Math 3110 Lecture 3

Greg Oman

University of Colorado
Colorado Springs

Induction

Let's begin by recalling the Principle of Mathematical Induction for the set $\mathbb{Z}^+$ of positive integers.

Induction

Let's begin by recalling the Principle of Mathematical Induction for the set $\mathbb{Z}^+$ of positive integers.

Theorem (Principle of Mathematical Induction)

Suppose that $S \subseteq \mathbb{Z}$ is such that

1. $1 \in S$, *and*

Induction

Let's begin by recalling the Principle of Mathematical Induction for the set $\mathbb{Z}^+$ of positive integers.

Theorem (Principle of Mathematical Induction)

Suppose that $S \subseteq \mathbb{Z}$ is such that

1. $1 \in S$, *and*
2. *for every positive integer n, if $n \in S$, then $n + 1 \in S$.*

Induction

Let's begin by recalling the Principle of Mathematical Induction for the set $\mathbb{Z}^+$ of positive integers.

Theorem (Principle of Mathematical Induction)

Suppose that $S \subseteq \mathbb{Z}$ is such that

1. $1 \in S$, *and*
2. *for every positive integer n, if $n \in S$, then $n + 1 \in S$.*
3. *Conclusion: $S = \mathbb{Z}^+$.*

Induction

Let's begin by recalling the Principle of Mathematical Induction for the set $\mathbb{Z}^+$ of positive integers.

Theorem (Principle of Mathematical Induction)

Suppose that $S \subseteq \mathbb{Z}$ is such that

1. $1 \in S$, *and*
2. *for every positive integer n, if $n \in S$, then $n + 1 \in S$.*
3. *Conclusion: $S = \mathbb{Z}^+$.*

There are actually two other equivalent forms of the Principle of Mathematical Induction: so-called 'Strong Induction' and the 'Well-Ordering Principle'.

Induction

Let's begin by recalling the Principle of Mathematical Induction for the set $\mathbb{Z}^+$ of positive integers.

Theorem (Principle of Mathematical Induction)

Suppose that $S \subseteq \mathbb{Z}$ is such that

1. $1 \in S$, *and*
2. *for every positive integer n, if $n \in S$, then $n+1 \in S$.*
3. *Conclusion: $S = \mathbb{Z}^+$.*

There are actually two other equivalent forms of the Principle of Mathematical Induction: so-called 'Strong Induction' and the 'Well-Ordering Principle'. both of these principles may be used in this course, and so I would like to prove them for you from the 'regular' Principle of Mathematical Induction.

Induction

Let's begin by recalling the Principle of Mathematical Induction for the set $\mathbb{Z}^+$ of positive integers.

Theorem (Principle of Mathematical Induction)

Suppose that $S \subseteq \mathbb{Z}$ is such that

1. $1 \in S$, *and*
2. *for every positive integer n, if $n \in S$, then $n+1 \in S$.*
3. *Conclusion: $S = \mathbb{Z}^+$.*

There are actually two other equivalent forms of the Principle of Mathematical Induction: so-called 'Strong Induction' and the 'Well-Ordering Principle'. both of these principles may be used in this course, and so I would like to prove them for you from the 'regular' Principle of Mathematical Induction.

Induction

Theorem (Principle of Strong Induction)

Suppose that $S \subseteq \mathbb{Z}^+$ *is such that*

Induction

Theorem (Principle of Strong Induction)

Suppose that $S \subseteq \mathbb{Z}^+$ *is such that*

1. $1 \in S$, *and*

Induction

Theorem (Principle of Strong Induction)

Suppose that $S \subseteq \mathbb{Z}^+$ *is such that*

1. $1 \in S$, *and*
2. *for every positive integer* n, *if* $1, 2, \ldots, n \in S$, *then* $n + 1 \in S$.

Induction

Theorem (Principle of Strong Induction)

Suppose that $S \subseteq \mathbb{Z}^+$ *is such that*

1. $1 \in S$, *and*
2. *for every positive integer* n, *if* $1, 2, \ldots, n \in S$, *then* $n + 1 \in S$.
3. *Conclusion:* $S = \mathbb{Z}^+$.

Induction

Theorem (Principle of Strong Induction)

Suppose that $S \subseteq \mathbb{Z}^+$ is such that

1. $1 \in S$, *and*
2. *for every positive integer n, if $1, 2, \ldots, n \in S$, then $n + 1 \in S$.*
3. *Conclusion: $S = \mathbb{Z}^+$.*

Proof.

Suppose that $S \subseteq \mathbb{Z}^+$ satisfies (i) and (ii) above.

Induction

Theorem (Principle of Strong Induction)

Suppose that $S \subseteq \mathbb{Z}^+$ is such that

1. $1 \in S$, *and*
2. *for every positive integer n, if $1, 2, \ldots, n \in S$, then $n + 1 \in S$.*
3. *Conclusion: $S = \mathbb{Z}^+$.*

Proof.

Suppose that $S \subseteq \mathbb{Z}^+$ satisfies (i) and (ii) above. Now let $T = \{n \in \mathbb{Z}^+ : 1, 2, \ldots, n \in S\}$.

Induction

Theorem (Principle of Strong Induction)

Suppose that $S \subseteq \mathbb{Z}^+$ *is such that*

1. $1 \in S$, *and*
2. *for every positive integer* n, *if* $1, 2, \ldots, n \in S$, *then* $n + 1 \in S$.
3. *Conclusion:* $S = \mathbb{Z}^+$.

Proof.

Suppose that $S \subseteq \mathbb{Z}^+$ satisfies (i) and (ii) above. Now let $T = \{n \in \mathbb{Z}^+ : 1, 2, \ldots, n \in S\}$. Let us show that T satisfies properties (i) and (ii) of 'regular induction'.

Induction

Theorem (Principle of Strong Induction)

Suppose that $S \subseteq \mathbb{Z}^+$ *is such that*

1. $1 \in S$, *and*
2. *for every positive integer* n, *if* $1, 2, \ldots, n \in S$, *then* $n + 1 \in S$.
3. *Conclusion:* $S = \mathbb{Z}^+$.

Proof.

Suppose that $S \subseteq \mathbb{Z}^+$ satisfies (i) and (ii) above. Now let $T = \{n \in \mathbb{Z}^+ : 1, 2, \ldots, n \in S\}$. Let us show that T satisfies properties (i) and (ii) of 'regular induction'.

(i) (base case) We must show that $1 \in T$.

Induction

Theorem (Principle of Strong Induction)

Suppose that $S \subseteq \mathbb{Z}^+$ *is such that*

1. $1 \in S$, *and*
2. *for every positive integer* n, *if* $1, 2, \ldots, n \in S$, *then* $n + 1 \in S$.
3. *Conclusion:* $S = \mathbb{Z}^+$.

Proof.

Suppose that $S \subseteq \mathbb{Z}^+$ satisfies (i) and (ii) above. Now let $T = \{n \in \mathbb{Z}^+ : 1, 2, \ldots, n \in S\}$. Let us show that T satisfies properties (i) and (ii) of 'regular induction'.

(i) (base case) We must show that $1 \in T$. Note by definition that this simply means that $1 \in S$, which is true by our assumption (i) above on S. □

Induction

Proof.

(ii) (inductive step) Now let n be any positive integer, and assume that $n \in T$.

Induction

Proof.

(ii) (inductive step) Now let n be any positive integer, and assume that $n \in T$. We will show that $n + 1 \in T$.

Induction

Proof.

(ii) (inductive step) Now let n be any positive integer, and assume that $n \in T$. We will show that $n+1 \in T$. Since $n \in T$, by definition of T, $1, 2, \ldots, n \in S$.

Induction

Proof.

(ii) (inductive step) Now let n be any positive integer, and assume that $n \in T$. We will show that $n+1 \in T$. Since $n \in T$, by definition of T, $1, 2, \ldots, n \in S$. By assumption (ii) on S, we see that $n+1 \in S$.

Induction

Proof.

(ii) (inductive step) Now let n be any positive integer, and assume that $n \in T$. We will show that $n+1 \in T$. Since $n \in T$, by definition of T, $1, 2, \ldots, n \in S$. By assumption (ii) on S, we see that $n+1 \in S$. So now $1, 2, \ldots, n, n+1 \in S$.

Induction

Proof.

(ii) (inductive step) Now let n be any positive integer, and assume that $n \in T$. We will show that $n+1 \in T$. Since $n \in T$, by definition of T, $1, 2, \ldots, n \in S$. By assumption (ii) on S, we see that $n+1 \in S$. So now $1, 2, \ldots, n, n+1 \in S$. This means that $n+1 \in T$.

Induction

Proof.

(ii) (inductive step) Now let n be any positive integer, and assume that $n \in T$. We will show that $n+1 \in T$. Since $n \in T$, by definition of T, $1, 2, \ldots, n \in S$. By assumption (ii) on S, we see that $n+1 \in S$. So now $1, 2, \ldots, n, n+1 \in S$. This means that $n+1 \in T$.

By the Principle of Induction, $T = \mathbb{Z}^+$.

Induction

Proof.

(ii) (inductive step) Now let n be any positive integer, and assume that $n \in T$. We will show that $n+1 \in T$. Since $n \in T$, by definition of T, $1, 2, \ldots, n \in S$. By assumption (ii) on S, we see that $n+1 \in S$. So now $1, 2, \ldots, n, n+1 \in S$. This means that $n+1 \in T$.

By the Principle of Induction, $T = \mathbb{Z}^+$. We want to show that $S = \mathbb{Z}^+$.

Induction

Proof.

(ii) (inductive step) Now let n be any positive integer, and assume that $n \in T$. We will show that $n+1 \in T$. Since $n \in T$, by definition of T, $1, 2, \ldots, n \in S$. By assumption (ii) on S, we see that $n+1 \in S$. So now $1, 2, \ldots, n, n+1 \in S$. This means that $n+1 \in T$.

By the Principle of Induction, $T = \mathbb{Z}^+$. We want to show that $S = \mathbb{Z}^+$. So let n be any positive integer.

Induction

Proof.

(ii) (inductive step) Now let n be any positive integer, and assume that $n \in T$. We will show that $n+1 \in T$. Since $n \in T$, by definition of T, $1, 2, \ldots, n \in S$. By assumption (ii) on S, we see that $n+1 \in S$. So now $1, 2, \ldots, n, n+1 \in S$. This means that $n+1 \in T$.

By the Principle of Induction, $T = \mathbb{Z}^+$. We want to show that $S = \mathbb{Z}^+$. So let n be any positive integer. Then $n \in T$.

Induction

Proof.

(ii) (inductive step) Now let n be any positive integer, and assume that $n \in T$. We will show that $n+1 \in T$. Since $n \in T$, by definition of T, $1, 2, \ldots, n \in S$. By assumption (ii) on S, we see that $n+1 \in S$. So now $1, 2, \ldots, n, n+1 \in S$. This means that $n+1 \in T$.

By the Principle of Induction, $T = \mathbb{Z}^+$. We want to show that $S = \mathbb{Z}^+$. So let n be any positive integer. Then $n \in T$. This means that $1, 2, \ldots, n \in S$, and so $n \in S$.

Induction

Proof.

(ii) (inductive step) Now let n be any positive integer, and assume that $n \in T$. We will show that $n+1 \in T$. Since $n \in T$, by definition of T, $1, 2, \ldots, n \in S$. By assumption (ii) on S, we see that $n+1 \in S$. So now $1, 2, \ldots, n, n+1 \in S$. This means that $n+1 \in T$.

By the Principle of Induction, $T = \mathbb{Z}^+$. We want to show that $S = \mathbb{Z}^+$. So let n be any positive integer. Then $n \in T$. This means that $1, 2, \ldots, n \in S$, and so $n \in S$. Hence $S = \mathbb{Z}^+$, as desired. $\square$

Induction

Proof.

(ii) (inductive step) Now let n be any positive integer, and assume that $n \in T$. We will show that $n+1 \in T$. Since $n \in T$, by definition of T, $1, 2, \ldots, n \in S$. By assumption (ii) on S, we see that $n+1 \in S$. So now $1, 2, \ldots, n, n+1 \in S$. This means that $n+1 \in T$.

By the Principle of Induction, $T = \mathbb{Z}^+$. We want to show that $S = \mathbb{Z}^+$. So let n be any positive integer. Then $n \in T$. This means that $1, 2, \ldots, n \in S$, and so $n \in S$. Hence $S = \mathbb{Z}^+$, as desired. □

Example

Show that for every integer $n \geq 2$, one can obtain n cents of postage using only 2 and 3 cent stamps.

Induction

Proof.

(ii) (inductive step) Now let n be any positive integer, and assume that $n \in T$. We will show that $n+1 \in T$. Since $n \in T$, by definition of T, $1, 2, \ldots, n \in S$. By assumption (ii) on S, we see that $n+1 \in S$. So now $1, 2, \ldots, n, n+1 \in S$. This means that $n+1 \in T$.

By the Principle of Induction, $T = \mathbb{Z}^+$. We want to show that $S = \mathbb{Z}^+$. So let n be any positive integer. Then $n \in T$. This means that $1, 2, \ldots, n \in S$, and so $n \in S$. Hence $S = \mathbb{Z}^+$, as desired. □

Example

Show that for every integer $n \geq 2$, one can obtain n cents of postage using only 2 and 3 cent stamps.

Proof.

In class. □

Induction

We can use the Principle of Strong Induction to prove the Well-Ordering Principle, the final equivalent form of Mathematical Induction.

Induction

We can use the Principle of Strong Induction to prove the Well-Ordering Principle, the final equivalent form of Mathematical Induction.

Theorem (Well-Ordering Principle)

Suppose that S is a nonempty subset of $\mathbb{Z}^+$.

Induction

We can use the Principle of Strong Induction to prove the Well-Ordering Principle, the final equivalent form of Mathematical Induction.

Theorem (Well-Ordering Principle)

Suppose that S is a nonempty subset of $\mathbb{Z}^+$. Then S has a least element (that is, a smallest element).

Induction

We can use the Principle of Strong Induction to prove the Well-Ordering Principle, the final equivalent form of Mathematical Induction.

Theorem (Well-Ordering Principle)

Suppose that S is a nonempty subset of $\mathbb{Z}^+$. Then S has a least element (that is, a smallest element).

Proof.

Suppose by way of contradiction that there exists a nonempty subset A of $\mathbb{Z}^+$ with no least element.

Induction

We can use the Principle of Strong Induction to prove the Well-Ordering Principle, the final equivalent form of Mathematical Induction.

Theorem (Well-Ordering Principle)

Suppose that S is a nonempty subset of $\mathbb{Z}^+$. Then S has a least element (that is, a smallest element).

Proof.

Suppose by way of contradiction that there exists a nonempty subset A of $\mathbb{Z}^+$ with no least element. Now let $S = \{n \in \mathbb{Z}^+ : n \notin A\}$.

Induction

We can use the Principle of Strong Induction to prove the Well-Ordering Principle, the final equivalent form of Mathematical Induction.

Theorem (Well-Ordering Principle)

Suppose that S is a nonempty subset of $\mathbb{Z}^+$. Then S has a least element (that is, a smallest element).

Proof.

Suppose by way of contradiction that there exists a nonempty subset A of $\mathbb{Z}^+$ with no least element. Now let $S = \{n \in \mathbb{Z}^+ : n \notin A\}$. We will use the Principle of Strong Induction to show that $S = \mathbb{Z}^+$.

Induction

We can use the Principle of Strong Induction to prove the Well-Ordering Principle, the final equivalent form of Mathematical Induction.

Theorem (Well-Ordering Principle)

Suppose that S is a nonempty subset of $\mathbb{Z}^+$. Then S has a least element (that is, a smallest element).

Proof.

Suppose by way of contradiction that there exists a nonempty subset A of $\mathbb{Z}^+$ with no least element. Now let $S = \{n \in \mathbb{Z}^+ : n \notin A\}$. We will use the Principle of Strong Induction to show that $S = \mathbb{Z}^+$.

(i) (base case) $1 \in S$:

Induction

We can use the Principle of Strong Induction to prove the Well-Ordering Principle, the final equivalent form of Mathematical Induction.

Theorem (Well-Ordering Principle)

Suppose that S is a nonempty subset of $\mathbb{Z}^+$. Then S has a least element (that is, a smallest element).

Proof.

Suppose by way of contradiction that there exists a nonempty subset A of $\mathbb{Z}^+$ with no least element. Now let $S = \{n \in \mathbb{Z}^+ : n \notin A\}$. We will use the Principle of Strong Induction to show that $S = \mathbb{Z}^+$.

(i) (base case) $1 \in S$: we must check that $1 \notin A$.

Induction

We can use the Principle of Strong Induction to prove the Well-Ordering Principle, the final equivalent form of Mathematical Induction.

Theorem (Well-Ordering Principle)

Suppose that S is a nonempty subset of $\mathbb{Z}^+$. Then S has a least element (that is, a smallest element).

Proof.

Suppose by way of contradiction that there exists a nonempty subset A of $\mathbb{Z}^+$ with no least element. Now let $S = \{n \in \mathbb{Z}^+ : n \notin A\}$. We will use the Principle of Strong Induction to show that $S = \mathbb{Z}^+$.

(i) (base case) $1 \in S$: we must check that $1 \notin A$. If $1 \in A$, then certainly 1 is the smallest member of A, since 1 is the smallest positive integer and A is a set of positive integers.

Induction

We can use the Principle of Strong Induction to prove the Well-Ordering Principle, the final equivalent form of Mathematical Induction.

Theorem (Well-Ordering Principle)

Suppose that S is a nonempty subset of $\mathbb{Z}^+$. Then S has a least element (that is, a smallest element).

Proof.

Suppose by way of contradiction that there exists a nonempty subset A of $\mathbb{Z}^+$ with no least element. Now let $S = \{n \in \mathbb{Z}^+ : n \notin A\}$. We will use the Principle of Strong Induction to show that $S = \mathbb{Z}^+$.

(i) (base case) $1 \in S$: we must check that $1 \notin A$. If $1 \in A$, then certainly 1 is the smallest member of A, since 1 is the smallest positive integer and A is a set of positive integers. But this contradicts our assumption that A has no least element. □

Induction

Proof.

(ii) (inductive step) Let n be an arbitrary positive integer, and assume that $1, 2, \ldots, n \in S$.

Induction

Proof.

(ii) (inductive step) Let n be an arbitrary positive integer, and assume that $1, 2, \ldots, n \in S$. We will show that $n + 1 \in S$.

Induction

Proof.

(ii) (inductive step) Let n be an arbitrary positive integer, and assume that $1, 2, \ldots, n \in S$. We will show that $n + 1 \in S$. Since $1, 2, \ldots, n \in S$, this means that

Induction

Proof.

(ii) (inductive step) Let n be an arbitrary positive integer, and assume that $1, 2, \ldots, n \in S$. We will show that $n + 1 \in S$. Since $1, 2, \ldots, n \in S$, this means that $1 \notin A, 2 \notin A, \ldots, n \notin A$.

Induction

Proof.

(ii) (inductive step) Let n be an arbitrary positive integer, and assume that $1, 2, \ldots, n \in S$. We will show that $n+1 \in S$. Since $1, 2, \ldots, n \in S$, this means that $1 \notin A, 2 \notin A, \ldots, n \notin A$. Note that if $n+1 \in A$, then $n+1$ would be the smallest member of A, a contradiction to our assumption.

Induction

Proof.

(ii) (inductive step) Let n be an arbitrary positive integer, and assume that $1, 2, \ldots, n \in S$. We will show that $n+1 \in S$. Since $1, 2, \ldots, n \in S$, this means that $1 \notin A, 2 \notin A, \ldots, n \notin A$. Note that if $n+1 \in A$, then $n+1$ would be the smallest member of A, a contradiction to our assumption. So by the Principle of Strong Induction, $S = \mathbb{Z}^+$.

Induction

Proof.

(ii) (inductive step) Let n be an arbitrary positive integer, and assume that $1, 2, \ldots, n \in S$. We will show that $n+1 \in S$. Since $1, 2, \ldots, n \in S$, this means that $1 \notin A, 2 \notin A, \ldots, n \notin A$. Note that if $n+1 \in A$, then $n+1$ would be the smallest member of A, a contradiction to our assumption. So by the Principle of Strong Induction, $S = \mathbb{Z}^+$.

So we have shown that NO positive integer is a member of A.

Induction

Proof.

(ii) (inductive step) Let n be an arbitrary positive integer, and assume that $1, 2, \ldots, n \in S$. We will show that $n+1 \in S$. Since $1, 2, \ldots, n \in S$, this means that $1 \notin A, 2 \notin A, \ldots, n \notin A$. Note that if $n+1 \in A$, then $n+1$ would be the smallest member of A, a contradiction to our assumption. So by the Principle of Strong Induction, $S = \mathbb{Z}^+$.

So we have shown that NO positive integer is a member of A. This contradicts that A is *nonempty* and completes the proof. □

Induction

Proof.

(ii) (inductive step) Let n be an arbitrary positive integer, and assume that $1, 2, \ldots, n \in S$. We will show that $n+1 \in S$. Since $1, 2, \ldots, n \in S$, this means that $1 \notin A, 2 \notin A, \ldots, n \notin A$. Note that if $n+1 \in A$, then $n+1$ would be the smallest member of A, a contradiction to our assumption. So by the Principle of Strong Induction, $S = \mathbb{Z}^+$.

So we have shown that NO positive integer is a member of A. This contradicts that A is *nonempty* and completes the proof. □

Example

Show that there is no positive integer n such that $0 < n < 1$.

Induction

Proof.

(ii) (inductive step) Let n be an arbitrary positive integer, and assume that $1, 2, \ldots, n \in S$. We will show that $n+1 \in S$. Since $1, 2, \ldots, n \in S$, this means that $1 \notin A, 2 \notin A, \ldots, n \notin A$. Note that if $n+1 \in A$, then $n+1$ would be the smallest member of A, a contradiction to our assumption. So by the Principle of Strong Induction, $S = \mathbb{Z}^+$.

So we have shown that NO positive integer is a member of A. This contradicts that A is *nonempty* and completes the proof. □

Example

Show that there is no positive integer n such that $0 < n < 1$.

Proof.

In class. □

Induction

Proof.

(ii) (inductive step) Let n be an arbitrary positive integer, and assume that $1, 2, \ldots, n \in S$. We will show that $n+1 \in S$. Since $1, 2, \ldots, n \in S$, this means that $1 \notin A, 2 \notin A, \ldots, n \notin A$. Note that if $n+1 \in A$, then $n+1$ would be the smallest member of A, a contradiction to our assumption. So by the Principle of Strong Induction, $S = \mathbb{Z}^+$.

So we have shown that NO positive integer is a member of A. This contradicts that A is *nonempty* and completes the proof. □

Example

Show that there is no positive integer n such that $0 < n < 1$.

Proof.

In class. □

Division Algorithm

You may recall from elementary school the process of dividing a positive integer by another positive integer to produce a **quotient** and a **remainder**.

Division Algorithm

You may recall from elementary school the process of dividing a positive integer by another positive integer to produce a **quotient** and a **remainder**.

Example

Note that 3 'goes into' 17 five times (so five is the quotient) with a remainder of two.

Division Algorithm

You may recall from elementary school the process of dividing a positive integer by another positive integer to produce a **quotient** and a **remainder**.

Example

Note that 3 'goes into' 17 five times (so five is the quotient) with a remainder of two.

Can one always divide an integer by a positive (more on this later) integer to produce a quotient and a remainder?

Division Algorithm

You may recall from elementary school the process of dividing a positive integer by another positive integer to produce a **quotient** and a **remainder**.

Example

Note that 3 'goes into' 17 five times (so five is the quotient) with a remainder of two.

Can one always divide an integer by a positive (more on this later) integer to produce a quotient and a remainder? How exactly do we rigorously define 'quotient' and 'remainder'?

Division Algorithm

You may recall from elementary school the process of dividing a positive integer by another positive integer to produce a **quotient** and a **remainder**.

Example

Note that 3 'goes into' 17 five times (so five is the quotient) with a remainder of two.

Can one always divide an integer by a positive (more on this later) integer to produce a quotient and a remainder? How exactly do we rigorously define 'quotient' and 'remainder'?And are the quotient and remainder (once they have been defined) unique?

Division Algorithm

You may recall from elementary school the process of dividing a positive integer by another positive integer to produce a **quotient** and a **remainder**.

Example

Note that 3 'goes into' 17 five times (so five is the quotient) with a remainder of two.

Can one always divide an integer by a positive (more on this later) integer to produce a quotient and a remainder? How exactly do we rigorously define 'quotient' and 'remainder'?And are the quotient and remainder (once they have been defined) unique? Our next job is to answer the above questions.

Division Algorithm

You may recall from elementary school the process of dividing a positive integer by another positive integer to produce a **quotient** and a **remainder**.

Example

Note that 3 'goes into' 17 five times (so five is the quotient) with a remainder of two.

Can one always divide an integer by a positive (more on this later) integer to produce a quotient and a remainder? How exactly do we rigorously define 'quotient' and 'remainder'?And are the quotient and remainder (once they have been defined) unique? Our next job is to answer the above questions. We will conclude today with a lemma in this direction.

Division Algorithm

You may recall from elementary school the process of dividing a positive integer by another positive integer to produce a **quotient** and a **remainder**.

Example

Note that 3 'goes into' 17 five times (so five is the quotient) with a remainder of two.

Can one always divide an integer by a positive (more on this later) integer to produce a quotient and a remainder? How exactly do we rigorously define 'quotient' and 'remainder'?And are the quotient and remainder (once they have been defined) unique? Our next job is to answer the above questions. We will conclude today with a lemma in this direction.

Division Algorithm

Lemma

Let m be an integer and let n be a positive integer.

Division Algorithm

Lemma

Let m be an integer and let n be a positive integer. Now let $S = \{m - nx : x \in \mathbb{Z} \text{ and } m - nx \geq 0\}$.

Division Algorithm

Lemma

Let m be an integer and let n be a positive integer. Now let $S = \{m - nx : x \in \mathbb{Z} \text{ and } m - nx \geq 0\}$. Then S has a least element.

Division Algorithm

Lemma

Let m be an integer and let n be a positive integer. Now let $S = \{m - nx : x \in \mathbb{Z} \text{ and } m - nx \geq 0\}$. Then S has a least element.

Proof.

Let m, n, and S be as defined above.

Division Algorithm

Lemma

Let m be an integer and let n be a positive integer. Now let $S = \{m - nx : x \in \mathbb{Z} \text{ and } m - nx \geq 0\}$. Then S has a least element.

Proof.

Let m, n, and S be as defined above. Note by definition that $S \subseteq \mathbb{N}$.

Division Algorithm

Lemma

Let m be an integer and let n be a positive integer. Now let $S = \{m - nx : x \in \mathbb{Z} \text{ and } m - nx \geq 0\}$. Then S has a least element.

Proof.

Let m, n, and S be as defined above. Note by definition that $S \subseteq \mathbb{N}$. So by (a slightly more general version of) the Well-Ordering Principle, as long as S is nonempty, then S has a least element.

Division Algorithm

Lemma

Let m be an integer and let n be a positive integer. Now let $S = \{m - nx : x \in \mathbb{Z} \text{ and } m - nx \geq 0\}$. Then S has a least element.

Proof.

Let m, n, and S be as defined above. Note by definition that $S \subseteq \mathbb{N}$. So by (a slightly more general version of) the Well-Ordering Principle, as long as S is nonempty, then S has a least element. So all we have to do is show that there is some integer x such that $m - nx \geq 0$, that is, $nx \leq m$.

Division Algorithm

Lemma

Let m be an integer and let n be a positive integer. Now let $S = \{m - nx : x \in \mathbb{Z} \text{ and } m - nx \geq 0\}$. Then S has a least element.

Proof.

Let m, n, and S be as defined above. Note by definition that $S \subseteq \mathbb{N}$. So by (a slightly more general version of) the Well-Ordering Principle, as long as S is nonempty, then S has a least element. So all we have to do is show that there is some integer x such that $m - nx \geq 0$, that is, $nx \leq m$. But this is equivalent to the existence of an integer x such that $x \leq \frac{m}{n}$.

Division Algorithm

Lemma

Let m be an integer and let n be a positive integer. Now let $S = \{m - nx : x \in \mathbb{Z} \text{ and } m - nx \geq 0\}$. Then S has a least element.

Proof.

Let m, n, and S be as defined above. Note by definition that $S \subseteq \mathbb{N}$. So by (a slightly more general version of) the Well-Ordering Principle, as long as S is nonempty, then S has a least element. So all we have to do is show that there is some integer x such that $m - nx \geq 0$, that is, $nx \leq m$. But this is equivalent to the existence of an integer x such that $x \leq \frac{m}{n}$. For every real number r, there is an integer $x \leq r$, so this proves it. $\square$