

Discrete Mathematics

Daniel Gonzalez Cedre

University of Notre Dame
Spring of 2023

Chapter 7

Number Theory

7.1 Ancient Greece

Definition 7.1 (*Divisibility*).

Given two integers $a, b \in \mathbb{Z}$, we say $a \mid b \Leftrightarrow (\exists k \in \mathbb{Z})(ak = b)$. We read $a \mid b$ as a divides b , meaning $b/a \in \mathbb{Z}$. ┘

Lemma 7.1 (*Initial object*).

If $x \in \mathbb{Z}$, then $1 \mid x$. ┘

Proof. Let $x \in \mathbb{Z}$ and observe that $1 \cdot x = x$. Therefore, $1 \mid x$ by definition. Q.E.D.

Lemma 7.2 (*Terminal object*).

If $x \in \mathbb{Z}$, then $x \mid 0$. ┘

Proof. Let $x \in \mathbb{Z}$ and observe that $0 \cdot x = 0$. Therefore, $x \mid 0$ by definition. Q.E.D.

Lemma 7.3 (*Divisibility is a Partial Order*).

The following statements hold for all $a, b, c \in \mathbb{Z}$:

I. $a \mid a$

Proof. Let $a \in \mathbb{Z}$ and observe that $1 \cdot a = a$. Therefore, $a \mid a$ by definition. Q.E.D.

II. $\left((a \mid b) \wedge (b \mid a) \right) \Rightarrow |a| = |b|$

Proof. Let $a, b \in \mathbb{Z}$ and suppose $a \mid b$ and $b \mid a$. Then, there exist $k_1, k_2 \in \mathbb{Z}$ such that $ak_1 = b$ and $bk_2 = a$ by definition. But then $bk_2 = (ak_1)k_2 = a$, so $ak_1k_2 = a$, yielding $k_1k_2 = 1$. Since the only integers with multiplicative inverses are 1 and -1 , we have $\{k_1, k_2\} \subseteq \{1, -1\}$, so $a = b$ or $a = -b$. Thus, $|a| = |b|$. Q.E.D.

III. $\left((a \mid b) \wedge (b \mid c) \right) \Rightarrow a \mid c$

Proof. Let $a, b, c \in \mathbb{Z}$ and suppose $a \mid b$ and $b \mid c$. Then, there exist $k_1, k_2 \in \mathbb{Z}$ such that $ak_1 = b$ and $bk_2 = c$. This yields $ak_1k_2 = c$. Since $k_1, k_2 \in \mathbb{Z}$, we observe $k_1k_2 \in \mathbb{Z}$ and conclude $a \mid c$ by definition. Q.E.D.

Lemma 7.4 (*Useful facts*).

The following statements hold for all $a, b, c \in \mathbb{Z}$:

I. $\left((a \mid b) \wedge (a \mid c) \right) \Rightarrow a \mid b + c$

II. $a \mid b \Rightarrow (\forall \ell \in \mathbb{Z})(a \mid b\ell)$

III. $a \mid b \Rightarrow |a| \leq |b|$

The proofs of the above lemmata are left as exercises to the reader. ┘

Corollary 7.1.

Given $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $a \mid c$, then $(\forall \ell_1, \ell_2 \in \mathbb{Z})(a \mid \ell_1 b + \ell_2 c)$. ┘

Definition 7.2 (Primality).

We say that a natural number $p \in \mathbb{N}$ is *prime* $:\Leftrightarrow (p > 1)$ and $(\forall n \in \mathbb{N})(n \mid p \Rightarrow n \in \{1, p\})$.

We say $n \in \mathbb{N}$ is *composite* $:\Leftrightarrow n$ is not prime. ┘

Lemma 7.5 (Fundamental Lemma of Arithmetic).

If $n \in \mathbb{N}$ and $n > 1$, then $(\exists p \in \mathbb{N})(p \text{ is prime} \wedge p \mid n)$. ┘

Proof. TODO Q.E.D.

Theorem 7.1 (Fundamental Theorem of Arithmetic).

Every natural number greater than 1 has a *unique* prime factorization. Formally, for every natural number $n \in \mathbb{N}_{\geq 2}$ greater than 1, there exist *unique, distinct* primes $p_1, \dots, p_\ell \in \mathbb{N}_+$ with *unique* exponents $k_1, \dots, k_\ell \in \mathbb{N}_+$ such that

- I. $(\forall i, j \in \{1, \dots, \ell\})(i \neq j \Rightarrow p_i \neq p_j)$
 - II. $(\forall i \in \{1, \dots, \ell\})(p_i \text{ is prime})$
 - III. $n = p_1^{k_1} p_2^{k_2} \dots p_\ell^{k_\ell}$.
- ┘

Theorem 7.2 (Euclid's Theorem).

There are infinitely-many prime numbers. ┘

Proof. TODO Q.E.D.

Definition 7.3 (Greatest Common Divisor).

Given two integers $a, b \in \mathbb{Z}$, we say that $g \in \mathbb{Z}$ is the *greatest common divisor* (a.k.a. *greatest common factor*) of a and b $:\Leftrightarrow$

$$(g \mid a) \wedge (g \mid b) \wedge (\forall h \in \mathbb{Z}) \left((h \mid a) \wedge (h \mid b) \Rightarrow h \mid g \right).$$

Notice that, since $(\forall x)(1 \mid x)$, every pair of integers shares a common factor. Since common factors of a and b are bounded above by $\min\{a, b\}$, that means the set of all common factors of a and b is nonempty and bounded above, so it has a maximal element. Therefore, the greatest common divisor of any two integers always exists. ┘

Definition 7.4 (Co-Primality).

We say that two integers $a, b \in \mathbb{Z}$ are *co-prime* $:\Leftrightarrow$ their greatest common divisor is 1. ┘

Theorem 7.3 (Euclid's Division Theorem).

If $a, b \in \mathbb{Z}$, then there exist two *unique* integers $q, r \in \mathbb{Z}$ such that

$$a = bq + r \text{ and } 0 \leq r < b.$$

Here, q is called the *quotient* when a is divided by b , and r is the *remainder*, as illustrated by $a/b = q + r/b$. ┘