Math 245: Discrete Mathematics

Sequences and Mathematical Induction

Mathematical Induction

Lecture Notes #8

Peter Blomgren
Department of Mathematics and Statistics
San Diego State University
San Diego, CA 92182-7720
`blomgren@terminus.SDSU.EDU`
`http://terminus.SDSU.EDU`

$Id: lecture.tex,v 1.8 2006/10/24 19:53:21 blomgren Exp $

Last Time: Sequences

Last time we talked about sequences, and introduced quite a bit of terminology. Some new words in our vocabulary:

sequence A list of elements (numbers) arranged in a linear fashion; such that each member comes either before, or after, every other member, and the order of members is important.

term An individual element a_k in a sequence.

index The index / subscript k in the term a_k. It indicates the the term's location in the sequence.

initial term The term in a sequence with the lowest index.

finite sequence A sequence with a finite number of terms.

infinite sequence A sequence with infinitely many terms.

final term In a finite sequence, the term with the largest index.

explicit formula An expression for the terms a_k, using k only. (No dependence on preceding terms.) [also: General Formula].

Sequences: The Collatz Conjecture 1 of 2

Consider the following sequence: *Given an initial term $a_1 \in \mathbb{Z}^+$, we define the rest of the sequence as follows:*

$$a_{n+1} = \begin{cases} a_n/2 & \text{if } a_n \text{ is even} \\ 3a_n + 1 & \text{if } a_n \text{ is odd} \end{cases}$$

We notice that if $a_k = 1$, then

$$a_{k+1} = 4, \quad a_{k+2} = 2, \quad a_{k+3} = 1$$

and we end up ***cycling*** through the values {1,4,2} forever.

In 1937 L. Collatz conjectured "$\forall a_1 \in \mathbb{Z}^+$, *the sequence will reach the {1,4,2}-cycle.*"

The proof is left as a homework exercise... (Not!)

Sequences: The Collatz Conjecture 2 of 2

The Collatz conjecture is another example of a mathematical question that is easy to ask (it almost ***looks*** like a homework / test problem), but very hard to answer.

There is still no proof (or counter-example) to the conjecture.

In 1972 H. Conway (Princeton) showed *"if the sequence enters into another cycle, that cycle must have at least 400 different numbers."*

In 1985 J.C. Lagarias extended the bound from 400 to 275,000.

In 1999 Tomás Oliveira e Silva showed (using a computer) that the Collatz conjecture is true for starting values less than $2.7 \cdot 10^{16}$.

2005 (March) Eric Roosendaal (and collaborators) have independently checked up to $322 \cdot 2^{50}$.

2006 (May) $10 \cdot 2^{58}$...

Web references: (http://www-personal.ksu.edu/∼kconrow/allgifs.html)
(http://www.ieeta.pt/∼tos/3x+1.html)

Mathematical Induction: Introduction

Mathematical Induction is a ***proof technique*** used to validate conjectures about statements that follow definite sequential patterns.

Brief history:

The first known use of mathematical induction: Francesco Maurolico (1575); In the 17th century Pierre de Fermat ("the Fermat") and Blaise Pascal (you may recall Pascal's Triangle?) used the technique. Augustus De Morgan (remember his laws for logic?) gave mathematical induction its name and described the process rigorously (1883).

The Idea (informally):

If we ***know*** how to solve a problem (prove a statement) of size k, **and** we can use that knowledge to solve a problem of size $k+1$, **and** we can solve a problem of a particular size, *e.g.* $k = 1$, **then** we can solve a problem of any size.

Mathematical Induction — Formal Statement

The Principle of Mathematical Induction:

Let $P(n)$ be a predicate that is defined for integers n, and let a be a fixed integer. Suppose the following two statements are true:

1. $P(a)$ is true.

2. For all integers $k \geq a$, if $P(k)$ is true, then $P(k+1)$ is true, *i.e.*

$$\forall k \in \mathbb{Z}, k \geq a,\ P(k) \Rightarrow P(k+1)$$

Then the statement

$$\forall n \geq a, P(n)$$

is true.

2. is referred to as the ***inductive hypothesis.***

Mathematical Induction Another View

Connecting to our logic "toolbox" we can think of the second supposition as a chain of implications:

$$\cdots \Rightarrow P(k) \Rightarrow P(k+1) \Rightarrow P(k+2) \Rightarrow \cdots \Rightarrow P(k+n) \Rightarrow \cdots$$

Connecting to our logic "toolbox" we can think of the second supposition as a chain of implications:

$$\cdots \Rightarrow P(k) \Rightarrow P(k+1) \Rightarrow P(k+2) \Rightarrow \cdots \Rightarrow P(k+n) \Rightarrow \cdots$$

We use the first supposition (that $P(a)$ is true for a particular a) and ***Universal Modus Ponens*** to show:

$$\begin{array}{ll} & \forall k \in \mathbb{Z},\ P(k) \Rightarrow P(k+1) \\ & P(a), \text{ for a particular } a \in \mathbb{Z} \\ \therefore & P(a+1) \end{array}$$

Mathematical Induction Another View

Connecting to our logic "toolbox" we can think of the second supposition as a chain of implications:

$$\cdots \Rightarrow P(k) \Rightarrow P(k+1) \Rightarrow P(k+2) \Rightarrow \cdots \Rightarrow P(k+n) \Rightarrow \cdots$$

We use the first supposition (that $P(a)$ is true for a particular a) and ***Universal Modus Ponens*** to show:

$$\begin{array}{rl} & \forall k \in \mathbb{Z},\ P(k) \Rightarrow P(k+1) \\ & P(a), \text{ for a particular } a \in \mathbb{Z} \\ \therefore & P(a+1) \end{array}$$

Now that we have established that $P(a+1)$ is true, we can use ***Universal Modus Ponens*** again:

$$\begin{array}{rl} & \forall k \in \mathbb{Z},\ P(k) \Rightarrow P(k+1) \\ & P(a+1), \text{ for a particular } a \in \mathbb{Z} \\ \therefore & P(a+2) \end{array}$$

And so it goes forever.....

To prove something by mathematical induction:

Step 1: [The ***basis step*** step]
First, prove that $P(a)$ is true for a particular integer a.

Step 2: [The ***inductive step***]
Prove for all integers $k \geq a$: if $P(k)$ is true, then $P(k+1)$ is true.

To show the inductive step correctly, we assume that k ***is a particular, but arbitrarily chosen*** integer greater than or equal to a. — We use the method of *"generalizing from the generic particular."*

Examples!!! — Making Change 1 of 2

Scenario: In its infinite wisdom, the Federal Reserve has decided to stop making pennies (1¢ coins) and have introduced a 2¢ coin (featuring a famous mathematician?) People are worried that they will no longer be able to get correct change – it turns out we can give correct change except for 1¢ and 3¢...

Proposition: ***Giving Change*** —
Let $P(n)$ be the property "n¢ can be obtained using 2¢ and 5¢ coins." Then $P(n)$ is true for all integers $n \geq 4$.

Proof:

Examples!!! — Making Change 1 of 2

Scenario: In its infinite wisdom, the Federal Reserve has decided to stop making pennies (1¢ coins) and have introduced a 2¢ coin (featuring a famous mathematician?) People are worried that they will no longer be able to get correct change – it turns out we can give correct change except for 1¢ and 3¢...

Proposition: ***Giving Change*** —
Let $P(n)$ be the property "n¢ can be obtained using 2¢ and 5¢ coins." Then $P(n)$ is true for all integers $n \geq 4$.

Proof:

Step 1 The property is true for $n = 4$, since 4¢ = 2¢ + 2¢.

Examples!!! — Making Change 2 of 2

Proposition: ***Giving Change* —**
Let $P(n)$ be the property "n¢ can be obtained using 2¢ and 5¢ coins." Then $P(n)$ is true for all integers $n \geq 4$.

Proof:

Step 1 The property is true for $n = 4$, since 4¢ = 2¢ + 2¢.

Examples!!! — Making Change 2 of 2

Proposition: ***Giving Change*** —
Let $P(n)$ be the property "n¢ can be obtained using 2¢ and 5¢ coins." Then $P(n)$ is true for all integers $n \geq 4$.

Proof:

Step 1 The property is true for $n = 4$, since 4¢ = 2¢ + 2¢.

Step 2 Suppose $P(k)$ is true, *i.e.* k¢ can be obtained using 2¢ and 5¢ coins for some integer $k \geq 4$. We have 2 cases:

Examples!!! — Making Change 2 of 2

Proposition: ***Giving Change*** —
Let $P(n)$ be the property "n¢ can be obtained using 2¢ and 5¢ coins." Then $P(n)$ is true for all integers $n \geq 4$.

Proof:

Step 1 The property is true for $n = 4$, since 4¢ = 2¢ + 2¢.

Step 2 Suppose $P(k)$ is true, *i.e.* k¢ can be obtained using 2¢ and 5¢ coins for some integer $k \geq 4$. We have 2 cases:

1: In this case, we have at least one 5¢ coin among the ones that make up k¢. Replace it by three 2¢ coins, and the result is correct change for $(k+1)$¢.

Examples!!! — Making Change 2 of 2

Proposition: ***Giving Change* —**
Let $P(n)$ be the property "n¢ can be obtained using 2¢ and 5¢ coins." Then $P(n)$ is true for all integers $n \geq 4$.

Proof:

Step 1 The property is true for $n = 4$, since 4¢ = 2¢ + 2¢.

Step 2 Suppose $P(k)$ is true, *i.e.* k¢ can be obtained using 2¢ and 5¢ coins for some integer $k \geq 4$. We have 2 cases:

1: In this case, we have at least one 5¢ coin among the ones that make up k¢. Replace it by three 2¢ coins, and the result is correct change for $(k+1)$¢.

2: In this case, we have no 5¢ coin among the ones that make up k¢. However, since $k \geq 4$ we must have at least two 2¢ coins; replace two 2¢ coins by a 5¢ coin, and the result is correct change for $(k+1)$¢.

Examples!!! — Making Change 2 of 2

Proposition: ***Giving Change*** —
Let $P(n)$ be the property "n¢ can be obtained using 2¢ and 5¢ coins." Then $P(n)$ is true for all integers $n \geq 4$.

Proof:

Step 1 The property is true for $n = 4$, since 4¢ = 2¢ + 2¢.

Step 2 Suppose $P(k)$ is true, *i.e.* k¢ can be obtained using 2¢ and 5¢ coins for some integer $k \geq 4$. We have 2 cases:

1: In this case, we have at least one 5¢ coin among the ones that make up k¢. Replace it by three 2¢ coins, and the result is correct change for $(k+1)$¢.

2: In this case, we have no 5¢ coin among the ones that make up k¢. However, since $k \geq 4$ we must have at least two 2¢ coins; replace two 2¢ coins by a 5¢ coin, and the result is correct change for $(k+1)$¢.

Thus in either case, we can make correct change for $(k+1)$¢. □

Example: $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ 1 of 2

Proposition: $\forall n \in \mathbb{Z},\ n \geq 1, \quad \displaystyle\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$

Proof:

Example: $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ 1 of 2

Proposition: $\forall n \in \mathbb{Z}$, $n \geq 1$, $\displaystyle\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Proof:

Basis Step: For $n = 1$: $1 = \frac{1(1+1)}{2} = \frac{2}{2} = 1$.

Example: $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ 1 of 2

Proposition: $\forall n \in \mathbb{Z},\, n \geq 1, \quad \displaystyle\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$

Proof:

Basis Step: For $n = 1$: $1 = \frac{1(1+1)}{2} = \frac{2}{2} = 1.$

Inductive: Suppose the formula is true for $n = m$, *i.e.*

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

Example: $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ 1 of 2

Proposition: $\forall n \in \mathbb{Z},\ n \geq 1, \quad \displaystyle\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$

Proof:

Basis Step: For $n = 1$: $1 = \frac{1(1+1)}{2} = \frac{2}{2} = 1.$

Inductive: Suppose the formula is true for $n = m$, *i.e.*

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

Now, for $n = (m+1)$ we have

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

[continued...]

Example: $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ 2 of 2

We have:

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

A little bit of algebra —

$$\begin{aligned}
\sum_{k=1}^{m+1} k &= \frac{m(m+1)}{2} + (m+1) \\
&= \frac{m(m+1)}{2} + \frac{2(m+1)}{2} \\
&= \frac{m(m+1) + 2(m+1)}{2} \\
&= \frac{(m+2)(m+1)}{2} = \frac{(m+1)(m+2)}{2}
\end{aligned}$$

This shows that $P(m) \Rightarrow P(m+1)$.

Since we have proved both the basis and inductive steps, the conclude that the proposition is true. □

A Tall Tale about $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$?

Disclaimer: *This is the way I heard the story...*

Carl Friedrich Gauss (1777–1855), one of the most prominent mathematicians in history, was given the task to sum up all integers from 1 to 100 by his teacher. — Supposedly to keep this smart/annoying student quiet for a while.

Gauss quickly come up with the answer: 5,050.

He deduced the formula we just proved by pairing numbers (or folding the sequence):

1	2	3	$\cdots$	49	50
100	99	98	$\cdots$	52	51

50 pairs, each with a sum of 101 $\Rightarrow 50 \cdot 101 = 5,050$.
Here, of course $50 = n/2$, and $101 = (n+1)$.

Example: Geometric Sums 1 of 2

Proposition: For any real number $r \neq 1$, and any non-negative integer n,

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}.$$

Proof:

Example: Geometric Sums 1 of 2

Proposition: For any real number $r \neq 1$, and any non-negative integer n,

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}.$$

Proof: Suppose r is a particular but arbitrarily chosen real number not equal to 1.

Example: Geometric Sums 1 of 2

Proposition: For any real number $r \neq 1$, and any non-negative integer n,

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}.$$

Proof: Suppose r is a particular but arbitrarily chosen real number not equal to 1.

Basis: For $n = 0$ we have:

$$1 = r^0 = \sum_{i=0}^{0} r^i = \frac{r^{0+1} - 1}{r - 1} = \frac{r - 1}{r - 1} = 1.$$

Hence the formula is true for $n = 0$.

Example: The Sum of a Geometric Sum 2 of 2

Inductive: Suppose the formula is true for $n = k$, *i.e.* for $k \geq 0$

$$\sum_{i=0}^{k} r^i = \frac{r^{k+1} - 1}{r - 1}.$$

Example: The Sum of a Geometric Sum 2 of 2

Inductive: Suppose the formula is true for $n = k$, *i.e.* for $k \geq 0$

$$\sum_{i=0}^{k} r^i = \frac{r^{k+1} - 1}{r - 1}.$$

Now

$$\begin{aligned}
\sum_{i=0}^{k+1} r^i &= \frac{r^{k+1} - 1}{r - 1} + r^{k+1} = \frac{r^{k+1} - 1}{r - 1} + \frac{r^{k+1}(r - 1)}{r - 1} \\
&= \frac{\mathbf{r^{k+1}} - 1 + r^{k+2} \mathbf{- r^{k+1}}}{r - 1} = \frac{r^{k+2} - 1}{r - 1}
\end{aligned}$$

Example: The Sum of a Geometric Sum 2 of 2

Inductive: Suppose the formula is true for $n = k$, *i.e.* for $k \geq 0$

$$\sum_{i=0}^{k} r^i = \frac{r^{k+1} - 1}{r - 1}.$$

Now

$$\begin{aligned} \sum_{i=0}^{k+1} r^i &= \frac{r^{k+1} - 1}{r - 1} + r^{k+1} = \frac{r^{k+1} - 1}{r - 1} + \frac{r^{k+1}(r-1)}{r - 1} \\ &= \frac{\mathbf{r^{k+1}} - 1 + r^{k+2} \mathbf{- r^{k+1}}}{r - 1} = \frac{r^{k+2} - 1}{r - 1} \end{aligned}$$

This proves the inductive step $P(k) \Rightarrow P(k+1)$.

Example: The Sum of a Geometric Sum 2 of 2

Inductive: Suppose the formula is true for $n = k$, *i.e.* for $k \geq 0$

$$\sum_{i=0}^{k} r^i = \frac{r^{k+1} - 1}{r - 1}.$$

Now

$$\begin{aligned}
\sum_{i=0}^{k+1} r^i &= \frac{r^{k+1} - 1}{r - 1} + r^{k+1} = \frac{r^{k+1} - 1}{r - 1} + \frac{r^{k+1}(r - 1)}{r - 1} \\
&= \frac{\mathbf{r}^{\mathbf{k+1}} - 1 + r^{k+2} \mathbf{-} \mathbf{r}^{\mathbf{k+1}}}{r - 1} = \frac{r^{k+2} - 1}{r - 1}
\end{aligned}$$

This proves the inductive step $P(k) \Rightarrow P(k+1)$.

Together, the basis step and the inductive step show that the proposition is true. $\square$

Example: $\forall n \in \mathbb{Z}^+,\ 3 \,|\, (2^{2n} - 1)$ 1 of 2

Proposition: $\forall$ integers $n \geq 1$, $(2^{2n} - 1)$ is divisible by 3.

Proof:

Example: $\forall n \in \mathbb{Z}^+,\ 3 \,|\, (2^{2n} - 1)$ 1 of 2

Proposition: $\forall$ integers $n \geq 1$, $(2^{2n} - 1)$ is divisible by 3.

Proof: ***Basis step***, $n = 1$ — The statement is true for $n = 1$ since

$$2^{2 \cdot 1} - 1 = 2^2 - 1 = 4 - 1 = 3 = 3 \cdot 1.$$

Example: $\forall n \in \mathbb{Z}^+,\ 3 \mid (2^{2n} - 1)$ 1 of 2

Proposition: $\forall$ integers $n \geq 1$, $(2^{2n} - 1)$ is divisible by 3.

Proof: ***Basis step***, $n = 1$ — The statement is true for $n = 1$ since

$$2^{2\cdot 1} - 1 = 2^2 - 1 = 4 - 1 = 3 = 3 \cdot 1.$$

Inductive step: Suppose $2^{2k} - 1$ is divisible by 3. (THE INDUCTIVE HYPOTHESIS) — Then,

$$2^{2(k+1)} - 1 = 2^{2k+2} - 1 = 2^2 \cdot 2^{2k} - 1 = 4 \cdot 2^{2k} - 1$$

$$= 3 \cdot 2^{2k} + (2^{2k} - 1) = \{\text{by assumption, for some integer } m\}$$

$$= 3 \cdot 2^{2k} + 3 \cdot m = 3 \cdot \underbrace{(2^{2k} + m)}_{\text{an integer}}$$

Example: $\forall n \in \mathbb{Z}^+,\ 3 \,|\, (2^{2n} - 1)$ 1 of 2

Proposition: $\forall$ integers $n \geq 1$, $(2^{2n} - 1)$ is divisible by 3.

Proof: ***Basis step***, $n = 1$ — The statement is true for $n = 1$ since

$$2^{2\cdot 1} - 1 = 2^2 - 1 = 4 - 1 = 3 = 3 \cdot 1.$$

Inductive step: Suppose $2^{2k} - 1$ is divisible by 3. (The Inductive Hypothesis) — Then,

$$2^{2(k+1)} - 1 = 2^{2k+2} - 1 = 2^2 \cdot 2^{2k} - 1 = 4 \cdot 2^{2k} - 1$$

$$= 3 \cdot 2^{2k} + (2^{2k} - 1) = \{\text{by assumption, for some integer } m\}$$

$$= 3 \cdot 2^{2k} + 3 \cdot m = 3 \cdot \underbrace{(2^{2k} + m)}_{\text{an integer}}$$

This shows that $(2^{2(k+1)} - 1)$ is divisible by 3. Together the basis step and the inductive step show that the proposition is true. □

Example: $\forall n \in \mathbb{Z},\ n \geq 3,\ (2n+1) < 2^n$

Proposition: $\forall$ integers $n \geq 3$, $(2n+1) < 2^n$.

Proof:

Example: $\forall n \in \mathbb{Z},\ n \geq 3,\ (2n+1) < 2^n$

Proposition: $\forall$ integers $n \geq 3$, $(2n+1) < 2^n$.

Proof: ***Basis step***, the inequality is true for $n = 3$ since

$$(2 \cdot 3 + 1) = 7 < 8 = 2^3.$$

Example: $\forall n \in \mathbb{Z},\ n \geq 3,\ (2n+1) < 2^n$

Proposition: $\forall$ integers $n \geq 3$, $(2n+1) < 2^n$.

Proof: ***Basis step***, the inequality is true for $n = 3$ since

$$(2 \cdot 3 + 1) = 7 < 8 = 2^3.$$

Inductive step: Suppose $(2k+1) < 2^k$ for some integer $k \geq 3$ (THE INDUCTIVE HYPOTHESIS). [WE MUST SHOW $(2(k+1)+1) < 2^{k+1}$]

Example: $\forall n \in \mathbb{Z},\ n \geq 3,\ (2n+1) < 2^n$

Proposition: $\forall$ integers $n \geq 3$, $(2n+1) < 2^n$.

Proof: ***Basis step***, the inequality is true for $n = 3$ since

$$(2 \cdot 3 + 1) = 7 < 8 = 2^3.$$

Inductive step: Suppose $(2k+1) < 2^k$ for some integer $k \geq 3$ (The Inductive Hypothesis). [We must show $(2(k+1)+1) < 2^{k+1}$]

$$\begin{aligned} 2(k+1)+1 &= (2k+1)+2 \\ &< 2^k + 2, && \text{by the hypothesis} \\ &< 2^k + 2^k, && \text{since } 2 < 2^k,\ k > 1 \\ &= 2 \cdot 2^k = 2^{k+1} \end{aligned}$$

Example: $\forall n \in \mathbb{Z},\ n \geq 3,\ (2n+1) < 2^n$

Proposition: $\forall$ integers $n \geq 3$, $(2n+1) < 2^n$.

Proof: ***Basis step***, the inequality is true for $n = 3$ since

$$(2 \cdot 3 + 1) = 7 < 8 = 2^3.$$

Inductive step: Suppose $(2k+1) < 2^k$ for some integer $k \geq 3$ (THE INDUCTIVE HYPOTHESIS). [WE MUST SHOW $(2(k+1)+1) < 2^{k+1}$]

$$\begin{aligned} 2(k+1)+1 &= (2k+1)+2 \\ &< 2^k + 2, && \text{by the hypothesis} \\ &< 2^k + 2^k, && \text{since } 2 < 2^k,\ k > 1 \\ &= 2 \cdot 2^k = 2^{k+1} \end{aligned}$$

This is what we needed to show. Basis & Inductive steps prove that the proposition is true. □

Mathematical Induction — Summary

To show something by mathematical induction: —

1. Show that the statement ($P(n)$) is true for the basis case $P(a)$, where a is a particular integer.

2. Assume that $P(k)$ is true for some integer k, show that $P(k+1)$ is true.

Together ***1*** and **2** show that $P(n)$ is true for $n \geq a$.

"Mathematics is not a spectator sport"

(Stanley Osher, Professor of Mathematics, UCLA)

$\Rightarrow$ **Homework follows!**

Next: ***Strong mathematical induction*** and the ***well-ordering principle***.

Homework #7 — Due Friday 11/3/2006, 12noon, GMCS-587 Version $\frac{1}{2}$

(Epp v3.0)

Epp-4.2.1, ***Epp-4.2.3***, ***Epp-4.2.10***, ***Epp-4.2.31***

(Epp v2.0)

Epp-4.2.1, ***Epp-4.2.3***, ***Epp-4.2.9***, ***Epp-4.2.28***

Recap... — Mathematical Induction

We started talking about ***the principle of mathematical induction***.

The typical use of the principle is when we want to show that a particular predicate $P(n)$ is ***true*** for all integers n greater than some lowest integer a.

The first step is to show that the predicate is indeed ***true*** for a, *i.e.* we check the ***basis case*** $P(a)$.

The second step (***inductive step***) involves showing that if we assume that $P(k)$ is ***true*** for some $k \geq a$, then $P(k+1)$ must also be ***true*** (by known theorems, definitions, algebra, and laws of logic).

Together these two steps show that $P(k)$ is ***true*** $\forall k \geq a$.

Revisited Example: $\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$ 1 of 3

Proposition: $\forall n \in \mathbb{Z},\, n \geq 1,\, \displaystyle\sum_{j=1}^{n} j = \frac{n(n+1)}{2}.$

We have already proved this... But let's revisit the proof and try to add some extra clarity!

Proof:

[First we must show the basis case, *i.e* that the formula is true for $n = 1$.]

Revisited Example: $\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$ 1 of 3

Proposition: $\forall n \in \mathbb{Z}$, $n \geq 1$, $\displaystyle\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$.

We have already proved this... But let's revisit the proof and try to add some extra clarity!

Proof:

[First we must show the basis case, *i.e* that the formula is true for $n = 1$.]

Basis Step: For $n = 1$:

$$\sum_{j=1}^{1} j = 1, \quad \text{and} \quad \frac{1 \cdot 2}{2} = 1$$

so, the formula holds for $n = 1$.

Revisited Example: $\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$ 2 of 3

Proposition: $\forall n \in \mathbb{Z},\ n \geq 1,\ \sum_{j=1}^{n} j = \frac{n(n+1)}{2}.$

Proof Continued:

[Next we must show that assuming $P(k)$ holds, then $P(k+1)$ holds.]

Revisited Example: $\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$ 2 of 3

Proposition: $\forall n \in \mathbb{Z},\ n \geq 1,\ \displaystyle\sum_{j=1}^{n} j = \frac{n(n+1)}{2}.$

Proof Continued:

[Next we must show that assuming $P(k)$ holds, then $P(k+1)$ holds.]

Inductive: Suppose the formula is true for $n = k$, *i.e.*

$$\sum_{j=1}^{k} j = \mathbf{1} + \mathbf{2} + \ldots + (\mathbf{k} - \mathbf{1}) + \mathbf{k} = \frac{k(k+1)}{2}.$$

Revisited Example: $\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$

Proposition: $\forall n \in \mathbb{Z},\ n \geq 1,\ \sum_{j=1}^{n} j = \frac{n(n+1)}{2}.$

Proof Continued:

[Next we must show that assuming $P(k)$ holds, then $P(k+1)$ holds.]

Inductive: Suppose the formula is true for $n = k$, *i.e.*

$$\sum_{j=1}^{k} j = \mathbf{1} + \mathbf{2} + \ldots + (\mathbf{k} - \mathbf{1}) + \mathbf{k} = \frac{k(k+1)}{2}.$$

Now, for $n = (k+1)$ we have

$$\sum_{j=1}^{k+1} j = \underbrace{\mathbf{1} + \mathbf{2} + \ldots + (\mathbf{k} - \mathbf{1}) + \mathbf{k}}_{\text{We know/assume this from } n = k} + (\mathbf{k} + \mathbf{1}) = \underbrace{\frac{\mathbf{k}(\mathbf{k}+\mathbf{1})}{\mathbf{2}}}_{\text{known/assumed}} + (\mathbf{k} + \mathbf{1}).$$

Revisited Example: $\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$ 3 of 3

At this point, we ***know***: $\displaystyle\sum_{j=1}^{k+1} j = \frac{k(k+1)}{2} + (k+1).$

[Our goal is to show that $\displaystyle\sum_{j=1}^{k+1} j = \frac{(k+1)(k+2)}{2}.$]

Revisited Example: $\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$ 3 of 3

At this point, we ***know***: $\displaystyle\sum_{j=1}^{k+1} j = \frac{k(k+1)}{2} + (k+1).$

[Our goal is to show that $\displaystyle\sum_{j=1}^{k+1} j = \frac{(k+1)(k+2)}{2}.$]

A little bit of algebra —

$$\begin{aligned}\sum_{j=1}^{k+1} j &= \frac{k(k+1)}{2} + (k+1) &&= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\ &= \frac{k(k+1)+2(k+1)}{2} &&= \frac{(k+2)(k+1)}{2} = \mathbf{\frac{(k+1)(k+2)}{2}}.\end{aligned}$$

Revisited Example: $\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$ 3 of 3

At this point, we ***know***: $\displaystyle\sum_{j=1}^{k+1} j = \frac{k(k+1)}{2} + (k+1).$

[Our goal is to show that $\displaystyle\sum_{j=1}^{k+1} j = \frac{(k+1)(k+2)}{2}.$]

A little bit of algebra —

$$\begin{aligned}\sum_{j=1}^{k+1} j &= \frac{k(k+1)}{2} + (k+1) &&= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\ &= \frac{k(k+1) + 2(k+1)}{2} &&= \frac{(k+2)(k+1)}{2} = \mathbf{\frac{(k+1)(k+2)}{2}}.\end{aligned}$$

This shows that $P(k) \Rightarrow P(k+1)$.

Revisited Example: $\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$ 3 of 3

At this point, we ***know***: $\displaystyle\sum_{j=1}^{k+1} j = \frac{k(k+1)}{2} + (k+1).$

[Our goal is to show that $\displaystyle\sum_{j=1}^{k+1} j = \frac{(k+1)(k+2)}{2}.$]

A little bit of algebra —

$$\begin{aligned}\sum_{j=1}^{k+1} j &= \frac{k(k+1)}{2} + (k+1) &&= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\ &= \frac{k(k+1)+2(k+1)}{2} &&= \frac{(k+2)(k+1)}{2} = \frac{\mathbf{(k+1)(k+2)}}{\mathbf{2}}.\end{aligned}$$

This shows that $P(k) \Rightarrow P(k+1)$.

Since we have proved both the basis $\mathbf{P(1)}$, and inductive $\mathbf{P(k)} \Rightarrow \mathbf{P(k+1)}$ steps, we conclude that the proposition is true for all $n \geq 1$. $\Box$

The Principle of Strong Mathematical Induction (PSMI)

The Principle of Strong Mathematical Induction:

Let $P(n)$ be a predicate that is defined for integers n, and let a **and** b be a fixed integers, **with** $a \leq b$. Suppose the following two statements are ***true***:

1. $P(a)$, $P(a+1)$, $\ldots$, $P(b)$ **are all *true***.

2. For all integers $\mathbf{k} > \mathbf{b}$, if $P(k)$ is true, then $P(k+1)$ is true. [Inductive Step]

Then the statement

$$\forall n \in \mathbb{Z},\ n \geq a, P(n)$$

is true.

Clearly, if $a = b$, then the principle of strong mathematical induction reduces to the ordinary principle of mathematical induction.

Example: Divisibility by a Prime 1 of 2

Proposition: Any integer greater than 1 is divisible by a prime number.

Proof (by use of PSMI): [As always we have to show the basis case... Here is it enough to show for $n = 2$. (Why?)]

Example: Divisibility by a Prime 1 of 2

Proposition: Any integer greater than 1 is divisible by a prime number.

Proof (by use of PSMI): [As always we have to show the basis case... Here is it enough to show for $n = 2$. (Why?)]

The divisibility property holds for $n = 2$ since 2 is a prime number and $2|2$.

Example: Divisibility by a Prime 1 of 2

Proposition: Any integer greater than 1 is divisible by a prime number.

Proof (by use of PSMI): [As always we have to show the basis case... Here is it enough to show for $n = 2$. (Why?)]

The divisibility property holds for $n = 2$ since 2 is a prime number and $2|2$.

The Inductive Hypothesis: Let $k > 2$, and suppose that for all integers i with $2 \leq i < k$, i is divisible by a prime number.

Example: Divisibility by a Prime 1 of 2

Proposition: Any integer greater than 1 is divisible by a prime number.

Proof (by use of PSMI): [As always we have to show the basis case... Here is it enough to show for $n = 2$. (Why?)]

The divisibility property holds for $n = 2$ since 2 is a prime number and $2|2$.

The Inductive Hypothesis: Let $k > 2$, and suppose that for all integers i with $2 \leq i < k$, i is divisible by a prime number.

Now, k is either a prime (in which case it is divisible by itself), or a composite

Example: Divisibility by a Prime 1 of 2

Proposition: Any integer greater than 1 is divisible by a prime number.

Proof (by use of PSMI): [As always we have to show the basis case... Here is it enough to show for $n = 2$. (Why?)]

The divisibility property holds for $n = 2$ since 2 is a prime number and $2|2$.

The Inductive Hypothesis: Let $k > 2$, and suppose that for all integers i with $2 \leq i < k$, i is divisible by a prime number.

Now, k is either a prime (in which case it is divisible by itself), or a composite — if the latter is true, then $k = a \cdot b$, where $2 \leq a < k$ and $2 \leq b < k$.

Example: Divisibility by a Prime 1 of 2

Proposition: Any integer greater than 1 is divisible by a prime number.

Proof (by use of PSMI): [As always we have to show the basis case... Here is it enough to show for $n = 2$. (Why?)]

The divisibility property holds for $n = 2$ since 2 is a prime number and $2|2$.

The Inductive Hypothesis: Let $k > 2$, and suppose that for all integers i with $2 \leq i < k$, i is divisible by a prime number.

Now, k is either a prime (in which case it is divisible by itself), or a composite — if the latter is true, then $k = a \cdot b$, where $2 \leq a < k$ and $2 \leq b < k$. By the inductive hypothesis a (and b) is divisible by a prime, so it follows that k is divisible by that same prime.

Example: Divisibility by a Prime 1 of 2

Proposition: Any integer greater than 1 is divisible by a prime number.

Proof (by use of PSMI): [As always we have to show the basis case... Here is it enough to show for $n = 2$. (Why?)]

The divisibility property holds for $n = 2$ since 2 is a prime number and $2|2$.

The Inductive Hypothesis: Let $k > 2$, and suppose that for all integers i with $2 \leq i < k$, i is divisible by a prime number.

Now, k is either a prime (in which case it is divisible by itself), or a composite — if the latter is true, then $k = a \cdot b$, where $2 \leq a < k$ and $2 \leq b < k$. By the inductive hypothesis a (and b) is divisible by a prime, so it follows that k is divisible by that same prime. Hence, regardless of whether k is prime or composite, it is divisible by a prime.

□

Example: Divisibility by a Prime 2 of 2

Is may seem like something is wrong with this proof...

Did we really use PSMI??? — First, we only showed ***one*** base case! — Second, we used an inductive hypothesis which may seem unfounded!

In this instance PSMI works like an accordion! ... (???)

Example: Divisibility by a Prime 2 of 2

Is may seem like something is wrong with this proof...

Did we really use PSMI??? — First, we only showed ***one*** base case! — Second, we used an inductive hypothesis which may seem unfounded!

In this instance PSMI works like an accordion! ... (???)

The proved basis case $n = 2$ enables us to apply the theorem to $n = 3$ (which shows $P(3)$ since 3 is a prime);

Example: Divisibility by a Prime 2 of 2

Is may seem like something is wrong with this proof...

Did we really use PSMI??? — First, we only showed ***one*** base case! — Second, we used an inductive hypothesis which may seem unfounded!

In this instance PSMI works like an accordion! ... (???)

The proved basis case $n = 2$ enables us to apply the theorem to $n = 3$ (which shows $P(3)$ since 3 is a prime); after that $P(2)$ and $P(3)$ serve as proved basis cases, and we can apply to $n = 4$ (which shows $P(4)$ since $4 = 2 \cdot 2$);

Example: Divisibility by a Prime 2 of 2

Is may seem like something is wrong with this proof...

Did we really use PSMI??? — First, we only showed ***one*** base case! — Second, we used an inductive hypothesis which may seem unfounded!

In this instance PSMI works like an accordion! ... (???)

The proved basis case $n = 2$ enables us to apply the theorem to $n = 3$ (which shows $P(3)$ since 3 is a prime); after that $P(2)$ and $P(3)$ serve as proved basis cases, and we can apply to $n = 4$ (which shows $P(4)$ since $4 = 2 \cdot 2$); from this point $P(2)$, $P(3)$ and $P(4)$ serve as basis cases... repeat, repeat, repeat...

Example: Divisibility by a Prime 2 of 2

Is may seem like something is wrong with this proof...

Did we really use PSMI??? — First, we only showed ***one*** base case! — Second, we used an inductive hypothesis which may seem unfounded!

In this instance PSMI works like an accordion! ... (???)

The proved basis case $n = 2$ enables us to apply the theorem to $n = 3$ (which shows $P(3)$ since 3 is a prime); after that $P(2)$ and $P(3)$ serve as proved basis cases, and we can apply to $n = 4$ (which shows $P(4)$ since $4 = 2 \cdot 2$); from this point $P(2)$, $P(3)$ and $P(4)$ serve as basis cases... repeat, repeat, repeat...

Note that we really need ***all*** the previous $P(i)$, $2 \leq i < k$ basis cases to show $P(k)$.

Example: The Properties of a Sequence 1 of 4

We define a sequence a_1, a_2, $\ldots$ as follows:

$$a_1 = 0, \quad a_2 = 2, \quad a_k = 3 \cdot a_{\lfloor k/2 \rfloor} + 2,\ k \geq 3$$

We are going to prove that all the terms a_n, $n \geq 1$ are even, but first we look at the first 8 terms of the sequence:

$$\begin{aligned}
a_1 &= 0 \\
a_2 &= 2 \\
a_3 &= 3a_{\lfloor 3/2 \rfloor} + 2 = 3a_1 + 2 = 3 \cdot 0 + 2 = 2 \\
a_4 &= 3a_{\lfloor 4/2 \rfloor} + 2 = 3a_2 + 2 = 3 \cdot 2 + 2 = 8 \\
a_5 &= 3a_{\lfloor 5/2 \rfloor} + 2 = 3a_2 + 2 = 3 \cdot 2 + 2 = 8 \\
a_6 &= 3a_{\lfloor 6/2 \rfloor} + 2 = 3a_3 + 2 = 3 \cdot 2 + 2 = 8 \\
a_7 &= 3a_{\lfloor 7/2 \rfloor} + 2 = 3a_3 + 2 = 3 \cdot 2 + 2 = 8 \\
a_8 &= 3a_{\lfloor 8/2 \rfloor} + 2 = 3a_4 + 2 = 3 \cdot 8 + 2 = 26
\end{aligned}$$

Example: The Properties of a Sequence 2 of 4

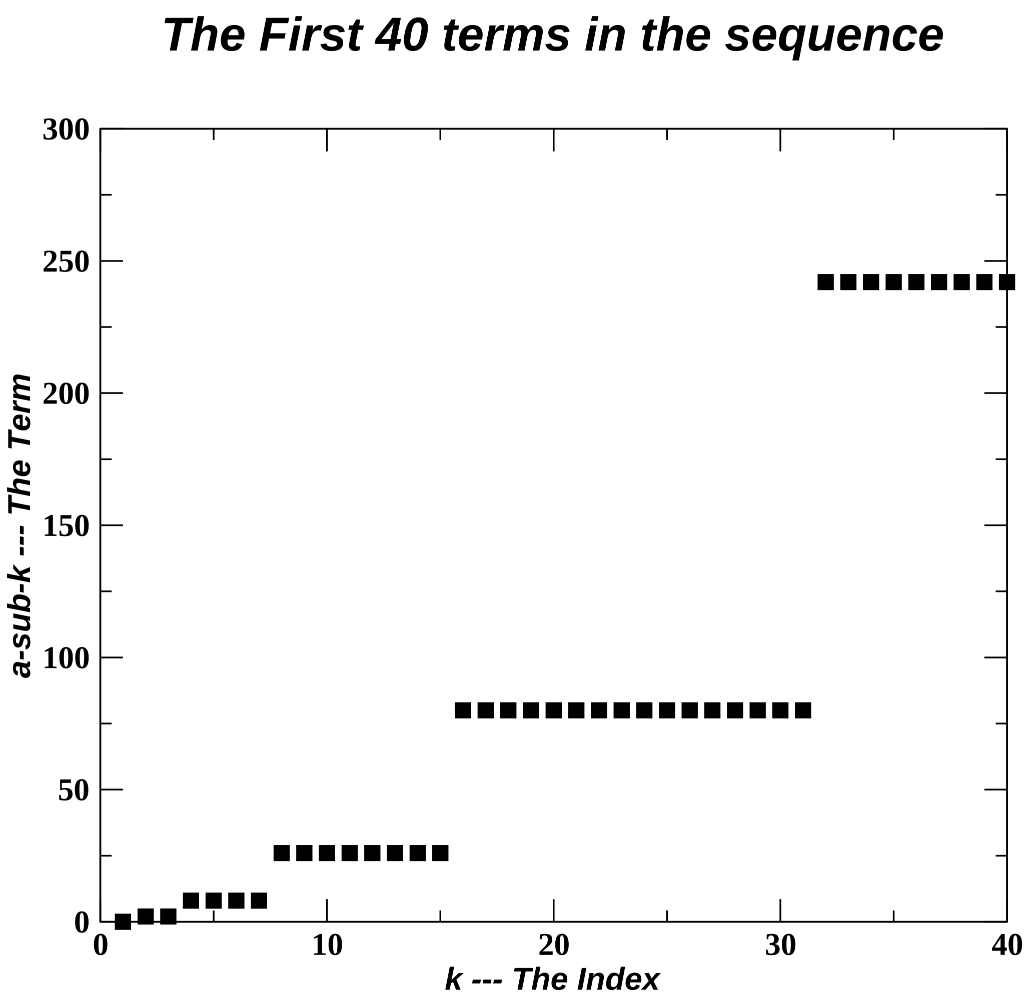

Figure: The sequence is not all that exciting... Each plateau has twice the number of terms of the previous one, and the levels follow the rule $L_n = 3 \cdot L_{n-1} + 2, n \geq 3$ where $L_1 = 0$ and $L_2 = 2$.

Example: The Properties of a Sequence 3 of 4

Now that we have a “feeling” for the sequence, lets prove that all the terms are even…

Proof: [We want to prove that the property “$P(n)$ = ’a_n is even’ ” $\forall\, n \geq 1$.]

Example: The Properties of a Sequence 3 of 4

Now that we have a "feeling" for the sequence, lets prove that all the terms are even...

Proof: [We want to prove that the property "$P(n)$ = 'a_n is even'" $\forall\ n \geq 1$.]

Basis case: The property holds for $n = 1$ and $n = 2$, since "$P(1)$ = 'a_1 is even' ' is ***true*** (since $a_1 = 0$), and "$P(2)$ = 'a_2 is even' ' is ***true*** (since $a_2 = 2$).

Example: The Properties of a Sequence 3 of 4

Now that we have a "feeling" for the sequence, lets prove that all the terms are even...

Proof: [We want to prove that the property "$P(n)$ = 'a_n is even' " $\forall$ $n \geq 1$.]

Basis case: The property holds for $n = 1$ and $n = 2$, since "$P(1)$ $=$ 'a_1 is even' ' is ***true*** (since $a_1 = 0$), and "$P(2) =$ 'a_2 is even' ' is ***true*** (since $a_2 = 2$).

Inductive step: Let $k > 2$ be an integer, and suppose that

a_i is even $\forall i$: $1 \leq i < k$. [The Inductive Hypothesis]

Example: The Properties of a Sequence 3 of 4

Now that we have a "feeling" for the sequence, lets prove that all the terms are even...

Proof: [We want to prove that the property "$P(n)$ = 'a_n is even' " $\forall\ n \geq 1$.]

Basis case: The property holds for $n = 1$ and $n = 2$, since "$P(1)$ = 'a_1 is even' ' is ***true*** (since $a_1 = 0$), and "$P(2)$ = 'a_2 is even' ' is ***true*** (since $a_2 = 2$).

Inductive step: Let $k > 2$ be an integer, and suppose that

a_i is even $\forall i$: $1 \leq i < k$. [The Inductive Hypothesis]

[We must show that a_k is even] By the definition of the sequence

$$a_k = 3 \cdot a_{\lfloor k/2 \rfloor} + 2, \ \forall k \geq 3$$

Example: The Properties of a Sequence 4 of 4

Proof continued: By the definition of the sequence

$$a_k = 3 \cdot a_{\lfloor k/2 \rfloor} + 2, \ \forall k \geq 3$$

Now, $a_{\lfloor k/2 \rfloor}$ is even by the inductive hypothesis, since $k > 2$ and $1 \leq \lfloor k/2 \rfloor < k$.

Example: The Properties of a Sequence 4 of 4

Proof continued: By the definition of the sequence

$$a_k = 3 \cdot a_{\lfloor k/2 \rfloor} + 2, \ \forall k \geq 3$$

Now, $a_{\lfloor k/2 \rfloor}$ is even by the inductive hypothesis, since $k > 2$ and $1 \leq \lfloor k/2 \rfloor < k$.

By our usual argument $a_{\lfloor k/2 \rfloor} = 2 \cdot m$, for some particular integer m, and

$$a_k = 3 \cdot a_{\lfloor k/2 \rfloor} + 2 = 3 \cdot 2 \cdot m + 2 = 2 \cdot (\underbrace{3 \cdot m + 1}_{\text{an integer}})$$

and it follows that a_k is even.

Example: The Properties of a Sequence 4 of 4

Proof continued: By the definition of the sequence

$$a_k = 3 \cdot a_{\lfloor k/2 \rfloor} + 2, \ \forall k \geq 3$$

Now, $a_{\lfloor k/2 \rfloor}$ is even by the inductive hypothesis, since $k > 2$ and $1 \leq \lfloor k/2 \rfloor < k$.

By our usual argument $a_{\lfloor k/2 \rfloor} = 2 \cdot m$, for some particular integer m, and

$$a_k = 3 \cdot a_{\lfloor k/2 \rfloor} + 2 = 3 \cdot 2 \cdot m + 2 = 2 \cdot (\underbrace{3 \cdot m + 1}_{\text{an integer}})$$

and it follows that a_k is even.

Since we have proved the basis and inductive steps of the strong mathematical induction, we conclude that the given statement is ***true***.

□

The Well-Ordering Principle of the Integers

The Well-Ordering Principle of the Integers

Let $\mathcal{S}$ be a set containing one or more integers all of which are greater than some fixed integer. Then $\mathcal{S}$ has a least element.

The well-ordering principle, ***the principle of mathematical induction*** and ***the principle of strong mathematical induction*** are **equivalent**.

— It can be shown that if any ***one*** of them is true, then so are both of the others.

The proofs are given on slides 37 and 38, but you are not required to know them.

Example: Finding Least Elements 1 of 2

Problem: For each set, if the set has a least element, state what it is. If not, explain why the well-ordering principle is not violated.

(a) The set of all positive real numbers.

(b) The set of all non-negative integers n such that $n^2 < n$.

(c) The set of all non-negative integers of the form $46 - 7k$, where k is an integer.

Solutions:

Example: Finding Least Elements 1 of 2

Problem: For each set, if the set has a least element, state what it is. If not, explain why the well-ordering principle is not violated.

(a) The set of all positive real numbers.

(b) The set of all non-negative integers n such that $n^2 < n$.

(c) The set of all non-negative integers of the form $46 - 7k$, where k is an integer.

Solutions:

(a) The is no least real number. If x is a positive real number, then so is $x/2$, and $x/2 < x$. The well-ordering principle only applies to ***integers***.

Example: Finding Least Elements 1 of 2

Problem: For each set, if the set has a least element, state what it is. If not, explain why the well-ordering principle is not violated.

(a) The set of all positive real numbers.

(b) The set of all non-negative integers n such that $n^2 < n$.

(c) The set of all non-negative integers of the form $46 - 7k$, where k is an integer.

Solutions:

(a) The is no least real number. If x is a positive real number, then so is $x/2$, and $x/2 < x$. The well-ordering principle only applies to ***integers***.

(b) The set of non-negative integers for which $n^2 < n$ is ***empty***. An empty set has no least member. The well-ordering principle does not apply to empty sets.

Example: Finding Least Elements 2 of 2

Problem: For each set, if the set has a least element, state what it is. If not, explain why the well-ordering principle is not violated.

(c) The set of all non-negative integers of the form $46 - 7k$, where k is an integer.

Solutions:

(c) Consider the values of $46 - 7k$ for various values of k:

k	$\dots$	-3	-2	-1	0	1	$\dots$	5	**6**	7	$\dots$
$46 - 7k$	$\dots$	67	60	53	46	39	$\dots$	11	**4**	-3	$\dots$

The table suggests that

$$46 - 7k < 0 \text{ for } k \geq 7, \quad \text{and} \quad 46 - 7k \geq 46 \text{ for } k \leq 0.$$

From the other values in the table it is clear that 4 is the least non-negative number of the form $46 - 7k$. It is achieved when $k = 6$.

Proving the Quotient-Remainder Theorem (Existence)

The Well-Ordering Principle is at the core of the proof of:

Theorem: $\forall n \in \mathbb{Z}$, and $\forall d \in \mathbb{N}$, $\exists$ unique $q, r \in \mathbb{Z}$ such that

$$n = d \cdot q + r, \quad \text{and} \quad 0 \le r < d$$

Proof: Let n be an integer, and d be a positive integer.

Proving the Quotient-Remainder Theorem (Existence)

The Well-Ordering Principle is at the core of the proof of:

Theorem: $\forall n \in \mathbb{Z}$, and $\forall d \in \mathbb{N}$, $\exists$ unique $q, r \in \mathbb{Z}$ such that

$$n = d \cdot q + r, \quad \text{and} \quad 0 \leq r < d$$

Proof: Let n be an integer, and d be a positive integer. Let S be the set of all non-negative integers of the form $(n - d \cdot k)$, where k is an integer.

Proving the Quotient-Remainder Theorem (Existence)

The Well-Ordering Principle is at the core of the proof of:

Theorem: $\forall n \in \mathbb{Z}$, and $\forall d \in \mathbb{N}$, $\exists$ unique $q, r \in \mathbb{Z}$ such that

$$n = d \cdot q + r, \quad \text{and} \quad 0 \leq r < d$$

Proof: Let n be an integer, and d be a positive integer. Let S be the set of all non-negative integers of the form $(n - d \cdot k)$, where k is an integer. This set has at least one element: [If n is non-negative, then $n - 0 \cdot d = n \geq 0$ and hence $n \in S$. If n is negative $(n - n \cdot d) = n \cdot (1 - d) \geq 0$ and hence $(n - n \cdot d) \in S$.]

Proving the Quotient-Remainder Theorem (Existence)

The Well-Ordering Principle is at the core of the proof of:

Theorem: $\forall n \in \mathbb{Z}$, and $\forall d \in \mathbb{N}$, $\exists$ unique $q, r \in \mathbb{Z}$ such that

$$n = d \cdot q + r, \quad \text{and} \quad 0 \le r < d$$

Proof: Let n be an integer, and d be a positive integer. Let S be the set of all non-negative integers of the form $(n - d \cdot k)$, where k is an integer. This set has at least one element: [If n is non-negative, then $n - 0 \cdot d = n \ge 0$ and hence $n \in S$. If n is negative $(n - n \cdot d) = n \cdot (1 - d) \ge 0$ and hence $(n - n \cdot d) \in S$.] By the well-ordering principle, S contains a least element r.

Proving the Quotient-Remainder Theorem (Existence)

The Well-Ordering Principle is at the core of the proof of:

Theorem: $\forall n \in \mathbb{Z}$, and $\forall d \in \mathbb{N}$, $\exists$ unique $q, r \in \mathbb{Z}$ such that

$$n = d \cdot q + r, \quad \text{and} \quad 0 \leq r < d$$

Proof: Let n be an integer, and d be a positive integer. Let S be the set of all non-negative integers of the form $(n - d \cdot k)$, where k is an integer. This set has at least one element: [If n is non-negative, then $n - 0 \cdot d = n \geq 0$ and hence $n \in S$. If n is negative $(n - n \cdot d) = n \cdot (1 - d) \geq 0$ and hence $(n - n \cdot d) \in S$.] By the well-ordering principle, S contains a least element r. Then for some specific integer $k = q$, $(n - d \cdot q = r)$ [since every member of S can be written in this form]

[Continued...]

Proving the Quotient-Remainder Theorem (Existence)

Proof: Let n be an integer, and d be a positive integer. Let S be the set of all non-negative integers of the form $(n - d \cdot k)$, where k is an integer. This set has at least one element: By the well-ordering principle, S contains a least element r. Then for some specific integer $k = q$, $(n - d \cdot q = r)$.

Proving the Quotient-Remainder Theorem (Existence)

Proof: Let n be an integer, and d be a positive integer. Let S be the set of all non-negative integers of the form $(n - d \cdot k)$, where k is an integer. This set has at least one element: By the well-ordering principle, S contains a least element r. Then for some specific integer $k = q$, $(n - d \cdot q = r)$. Adding $(d \cdot q)$ to both sides gives

$$n = d \cdot q + r.$$

Proving the Quotient-Remainder Theorem (Existence)

Proof: Let n be an integer, and d be a positive integer. Let S be the set of all non-negative integers of the form $(n - d \cdot k)$, where k is an integer. This set has at least one element: By the well-ordering principle, S contains a least element r. Then for some specific integer $k = q$, $(n - d \cdot q = r)$. Adding $(d \cdot q)$ to both sides gives

$$n = d \cdot q + r.$$

Further, $r < d$ [Suppose $r \geq d$, then

$$n - d \cdot (q + 1) = n - d \cdot q - d = r - d \geq 0,$$

and so $n - d \cdot (q + 1)$ would be a non-negative integer in S that would be smaller than r. But r is the smallest integer in S. This contradiction shows that $r < d$.]

Proving the Quotient-Remainder Theorem (Existence)

Proof: Let n be an integer, and d be a positive integer. Let S be the set of all non-negative integers of the form $(n - d \cdot k)$, where k is an integer. This set has at least one element: By the well-ordering principle, S contains a least element r. Then for some specific integer $k = q$, $(n - d \cdot q = r)$. Adding $(d \cdot q)$ to both sides gives

$$n = d \cdot q + r.$$

Further, $r < d$ [Suppose $r \geq d$, then

$$n - d \cdot (q + 1) = n - d \cdot q - d = r - d \geq 0,$$

and so $n - d \cdot (q + 1)$ would be a non-negative integer in S that would be smaller than r. But r is the smallest integer in S. This contradiction shows that $r < d$.] We have shown that there exists integers r and q for which,

$$n = d \cdot q + r, \quad \text{and} \quad 0 \leq r < d. \qquad \square$$

Homework #7 — Due Friday 11/3/2006, 12noon, GMCS-587 Final Version

(Epp v3.0)

Epp-4.2.1, ***Epp-4.2.3***, ***Epp-4.2.10***, ***Epp-4.2.31***

Epp-4.3.5

Epp-4.4.1, ***Epp-4.4.2***, ***Epp-4.4.4***, ***Epp-4.4.22***

(Epp v2.0)

Epp-4.2.1, ***Epp-4.2.3***, ***Epp-4.2.9***, ***Epp-4.2.28***

Epp-4.3.5

Epp-4.4.1, —, ***Epp-4.4.4***, ***Epp-4.4.11***

Induction Implies Well-Ordering

Proof: Assume the Induction Principle exists for $\mathbb{N}$. Let the set $J \subset \mathbb{N}$ and $J \neq \emptyset$. Suppose J has no least element. Let $S = \{n \in \mathbb{N} : \{1, 2, ...\} \cap J = \emptyset\}$. Note that $1 \notin J$ since J would have a least element. Thus, $1 \in S$. Suppose that $n \in S$, then $\{1, 2, ...n\} \cap J \neq \emptyset$. Consider $n + 1$: $n + 1 \notin J$ since otherwise $n+1$ would be the least element of J. So, $n+1 \in S$. Hence, by the induction principle, $S = \mathbb{N}$. Thus, J has no elements $(J = \emptyset)$ and so we have a contradiction. □

Here $\mathbb{N}$ is the set of natural numbers, and $\emptyset$ is the empty set. $\cap$ denotes the intersection of two set, *i.e.* the common members of the two sets.

Well-Ordering Implies Induction

Proof: Let P(n) be a proposition defined for each $\mathbb{N}$. Suppose $P(1)$ is true and $P(n) \Rightarrow P(n+1)$. If $P(n)$ does not hold for all $n \in \mathbb{N}$, then there exists a non-empty set $X \subset \mathbb{N}$ defined as $\{n \in \mathbb{N} : P(n)$ is false$\}$.

Given the Well-Ordering Principle, there exists an $m \in X$ that is the least element of X. Let B be the set $\{n \in \mathbb{N} : 1 \leq n \leq m\}$. Since $P(1)$ is true and $1 \in B$ we can then apply $P(n) \Rightarrow P(n+1)$ to B from 1 to m proving $P(n)$ for each element of B including m. Since $m \in B$, $P(m)$ is true but since $m \in X$, $P(m)$ is false. Since this is a contradiction, X must be empty and, thus, $P(n)$ holds for all of $\mathbb{N}$. So, if $P(1)$ and $P(n) \Rightarrow P(n+1)$, then $P(n)$ holds for all of $\mathbb{N}$. □