IV.16. The Euclidean algorithm

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 16.1.2) For positive integers $a$ and $b$ suppose that

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

Then

\[ \gcd(a, b) = \gcd(b, r). \]

Proof. Suppose that $c$ is a common divisor of $a$ and $b$. Then $c$ divides $1 \cdot a + (-q) \cdot b = a - bq = r$. Hence $c$ is a common divisor of $b$ and $r$.

Conversely, if $c$ is a common divisor of $b$ and $r$, then $c$ divides $q \cdot b + 1 \cdot r = bq + r = a$. Hence $c$ is a common divisor of $a$ and $b$.

Since the common divisors of $a$ and $b$ are the same as the common divisors of $b$ and $r$, we conclude that $\gcd(a, b) = \gcd(b, r)$. □

Remark. We proved that if $c$ is a common divisor of $a$ and $b$, then $c$ is a common divisor of $b$ and $r$. That is, if $c \in D(a) \cap D(b)$, then $c \in D(b) \cap D(r)$. Thus

\[ \gcd(a, b) = \max(D(a) \cap D(b)) \leq \max(D(b) \cap D(r)) = \gcd(b, r). \]

Similarly, what we did in the second paragraph of the proof yields $\gcd(b, r) \leq \gcd(a, b)$. Hence we have equality.

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.

(2) Divide 1748 by 703 to obtain

\[ 1748 = 2 \cdot 703 + 342, \]
which yields the remainder 342.

(3) Divide 703 by 342 to obtain

\[ 703 = 2 \cdot 342 + 19, \]

which yields the remainder 19.

(4) Divide 342 by 19 to obtain

\[ 342 = 18 \cdot 19 + 0, \]

which yields the remainder 0.

The Euclidean algorithm says that the gcd of 4199 and 1748 is the last nonzero remainder, namely 19.

Let us understand why. By Eccles Lemma 16.1.2,

\[
gcd(4199, 1748) = gcd(1748, 703) \\
= gcd(703, 342) \\
= gcd(342, 19) \\
= 19
\]

since 19 divides 342.

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:

\[
4199 = 2 \cdot 1748 + 703, \\
1748 = 2 \cdot 703 + 342, \\
703 = 2 \cdot 342 + 19 \\
342 = 18 \cdot 19 + 0.
\]

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 $703 = 4199 - 2 \cdot 1748$,

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

Formalizing the Euclidean algorithm:

**Theorem 2 (Eccles 16.2.1)** We have the following table of positive integers:

\[
\begin{array}{c|c|c|c|c}
\hline
a_0 \div a & a_1 \div b & \gcd(a_0, a_1) = \gcd(a, b) \\
\hline
a_1 = b & a_2 = r \div r_1 & a_0 = a = bq + r \div a_1q_1 + r_1 & \gcd(a_1, a_2) = \gcd(b, r) = \gcd(a, b) \\
\hline
a_2 = r_1 & a_3 = r_2 & a_1 = b = rq_2 + r_2 = a_2q_2 + r_2 & \gcd(a_2, a_3) = \gcd(a, b) \\
\hline
a_3 = r_2 & a_4 = r_3 & a_2 = r_2q_3 + r_3 = a_3q_3 + r_3 & \gcd(a_3, a_4) = \gcd(a, b) \\
\hline
\vdots & \vdots & \vdots & \vdots \\
\hline
a_k+1 = r_k & a_k = r_kq_{k+1} + 0 = a_{k+1}q_{k+1} + 0 & a_{k+1} = r_k = \gcd(a, b) \\
\hline
\end{array}
\]

That is, by division and calculating remainders, we obtain a strictly decreasing sequence of positive integers ending at zero:

\[
a_0 = a > a_1 = b > a_2 = r > r_2 > \cdots > r_k > r_{k+1} = 0.
\]

Then \( \gcd(a, b) = r_k \) is the penultimate remainder.

The statement that \( 19 = \gcd(4199, 1748) \) can be written as an integer combination of 4199 and 1748 (i.e., \( 19 = 5 \cdot 4199 - 12 \cdot 1748 \)) is an example of the following result.

**Theorem 3 (Eccles 17.1.1)** If \( a, b \in \mathbb{Z}^+ \), then there exist \( m, n \in \mathbb{Z} \) such that

\[
\gcd(a, b) = am + bn.
\]

That is, the gcd of \( a \) and \( b \) can be written as an integral linear combination of \( a \) and \( b \) (i.e., a linear combination of \( a \) and \( b \) using integer coefficients).