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

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 equation like $b = ax$. Whether it's substituting b for ax or vice-versa, or adding/subtracting/multiplying/dividing $b = ax$.

Many definitions and theorems will build off one another. It's crucial to understand what concepts mean rather than memorizing them. This means having the ability to prove theorems and definitions from scratch.

Observe the following:

Theorem 1.1: Properties of Divisibility

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 $a, b \in \mathbb{Z}$: $a \mid b \land b \mid a \iff a = \pm b$. Additionally, $a \mid 1 \iff a = \pm 1$.

Proof 1.2: Reflexive Divisibility

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

Proving $a \mid b \land b \mid a \implies a = \pm b$:

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

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

$$\begin{aligned} b = a(1) \quad a = b(1) & \qquad \textit{Substitute} \\ a = b & \qquad \textit{Simplify} \end{aligned}$$

x or y could be ±, so $\underline{a = \pm b.}$ 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, $\underline{a \mid b \text{ or } b \mid a.}$

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

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

a must be 1, x could be ±, so $a = \pm 1$ then $\underline{a \mid \pm 1 \text{ so } a \mid 1}$. ■

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 $a, b \in \mathbb{Z}$, $b > 0$, 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:

$$a = bq + r$$

$$\textbf{Dividend} = \textbf{Divisor} \cdot \textbf{Quotient} + \textbf{Remainder}$$

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 $a, b \in \mathbb{Z}$, $b > 0$, 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., $a = 6$, $b = 2$:

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, $\underline{a = bq + r}$.

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: it's between nothing left or nothing shared, i.e., $\underline{0 \leq r < b}$.

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

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, also 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 $(n < 0 \cdot m \leq 0) = h \geq 0$ for some $n, m, h \in \mathbb{Z}$. So $\underline{S \text{ is not empty.}}$

For $\underline{r < b}$ say $r \geq b$, $\underline{r \text{ is the smallest element.}}$ 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', $r - b = a - bq'$. There exists some b, $\underline{(r - b) < r \text{ contradicting our assumption.}}$

For q, r uniqueness, say there's 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 $\underline{r \text{ is unique}}$. $b(q - q') = 0$ therefore $(q - q') = 0$ hence $q = q'$ showing $\underline{q \text{ is unique}}$. ■

2.2 Modular Arithmetic & Residues

Remember: For $a \in \mathbb{R}$, $\underline{a \in [0,1) \text{ is a range}}$, i.e., including decimals from 0 to 1 (excluding 1).

Definition 2.1: Floor & Ceiling

For $x \in \mathbb{R}$, $m, n \in \mathbb{Z}$ we map $\mathbb{R} \to \mathbb{Z}$,

Floor x, $\lfloor x \rfloor$, is the largest m such that $m \leq x < m + \varepsilon$, where $\varepsilon \in [0,1)$.

Ceiling x, $\lceil x \rceil$, is the smallest n such that $n - \varepsilon < x \leq n$, where $\varepsilon \in [0,1)$.

Definition 2.2: Mod Operator

Let $a, b \in \mathbb{Z}$, $b\,0$: The remainder of a divided by b. I.e., $a - b\lfloor \frac{a}{b} \rfloor$.

Denoted: "a mod b" or "$a \,\%\, b$".

Examples: 8 mod 3 = 2, and 5 mod 2 = 1

From The Division Algorithm (1.3) we see for all $a, b \in \mathbb{Z}$, $b \neq 0$: $a = bq + r$ then $r = a \bmod b$.

Proof 2.1: Mod Operator

$\underline{\text{The Division Algorithm (1.3) only works for } b > 0.}$ To generalize for $b < 0$,

$$\begin{aligned} a &= bq + r && \textit{Given} \\ a/b &= q + r/b && \textit{Divide both sides by } b \end{aligned}$$

We know $0 \leq r < b$, dividing b yielded $0 \leq \dfrac{r}{b} < 1$, so

$$\frac{r}{b} \in [0,1) \in \mathbb{R}$$

We notice $q = \left\lfloor \dfrac{a}{b} \right\rfloor$, as q is the largest integer that fits into a, b times. ■

Tip: $q = \left\lfloor \dfrac{a}{b} \right\rfloor$ is similar to integer division in programming languages.

Theorem 2.1: Division Algorithm Extended

Let $a, b \in \mathbb{Z}$ with $b > 0$, and let $x \in \mathbb{R}$. Then there exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $r \in [x, x + b)$.

$r \in [x, x + b)$ allows us to work with negative numbers and different intervals. Let's try to build some intuition about division and remainders:

$$a, b, r \in \mathbb{Z} \text{ and } S = \{r = a - bq : q \in \mathbb{Z}\},\ a = 6,\ b = 2:$$

(0)

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	$= 6 - 2 \cdot 4$
5	-4	$= 6 - 2 \cdot 5$
6	-6	$= 6 - 2 \cdot 6$
7	-8	$= 6 - 2 \cdot 7$

Dividing two numbers varying the divisor:

(1)

b	3 mod b
1	0
2	1
3	0
4	3
5	3
6	3
7	3
8	3

b	9 mod b
1	0
2	1
3	0
4	1
5	4
6	3
7	2
8	1
9	0
10	9

b	7 mod b
1	0
2	1
3	1
4	3
5	2
6	1
7	0
8	7

Grouping them by the remainder:

(2)

r	3 mod b
0	1, 3
1	2
3	4, 5, 6, …

r	9 mod b
0	1, 3, 9
1	2, 4, 8
3	5, 6, 7
9	10, 11, 12, …

r	7 mod b
0	1, 7
1	2, 6
2	5
3	4
7	8, 9, 10, …

Let's try the other way around.

(3)

a	a mod 3
0	0
1	1
2	2
3	0
4	1
5	2
6	0
7	1
8	2
9	0

a	a mod 9
0	0
1	1
2	2
3	3
…	…
9	0
10	1
11	2
…	…
18	0
19	1

a	a mod 7
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	0
8	1
9	2

Grouping them by the remainder:

(4)

r	a mod 3
0	0, 3, 6, 9
1	1, 4, 7
2	2, 5, 8

r	a mod 9
0	0, 9, 18
1	1, 10, 19
2	2, 11
3	3, 12
4	4, 13
5	5, 14
6	6, 15
7	7, 16
8	8, 17

r	a mod 7
0	0, 7
1	1, 8
2	2, 9
3	3
4	4
5	5
6	6

(5) **Table with increments of 3**

a	$a+1$	$a+2$
0	1	2
3	4	5
6	7	8
9	10	11
12	13	14
15	16	17
...	...	...

What is multiplication but repeated addition? What is division but repeated subtraction?

Column a in (5)-(7) shows multiples of b, and is example (4) transposed (highlighted). We can think of the width of a table as a's period.

Add 10 to 8, yields numbers always ending in 8. Add add 5 to 8, yields numbers ending in 3 or 8. These periods are more predictable than the other examples.

(6) **Table with increments of 7**

a	$a+1$	$a+2$	$a+3$	$a+4$	$a+5$	$a+6$
0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	32	33	34
35	36	37	38	39	40	41
...	...	...	...	...	...	...

(7) **Table with increments of 9**

a	$a+1$	$a+2$	$a+3$	$a+4$	$a+5$	$a+6$	$a+7$	$a+8$
0	1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16	17
18	19	20	21	22	23	24	25	26
27	28	29	30	31	32	33	34	35
36	37	38	39	40	41	42	43	44
45	46	47	48	49	50	51	52	53
...	...	...	...	...	...	...	...	...

This is $[x, x+b)$: Expanding the definition beyond 0, allows us to represent rows 3 or 5 in (5)-(7). Whether we shift the table, starting at columns 1 or 2, the period/interval remains the same.

We formally group (5)-(7)'s column headers into classes, which we call ***residues.***

Definition 2.3: Residue

Let $a, n \in \mathbb{Z}$, $n > 0$.

Set $R = \{a \bmod n : n \in \mathbb{Z}, n \neq 0\}$ produces remainders $r \in [0, n-1]$.
Each remainder r is a **residue** of a modulo n.

Definition 2.4: Residue Class

The set of numbers produced by a residue.

Denoted: $[a]_n$ or $a(\bmod n)$, a the residue under modulo n.

Definition 2.5: Representative

The smallest non-negative integer in a residue class, i.e., the residue itself.

Residue and **Representative** are used interchangeably.

Example:

mod 3:

- $[0]_3 = \{0, 3, 6, 9, \dots\}$
- $[1]_3 = \{1, 4, 7, 10, \dots\}$
- $[2]_3 = \{2, 5, 8, 11, \dots\}$

The representative of $[1]_3$ is 1.

Definition 2.6: Congruence

Let $a, b, n \in \mathbb{Z}$, $n > 0$.

a is **congruent** to b modulo n, if a and b produce the same remainder modulo n.

Denoted: $a \equiv b \pmod{n}$.

Example: $8 \equiv 22 \pmod{7}$, as $8 \bmod 7 = 1$ and $22 \bmod 7 = 1$.