CISS451: Cryptography

Y. Liow (February 10, 2025)

Contents

Chapter 1

Basic number theory

1.1 Axioms of $\mathbb{Z}$ debug: axioms-of-Z.tex

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 $(y + z) \cdot x = y \cdot x + z \cdot x$

additive inverse

(In the Inverse axiom above, we say that y is *an* additive inverse of x. Later we will show that x has only one additive inverse. Therefore we can say y is *the* additive invers of x.) Also, it is conventional to write xy for $x \cdot y$.

A set R with operations $+_R, \cdot_R$ and elements $0_R, 1_R$ satisfying the above properties 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 $\mathbb{Z}$. If the commutativity of multiplication is left out, then we have the concept of a **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. By convention, **ring** means commutative ring. We will return to the concept of commutative and non-commutative rings later.

commutative ring

non-commutative rings

ring

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

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

In general a ring satisfying the integrality condition is called an **integral domain**. Therefore $\mathbb{Z}$ is not just a commutative ring – it is an integral domain. Another property of $\mathbb{Z}$ that we will assume is

integral domain

- Nontriviality: $0 \neq 1$

The nontriviality 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 $\mathbb{N}$. (See my Calculus notes.) 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 $\mathbb{N}$

- Induction of $\mathbb{N}$: If X is a subset of $\mathbb{N}$ satisfying
  - $0 \in X$
  - If $n \in X$, then $n + 1 \in X$

  Then $X = \mathbb{N}$.

It can be proven that as a consequence of the induction axiom of $\mathbb{N}$, we have

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

  $$m \leq x$$

  for all $x \in X$.

least element

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 properties, 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 for $\mathbb{N}$: 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 for $\mathbb{N}$: 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 $n \in \mathbb{N}$.

There are statements analogous to the above, but for $\mathbb{Z}$:

- WOP for $\mathbb{Z}$: If X is a nonempty subset of $\mathbb{Z}$ that is bounded below, then X contains a **least element**, i.e., there is some $m \in X$ such that

  least element

  $$m \leq x$$

  for all $x \in X$. Here, X is **bounded below** means there is some $b \in \mathbb{Z}$ such that

  bounded below

  $$b \leq x$$

  for all $x \in X$. Note that b in the above is in $\mathbb{Z}$ and need not be in X. For instance if $X = -1, 1, 42$, then the least element of X is -1 and $b = -3 \in Z$ is a lower bound of X. However the least element of X must be an element of X.

- Weak Mathematical Induction for $\mathbb{Z}$: Let $n_0 \in \mathbb{Z}$. Let $P(n)$ be a proposition for $n \in \mathbb{Z}$ and $n \geq n_0$ satisyfing the following two conditions:
  - $P(n_0)$ is true and
  - Let $n \in \mathbb{Z}$ with $n \geq n_0$. If $P(n)$ is true, then $P(n+1)$ is true.

  Then $P(n)$ is true for all $n \in \mathbb{Z}$, $n \geq n_0$.

- Strong Mathematical Induction for $\mathbb{Z}$: Let $P(n)$ be a proposition for $n \in \mathbb{Z}, n \geq n_0 \in Z$ satisyfing the following two conditions:
  - $P(n_0)$ is true and
  - Let $n \in \mathbb{Z}$. If $k \in X$ for all $0 \leq k \leq n$, then $n+1 \in X$.
  - Let $n \in \mathbb{Z}$. If $P(k)$ is true for $0 \leq k \leq n$, then $P(n+1)$ is true.

  Then $P(n)$ is true for all $n \in \mathbb{Z}$, $n \geq n_0$.

It can be shown that from the induction axiom of $\mathbb{N}$, we can prove that the WOP of $\mathbb{N}$, the weak induction of $\mathbb{N}$, and the strong induction of $\mathbb{N}$ hold. Furthermore, these implies the WOP for $\mathbb{Z}$, the weak induction of $\mathbb{Z}$, and the strong induction of $\mathbb{Z}$ holds.

Note that obvious statement of "WOP for $\mathbb{R}$" does not hold. For instance the open interval $X = (0, 1)$ is bounded below (for instance by -42). However there is no m in X such that $m \leq x$ for all x in X. For instance $m = 0.01 \in X$ is not a least element of X since $0.0001 \in X$ is smaller than m. Also, $m = 0.0000001 \in X$ is also not a least element of X since $0.0000000001 \in X$ is less than m. In fact for any $m \in X$, $(1/2)m$ is in X and is less than m. In other words no value in X can be a minimum value of X.

(See end of this section for exercises on WOP and induction.)

The above are the algebraic and inductive-type axioms of $\mathbb{Z}$. There are also the order relations such as $<$ and $\leq$ of $\mathbb{Z}$. Technically speaking, the order relation should come before the inductive axiom, WOP, and induction (weak and strong) since they use order relations.

The following are the order axioms of $\mathbb{Z}$. We assume there is a subset $\mathbb{Z}^+$ of $\mathbb{Z}$ satisfying the following: $\mathbb{Z}^+$

- Trichotomy for $\mathbb{Z}$: If $x \in \mathbb{Z}$, then exactly one of the following holds:

$$-x \in \mathbb{Z}^+, \quad x = 0, \quad x \in \mathbb{Z}^+$$

- Closure of $+$ for $\mathbb{Z}^+$: If $x, y \in \mathbb{Z}^+$, then $x + y \in \mathbb{Z}^+$.
- Closure of $\cdot$ for $\mathbb{Z}^+$: If $x, y \in \mathbb{Z}^+$, then $x \cdot y \in \mathbb{Z}^+$.

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

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

i.e., there is some $z \in \mathbb{Z}^+$ such that

$$y - x = z$$

i.e.,

$$y = x + z$$

Since $<$ is defined (on $\mathbb{Z}$), we can define $x \leq y$ (on $\mathbb{Z}$) to mean "either $x < y$ or $x = y$". The above order relation is expressed abstractly without referring 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. Of course you define $x > y$ to be the same as $y < x$ and $x \geq y$ to be $y \leq x$. Also, we say $x \in \mathbb{Z}$ is **positive** is $x > 0$.

≤

positive

The three axioms in the order relation on $\mathbb{Z}$ can be derived from the order relation axioms of $\mathbb{N}$. The order relation on $\mathbb{N}$ is defined as follows: For $\mathbb{N} = \{0, 1, 2, 3, ...\}$, we simply define

$$x \geq 0$$

for all $x \in \mathbb{N}$. For $x, y \in \mathbb{N}$, we define

$$x \geq y$$

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

$$x = y + z$$

Finally $x > y$ is defined to be $x \geq y$ and $x \neq y$. If $x > 0$, we say that x is **positive**. Just like positivity in $\mathbb{Z}$, if $x \in \mathbb{N}$, we say that x if **positive** if $x > 0$.

positive

Also, we will define $|x|$ in the usual way:

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{otherwise} \end{cases}$$

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

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

$$x < y < x + 1$$

This can derived from this:

- Topology for $\mathbb{N}$: There is no $x \in \mathbb{N}$ such that

$$0 < x < 1$$

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**. On the other hand $\mathbb{Q}$ and $\mathbb{R}$ are "dense". (I won't go further into topology since we won't need it. See my notes on topology.) The above assumes the existence of an order relation of $\mathbb{Z}$, i.e., $<$.

discrete topology

Now let's prove some algebraic facts about $\mathbb{Z}$ that can be deduced from the fact that $\mathbb{Z}$ is a commutative ring.

Proposition 1.1.1. (**Uniqueness of additive inverse**). *The additive inverse for x is unique. In other words, if y, y' satisfy*

Uniqueness of additive inverse

$$x + y = 0 = y + x \tag{1}$$
$$x + y' = 0 = y' + x \tag{2}$$

then $y = y'$.

Proof.

$$\begin{aligned}
y &= 0 + y && \text{by Identity of } + \\
&= (y' + x) + y && \text{by RHS of (2)} \\
&= y' + (x + y) && \text{by Associativity of } + \\
&= y' + 0 && \text{by LHS of (1)} \\
&= y' && \text{by Neutrality of } +
\end{aligned}$$

□

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 $-x$. (Had it been the case that the additive inverse of x is not unique, we would have to denote the additive inverses of x by $(-x)_1$, $(-x)_2$, etc.)

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 value in $\mathbb{Z}$ has an additive inverse, but we do not require values of $\mathbb{Z}$ to have multiplicative inverses:

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

multiplicative inverse

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

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

unit

invertible

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

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

Uniqueness of multiplicative inverse

$$xy = 1 = yx \tag{1}$$
$$xy' = 1 = y'x \tag{2}$$

then $y = y'$.

Proof.

$$\begin{aligned}
y &= 1 \cdot y && \text{by Identity axiom of } \cdot \\
&= (y' \cdot x) \cdot y && \text{by RHS of (1)} \\
&= y' \cdot (x \cdot y) && \text{by Associativity of } \cdot \\
&= y' \cdot 1 && \text{by LHS of (2)} \\
&= y' && \text{by Neutrality of } \cdot
\end{aligned}$$

□

Definition 1.1.3. The multiplicative inverse of x, if is exists, is denoted by x^{-1}. The set of all units of $\mathbb{Z}$ is denoted by either $U(\mathbb{Z})$ or $\mathbb{Z}^\times$. We will show later that $U(\mathbb{Z}) = \{-1, 1\}$.

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

Cancellation law for addition

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

Proof. TODO □

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

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

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

$$\begin{aligned} 0x &= (0+0)x && \text{by Neutrality of } + \\ &= 0x + 0x && \text{by Distributivity} \\ \therefore\ 0 + 0x &= 0x + 0x && \text{by Neutrality of } + \\ 0 &= 0x && \text{by Cancellation Law of Addition} \end{aligned}$$

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* $x, y, c \in \mathbb{Z}$.

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

Proof. TODO □

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

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

Proof. TODO □

For general expressions involving n terms, instead of writing $x_1 + \cdots + x_n$, we formally define $\sum_{i=1}^{n}$

$$\sum_{i=1}^{n} x_i = \begin{cases} 0 & \text{if } n = 0 \\ \sum_{i=1}^{n-1} x_i + x_n & \text{if } n > 0 \end{cases}$$

Note that the definition above implies that our summation is left associative, i.e.,

$$\begin{aligned} \sum_{i=1}^{3} x_i &= \sum_{i=1}^{2} x_i + x_3 \\ &= \left(\sum_{i=1}^{1} x_i + x_2 \right) + x_3 \\ &= \left(\left(\sum_{i=1}^{0} x_i + x_1 \right) + x_2 \right) + x_3 \\ &= ((0 + x_1) + x_2) + x_3 \\ &= (x_1 + x_2) + x_3 \end{aligned}$$

This conforms with the standard practice. Likewise, we define $\prod_{i=1}^{n}$

$$\prod_{i=1}^{n} x_i = \begin{cases} 1 & \text{if } n = 0 \\ \prod_{i=1}^{n-1} x_i + x_n & \text{if } n > 0 \end{cases}$$

Proposition 1.1.7. (**General associativity**) *Let* $x_1, \ldots, x_n \in \mathbb{Z}$. General associativity

(a) *Different fully parenthesized expressions of* $x_1 + \cdots + x_n$ *evaluates to the same value.*
(b) *Different fully parenthesized expressions of* $x_1 \cdot \cdots \cdot x_n$ *evaluates to the same value.*

Proof. The proof for both statements are similar. We will only prove (b).

TODO □

Now for the case when the summation or product involves the same value, we have the following. For convenience, I will write $x^2 = xx$ and in general $()^n$

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

Note that

$$x^3 = x^2x = (x^1x)x = ((x^0x)x)x = ((1x)x)x = (xx)x$$

i.e., the above recursive definition of x^n is left recursive. If x has a multiplicative inverse, i.e., if x^{-1} exists, then, for $n \geq 0$, I will define

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

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

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

$[n]x$ is just a notation that is easier to write than $\sum_{i=1}^{n} x$. And if n is negative, we define

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

I'll write $[\bullet]$ for the function $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ as defined above.

Proposition 1.1.8. *Let $x \in \mathbb{Z}$. Then $[n]x = n \cdot x$, i.e., "add n copies of x" is the same as "multiply n and x".*

Proof. We will prove two proofs, using weak induction and WOP.

First we proof the above for $n \geq 0$ using weak induction. For $n \geq 0$, let $P(n)$ be the statement that $[n]x = n \cdot x$.

Base case: We now prove $P(0)$ holds. By definition, $[0]x = 0$. By Proposition 1.1.4 (page 11), $0 \cdot x = 0$. Hence $[0]x = 0 \cdot x$, i.e., $P(0)$ holds.

Inductive case: Now assume $P(n)$ holds, i.e, $[n]x = n \cdot x$. We will prove that $P(n+1)$ holds. We have

$$\begin{aligned}
[n+1]x &= [n]x + x && \text{by definition of } [\bullet] \\
&= n \cdot x + x && \text{by inductive hypothesis } P(n) \\
&= n \cdot x + 1 \cdot x && \text{by Neutrality of } \cdot \\
&= (n+1) \cdot x && \text{by Distributivity}
\end{aligned}$$

Hence $P(n+1)$ holds.

Therefore by weak induction $P(n)$ holds for all integers $n \geq 0$.

We now prove $P(n)$ holds for integers $n < 0$:

$$\begin{aligned}
[n]x &= -([-n]x) && \text{by definition of } [\bullet] \\
&= -((-n) \cdot x) && \text{by } P(-n) \\
&= (-1) \cdot ((-n) \cdot x) && \text{by Proposition 1.1.5(c) (page 11)} \\
&= ((-1) \cdot (-n)) \cdot x) && \text{by Associativity of } \cdot \\
&= (1 \cdot n) \cdot x && \text{by Proposition 1.1.5(e) (page 11)} \\
&= n \cdot x && \text{by Neutrality of } \cdot
\end{aligned}$$

Next, we proof the above for $n \geq 0$ using WOP.

TODO □

Now let us look at order relations on $\mathbb{Z}$.

Proposition 1.1.9. *Let $a, b, c, d \in \mathbb{Z}$ with $x > 0$.*

(a) *If $a < b$, then $a + c < b + c$.*
(b) *If $a < b$, then $ax < bx$.*
(c) *If $a < b$, then $a(-x) > b(-x)$.*
(d) $a < a + c$
(e) $a \leq ac$

There are analogous statements for (a)-(c) where $<$ and $>$ are replaced by $\leq$ and $\geq$.

Proof. (a) Note that

$$\begin{aligned}
(b+c)-(a+c) &= (b+c)+(-(a+c)) && \text{by definition of } - \\
&= b+(c+(-(a+c))) && \text{by Associativity of } + \\
&= b+(c+(-a+-c)) && \text{by Proposition 1.1.5 (page 11)} \\
&= b+(c+(-c+-a)) && \text{by Commutativity of } + \\
&= b+((c+-c)+-a) && \text{by Associativty of } + \\
&= b+(0+-a)) && \text{by Inverse of } + \\
&= b+-a && \text{by Neutrality of } + \\
&= b-a && \text{by definition of } - \qquad (1)
\end{aligned}$$

We have

$$\begin{aligned}
& a<b \\
\therefore\ & b-a\in\mathbb{Z}^+ && \text{by definition of } < \\
\therefore\ & (b+c)-(a+c)=b-a\in\mathbb{Z}^+ && \text{by (1)} \\
\therefore\ & b+c>a+c && \text{by definition of } <
\end{aligned}$$

□

Proposition 1.1.10. $1\in\mathbb{Z}^+$, *i.e.,* 1 *is positive.*

Proof. TODO □

Proposition 1.1.11. $\mathbb{Z}^+=\{1,2,3,...\}=\mathbb{N}-\{0\}$.

Proof. TODO □

Proposition 1.1.12. *The only units of* $\mathbb{Z}$ *are* $-1,1$, $U(\mathbb{Z})=\{-1,1\}$.

Proof. TODO □

The following are examples of proofs using WOP and induction.

Exercise 1.1.1. For $n \in \mathbb{N}$,

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

Here, when $n = 0$, $1 + 2 + \cdot + n$ is defined to be 0.

(a) Prove the above using weak induction.
(b) Prove the above using WOP.

Proof. TODO □

Exercise 1.1.2. For $n \in \mathbb{N}$,

$$1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)$$

Here, when $n = 0$, $1 + 2 + \cdot + n$ is defined to be 0.

(a) Prove the above using weak induction.
(b) Prove the above using WOP.

Proof. TODO □

Exercise 1.1.3. What is wrong with this proof? I claim that every man wears brown pants. I will prove this by weak induction. Let $P(n)$ be the statement that every man in a set of n men wears brown pants. Clearly $P(0)$ is true. For, if $P(0)$ does not hold, then there is a man in an empty set that does not wear brown pants. But an empty set cannot contain a man. Now, let $n \geq 0$ and assume $P(n)$ hold. I will prove that $P(n+1)$ holds. Let X be a set with $n+1$ men. Let Y be a subset of X with exactly n men. Since there are n men in Y, by induction hypothesis, every men in Y wears brown pants. Of course Y misses one man from X, say John. Now form another subset Z of X with exactly n men that contains John. Again by induction hypothesis $P(n)$ hold and therefore every men in Z wears brown pants, including John. Since X is made up of men in Y together with John, we have shown that every men in X wears brown pants. Therefore by weak induction, every men wears brown pants.

(Of course the above cannot possible be true. In fact: you can change "every man wears brown pants" to "every man wears the same pair of pants".)

TODO

Exercise 1.1.4. What is wrong with this proof? I claim that every man has the same favorite number. I will prove this by weak induction. Let $P(n)$ be the statement that every man in a set of n men has the same favorite number as the rest. Clearly $P(0)$ is true vacuously like the previous exercise. Now, let $n \geq 0$ and assume $P(n)$ hold. I will prove that $P(n+1)$ holds. Let X be a set of $n+1$ men. Line the men in X in a line. The set Y of the first n men of X must all share the same favorite number since there are n men in Y. Let Z be the set of n men of X that excludes the first man. All the men in Z must have the same favorite number as well. Clearly every men in Y has the same favorite number as the man in the middle of the line and every men in Z also has the same favorite number as this man in the middle. Therefore all men in X have the same favorite number. Hence every men shared the same favorite number.

TODO

Exercise 1.1.5. What is wrong with this proof? I claim that every day is Monday. I will prove this by strong induction. Let $P(n)$ be the statement that every day in a set of n days is Monday. Clearly $P(0)$ is true. For, if $P(0)$ does not hold, then there is a day in an empty set that is not Monday. But an empty set cannot have a day. Now, let $n \geq 0$ and assume $P(0), P(1), ..., P(n)$ hold. I will prove that $P(n+1)$ holds. Let X be a set with $n+1$ days. Let Y be a subset of X with exactly n days. Since there are n days in Y, by induction hypothesis, every day in Y in Monday. Y misses one day in X, say x. Also by $P(1)$, since $\{x\}$ is a set of size 1, x is also Monday. Since $X = Y \cup \{x\}$, we have shown that every day in X is Monday, Therefore by strong induction, every day is Monday.

TODO

Exercise 1.1.6. What is wrong with this proof? I will prove by strong induction that $e^n = 1$ for all $n \geq 0$. Let $P(n)$ be the statement that $e^n = 1$. Clearly $e^0 = 1$. Therefore $P(0)$ holds. Now assume $P(0), P(1), ..., P(n)$ holds. Since $P(n)$ and $P(1)$ holds, we have $e^{n+1} = e^n \cdot e^1 = 1 \cdot 1 = 1$. Hence $P(n+1)$ holds. Therefore, by strong induction, $P(n)$ holds for all n, i.e., $e^n = 1$ for all $n \geq 0$.

TODO

Exercise 1.1.7. What is wrong with this proof? I will prove by strong induction that given $x \in \mathbb{R}$, $\sum_{i=1}^{n} x = 0$ for $n \geq 0$. Let $P(n)$ be the above statement. $P(0)$ holds since $\sum_{i=1}^{0} x$ is a sum with no terms and by convention is 0. Now assume $P(0), P(1), ..., P(n)$ holds. Let $n+1 = a+b$ with both a, b approximately equal. (For instance if $n+1$ is even, $a = b = (n+1)/2$. And if $n+1$ is odd, $a = \lfloor (n+1)/2 \rfloor$ and $b = n+1-a$.) Since $P(a)$ and $P(b)$ holds, $\sum_{i=1}^{a} x = 0$ and $\sum_{i=1}^{b} x = 0$. Clearly $\sum_{i=1}^{n+1} x = \sum_{i=1}^{a} x + \sum_{i=1}^{b} x$ since the LHS is a sum of $n+1$ x's and there are $a+b$ x's on the RHS. Hence

$$\sum_{i=1}^{n+1} x = \sum_{i=1}^{a} x + \sum_{i=1}^{b} x = 0 + 0 = 0$$

Therefore $P(n+1)$ holds. By strong induction $P(n)$ holds for all $n \geq 0$, i.e., $\sum_{i=1}^{n} x = 0$ for $n \geq 0$.

TODO

1.2 Divisibility debug: divisibility.tex

Definition 1.2.1. Let $a, n \in \mathbb{Z}$ with $a \neq 0$. Then we say that a **divides** b, and we write $a \mid b$, if there is some $x \in \mathbb{Z}$ such that $ax = b$, i.e.,

$$\exists x \in \mathbb{Z} \cdot [ax = b]$$

(The "$\in \mathbb{Z}$" is not necessary as long as it is clear the universe is $\mathbb{Z}$.) Note that when you write $a \mid b$, the a is always nonzero.

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

(a) $1 \mid a$.
(b) $a \mid 0$.
(c) Reflexivity*: $a \mid a$.*
(d) Transitivity*: If $a \mid b$ and $b \mid c$, then $a \mid c$.*
(e) Antisymmetry: *If $a \mid b$ and $b \mid a$, then $a = \pm b$.*
(f) *If $a \mid b$, then $a \mid bc$.*
(g) *If $a \mid b$ and $a \mid c$, then $a \mid b + c$.*
(h) Linearity*: If $a \mid b$, $a \mid c$, then $a \mid bx + cy$ for $x, y \in \mathbb{Z}$.*
(i) *If $a \mid b$, then $|a| \leq |b|$.*

Proof. TODO □

1.3 Congruences debug: congruences.tex

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 $N \mid a - b$. In the above expression

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

we say that N is the modulus of the above relation between a and b.

Proposition 1.3.1. *Let $a, b, c, a', b' \in \mathbb{Z}$ and $N, N' \geq$ be 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) Additivity: *If* $a \equiv b$, $a' \equiv b' \pmod{N}$, *then* $a + a' \equiv b + b' \pmod{N}$.
(e) Multiplicativity: *If* $a \equiv b$, $a' \equiv b' \pmod{N}$, *then* $aa' \equiv bb' \pmod{N}$.
(f) *If* $a \equiv b \pmod{NN'}$, *then* $a \equiv b \pmod{N}$

Proof. TODO □

The following connects the Euclidean property and the congruence relation:

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

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

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

Proof. TODO

Definition 1.3.2. Let $a, N \in \mathbb{Z}$ with $N > 0$. By the Euclidean property of $\mathbb{Z}$, there exist unique q, r such that

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

r is called the "**residue** of a mod N" ("residue" = "what is left" after a is divided by N, i.e., the remainder after a is divided by N). It is common to

write r as $a \bmod N$.

Sometimes $a \bmod N$ is written as $r_N(a)$. For instance to find the residue of 15 mod 4, there is some q such that

$$15 = 4q + 3, \;\; 0 \leq 1 < 4$$

i.e.

$$15 \equiv 3 \pmod 4$$

where $0 \leq 1 < 4$. Therefore the residue of 15 mod 4 is 1, or we simple write

$$15 \bmod 4 = 3$$

i.e., $r_4(15) = 3$.

Warning: "mod" now has two meanings. "mod N", where $N > 0$ is an integer, can be used to denote a relation between integers

$$a \equiv b \pmod N$$

and "mod N" can also be used to denote a function

$$a \bmod N = r$$

Exercise 1.3.1. Show that the cancellation law for $\mathbb{Z}$ does not translate to $\mathbb{Z}$ mod N. In other words, find N, a, b, c such that $c \not\equiv 0 \pmod N$ and

debug: exercises/nt-50/question.tex

$$ac \equiv bc \pmod N, \;\; a \not\equiv b \pmod N$$

(Go to solution, page 22) □

Solutions

Solution to Exercise 1.3.1.

debug: exercises/nt-50/answer.tex

Solution not provided.

Index

Bibliography