Chapter 1: The Integers

Dana C. Ernst

Plymouth State University
Department of Mathematics
http://oz.plymouth.edu/~dcernst

Spring 2010

In this chapter, we will review:

In this chapter, we will review:

- The First Principle of Mathematical Induction (also called the Principle of Mathematical Induction, or just PMI),

In this chapter, we will review:

- The First Principle of Mathematical Induction (also called the Principle of Mathematical Induction, or just PMI),
- The Second Principle of Mathematical Induction (also called the Principle of Complete Induction, or just PCI), and

In this chapter, we will review:

- The First Principle of Mathematical Induction (also called the Principle of Mathematical Induction, or just PMI),
- The Second Principle of Mathematical Induction (also called the Principle of Complete Induction, or just PCI), and
- The Principle of Well-Ordering (also called the Well-Ordering Principle).

In this chapter, we will review:

- The First Principle of Mathematical Induction (also called the Principle of Mathematical Induction, or just PMI),
- The Second Principle of Mathematical Induction (also called the Principle of Complete Induction, or just PCI), and
- The Principle of Well-Ordering (also called the Well-Ordering Principle).

We will also introduce:

In this chapter, we will review:

- The First Principle of Mathematical Induction (also called the Principle of Mathematical Induction, or just PMI),
- The Second Principle of Mathematical Induction (also called the Principle of Complete Induction, or just PCI), and
- The Principle of Well-Ordering (also called the Well-Ordering Principle).

We will also introduce:

- The Division Algorithm,

In this chapter, we will review:

- The First Principle of Mathematical Induction (also called the Principle of Mathematical Induction, or just PMI),
- The Second Principle of Mathematical Induction (also called the Principle of Complete Induction, or just PCI), and
- The Principle of Well-Ordering (also called the Well-Ordering Principle).

We will also introduce:

- The Division Algorithm,
- The concept of greatest common divisor (abbreviated gcd),

In this chapter, we will review:

- The First Principle of Mathematical Induction (also called the Principle of Mathematical Induction, or just PMI),
- The Second Principle of Mathematical Induction (also called the Principle of Complete Induction, or just PCI), and
- The Principle of Well-Ordering (also called the Well-Ordering Principle).

We will also introduce:

- The Division Algorithm,
- The concept of greatest common divisor (abbreviated gcd),
- The Euclidean Algorithm, and

In this chapter, we will review:

- The First Principle of Mathematical Induction (also called the Principle of Mathematical Induction, or just PMI),
- The Second Principle of Mathematical Induction (also called the Principle of Complete Induction, or just PCI), and
- The Principle of Well-Ordering (also called the Well-Ordering Principle).

We will also introduce:

- The Division Algorithm,
- The concept of greatest common divisor (abbreviated gcd),
- The Euclidean Algorithm, and
- The Fundamental Theorem of Arithmetic.

Recall

Recall

- A proposition (or statement) is a sentence that can be determined to be either true or false but not both.

Recall

- A proposition (or statement) is a sentence that can be determined to be either true or false but not both.

  For example, "For all $x \in \mathbb{N}, x^2 - 1 = 0$" is a proposition, which happens to be false.

Recall

- A proposition (or statement) is a sentence that can be determined to be either true or false but not both.

  For example, "For all $x \in \mathbb{N}, x^2 - 1 = 0$" is a proposition, which happens to be false.

- An open sentence with variable x (and possibly more variables) is a sentence whose truth value depends on the value of the variable.

Recall

- A proposition (or statement) is a sentence that can be determined to be either true or false but not both.

  For example, "For all $x \in \mathbb{N}, x^2 - 1 = 0$" is a proposition, which happens to be false.

- An open sentence with variable x (and possibly more variables) is a sentence whose truth value depends on the value of the variable.

  For example, "$x^2 - 1 = 0$" is an open sentence (and *not* a proposition) since its truth value depends on x.

Recall

- A proposition (or statement) is a sentence that can be determined to be either true or false but not both.

  For example, "For all $x \in \mathbb{N}, x^2 - 1 = 0$" is a proposition, which happens to be false.

- An open sentence with variable x (and possibly more variables) is a sentence whose truth value depends on the value of the variable.

  For example, "$x^2 - 1 = 0$" is an open sentence (and *not* a proposition) since its truth value depends on x.

- We may denote an open sentence by things like $S(x)$.

Recall

- A proposition (or statement) is a sentence that can be determined to be either true or false but not both.

  For example, "For all $x \in \mathbb{N}, x^2 - 1 = 0$" is a proposition, which happens to be false.

- An open sentence with variable x (and possibly more variables) is a sentence whose truth value depends on the value of the variable.

  For example, "$x^2 - 1 = 0$" is an open sentence (and *not* a proposition) since its truth value depends on x.

- We may denote an open sentence by things like $S(x)$. For example, let $S(x)$ be the open sentence "$x^2 - 1 = 0$".

Recall

- A proposition (or statement) is a sentence that can be determined to be either true or false but not both.

  For example, "For all $x \in \mathbb{N}, x^2 - 1 = 0$" is a proposition, which happens to be false.

- An open sentence with variable x (and possibly more variables) is a sentence whose truth value depends on the value of the variable.

  For example, "$x^2 - 1 = 0$" is an open sentence (and *not* a proposition) since its truth value depends on x.

- We may denote an open sentence by things like $S(x)$. For example, let $S(x)$ be the open sentence "$x^2 - 1 = 0$".

- *Warning*: Writing things like $S(x) = x^2 - 1 = 0$ is BAD!

Recall

- A proposition (or statement) is a sentence that can be determined to be either true or false but not both.

  For example, "For all $x \in \mathbb{N}, x^2 - 1 = 0$" is a proposition, which happens to be false.

- An open sentence with variable x (and possibly more variables) is a sentence whose truth value depends on the value of the variable.

  For example, "$x^2 - 1 = 0$" is an open sentence (and *not* a proposition) since its truth value depends on x.

- We may denote an open sentence by things like $S(x)$. For example, let $S(x)$ be the open sentence "$x^2 - 1 = 0$".
- *Warning*: Writing things like $S(x) = x^2 - 1 = 0$ is BAD!
- Quantifying ("for all" and "there exists... such that") all of the variables of an open sentence always results in a proposition.

Recall

Recall

- The set of integers is given by

Recall

- The set of integers is given by $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.

Recall

- The set of integers is given by $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.
- The set of natural numbers is given by

Recall

- The set of integers is given by$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.
- The set of natural numbers is given by $\mathbb{N} = \{1, 2, 3, \ldots\}$.

Recall

- The set of integers is given by$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.
- The set of natural numbers is given by $\mathbb{N} = \{1, 2, 3, \ldots\}$.
- Mathematical induction is useful for proving propositions of the form "For all $n \in \mathbb{N}$, $S(n)$," where $S(n)$ is some open sentence.

Recall

- The set of integers is given by $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.
- The set of natural numbers is given by $\mathbb{N} = \{1, 2, 3, \ldots\}$.
- Mathematical induction is useful for proving propositions of the form "For all $n \in \mathbb{N}$, $S(n)$," where $S(n)$ is some open sentence.

First Principle of Mathematical Induction

Recall

- The set of integers is given by$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.
- The set of natural numbers is given by $\mathbb{N} = \{1, 2, 3, \ldots\}$.
- Mathematical induction is useful for proving propositions of the form "For all $n \in \mathbb{N}$, $S(n)$," where $S(n)$ is some open sentence.

First Principle of Mathematical Induction

Suppose $S(n)$ is an open sentence.

Recall

- The set of integers is given by$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$.
- The set of natural numbers is given by $\mathbb{N} = \{1, 2, 3, \dots\}$.
- Mathematical induction is useful for proving propositions of the form "For all $n \in \mathbb{N}$, $S(n)$," where $S(n)$ is some open sentence.

First Principle of Mathematical Induction

Suppose $S(n)$ is an open sentence. If

(i) $S(n_0)$ is true for some $n_0 \in \mathbb{N}$, and

Recall

- The set of integers is given by$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.
- The set of natural numbers is given by $\mathbb{N} = \{1, 2, 3, \ldots\}$.
- Mathematical induction is useful for proving propositions of the form "For all $n \in \mathbb{N}$, $S(n)$," where $S(n)$ is some open sentence.

First Principle of Mathematical Induction

Suppose $S(n)$ is an open sentence. If

(i) $S(n_0)$ is true for some $n_0 \in \mathbb{N}$, and

(ii) for all $k \geq n_0$, $S(k)$ implies $S(k+1)$ is true,

Recall

- The set of integers is given by$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.
- The set of natural numbers is given by $\mathbb{N} = \{1, 2, 3, \ldots\}$.
- Mathematical induction is useful for proving propositions of the form "For all $n \in \mathbb{N}$, $S(n)$," where $S(n)$ is some open sentence.

First Principle of Mathematical Induction

Suppose $S(n)$ is an open sentence. If

(i) $S(n_0)$ is true for some $n_0 \in \mathbb{N}$, and

(ii) for all $k \geq n_0$, $S(k)$ implies $S(k+1)$ is true,

then $S(n)$ is true for all natural numbers $n \geq n_0$.

Recall

- The set of integers is given by$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.
- The set of natural numbers is given by $\mathbb{N} = \{1, 2, 3, \ldots\}$.
- Mathematical induction is useful for proving propositions of the form "For all $n \in \mathbb{N}$, $S(n)$," where $S(n)$ is some open sentence.

First Principle of Mathematical Induction

Suppose $S(n)$ is an open sentence. If

(i) $S(n_0)$ is true for some $n_0 \in \mathbb{N}$, and

(ii) for all $k \geq n_0$, $S(k)$ implies $S(k+1)$ is true,

then $S(n)$ is true for all natural numbers $n \geq n_0$.

In particular, if $n_0 = 1$, then $S(n)$ is true for all $n \in \mathbb{N}$. That is, the statement "For all $n \in \mathbb{N}$, $S(n)$" is true.

Proposition

Proposition

For all $n \in \mathbb{N}$,

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Proposition

For all $n \in \mathbb{N}$,

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Proof.

Proposition

For all $n \in \mathbb{N}$,

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Proof.

We will proceed by induction.

Proposition

For all $n \in \mathbb{N}$,

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Proof.

We will proceed by induction.

Base case:

Proposition

For all $n \in \mathbb{N}$,

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Proof.

We will proceed by induction.

Base case: We see that when $n = 1$, $\sum_{i=1}^{n} i = 1$, and on the other hand,

Proposition

For all $n \in \mathbb{N}$,

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Proof.

We will proceed by induction.

Base case: We see that when $n = 1$, $\sum_{i=1}^{n} i = 1$, and on the other hand,

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

Proposition

For all $n \in \mathbb{N}$*,*

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Proof.

We will proceed by induction.

Base case: We see that when $n = 1$, $\sum_{i=1}^{n} i = 1$, and on the other hand,

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

which verifies the base case.

Proposition

For all $n \in \mathbb{N}$,

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Proof.

We will proceed by induction.

Base case: We see that when $n = 1$, $\sum_{i=1}^{n} i = 1$, and on the other hand,

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

which verifies the base case.

Inductive step:

Proposition

For all $n \in \mathbb{N}$,

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Proof.

We will proceed by induction.

Base case: We see that when $n = 1$, $\sum_{i=1}^{n} i = 1$, and on the other hand,

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

which verifies the base case.

Inductive step: Let $k \in \mathbb{N}$ and suppose that

$$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}.$$

Proof (continued).

Proof (continued).

We see that

Proof (continued).

We see that

$$\sum_{i=1}^{k+1} i = \left(\sum_{i=1}^{k} i\right) + (k+1)$$

□

Proof (continued).

We see that

$$\begin{aligned}\sum_{i=1}^{k+1} i &= \left(\sum_{i=1}^{k} i\right) + (k+1) \\ &= \frac{k(k+1)}{2} + k + 1 && \text{(by inductive hypothesis)}\end{aligned}$$

$\square$

Proof (continued).

We see that

$$\begin{aligned}
\sum_{i=1}^{k+1} i &= \left(\sum_{i=1}^{k} i\right) + (k+1) \\
&= \frac{k(k+1)}{2} + k + 1 && \text{(by inductive hypothesis)} \\
&= \frac{k(k+1) + 2(k+1)}{2}
\end{aligned}$$

$\square$

Proof (continued).

We see that

$$\begin{aligned}
\sum_{i=1}^{k+1} i &= \left(\sum_{i=1}^{k} i\right) + (k+1) \\
&= \frac{k(k+1)}{2} + k + 1 && \text{(by inductive hypothesis)} \\
&= \frac{k(k+1) + 2(k+1)}{2} \\
&= \frac{(k+1)(k+2)}{2}
\end{aligned}$$

$\square$

Proof (continued).

We see that

$$\begin{aligned}
\sum_{i=1}^{k+1} i &= \left(\sum_{i=1}^{k} i\right) + (k+1) \\
&= \frac{k(k+1)}{2} + k + 1 && \text{(by inductive hypothesis)} \\
&= \frac{k(k+1) + 2(k+1)}{2} \\
&= \frac{(k+1)(k+2)}{2} \\
&= \frac{(k+1)((k+1)+1)}{2}.
\end{aligned}$$

$\square$

Proof (continued).

We see that

$$\begin{aligned}
\sum_{i=1}^{k+1} i &= \left(\sum_{i=1}^{k} i\right) + (k+1) \\
&= \frac{k(k+1)}{2} + k + 1 && \text{(by inductive hypothesis)} \\
&= \frac{k(k+1) + 2(k+1)}{2} \\
&= \frac{(k+1)(k+2)}{2} \\
&= \frac{(k+1)((k+1)+1)}{2}.
\end{aligned}$$

Thus, the formula is true for $k+1$. □

Proof (continued).

We see that

$$\begin{aligned}
\sum_{i=1}^{k+1} i &= \left(\sum_{i=1}^{k} i\right) + (k+1) \\
&= \frac{k(k+1)}{2} + k + 1 && \text{(by inductive hypothesis)} \\
&= \frac{k(k+1) + 2(k+1)}{2} \\
&= \frac{(k+1)(k+2)}{2} \\
&= \frac{(k+1)((k+1)+1)}{2}.
\end{aligned}$$

Thus, the formula is true for $k+1$.

Therefore, by induction, the formula is true for all $n \in \mathbb{N}$. $\square$

Second Principle of Mathematical Induction

Second Principle of Mathematical Induction

Suppose $S(n)$ is an open sentence.

Second Principle of Mathematical Induction

Suppose $S(n)$ is an open sentence. If

(i) $S(n_0)$ is true for some $n_0 \in \mathbb{N}$, and

Second Principle of Mathematical Induction

Suppose $S(n)$ is an open sentence. If

(i) $S(n_0)$ is true for some $n_0 \in \mathbb{N}$, and

(ii) for all $k \geq n_0$, $S(n_0), S(n_1), \ldots, S(k)$ implies $S(k+1)$ is true,

Second Principle of Mathematical Induction

Suppose $S(n)$ is an open sentence. If

(i) $S(n_0)$ is true for some $n_0 \in \mathbb{N}$, and

(ii) for all $k \geq n_0$, $S(n_0), S(n_1), \ldots, S(k)$ implies $S(k+1)$ is true,

then $S(n)$ is true for all natural numbers $n \geq n_0$.

Second Principle of Mathematical Induction

Suppose $S(n)$ is an open sentence. If

(i) $S(n_0)$ is true for some $n_0 \in \mathbb{N}$, and

(ii) for all $k \geq n_0$, $S(n_0), S(n_1), \ldots, S(k)$ implies $S(k+1)$ is true,

then $S(n)$ is true for all natural numbers $n \geq n_0$.

In particular, if $n_0 = 1$, then $S(n)$ is true for all $n \in \mathbb{N}$. That is, the statement "For all $n \in \mathbb{N}$, $S(n)$" is true.

Second Principle of Mathematical Induction

Suppose $S(n)$ is an open sentence. If

(i) $S(n_0)$ is true for some $n_0 \in \mathbb{N}$, and

(ii) for all $k \geq n_0$, $S(n_0), S(n_1), \ldots, S(k)$ implies $S(k+1)$ is true,

then $S(n)$ is true for all natural numbers $n \geq n_0$.

In particular, if $n_0 = 1$, then $S(n)$ is true for all $n \in \mathbb{N}$. That is, the statement "For all $n \in \mathbb{N}$, $S(n)$" is true.

Note

Second Principle of Mathematical Induction

Suppose $S(n)$ is an open sentence. If

(i) $S(n_0)$ is true for some $n_0 \in \mathbb{N}$, and

(ii) for all $k \geq n_0$, $S(n_0), S(n_1), \ldots, S(k)$ implies $S(k+1)$ is true,

then $S(n)$ is true for all natural numbers $n \geq n_0$.

In particular, if $n_0 = 1$, then $S(n)$ is true for all $n \in \mathbb{N}$. That is, the statement "For all $n \in \mathbb{N}$, $S(n)$" is true.

Note

The second principle of mathematical induction is sometimes called strong induction since you make a much stronger assumption during the induction step.

Second Principle of Mathematical Induction

Suppose $S(n)$ is an open sentence. If

(i) $S(n_0)$ is true for some $n_0 \in \mathbb{N}$, and

(ii) for all $k \geq n_0$, $S(n_0), S(n_1), \ldots, S(k)$ implies $S(k+1)$ is true,

then $S(n)$ is true for all natural numbers $n \geq n_0$.

In particular, if $n_0 = 1$, then $S(n)$ is true for all $n \in \mathbb{N}$. That is, the statement "For all $n \in \mathbb{N}$, $S(n)$" is true.

Note

The second principle of mathematical induction is sometimes called strong induction since you make a much stronger assumption during the induction step. Strong induction is useful when you need to "reach back" farther than one step during the inductive step.

Second Principle of Mathematical Induction

Suppose $S(n)$ is an open sentence. If

(i) $S(n_0)$ is true for some $n_0 \in \mathbb{N}$, and

(ii) for all $k \geq n_0$, $S(n_0), S(n_1), \ldots, S(k)$ implies $S(k+1)$ is true,

then $S(n)$ is true for all natural numbers $n \geq n_0$.

In particular, if $n_0 = 1$, then $S(n)$ is true for all $n \in \mathbb{N}$. That is, the statement "For all $n \in \mathbb{N}$, $S(n)$" is true.

Note

The second principle of mathematical induction is sometimes called strong induction since you make a much stronger assumption during the induction step. Strong induction is useful when you need to "reach back" farther than one step during the inductive step.

Claim

Second Principle of Mathematical Induction

Suppose $S(n)$ is an open sentence. If

(i) $S(n_0)$ is true for some $n_0 \in \mathbb{N}$, and

(ii) for all $k \geq n_0$, $S(n_0), S(n_1), \ldots, S(k)$ implies $S(k+1)$ is true,

then $S(n)$ is true for all natural numbers $n \geq n_0$.

In particular, if $n_0 = 1$, then $S(n)$ is true for all $n \in \mathbb{N}$. That is, the statement "For all $n \in \mathbb{N}$, $S(n)$" is true.

Note

The second principle of mathematical induction is sometimes called strong induction since you make a much stronger assumption during the induction step. Strong induction is useful when you need to "reach back" farther than one step during the inductive step.

Claim

The first and second principles of mathematical induction are equivalent.

Definition

Definition

A nonempty subset $S \subseteq \mathbb{Z}$ is well-ordered if it contains a least element.

Definition

A nonempty subset $S \subseteq \mathbb{Z}$ is well-ordered if it contains a least element.

Example

Definition

A nonempty subset $S \subseteq \mathbb{Z}$ is well-ordered if it contains a least element.

Example

Notice that the integers themselves are not well-ordered.

Definition

A nonempty subset $S \subseteq \mathbb{Z}$ is well-ordered if it contains a least element.

Example

Notice that the integers themselves are not well-ordered. However, the natural numbers $\mathbb{N}$ are well-ordered.

Definition

A nonempty subset $S \subseteq \mathbb{Z}$ is well-ordered if it contains a least element.

Example

Notice that the integers themselves are not well-ordered. However, the natural numbers $\mathbb{N}$ are well-ordered. In fact, we have the following.

Definition

A nonempty subset $S \subseteq \mathbb{Z}$ is well-ordered if it contains a least element.

Example

Notice that the integers themselves are not well-ordered. However, the natural numbers $\mathbb{N}$ are well-ordered. In fact, we have the following.

Principle of Well-Ordering

Definition

A nonempty subset $S \subseteq \mathbb{Z}$ is well-ordered if it contains a least element.

Example

Notice that the integers themselves are not well-ordered. However, the natural numbers $\mathbb{N}$ are well-ordered. In fact, we have the following.

Principle of Well-Ordering

Every nonempty subset of the natural numbers is well-ordered.

Definition

A nonempty subset $S \subseteq \mathbb{Z}$ is well-ordered if it contains a least element.

Example

Notice that the integers themselves are not well-ordered. However, the natural numbers $\mathbb{N}$ are well-ordered. In fact, we have the following.

Principle of Well-Ordering

Every nonempty subset of the natural numbers is well-ordered.

It turns out that the Principle of Well-Ordering is equivalent to the PMI.

Definition

A nonempty subset $S \subseteq \mathbb{Z}$ is well-ordered if it contains a least element.

Example

Notice that the integers themselves are not well-ordered. However, the natural numbers $\mathbb{N}$ are well-ordered. In fact, we have the following.

Principle of Well-Ordering

Every nonempty subset of the natural numbers is well-ordered.

It turns out that the Principle of Well-Ordering is equivalent to the PMI. We will prove that the PMI implies the Principle of Well-Ordering.

Definition

A nonempty subset $S \subseteq \mathbb{Z}$ is well-ordered if it contains a least element.

Example

Notice that the integers themselves are not well-ordered. However, the natural numbers $\mathbb{N}$ are well-ordered. In fact, we have the following.

Principle of Well-Ordering

Every nonempty subset of the natural numbers is well-ordered.

It turns out that the Principle of Well-Ordering is equivalent to the PMI. We will prove that the PMI implies the Principle of Well-Ordering.

Lemma 1.1

Definition
A nonempty subset $S \subseteq \mathbb{Z}$ is well-ordered if it contains a least element.

Example
Notice that the integers themselves are not well-ordered. However, the natural numbers $\mathbb{N}$ are well-ordered. In fact, we have the following.

Principle of Well-Ordering
Every nonempty subset of the natural numbers is well-ordered.

It turns out that the Principle of Well-Ordering is equivalent to the PMI. We will prove that the PMI implies the Principle of Well-Ordering.

Lemma 1.1
The PMI implies that 1 is the smallest natural number.

Definition
A nonempty subset $S \subseteq \mathbb{Z}$ is well-ordered if it contains a least element.

Example
Notice that the integers themselves are not well-ordered. However, the natural numbers $\mathbb{N}$ are well-ordered. In fact, we have the following.

Principle of Well-Ordering
Every nonempty subset of the natural numbers is well-ordered.

It turns out that the Principle of Well-Ordering is equivalent to the PMI. We will prove that the PMI implies the Principle of Well-Ordering.

Lemma 1.1
The PMI implies that 1 is the smallest natural number.

Proof.
Let $S = \{n \in \mathbb{N} : n \geq 1\}$.

Definition

A nonempty subset $S \subseteq \mathbb{Z}$ is well-ordered if it contains a least element.

Example

Notice that the integers themselves are not well-ordered. However, the natural numbers $\mathbb{N}$ are well-ordered. In fact, we have the following.

Principle of Well-Ordering

Every nonempty subset of the natural numbers is well-ordered.

It turns out that the Principle of Well-Ordering is equivalent to the PMI. We will prove that the PMI implies the Principle of Well-Ordering.

Lemma 1.1

The PMI implies that 1 is the smallest natural number.

Proof.

Let $S = \{n \in \mathbb{N} : n \geq 1\}$. Then $1 \in S$ (base case).

Definition

A nonempty subset $S \subseteq \mathbb{Z}$ is well-ordered if it contains a least element.

Example

Notice that the integers themselves are not well-ordered. However, the natural numbers $\mathbb{N}$ are well-ordered. In fact, we have the following.

Principle of Well-Ordering

Every nonempty subset of the natural numbers is well-ordered.

It turns out that the Principle of Well-Ordering is equivalent to the PMI. We will prove that the PMI implies the Principle of Well-Ordering.

Lemma 1.1

The PMI implies that 1 is the smallest natural number.

Proof.

Let $S = \{n \in \mathbb{N} : n \geq 1\}$. Then $1 \in S$ (base case). Next, assume that $n \in S$ (so that $n \geq 1$).

Definition

A nonempty subset $S \subseteq \mathbb{Z}$ is well-ordered if it contains a least element.

Example

Notice that the integers themselves are not well-ordered. However, the natural numbers $\mathbb{N}$ are well-ordered. In fact, we have the following.

Principle of Well-Ordering

Every nonempty subset of the natural numbers is well-ordered.

It turns out that the Principle of Well-Ordering is equivalent to the PMI. We will prove that the PMI implies the Principle of Well-Ordering.

Lemma 1.1

The PMI implies that 1 is the smallest natural number.

Proof.

Let $S = \{n \in \mathbb{N} : n \geq 1\}$. Then $1 \in S$ (base case). Next, assume that $n \in S$ (so that $n \geq 1$). Since $n + 1 \geq 1$,

Definition

A nonempty subset $S \subseteq \mathbb{Z}$ is well-ordered if it contains a least element.

Example

Notice that the integers themselves are not well-ordered. However, the natural numbers $\mathbb{N}$ are well-ordered. In fact, we have the following.

Principle of Well-Ordering

Every nonempty subset of the natural numbers is well-ordered.

It turns out that the Principle of Well-Ordering is equivalent to the PMI. We will prove that the PMI implies the Principle of Well-Ordering.

Lemma 1.1

The PMI implies that 1 is the smallest natural number.

Proof.

Let $S = \{n \in \mathbb{N} : n \geq 1\}$. Then $1 \in S$ (base case). Next, assume that $n \in S$ (so that $n \geq 1$). Since $n + 1 \geq 1$, $n + 1 \in S$, as well (inductive step).

Definition
A nonempty subset $S \subseteq \mathbb{Z}$ is well-ordered if it contains a least element.

Example
Notice that the integers themselves are not well-ordered. However, the natural numbers $\mathbb{N}$ are well-ordered. In fact, we have the following.

Principle of Well-Ordering
Every nonempty subset of the natural numbers is well-ordered.

It turns out that the Principle of Well-Ordering is equivalent to the PMI. We will prove that the PMI implies the Principle of Well-Ordering.

Lemma 1.1
The PMI implies that 1 is the smallest natural number.

Proof.
Let $S = \{n \in \mathbb{N} : n \geq 1\}$. Then $1 \in S$ (base case). Next, assume that $n \in S$ (so that $n \geq 1$). Since $n+1 \geq 1$, $n+1 \in S$, as well (inductive step). By induction, every natural number is greater than or equal to 1. □

Theorem 1.2

Theorem 1.2
The PMI implies that $\mathbb{N}$ is well-ordered.

Theorem 1.2

The PMI implies that $\mathbb{N}$ is well-ordered.

Proof.

Theorem 1.2

The PMI implies that $\mathbb{N}$ is well-ordered.

Proof.

Suppose T is a nonempty subset of $\mathbb{N}$.

Theorem 1.2
The PMI implies that $\mathbb{N}$ is well-ordered.

Proof.
Suppose T is a nonempty subset of $\mathbb{N}$. Let $S = \mathbb{N} \setminus T$.

Theorem 1.2

The PMI implies that $\mathbb{N}$ is well-ordered.

Proof.

Suppose T is a nonempty subset of $\mathbb{N}$. Let $S = \mathbb{N} \setminus T$. Since $T \neq \emptyset$, $S \neq \mathbb{N}$.

Theorem 1.2

The PMI implies that $\mathbb{N}$ is well-ordered.

Proof.

Suppose T is a nonempty subset of $\mathbb{N}$. Let $S = \mathbb{N} \setminus T$. Since $T \neq \emptyset$, $S \neq \mathbb{N}$. For sake of a contradiction, assume that T has no smallest element.

Theorem 1.2
The PMI implies that $\mathbb{N}$ is well-ordered.

Proof.
Suppose T is a nonempty subset of $\mathbb{N}$. Let $S = \mathbb{N} \setminus T$. Since $T \neq \emptyset$, $S \neq \mathbb{N}$. For sake of a contradiction, assume that T has no smallest element. We will show that $S = \mathbb{N}$ by induction.

Theorem 1.2

The PMI implies that $\mathbb{N}$ is well-ordered.

Proof.

Suppose T is a nonempty subset of $\mathbb{N}$. Let $S = \mathbb{N} \setminus T$. Since $T \neq \emptyset$, $S \neq \mathbb{N}$. For sake of a contradiction, assume that T has no smallest element. We will show that $S = \mathbb{N}$ by induction.

Base case:

Theorem 1.2

The PMI implies that $\mathbb{N}$ is well-ordered.

Proof.

Suppose T is a nonempty subset of $\mathbb{N}$. Let $S = \mathbb{N} \setminus T$. Since $T \neq \emptyset$, $S \neq \mathbb{N}$. For sake of a contradiction, assume that T has no smallest element. We will show that $S = \mathbb{N}$ by induction.

Base case: Since 1 is the smallest element of $\mathbb{N}$ (by Lemma 1.1)

Theorem 1.2

The PMI implies that $\mathbb{N}$ is well-ordered.

Proof.

Suppose T is a nonempty subset of $\mathbb{N}$. Let $S = \mathbb{N} \setminus T$. Since $T \neq \emptyset$, $S \neq \mathbb{N}$. For sake of a contradiction, assume that T has no smallest element. We will show that $S = \mathbb{N}$ by induction.

Base case: Since 1 is the smallest element of $\mathbb{N}$ (by Lemma 1.1) and T has no smallest element,

Theorem 1.2

The PMI implies that $\mathbb{N}$ is well-ordered.

Proof.

Suppose T is a nonempty subset of $\mathbb{N}$. Let $S = \mathbb{N} \setminus T$. Since $T \neq \emptyset$, $S \neq \mathbb{N}$. For sake of a contradiction, assume that T has no smallest element. We will show that $S = \mathbb{N}$ by induction.

Base case: Since 1 is the smallest element of $\mathbb{N}$ (by Lemma 1.1) and T has no smallest element, $1 \neq T$.

Theorem 1.2

The PMI implies that $\mathbb{N}$ is well-ordered.

Proof.

Suppose T is a nonempty subset of $\mathbb{N}$. Let $S = \mathbb{N} \setminus T$. Since $T \neq \emptyset$, $S \neq \mathbb{N}$. For sake of a contradiction, assume that T has no smallest element. We will show that $S = \mathbb{N}$ by induction.

Base case: Since 1 is the smallest element of $\mathbb{N}$ (by Lemma 1.1) and T has no smallest element, $1 \neq T$. Therefore, $1 \in S$.

Theorem 1.2

The PMI implies that $\mathbb{N}$ is well-ordered.

Proof.

Suppose T is a nonempty subset of $\mathbb{N}$. Let $S = \mathbb{N} \setminus T$. Since $T \neq \emptyset$, $S \neq \mathbb{N}$. For sake of a contradiction, assume that T has no smallest element. We will show that $S = \mathbb{N}$ by induction.

Base case: Since 1 is the smallest element of $\mathbb{N}$ (by Lemma 1.1) and T has no smallest element, $1 \neq T$. Therefore, $1 \in S$.

Inductive step:

Theorem 1.2

The PMI implies that $\mathbb{N}$ is well-ordered.

Proof.

Suppose T is a nonempty subset of $\mathbb{N}$. Let $S = \mathbb{N} \setminus T$. Since $T \neq \emptyset$, $S \neq \mathbb{N}$. For sake of a contradiction, assume that T has no smallest element. We will show that $S = \mathbb{N}$ by induction.

Base case: Since 1 is the smallest element of $\mathbb{N}$ (by Lemma 1.1) and T has no smallest element, $1 \neq T$. Therefore, $1 \in S$.

Inductive step: Suppose $k \in S$.

Theorem 1.2

The PMI implies that $\mathbb{N}$ is well-ordered.

Proof.

Suppose T is a nonempty subset of $\mathbb{N}$. Let $S = \mathbb{N} \setminus T$. Since $T \neq \emptyset$, $S \neq \mathbb{N}$. For sake of a contradiction, assume that T has no smallest element. We will show that $S = \mathbb{N}$ by induction.

Base case: Since 1 is the smallest element of $\mathbb{N}$ (by Lemma 1.1) and T has no smallest element, $1 \neq T$. Therefore, $1 \in S$.

Inductive step: Suppose $k \in S$. Since T has no least element, $1, 2, \ldots, k-1 \notin T$, otherwise one of these numbers would be the smallest in T.

Theorem 1.2

The PMI implies that $\mathbb{N}$ is well-ordered.

Proof.

Suppose T is a nonempty subset of $\mathbb{N}$. Let $S = \mathbb{N} \setminus T$. Since $T \neq \emptyset$, $S \neq \mathbb{N}$. For sake of a contradiction, assume that T has no smallest element. We will show that $S = \mathbb{N}$ by induction.

Base case: Since 1 is the smallest element of $\mathbb{N}$ (by Lemma 1.1) and T has no smallest element, $1 \neq T$. Therefore, $1 \in S$.

Inductive step: Suppose $k \in S$. Since T has no least element, $1, 2, \ldots, k-1 \notin T$, otherwise one of these numbers would be the smallest in T. We know $k \notin T$ since $k \in S$.

Theorem 1.2

The PMI implies that $\mathbb{N}$ is well-ordered.

Proof.

Suppose T is a nonempty subset of $\mathbb{N}$. Let $S = \mathbb{N} \setminus T$. Since $T \neq \emptyset$, $S \neq \mathbb{N}$. For sake of a contradiction, assume that T has no smallest element. We will show that $S = \mathbb{N}$ by induction.

Base case: Since 1 is the smallest element of $\mathbb{N}$ (by Lemma 1.1) and T has no smallest element, $1 \neq T$. Therefore, $1 \in S$.

Inductive step: Suppose $k \in S$. Since T has no least element, $1, 2, \ldots, k-1 \notin T$, otherwise one of these numbers would be the smallest in T. We know $k \notin T$ since $k \in S$. Therefore, $k+1 \notin T$ either, or else it would be the smallest element of T.

Theorem 1.2

The PMI implies that $\mathbb{N}$ is well-ordered.

Proof.

Suppose T is a nonempty subset of $\mathbb{N}$. Let $S = \mathbb{N} \setminus T$. Since $T \neq \emptyset$, $S \neq \mathbb{N}$. For sake of a contradiction, assume that T has no smallest element. We will show that $S = \mathbb{N}$ by induction.

Base case: Since 1 is the smallest element of $\mathbb{N}$ (by Lemma 1.1) and T has no smallest element, $1 \neq T$. Therefore, $1 \in S$.

Inductive step: Suppose $k \in S$. Since T has no least element, $1, 2, \ldots, k-1 \notin T$, otherwise one of these numbers would be the smallest in T. We know $k \notin T$ since $k \in S$. Therefore, $k+1 \notin T$ either, or else it would be the smallest element of T. So, $k+1 \in S$.

By induction, $S = \mathbb{N}$.

PMI implies the Principle of Well-Ordering

Theorem 1.2

The PMI implies that $\mathbb{N}$ is well-ordered.

Proof.

Suppose T is a nonempty subset of $\mathbb{N}$. Let $S = \mathbb{N} \setminus T$. Since $T \neq \emptyset$, $S \neq \mathbb{N}$. For sake of a contradiction, assume that T has no smallest element. We will show that $S = \mathbb{N}$ by induction.

Base case: Since 1 is the smallest element of $\mathbb{N}$ (by Lemma 1.1) and T has no smallest element, $1 \neq T$. Therefore, $1 \in S$.

Inductive step: Suppose $k \in S$. Since T has no least element, $1, 2, \ldots, k-1 \notin T$, otherwise one of these numbers would be the smallest in T. We know $k \notin T$ since $k \in S$. Therefore, $k+1 \notin T$ either, or else it would be the smallest element of T. So, $k+1 \in S$.

By induction, $S = \mathbb{N}$. This implies that T is empty, which is a contradiction, and hence, we have our desired result.

$\square$

Here is an application of the Principle of Well-Ordering that we will occasionally make use of.

Here is an application of the Principle of Well-Ordering that we will occasionally make use of.

Theorem 1.3 (Division Algorithm)

Here is an application of the Principle of Well-Ordering that we will occasionally make use of.

Theorem 1.3 (Division Algorithm)

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

Here is an application of the Principle of Well-Ordering that we will occasionally make use of.

Theorem 1.3 (Division Algorithm)

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists unique integers q and r such that

Here is an application of the Principle of Well-Ordering that we will occasionally make use of.

Theorem 1.3 (Division Algorithm)

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists unique integers q and r such that

$$a = bq + r,$$

Here is an application of the Principle of Well-Ordering that we will occasionally make use of.

Theorem 1.3 (Division Algorithm)

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists unique integers q and r such that

$$a = bq + r,$$

where $0 \leq r < b$.

Here is an application of the Principle of Well-Ordering that we will occasionally make use of.

Theorem 1.3 (Division Algorithm)

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists unique integers q and r such that

$$a = bq + r,$$

where $0 \leq r < b$.

(*Note*: We regard r as the remainder and q as the quotient.)

Here is an application of the Principle of Well-Ordering that we will occasionally make use of.

Theorem 1.3 (Division Algorithm)

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists unique integers q and r such that

$$a = bq + r,$$

where $0 \leq r < b$.

(*Note*: We regard r as the remainder and q as the quotient.)

Proof.

Here is an application of the Principle of Well-Ordering that we will occasionally make use of.

Theorem 1.3 (Division Algorithm)

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists unique integers q and r such that

$$a = bq + r,$$

where $0 \leq r < b$.

(*Note*: We regard r as the remainder and q as the quotient.)

Proof.

This proof has two halves.

Here is an application of the Principle of Well-Ordering that we will occasionally make use of.

Theorem 1.3 (Division Algorithm)

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists unique integers q and r such that

$$a = bq + r,$$

where $0 \leq r < b$.

(*Note*: We regard r as the remainder and q as the quotient.)

Proof.

This proof has two halves. First, we need to prove that there are integers q and r with the desired properties (existence).

Here is an application of the Principle of Well-Ordering that we will occasionally make use of.

Theorem 1.3 (Division Algorithm)

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists unique integers q and r such that

$$a = bq + r,$$

where $0 \leq r < b$.

(*Note*: We regard r as the remainder and q as the quotient.)

Proof.

This proof has two halves. First, we need to prove that there are integers q and r with the desired properties (existence). Second, we need to show that they are unique (uniqueness).

Here is an application of the Principle of Well-Ordering that we will occasionally make use of.

Theorem 1.3 (Division Algorithm)

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists unique integers q and r such that

$$a = bq + r,$$

where $0 \leq r < b$.

(*Note*: We regard r as the remainder and q as the quotient.)

Proof.

This proof has two halves. First, we need to prove that there are integers q and r with the desired properties (existence). Second, we need to show that they are unique (uniqueness).

Existence:

Here is an application of the Principle of Well-Ordering that we will occasionally make use of.

Theorem 1.3 (Division Algorithm)

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists unique integers q and r such that

$$a = bq + r,$$

where $0 \leq r < b$.

(*Note*: We regard r as the remainder and q as the quotient.)

Proof.

This proof has two halves. First, we need to prove that there are integers q and r with the desired properties (existence). Second, we need to show that they are unique (uniqueness).

Existence: Define the set

Here is an application of the Principle of Well-Ordering that we will occasionally make use of.

Theorem 1.3 (Division Algorithm)

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists unique integers q and r such that

$$a = bq + r,$$

where $0 \leq r < b$.

(*Note*: We regard r as the remainder and q as the quotient.)

Proof.

This proof has two halves. First, we need to prove that there are integers q and r with the desired properties (existence). Second, we need to show that they are unique (uniqueness).

Existence: Define the set

$$S = \{a - bk : k \in \mathbb{Z} \text{ and } a - bk \geq 0\}.$$

Here is an application of the Principle of Well-Ordering that we will occasionally make use of.

Theorem 1.3 (Division Algorithm)

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists unique integers q and r such that

$$a = bq + r,$$

where $0 \leq r < b$.

(*Note*: We regard r as the remainder and q as the quotient.)

Proof.

This proof has two halves. First, we need to prove that there are integers q and r with the desired properties (existence). Second, we need to show that they are unique (uniqueness).

Existence: Define the set

$$S = \{a - bk : k \in \mathbb{Z} \text{ and } a - bk \geq 0\}.$$

(What the heck is this set?)

Here is an application of the Principle of Well-Ordering that we will occasionally make use of.

Theorem 1.3 (Division Algorithm)

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists unique integers q and r such that

$$a = bq + r,$$

where $0 \leq r < b$.

(*Note*: We regard r as the remainder and q as the quotient.)

Proof.

This proof has two halves. First, we need to prove that there are integers q and r with the desired properties (existence). Second, we need to show that they are unique (uniqueness).

Existence: Define the set

$$S = \{a - bk : k \in \mathbb{Z} \text{ and } a - bk \geq 0\}.$$

(What the heck is this set?) If $0 \in S$, then b divides a,

Here is an application of the Principle of Well-Ordering that we will occasionally make use of.

Theorem 1.3 (Division Algorithm)

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists unique integers q and r such that

$$a = bq + r,$$

where $0 \leq r < b$.

(*Note*: We regard r as the remainder and q as the quotient.)

Proof.

This proof has two halves. First, we need to prove that there are integers q and r with the desired properties (existence). Second, we need to show that they are unique (uniqueness).

Existence: Define the set

$$S = \{a - bk : k \in \mathbb{Z} \text{ and } a - bk \geq 0\}.$$

(What the heck is this set?) If $0 \in S$, then b divides a, in which case we can let $q = a/b$ and $r = 0$.

Here is an application of the Principle of Well-Ordering that we will occasionally make use of.

Theorem 1.3 (Division Algorithm)

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists unique integers q and r such that

$$a = bq + r,$$

where $0 \leq r < b$.

(*Note*: We regard r as the remainder and q as the quotient.)

Proof.

This proof has two halves. First, we need to prove that there are integers q and r with the desired properties (existence). Second, we need to show that they are unique (uniqueness).

Existence: Define the set

$$S = \{a - bk : k \in \mathbb{Z} \text{ and } a - bk \geq 0\}.$$

(What the heck is this set?) If $0 \in S$, then b divides a, in which case we can let $q = a/b$ and $r = 0$. Assume that $0 \notin S$.

Here is an application of the Principle of Well-Ordering that we will occasionally make use of.

Theorem 1.3 (Division Algorithm)

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists unique integers q and r such that

$$a = bq + r,$$

where $0 \leq r < b$.

(*Note*: We regard r as the remainder and q as the quotient.)

Proof.

This proof has two halves. First, we need to prove that there are integers q and r with the desired properties (existence). Second, we need to show that they are unique (uniqueness).

Existence: Define the set

$$S = \{a - bk : k \in \mathbb{Z} \text{ and } a - bk \geq 0\}.$$

(What the heck is this set?) If $0 \in S$, then b divides a, in which case we can let $q = a/b$ and $r = 0$. Assume that $0 \notin S$. We need to show that $S \neq \emptyset$ (why?).

Proof (continued).

Proof (continued).

If $a > 0$, then $a - b \cdot 0 \in S$, which shows that $S \neq \emptyset$.

Proof (continued).

If $a > 0$, then $a - b \cdot 0 \in S$, which shows that $S \neq \emptyset$. On the other hand, if $a < 0$,

Proof (continued).

If $a > 0$, then $a - b \cdot 0 \in S$, which shows that $S \neq \emptyset$. On the other hand, if $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$.

Proof (continued).

If $a > 0$, then $a - b \cdot 0 \in S$, which shows that $S \neq \emptyset$. On the other hand, if $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$. Note that the case with $a = 0$ is handled when $0 \in S$ and we are assuming that $0 \notin S$.

Proof (continued).

If $a > 0$, then $a - b \cdot 0 \in S$, which shows that $S \neq \emptyset$. On the other hand, if $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$. Note that the case with $a = 0$ is handled when $0 \in S$ and we are assuming that $0 \notin S$. So, in either case, $S \neq \emptyset$.

Proof (continued).

If $a > 0$, then $a - b \cdot 0 \in S$, which shows that $S \neq \emptyset$. On the other hand, if $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$. Note that the case with $a = 0$ is handled when $0 \in S$ and we are assuming that $0 \notin S$. So, in either case, $S \neq \emptyset$. By the Principle of Well-Ordering, S must have a smallest element, say $r = a - bq$, where $q \in \mathbb{Z}$.

Proof (continued).

If $a > 0$, then $a - b \cdot 0 \in S$, which shows that $S \neq \emptyset$. On the other hand, if $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$. Note that the case with $a = 0$ is handled when $0 \in S$ and we are assuming that $0 \notin S$. So, in either case, $S \neq \emptyset$. By the Principle of Well-Ordering, S must have a smallest element, say $r = a - bq$, where $q \in \mathbb{Z}$. Therefore, $a = bq + r$ with $r \geq 0$.

Proof (continued).

If $a > 0$, then $a - b \cdot 0 \in S$, which shows that $S \neq \emptyset$. On the other hand, if $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$. Note that the case with $a = 0$ is handled when $0 \in S$ and we are assuming that $0 \notin S$. So, in either case, $S \neq \emptyset$. By the Principle of Well-Ordering, S must have a smallest element, say $r = a - bq$, where $q \in \mathbb{Z}$. Therefore, $a = bq + r$ with $r \geq 0$. Next, we need to show that $r < b$.

Proof (continued).

If $a > 0$, then $a - b \cdot 0 \in S$, which shows that $S \neq \emptyset$. On the other hand, if $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$. Note that the case with $a = 0$ is handled when $0 \in S$ and we are assuming that $0 \notin S$. So, in either case, $S \neq \emptyset$. By the Principle of Well-Ordering, S must have a smallest element, say $r = a - bq$, where $q \in \mathbb{Z}$. Therefore, $a = bq + r$ with $r \geq 0$. Next, we need to show that $r < b$. For sake of a contradiction, assume that $b < r$.

Proof (continued).

If $a > 0$, then $a - b \cdot 0 \in S$, which shows that $S \neq \emptyset$. On the other hand, if $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$. Note that the case with $a = 0$ is handled when $0 \in S$ and we are assuming that $0 \notin S$. So, in either case, $S \neq \emptyset$. By the Principle of Well-Ordering, S must have a smallest element, say $r = a - bq$, where $q \in \mathbb{Z}$. Therefore, $a = bq + r$ with $r \geq 0$. Next, we need to show that $r < b$. For sake of a contradiction, assume that $b < r$. We see that

$$0 < r - b = a - bq - b = a - b(q + 1).$$

Proof (continued).

If $a > 0$, then $a - b \cdot 0 \in S$, which shows that $S \neq \emptyset$. On the other hand, if $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$. Note that the case with $a = 0$ is handled when $0 \in S$ and we are assuming that $0 \notin S$. So, in either case, $S \neq \emptyset$. By the Principle of Well-Ordering, S must have a smallest element, say $r = a - bq$, where $q \in \mathbb{Z}$. Therefore, $a = bq + r$ with $r \geq 0$. Next, we need to show that $r < b$. For sake of a contradiction, assume that $b < r$. We see that

$$0 < r - b = a - bq - b = a - b(q + 1).$$

Then $a - b(q + 1) \in S$.

Proof (continued).

If $a > 0$, then $a - b \cdot 0 \in S$, which shows that $S \neq \emptyset$. On the other hand, if $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$. Note that the case with $a = 0$ is handled when $0 \in S$ and we are assuming that $0 \notin S$. So, in either case, $S \neq \emptyset$. By the Principle of Well-Ordering, S must have a smallest element, say $r = a - bq$, where $q \in \mathbb{Z}$. Therefore, $a = bq + r$ with $r \geq 0$. Next, we need to show that $r < b$. For sake of a contradiction, assume that $b < r$. We see that

$$0 < r - b = a - bq - b = a - b(q + 1).$$

Then $a - b(q + 1) \in S$. Note that $q + 1 > q$,

Proof (continued).

If $a > 0$, then $a - b \cdot 0 \in S$, which shows that $S \neq \emptyset$. On the other hand, if $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$. Note that the case with $a = 0$ is handled when $0 \in S$ and we are assuming that $0 \notin S$. So, in either case, $S \neq \emptyset$. By the Principle of Well-Ordering, S must have a smallest element, say $r = a - bq$, where $q \in \mathbb{Z}$. Therefore, $a = bq + r$ with $r \geq 0$. Next, we need to show that $r < b$. For sake of a contradiction, assume that $b < r$. We see that

$$0 < r - b = a - bq - b = a - b(q + 1).$$

Then $a - b(q + 1) \in S$. Note that $q + 1 > q$, which implies that $b(q + 1) > bq$ since $b > 0$.

Proof (continued).

If $a > 0$, then $a - b \cdot 0 \in S$, which shows that $S \neq \emptyset$. On the other hand, if $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$. Note that the case with $a = 0$ is handled when $0 \in S$ and we are assuming that $0 \notin S$. So, in either case, $S \neq \emptyset$. By the Principle of Well-Ordering, S must have a smallest element, say $r = a - bq$, where $q \in \mathbb{Z}$. Therefore, $a = bq + r$ with $r \geq 0$. Next, we need to show that $r < b$. For sake of a contradiction, assume that $b < r$. We see that

$$0 < r - b = a - bq - b = a - b(q + 1).$$

Then $a - b(q + 1) \in S$. Note that $q + 1 > q$, which implies that $b(q + 1) > bq$ since $b > 0$. But then $a - b(q + 1) < a - bq$,

Proof (continued).

If $a > 0$, then $a - b \cdot 0 \in S$, which shows that $S \neq \emptyset$. On the other hand, if $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$. Note that the case with $a = 0$ is handled when $0 \in S$ and we are assuming that $0 \notin S$. So, in either case, $S \neq \emptyset$. By the Principle of Well-Ordering, S must have a smallest element, say $r = a - bq$, where $q \in \mathbb{Z}$. Therefore, $a = bq + r$ with $r \geq 0$. Next, we need to show that $r < b$. For sake of a contradiction, assume that $b < r$. We see that

$$0 < r - b = a - bq - b = a - b(q + 1).$$

Then $a - b(q + 1) \in S$. Note that $q + 1 > q$, which implies that $b(q + 1) > bq$ since $b > 0$. But then $a - b(q + 1) < a - bq$, which contradicts $a - bq$ being the smallest element of S.

Proof (continued).

If $a > 0$, then $a - b \cdot 0 \in S$, which shows that $S \neq \emptyset$. On the other hand, if $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$. Note that the case with $a = 0$ is handled when $0 \in S$ and we are assuming that $0 \notin S$. So, in either case, $S \neq \emptyset$. By the Principle of Well-Ordering, S must have a smallest element, say $r = a - bq$, where $q \in \mathbb{Z}$. Therefore, $a = bq + r$ with $r \geq 0$. Next, we need to show that $r < b$. For sake of a contradiction, assume that $b < r$. We see that

$$0 < r - b = a - bq - b = a - b(q + 1).$$

Then $a - b(q + 1) \in S$. Note that $q + 1 > q$, which implies that $b(q + 1) > bq$ since $b > 0$. But then $a - b(q + 1) < a - bq$, which contradicts $a - bq$ being the smallest element of S. Thus, $r \leq b$.

Proof (continued).

If $a > 0$, then $a - b \cdot 0 \in S$, which shows that $S \neq \emptyset$. On the other hand, if $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$. Note that the case with $a = 0$ is handled when $0 \in S$ and we are assuming that $0 \notin S$. So, in either case, $S \neq \emptyset$. By the Principle of Well-Ordering, S must have a smallest element, say $r = a - bq$, where $q \in \mathbb{Z}$. Therefore, $a = bq + r$ with $r \geq 0$. Next, we need to show that $r < b$. For sake of a contradiction, assume that $b < r$. We see that

$$0 < r - b = a - bq - b = a - b(q + 1).$$

Then $a - b(q + 1) \in S$. Note that $q + 1 > q$, which implies that $b(q + 1) > bq$ since $b > 0$. But then $a - b(q + 1) < a - bq$, which contradicts $a - bq$ being the smallest element of S. Thus, $r \leq b$. However, if $r = b$, then $0 \in S$ (why?),

Proof (continued).

If $a > 0$, then $a - b \cdot 0 \in S$, which shows that $S \neq \emptyset$. On the other hand, if $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$. Note that the case with $a = 0$ is handled when $0 \in S$ and we are assuming that $0 \notin S$. So, in either case, $S \neq \emptyset$. By the Principle of Well-Ordering, S must have a smallest element, say $r = a - bq$, where $q \in \mathbb{Z}$. Therefore, $a = bq + r$ with $r \geq 0$. Next, we need to show that $r < b$. For sake of a contradiction, assume that $b < r$. We see that

$$0 < r - b = a - bq - b = a - b(q + 1).$$

Then $a - b(q + 1) \in S$. Note that $q + 1 > q$, which implies that $b(q + 1) > bq$ since $b > 0$. But then $a - b(q + 1) < a - bq$, which contradicts $a - bq$ being the smallest element of S. Thus, $r \leq b$. However, if $r = b$, then $0 \in S$ (why?),which we are assuming it's not.

Proof (continued).

If $a > 0$, then $a - b \cdot 0 \in S$, which shows that $S \neq \emptyset$. On the other hand, if $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$. Note that the case with $a = 0$ is handled when $0 \in S$ and we are assuming that $0 \notin S$. So, in either case, $S \neq \emptyset$. By the Principle of Well-Ordering, S must have a smallest element, say $r = a - bq$, where $q \in \mathbb{Z}$. Therefore, $a = bq + r$ with $r \geq 0$. Next, we need to show that $r < b$. For sake of a contradiction, assume that $b < r$. We see that

$$0 < r - b = a - bq - b = a - b(q + 1).$$

Then $a - b(q + 1) \in S$. Note that $q + 1 > q$, which implies that $b(q + 1) > bq$ since $b > 0$. But then $a - b(q + 1) < a - bq$, which contradicts $a - bq$ being the smallest element of S. Thus, $r \leq b$. However, if $r = b$, then $0 \in S$ (why?),which we are assuming it's not. Therefore, we actually have $r < b$.

Proof (continued).

If $a > 0$, then $a - b \cdot 0 \in S$, which shows that $S \neq \emptyset$. On the other hand, if $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$. Note that the case with $a = 0$ is handled when $0 \in S$ and we are assuming that $0 \notin S$. So, in either case, $S \neq \emptyset$. By the Principle of Well-Ordering, S must have a smallest element, say $r = a - bq$, where $q \in \mathbb{Z}$. Therefore, $a = bq + r$ with $r \geq 0$. Next, we need to show that $r < b$. For sake of a contradiction, assume that $b < r$. We see that

$$0 < r - b = a - bq - b = a - b(q + 1).$$

Then $a - b(q + 1) \in S$. Note that $q + 1 > q$, which implies that $b(q + 1) > bq$ since $b > 0$. But then $a - b(q + 1) < a - bq$, which contradicts $a - bq$ being the smallest element of S. Thus, $r \leq b$. However, if $r = b$, then $0 \in S$ (why?),which we are assuming it's not. Therefore, we actually have $r < b$. We have shown that there exists integers q and r with the desired properties.

Proof (continued).

If $a > 0$, then $a - b \cdot 0 \in S$, which shows that $S \neq \emptyset$. On the other hand, if $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$. Note that the case with $a = 0$ is handled when $0 \in S$ and we are assuming that $0 \notin S$. So, in either case, $S \neq \emptyset$. By the Principle of Well-Ordering, S must have a smallest element, say $r = a - bq$, where $q \in \mathbb{Z}$. Therefore, $a = bq + r$ with $r \geq 0$. Next, we need to show that $r < b$. For sake of a contradiction, assume that $b < r$. We see that

$$0 < r - b = a - bq - b = a - b(q + 1).$$

Then $a - b(q + 1) \in S$. Note that $q + 1 > q$, which implies that $b(q + 1) > bq$ since $b > 0$. But then $a - b(q + 1) < a - bq$, which contradicts $a - bq$ being the smallest element of S. Thus, $r \leq b$. However, if $r = b$, then $0 \in S$ (why?),which we are assuming it's not. Therefore, we actually have $r < b$. We have shown that there exists integers q and r with the desired properties.

Uniqueness:

Proof (continued).

If $a > 0$, then $a - b \cdot 0 \in S$, which shows that $S \neq \emptyset$. On the other hand, if $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$. Note that the case with $a = 0$ is handled when $0 \in S$ and we are assuming that $0 \notin S$. So, in either case, $S \neq \emptyset$. By the Principle of Well-Ordering, S must have a smallest element, say $r = a - bq$, where $q \in \mathbb{Z}$. Therefore, $a = bq + r$ with $r \geq 0$. Next, we need to show that $r < b$. For sake of a contradiction, assume that $b < r$. We see that

$$0 < r - b = a - bq - b = a - b(q + 1).$$

Then $a - b(q + 1) \in S$. Note that $q + 1 > q$, which implies that $b(q + 1) > bq$ since $b > 0$. But then $a - b(q + 1) < a - bq$, which contradicts $a - bq$ being the smallest element of S. Thus, $r \leq b$. However, if $r = b$, then $0 \in S$ (why?),which we are assuming it's not. Therefore, we actually have $r < b$. We have shown that there exists integers q and r with the desired properties.

Uniqueness: Assume that there exists integers r, r', q, and q' such that

Proof (continued).

If $a > 0$, then $a - b \cdot 0 \in S$, which shows that $S \neq \emptyset$. On the other hand, if $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$. Note that the case with $a = 0$ is handled when $0 \in S$ and we are assuming that $0 \notin S$. So, in either case, $S \neq \emptyset$. By the Principle of Well-Ordering, S must have a smallest element, say $r = a - bq$, where $q \in \mathbb{Z}$. Therefore, $a = bq + r$ with $r \geq 0$. Next, we need to show that $r < b$. For sake of a contradiction, assume that $b < r$. We see that

$$0 < r - b = a - bq - b = a - b(q + 1).$$

Then $a - b(q + 1) \in S$. Note that $q + 1 > q$, which implies that $b(q + 1) > bq$ since $b > 0$. But then $a - b(q + 1) < a - bq$, which contradicts $a - bq$ being the smallest element of S. Thus, $r \leq b$. However, if $r = b$, then $0 \in S$ (why?),which we are assuming it's not. Therefore, we actually have $r < b$. We have shown that there exists integers q and r with the desired properties.

Uniqueness: Assume that there exists integers r, r', q, and q' such that

$$a = bq + r, 0 \leq r < b \quad \text{and}$$

Proof (continued).

If $a > 0$, then $a - b \cdot 0 \in S$, which shows that $S \neq \emptyset$. On the other hand, if $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$. Note that the case with $a = 0$ is handled when $0 \in S$ and we are assuming that $0 \notin S$. So, in either case, $S \neq \emptyset$. By the Principle of Well-Ordering, S must have a smallest element, say $r = a - bq$, where $q \in \mathbb{Z}$. Therefore, $a = bq + r$ with $r \geq 0$. Next, we need to show that $r < b$. For sake of a contradiction, assume that $b < r$. We see that

$$0 < r - b = a - bq - b = a - b(q + 1).$$

Then $a - b(q + 1) \in S$. Note that $q + 1 > q$, which implies that $b(q + 1) > bq$ since $b > 0$. But then $a - b(q + 1) < a - bq$, which contradicts $a - bq$ being the smallest element of S. Thus, $r \leq b$. However, if $r = b$, then $0 \in S$ (why?),which we are assuming it's not. Therefore, we actually have $r < b$. We have shown that there exists integers q and r with the desired properties.

Uniqueness: Assume that there exists integers r, r', q, and q' such that

$$a = bq + r, 0 \leq r < b \quad \text{and} \quad a = bq' + r', 0 \leq r' < b.$$

Proof (continued).

Proof (continued).

Then $bq + r = bq' + r'$,

Proof (continued).

Then $bq + r = bq' + r'$, which is equivalent to $b(q - q') = r' - r$.

Proof (continued).

Then $bq + r = bq' + r'$, which is equivalent to $b(q - q') = r' - r$. This implies that b divides $r' - r$.

Proof (continued).

Then $bq + r = bq' + r'$, which is equivalent to $b(q - q') = r' - r$. This implies that b divides $r' - r$. Certainly, either $r' \geq r$ or $r \geq r'$.

Proof (continued).

Then $bq + r = bq' + r'$, which is equivalent to $b(q - q') = r' - r$. This implies that b divides $r' - r$. Certainly, either $r' \geq r$ or $r \geq r'$. Without loss of generality, assume that $r' \geq r$.

Proof (continued).

Then $bq + r = bq' + r'$, which is equivalent to $b(q - q') = r' - r$. This implies that b divides $r' - r$. Certainly, either $r' \geq r$ or $r \geq r'$. Without loss of generality, assume that $r' \geq r$. This implies that $0 \leq r' - r < r'$,

Proof (continued).

Then $bq + r = bq' + r'$, which is equivalent to $b(q - q') = r' - r$. This implies that b divides $r' - r$. Certainly, either $r' \geq r$ or $r \geq r'$. Without loss of generality, assume that $r' \geq r$. This implies that $0 \leq r' - r < r'$, which is less than b by hypothesis.

Proof (continued).

Then $bq + r = bq' + r'$, which is equivalent to $b(q - q') = r' - r$. This implies that b divides $r' - r$. Certainly, either $r' \geq r$ or $r \geq r'$. Without loss of generality, assume that $r' \geq r$. This implies that $0 \leq r' - r < r'$, which is less than b by hypothesis. The only way b (which is positive) can divide the non-negative number $r' - r$ (which is strictly less than b) is if $r' - r = 0$.

Proof (continued).

Then $bq + r = bq' + r'$, which is equivalent to $b(q - q') = r' - r$. This implies that b divides $r' - r$. Certainly, either $r' \geq r$ or $r \geq r'$. Without loss of generality, assume that $r' \geq r$. This implies that $0 \leq r' - r < r'$, which is less than b by hypothesis. The only way b (which is positive) can divide the non-negative number $r' - r$ (which is strictly less than b) is if $r' - r = 0$. Thus, it must be the case that $r' = r$.

Proof (continued).

Then $bq + r = bq' + r'$, which is equivalent to $b(q - q') = r' - r$. This implies that b divides $r' - r$. Certainly, either $r' \geq r$ or $r \geq r'$. Without loss of generality, assume that $r' \geq r$. This implies that $0 \leq r' - r < r'$, which is less than b by hypothesis. The only way b (which is positive) can divide the non-negative number $r' - r$ (which is strictly less than b) is if $r' - r = 0$. Thus, it must be the case that $r' = r$. It immediately follows that $q = q'$.

Proof (continued).

Then $bq + r = bq' + r'$, which is equivalent to $b(q - q') = r' - r$. This implies that b divides $r' - r$. Certainly, either $r' \geq r$ or $r \geq r'$. Without loss of generality, assume that $r' \geq r$. This implies that $0 \leq r' - r < r'$, which is less than b by hypothesis. The only way b (which is positive) can divide the non-negative number $r' - r$ (which is strictly less than b) is if $r' - r = 0$. Thus, it must be the case that $r' = r$. It immediately follows that $q = q'$. We have shown that q and r must be unique.

□

Proof (continued).

Then $bq + r = bq' + r'$, which is equivalent to $b(q - q') = r' - r$. This implies that b divides $r' - r$. Certainly, either $r' \geq r$ or $r \geq r'$. Without loss of generality, assume that $r' \geq r$. This implies that $0 \leq r' - r < r'$, which is less than b by hypothesis. The only way b (which is positive) can divide the non-negative number $r' - r$ (which is strictly less than b) is if $r' - r = 0$. Thus, it must be the case that $r' = r$. It immediately follows that $q = q'$. We have shown that q and r must be unique. $\square$

Definition

Proof (continued).

Then $bq + r = bq' + r'$, which is equivalent to $b(q - q') = r' - r$. This implies that b divides $r' - r$. Certainly, either $r' \geq r$ or $r \geq r'$. Without loss of generality, assume that $r' \geq r$. This implies that $0 \leq r' - r < r'$, which is less than b by hypothesis. The only way b (which is positive) can divide the non-negative number $r' - r$ (which is strictly less than b) is if $r' - r = 0$. Thus, it must be the case that $r' = r$. It immediately follows that $q = q'$. We have shown that q and r must be unique. □

Definition

- Let $a, b \in \mathbb{Z}$.

Proof (continued).

Then $bq + r = bq' + r'$, which is equivalent to $b(q - q') = r' - r$. This implies that b divides $r' - r$. Certainly, either $r' \geq r$ or $r \geq r'$. Without loss of generality, assume that $r' \geq r$. This implies that $0 \leq r' - r < r'$, which is less than b by hypothesis. The only way b (which is positive) can divide the non-negative number $r' - r$ (which is strictly less than b) is if $r' - r = 0$. Thus, it must be the case that $r' = r$. It immediately follows that $q = q'$. We have shown that q and r must be unique. □

Definition

- Let $a, b \in \mathbb{Z}$. If there exists $k \in \mathbb{Z}$ such that $b = ak$, then we write $a|b$.

Proof (continued).

Then $bq + r = bq' + r'$, which is equivalent to $b(q - q') = r' - r$. This implies that b divides $r' - r$. Certainly, either $r' \geq r$ or $r \geq r'$. Without loss of generality, assume that $r' \geq r$. This implies that $0 \leq r' - r < r'$, which is less than b by hypothesis. The only way b (which is positive) can divide the non-negative number $r' - r$ (which is strictly less than b) is if $r' - r = 0$. Thus, it must be the case that $r' = r$. It immediately follows that $q = q'$. We have shown that q and r must be unique. □

Definition

- Let $a, b \in \mathbb{Z}$. If there exists $k \in \mathbb{Z}$ such that $b = ak$, then we write $a|b$.
- An integer d is called a common divisor of a and b if $d|a$ and $d|b$.

Proof (continued).

Then $bq + r = bq' + r'$, which is equivalent to $b(q - q') = r' - r$. This implies that b divides $r' - r$. Certainly, either $r' \geq r$ or $r \geq r'$. Without loss of generality, assume that $r' \geq r$. This implies that $0 \leq r' - r < r'$, which is less than b by hypothesis. The only way b (which is positive) can divide the non-negative number $r' - r$ (which is strictly less than b) is if $r' - r = 0$. Thus, it must be the case that $r' = r$. It immediately follows that $q = q'$. We have shown that q and r must be unique.

□

Definition

- Let $a, b \in \mathbb{Z}$. If there exists $k \in \mathbb{Z}$ such that $b = ak$, then we write $a|b$.
- An integer d is called a common divisor of a and b if $d|a$ and $d|b$.
- The greatest common divisor of a and b is a positive integer d such that d is a common divisor of a and b

Proof (continued).

Then $bq + r = bq' + r'$, which is equivalent to $b(q - q') = r' - r$. This implies that b divides $r' - r$. Certainly, either $r' \geq r$ or $r \geq r'$. Without loss of generality, assume that $r' \geq r$. This implies that $0 \leq r' - r < r'$, which is less than b by hypothesis. The only way b (which is positive) can divide the non-negative number $r' - r$ (which is strictly less than b) is if $r' - r = 0$. Thus, it must be the case that $r' = r$. It immediately follows that $q = q'$. We have shown that q and r must be unique.

□

Definition

- Let $a, b \in \mathbb{Z}$. If there exists $k \in \mathbb{Z}$ such that $b = ak$, then we write $a|b$.
- An integer d is called a common divisor of a and b if $d|a$ and $d|b$.
- The greatest common divisor of a and b is a positive integer d such that d is a common divisor of a and b and if d' is any other common divisor of a and b, then $d'|d$.

Proof (continued).

Then $bq + r = bq' + r'$, which is equivalent to $b(q - q') = r' - r$. This implies that b divides $r' - r$. Certainly, either $r' \geq r$ or $r \geq r'$. Without loss of generality, assume that $r' \geq r$. This implies that $0 \leq r' - r < r'$, which is less than b by hypothesis. The only way b (which is positive) can divide the non-negative number $r' - r$ (which is strictly less than b) is if $r' - r = 0$. Thus, it must be the case that $r' = r$. It immediately follows that $q = q'$. We have shown that q and r must be unique. $\square$

Definition

- Let $a, b \in \mathbb{Z}$. If there exists $k \in \mathbb{Z}$ such that $b = ak$, then we write $a|b$.
- An integer d is called a common divisor of a and b if $d|a$ and $d|b$.
- The greatest common divisor of a and b is a positive integer d such that d is a common divisor of a and b and if d' is any other common divisor of a and b, then $d'|d$. In this case, we write $d = \gcd(a, b)$.

Proof (continued).

Then $bq + r = bq' + r'$, which is equivalent to $b(q - q') = r' - r$. This implies that b divides $r' - r$. Certainly, either $r' \geq r$ or $r \geq r'$. Without loss of generality, assume that $r' \geq r$. This implies that $0 \leq r' - r < r'$, which is less than b by hypothesis. The only way b (which is positive) can divide the non-negative number $r' - r$ (which is strictly less than b) is if $r' - r = 0$. Thus, it must be the case that $r' = r$. It immediately follows that $q = q'$. We have shown that q and r must be unique. $\square$

Definition

- Let $a, b \in \mathbb{Z}$. If there exists $k \in \mathbb{Z}$ such that $b = ak$, then we write $a|b$.
- An integer d is called a common divisor of a and b if $d|a$ and $d|b$.
- The greatest common divisor of a and b is a positive integer d such that d is a common divisor of a and b and if d' is any other common divisor of a and b, then $d'|d$. In this case, we write $d = \gcd(a, b)$. For example, $\gcd(12, 16) = 4$.

Proof (continued).

Then $bq + r = bq' + r'$, which is equivalent to $b(q - q') = r' - r$. This implies that b divides $r' - r$. Certainly, either $r' \geq r$ or $r \geq r'$. Without loss of generality, assume that $r' \geq r$. This implies that $0 \leq r' - r < r'$, which is less than b by hypothesis. The only way b (which is positive) can divide the non-negative number $r' - r$ (which is strictly less than b) is if $r' - r = 0$. Thus, it must be the case that $r' = r$. It immediately follows that $q = q'$. We have shown that q and r must be unique. $\square$

Definition

- Let $a, b \in \mathbb{Z}$. If there exists $k \in \mathbb{Z}$ such that $b = ak$, then we write $a|b$.
- An integer d is called a common divisor of a and b if $d|a$ and $d|b$.
- The greatest common divisor of a and b is a positive integer d such that d is a common divisor of a and b and if d' is any other common divisor of a and b, then $d'|d$. In this case, we write $d = \gcd(a, b)$. For example, $\gcd(12, 16) = 4$.
- If $\gcd(a, b) = 1$, we say that a and b are relatively prime.

Proof (continued).

Then $bq + r = bq' + r'$, which is equivalent to $b(q - q') = r' - r$. This implies that b divides $r' - r$. Certainly, either $r' \geq r$ or $r \geq r'$. Without loss of generality, assume that $r' \geq r$. This implies that $0 \leq r' - r < r'$, which is less than b by hypothesis. The only way b (which is positive) can divide the non-negative number $r' - r$ (which is strictly less than b) is if $r' - r = 0$. Thus, it must be the case that $r' = r$. It immediately follows that $q = q'$. We have shown that q and r must be unique. □

Definition

- Let $a, b \in \mathbb{Z}$. If there exists $k \in \mathbb{Z}$ such that $b = ak$, then we write $a|b$.
- An integer d is called a common divisor of a and b if $d|a$ and $d|b$.
- The greatest common divisor of a and b is a positive integer d such that d is a common divisor of a and b and if d' is any other common divisor of a and b, then $d'|d$. In this case, we write $d = \gcd(a, b)$. For example, $\gcd(12, 16) = 4$.
- If $\gcd(a, b) = 1$, we say that a and b are relatively prime. For example, 12 and 35 are relatively prime since $\gcd(12, 35) = 1$.

Theorem 1.4

Theorem 1.4

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

Theorem 1.4

Let $a, b \in \mathbb{Z}$. Then there exists $r, s \in \mathbb{Z}$ such that

Theorem 1.4

Let $a, b \in \mathbb{Z}$. Then there exists $r, s \in \mathbb{Z}$ such that

$$\gcd(a, b) = ar + bs.$$

Theorem 1.4

Let $a, b \in \mathbb{Z}$. Then there exists $r, s \in \mathbb{Z}$ such that

$$\gcd(a, b) = ar + bs.$$

Furthermore, the greatest common divisor of a and b is unique.

Theorem 1.4

Let $a, b \in \mathbb{Z}$. Then there exists $r, s \in \mathbb{Z}$ such that

$$\gcd(a, b) = ar + bs.$$

Furthermore, the greatest common divisor of a and b is unique.

Proof.

See *AATA*. $\square$

Theorem 1.4

Let $a, b \in \mathbb{Z}$. Then there exists $r, s \in \mathbb{Z}$ such that

$$\gcd(a, b) = ar + bs.$$

Furthermore, the greatest common divisor of a and b is unique.

Proof.

See *AATA*. $\square$

Corollary 1.5

Theorem 1.4

Let $a, b \in \mathbb{Z}$. Then there exists $r, s \in \mathbb{Z}$ such that

$$\gcd(a, b) = ar + bs.$$

Furthermore, the greatest common divisor of a and b is unique.

Proof.

See *AATA*. $\square$

Corollary 1.5

Let $a, b \in \mathbb{Z}$ such a and b are relatively prime.

Theorem 1.4

Let $a, b \in \mathbb{Z}$. Then there exists $r, s \in \mathbb{Z}$ such that

$$\gcd(a, b) = ar + bs.$$

Furthermore, the greatest common divisor of a and b is unique.

Proof.

See *AATA*. $\square$

Corollary 1.5

Let $a, b \in \mathbb{Z}$ such a and b are relatively prime. Then there exists $r, s \in \mathbb{Z}$ such that $ar + bs = 1$.

Theorem 1.4

Let $a, b \in \mathbb{Z}$. Then there exists $r, s \in \mathbb{Z}$ such that

$$\gcd(a, b) = ar + bs.$$

Furthermore, the greatest common divisor of a and b is unique.

Proof.

See *AATA*. □

Corollary 1.5

Let $a, b \in \mathbb{Z}$ such a and b are relatively prime. Then there exists $r, s \in \mathbb{Z}$ such that $ar + bs = 1$.

Proof.

Theorem 1.4

Let $a, b \in \mathbb{Z}$. Then there exists $r, s \in \mathbb{Z}$ such that

$$\gcd(a, b) = ar + bs.$$

Furthermore, the greatest common divisor of a and b is unique.

Proof.

See *AATA*. □

Corollary 1.5

Let $a, b \in \mathbb{Z}$ such a and b are relatively prime. Then there exists $r, s \in \mathbb{Z}$ such that $ar + bs = 1$.

Proof.

This follows immediately from Theorem 1.4 and the definition of relatively prime. □

The Euclidean Algorithm is a process involving repeated division by which we can find the greatest common divisor of any two nonzero integers.

The Euclidean Algorithm is a process involving repeated division by which we can find the greatest common divisor of any two nonzero integers. Theorem 1.4 guarantees that this process terminates.

The Euclidean Algorithm is a process involving repeated division by which we can find the greatest common divisor of any two nonzero integers. Theorem 1.4 guarantees that this process terminates. The algorithm itself is best illustrated with an example.

The Euclidean Algorithm is a process involving repeated division by which we can find the greatest common divisor of any two nonzero integers. Theorem 1.4 guarantees that this process terminates. The algorithm itself is best illustrated with an example.

Example

The Euclidean Algorithm is a process involving repeated division by which we can find the greatest common divisor of any two nonzero integers. Theorem 1.4 guarantees that this process terminates. The algorithm itself is best illustrated with an example.

Example

We will compute $\gcd(312, 1110)$.

The Euclidean Algorithm is a process involving repeated division by which we can find the greatest common divisor of any two nonzero integers. Theorem 1.4 guarantees that this process terminates. The algorithm itself is best illustrated with an example.

Example

We will compute $\gcd(312, 1110)$. Observe that

$$\begin{aligned} 1110 &= 312 \cdot 3 + 174 && \text{(1110 divided by 312 is 3 with remainder of 174)} \\ 312 &= 174 \cdot 1 + 138 && \text{(312 divided by 174 is 1 with remainder 138)} \\ 174 &= 138 \cdot 1 + 36 \end{aligned}$$

The Euclidean Algorithm is a process involving repeated division by which we can find the greatest common divisor of any two nonzero integers. Theorem 1.4 guarantees that this process terminates. The algorithm itself is best illustrated with an example.

Example

We will compute $\gcd(312, 1110)$. Observe that

$$\begin{aligned} 1110 &= 312 \cdot 3 + 174 && \text{(1110 divided by 312 is 3 with remainder of 174)} \\ 312 &= 174 \cdot 1 + 138 && \text{(312 divided by 174 is 1 with remainder 138)} \\ 174 &= 138 \cdot 1 + 36 \\ 138 &= 36 \cdot 3 + 30 \end{aligned}$$

The Euclidean Algorithm is a process involving repeated division by which we can find the greatest common divisor of any two nonzero integers. Theorem 1.4 guarantees that this process terminates. The algorithm itself is best illustrated with an example.

Example

We will compute $\gcd(312, 1110)$. Observe that

$$
\begin{aligned}
1110 &= 312 \cdot 3 + 174 && \text{(1110 divided by 312 is 3 with remainder of 174)} \\
312 &= 174 \cdot 1 + 138 && \text{(312 divided by 174 is 1 with remainder 138)} \\
174 &= 138 \cdot 1 + 36 \\
138 &= 36 \cdot 3 + 30 \\
36 &= 30 \cdot 1 + 6
\end{aligned}
$$

The Euclidean Algorithm is a process involving repeated division by which we can find the greatest common divisor of any two nonzero integers. Theorem 1.4 guarantees that this process terminates. The algorithm itself is best illustrated with an example.

Example

We will compute $\gcd(312, 1110)$. Observe that

$$\begin{aligned}
1110 &= 312 \cdot 3 + 174 && \text{(1110 divided by 312 is 3 with remainder of 174)}\\
312 &= 174 \cdot 1 + 138 && \text{(312 divided by 174 is 1 with remainder 138)}\\
174 &= 138 \cdot 1 + 36\\
138 &= 36 \cdot 3 + 30\\
36 &= 30 \cdot 1 + 6\\
30 &= 6 \cdot 5 + 0
\end{aligned}$$

The Euclidean Algorithm is a process involving repeated division by which we can find the greatest common divisor of any two nonzero integers. Theorem 1.4 guarantees that this process terminates. The algorithm itself is best illustrated with an example.

Example

We will compute $\gcd(312, 1110)$. Observe that

$$
\begin{aligned}
1110 &= 312 \cdot 3 + 174 && \text{(1110 divided by 312 is 3 with remainder of 174)}\\
312 &= 174 \cdot 1 + 138 && \text{(312 divided by 174 is 1 with remainder 138)}\\
174 &= 138 \cdot 1 + 36\\
138 &= 36 \cdot 3 + 30\\
36 &= 30 \cdot 1 + 6\\
30 &= 6 \cdot 5 + 0
\end{aligned}
$$

Claim: $\gcd(312, 1110) = 6$.

The Euclidean Algorithm is a process involving repeated division by which we can find the greatest common divisor of any two nonzero integers. Theorem 1.4 guarantees that this process terminates. The algorithm itself is best illustrated with an example.

Example

We will compute $\gcd(312, 1110)$. Observe that

$$
\begin{aligned}
1110 &= 312 \cdot 3 + 174 && \text{(1110 divided by 312 is 3 with remainder of 174)}\\
312 &= 174 \cdot 1 + 138 && \text{(312 divided by 174 is 1 with remainder 138)}\\
174 &= 138 \cdot 1 + 36\\
138 &= 36 \cdot 3 + 30\\
36 &= 30 \cdot 1 + 6\\
30 &= 6 \cdot 5 + 0
\end{aligned}
$$

Claim: $\gcd(312, 1110) = 6$. Why?

The Euclidean Algorithm is a process involving repeated division by which we can find the greatest common divisor of any two nonzero integers. Theorem 1.4 guarantees that this process terminates. The algorithm itself is best illustrated with an example.

Example

We will compute $\gcd(312, 1110)$. Observe that

$$\begin{aligned}
1110 &= 312 \cdot 3 + 174 && \text{(1110 divided by 312 is 3 with remainder of 174)}\\
312 &= 174 \cdot 1 + 138 && \text{(312 divided by 174 is 1 with remainder 138)}\\
174 &= 138 \cdot 1 + 36\\
138 &= 36 \cdot 3 + 30\\
36 &= 30 \cdot 1 + 6\\
30 &= 6 \cdot 5 + 0
\end{aligned}$$

Claim: $\gcd(312, 1110) = 6$. Why?

If we reverse our steps, we see that $6|36$, $6|138$, $6|174$, $6|312$, and $6|1110$.

The Euclidean Algorithm is a process involving repeated division by which we can find the greatest common divisor of any two nonzero integers. Theorem 1.4 guarantees that this process terminates. The algorithm itself is best illustrated with an example.

Example

We will compute $\gcd(312, 1110)$. Observe that

$$\begin{aligned}
1110 &= 312 \cdot 3 + 174 && \text{(1110 divided by 312 is 3 with remainder of 174)}\\
312 &= 174 \cdot 1 + 138 && \text{(312 divided by 174 is 1 with remainder 138)}\\
174 &= 138 \cdot 1 + 36\\
138 &= 36 \cdot 3 + 30\\
36 &= 30 \cdot 1 + 6\\
30 &= 6 \cdot 5 + 0
\end{aligned}$$

Claim: $\gcd(312, 1110) = 6$. Why?

If we reverse our steps, we see that $6|36$, $6|138$, $6|174$, $6|312$, and $6|1110$. This shows that 6 is a common divisor of 312 and 1110,

The Euclidean Algorithm is a process involving repeated division by which we can find the greatest common divisor of any two nonzero integers. Theorem 1.4 guarantees that this process terminates. The algorithm itself is best illustrated with an example.

Example

We will compute $\gcd(312, 1110)$. Observe that

$$\begin{aligned} 1110 &= 312 \cdot 3 + 174 && \text{(1110 divided by 312 is 3 with remainder of 174)} \\ 312 &= 174 \cdot 1 + 138 && \text{(312 divided by 174 is 1 with remainder 138)} \\ 174 &= 138 \cdot 1 + 36 \\ 138 &= 36 \cdot 3 + 30 \\ 36 &= 30 \cdot 1 + 6 \\ 30 &= 6 \cdot 5 + 0 \end{aligned}$$

Claim: $\gcd(312, 1110) = 6$. Why?

If we reverse our steps, we see that $6|36$, $6|138$, $6|174$, $6|312$, and $6|1110$. This shows that 6 is a common divisor of 312 and 1110, but why is it the *greatest*?

The Euclidean Algorithm (continued)

Example (continued)

Example (continued)

By construction, any common divisor of 1110 and 312 would have to divide the remainders in each step.

Example (continued)

By construction, any common divisor of 1110 and 312 would have to divide the remainders in each step. (To see why this is true, look at the very first line:

Example (continued)

By construction, any common divisor of 1110 and 312 would have to divide the remainders in each step. (To see why this is true, look at the very first line: d divides 1110 and 312, so it must divide the very first remainder.

Example (continued)

By construction, any common divisor of 1110 and 312 would have to divide the remainders in each step. (To see why this is true, look at the very first line: d divides 1110 and 312, so it must divide the very first remainder. Continue this way.)

Example (continued)

By construction, any common divisor of 1110 and 312 would have to divide the remainders in each step. (To see why this is true, look at the very first line: d divides 1110 and 312, so it must divide the very first remainder. Continue this way.) But 6 is one of the remainders, which implies that any common divisor d must divide 6.

Example (continued)

By construction, any common divisor of 1110 and 312 would have to divide the remainders in each step. (To see why this is true, look at the very first line: d divides 1110 and 312, so it must divide the very first remainder. Continue this way.) But 6 is one of the remainders, which implies that any common divisor d must divide 6. The only way this can be true is if $6 = \gcd(1110, 312)$.

Example (continued)

By construction, any common divisor of 1110 and 312 would have to divide the remainders in each step. (To see why this is true, look at the very first line: d divides 1110 and 312, so it must divide the very first remainder. Continue this way.) But 6 is one of the remainders, which implies that any common divisor d must divide 6. The only way this can be true is if $6 = \gcd(1110, 312)$.

Now, if we work backward through our previous sequence of equations, we can also find the integers r and s guaranteed to exist according to Theorem 1.4.

Example (continued)

By construction, any common divisor of 1110 and 312 would have to divide the remainders in each step. (To see why this is true, look at the very first line: d divides 1110 and 312, so it must divide the very first remainder. Continue this way.) But 6 is one of the remainders, which implies that any common divisor d must divide 6. The only way this can be true is if $6 = \gcd(1110, 312)$.

Now, if we work backward through our previous sequence of equations, we can also find the integers r and s guaranteed to exist according to Theorem 1.4.

In this case, we are looking for integers r and s such that $1110r + 312s = 6$.

Example (continued)

Example (continued)

By doing repeated substitutions, we see that

Example (continued)

By doing repeated substitutions, we see that

$$\begin{aligned}
6 &= 36 + (-1)30 \\
&= 36 + (-1)(138 + (-3)36) \\
&= (4)36 + (-1)138 \\
&= (4)(174 + (-1)138) + (-1)138 \\
&= (4)174 + (-5)138 \\
&= (4)174 + (-5)(312 + (-1)174) \\
&= (9)174 + (-5)312 \\
&= (9)(1110 + (-3)312) + (-5)312 \\
&= (9)1110 + (-32)312.
\end{aligned}$$

Example (continued)

By doing repeated substitutions, we see that

$$\begin{aligned} 6 &= 36 + (-1)30 \\ &= 36 + (-1)(138 + (-3)36) \\ &= (4)36 + (-1)138 \\ &= (4)(174 + (-1)138) + (-1)138 \\ &= (4)174 + (-5)138 \\ &= (4)174 + (-5)(312 + (-1)174) \\ &= (9)174 + (-5)312 \\ &= (9)(1110 + (-3)312) + (-5)312 \\ &= (9)1110 + (-32)312. \end{aligned}$$

So, $r = 9$ and $s = -32$.

Example (continued)

By doing repeated substitutions, we see that

$$\begin{aligned}
6 &= 36 + (-1)30 \\
&= 36 + (-1)(138 + (-3)36) \\
&= (4)36 + (-1)138 \\
&= (4)(174 + (-1)138) + (-1)138 \\
&= (4)174 + (-5)138 \\
&= (4)174 + (-5)(312 + (-1)174) \\
&= (9)174 + (-5)312 \\
&= (9)(1110 + (-3)312) + (-5)312 \\
&= (9)1110 + (-32)312.
\end{aligned}$$

So, $r = 9$ and $s = -32$. Note that r and s are not unique.

Definition

Definition

Let p be a natural number greater than 1.

Definition

Let p be a natural number greater than 1. We say that p is prime if

Definition

Let p be a natural number greater than 1. We say that p is prime if the only natural numbers that divide p are 1 and p itself.

Definition

Let p be a natural number greater than 1. We say that p is prime if the only natural numbers that divide p are 1 and p itself. A natural number greater than 1 that is not prime is called composite.

Definition

Let p be a natural number greater than 1. We say that p is prime if the only natural numbers that divide p are 1 and p itself. A natural number greater than 1 that is not prime is called composite.

Lemma 1.6

Definition

Let p be a natural number greater than 1. We say that p is prime if the only natural numbers that divide p are 1 and p itself. A natural number greater than 1 that is not prime is called composite.

Lemma 1.6

Let $a, b \in \mathbb{Z}$ and let p be prime.

Definition

Let p be a natural number greater than 1. We say that p is prime if the only natural numbers that divide p are 1 and p itself. A natural number greater than 1 that is not prime is called composite.

Lemma 1.6

Let $a, b \in \mathbb{Z}$ and let p be prime. If $p|ab$, then either $p|a$ or $p|b$.

Definition

Let p be a natural number greater than 1. We say that p is prime if the only natural numbers that divide p are 1 and p itself. A natural number greater than 1 that is not prime is called composite.

Lemma 1.6

Let $a, b \in \mathbb{Z}$ and let p be prime. If $p | ab$, then either $p | a$ or $p | b$.

Proof.

See *AATA*. $\square$

Definition
Let p be a natural number greater than 1. We say that p is prime if the only natural numbers that divide p are 1 and p itself. A natural number greater than 1 that is not prime is called composite.

Lemma 1.6
Let $a, b \in \mathbb{Z}$ and let p be prime. If $p|ab$, then either $p|a$ or $p|b$.

Proof.
See *AATA*. $\square$

Warning!

Definition

Let p be a natural number greater than 1. We say that p is prime if the only natural numbers that divide p are 1 and p itself. A natural number greater than 1 that is not prime is called composite.

Lemma 1.6

Let $a, b \in \mathbb{Z}$ and let p be prime. If $p|ab$, then either $p|a$ or $p|b$.

Proof.

See *AATA*. $\square$

Warning!

Replacing p with a composite number in Lemma 1.6 doesn't work, in general.

Definition

Let p be a natural number greater than 1. We say that p is prime if the only natural numbers that divide p are 1 and p itself. A natural number greater than 1 that is not prime is called composite.

Lemma 1.6

Let $a, b \in \mathbb{Z}$ and let p be prime. If $p|ab$, then either $p|a$ or $p|b$.

Proof.

See *AATA*. $\square$

Warning!

Replacing p with a composite number in Lemma 1.6 doesn't work, in general.

Theorem 1.7

Definition

Let p be a natural number greater than 1. We say that p is prime if the only natural numbers that divide p are 1 and p itself. A natural number greater than 1 that is not prime is called composite.

Lemma 1.6

Let $a, b \in \mathbb{Z}$ and let p be prime. If $p|ab$, then either $p|a$ or $p|b$.

Proof.

See *AATA*. $\square$

Warning!

Replacing p with a composite number in Lemma 1.6 doesn't work, in general.

Theorem 1.7

There exist an infinite number of primes.

Definition

Let p be a natural number greater than 1. We say that p is prime if the only natural numbers that divide p are 1 and p itself. A natural number greater than 1 that is not prime is called composite.

Lemma 1.6

Let $a, b \in \mathbb{Z}$ and let p be prime. If $p|ab$, then either $p|a$ or $p|b$.

Proof.

See *AATA*. $\square$

Warning!

Replacing p with a composite number in Lemma 1.6 doesn't work, in general.

Theorem 1.7

There exist an infinite number of primes.

Proof.

See *AATA*. The proof is one from "the book" and one that you should know. The proof uses contradiction. $\square$

Theorem 2.8 (Fundamental Theorem of Arithmetic)

Theorem 2.8 (Fundamental Theorem of Arithmetic)

Let n be a natural number greater than 1.

Theorem 2.8 (Fundamental Theorem of Arithmetic)

Let n be a natural number greater than 1. Then

$$n = p_1 p_2 \cdots p_k,$$

Theorem 2.8 (Fundamental Theorem of Arithmetic)

Let n be a natural number greater than 1. Then

$$n = p_1 p_2 \cdots p_k,$$

where $p_1, \ldots, p_k$ are primes (not necessarily distinct).

Theorem 2.8 (Fundamental Theorem of Arithmetic)

Let n be a natural number greater than 1. Then

$$n = p_1 p_2 \cdots p_k,$$

where $p_1, \ldots, p_k$ are primes (not necessarily distinct). Furthermore, this factorization is unique (up to rearrangement of the factors).

Theorem 2.8 (Fundamental Theorem of Arithmetic)

Let n be a natural number greater than 1. Then

$$n = p_1 p_2 \cdots p_k,$$

where $p_1, \ldots, p_k$ are primes (not necessarily distinct). Furthermore, this factorization is unique (up to rearrangement of the factors).

Proof.

See *AATA*. $\square$

Theorem 2.8 (Fundamental Theorem of Arithmetic)

Let n be a natural number greater than 1. Then

$$n = p_1 p_2 \cdots p_k,$$

where $p_1, \dots, p_k$ are primes (not necessarily distinct). Furthermore, this factorization is unique (up to rearrangement of the factors).

Proof.

See *AATA*. $\square$

Example

Theorem 2.8 (Fundamental Theorem of Arithmetic)

Let n be a natural number greater than 1. Then

$$n = p_1 p_2 \cdots p_k,$$

where $p_1, \ldots, p_k$ are primes (not necessarily distinct). Furthermore, this factorization is unique (up to rearrangement of the factors).

Proof.

See *AATA*. $\square$

Example

(a) $12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$

Theorem 2.8 (Fundamental Theorem of Arithmetic)

Let n be a natural number greater than 1. Then

$$n = p_1 p_2 \cdots p_k,$$

where $p_1, \ldots, p_k$ are primes (not necessarily distinct). Furthermore, this factorization is unique (up to rearrangement of the factors).

Proof.

See *AATA*. $\square$

Example

(a) $12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$

(b) $2610 = 2 \cdot 3^2 \cdot 5 \cdot 29$