Notes on the EUCLIDEAN ALGORITHM

Recall the following fact about divisors.

**Lemma 1 (See Exercise 62 in Chapter 1)** Let \(a, b, c, m, n\) be integers. If \(a\) divides both \(b\) and \(c\), then \(a\) divides \(bm + cn\).

**Remark 2** For example, since \(6\) divides \(18\) and \(24\), for any \(m, n \in \mathbb{Z}\), we have that \(6\) divides \(18m + 24n\).

**Proof of Lemma 1.** By hypothesis, there exist \(k, \ell \in \mathbb{Z}\) such that \(b = ka\) and \(c = \ell a\).

This implies \(bm + cn = (ka) m + (\ell a) n = a (mk + n\ell)\).

Since \(mk + n\ell \in \mathbb{Z}\), the conclusion follows. \(\blacksquare\)

**Fact.** If \(d_1\) and \(d_2\) are natural numbers such that \(d_1 \mid d_2\) and \(d_2 \mid d_1\), then \(d_1 = d_2\). (Reason: \(a \in \mathbb{Z}\), \(b \in \mathbb{N}\), and \(a\mid b\) implies \(a \leq b\).

**Definition 3** (gcd) Let \(a\) and \(b\) be integers, not both 0. Then the largest natural number that divides both \(a\) and \(b\) is called the **greatest common divisor** of \(a\) and \(b\) and is denoted by \(\gcd (a, b)\).

**Example.** The gcd of 18 and 60 is equal to 6.

We have the following fact about the gcd and the division algorithm.

**Lemma 4 (See Exercise 92 in Chapter 3)** If \(b \in \mathbb{Z} - \{0\}\) and \(a, q, r \in \mathbb{Z}\) satisfy

\[ a = bq + r, \]

then

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

**Proof.** \((\leq)\) Let \(d = \gcd (b, r)\). Since \(d\mid b\) and \(d\mid r\), by Lemma 1 we have \(d\) divides \(bq + r = a\). That is, \(d\) is a common divisor of \(a\) and \(b\). Hence

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

\((\geq)\) Let \(e = \gcd (a, b)\). Since \(e\mid a\) and \(e\mid b\), by Lemma 1 we have \(e\) divides \(a - bq = r\). That is, \(e\) is a common divisor of \(b\) and \(r\). Hence

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

We conclude that \(\gcd (a, b) = \gcd (b, r)\). \(\blacksquare\)
Part of the Euclidean algorithm (writing the gcd as a combination of $a$ and $b$). Let $a$ and $b$ be integers, not both 0. Then there exist integers $m, n \in \mathbb{Z}$ such that
\[ \gcd(a, b) = am + bn. \]
For example, since the gcd of 8 and 60 is 4, there exist $m, n \in \mathbb{Z}$ such that
\[ 4 = 8m + 60n. \]
For example, $4 = 8 \cdot 8 + 60 \cdot (-1)$.

**Theorem 5 (See Theorem 3.9)** Let $a$ and $b$ be integers, not both 0. Then $\gcd(a, b)$ is the only natural number $d$ such that

1. $d$ divides both $a$ and $b$, and
2. If $c$ is an integer such that $c$ divides both $a$ and $b$, then $c$ divides $d$.$^{1}$

**Proof.** By the Euclidean Algorithm (see below), there exist integers $m, n \in \mathbb{Z}$ such that
\[ \gcd(a, b) = am + bn. \]
Hence by Lemma 1, if $c$ divides both $a$ and $b$, then $c$ divides $\gcd(a, b)$. This shows that $\gcd(a, b) \in \mathbb{N}$ has properties (1) and (2).

Suppose $d, d' \in \mathbb{N}$ both satisfy properties (1) and (2). Then $d|d'$ and $d'|d$. So $d = d'$. This proves that $\gcd(a, b)$ is the only natural number satisfying properties (1) and (2). $\blacksquare$

**Example.** The gcd of 36 and 60 is equal to 12. (1) 12 divides both 36 and 60. (2) The common divisors of 36 and 60 are
\[ 1, -1, 2, -2, 3, -3, 4, -4, 6, -6, 12, -12. \]
Each of these common divisors divides 12.

The Euclidean algorithm (to find the gcd and to write it as a combination of $a$ and $b$).

**Example of Euclidean Algorithm.** Find the gcd of 4199 and 1748. Applying the division algorithm repeated, we have the following:
\[
\begin{align*}
4199 &= 2 \cdot 1748 + 703, \\
1748 &= 2 \cdot 703 + 342, \\
703 &= 2 \cdot 342 + 19 \\
342 &= 18 \cdot 19 + 0.
\end{align*}
\]
The gcd of 4199 and 1748 is the last nonzero remainder, namely 19.

$^{1}$If the conclusion was instead that $c \leq d$, we would just be repeating the definition of $\gcd$.
We can write 19 as a combination of 4199 and 1748 by working backward:

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

Substituting 342 = 1748 − 2 · 703,

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

Substituting 703 = 4199 − 2 · 1748,

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

**Lemma 6** If \( d \) is a common divisor of \( a \) and \( b \) and if \( d \) and be written as a combination of \( a \) and \( b \), then \( d = \gcd (a, b) \).

**Proof.** By hypothesis, there exist integers \( m, n \in \mathbb{Z} \) such that

\[ d = am + bn. \quad (1) \]

Suppose \( c \) divides both \( a \) and \( b \). Then by (1), \( c \) divides \( d \). By Theorem 5, \( d = \gcd (a, b) \). □

**General Case of the Euclidean Algorithm.** Let \( a \in \mathbb{Z} \) and \( b \in \mathbb{N} \). The division algorithm for \((a, b)\) implies that there exist \( q_1, r_1 \in \mathbb{Z} \) such that

\[ a = bq_1 + r_1 \quad \text{and} \quad 0 \leq r_1 < b. \]

If \( r_1 = 0 \), then \( a = bq_1 \), so that

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

which of course is a combination of \( a \) and \( b \) (\( = 0 \cdot a + 1 \cdot b \)).

So suppose \( r_1 > 0 \). Then the division algorithm for \((b, r_1)\) implies that there exist \( q_2, r_2 \in \mathbb{Z} \) such that

\[ b = r_1q_2 + r_2 \quad \text{and} \quad 0 \leq r_2 < r_1. \]

If \( r_2 = 0 \), then \( b = r_1q_2 \) so that \( r_1 \) divides \( b \). Moreover,

\[ a = bq_1 + r_1, \]

so that \( r_1 \) divides \( a \) and

\[ r_1 = a - bq_1, \]

which is a combination of \( a \) and \( b \). By Lemma 6, \( r_1 = \gcd (a, b) \).

Continuing this way we get a sequence of divisors:

\[ r_1 > r_2 > \cdots > r_n > r_{n+1} = 0. \]

One can show that \( r_n = \gcd (a, b) \). We will not discuss this proof in detail. For the interested reader, see the proof of Theorem 3.9 in the book.