Introduction to Number Theory and Algorithms

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.

See https://shoup.net/ntb/ for the original text and practice problems.

— 1 —

Prerequisites

Definition 0.1: Well-Ordering Principle

Every non-empty set of positive integers has a least element.

— 2 —

Basic properties of Integers

2.1 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) "$0 \mid a$" $\iff$ "$a = 0$"

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

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

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

Try to prove these properties before reading the proof below.

Proof 1.1: Properties of Divisibility

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 $a \mid b \iff -a \mid b$:

- 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 $-a \mid b \iff a \mid -b$:

- 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, "$a \mid 1$" $\iff$ "$a = \pm 1$".

Proof 1.2: Reflexive Divisibility

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

Proving "$a \mid b$" $\wedge$ "$b \mid a$" $\implies$ "$a = \pm b$":

$$\begin{array}{rll} a \mid b & a \mid b & \textit{Given} \\ b = ax & a = by & \textit{Definition of Division} \\ ab = (ax)(by) & & \textit{Multiplying both equations} \\ ab = (ab)(xy) & & \textit{Shift terms} \\ 1 = xy & & \textit{Divide both sides by } ab \end{array}$$

x and y are integers, so "$x = y = 1$". Substitute x and y,

$$\begin{array}{rll} b = a(1) & a = b(1) & \textit{Substitute} \\ & a = b & \textit{Simplify} \end{array}$$

x or y could be $\pm$, so "$a = \pm b$". Now "$a = \pm b$" $\implies$ "$a \mid b$" and "$b \mid a$". From Theorem 1.1, we can use (i) to show "$a \mid a$" substitute b in for a, "$a \mid b$" or $b \mid a$.

Proving "$a \mid 1$" $\implies$ "$a = \pm 1$":

$$\begin{array}{rl} a \mid 1 & \textit{Given} \\ 1 = ax & \textit{Definition of Division} \\ 1 = a(1) & \textit{Simplify} \end{array}$$

a must be 1, x could be $\pm$, so "$a = \pm 1$" then "$a \mid \pm 1$" so "$a \mid 1$". ■

Definition 1.2: Cancellation Law

Let $a, b, c \in \mathbb{Z}$: If "$ab = ac$" and "$a \neq 0$" then "$b = c$".

I.e., given "$b = c$" multiplying both sides by a yields "$ab = ac$", and still $b = c$.

Definition 1.3: Prime Numbers

$p \in \mathbb{Z}$ is prime if $p \neq 0$ and p has no divisors other than 1 and p.

We will **only consider positive prime numbers**, in this text. Examples of primes are:

$$2, 3, 5, 7, 11, 13, 17, \ldots$$

Definition 1.4: Composite Numbers

$n, a, b \in \mathbb{Z}$ is composite if $n = ab$ and $1 < a < n$ and $1 < b < n$.

I.e., a composite number is a number can be factor into two integers, other than 1 and itself.
Examples:

- 4 is composite because $4 = 2 \cdot 2$.
- 6 is composite because $6 = 2 \cdot 3$.

Briefly observe the following:

Theorem 1.3: Division Algorithm

For all $a, b \in \mathbb{Z}$, $b \neq 0$, there exists unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < |b|$.

To dissect, for all $a, b, q, r \in \mathbb{Z}$, $b \neq 0$, q and r exist uniquely such that:

$$\text{“}a{=}bq{+}r\text{”}$$

Dividend = **Divisor** · **Quotient** + **Remainder**

b fits into a q times with r left over.

Examples:

- $8 = 4 \cdot 2 + 0$
- $5 = 3 \cdot 1 + 2$

Note: Theorem 1.3 is called the Division Algorithm, despite not being an algorithm.

Proof 1.3: Division Algorithm

Proof. For all $a, b \in \mathbb{Z}$, $b \neq 0$, there exists unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < |b|$.

The definition of division "$b \mid a$" then "$a = bx$", $x \in \mathbb{Z}$. Subtract bx from both sides, "$a - bx = 0$", working out evenly to 0. Freeze a and b, and vary x yields a set of outputs, S:

$$S = \{a - bx : x \in \mathbb{Z}\}$$

What's left of a after taking b, x times. E.g., "$b = 2$, $a = 6$":

x	$a - bx$	
0	0	$= 6 - 2 \cdot 0$
1	4	$= 6 - 2 \cdot 1$
2	2	$= 6 - 2 \cdot 2$
3	0	$= 6 - 2 \cdot 3$
4	-2	$= 6 - 2 \cdot 4$

Let r be outputs of S and "$q := x$" then "$a - bq = r$" add bx to both sides, "$a = bq + r$".

Intuitively: I cut a cake of size a into pieces of b width for q people. Leftovers r can't exceed the size of the original cake: between nothing left or sharing nothing, i.e., "$0 \leq r < b$".

We found our lower bound: $S = \{a - bx : x \in \mathbb{Z}, a - bx \geq 0\}$.

Formally: By the Well-Ordering Principle, there exists a smallest element in S, say r. To show existence in S, choose "$x = 0$" then "$a - b(0) = a$" we are left with "$a \geq 0$".

Without loss of generality, assume "$a < 0$". To satisfy "$a - bx \geq 0$" choose "$x = a$" yielding "$a - ba = a(1 - b)$" we know "$(a < 0)$" and "$(b \geq 1)$" as "$0 \leq r < b$". So "$(1 - b) \leq 0$". Hence "$a(1 - b) \geq 0$" as "$(n < 0 \cdot m \leq 0) = p \geq 0$" for some $n, m, p \in \mathbb{Z}$. So S is not empty.

For "$r < b$" we argue by contradiction "$r \geq b$" then "$r = a - bq \geq b$". Subtract b from both sides, "$(r - b = a - bq - b) \geq (b - b = 0)$" factoring we see "$r - b = a - b(q + 1)$". Since "$q + 1$" is some integer say q', "$r - b = a - bq'$" showing "$(r - b) < r$" contradicting our assumption.

For q, r uniqueness, we argue by contradiction, assume another pair q', r' such that "$a = (bq' + r') = (bq + r)$" and "$0 \leq r' < b$". Without loss of generality, assume "$r' \geq r$". re-arrange both sides, "$r' - r = bq - bq'$" factor "$r' - r = b(q - q')$". Then "$b \mid r' - r$" , but "$0 \leq r' - r < b$" so "$r' - r = 0$" therefore "$r' = r$" showing "r is unique". "$b(q - q') = 0$" therefore "$(q - q') = 0$" hence "$q = q'$" showing "q is unique". ■