IV.16. The Euclidean algorithm

Given integers $a$ and $b$, we say that $d$ is a **common divisor** of $a$ and $b$ if $d$ divides $a$ and $d$ divides $b$.

Given integers $a$ and $b$, not both equal to zero, their **greatest common divisor** $\gcd(a, b)$ is the largest integer that is a common divisor of $a$ and $b$. (Definition 11.3.1 in Eccles is more formally worded.)

**Exercise.** Show that such an integer always exists. Hint: If $d \mid b$ and $b \neq 0$, then $d \leq |b|$.

The division theorem and the following lemma form the basis for the Euclidean algorithm which is a method to compute the greatest common divisor of two positive integers.

**Lemma 1 (Eccles 16.1.1)** Suppose that $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$ are such that $b$ divides $a$. Then $\gcd (a, b) = b$.

**Proof.** Since $b$ divides $b$ and by the hypothesis, $b$ is a common divisor of $a$ and $b$. On the other hand, since any common divisor $d$ of $a$ and $b$ must be a divisor of $b$, we have $d \leq |b| = b$ (the equality since $b \in \mathbb{Z}^+$). Hence $b$ is the greatest common divisor of $a$ and $b$.

**Lemma 2 (Eccles 16.1.2)** For nonzero integers $a$ and $b$ suppose that

$$a = bq + r \text{ where } q, r \in \mathbb{Z}.$$  

Then

$$\gcd (a, b) = \gcd (b, r).$$

**Proof.** Suppose that $d$ is a common divisor of $a$ and $b$. Then $d$ divides the integer combination of $a$ and $b$:

$$a - bq = r.$$  

Hence $d$ is a common divisor of $b$ and $r$.

Conversely, if $d$ is a common divisor of $b$ and $r$, then $d$ divides the integer combination of $b$ and $r$:

$$bq + r = a.$$  

Hence $d$ is a common divisor of $b$ and $a$.

Since the common divisors of $a$ and $b$ are the same as the common divisors of $b$ and $r$, we conclude that $\gcd (a, b) = \gcd (b, r)$. $\square$
The **Euclidean algorithm** is a way to find the gcd of two positive integers $a$ and $b$. It is best to describe this by an example. Let us find the gcd of 4199 and 1748. The idea is to apply the division algorithm repeatedly.

(1) Divide the larger integer 4199 and by the smaller 1748 to get

$$4199 = 2 \cdot 1748 + 703,$$

which yields the remainder 703. By Theorem 16.1.2, \( \gcd(4199, 1748) = \gcd(1748, 703) \).

(2) Divide 1748 by 703 to obtain

$$1748 = 2 \cdot 703 + 342,$$

which yields the remainder 342. By T16.1.2, \( \gcd(1748, 703) = \gcd(703, 342) \).

(3) Divide 703 by 342 to obtain

$$703 = 2 \cdot 342 + 19,$$

which yields the remainder 19. As above, \( \gcd(703, 342) = \gcd(342, 19) \).

(4) Divide 342 by 19 to obtain

$$342 = 18 \cdot 19 + 0,$$

which yields the remainder 0. By Theorem 16.1.1, \( \gcd(342, 19) = 19 \).

To summarize, by the Euclidean algorithm,

\[
\gcd (4199, 1748) = \gcd (1748, 703) \\
= \gcd (703, 342) \\
= \gcd (342, 19) \\
= 19.
\]
Next we show how we may use the Euclidean algorithm to write the gcd 19 as an integer combination of 4199 and 1748. Summarizing the Euclidean algorithm, we computed:

\[
\begin{align*}
4199 &= 2 \cdot 1748 + 703, \\
1748 &= 2 \cdot 703 + 342, \\
703 &= 2 \cdot 342 + 19 \\
342 &= 18 \cdot 19 + 0.
\end{align*}
\]

Using this, we can write 19 as a combination of 4199 and 1748 by working backward. We have

\[
19 = 703 - 2 \cdot 342.
\]

Substituting 342 = 1748 - 2 \cdot 703, we have

\[
19 = 703 - 2 \cdot (1748 - 2 \cdot 703) = -2 \cdot 1748 + 5 \cdot 703.
\]

Substituting 703 = 4199 - 2 \cdot 1748,

\[
19 = -2 \cdot 1748 + 5 \cdot (4199 - 2 \cdot 1748) = 5 \cdot 4199 - 12 \cdot 1748. \tag{1}
\]