Prof. Pablo Rosero.
Abstract Algebra: Lesson 1

1 Basic properties of the integers

1

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 $a \neq 0$. We say a is a divisor of b if there is an integer c such that $a \cdot c = b$. In this case, we write $a \mid b$.

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 the particular case when $(a, b) = 1$, we say a and b are coprimes.

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

Theorem 1.2 (Division algorithm). *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. $\square$

Euclidean Algortihm. This is an efficient method to compute the gcd of any two integers. It is based on the division algorithm. (Keep in mind that, despite the name, the *division algorithm* is a theorem whereas the *euclidean algorithm* is a procedure.)

If a and b are nonzero integers, then by the division algorithm we get $q, r \in \mathbb{Z}$ such that $a = qb + r$. Let $q_0 = q$ and $r_0 = r$. By applying the division algorithm again with q_0 and r_0 we obtain a new quotient q_1 and a new remainder r_1. The idea of this procedure is to continue applying the division algorithm until we reach a zero remainder. From one step to the next, the divisor becomes the dividend and the remainder the divisor, as follows:

$$\begin{aligned}
a &= q_0 b + r_0 \\
b &= q_1 r_0 + r_1 \\
r_0 &= q_2 r_1 + r_2 \\
r_1 &= q_3 r_2 + r_3 \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n \\
r_{n-1} &= q_{n+1} r_n
\end{aligned}$$

Remark 3. Keep in mind the condition $0 \leq r < |b|$ in the division algorithm. This means the remainder always gets smaller.

Question 2. Why the Euclidean algorithm always terminates? In other words, why we always get a zero remainder at the end of the Euclidean algorithm?

Exercise 1. Compute $(1761, 1567)$ and write this integer as a linear combination of 1761 and 1567.

***Solution* 1.** By the Euclidean algorithm,

$$\begin{aligned}
1761 &= 1 \cdot 1567 + 194 \\
1567 &= 8 \cdot 194 + 15 \\
194 &= 12 \cdot 15 + 14 \\
15 &= 1 \cdot 14 + 1 \\
14 &= 14 \cdot 1 + 0.
\end{aligned}$$

From the next to laxt line we get $(1761, 1567) = 1$.

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

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

Prove this claim.

Proposition 1.1. *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 5. 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 $d \in I$.

Proof. If $I = \{0\}$, take $d = 0$. Suppose $I \neq \{0\}$ and $a \in I$. By (ii), if $a \in I$, then $-a \in I$, so I contains both positive and negative integers. Since $I \cap \mathbb{Z}^+ \neq \varnothing$, the Well Ordering Principle (W.O.P.) implies there is a smallest positive integer in I. Take d as this integer. By (iii), we have $(d) \subseteq I$. Let's see the other inclusion. If $a \in I$, then by the division algorithm, $a = qd + r$ for some $q, r \in Z$ with $0 \leq r < d$. By (ii), $r = a - qd \in I$. However, d is the smallest positive integer contained in I. Since $0 \leq r < d$, the only possibility for this inequality to be true is when $r = 0$. Therefore $a = qd$. It follows $I = (d)$, and the proof is complete. $\square$

Theorem 1.3 (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. $\square$

Exercise 2. 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 $i \in \{1, \dots, n\}$ 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 1.2. *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. $\square$

Proposition 1.3. *Let $a, b, c \in Z$. If*

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

(ii) $c \mid ab$

then $c \mid b$.

Proof. $\square$

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. $\square$

Proposition 1.4. $\sqrt{2}$ *is irrational.*

Proof. $\square$

Theorem 1.4 (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.