that $d \mid b$. □

Corollary : (1.2)

Let $(a, b) = d$, and suppose that $c \mid a$ and $c \mid b$, then $c \mid d$.

Proof. From Theorem 4, we have that there are integers x and y such that

$$ax + by = d$$

Since $c \mid (ax)$ and $c \mid (by)$, we have that $c \mid d$. □

Corollary : (1.3)

If $a \mid m$, $b \mid m$, and $(a, b) = 1$, then $(ab) \mid m$.

Proof. There is an integer q such that $m = bq$. Since $a \mid m$ and $(a, b) = 1$, Corollary 1.1 says that $a \mid q$. Therefore, there is an integer r such that $q = ar$. Thus, we have that $m = bq = bar$. This shows $(ab) \mid m$. □