

Introduction to Number Theory and Algorithms

Christian Rudder

August 2024

Contents

Contents	1
1 Prerequisites	4
2 Basic properties of Integers	5
2.1 Divisibility	5
2.2 Modular Arithmetic & Residues	10
2.3 Ring Theory	14
2.4 The Integer Ideal & Primality	17

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.

Definition 0.1: Well-Ordering Principle

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

Definition 0.2: “Without Loss of Generality”

A phrase that indicates that the proceeding logic also applies to the other cases. i.e., For a proposition not to lose the assumption that it works other ways as well.

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.

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

Proof 1.2: Reflexive Divisibility

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

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

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

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

$$\begin{array}{ll}
 b = a(1) & a = b(1) \quad \text{Substitute} \\
 a = b & \text{Simplify}
 \end{array}$$

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

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

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:

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

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 that 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 $a, b, q, r \in \mathbb{Z}$, $b > 0$, q and r exist uniquely such that:

$$a = bq + r$$

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

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, $a = bq + r$.

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., $0 \leq r < b$.

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

Formally: By the Well-Ordering Principle (0.1), 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 S is not empty.

For $r < b$ say $r \geq b$, r 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 , $(r - b) < r$ 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 r is unique. $b(q - q') = 0$ therefore $(q - q') = 0$ hence $q = q'$ showing q is unique. ■

2.2 Modular Arithmetic & Residues

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

Definition 2.1: Floor & Ceiling

For $x \in \mathbb{R}$ and $m, n \in \mathbb{Z}$. Functions map $\mathbb{R} \rightarrow \mathbb{Z}$,

Floor x , $\lfloor x \rfloor$, is the largest m such that $m \leq x < m + \varepsilon$, where $\varepsilon \in [0, 1)$.
i.e., round down to the nearest integer.

Ceiling x , $\lceil x \rceil$, is the smallest n such that $n - \varepsilon < x \leq n$, where $\varepsilon \in [0, 1)$.
i.e., round up to the nearest integer.

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: “ $a \bmod b$ ” or “ $a \% b$ ”.

Examples: $8 \bmod 3 = 2$, and $5 \bmod 2 = 1$

Proof 2.1: Mod Operator

The Division Algorithm (1.3) only works for $b > 0$. To generalize for $b < 0$,

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

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

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

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

Tip: $q = \lfloor \frac{a}{b} \rfloor$ is similar to integer division in programming, and $\frac{a}{b} = c$ implies $c \in \mathbb{R}$.

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:

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

x	$a - bx$	
0	0	$= 6 - 2 \cdot 0$
1	4	$= 6 - 2 \cdot 1$
2	2	$= 6 - 2 \cdot 2$
(0) 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:

b	$3 \bmod b$	b	$9 \bmod b$	b	$7 \bmod b$
1	0	1	0	1	0
2	1	2	1	2	1
3	0	3	0	3	1
(1) 4	3	4	1	4	3
5	3	5	4	5	2
6	3	6	3	6	1
7	3	7	2	7	0
8	3	8	1	8	7
		9	0		
		10	9		

Grouping them by the remainder:

(2)	r	$3 \bmod b$	r	$9 \bmod b$	r	$7 \bmod b$
	0	1, 3	0	1, 3, 9	0	1, 7
	1	2	1	2, 4, 8	1	2, 6
	2		2		2	5
	3	4, 5, 6, ...	3	5, 6, 7	3	4
			9	10, 11, 12, ...	7	8, 9, 10, ...

Let's try the other way around.

(3)	a	$a \bmod 3$	a	$a \bmod 9$	a	$a \bmod 7$
	0	0	0	0	0	0
	1	1	1	1	1	1
	2	2	2	2	2	2
	3	0	3	3	3	3
	4	1	4	4
	5	2	9	0	5	5
	6	0	10	1	6	6
	7	1	11	2	7	0
	8	2	8	1
	9	0	18	0	9	2
			19	1		

Grouping them by the remainder:

(4)	r	$a \bmod 3$	r	$a \bmod 9$	r	$a \bmod 7$
	0	0, 3, 6, 9	0	0, 9, 18	0	0, 7
	1	1, 4, 7	1	1, 10, 19	1	1, 8
	2	2, 5, 8	2	2, 11	2	2, 9
			3	3, 12	3	3
			4	4, 13	4	4
			5	5, 14	5	5
			6	6, 15	6	6
			7	7, 16		
			8	8, 17		

(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 , which 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 5 to 8, yields numbers ending in 3 or 8.
Then there are periods like (3).

We can see from the table (3), if we keep adding 3 to 2, we get 5, 8, 11, 14, etc.

(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
...

We can represent these periods by $[x, x + b)$. Expanding the Division Algorithm (1.3) beyond $b > 0$, allows us to represent intervals no matter where we start on the number line.

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 is the residue under modulo n .

Note: If modulo n has already been defined, $[a]_n$, then $[a]$ might be used.

Definition 2.5: Representative

If $x \in [a]$, x is a representative of $[a]$.

2.3 Ring Theory

We will primarily focus on **ideals** and the behavior of primes; Though to understand ideals, is to understand **groups**, **rings**, and **fields**.

Definition 3.1: Group

A *group* is a set G that is closed under one operation, say ' $*$ ', that satisfies four properties:

- **Closure:** For all $a, b \in G$, $a * b \in G$.
- **Associativity:** For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.
- **Identity:** There exists an element $e \in G$ such that for all $a \in G$, $a * e = e * a = a$.
- **Inverse:** $\forall a \exists a^{-1} \in G$, such that $a * a^{-1} = a^{-1} * a$ equates to the identity.

Examples: The following are groups:

- Set $S = \{-1, 1\}$ closed under multiplication.
 - **Closure:** $-1 \cdot -1 = 1 \in S$.
 - **Associativity:** $(-1 \cdot 1) \cdot -1 = 1 \cdot -1 = -1$ and $-1 \cdot (1 \cdot -1) = -1 \cdot 1 = -1$.
 - **Identity:** 1, as $1 \cdot -1 = -1 \cdot 1 = -1$.
 - **Inverse:** -1 as $-1 \cdot -1 = 1 =$ the identity.
- Set $I = \mathbb{Z}$ closed under addition.
 - **Closure:** $a + b \in I$ for all $a, b \in I$.
 - **Associativity:** $(a + b) + c = a + (b + c)$ for all $a, b, c \in I$.
 - **Identity:** 0, as $a + 0 = 0 + a = a$ for all $a \in I$.
 - **Inverse:** $-a$ for all $a \in I$, as $a + (-a) = (-a) + a = 0$.

Definition 3.2: Abelian Group

An *Abelian group* is a group that also satisfies the commutative property, i.e., for all $a, b \in G$, $a * b = b * a$. for some operation ‘*’.

Definition 3.3: Ring

A *ring* is a non-empty set R that is closed under additive (+) and multiplicative (\cdot) operations, such that:

- **Additive Group:** (R) is an Abelian group.
- **Multiplicative Closure:** For all $a, b \in R$, $a \cdot b \in R$.
- **Distributive Property:** For all $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.

Examples: \mathbb{Z} , \mathbb{Q} , \mathbb{R} , and \mathbb{C} are all rings standard addition and multiplication.

Note: Operations aren’t literally addition and multiplication. For example, the set of 2×2 matrices with \mathbb{R} entries forms a ring.

Tip: Numbers and symbols are just placeholders for the concepts they represent. 1,2 or (\div) don’t have inherent properties; they are just symbols, changing meaning in different contexts.

Definition 3.4: Ideal

An *ideal* I , is a special subset of a ring R , such that for all $a, b \in I$ and $r \in R$:

- **Additive:** $a + b \in I$.
- **Multiplicative under the ring:** $a \cdot r \in I$ or $r \cdot a \in I$.
- **Additive inverse:** $-a \in I$.
- **Additive identity:** $a, a' \in I$ such that $a + a' = a' + a = a'$.

Example: The set of all multiples of 2, $2\mathbb{Z}$, is an ideal of \mathbb{Z} .

- **Additive:** $(2 \cdot a) + (2 \cdot b) = 2(a + b) \in 2\mathbb{Z}$.
- **Multiplicative:** $(2 \cdot a) \cdot r = 2(a \cdot r) \in 2\mathbb{Z}$.
- **Additive inverse:** $-2 \in 2\mathbb{Z}$.
- **Additive identity:** $0 \in 2\mathbb{Z}$.

Definition 3.5: Field

A *field* is a ring \mathbb{F} with additional properties:

- **Additive Structure:** $(\mathbb{F}, +)$ forms an Abelian group.
- **Multiplicative Structure:** (\mathbb{F}, \cdot) forms an Abelian group excluding 0:
- **Distributive:** For all $a, b, c \in \mathbb{F}$, $a \cdot (b + c) = a \cdot b + a \cdot c$.

Example: \mathbb{Q} , the set of rational numbers:

- **Multiplicative identity:** $1 \in \mathbb{Q}$ as $1 \cdot a = a \cdot 1 = a$ for all $a \in \mathbb{Q}$.
- **Multiplicative inverse:** $a^{-1} = \frac{1}{a}$ as $a \cdot \frac{1}{a} = 1$.
- **Excludes 0:** As 0 has no multiplicative inverse, i.e., $\frac{1}{0}$ is undefined.

Tip: A **group** defines operations, an **abelian group** ensures commutativity, a **ring** has an abelian group $(+)$, multiplication (\cdot) , and distribution, an **ideal** $I \subseteq R$ ring, such that $a \in I, r \in R, a \cdot r \in I$, and a **field** is a ring excluding 0 in its multiplicative abelian group.

2.4 The Integer Ideal & Primality