7 THE EUCLIDEAN ALGORITHM

This is a method for finding the greatest common divisor of two integers, and of expressing this in terms of the original integers. It involves repeated application of a type of division.

Before we start we state a technical lemma which we will need later.

Lemma 7.1 Let \( A \) be a non-empty finite set of real numbers. Then \( A \) has a minimum and a maximum element (i.e., \( \exists a, b \in A \) such that \( \forall x \in A, a \leq x \leq b \)).

Proof. An easy induction argument. \( \square \)

7.1 The Division Theorem

Theorem 7.2 (Division Theorem) Let \( a, b \in \mathbb{Z} \) with \( b > 0 \). Then there are unique integers \( q \) and \( r \) such that \( a = bq + r \) and \( 0 \leq r < b \).

Remark: We call \( r \) the remainder.

Proof. Suppose first that \( a > 0 \). Write \( A = \{ k \in \mathbb{Z} : k \geq 0, bk \leq a \} \). Since \( 0 \in A \), we have \( A \neq \emptyset \). Also \( A \) is finite since \( k \in A \Rightarrow 0 \leq k \leq bk \leq a \). Hence by Lemma 7.1 \( A \) has a maximal element, say \( q \).

Set \( r = a - bq \). Note that \( r \geq 0 \) since \( q \in A \). We need to show that \( r < b \).

Suppose that \( r \geq b \).

Then \( r = b + s \) for some \( s \in \mathbb{Z} \) with \( s \geq 0 \). So

\[
q + 1 \in A,
\]

so \( q + 1 \in A \), contradicting the maximality of \( q \). So \( r < b \) after all.

Hence we have proved that (when \( a > 0 \)) \( q = bq + r \) with \( 0 \leq r < b \).

If \( a = 0 \), then we may take \( r = 0 \).

Suppose \( a < 0 \). Then \( -a > 0 \), and by the first part of the proof \( \exists q_1, r_1 \in \mathbb{Z} \) with \( 0 \leq r_1 < b \) such that \( -a = bq_1 + r_1 \). So \( a = b(-q_1) - r_1 \).

If \( r_1 = 0 \), then \( a = b(-q_1) \) as required.

If \( r_1 > 0 \), then \( a = b(-q_1 - 1) + (b - r_1) \). Since \( 0 < r_1 < b \), we have \( 0 < b - r_1 < b \) (so we may take \( q = -(q_1 - 1) \) and \( r = b - r_1 \)).

Uniqueness of \( q \) and \( r \): Suppose \( a = bq_1 + r_1 = bq_2 + r_2 \), where \( q_1, q_2, r_1, r_2 \in \mathbb{Z} \), \( 0 \leq r_1 < b \) and \( 0 \leq r_2 < b \). We will show that \( q_1 = q_2 \) and \( r_1 = r_2 \).

Without loss of generality we may assume that \( q_1 \geq q_2 \).

0 \leq r_1 = a - bq_1 \leq a - bq_2 = r_2 < b \) (since \( b > 0 \) implies \( bq_1 \geq bq_2 \)).

So \( 0 \leq r_2 - r_1 = (a - bq_2) - (a - bq_1) = -bq_2 + bq_1 = b(q_1 - q_2) \).

Now \( r_2 - r_1 < b \) (since \( 0 \leq r_1 < b \) and \( 0 \leq r_2 < b \), so \( 0 \leq (q_1 - q_2)b < b \)). Hence \( 0 \leq q_1 - q_2 < 1 \).

But \( q_1 - q_2 \in \mathbb{Z} \), so \( q_1 - q_2 = 0 \). Hence \( q_1 = q_2 \), so \( r_1 = r_2 \). \( \square \)
7.2 The greatest common divisor

We will define the greatest common divisor of two integers. To do this we first introduce some new notation.

Let \( a \in \mathbb{Z} \). Define \( D(a) = \{d : d \in \mathbb{Z}, d|a\} \), the set of divisors of \( a \). Note that 1, \( a \in D(a) \), so \( D(a) \neq \emptyset \).

Note that \( D(0) = \mathbb{Z} \), since \( \forall d \in \mathbb{Z}, 0 = 0.d \).

If \( a \neq 0 \), then \( D(a) \subseteq \{d : d \in \mathbb{Z}, |d| \leq |a|\} \), so \( D(a) \) is finite.

If \( a, b \in \mathbb{Z} \), not both zero, then \( D(a) \cap D(b) \) is finite and non-empty (since 1 \( \in D(a) \cap D(b) \)). Hence by Lemma 7.1 \( D(a) \cap D(b) \) has a maximal element. We call this maximal element the greatest common divisor of \( a \) and \( b \), written gcd\((a, b)\).

[The greatest common divisor is sometimes called the highest common factor, and written hcf\((a, b)\).]

Equivalent definition of gcd\((a, b)\): If \( d = \text{gcd}(a, b) \), then \( d|a \) and \( d|b \), and if \( c \in \mathbb{Z} \) such that \( c|a \) and \( c|b \), then \( c \leq d \).

Example: \( a = 24, b = 15 \).
\[
D(a) = \{-1, 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24\}.
\]
\[
D(b) = \{-1, 1, \pm 3, \pm 5, \pm 15\}.
\]
\[
D(a) \cap D(b) = \{-1, 1, \pm 3\}.
\]
\[
gcd(24, 15) = 3.
\]

Remarks:
(i) If \( a \neq 0 \), then \( \text{gcd}(a, 0) = a \).
(ii) If \( p \) is prime and \( a \neq 0 \), then
\[
\text{gcd}(p, a) = \begin{cases} 1 & \text{if } p \nmid a \\ p & \text{if } p|a. \end{cases}
\]

Lemma 7.3 Let \( a, b \in \mathbb{Z} \) with \( a \neq 0 \) and \( b \neq 0 \). Suppose \( q, r \in \mathbb{Z} \) with \( a = qb + r \). Then
\[
\text{gcd}(a, b) = \text{gcd}(b, r).
\]
In particular, if \( a = qb \), then \( \text{gcd}(a, b) = \text{gcd}(b, 0) = b. \)

Proof. Write \( d = \text{gcd}(a, b) \) and \( e = \text{gcd}(b, r) \).
Then \( d|a \) and \( d|b \), so \( d|(a - bq) \), and so \( d|r \) (and \( d|b \)). Hence \( d \leq \text{gcd}(b, r) = e \).
Also \( e|b \) and \( e|r \), so \( e|(bq + r) \), and so \( e|a \) (and \( e|b \)). Hence \( e \leq \text{gcd}(a, b) = d \).
Hence \( d = e \).
7.3 The Euclidean algorithm

Let \( a, b \in \mathbb{N} \). Assume that \( a > b \).

Using the Division Theorem and Lemma 7.3, define integers \( a_0, a_1, a_2, \ldots, q_1, q_2, \ldots \) and \( r_1, r_2, \ldots \) as follows:

\[
\begin{align*}
a_0 &= a \\
a_1 &= b \\
a_0 &= q_1a_1 + r_1, & \text{where } 0 \leq r_1 < a_1 \\
\text{If } r_1 = 0, \text{ then stop} \\
\text{If } r_1 \neq 0, \text{ then write } a_2 &= r_1 \\
\text{If } r_2 = 0, \text{ then stop} \\
\text{If } r_2 \neq 0, \text{ then write } a_3 &= r_2 \\
\vdots & \quad \vdots \\
\vdots & \quad \vdots \\
a_{n-2} &= q_{n-1}a_{n-1} + r_{n-1}, & \text{where } 0 \leq r_{n-1} < a_{n-1} \\
\text{If } r_{n-1} = 0, \text{ then stop} \\
\text{If } r_{n-1} \neq 0, \text{ then write } a_n &= r_{n-1} \\
a_{n-1} &= a_nq_n \\
\text{gcd}(a_0, a_1) &= \text{gcd}(a_1, a_2) \\
\text{gcd}(a_1, a_2) &= \text{gcd}(a_2, a_3) \\
\text{gcd}(a_{n-2}, a_{n-1}) &= \text{gcd}(a_{n-1}, a_n) \\
\text{gcd}(a_{n-1}, a_n) &= a_n
\end{align*}
\]

Note that \( a_n < a_{n-1} < \cdots < a_1 < a_0 \), so the process must eventually stop (in the description above we are illustrating it stopping at \( a_n \)).

By this process \( \text{gcd}(a, b) = r_{n-1} = a_n \).

Examples:

(i) \( a = 2301, b = 1989 \).

\[
\begin{align*}
2301 &= 1 \times 1989 + 312 \\
(2301 &= q_1 \times a_1 + r_1 = a_2) \\
1989 &= 6 \times 312 + 117 \\
(a_1 &= q_2 \times a_2 + r_2 = a_3) \\
312 &= 2 \times 117 + 78 \\
(a_2 &= q_3 \times a_3 + r_3 = a_4) \\
117 &= 1 \times 78 + 39 \\
(a_3 &= q_4 \times a_4 + r_4 = a_5) \\
78 &= 2 \times 39 \\
(a_4 &= q_5 \times a_5) \\
\text{gcd}(a, b) &= a_5 = 39.
\end{align*}
\]

(ii) \( a = 1239, b = 336 \).

\[
\begin{align*}
1239 &= 3 \times 336 + 231 \\
336 &= 1 \times 231 + 105 \\
231 &= 2 \times 105 + 21 \\
105 &= 5 \times 21 \\
\text{gcd}(a, b) &= \text{gcd}(1239, 336) = 21.
\end{align*}
\]

Reversing the process:
\[ 21 = 231 - 2 \times 105 \]
\[ = 231 - 2 \times (336 - 1 \times 231) \]
\[ = -2 \times 336 + 3 \times 231 \]
\[ = -2 \times 336 + 3 \times (1239 - 3 \times 336) \]
\[ = 3 \times 1239 - 11 \times 336 \]

Hence \( \gcd(a, b) = 3a - 11b \).

More generally, reversing the Euclidean algorithm the following very powerful result is clear:

**Theorem 7.4** Let \( a, b, \in \mathbb{Z} \) with \( a, b > 0 \). Then \( \exists s, t \in \mathbb{Z} \) such that \( \gcd(a, b) = sa + tb \).

As an application, we can complete the proof of the alternative characterisation of primes from Section 2.

**Corollary 7.5** Let \( p \) be a prime. Then \( \forall a, b, \in \mathbb{N}, p \mid ab \Rightarrow p \mid a \) or \( p \mid b \).

**Proof.** If \( p \mid a \), then we are done. Suppose that \( p \nmid a \). Then \( \gcd(p, a) = 1 \), and so by Theorem 7.4 \( \exists s, t \in \mathbb{Z} \) such that \( sp + ta = 1 \). Hence \( b = sp + tab \). Since \( p \mid spb \) and \( p \mid tab \), we have \( p \mid b \), as required.