Peano's Axioms

- There is a number 0.
- Every number has a successor, denoted by S(a).
- There is no number whose successor is 0, i.e., $\forall x\, (S(x) \neq 0)$.
- Two numbers with the same successor are themselves equal, i.e., $\forall x\, \forall y (S(x) = S(y) \rightarrow x = y)$
- If a property is possessed by 0 and if the successor of every number possessing the property also possesses it, then it is possessed by every number, i.e., $[Q(0) \wedge \forall x(Q(x) \rightarrow Q(S(x))] \rightarrow \forall x Q(x)$

The Principle of Mathematical Induction

A proof by mathematical induction that a proposition P(n) is true for every positive integer n consists of two steps:

BASE CASE: Show that P(1) is true.

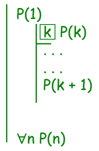
INDUCTIVE STEP: Assume that P(k) is true for an arbitrarily chosen positive integer k and show that under that assumption, P(k + 1) must be true.

From these two steps we conclude (by the principle of mathematical induction) that for all positive integers n, P(n) is true.

Note that in the inductive step, you are proving a conditional:

IF P(k) for some arbitrary k, THEN P(k + 1).

Here is a Fitch version



Show that for any positive integer n, $n^5 - n$ is divisible by 5.

Proof by Mathematical Induction.
P(n): $n^5 - n$ is divisible by 5

BASE CASE: P(1) asserts that $1^5 - 1$ is divisible by 5.
$1^5 - 1 = 0$, and since 0 is divisible by 5, P(1) is true.

INDUCTIVE STEP:
Assume for some positive integer k, P(k): $k^5 - k$ is divisible by 5

Show P(k + 1): $(k + 1)^5 - (k + 1)$ is divisible by 5

Proof of the inductive step:

$$(k + 1)^5 - (k + 1) = k^5 + 5k^4 + 10k^3 + 10k^2 + 5k + 1 - k - 1$$
$$= (k^5 - k) + 5(k^4 + 2k^3 + 2k^2 + k)$$

Since $k^5 - k$ is divisible by 5 by the inductive hypothesis, the RHS is divisible by 5 and P(k + 1) is true.

Thus $n^5 - n$ is divisible by 5 for any $n > 0$ by the principle of mathematical induction.

Bad Induction

Show that for any positive n, $n^3 - n + 1$ is a multiple of 3.

P(n): $n^3 - n + 1$ is a multiple of 3

We will show that if we assume P(k) is true, then P(k + 1) is true

$$(k + 1)^3 - (k + 1) + 1 = k^3 + 3k^2 + 3k + 1 - k = \underbrace{k^3 - k + 1} + \underbrace{3(k^2 + k)}$$

Divisible by 3 by inductive hypothesis

Obviously divisible by 3

Bad Induction

Show that for any positive n, $n^3 - n + 1$ is a multiple of 3.

P(n): $n^3 - n + 1$ is a multiple of 3

We will show that if we assume P(k) is true, then P(k + 1) is true

$$(k + 1)^3 - (k + 1) + 1 = k^3 + 3k^2 + 3k + 1 - k = \underbrace{k^3 - k + 1} + \underbrace{3(k^2 + k)}$$

Divisible by 3 by inductive hypothesis

Obviously divisible by 3

So P(k + 1) is true and P(n) is true for all n.

What's wrong?

The Well-Ordering Property

Every non-empty set of positive integers has a least element.

From this axiom, we can prove that the Principle of Mathematical Induction is correct.

The Well-Ordering Property

Every non-empty set of positive integers has a least element.

From this axiom, we can prove that the Principle of Mathematical Induction is correct.

Suppose that for some P(n) we show the base case P(1) and the inductive step $\forall k \geq 1$ (P(k) → P(k+1)). In order to derive a contradiction, suppose that it is not the case that $\forall n$P(n) where $n \geq 1$. Then $\exists n(\neg P(n))$.

Let S be the set of positive integers for which $\neg$P(n). Since S is not empty, by the well-ordering property it must have a least element, which we will call m.

$m > 1$, since we know that P(1) is true. So $m - 1$ is a positive integer, and since $m - 1 < m$, $m - 1$ is not in S. But in that case, P(m-1) is true and the inductive step tells us that P(m) must be true, which contradicts the fact that m is in S.

Therefore it must be the case that $\forall n$P(n).

Weak Mathematical Induction

To show that P(n) is true for every positive integer $n \geq$ base:

BASE CASE: Show that P(base) is true.

INDUCTIVE STEP: Assume that P(k) is true for some $k \geq$ base.
Show that P(k+1) must be true.

Strong (Complete) Mathematical Induction

To show that P(n) is true for every positive integer $n \geq$ base:

BASE CASE: Show that P(base) is true.

INDUCTIVE STEP: Assume that P(base), P(base+1),...P(k) is true for some $k \geq$ base.
Show that P(k+1) must be true.

We can prove that Strong Induction works using an argument like the one we gave for Weak Induction.

Fundamental Theorem of Arithmetic

For all integers $n \geq 2$, the following is true:

P(n): either n is prime or n is the product of primes.

BASE CASE: P(2) is true since 2 is prime.

INDUCTION STEP (strong induction on n):

Assume: for an arbitrary integer k, P(i) for $2 \leq i \leq k$
Show: P(k+1), i.e., that k+1 is prime or has a prime factorization.

Fundamental Theorem of Arithmetic

For all integers $n \geq 2$, the following is true:

P(n): either n is prime or n is the product of primes.

BASE CASE: P(2) is true since 2 is prime.

INDUCTION STEP (strong induction on n):

Assume: for an arbitrary integer k, P(i) for $2 \leq i \leq k$
Show: P(k+1), i.e., that k+1 is prime or has a prime factorization.

We introduce a new variable i
in order to state the assumption.

Fundamental Theorem of Arithmetic

For all integers $n \geq 2$, the following is true:

P(n): either n is prime or n is the product of primes.

BASE CASE: P(2) is true since 2 is prime.

INDUCTION STEP (strong induction on n):

Assume: for an arbitrary integer k, P(i) for $2 \leq i \leq k$
Show: P(k+1), i.e., that k+1 is prime or has a prime factorization.

If k+1 is prime, we are done.

Fundamental Theorem of Arithmetic

For all integers $n \geq 2$, the following is true:

P(n): either n is prime or n is the product of primes.

BASE CASE: P(2) is true since 2 is prime.

INDUCTION STEP (strong induction on n):

Assume: for an arbitrary integer k, P(i) for $2 \leq i \leq k$
Show: P(k+1), i.e., that k+1 is prime or has a prime factorization.

If k+1 is prime, we are done.

"we have shown the desired result for this case."

"then P(k+1) trivially holds."

"then P(k+1) is true."

Fundamental Theorem of Arithmetic

For all integers $n \geq 2$, the following is true:

P(n): either n is prime or n is the product of primes.

BASE CASE: P(2) is true since 2 is prime.

INDUCTION STEP (strong induction on n):

Assume: for an arbitrary integer k, P(i) for $2 \leq i \leq k$
Show: P(k+1), i.e., that k+1 is prime or has a prime factorization.

If k+1 is prime, then P(k+1) is true.

Fundamental Theorem of Arithmetic

For all integers $n \geq 2$, the following is true:

P(n): either n is prime or n is the product of primes.

BASE CASE: P(2) is true since 2 is prime.

INDUCTION STEP (strong induction on n):

Assume: for an arbitrary integer k, P(i) for $2 \leq i \leq k$
Show: P(k+1), i.e., that k+1 is prime or has a prime factorization.

If k+1 is prime, then P(k+1) is true.

If k+1 is composite, there exist integers a and $b \neq 1$ such that ab = k+1.
Clearly, $2 \leq a \leq k$ and $2 \leq b \leq k$.

"The following should be obvious to readers of this proof."

"You may not see this right away, but work on it a little bit and you will."

Fundamental Theorem of Arithmetic

For all integers $n \geq 2$, the following is true:

P(n): either n is prime or n is the product of primes.

BASE CASE: P(2) is true since 2 is prime.

INDUCTION STEP (strong induction on n):

Assume: for an arbitrary integer k, P(i) for $2 \leq i \leq k$
Show: P(k+1), i.e., that k+1 is prime or has a prime factorization.

If k+1 is prime, then P(k+1) is true.

If k+1 is composite, there exist integers a and $b \neq 1$ such that ab = k+1.
Clearly, $2 \leq a \leq k$ and $2 \leq b \leq k$, since a or b > k would mean ab > k+1.

Fundamental Theorem of Arithmetic

For all integers $n \geq 2$, the following is true:

P(n): either n is prime or n is the product of primes.

BASE CASE: P(2) is true since 2 is prime.

INDUCTION STEP (strong induction on n):

Assume: for an arbitrary integer k, P(i) for $2 \leq i \leq k$
Show: P(k+1), i.e., that k+1 is prime or has a prime factorization.

If k+1 is prime, then P(k+1) is true.

If k+1 is composite, there exist integers a and $b \neq 1$ such that ab = k+1.
Clearly, $2 \leq a \leq k$ and $2 \leq b \leq k$, since a or b > k would mean ab > k+1.

By the inductive hypothesis, a and b have prime factorizations or are primes, so k+1 is the product of a or its prime factors and b or its prime factors. Thus k+1 is the product of primes, and P(k+1) is true.

Therefore P(n) is true for all $n \geq 2$. (We also need to show uniqueness.)

Fundamental Theorem of Arithmetic

For all integers $n \geq 2$, the following is true:

P(n): either n is prime or n is the product of primes.

BASE CASE: P(2) is true since 2 is prime.

INDUCTION STEP (strong induction on n):

Assume: for an arbitrary integer k, P(i) for $2 \leq i \leq k$
Show: P(k+1), i.e., that k+1 is prime or has a prime factorization.

If k+1 is prime, then P(k+1) is true. Not necessarily k

If k+1 is composite, there exist integers a and $b \neq 1$ such that ab = k+1.
Clearly, $2 \leq a \leq k$ and $2 \leq b \leq k$, since a or b > k would mean ab > k+1.

By the inductive hypothesis, a and b have prime factorizations or are primes, so k+1 is the product of a or its prime factors and b or its prime factors. Thus k+1 is the product of primes, and P(k+1) is true.

Therefore P(n) is true for all $n \geq 2$. (We also need to show uniqueness.)

Suppose $b_0, b_1, b_2, \ldots$ is the sequence defined as follows:

$b_0 = 1$,
$b_1 = 2$,
$b_2 = 3$,
$b_j = b_{j-3} + b_{j-2} + b_{j-1}$ for all integers $j \geq 3$.

Let P(n) be the assertion $b_n \leq 3^n$.

Show that P(n) is true for $n \geq 0$.

BASE CASE: We will establish the three base cases: P(0), P(1), P(2).

$b_0 = 1$, which is $\leq 3^0$
$b_1 = 2$, which is $\leq 3^1$
$b_2 = 3$, which is $\leq 3^2$

So P(0), P(1), and P(2) are true.

Suppose b_0, b_1, b_2,...is the sequence defined as follows:
$b_0 = 1$,
$b_1 = 2$,
$b_2 = 3$,
$b_j = b_{j-3} + b_{j-2} + b_{j-1}$ for all integers $j \geq 3$.

Let P(n) be the assertion $b_n \leq 3^n$.

Show that P(n) is true for $n \geq 0$.

INDUCTION STEP:
For an arbitrary integer $k > 2$, assume P(i) for $0 \leq i < k$; that is, $b_i \leq 3^i$
Show P(k): $b_k \leq 3^k$

Note the slightly different pattern:

i strictly less than k

k rather than k+1 here

Suppose b_0, b_1, b_2,...is the sequence defined as follows:
$b_0 = 1$,
$b_1 = 2$,
$b_2 = 3$,
$b_j = b_{j-3} + b_{j-2} + b_{j-1}$ for all integers $j \geq 3$.

Let P(n) be the assertion $b_n \leq 3^n$.

Show that P(n) is true for $n \geq 0$.

INDUCTION STEP:
For an arbitrary integer $k > 2$, assume P(i) for $0 \leq i < k$; that is, $b_i \leq 3^i$
Show P(k): $b_k \leq 3^k$

By the inductive hypothesis, $b_{k-3} + b_{k-2} + b_{k-1} \leq 3^{k-3} + 3^{k-2} + 3^{k-1}$

$$\leq 3^{k-1} + 3^{k-1} + 3^{k-1}$$

$$\leq 3(3^{k-1}) = 3^k$$

$$b_k \leq 3^k$$

So P(n) is true for $n \geq 0$.

Show that any amount of money of at least 8¢ can be obtained from 3¢ and 5¢ coins.

BASE CASE: 8¢ can be obtained from 3¢ + 5¢

Show that any amount of money of at least 8¢ can be obtained from 3¢ and 5¢ coins.

BASE CASE: 8¢ can be obtained from 3¢ + 5¢

INDUCTION STEP:
Assume k¢ can be obtained for $k \geq 8$, show (k+1)¢ can be obtained.

Case 1: k includes a 5¢ coin.

Case 2: k does not include a 5¢ coin.

Show that any amount of money of at least 8¢ can be obtained from 3¢ and 5¢ coins.

BASE CASE: 8¢ can be obtained from 3¢ + 5¢

INDUCTION STEP:
Assume k¢ can be obtained for $k \geq 8$, show (k+1)¢ can be obtained.

Case 1: k includes a 5¢ coin.
Remove 5¢ and add two 3¢ coins to obtain (k+1)¢.

Case 2: k does not include a 5¢ coin.
k must be at least 9¢.
Remove three 3¢ coins and add two 5¢ coins to obtain (k+1)¢.

The jigsaw problem (Example 7) from Handout #48:

Block: a single piece or a number of pieces with matched boundaries that have been put together

Blocks can be put together to make larger blocks.

Putting two blocks together is called a move.

Show that a puzzle of n pieces always takes n-1 moves to solve.

BASE CASE: A puzzle of 1 piece takes no moves to solve.

The jigsaw problem (Example 7) from Handout #48:

Block: a single piece or a number of pieces with matched boundaries that have been put together

Blocks can be put together to make larger blocks.

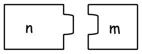
Putting two blocks together is called a move.

Show that a puzzle of n pieces always takes n-1 moves to solve.

BASE CASE: A puzzle of 1 piece takes no moves to solve.

INDUCTION STEP: Assume P(i) for $1 \le i \le k$: a puzzle of i pieces takes i-1 moves to solve.
Show P(k+1): a puzzle of k+1 pieces takes k moves.

Last move in k+1 piece puzzle



The jigsaw problem (Example 7) from Handout #48:

Block: a single piece or a number of pieces with matched boundaries that have been put together

Blocks can be put together to make larger blocks.

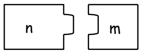
Putting two blocks together is called a move.

Show that a puzzle of n pieces always takes n-1 moves to solve.

BASE CASE: A puzzle of 1 piece takes no moves to solve.

INDUCTION STEP: Assume P(i) for $1 \le i \le k$: a puzzle of i pieces takes i-1 moves to solve.
Show P(k+1): a puzzle of k+1 pieces takes k moves.

Last move in k+1 piece puzzle



total pieces n + m = k+1

total moves = n – 1 + m – 1 + 1
= n + m -1
= (k + 1) – 1
= k

The Law of Bad Proofs:

You can prove anything you want if your proof is wrong.

P(n) denotes that every set of n horses are all the same color. Show P(n) for all $n \ge 1$.

BASE CASE: prove that P(1) is true. If X is a set of 1 horse, then all the horses in X are the same color.
INDUCTION STEP:
Assume P(k) is true: every set of k horses are all the same color.
Show P(k+1): every set of k+1 horses are all the same color.
Suppose X is a set of k+1 horses. To show that all the horses in X are the same color, it's enough to show that

If h1 is in X and h2 is in X, then h1 is the same color as h2.

If we can prove this, we are done because either h1 or h2 is in a set of k horses, and we know that a set of k horses are all the same color.

P(n) denotes that every set of n horses are all the same color. Show P(n) for all $n \ge 1$.

BASE CASE: prove that P(1) is true. If X is a set of 1 horse, then all the horses in X are the same color.
INDUCTION STEP:
Assume P(k) is true: every set of k horses are all the same color.
Show P(k+1): every set of k+1 horses are all the same color.
Suppose X is a set of k+1 horses. To show that all the horses in X are the same color, it's enough to show that

If h1 is in X and h2 is in X, then h1 is the same color as h2.

If we can prove this, we are done because either h1 or h2 is in a set of k horses, and we know that a set of k horses are all the same color.

Let X1 = X - h1 and X2 = X - h2

X1 and X2 have k horses and by the inductive hypothesis, the k horses in each of these sets are all the same color. So, if we take a horse z which is a horse in the intersection of X1 and X2 (that being one of the horses that X1 and X2 have in common), we know that

h1 must be the same color as z, and
h2 must be the same color as z;

therefore, h1 is the same color as h2. We have proven that all horses are the same color.