The Euclidean Algorithm

Learning Objectives. By the end of class, students will be able to:

- Prove the Euclidean Algorithm halts and generates the greatest common divisor of two positive integers
- Use the Euclidean Algorithm to findd the greate common divisor of two integers
- Use the (extended) Euclidean algorithm to write (a, b) as a linear combination of a and b.

Typically by *Euclidean Algorithm*, we mean both the algorithm and the theorem that the algorithm always generates the greatest common divisor of two (positive) integers.

Theorem (Euclidean algorithm)**.** *Let $a, b \in \mathbb{Z}$ with $a \geq b > 0$. By the* **??**, *there exist $q_1, r_1 \in \mathbb{Z}$ such that*

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b.$$

If $r_1 > 0$, there exist $q_2, r_2 \in \mathbb{Z}$ such that

$$b = r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1.$$

If $r_2 > 0$, there exist $q_3, r_3 \in \mathbb{Z}$ such that

$$r_1 = r_2 q_3 + r_3, \quad 0 \leq r_3 < r_2.$$

Continuing this process, $r_n = 0$ for some n. If $n > 1$, then $\gcd(a, b) = r_{n-1}$. If $n = 1$, then $\gcd(a, b) = b$.

Proof *Note that $r_1 > r_2 > r_3 > \cdots \geq 0$ by construction. If the sequence did not stop, then we would have an infinite, decreasing sequence of positive integers, which is not possible. Thus, $r_n = 0$ for some n.*

When $n = 1$, $a = bq + 0$ and $\gcd(a, b) = b$.

?? *states that for $a = bq_1 + r_1$, $\gcd(a, b) = \gcd(b, r_1)$. This is because any common divisor of a and b is also a divisor of $r_1 = a - bq_1$.*

If $n > 1$, then by repeated application of the **??**, *we have*

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-2}, r_{n-1})$$

Then $r_{n-2} = r_{n-1} q_n + 0$. Thus $\gcd(r_{n-2}, r_{n-1}) = r_{n-1}$. ∎

When using the Euclidean algorithm, it can be tricky to keep track of what is happening. Doing a lot of examples can help.

Work in pairs to answer the following. Each pair will be assigned parts the following question.

In-class Problem 1 *Find the greatest common divisors of the pairs of integers below and write the greatest common divisor as a linear combination of the integers.*

(a) $(21, 28)$

Learning outcomes:
Author(s): Claire Merriman

Solution: *By inspection:* $28 - 21 = 7$.

Using the Euclidean algorithm: $a = 28, b = 21$

$$\begin{array}{lll} 28 = 21(1) + 7 & q_1 = 1, r_1 = 7 & 7 = 21(1) + 28(-1) \\ 21 = 7(3) + 0 & q_2 = 3, r_2 = 0 & \end{array}$$

so $28 + (-1)21 = 7 = (28, 21)$

(b) $(32, 56)$

Solution: *Using the Euclidean algorithm:* $a = 56, b = 32$

$$\begin{array}{lll} 56 = 32(1) + 24 & q_1 = 1, r_1 = 24 & 24 = 56(1) + 32(-1) \\ 32 = 24(1) + 8 & q_2 = 1, r_2 = 8 & 8 = 32(1) + 24(-1) = 32(1) + (56(1) + 32(-1))(-1) = 32(2) + 56(-1) \\ 32 = 8(4) + 0 & q_3 = 4, r_3 = 0. & \end{array}$$

so $56(-1) + 32(2) = 8 = (56, 32)$

(c) $(0, 113)$

Solution: *Since* $0 = 113(0)$, $(0, 113) = 113 = 0(0) = 113(1)$.

(a) $(78, 708)$

Solution: *Using the Euclidean algorithm:* $a = 708, b = 78$

$$\begin{array}{lll} 708 = 78(9) + 6 & q_1 = 9, r_1 = 6 & 6 = 708(1) + 78(-9) \\ 78 = 6(13) + 0 & q_2 = 13, r_2 = 0. & \end{array}$$

so $708(1) + 78(-6) = 6 = (78, 708)$