1 Basic properties of the integers

In this lesson and onwards, we consider $\mathbb{Z}$ to be the set of integers numbers, whereas $\mathbb{Z}^+$ is the set of strictly positive integers numbers.

Definition 1.1. Let $a, b \in \mathbb{Z}$, with $a \neq 0$, then a is a divisor of b if there is an integer c such that $a \cdot c = b$. We denote this by $a \mid b$.

Remark 1. If a does not divide b, we write $a \nmid b$.

Theorem 1.1. *Let $a, b \in \mathbb{Z} \setminus \{0\}$, there is a unique positive integer d, called the **greatest common divisor of** a **and** b, satisfying*

1. *$d \mid a$ and $d \mid b$.*
2. *If $e \mid a$ and $e \mid b$ then $e \mid d$.*

Remark 2. If d is the greatest common divisor of a and b, we write $d = (a, b)$. In particular, if $(a, b) = 1$, then a and b are called coprimes.

Question 1. Why does (a, b) always exist for $a, b \in \mathbb{Z} \setminus \{0\}$?

Theorem 1.2. *If $a, b \in \mathbb{Z} \setminus \{0\}$, there are unique $q, r \in Z$ such that*

$$a = qb + r \quad \textit{and} \quad 0 \leq r < |b|.$$

We call q the quotient and r the remainder.

Proof. □

Theorem 1.3 (Euclidean Algortihm).

Exercise 1. Compute $(1716, 1657)$ and write this integer as a linear combination of 1716 and 1657.

Definition 1.2. An integer p is prime iff

(i) $p > 1$, and

(ii) the only positive divisors of p are p and 1.

An integer is *composite* iff it not prime.

Remark 3. If p is a prime and $b \in \mathbb{Z} \setminus \{0\}$ then

$$(p, b) = \begin{cases} p & \text{if } p|b \\ s & \text{othemerre} \end{cases}$$

Prove this claim.

Exercise 2. Let $I \subseteq \mathbb{Z}$ be such that

(i) $0 \in I$,

(ii) if $a, b \in I$, then $a - b \in I$,

(iii) if $a \in I$ and $q \in I$, then $aq \subseteq I$.

Then, there is some nonnegative integer $d \in I$ such that

$$I = \{dk : k \in \mathbb{Z}\}.$$

Remark 4. If $A \subseteq \mathbb{Z}$ and $n \in \mathbb{Z}$, we denote $nA = \{na : a \in A\}$. If $A = \mathbb{Z}$, then $(n) = n\mathbb{Z}$. Thus, this result states that $I = (d)$ for some $d \in I$.

***Solution* 1.**

Theorem 1.4 (Euclid's lemma)**.** *Let $a, b \in \mathbb{Z}$. If p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof. □

Exercise 3. Let $a_1 a_2 \cdots a_n \in \mathbb{Z}$. Prove, by induction, that if p is prime and $p \mid a_1 a_2 \cdots a_n$, then there is $i \in \{1, \ldots, n\}$ such that $p \mid a_i$, i.e., p must divide at least one integer in the product.

The converse of Euclid's lemma is also true.

Proposition 1.1. *Let $p > 1$. If*

$$\forall a, b \in \mathbb{Z} : p \mid ab \implies p \mid a \text{ or } p \mid b,$$

then p is prime.

Proof. By contradiction. □

Proposition 1.2. *Let $a, b, c \in Z$. If*

(i) $(a, c) = 1$, *and*

(ii) $c \mid ab$

then $c \mid b$.

Proof. □

Definition 1.3. Let $a, b \in \mathbb{Z}$ with $b \neq 0$. We say $\frac{a}{b}$ is in lowest terms if $(a, b) = 1$.

Lemma 1.1. *Every nonzero rational number equals a fraction in lowest terms.*

Proof. □

Proposition 1.3. $\sqrt{2}$ *is irrational.*

Proof. □

Theorem 1.5 (Fundamental Theorem of Arithmetic)**.**

The following function computes the amount of smaller integers that are coprime to a given integer.

Definition 1.4 (Euler's totient function φ)**.** Define $\varphi\colon \mathbb{Z}^+ \to \mathbb{Z}$ by

$$\varphi(n) = |\{a \leq n : (a, n) = 1\}|.$$

Properties.