Title

Christian Rudder

August 2024

Contents

This page is left intentionally blank.

Preface

This is a Distillation of:
A Computational Introduction to Number Theory and Algebra
(Version 2), by Victor Shoup.

— 1 —

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) $0 \mid a$ if and only if $a = 0$;

(iii) $a \mid b$ if and only if $-a \mid b$ if and only if $a \mid -b$;

(iv) $a \mid b$ and $a \mid c$ implies $a \mid (b + c)$;

(v) $a \mid b$ and $b \mid c$ implies $a \mid c$.

To prove,

Proof 1.1: Theorem 1.1

- hi