Introduction to Number Theory and Algorithms

Christian Rudder

August 2024

Contents

This page is left intentionally blank.

Preface

Basic properties of Integers

1.1 Divisibility and primality

"a divides b", i.e., $\left(\frac{b}{a}\right)$, means b is reached by a, when a is multiplied by **some integer**.

Definition 1.1: Division

Let $a, b, x \in \mathbb{Z}$: $\left(\frac{b}{a}\right)$ means "$b = ax$".

Denoted: $a|b$,
read "a divides b," and "a doesn't divide b" is, $a \nmid b$.

Examples:

- $3 \mid 6$ because $6 = 3 \cdot 2$.
- $3 \nmid 5$ because $5 \neq 3 \cdot x$ for any $x \in \mathbb{Z}$.
- $2 \mid 0$ because $0 = 2 \cdot 0$.
- $0 \nmid 2$ because $2 \neq 0 \cdot x$ for any $x \in \mathbb{Z}$.

Note: $a, b, x \in \mathbb{Z}$ for, "$\left(\frac{b}{a}\right)$" or "$b = ax$" are labeled, a: divisor, b: dividend, x: quotient.

Tip: Many problems will involve manipulating this "$b = ax$" equation. Whether it's substituting b for ax or vice-versa, or adding/subtracting/multiplying/dividing "$b = ax$" to itself to reveal some property.

Many definitions and theorems will relate to each other or build off one another. It's crucial to understand what concepts mean rather than memorizing them. This means the ability to derive theorems or definitions from scratch, based on intuitive understanding of the content.

Observe the following:

Theorem 1.1: Properties of Divisibility

Theorem 1.1. For all $a, b, c \in \mathbb{Z}$:

  (i) "$a \mid a$", "$1 \mid a$", and "$a \mid 0$"

 (ii) "$0 \mid a$" $\Longleftrightarrow$ "$a = 0$"

(iii) "$a \mid b$" $\Longleftrightarrow$ "$-a \mid b$" $\Longleftrightarrow$ "$a \mid -b$"

(iv) "$a \mid b$" $\wedge$ "$a \mid c$" $\Longrightarrow$ "$a \mid (b + c)$"

 (v) "$a \mid b$" $\wedge$ "$b \mid c$" $\Longrightarrow$ "$a \mid c$"

Proof 1.1: Theorem 1.1

Proof. For all $a, b, x, y \in \mathbb{Z}$:

  (i)   – "$a \mid a$" means "$a = ax$", choosing $x = 1$ always satisfies.

       – "$1 \mid a$" because $a = 1 \cdot a$

       – "$a \mid 0$" because $0 = a \cdot 0$

 (ii) – If "$0 \mid a$" then "$a = 0 \cdot x$", 0 times any integer is 0, so $a = 0$

       – If "$a = 0$" then "$0 = 0 \cdot x$", x can be any integer.

(iii) Proving $a \mid b \Longleftrightarrow -a \mid b$:

       – If "$a \mid b$" then "$b = ax = (-a)(-x)$", $-x$ is some integer, say x'.
         So "$b = (-a)x'$" then "$-a \mid b$"

       – If "$-a \mid b$" then "$b = (-a)x$", choose x to be some negative integer.

     Proving $-a \mid b \Longleftrightarrow a \mid -b$:

       – If "$-a \mid b$" then "$b = (-a)x$", choose x positive integer.

       – If "$a \mid -b$" then "$-b = ax$", choose x to be some negative integer.

(iv) If "$a \mid b$" and "$a \mid c$" then "$b = ax$" and "$c = ay$" add both equations, "$b + c = ax + ay$" factor, "$b + c = a(x + y)$", $(x + y)$ is some integer, so "$a \mid (b + c)$"

 (v) If "$a \mid b$" and "$b \mid c$" then "$b = ax$" and "$c = by$" substitute b in c, "$c = (ax)y$" shift terms, "$c = a(xy)$", (xy) is some integer, so "$a \mid c$"

                                                               ■

Theorem 1.2: Reflexive Divisibility

For all $a, b \in \mathbb{Z}$: "$a \mid b$" $\wedge$ "$b \mid a$" $\iff$ "$a = \pm b$". Additionally, "$a \mid 1$" $\iff$ "$a = \pm 1$".