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. $\Big(\big(a \mid b\big) \wedge \big(b \mid a\big)\Big) \;\Rightarrow\; |a| = |b|$

Proof. Let $a, b \in Z$ 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. $\Big(\big(a \mid b\big) \wedge \big(b \mid c\big)\Big) \;\Rightarrow\; a \mid c$

Proof. Let $a, b, c \in Z$ 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. $\Big(\big(a \mid b\big) \wedge \big(a \mid c\big)\Big) \;\Rightarrow\; a \mid b + c$

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

III. $a \mid b \;\Rightarrow\; |a| \leqslant |b|$

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 $(\forall \ell_1, \ell_2 \in \mathbb{Z})\big(a \mid \ell_1 b + \ell_2 c\big)$. ⌟

Definition 7.2 ***(Primality).***
We say that a natural number $p \in \mathbb{N}$ is *prime* $:\Leftrightarrow$ $(p > 1)$ and $(\forall n \in \mathbb{N})\big(n \mid p \;\Rightarrow\; n \in \{1, p\}\big)$.
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 $(\exists p \in \mathbb{N})\big(p \text{ is prime} \wedge p \mid n\big)$. ⌟

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 $n \in \mathbb{N}_{\geqslant 2}$ greater than 1, there exist *unique, distinct* primes $p_1, \ldots p_\ell \in \mathbb{N}_+$ with *unique* exponents $k_1, \ldots k_\ell \in \mathbb{N}_+$ such that

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

⌟

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 $:\Leftrightarrow$

$$\big(g \mid a\big) \wedge \big(g \mid b\big) \wedge (\forall h \in \mathbb{Z})\Bigg(\Big(\big(h \mid a\big) \wedge \big(h \mid b\big)\Big) \;\Rightarrow\; h \mid g\Bigg).$$

Notice that, since $(\forall x)\big(1 \mid x\big)$, 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

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

Here, q is called the *quotient* when a is divided by b, and r is the *remainder*, as illustrated by ${}^a/_b = q + {}^r/_b$. ⌟

Algorithm 7.1 ***(Euclid's Division Algorithm).***
We can find the greatest common divisor of two integers by recursively computing

$$\begin{aligned} \gcd(a, 0) &\coloneqq a \\ \gcd(a, b) &\coloneqq \gcd(b, r) \text{ where } a = bq + r \\ &\qquad\qquad\qquad\; \text{and } 0 \leqslant r < b \\ &\qquad\qquad\qquad\; \text{and } q, r \in \mathbb{Z}. \end{aligned}$$

This algorithm correctly computes the greatest common divisor of two arbitrary integers. ⌟

7.2 Modular Arithmetic

Definition 7.5 ***(Modular Congruence).***
Let $m \in \mathbb{N}_+$ and let $x, y \in \mathbb{Z}$. We say that $x \equiv y \pmod{m} \;:\Leftrightarrow\; m \mid x - y$. We read the sentence $x \equiv y \pmod{m}$ in English as "x is congruent to y modulo m." This expresses the idea that x and y have the *same remainder* after division by m, as we can see below.

$$\left.\begin{aligned} x &= q_x m + r \\ y &= q_y m + r \end{aligned}\right\} \;\Leftrightarrow\; x - y = (q_x m + r) - \big(q_y m + r\big)$$
$$\Leftrightarrow\; x - y = \big(q_x - q_y\big)m + (r - r)$$
$$\Leftrightarrow\; x - y = \big(q_x - q_y\big)m$$
$$\Leftrightarrow\; m \mid x - y$$

┘

Exercise 7.1.
Let $m \in \mathbb{N}_+$ and $w, x, y, z \in \mathbb{Z}$. The following are some useful facts about modular congruence.

I. $x \equiv y \pmod{m} \;\Rightarrow\; x + z \equiv y + z \pmod{m}$.

II. $\Big(\big(w \equiv z \pmod{m}\big) \wedge \big(x \equiv y \pmod{m}\big)\Big) \;\Rightarrow\; wx \equiv yz \pmod{m}$.

┘

Theorem 7.4 ***(Modular Congruence is an Equivalence Relation).***
Let $m \in \mathbb{N}_+$ and $x, y, z \in \mathbb{Z}$. The following are true.

I. $x \equiv x \pmod{m}$

II. $x \equiv y \pmod{m} \;\Rightarrow\; y \equiv x \pmod{m}$

III. $\Big(\big(x \equiv y \pmod{m}\big) \wedge \big(y \equiv z \pmod{m}\big)\Big) \;\Rightarrow\; x \equiv z \pmod{m}$

┘

Definition 7.6 ***(Modular Residue Classes).***
Let $m \in \mathbb{N}_+$ and let $a \in \mathbb{Z}$. The set of solutions to the *linear congruence* $x \equiv a \pmod{m}$ is denoted by

$$[a]_m \coloneqq \big\{x \in \mathbb{Z} \;\big|\; x \equiv a \pmod{m}\big\}.$$

Each of these is known as an *equivalence class* of *residues* modulo m, indicating that all the integers in that class have remainder congruent to a after division by m. ┘

Definition 7.7 ***(Cyclic Groups).***
Let $m \in \mathbb{N}_+$. We define the *modular group* (*a.k.a.* the *cyclic group*) of size m by

$$\mathbb{Z}/m\mathbb{Z} \coloneqq \big\{[x]_m \;\big|\; x \in \mathbb{Z}\big\},$$

and we define *addition* and *multiplication* on it by

$$[x]_m + [y]_m \coloneqq [x + y]_m$$
$$[x]_m \cdot [y]_m \coloneqq [xy]_m.$$

┘