My cryptography book

John Doe (February 15, 2023)

Contents

Chapter 1

Basic number theory

SUGGESTIONS. For this chapter, state the basic axioms and properties/theorems of $\mathbb{Z}$. Provide proofs. But remember that most of the properties/theorems can be generlized to properties/theorems for rings. It's still a good idea to prove the facts for $\mathbb{Z}$ since $\mathbb{Z}$ is not as abstract as general rings and will prepare you for the general results.

1.1 Axioms of $\mathbb{Z}$

We will assume that $(\mathbb{Z}, +, \cdot, 0, 1)$ satisfies the following axioms.

- PROPERTIES OF $+$:
  - Closure: If $x, y \in \mathbb{Z}$, then $x + y \in \mathbb{Z}$.
  - Associativity: If $x, y, z \in \mathbb{Z}$, then $(x + y) + z = x + (y + z)$.
  - Inverse: If $x \in \mathbb{Z}$, then there is some y such that $x + y = 0 = y + x$. The y in the above is an additive inverse of x.
  - Neutrality: If $x \in \mathbb{Z}$, then $0 + x = x = x + 0$.
  - Commutativity: If $x, y \in \mathbb{Z}$, then $x + y = y + x$.

  (Memory aid for the first four: CAIN.)
- PROPERTIES OF $\cdot$:
  - Closure: If $x, y \in \mathbb{Z}$, then $x \cdot y \in \mathbb{Z}$.
  - Associativity: If $x, y, z \in \mathbb{Z}$, then $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
  - Neutrality: If $x \in \mathbb{Z}$, then $1 \cdot x = x = x + 1$.
  - Commutativity: If $x, y \in \mathbb{Z}$, then $x \cdot y = y \cdot x$.

  It is common to write xy instead of $x \cdot y$.
- DISTRIBUTIVITY: If $x, y, z \in \mathbb{Z}$, then $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$

A set R with operations $+, \cdot$ and elements $0_R, 1_R$ satisfying the above properties

the above is called a commutative ring. This is an important generalization because there are many very useful commutative rings and we want to prove results about commutative rings so that these results can be applied to all commutative rings, including but not restricted to $\mathbb{Z}$. And if the commutativity of multiplication is left out, then we have the concept of a ring; for emphasize these are called non-commutative rings. This is also an important concept since $n \times n$ matrices with $\mathbb{R}$ entries, $\mathrm{M}_{n\times n}(\mathbb{R})$, form a non-commutative ring. In fact, more generally, the set of $n \times n$ matrices with entries in a commutative ring R, $\mathrm{M}_{n\times n}(R)$, is itself a non-commutative ring. We will return to the concept of commutative and non-commutative rings later.

The next property of $\mathbb{Z}$, integrality, is very special and does not apply to many communtative rings and is therefore left out of the definition of commutative ring:

- Integrality: If $x, y \in \mathbb{Z}$, then $xy = 0 \implies x = 0$ or $y = 0$.

Another property of $\mathbb{Z}$ that we will assume is

- Nontriviality: $0 \neq 1$

This axiom of $\mathbb{Z}$ is extremely simple, but cannot be deduced from the previous axioms.

The above forms the algebraic properties of $\mathbb{Z}$, i.e., properties involving addition and multiplication.

It is actually possible to first define axioms for $\mathbb{N} = \{0, 1, 2, ...\}$ and then define $\mathbb{Z}$ in terms of $\mathbb{N}$. We will not do that except to mention that the axioms for $\mathbb{N}$ are called the Peano-Dedekind axioms and that one very important Peano-Dedekind axiom of $\mathbb{N}$ is the

- Well-ordering principle (WOP) for $\mathbb{N}$: If X is a nonempty subset of $\mathbb{N}$, then X contains a minimum element, i.e., there is some $m \in X$ such that
$$m \leq x$$
for all $x \in X$.

Without going into details, it can be shown that for $\mathbb{N}$, the WOP is equivalent to each of the following axioms:

- Weak Mathematical Induction for $\mathbb{N}$: Let X be a subset of $\mathbb{N}$ satisyfing the following two conditions:

- $0 \in X$ and
- Let $n \in \mathbb{N}$. If $n \in X$, then $n+1 \in X$.

Then $X = \mathbb{N}$.

and

- Strong Mathematical Induction for $\mathbb{N}$: Let X be a subset of $\mathbb{N}$ satisyfing the following two conditions:
  - $0 \in X$ and
  - Let $n \in \mathbb{N}$. If $k \in X$ for all $0 \leq k \leq n$, then $n+1 \in X$.

  Then $X = \mathbb{N}$.

In the above two induction axioms, if we write $X = \{n \mid P(n)\}$ where $P(n)$ is a propositional formula, then the induction axioms can be rewritten in the following way:

- Weak Mathematical Induction: Let $P(n)$ be a proposition for $n \in \mathbb{N}$ satisyfing the following two conditions:
  - $P(0)$ is true and
  - Let $n \in \mathbb{N}$. If $P(n)$ is true, then $P(n+1)$ is true.

  Then $P(n)$ is true for all $n \in \mathbb{N}$.

and

- Strong Mathematical Induction: Let $P(n)$ be a proposition for $n \in \mathbb{N}$ satisyfing the following two conditions:
  - $P(0)$ is true and
  - Let $n \in \mathbb{N}$. If $k \in X$ for all $0 \leq k \leq n$, then $n+1 \in X$.
  - Let $n \in \mathbb{N}$. If $P(k)$ is true for $0 \leq k \leq n$, then $P(n+1)$ is true.

  Then $P(n)$ is true for all $n \in \mathbb{N}$.

The above are the algebraic axioms of $\mathbb{Z}$. There's also the order relation of $\mathbb{Z}$ which is used in WOP and the two induction principles. I will formalize the axioms of the order relation later. For now one can assume that the order relation is defined as follows: If $x \in \mathbb{Z}$, then

$$x < y$$

if there is some $z \in \mathbb{N}$ such that

$$x + z = y$$

There is one more axiom of $\mathbb{Z}$ that is related to the "topology" of $\mathbb{Z}$ and uses the order relation:

- Topology: Given any $x \in \mathbb{Z}$, there is no $y \in \mathbb{Z}$ such that

$$x < y < x + 1$$

You can think of topology of a set as study of "closeness" of values in that set. For $\mathbb{Q}$, given any two distinct rational values $x < y$, there is also some $z \in \mathbb{Q}$ such that $x < z < y$. This is the same for $\mathbb{R}$. Therefore the topology of $\mathbb{Z}$ is very different from the topology of $\mathbb{Q}$ and $\mathbb{R}$ because there are "holes" in $\mathbb{Z}$ where there are no $\mathbb{Z}$ values. $\mathbb{Z}$ has what is called a discrete topology.

The above assume the existence of an order relation on $\mathbb{Z}$, i.e., $<$. We have to include the following axioms of $<$ on $\mathbb{Z}$. There is a set $\mathbb{Z}^+$ such that the following holds:

- Trichotomy: If $x \in \mathbb{Z}$, then exactly one of the following holds: $-x \in \mathbb{Z}^+$, $x = 0$, $x \in \mathbb{Z}^+$.
- Closure of $+$: If $x, y \in \mathbb{Z}^+$, then $x + y \in \mathbb{Z}^+$.
- Closure of $\cdot$: If $x, y \in \mathbb{Z}^+$, then $x \cdot y \in \mathbb{Z}^+$.

We then define $<$ as follows: If $x, y \in \mathbb{Z}$, then we write $x < y$ if

$$y - x \in \mathbb{Z}^+$$

Since $<$ is defined, we can define $x \leq y$ to mean "either $x < y$ or $x = y$". The above order relation is expressed abstractly without refering to the fact that $\mathbb{Z}^+$ is $\{1, 2, 3, ...\}$, i.e., the set of positive integers. In fact, you can prove $\mathbb{Z}^+ = \{1, 2, 3, ...\}$ from the above axioms – see exercises below.

Proposition 1.1.1. *The additive inverse for x is unique. In other words, if y, y' satisfies*

$$x + y = 0 = y + x$$
$$x + y' = 0 = y' + x$$

Then $y = y'$.

Since the additive inverse of x is unique, we can choose to write the additive inverse of x in terms of x. This is usually written $-x$. We define the operator $-$ in terms of the additive inverse:

Definition 1.1.1. Let $x, y \in \mathbb{Z}$. We define the subtraction operator as

$$x - y = x + (-y)$$

Note that every x in $\mathbb{Z}$ as an additive inverse, but we did not require value of $\mathbb{Z}$ to have multiplicative inverse:

Definition 1.1.2. Let $x \in \mathbb{Z}$. Then y is a multiplicative inverse of x if

$$x \cdot y = 1 = y \cdot x$$

We say that x is a **unit** if x has a multiplicative inverse. We can also say that x is **invertible**.

unit

invertible

Intuitively, you know that the only values of $\mathbb{Z}$ with multiplicative inverses are 1 and -1.

Proposition 1.1.2. *Let $x \in \mathbb{Z}$. If x is a unit, then the multiplicative inverse of x is unique. In other words if y, y' satisfies*

$$xy = 1 = yx$$
$$xy' = 1 = y'x$$

then $y = y'$.

Definition 1.1.3. The multiplicative inverse of x, it is exists, is is denoted by x^{-1}.

Proposition 1.1.3. *Cancellation law for addition. Let $x, y, z \in \mathbb{Z}$.*

(a) *If $x + z = y + z$, then $x = y$.*
(b) *If $z + x = z + y$, then $x = y$.*

Proposition 1.1.4. *Let $x \in \mathbb{Z}$.*

(a) $0x = 0 = x0$
(b) $-0 = 0$
(c) $x - 0 = x = 0 - x$.

Proof. (a) We will first prove $0x = 0$:

$$\begin{aligned} 0x &= (0+0)x && \text{by Neutrality of } + \\ &= 0x + 0x && \text{by Distributivity} \end{aligned} \tag{1}$$

Since $0x \in \mathbb{Z}$ by Closure of $\cdot$, there is exists some $y \in \mathbb{Z}$ which is an additive inverse of $0x$, i.e.,

$$0x + y = 0 = y + 0x \tag{2}$$

From (1),

$$\begin{aligned} y + 0x &= y + (0x + 0x) && \\ 0 &= y + (0x + 0x) && \text{by (2)} \\ 0 &= (y + 0x) + 0x && \text{by Associativity of } + \\ 0 &= 0 + 0x && \text{by (2)} \\ 0 &= 0x && \text{by Neutrality of } + \end{aligned}$$

To prove $0 = x0$, from above

$$\begin{aligned} 0 &= 0x \\ &= x0 && \text{by Commutativity of } \cdot \end{aligned}$$

(b) TODO

(c) TODO □

Proposition 1.1.5. *Let $x, y \in \mathbb{Z}$.*

(a) $-(-1) = 1$
(b) $-(-x) = x$
(c) $x(-1) = -x = (-1)x$
(d) $(-1)(-1) = 1$
(e) $(-x)(-y) = xy$

Proposition 1.1.6. *Cancellation law for multiplication. Let $x, y, z \in \mathbb{Z}$.*

(a) *If $xz = yz$ and $z \neq 0$, then $x = y$.*
(b) *If $zx = zy$ and $z \neq 0$, then $x = y$.*

For convenience, I will write $x^2 = xx$ and in general

$$x^n = \begin{cases} 1 & \text{if } n = 0 \\ x^{n-1}x & \text{if } n > 0 \end{cases}$$

If x has a multiplicative inverse, i.e., if x^{-1} exists, then, for $n \geq 0$, I will define

$$x^{-n} = \left(x^{-1}\right)^n$$

Proposition 1.1.7. *Let $x \in \mathbb{Z}$. Then $[n]x = n \cdot x$.*

Note that nx has two meanings: nx can be the multiplication of n and x and it can also be $x + \cdots + x$ with n number of x. Of course you would expect them to be the same. For now define

$$[n]x = \begin{cases} 0 & \text{if } n = 0 \\ [n-1]x + x & \text{if } n > 0 \end{cases}$$

and if n is negative, we define

$$[n]x = -([-n]x)$$

1.2 Divisibility

Definition 1.2.1. Let $m, n \in \mathbb{Z}$. Then we say that m **divides** n, and we write $m \mid n$, if there is some $x \in \mathbb{Z}$ such that $mx = n$, i.e.,

$$\exists x \in \mathbb{Z} \cdot [mx = n]$$

Proposition 1.2.1. *Let $a \in \mathbb{Z}$.*

(a) *Then $1 \mid a$.*
(b) *If $a \neq 0$, then $a \mid 0$.*
(c) *(Reflexive) If $a \neq 0$, then $a \mid a$.*
(d) *If $a \mid b$ and $b \mid a$, then $a = \pm b$.*
(e) *(Transitive) If $a \mid b$ and $b \mid c$, then $a \mid c$.*
(f) *If $a \mid b$, then $a \mid bc$.*
(g) *If $a \mid b$, $a \mid c$, then $a \mid b + c$.*
(h) *(Linearity) If $a \mid b$, $a \mid c$, then $a \mid bx + cy$ for $x, y \in \mathbb{Z}$.*

1.3 Congruences

Definition 1.3.1. Let $a, b \in \mathbb{Z}$ and $N \in \mathbb{Z}$ with $N > 0$. Then a is congruent to b mod N and we write

$$a \equiv b \pmod{N}$$

if $N \mid a - b$.

Proposition 1.3.1. *Let $a, b, c, a', b' \in \mathbb{Z}$.*

(a) *(Reflexivity)* $a \equiv a \pmod{N}$
(b) *(Symmetry) If* $a \equiv b \pmod{N}$, *then* $b \equiv a \pmod{N}$
(c) *(Transitivity) If* $a \equiv b, b \equiv c \pmod{N}$, *then* $a \equiv c \pmod{N}$
(d) *If* $a \equiv b$, $a' \equiv b' \pmod{N}$, *then* $a + a' \equiv b + b' \pmod{N}$.
(e) *If* $a \equiv b$, $a' \equiv b' \pmod{N}$, *then* $aa' \equiv bb' \pmod{N}$.

Proposition 1.3.2. *Let $a, N \in \mathbb{Z}$ with $N > 0$. Let $q, r \in \mathbb{Z}$ such that*

$$a = Nq + r, \quad 0 \leq r < N$$

Then $a \equiv r \pmod{N}$.

Chapter 2

Classical ciphers

2.1 Shift cipher

Definition 2.1.1. The **shift cipher** (E, D) is given by

$$E(k, x) = x + k \pmod{26}$$

and

$$D(k, x) = x - k \pmod{26}$$

Historically the shift cipher with key $k = 3$ was used by Julius Caesar and is called the **Caesar cipher**.

2.2 Affine cipher

2.3 Vigenère cipher

2.4 Substitution cipher

2.5 Permutation cipher

2.6 Hill cipher

2.7 One-time pad cipher

2.8 Linear feedback shift register

Chapter 3

Group theory

3.1 Definitions

The most basic mathematical object is $\mathbb{Z}$. $\mathbb{Z}$ has two operations: addition and multiplication. We first abstract the study of $\mathbb{Z}$ by focusing on just one operation, the $+$.

Definition 3.1.1. $(G, *, e)$ is a **group** if G is a set and $*$ satisfies group

(C) If $x, y \in G$, then $x * y \in G$. In other words $* : G \times G \to G$ is a binary operator.
(A) If $x, y, z \in G$, then $(x * y) * z = x * (y * z)$.
(I) If $x \in G$, then there is some $y \in G$ such that $x * y = e = y * x$. y is called an **inverse** of x. Later we will see that the inverse of x is uniquely determined by x. inverse
(N) If $x \in G$, then $x * e = x = e * x$.

Definition 3.1.2. $(G, *, e)$ is an **abelian group** if $(G, *, e)$ is a group such that if $x, y \in G$, then $x * y = y * x$. In other words, $(G, *, e)$ is an abelian group if $(G, *, e)$ is group and $*$ is a commutative operator. abelian group

The reason for now including the commutativity condition in the definition for groups is because there are many important groups which are not abelian.

Chapter 4

Ring theory

Chapter 5

Field theory

Index

Bibliography

[1] Leslie Lamport, *LaTeX: a document preparation system*, Addison Wesley, Massachusetts, 2nd edition, 1994. (EXAMPLE)