The Foundations: Logic and Proofs

Chapter 1, Part III: Proofs

Proofs

A proof is a valid argument that establishes the truth of a mathematical statement.

Ingredients:

- hypotheses of the theorem
- axioms assumed to be true
- previously proven theorems
- rules of inference

You get:
truth of the statement being proved

Usefulness

Computer Science

Verifying that computer programs are correct.
Establishing that operating systems are secure.
Making inferences in artificial intelligence.
Showing that system specifications are consistent.

Mathematics

Defining Formalism.
Providing specification in a common language.
Justification for the results.

Definitions

Deriving Additional Results about Even and Odd Integers

Suppose that you have already proved the following properties of even and odd integers:

1. The sum, product, and difference of any two even integers are even.
2. The sum and difference of any two odd integers are even.
3. The product of any two odd integers is odd.
4. The product of any even integer and any odd integer is even.
5. The sum of any odd integer and any even integer is odd.
6. The difference of any odd integer minus any even integer is odd.
7. The difference of any even integer minus any odd integer is odd.

Definitions

1.An integer n is even if, and only if, n = 2k for some integer k.

2. An integer n is odd if, and only if, n = 2k + 1 for some integer k.

3. An integer n is prime if, and only if, n > 1 and for all positive integers r and s, if n = r·s, then r = 1 or s = 1.

4. An integer n > 1 is composite if, and only if, n = r·s for some positive integers r and s with r ≠ 1 and s ≠ 1.

5. A real number r is rational if, and only if, r= $\frac{a}{b}$ for some integers a and b with b ≠ 0.

6. If n and d are integers and d ≠ 0, then d divides n, written d|n if, and only if, n = d.k for some integers k.

7. An integer n is called a perfect square if, and only if, n = k^2 for some integer k.

Types of Proofs

Proving conditional Statements

- Direct Proofs
- Indirect Proofs
  - **Proof by Contraposition**
  - **Proofs by Contradiction**

Proving Non-conditional Statements

- Indirect Proofs
- If-And-Only-If Proof
- Constructive Versus Non-constructive Proofs
- Existence Proofs; Existence and Uniqueness Proofs
- Disproofs (Counterexample, Contradiction, Existence Statement)
- Proofs Involving Sets

Mathematical Induction

Direct Proofs

p →q

first step is the assumption that *p is true*
subsequent steps constructed using rules of inference.
final step showing that *q must also be true*

showing that if *p is true,*
then q must also be true,
so that the combination
p true and q false never occurs

Outline for Direct Proof

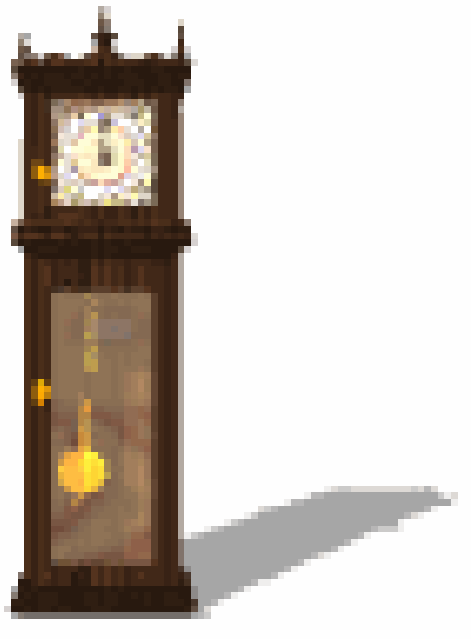
Proposition If P, then Q.

Proof. Suppose P.

⋮

Therefore Q. ■

Activity Time



Prove that the sum of two odd integers is even.

Prove that the sum of two odd integers is even.

Let **m** and **n** be two odd integers. Then by definition of odd numbers

$m = 2k + 1$ for some $k \in Z$

$n = 2l + 1$ for some $l \in Z$

Now $m + n = (2k + 1) + (2l + 1)$

$= 2k + 2l + 2$

$= 2(k + l + 1)$

$= 2r$ where $r = (k + l + 1) \in Z$

Hence $m + n$ is even.

EXERCISE:

Prove that if n is any even integer, then $(-1)^n = 1$

SOLUTION:

Suppose n is an even integer. Then $n = 2k$ for some integer k.

Now

$$(-1)^n = (-1)^{2k}$$
$$= [(-1)^2]^k$$
$$= (1)^k$$
$$= 1 \qquad \text{(proved)}$$

EXERCISE:

Prove that the product of an even integer and an odd integer is even.

SOLUTION:

Suppose m is an even integer and n is an odd integer. Then

$m = 2k$ for some integer k

and $n = 2l + 1$ for some integer l

Now

$$m \cdot n = 2k \cdot (2l + 1)$$
$$= 2 \cdot k\,(2l + 1)$$
$$= 2 \cdot r \quad \text{where } r = k(2l + 1) \text{ is an integer}$$

Hence $m \cdot n$ is even. (Proved)

EXERCISE:

Prove that the square of an even integer is even.

SOLUTION:

Suppose n is an even integer. Then $n = 2k$

Now

$$\text{square of } n = n^2 = (2 \cdot k)^2$$
$$= 4k^2$$
$$= 2 \cdot (2k^2)$$
$$= 2 \cdot p \text{ where } p = 2k^2 \in Z$$

Hence, n^2 is even. (proved)

Prove that if *n is an odd integer, then n^2 is an odd integer*

We assume that the hypothesis of this conditional statement is true, namely, we assume that *n is odd*. By the definition of an odd integer, it follows that *$n = 2k + 1$, where k is some integer.*

Square both sides $n^2 = (2k + 1)^2$

$4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$

Consequently, we have proved that if *n is an odd integer, then n^2 is an odd integer*

EXERCISE:

Prove that if n is an odd integer, then $n^3 + n$ is even.

SOLUTION:

Let n be an odd integer, then $n = 2k + 1$ for some $k \in Z$

Now $n^3 + n = n(n^2 + 1)$

$= (2k + 1)((2k+1)^2 + 1)$

$= (2k + 1)(4k^2 + 4k + 1 + 1)$

$= (2k + 1)(4k^2 + 4k + 2)$

$= (2k + 1)\,2.\,(2k^2 + 2k + 1)$

$= 2 \cdot (2k + 1)(2k^2 + 2k + 1)$ $\quad k \in Z$

= an even integer

Proposition If x is an even integer, then $x^2 - 6x + 5$ is odd.

Proof. Suppose x is an even integer.

Then $x = 2a$ for some $a \in \mathbb{Z}$, by definition of an even integer.

So $x^2 - 6x + 5 = (2a)^2 - 6(2a) + 5 = 4a^2 - 12a + 5 = 4a^2 - 12a + 4 + 1 = 2(2a^2 - 6a + 2) + 1$.

Therefore we have $x^2 - 6x + 5 = 2b + 1$, where $b = 2a^2 - 6a + 2 \in \mathbb{Z}$.

Consequently $x^2 - 6x + 5$ is odd, by definition of an odd number.

EXERCISE:

Prove that, if the sum of any two integers is even, then so is their difference.

SOLUTION:

Suppose m and n are integers so that m + n is even. Then by definition of even numbers

$m + n = 2k$ for some integer k

$\Rightarrow \quad m = 2k - n$ .....(1)

Now $m - n = (2k - n) - n$ using (1)

$= 2k - 2n$

$= 2(k - n) = 2r$ where $r = k - n$ is an integer

Hence m - n is even.

EXERCISE:

Prove that the sum of any two rational numbers is rational.

SOLUTION:

Suppose r and s are rational numbers.

Then by definition of rational

$$r = \frac{a}{b} \quad \text{and} \quad s = \frac{c}{d}$$

for some integers a, b, c, d with $b \neq 0$ and $d \neq 0$

Now

$$r + s = \frac{a}{b} + \frac{c}{d}$$

$$= \frac{ad + bc}{bd}$$

$$= \frac{p}{q}$$

where $p = ad + bc \in Z$ and $q = bd \in Z$ and $q \neq 0$

Hence r + s is rational.

EXERCISE:

Given any two distinct rational numbers r and s with $r < s$. Prove that there is a rational number x such that $r < x < s$.

SOLUTION:

Given two distinct rational numbers r and s such that

$r < s$ .....(1)

Adding r to both sides of (1), we get

$$r + r < r + s$$
$$2r < r + s$$

$\Rightarrow$

$$r < \frac{r+s}{2} \quad \text{.....(2)}$$

Next adding s to both sides of (1), we get

$$r + s < s + s$$

$\Rightarrow$ $r + s < 2s$

$\Rightarrow$

$$\frac{r+s}{2} < s \quad \text{.....(3)}$$

Combining (2) and (3), we may write

$$r < \frac{r+s}{2} < s \quad \text{.....(4)}$$

Since the sum of two rationals is rational, therefore $r + s$ is rational. Also the quotient of a rational by a non-zero rational, is rational, therefore $\frac{r+s}{2}$ is rational and by (4) it lies between r & s. Hence, we have found a rational number such that $r < x < s$. (proved)

EXERCISE:

Prove that the sum of any three consecutive integers is divisible by 3.

PROOF:

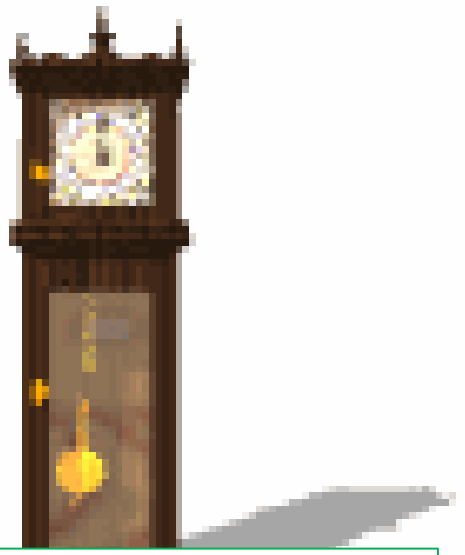
Let n, $n + 1$ and $n + 2$ be three consecutive integers.

Now

$$n + (n + 1) + (n + 2) = 3n + 3$$
$$= 3(n + 1)$$
$$= 3 \cdot k \quad \text{where } k = (n+1) \in Z$$

Hence, the sum of three consecutive integers is divisible by 3.

Activity Time



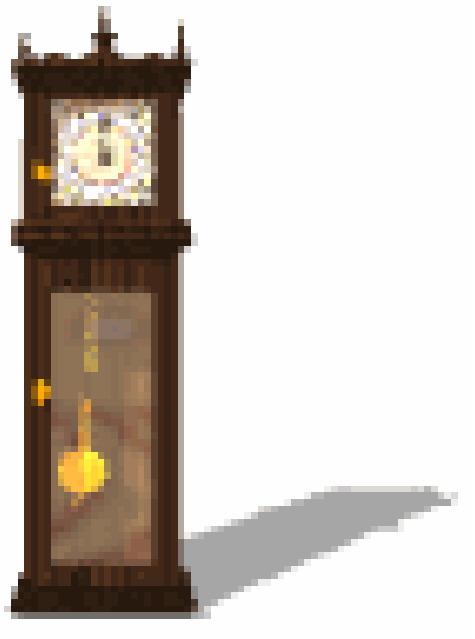
Use a direct proof to show that the product of two odd numbers is odd.

Give a direct proof that if *m and n are both perfect squares, then nm is also a perfect square.*

Proof

We assume that the hypothesis of this conditional statement is true, namely, we assume that m and n are both perfect squares.
By the definition of a perfect square, It follows that there are integers s and t such that
$m = s^2$ and $n = t^2$.
Multiplying both m and n to get s^2t^2.
Hence, $mn = s^2t^2 = (ss)(tt) = (st)(st) = (st)^2$, using commutativity and associativity of multiplication.
By the definition of perfect square, it follows that mn is also a perfect square, because it is the square of st, which is an integer.
We have proved that if m and n are both perfect squares, then mn is also a perfect square.

Activity Time



Give a direct proof that if *n is an integer and n is odd, then 3n + 2 is odd.*

The square of any odd integer has the form $8m + 1$ for some integer m.

The Square of an Odd Integer

Prove: The square of any odd integer has the form $8m + 1$ for some integer m.

Proof:

Suppose n is a *[particular but arbitrarily chosen]* odd integer. By the quotient-remainder theorem, n can be written in one of the forms

$$4q \quad \text{or} \quad 4q+1 \quad \text{or} \quad 4q+2 \quad \text{or} \quad 4q+3$$

for some integer q. In fact, since n is odd and $4q$ and $4q + 2$ are even, n must have one of the forms

$$4q+1 \quad \text{or} \quad 4q+3.$$

Case 1 ($n = 4q + 1$ for some integer q): *[We must find an integer m such that $n^2 = 8m + 1$.]* Since $n = 4q + 1$,

$$\begin{aligned} n^2 &= (4q+1)^2 && \text{by substitution} \\ &= (4q+1)(4q+1) && \text{by definition of square} \\ &= 16q^2 + 8q + 1 \\ &= 8(2q^2 + q) + 1 && \text{by the laws of algebra.} \end{aligned}$$

Let $m = 2q^2 + q$. Then m is an integer since 2 and q are integers and sums and products of integers are integers. Thus, substituting,

$$n^2 = 8m + 1 \quad \text{where } m \text{ is an integer.}$$

Case 2 ($n = 4q + 3$ for some integer q): *[We must find an integer m such that $n^2 = 8m + 1$.]* Since $n = 4q + 3$,

$$\begin{aligned} n^2 &= (4q + 3)^2 && \text{by substitution} \\ &= (4q + 3)(4q + 3) && \text{by definition of square} \\ &= 16q^2 + 24q + 9 \\ &= 16q^2 + 24q + (8 + 1) \\ &= 8(2q^2 + 3q + 1) + 1 && \text{by the laws of algebra.} \end{aligned}$$

Let $m = 2q^2 + 3q + 1$. Then m is an integer since 1, 2, 3, and q are integers and sums and products of integers are integers. Thus, substituting,

$$n^2 = 8m + 1 \quad \text{where } m \text{ is an integer.}$$

Cases 1 and 2 show that given any odd integer, whether of the form $4q + 1$ or $4q + 3$, $n^2 = 8m + 1$ for some integer m. *[This is what we needed to show.]*

Mistakes in Proofs

What is wrong with this famous supposed "proof" that $1 = 2$?

"Proof": We use these steps, where a and b are two equal positive integers.

Step	Reason
1. $a = b$	Given
2. $a^2 = ab$	Multiply both sides of (1) by a
3. $a^2 - b^2 = ab - b^2$	Subtract b^2 from both sides of (2)
4. $(a - b)(a + b) = b(a - b)$	Factor both sides of (3)
5. $a + b = b$	Divide both sides of (4) by $a - b$
6. $2b = b$	Replace a by b in (5) because $a = b$ and simplify
7. $2 = 1$	Divide both sides of (6) by b

Solution: Every step is valid except for step 5, where we divided both sides by $a - b$. The error is that $a - b$ equals zero; division of both sides of an equation by the same quantity is valid as long as this quantity is not zero. ◀

EXHAUSTIVE PROOF Some theorems can be proved by examining a relatively small number of examples. Such proofs are called **exhaustive proofs**, or **proofs by exhaustion** because these proofs proceed by exhausting all possibilities. An exhaustive proof is a special type of proof by cases where each case involves checking a single example. We now provide some illustrations of exhaustive proofs.

Example

For all integers n, $n^2 - n + 11$ is a prime number.

$1^2 - 1 + 11 = 11$, which is prime.
$2^2 - 2 + 11 = 13$, which is prime.
$3^2 - 3 + 11 = 17$, which is prime.
$4^2 - 4 + 11 = 23$, which is prime.
$5^2 - 5 + 11 = 31$, which is prime.
$6^2 - 6 + 11 = 41$, which is prime.
$7^2 - 7 + 11 = 53$, which is prime.
$8^2 - 8 + 11 = 67$, which is prime.
$9^2 - 9 + 11 = 83$, which is prime.
$10^2 - 10 + 11 = 101$, which is prime.

Prove that $(n + 1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$.

Solution: We use a proof by exhaustion. We only need verify the inequality $(n + 1)^3 \geq 3^n$ when $n = 1, 2, 3,$ and 4. For $n = 1$, we have $(n + 1)^3 = 2^3 = 8$ and $3^n = 3^1 = 3$; for $n = 2$, we have $(n + 1)^3 = 3^3 = 27$ and $3^n = 3^2 = 9$; for $n = 3$, we have $(n + 1)^3 = 4^3 = 64$ and $3^n = 3^3 = 27$; and for $n = 4$, we have $(n + 1)^3 = 5^3 = 125$ and $3^n = 3^4 = 81$. In each of these four cases, we see that $(n + 1)^3 \geq 3^n$. We have used the method of exhaustion to prove that $(n + 1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$. ◀

PROOF BY CASES A proof by cases must cover all possible cases that arise in a theorem. We illustrate proof by cases with a couple of examples. In each example, you should check that all possible cases are covered.

Example

Use a proof by cases to show that $|xy| = |x||y|$, where x and y are real numbers. (Recall that $|a|$, the absolute value of a, equals a when $a \geq 0$ and equals $-a$ when $a \leq 0$.)

Solution: In our proof of this theorem, we remove absolute values using the fact that $|a| = a$ when $a \geq 0$ and $|a| = -a$ when $a \leq 0$. Because both $|x|$ and $|y|$ occur in our formula, we will need four cases: *(i)* x and y both nonnegative, *(ii)* x nonnegative and y negative, *(iii)* x negative and y nonnegative, and *(iv)* x negative and y negative. We denote by p_1, p_2, p_3, and p_4, the proposition stating the assumption for each of these four cases, respectively.

Case (i): We see that $p_1 \rightarrow q$ because $xy \geq 0$ when $x \geq 0$ and $y \geq 0$, so that $|xy| = xy = |x||y|$.

Case (ii): To see that $p_2 \rightarrow q$, note that if $x \geq 0$ and $y < 0$, then $xy \leq 0$, so that $|xy| = -xy = x(-y) = |x||y|$. (Here, because $y < 0$, we have $|y| = -y$.)

Case (iii): To see that $p_3 \rightarrow q$, we follow the same reasoning as the previous case with the roles of x and y reversed.

Case (iv): To see that $p_4 \rightarrow q$, note that when $x < 0$ and $y < 0$, it follows that $xy > 0$. Hence, $|xy| = xy = (-x)(-y) = |x||y|$.

Because $|xy| = |x||y|$ holds in each of the four cases and these cases exhaust all possibilities, we can conclude that $|xy| = |x||y|$, whenever x and y are real numbers. ◀

Indirect Proofs

Direct proof begin with the premises, continue with a sequence of deductions, and end with the conclusion.
Attempts at direct proofs often reach dead ends
Proofs that **do not** start with the premises and end with the conclusion, are called **indirect proofs**

PROOF BY CONTRAPOSITION:

A proof by contraposition is based on the logical equivalence between a statement and its contrapositive. Therefore, the implication $p \rightarrow q$ can be proved by showing that its contrapositive $\sim q \rightarrow \sim p$ is true. The contrapositive is usually proved directly.

The method of proof by contrapositive may be summarized as:

1. Express the statement in the form if p then q.
2. Rewrite this statement in the contrapositive form
   if not q then not p.
3. Prove the contrapositive by a direct proof.

Outline for Contrapositive Proof

Proposition If P, then Q.

Proof. Suppose $\sim Q$.

⋮

Therefore $\sim P$. ■

Prove that if *n is an integer and 3n + 2 is odd, then n is odd.*

PROOF:

The contrapositive of the given conditional statement is

" if n is even then 3n + 2 is even"

Suppose n is even, then

$n = 2k$ for some $k \in Z$

Now $3n + 2 = 3(2k) + 2$

$= 2.(3k + 1)$

$= 2.r$ where $r = (3k + 1) \in Z$

Hence 3n + 2 is even. We conclude that the given statement is true since its contrapositive is true.

EXERCISE:

Prove that for all integers n, if n^2 is even then n is even.

PROOF:

The contrapositive of the given statement is:

"if n is not even (odd) then n^2 is not even (odd)"

We prove this contrapositive statement directly.

Suppose n is odd. Then $n = 2k + 1$ for some $k \in Z$

Now $n^2 = (2k+1)^2 = 4k^2 + 4k + 1$

$= 2 \cdot (2k^2 + 2k) + 1$

$= 2 \cdot r + 1$ where $r = 2k^2 + 2k \in Z$

Hence n^2 is odd. Thus the contrapositive statement is true and so the given statement is true.

20. Prove that if n is an integer and $3n + 2$ is even, then n is even using

a) a proof by contraposition.
b) a proof by contradiction.

a) We must prove the contrapositive: If n is odd, then $3n + 2$ is odd. Assume that n is odd. Then we can write $n = 2k + 1$ for some integer k. Then $3n + 2 = 3(2k + 1) + 2 = 6k + 5 = 2(3k + 2) + 1$. Thus $3n + 2$ is two times some integer plus 1, so it is odd.

b) Suppose that $3n + 2$ is even and that n is odd. Since $3n + 2$ is even, so is $3n$. If we add subtract an odd number from an even number, we get an odd number, so $3n - n = 2n$ is odd. But this is obviously not true. Therefore our supposition was wrong, and the proof by contradiction is complete.

EXERCISE:

Prove that if n is an integer and $n^3 + 5$ is odd, then n is even.

PROOF:

Suppose n is an odd integer. Since, a product of two odd integers is odd, therefore n^2 = n.n is odd; and $n^3 = n^2.n$ is odd.

Since a sum of two odd integers is even therefore $n^2 + 5$ is even.

Thus we have prove that if n is odd then $n^3 + 5$ is even.

Since this is the contrapositive of the given conditional statement, so the given statement is true.

The real number r is *rational* if there exist integers p and q with $q \neq 0$ such that $r = p/q$. A real number that is not rational is called *irrational*.

Activity

Determining Whether Numbers Are Rational or Irrational

a. Is $10/3$ a rational number?

b. Is $-\frac{5}{39}$ a rational number?

c. Is 0.281 a rational number?

d. Is 7 a rational number?

e. Is 0 a rational number?

f. Is $2/0$ a rational number?

g. Is $2/0$ an irrational number?

h. Is $0.12121212\ldots$ a rational number (where the digits 12 are assumed to repeat forever)?

THEOREM:

The sum of any rational number and any irrational number is irrational.

Proof:

Suppose r and s are rational numbers. *[We must show that $r + s$ is rational.]* Then, by definition of rational, $r = a/b$ and $s = c/d$ for some integers a, b, c, and d with $b \neq 0$ and $d \neq 0$. Thus

$$r + s = \frac{a}{b} + \frac{c}{d} \qquad \text{by substitution}$$

$$= \frac{ad + bc}{bd} \qquad \text{by basic algebra.}$$

Let $p = ad + bc$ and $q = bd$. Then p and q are integers because products and sums of integers are integers and because a, b, c, and d are all integers. Also $q \neq 0$ by the zero product property. Thus

$$r + s = \frac{p}{q} \text{ where } p \text{ and } q \text{ are integers and } q \neq 0.$$

Therefore, $r + s$ is rational by definition of a rational number. *[This is what was to be shown.]*

EXERCISE:

Prove that if n^2 is not divisible by 25, then n is not divisible by 5.

SOLUTION:

The contra positive statement is:

"if n is divisible by 5, then n^2 is divisible by 25"

Suppose n is divisible by 5. Then by definition of divisibility

$$n = 5 \cdot k \qquad \text{for some integer } k$$

Squaring both sides

$$n^2 = 25 \cdot k^2 \qquad \text{where } k^2 \in Z$$

n^2 is divisible by 25

Proofs by Contradiction

A proof by contradiction is based on the fact that either a statement is true or it is false but not both. Hence the supposition, that the statement to be proved is false, leads logically to a contradiction, impossibility or absurdity, then the supposition must be false. Accordingly, the given statement must be true.

The method of proof by contradiction may be summarized as follows:

1. Suppose the statement to be proved is false.

2. Show that this supposition leads logically to a contradiction.

3. Conclude that the statement to be proved is true.

Basic Idea

Assume that the statement we want to prove is *false, and then show* that this assumption leads to nonsense!

We are then led to conclude that we were wrong to assume the statement was false, so the statement must be true.

Outline for Proof by Contradiction

Proposition P.

Proof. Suppose $\sim P$.

⋮

Therefore $C \wedge \sim C$. ■

EXERCISE:

Give a proof by contradiction for the statement:

"If n^2 is an even integer then n is an even integer."

PROOF:

Suppose n^2 is an even integer and n is not even, so that n is odd.

Hence $n = 2k + 1$ for some integer k.

Now $n^2 = (2k + 1)^2$

$= 4k^2 + 4k + 1$

$= 2 \cdot (2k^2 + 2k) + 1$

$= 2r + 1$ where $r = (2k^2 + 2k) \in Z$

This shows that n^2 is odd, which is a contradiction to our supposition that n^2 is even. Hence the given statement is true.

EXERCISE:

Prove that if n is an integer and $n^3 + 5$ is odd, then n is even using contradiction method.

SOLUTION:

Suppose that $n^3 + 5$ is odd and n is not even (odd). Since n is odd and the product of two odd numbers is odd, it follows that n^2 is odd and $n^3 = n^2 . n$ is odd. Further, since the difference of two odd numbers is even, it follows that

$$5 = (n^3 + 5) - n^3$$

is even. But this is a contradiction. Therefore, the supposition that $n^3 + 5$ and n are both odd is wrong and so the given statement is true.

Prove that $\sqrt{2}$ is irrational by giving a proof by contradiction.

PROOF:

Suppose $\sqrt{2}$ is rational. Then there are integers m and n with no common factors so

$$\sqrt{2} = \frac{m}{n}$$

that

Squaring both sides gives

$$2 = \frac{m^2}{n^2}$$

Or $m^2 = 2n^2$ .....(1)

This implies that m^2 is even (by definition of even). It follows that m is even. Hence

$m = 2k$ for some integer k (2)

Substituting (2) in (1), we get

$$(2k)^2 = 2n^2$$
$$\Rightarrow \quad 4k^2 = 2n^2$$
$$\Rightarrow \quad n^2 = 2k^2$$

This implies that n^2 is even, and so n is even. But we also know that m is even. Hence both m and n have a common factor 2. But this contradicts the supposition that m and n have no common factors. Hence our supposition is false and so the theorem is true.

There exists an integer $k \geq 4$ such that $2k^2 - 5k + 2$ is prime.

Solution

To prove the given statement is false, we prove that its negation is true. The negation of the statement is "For all integers k with $k \geq 4$, $2k^2 - 5k + 2$ is not prime."

Proof of the negation: Suppose k is any integer with $k \geq 4$. *[We must show that* $2k^2 - 5k + 2$ *is not prime.]*. We can factor $2k^2 - 5k + 2$ to obtain $2k^2 - 5k + 2 = (2k - 1)(k - 2)$. But since $k \geq 4$, $k - 2 \geq 2$. Also $2k \geq 2 \cdot 4 = 8$, and thus $2k - 1 \geq 8 - 1 = 7$. This shows that each factor of $2k^2 - 5k + 2$ is a positive integer not equal to 1, and so $2k^2 - 5k + 2$ is not prime.

Proof by Counterexample

Disprove the statement by giving a counter example.
For all real numbers a and b, if $a < b$ then $a^2 < b^2$.

SOLUTION:

Suppose $a = -5$ and $b = -2$
then clearly $-5 < -2$
But $a^2 = (-5)^2 = 25$ and $b^2 = (-2)^2 = 4$
But $25 > 4$
This disproves the given statement.

Proposition

- For all real numbers a and b, if $a^2 = b^2$, then $a = b$.

Solution

- False! Counterexample: $a = 1$ and $b = -1$.
  In this example, $a^2 = b^2$ but $a \neq b$.

Proposition

- For all nonzero integers a and b, if $a|b$ and $b|a$, then $a = b$.

Solution

- False! Counterexample: $a = 1$ and $b = -1$.
  In this example, $a|b$ and $b|a$, however, $a \neq b$.

$2^n + 1$ is prime for any natural number n.

Try out a few examples.

$2^1 + 1 = 3$	prime
$2^2 + 1 = 5$	prime
$2^3 + 1 = 9 = 3^2$	composite

Find a pattern.

$2^n + 1$ can be either prime or composite.

$n^2 + n + 41$ is prime for any whole number n.

- Try out a few examples.

$0^2 + 0 + 41 = 41$	prime
$1^2 + 1 + 41 = 43$	prime
$2^2 + 2 + 41 = 47$	prime
$3^2 + 3 + 41 = 53$	prime
$4^2 + 4 + 41 = 61$	prime
$5^2 + 5 + 41 = 71$	prime

- Find a pattern.
  It seems like $n^2 + n + 41$ is always prime.

EXERCISE:

Prove or give counter example to disprove the statement.

For all integers n, $n^2 - n + 11$ is a prime number.

SOLUTION:

The statement is not true

For n = 11

we have , $n^2 - n + 11 = (11)^2 - 11 + 11$

$= (11)^2$

$= (11)(11)$

$= 121$

which is obviously not a prime number.

Proposition

- There is a natural number n such that $n^2 + 3n + 2$ is prime.

Workout

- Write a formal statement.
  $\exists$ natural number n such that $n^2 + 3n + 2$ is prime.
- Try out a few examples.

$1^2 + 3(1) + 2 = 6$	composite
$2^2 + 3(2) + 2 = 12$	composite
$3^2 + 3(3) + 2 = 20$	composite
$4^2 + 3(4) + 2 = 30$	composite
$5^2 + 3(5) + 2 = 42$	composite

- Find a pattern.
  It seems like $n^2 + 3n + 2$ is always composite.

There is a natural number n such that $n^2 + 3n + 2$ is prime.

Solution

- False!
- Proving that the given statement is false is equivalent to proving that its negation is true.
  Negation. $\forall$ natural number n, $n^2 + 3n + 2$ is composite.
- $n^2 + 3n + 2$
  $= n^2 + n + 2n + 2$ (split $3n$)
  $= n(n+1) + 2(n+1)$ (taking common factors)
  $= (n+1)(n+2)$ (distributive law)
  $=$ composite ($n + 1 > 1$ and $n + 2 > 1$)

Chapter 5

Mathematical Induction

5.1.7 Examples of Proofs by Mathematical Induction

Conjecture: The sum of the first n odd natural numbers equals n^2.

n	sum of the first n odd natural numbers	n^2
1	$1 = \ldots\ldots\ldots\ldots$	1
2	$1+3 = \ldots\ldots\ldots\ldots$	4
3	$1+3+5 = \ldots\ldots\ldots\ldots$	9
4	$1+3+5+7 = \ldots\ldots\ldots\ldots$	16
5	$1+3+5+7+9 = \ldots\ldots\ldots\ldots$	25
⋮	⋮	⋮
n	$1+3+5+7+9+11+\cdots+(2n-1) = \ldots\ldots$	n^2
⋮	⋮	⋮

An infinite ladder

Suppose that we have an infinite ladder, and we want to know whether we can reach every step on this ladder.

We know two things:

1. We can reach the first rung of the ladder.
2. If we can reach a particular rung of the ladder, then we can reach the next rung.

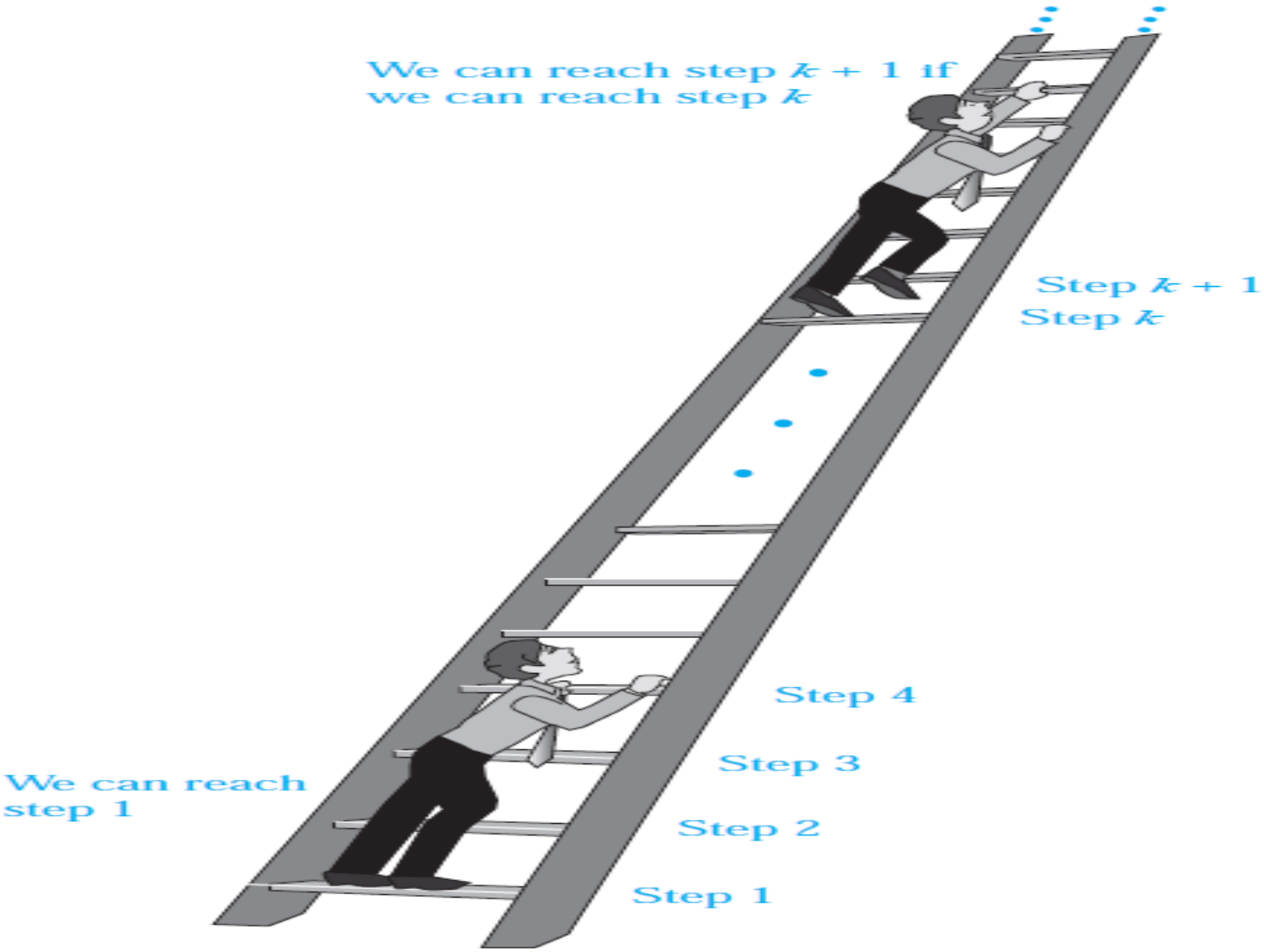


FIGURE 1 **Climbing an Infinite Ladder.**

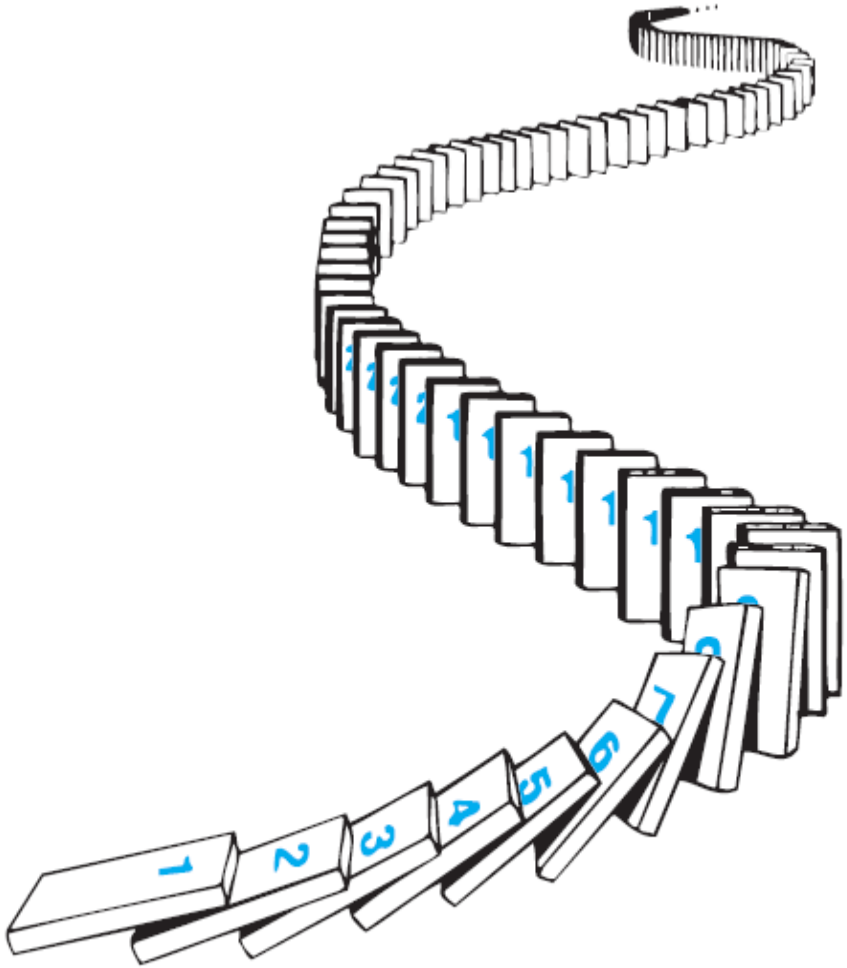
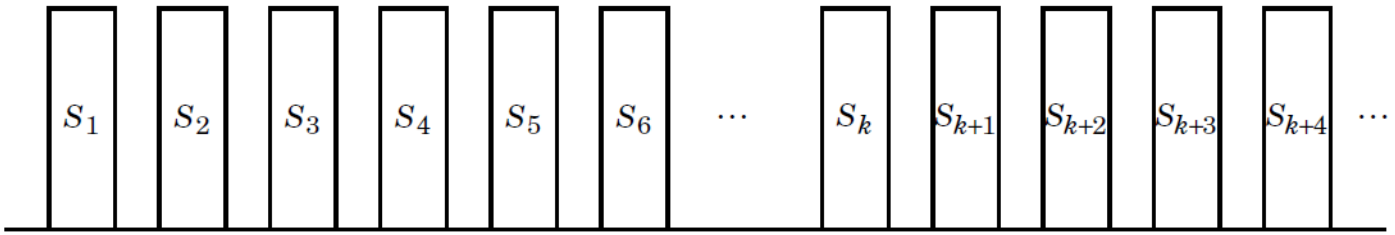
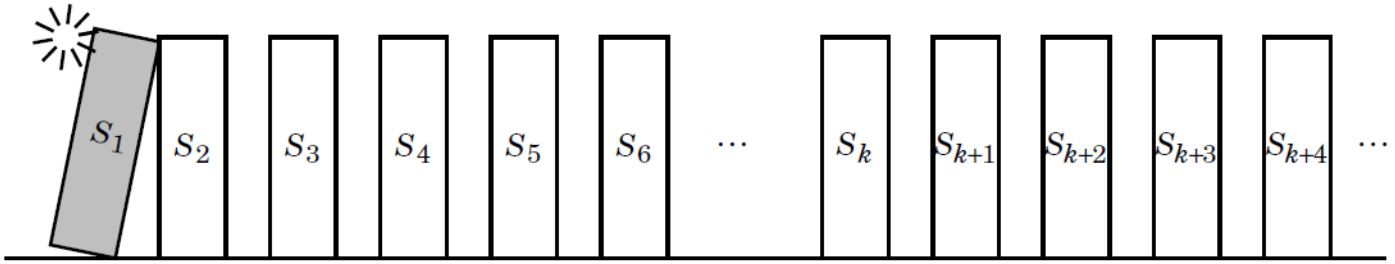


FIGURE 2 **Illustrating How Mathematical Induction Works Using Dominoes.**

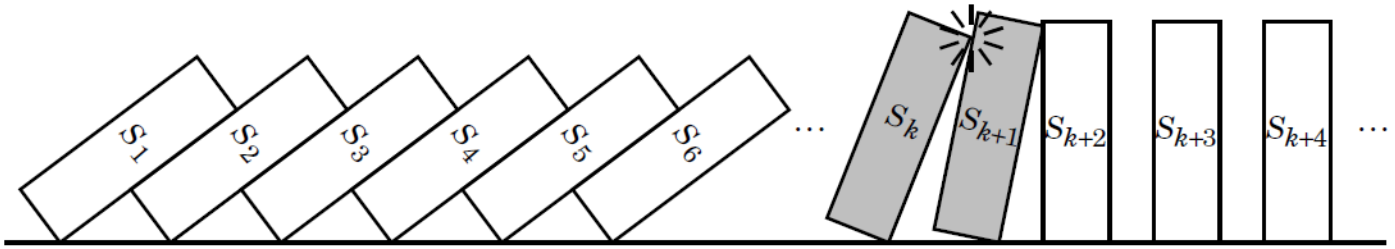
The Simple Idea Behind Mathematical Induction



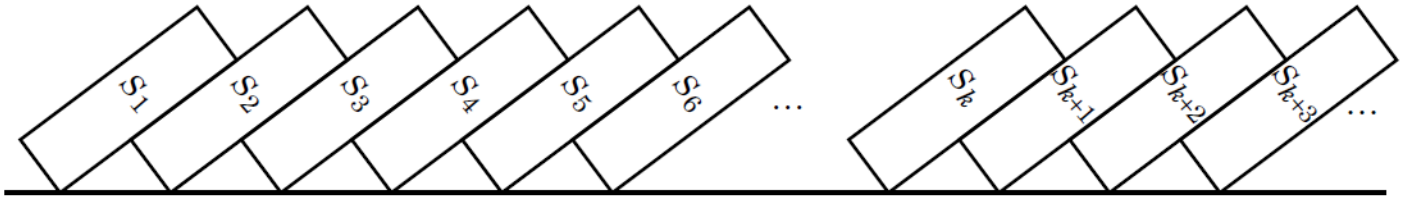
Statements are lined up like dominoes.



(1) Suppose the first statement falls (i.e. is proved true);



(2) Suppose the k^{th} falling always causes the $(k+1)^{th}$ to fall;



Then all must fall (i.e. all statements are proved true).

PRINCIPLE OF MATHEMATICAL INDUCTION:

Let P(n) be a propositional function defined for all positive integers n. P(n) is true for every positive integer n if

1.Basis Step:

The proposition P(1) is true.

2.Inductive Step:

If P(k) is true then P(k + 1) is true for all integers $k \geq 1$.

i.e. $\forall k \quad p(k) \rightarrow P(k+1)$

Example:

Use Mathematical Induction to prove that

$$1+2+3+\cdots+n=\frac{n(n+1)}{2} \quad \text{for all integers } n \geq 1$$

SOLUTION:

Let $$P(n): 1+2+3+\cdots+n=\frac{n(n+1)}{2}$$

1.Basis Step:

P(1) is true.

For n = 1, left hand side of P(1) is the sum of all the successive integers starting at 1 and ending at 1, so LHS = 1 and RHS is

$$R.H.S=\frac{1(1+1)}{2}=\frac{2}{2}=1$$

so the proposition is true for n = 1.

2. Inductive Step: Suppose P(k) is true for, some integers $k \geq 1$.

(1) $$1+2+3+\cdots+k=\frac{k(k+1)}{2}$$

To prove P(k + 1) is true. That is,

$$(2) \qquad 1+2+3+\cdots+(k+1)=\frac{(k+1)(k+2)}{2}$$

Consider L.H.S. of (2)

$$1+2+3+\cdots+(k+1) = 1+2+3+\cdots+k+(k+1)$$

$$= \frac{k(k+1)}{2}+(k+1) \qquad \text{using (1)}$$

$$= (k+1)\left[\frac{k}{2}+1\right]$$

$$= (k+1)\left[\frac{k+2}{2}\right]$$

$$= \frac{(k+1)(k+2)}{2} = \text{RHS of (2)}$$

Hence by principle of Mathematical Induction the given result true for all integers greater or equal to 1.

Applying the Formula for the Sum of the First n Integers

a. Evaluate $2 + 4 + 6 + \cdots + 500$.

b. Evaluate $5 + 6 + 7 + 8 + \cdots + 50$.

Solution

a. $$2 + 4 + 6 + \cdots + 500 = 2 \cdot (1 + 2 + 3 + \cdots + 250)$$
$$= 2 \cdot \left(\frac{250 \cdot 251}{2} \right)$$
$$= 62{,}750.$$

b. $$5 + 6 + 7 + 8 + \cdots + 50 = (1 + 2 + 3 + \cdots + 50) - (1 + 2 + 3 + 4)$$
$$= \frac{50 \cdot 51}{2} - 10$$
$$= 1{,}265$$

Example:

Use mathematical induction to prove that $1+3+5+\ldots+(2n-1) = n^2$ for all integers $n \geq 1$.

SOLUTION:

Let P(n) be the equation $1+3+5+\ldots+(2n-1) = n^2$

1. **Basis Step**:

   P(1) is true

   For n = 1, L.H.S of P(1) = 1and

   R.H.S = 12 = 1

   Hence the equation is true for n = 1

2. **Inductive Step**:

   Suppose P(k) is true for some integer $k \geq 1$. That is,

   $1 + 3 + 5 + \ldots + (2k - 1) = k^2$ .....(1)

   To prove P(k+1) is true; i.e.,

   $1 + 3 + 5 + \ldots + [2(k+1)-1] = (k+1)^2$ .....(2)

Consider L.H.S. of (2)

$$\begin{aligned} 1+3+5+\cdots+[2(k+1)-1] &= 1+3+5+\cdots+(2k+1) \\ &= 1+3+5+\cdots+(2k-1)+(2k+1) \\ &= k^2+(2k+1) \qquad \text{using (1)} \\ &= (k+1)^2 \end{aligned}$$

Example:

Prove by mathematical induction

$$1^2+2^2+3^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6}$$ for all integers n ≥1.

SOLUTION:

Let P(n) denotes the given equation

1. **Basis step:**

P(1) is true

For n = 1

L.H.S of P(1) = 1^2 = 1

$$\text{R.H.S of P(1)} = \frac{1(1+1)(2(1)+1)}{6} = \frac{(1)(2)(3)}{6} = \frac{6}{6} = 1$$

2.Inductive Step:

Suppose P(k) is true for some integer k ≥1;

$$1^2+2^2+3^2+\cdots+k^2=\frac{k(k+1)(2k+1)}{6}$$

To prove P(k+1) is true; i.e.;

$$1^2+2^2+3^2+\cdots+(k+1)^2=\frac{(k+1)(k+1+1)(2(k+1)+1)}{6}$$

$$1^2+2^2+3^2+\cdots+k^2=\frac{k(k+1)(2k+1)}{6}$$

Consider LHS

$$1^2+2^2+3^2+\cdots+(k+1)^2 = 1^2+2^2+3^2+\cdots+k^2+(k+1)^2$$

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

$$= (k+1)\left[\frac{k(2k+1)}{6}+(k+1)\right]$$

$$= (k+1)\left[\frac{k(2k+1)+6(k+1)}{6}\right]$$

$$= (k+1)\left[\frac{2k^2+k+6k+6}{6}\right]$$

$$= \frac{(k+1)(2k^2+7k+6)}{6}$$

$$= \frac{(k+1)(k+2)(2k+3)}{6}$$

$$= \frac{(k+1)(k+1+1)(2(k+1)+1)}{6}$$

Home Activity

Prove by mathematical induction

a) $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{n(n+1)}=\frac{n}{n+1}$ for all integers n≥1

b) $\left(1-\frac{1}{2^2}\right)\cdot\left(1-\frac{1}{3^2}\right)\cdots\left(1-\frac{1}{n^2}\right)=\frac{n+1}{2n}$ for all integers n ≥2

c) For all integers $n \geq 0$:

- $5^n - 1$ is divisible by 4
- $7^n - 1$ is divisible by 6
- $9^n + 3$ is divisible by 4

Example

$$P(n)\colon\ 2^0 + 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$$

Solution:

Basis step $P(0)\colon\ 2^0 = 1 = 2^{0+1} - 1.$

Inductive step:

$$P(k)\colon\ 2^0 + 2^1 + 2^2 + \cdots + 2^k = 2^{k+1} - 1$$

Let's prove $P(k+1)$:

$$\begin{aligned} 2^0 + 2^1 + 2^2 + \cdots + 2^k + 2^{k+1} &= 2^{k+1} - 1 + 2^{k+1} \\ &= 2(2^{k+1}) - 1 \\ &= 2^{k+2} - 1 \end{aligned}$$

$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{n\cdot(n+1)}=\frac{n}{n+1}$ for all integers $n\geq 1$.

Let $P(n)$ denote $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{n\cdot(n+1)}=\frac{n}{n+1}$.

- Basis step. $P(1)$ is true.
- Induction step.

  Assume $P(k)$: $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{k\cdot(k+1)}=\frac{k}{k+1}$ for some $k\geq 1$

  Prove $P(k+1)$: $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{(k+1)\cdot(k+2)}=\frac{k+1}{k+2}$

  LHS of $P(k+1)$

  $=\left(\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{k\cdot(k+1)}\right)+\frac{1}{(k+1)\cdot(k+2)}$

  $=\frac{k}{k+1}+\frac{1}{(k+1)\cdot(k+2)}$ ($\because P(k)$ is true)

  $=\frac{k^2+2k+1}{(k+1)\cdot(k+2)}$ ($\because$ common denominator)

  $=\frac{(k+1)^2}{(k+1)\cdot(k+2)}$ ($\because$ simplify)

  $=\frac{k+1}{k+2}$ ($\because$ remove common factor)

  $=$ RHS of $P(k+1)$

Example:

For all integers $n \geq 0$, $2^{2n} - 1$ is divisible by 3.

Solution:

Let the property $P(n)$ be the sentence "$2^{2n} - 1$ is divisible by 3."

$$2^{2n} - 1 \text{ is divisible by } 3. \quad \leftarrow P(n)$$

Show that P(0) is true:
To establish $P(0)$, we must show that

$$2^{2 \cdot 0} - 1 \text{ is divisible by } 3. \quad \leftarrow P(0)$$

$$2^{2 \cdot 0} - 1 = 2^0 - 1 = 1 - 1 = 0$$

and 0 is divisible by 3 because $0 = 3 \cdot 0$. Hence $P(0)$ is true.

Show that for all integers $k \geq 0$, if $P(k)$ is true then $P(k+1)$ is also true:

Let k be any integer with $k \geq 0$, and suppose that

$2^{2k} - 1$ is divisible by 3. ← $P(k)$ inductive hypothesis

By definition of divisibility, this means that

$2^{2k} - 1 = 3r$ for some integer r.

[We must show that $P(k+1)$ is true. That is:] We must show that

$2^{2(k+1)} - 1$ is divisible by 3. ← $P(k+1)$

$$
\begin{aligned}
2^{2(k+1)} - 1 &= 2^{2k+2} - 1 \\
&= 2^{2k} \cdot 2^2 - 1 \\
&= 2^{2k} \cdot 4 - 1 \\
&= 2^{2k}(3+1) - 1 \\
&= 2^{2k} \cdot 3 + (2^{2k} - 1) \\
&= 2^{2k} \cdot 3 + 3r \\
&= 3(2^{2k} + r)
\end{aligned}
$$

definition of divisibility, $2^{2(k+1)} - 1$ is divisible by 3

$2^{2n} - 1$ is divisible by 3, for all integers $n \geq 0$.

Proof:

Let $P(n)$ denote $2^{2n} - 1$ is divisible by 3.

- Basis step. $P(0)$ is true.
- Induction step. Suppose that $P(k)$ is true for some $k \geq 0$.
  Now, we want to show that $P(k+1)$ is true.
  LHS of $P(k+1)$
  $= 2^{2(k+1)} - 1$
  $= 2^2 \cdot 2^{2k} - 1$ $(\because a^{b+c} = a^b \cdot a^c)$
  $= (3+1) \cdot 2^{2k} - 1$ ($\because$ rewrite)
  $= 3 \cdot 2^{2k} + (2^{2k} - 1)$ ($\because$ distributive law)
  $= 3 \cdot 2^{2k} + 3r$ ($\because P(k)$ is true)
  $= 3 \cdot (2^{2k} + r)$ ($\because$ distributive law)
  $= 3 \cdot$ integer ($\because$ addition is closed on integers)
  $=$ RHS of $P(k+1)$

$n^2 < 2^n$, for all integers $n \geq 5$.

Proof:

Let $P(n)$ denote $n^2 < 2^n$.

- Basis step. $P(5)$ is true.
- Induction step. Suppose that $P(k)$ is true for some $k \geq 5$.
  Now, we want to show that $P(k+1)$ is true.

  LHS of $P(k+1)$

  $= (k+1)^2 = k^2 + 2k + 1$ ($\because$ expand)

  $< k^2 + 2k + k$ ($\because 1 < k$)

  $= k^2 + 3k$ ($\because$ simplify)

  $< k^2 + k^2$ ($\because 3 < k$)

  $= 2k^2$ ($\because$ simplify)

  $< 2 \cdot 2^k$ ($\because P(k)$ is true)

  $= 2^{k+1}$ ($\because a^b \cdot a^c = a^{b+c}$)

  $=$ RHS of $P(k+1)$

$2^n < n!$, for all integers $n \geq 4$.

Proof:

Let $P(n)$ denote $2^n < n!$.

- Basis step. $P(4)$ is true.
- Induction step. Suppose that $P(k)$ is true for some $k \geq 4$.
  Now, we want to show that $P(k+1)$ is true.
  LHS of $P(k+1)$
  $= 2^{k+1}$
  $= 2^k \cdot 2$ $\quad (\because a^{b+c} = a^b \cdot a^c)$
  $< k! \cdot 2$ $\quad (\because P(k)$ is true$)$
  $< k! \cdot (k+1)$ $\quad (\because 2 < (k+1)$ for $k \geq 4)$
  $= (k+1)!$ $\quad (\because$ factorial recursive definition$)$
  $=$ RHS of $P(k+1)$

Problem

- Prove that $\frac{1}{1^2}+\frac{1}{2^2}+\cdots+\frac{1}{n^2}<2$ for all natural numbers $n \geq 1$.

Basis step. $P(2)$ is true.

Induction step. Suppose that $P(k)$ is true for some $k \geq 2$.

We need to prove that $P(k+1)$ is true.

LHS of $P(k+1)$

$= \left(\frac{1}{1^2}+\frac{1}{2^2}+\cdots+\frac{1}{k^2}\right)+\frac{1}{(k+1)^2}$

$< \left(2-\frac{1}{k}\right)+\frac{1}{(k+1)^2}$ ($\because P(k)$ is true)

$= 2-\frac{(k+1)^2-k}{k(k+1)^2}$ ($\because$ taking common denominator)

$= 2-\frac{k(k+1)+1}{k(k+1)^2}$ ($\because$ simplify)

$< 2-\frac{k(k+1)}{k(k+1)^2}$ ($\because$ decrease 1 in the numerator)

$= 2-\frac{1}{k+1}$ ($\because$ canceling common factors)

$=$ RHS of $P(k+1)$

Example:

For all integers $n \geq 3$, $2n + 1 < 2^n$.

Solution:

Let the property $P(n)$ be the inequality

$$2n + 1 < 2^n. \quad \leftarrow P(n)$$

Show that P(3) is true:

To establish $P(3)$, we must show that

$$2 \cdot 3 + 1 < 2^3. \quad \leftarrow P(3)$$

But

$$2 \cdot 3 + 1 = 7 \quad \text{and} \quad 2^3 = 8 \quad \text{and} \quad 7 < 8.$$

Hence $P(3)$ is true.

Show that for all integers $k \geq 3$, if P(k) is true then P(k + 1) is also true:

$2k + 1 < 2^k$. $\leftarrow P(k)$ inductive hypothesis

[We must show that $P(k + 1)$ is true. That is:] We must show that

$$2(k + 1) + 1 < 2^{(k+1)},$$

or, equivalently,

$$2k + 3 < 2^{(k+1)}. \quad \leftarrow P(k + 1)$$

But

$$2k + 3 = (2k + 1) + 2$$
$$< 2^k + 2^k$$
$$\therefore 2k + 3 < 2 \cdot 2^k = 2^{k+1}$$

Practice:

Q1) Solve the following with defined type of proof method.

a) Prove the statement: There is an integer n > 5 such that $2^n - 1$ is prime.

b) Prove that for any integer a and any prime number p, if p | a, P | (a + 1).

c) Prove the statement: There are real numbers a and b such that $\sqrt{(a+b)} = \sqrt{a} + \sqrt{b}$.

d) Prove that if |x| > 1 then x > 1 or x < –1 for all x € R.

e) Find a counter example to the proposition: For every prime number n, n + 2 is prime.

f) Show that the set of prime numbers is infinite.

Q2) Prove by contradiction method, the statement:

a) If n and m are odd integers, then n + m is an eveninteger.

b) Prove the statement by contraposition: For all integers m and n, if m + n is even then m and nare both even or m and n are both odd.

c) Prove by contradiction that $6 - 7\sqrt{2}$ is irrational.

d) Prove by contradiction that $\sqrt{2} + \sqrt{3}$ is irrational.

Q3) By mathematical induction,

a) prove that following is true for all positive integral values of n.(a) $1^2 + 2^2 + 3^2 + \ldots\ldots + n^2 = (n(n+1)(2n+1))/6$

b) $1+2+2^2 + \ldots + 2^n = 2^{n+1} - 1$ for all integers $n \geq 0$

c) $1^3 + 2^3 + 3^3 + \ldots + n^3 = \frac{1}{4} n^2(n+1)^2$

- The greatest common divisor (GCD) of two integers a and b is the largest integer that divides both a and b.
- A simple way to compute GCD:
  1. Find the divisors of the two numbers
  2. Find the common divisors
  3. Find the greatest of the common divisors

Recursive algorithm (Euclidean algorithm)

Input: Nonnegative integers a and b such that $a > b$.
Output: Greatest common divisor of a and b.

1. if $b = 0$ then
2. return a
3. else
4. return $\mathrm{GCD}(b, a \bmod b)$

Examples

- $\mathrm{GCD}(2, 100) = 2$
- $\mathrm{GCD}(3, 99) = 3$
- $\mathrm{GCD}(3, 4) = 1$
- $\mathrm{GCD}(12, 30) = 6$
- $\mathrm{GCD}(1071, 462) = 21$

- Recurrence relation: Suppose $a > b$.

$$\mathrm{GCD}(a, b) = \begin{cases} a & \text{if } \ b = 0, \\ \mathrm{GCD}(b, a \bmod b) & \text{if } \ b \geq 1. \end{cases}$$

- $\mathrm{GCD}(1071, 462)$
  $= \mathrm{GCD}(462, 1071 \bmod 462)$
  $= \mathrm{GCD}(462, 147) \qquad (\because 1071 = 2 \cdot 462 + 147)$
  $= \mathrm{GCD}(147, 462 \bmod 147)$
  $= \mathrm{GCD}(147, 21) \qquad (\because 462 = 3 \cdot 147 + 21)$
  $= \mathrm{GCD}(21, 147 \bmod 21)$
  $= \mathrm{GCD}(21, 0) \qquad (\because 147 = 7 \cdot 21 + 0)$
  $= 21$