

# 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.  $\left( (a \mid b) \wedge (b \neq 0) \right) \Rightarrow |a| \leq |b|$

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  $a/b = q + r/b$ . ┘

**Algorithm 7.1 (Euclid's Division Algorithm).**

We can find the greatest common divisor of two integers by recursively computing

$$\gcd(a, b) := \begin{cases} a & \text{if } b = 0 \\ \gcd(b, r) & \text{where } \begin{cases} a = bq + r \\ 0 \leq r < b \\ q, r \in \mathbb{Z}. \end{cases} \text{ if } b \neq 0 \end{cases}$$

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.

$$\left. \begin{array}{l} x = q_x m + r \\ y = q_y m + r \end{array} \right\} \Leftrightarrow x - y = (q_x m + r) - (q_y m + r)$$

$$\Leftrightarrow x - y = (q_x - q_y)m + (r - r)$$

$$\Leftrightarrow x - y = (q_x - q_y)m$$

$$\Leftrightarrow m \mid x - y$$

### 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.  $\left( (w \equiv z \pmod{m}) \wedge (x \equiv y \pmod{m}) \right) \Rightarrow wx \equiv yz \pmod{m}$ .

### 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.  $\left( (x \equiv y \pmod{m}) \wedge (y \equiv z \pmod{m}) \right) \Rightarrow x \equiv z \pmod{m}$

### 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

$$[a]_m := \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}.$$

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 (Modular Rings).

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

$$\mathbb{Z}/m\mathbb{Z} := \{[x]_m \mid x \in \mathbb{Z}\}$$

and we define *modular addition* and *modular multiplication* on its elements by

$$[x]_m + [y]_m := [x + y]_m$$

$$[x]_m \cdot [y]_m := [xy]_m.$$

### Theorem 7.5 (Bézout's Identity).

Given  $x, y \in \mathbb{Z}$ , there exist  $k_1, k_2 \in \mathbb{Z}$  such that

$$xk_1 + yk_2 = \gcd(x, y).$$

**Algorithm 7.2 (Extended Euclidean Division Algorithm).**

We can find the greatest common divisor *and* the Bézout coefficients of two integers by recursively computing

$$\gcd(a, b) := \begin{cases} (a, 1, 0) & \text{if } b = 0 \\ (d, t, s - qt) & \begin{cases} \text{where } (d, s, t) = \text{egcd}(b, r) \\ \text{and } a = bq + r \\ \text{and } 0 \leq r < b \\ \text{and } q, r \in \mathbb{Z}. \end{cases} & \text{if } b \neq 0 \end{cases}$$

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

**Definition 7.8 (Euler's Totient Function).**

We define *Euler's totient function*  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  by the number of integers  $1 \leq z < n$  relatively prime with  $n \in \mathbb{N}$

$$\varphi(n) := \left| \left\{ z \in \mathbb{Z} \mid (1 \leq z < n) \wedge (\gcd(z, n) = 1) \right\} \right|$$
┘

**Lemma 7.6.**

If  $p \in \mathbb{N}_+$  is prime, then  $\varphi(p) = p - 1$ . ┘

**Theorem 7.6.**

Let  $x, y \in \mathbb{Z}$ . If  $\gcd(x, y) = 1$ , then  $\varphi(xy) = \varphi(x)\varphi(y)$ . ┘

**Theorem 7.7 (Férmát's Little Theorem).**

Let  $p \in \mathbb{N}_+$  be prime and  $a \in \mathbb{Z}$ . Then,  $a^p \equiv a \pmod{p}$ . Further, if  $\gcd(a, p) = 1$ , then  $a^{p-1} \equiv 1 \pmod{p}$ . ┘

**Theorem 7.8 (Euler's Theorem).**

Let  $n \in \mathbb{N}_+$  and  $a \in \mathbb{Z}$ . If  $\gcd(a, n) = 1$ , then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$
┘

**Algorithm 7.3 (RSA Encryption).**

The RSA\* cryptosystem is an algorithm for performing *asymmetric* (a.k.a. *public key*) encryption. Its security is reliant on two key observations:

- I. It takes roughly  $e^{\left(\sqrt[3]{64/9}\right)(\ln n)^{1/3}(\ln \ln n)^{2/3}}$  time to factor  $n \in \mathbb{N}$  into a product of primes.
- II. There is no known way of finding the  $k^{\text{th}}$  root of  $x$  in  $\mathbb{Z}/n\mathbb{Z}$  faster than by factoring  $n$ .

The algorithm has two stages, with **private** information that must be kept **secret** or **destroyed**, and **public** information that is shared through **insecure channels**.

**Key Generation**

1. Pick two (large) prime numbers **p** and **q**. Compute **n** :=  $pq$ .
2. Compute  **$\varphi(n)$**  =  $\varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$  using **Theorem 7.6**.
3. Pick a random number **e** in the range  $1 < e < \varphi(n)$  relatively prime with  $\varphi(n)$ .
4. When checking that  $\gcd(e, \varphi(n)) = 1$  in the previous step, use the *Extended Euclidean Algorithm* from **Algorithm 7.2** to simultaneously obtain **d** satisfying  $ed \equiv 1 \pmod{\varphi(n)}$ .
5. Publish  $(e, n)$  publicly while keeping  $(d, n)$  secret.

The **public encryption key** is the pair  $(e, n)$ , and the **private decryption key** is the pair  $(d, n)$ . All other **private** information should be immediately *destroyed* for security.

---

\*Named after Rivest, Shamir, and Adleman, the three coauthors of the original 1977 paper.

**Message Passing: Encryption**

1. Your friend takes a message  $m$ , which is a (binary) number, and—treating it like a string—chops it up into substrings  $m = m_0 m_1 \dots m_k$  so that each is in the range  $0 < m_i < n$  and  $\gcd(m_i, n) = 1$ .
2. For each sub-message  $m_i$ , your friend computes the encrypted sub-message  $c_i$  by  $c_i \equiv m_i^e \pmod{n}$ , where  $0 < c_i < n$ .
3. He then sends  $c_i$  over an insecure channel to you.

**Message Passing: Decryption**

1. Receive  $c_i$ , which has possibly been intercepted by other parties.
2. Decrypt the encrypted message with your private key by computing  $m_i \equiv c_i^d \pmod{n}$  such that  $0 < m_i < n$ .

┘

# Appendix A

## The Algebra of Modular Arithmetic

### Definition A.1 (*Some Basic Algebra*).

Suppose we have a set  $G$  with a binary operation on  $\mathbf{+} : G \times G \rightarrow G$  defined on it. We say this is a *monoid* if there exists an *identity element*  $e_0$  such that

- I.  $(\forall g \in G)(e_0 \mathbf{+} g = g \mathbf{+} e_0 = g)$
- II.  $(\forall g, h, k \in G)(g \mathbf{+} (h \mathbf{+} k) = (g \mathbf{+} h) \mathbf{+} k)$

We call  $G$  under  $\mathbf{+}$  a *group* if we also have

- III.  $(\forall g \in G)(\exists h \in G)(g \mathbf{+} h = e_0)$

We call  $G$  a *commutative group*<sup>\*</sup> if we additionally have

- IV.  $(\forall g, h \in G)(g \mathbf{+} h = h \mathbf{+} g)$

If we then define another binary operation  $\bullet : G \times G \rightarrow G$ , then we call  $G$  with these two operations a *ring* if we can find another identity element  $e_1 \in G$  such that

- V.  $G$  is a monoid under  $\bullet$  with identity  $e_1$
- VI.  $(\forall g, h, k \in G)(g \bullet (h \mathbf{+} k) = (g \bullet h) \mathbf{+} (g \bullet k))$
- VII.  $(\forall g, h, k \in G)((g \mathbf{+} h) \bullet k = (g \bullet k) \mathbf{+} (h \bullet k))$

Finally, we say that  $G$  is a *field* if we also have

- VIII.  $(\forall g \in G)(g \neq e_0 \Rightarrow (\exists h \in G)(g \bullet h = e_1))$

### Lemma A.1.

$G$  with  $\mathbf{+}$  and  $\bullet$  is a field *iff*  $G$  with  $\mathbf{+}$  is a group and  $G \setminus \{e_0\}$  with  $\bullet$  is a group.

### Theorem A.1.

If  $n \in \mathbb{N}_+$ , then  $\mathbb{Z}/n\mathbb{Z}$  forms a ring under modular arithmetic.

If  $n \in \mathbb{N}_+$ , then  $\mathbb{Z}/n\mathbb{Z}$  forms a field under modular arithmetic *iff*  $n$  is prime.

### Definition A.2 (*Order*).

The *order*  $|G|$  of a group  $G$  is its cardinality. The *order*  $|g|$  of  $g \in G$  is the smallest  $n \in \mathbb{N}$  such that  $g^{n+1} = e$ .

### Theorem A.2.

For any group  $G$  and any  $g \in G$ , we have that  $|g|$  divides  $|G|$ .

---

<sup>\*</sup>Usually referred to as an *Abelian group*, after Niels Henrik Abel.