1. Basic properties of the integers

In this lesson and onwards, $\mathbb{Z}$ denotes the set of integers and $\mathbb{Z}^+$ the set of positive integers.

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

Note the statement $a \mid b$ is equivalent to *b is a multiple of a*.

Definition 1.2. Let $a, b \in \mathbb{Z} \setminus \{0\}$. The **greatest common divisor of a and b**, denoted (a, b), is the largest positive integer d such that

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

If $(a, b) = 1$, we say a and b are **coprime** or **relatively prime**.

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

Exercise 1. (i) Prove the greatest common divisor of two integers is indeed unique.

(ii) Define least common multiple.

Theorem 1.3 (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. □

Euclidean Algorithm. This is an efficient method to compute the gcd of any two integers. It is based on the division algorithm.[1]

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

[1] Keep in mind that, despite the name, the *division algorithm* is a theorem whereas the *euclidean algorithm* is a procedure.

divisor becomes the dividend and the remainder the divisor, as follows:

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

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? Keep in mind the condition $0 \leq r < |b|$ in the division algorithm.

As a consequence of the Euclidean algorithm, the greatest common divisor of two integers can be written as a linear combination of those integers. This can be done by backward substitution in (1).

Theorem 1.4 (Bézout's identity)**.** *Let a and b be integers with $d = (a, b)$. Then there exist integers x and y such that $ax + by = d$.*

Exercise 2. Compute $(1761, 1567)$ and write this integer as a linear combination of 1761 and 1567.

Solution. 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 last line we get $(1761, 1567) = 1$. $\square$

Definition 1.5. An integer p is **prime** iff

(i) $p > 1$, and

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

A **composite** integer is an integer greater than 1 that is not prime.

Thus, every positive integer is composite, prime, or the unit 1.

Remark 1.5.1. If p is a prime and $b \in \mathbb{Z} \setminus \{0\}$ then

$$(p, b) = \begin{cases} p & \text{if } p \mid b, \\ 1 & \text{else.} \end{cases}$$

Prove this claim.

Proposition 1.6. *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 1.6.1. 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. Condition (i) states $I \neq \varnothing$. 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 $q, r \in \mathbb{Z}$ 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. □

Theorem 1.7 (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. Suppose p is prime and $p \mid ab$. We have to prove that $p \mid a$ or $p \mid b$. However, this is equivalent to

$$p \nmid a \implies p \mid b.$$

Thus, suppose also $p \nmid a$. Then $(p, a) = 1$ by Remark 1.5.1. By the division algorithm, there are $x, y \in \mathbb{Z}$ such that $1 = xp + ya$, so $b = xpb + yab$. Because $p \mid ab$, there is $c \in \mathbb{Z}$ such that $ab = cp$. Thus $b = xpb + ycp = (xb + yc)p$, i.e., b is a multiple of p. In other words $p \mid b$, as desired. The proof is complete. □

Corollary 1.8. *Let $a \in \mathbb{Z}$. If p is prime and $p \mid a^n$ for some $n \in \mathbb{Z}^+$, then $p \mid a$.*

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 1.9. *Let $p > 1$. Suppose*

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

Then p is prime.

Proof. Assume, for the sake of contradiction, that p is not prime. Then p is composite, which means $p = ab$ for some $a, b \in \{2, \ldots, p-1\}$. Since $p \mid ab$, the hypothesis implies $p \mid a$ or $p \mid b$. However, both cases are impossible because p is greater than a and b. This contradiction proves p is prime. □

Proposition 1.10. *Let $a, b, c \in \mathbb{Z}$. Suppose*

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

(ii) $c \mid ab$.

Then $c \mid b$.

Proof. By (ii), $ab = cd$ for some $d \in \mathbb{Z}$. Using (i), write $1 = ax + cy$ for some $x, y \in \mathbb{Z}$. Multiplying by b we get

$$b = abx + cby = cdx + cby = (dx + by)c.$$

Thus $c \mid b$. $\square$

Definition 1.11. Let $a, b \in \mathbb{Z}$ with $b \neq 0$. The rational number $\dfrac{a}{b}$ is in **lowest terms** iff $(a, b) = 1$.

Lemma 1.12. *Every nonzero rational number can be written as the quotient of two integer in lowest terms.*

Proof. $\square$

Proposition 1.13. $\sqrt{2}$ *is irrational.*

Proof. Suppose $\sqrt{2}$ is rational. Then $\sqrt{2} = a/b$ for some $a, b \in \mathbb{Z}$ in lowest terms. Write $\sqrt{2}b = a$ to get $2b^2 = a^2$. Hence $2 \mid a^2$, whence $2 \mid a$ by Euclid's lemma, meaning $a = 2k$ for some $k \in \mathbb{Z}$. By substitution, $2b^2 = 4k^2$, and so $b^2 = 2k^2$. As before, this implies b is even. Therefore, both a and b share 2 as a common factor. However, this contradicts $(a, b) = 1$. This shows our initial assumption was false, meaning $\sqrt{2}$ is irrational. $\square$

Theorem 1.14 (Fundamental Theorem of Arithmetic)**.** *For every integer $n > 1$, there are unique distinct primes $p_1, \ldots, p_k$ and unique positive integers $a_1, \ldots, a_k$ such that*

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}.$$

Moreover, this factorization is unique up to reordering.[2]

Proof. (Existence) By (strong) induction on n. Lets us denote the set of prime numbers by $\mathbb{P}$ Define

$$A = \{n \in \mathbb{Z}^+ \mid \exists p_1, \ldots, p_k \in \mathbb{P}, \exists a_1, \ldots, a_k \in \mathbb{Z}^+ : n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}\}.$$

For $n = 2$, it is clear that $n \in A$ as $n = 2^1$ and 2 is prime. Now, fix $m \in \mathbb{Z}^+$ and assume that $2, \ldots, m \in A$. Lets see that $m + 1 \in A$. There are two cases. Either $m + 1$ is prime or it is not. If $m + 1$ is prime, there is nothing to show. If $m + 1$ is not prime, then it is composite. Thus, there are $m_1, m_2 \in \mathbb{Z}^+$ such that $m + 1 = m_1 m_2$. But, given that $m_1, m_2 \in \{2, \ldots, m\}$, it follows that $m_1, m_2 \in A$,

[2] This means that the product can be rearranged in any different order, but these primes and their powers are always the same.

by the (inductive) hypothesis. Hence $m+1$ can be expressed as the product of prime numbers, i.e., $m+1 \in A$.

By the principle of mathematical induction, $n \in A$ for every $n \geq 2$.

(Uniqueness) Suppose an integer $n \geq 2$ has two prime decompositions, e.g.,

$$p_1^{a_1} \cdots p_k^{a_k} = n = q_1^{b_1} \cdots q_l^{b_l}. \tag{2}$$

where $p_i, q_j \in \mathbb{P}$ and $a_i, b_j \in \mathbb{Z}^+$ for $i \in [k]$ and $j \in [l]$. We prove first that the prime numbers on the left are the same as those on the right. Let $i_0 \in [k]$. Since p_{i_0} appears at least once in $p_1^{a_1} \cdots p_k^{a_k}$, we have $p_{i_0} \mid p_1^{b_1} \cdots p_k^{b_k}$. Thus, $p_{i_0} \mid q_1^{b_1} \cdots q_1^{b_1}$. By Euclid's lemma, there is some $j_0 \in [l]$ such that $p_{i_0} \mid q_{j_0}^{b_{j_0}}$., whence $p_{i_0} \mid q_{j_0}$. But q_{j0} is prime, so it can only be divided by 1 or by itself. Since $p_{i_0} \neq 1, p_{i_0} = q_{i_0}$. Since $i_0 \in [k]$ was arbitrary, we deduce that

$$\forall i \in [k], \exists j \in J : p_i = q_j.$$

This shows that to every prime on the left of (2) there corresponds a prime on the right. In an entirely anlogous manner, it follows that to every prime on the right of (2) there corresponds a prime on the left. Therefore, $k = l$. Now we can write

$$p_1^{a_1} \cdots p_k^{a_k} = p_1^{b_1} \cdots p_k^{b_k}.$$

The proof that the exponents are equal is left as an *easy* exercise to the reader.

The proof is complete. □

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

Definition 1.15. Euler's totient function is the map $\varphi\colon \mathbb{Z}^+ \to \mathbb{Z}$ defined by

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

Properties.

(i) $\varphi(p) = p - 1$ if p is prime

(ii) $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$ for any prime p and any $k \in \mathbb{Z}^+$

(iii) $\varphi(ab) = \varphi(a)\varphi(b) =$ if $(a,b) = 1$

(iv) $\varphi(n) = \varphi(p_1^{a_1}) \cdots \varphi(p_k^{a_k})$ if $n > 1$ has the prime factorization $p_1^{a_1} \cdots p_k^{a_k}$

Note that

$$\varphi(n) = \big|\{a \leq n \mid (a,n) = 1\}\big|$$

Example 1. $\varphi(12) = 4$

Exercise 4. Compute $\varphi(30)$.