Math 321: Mathematical Induction

Kameryn J Williams

University of Hawaiʻi at Mānoa

Spring 2021

Previously in Math 321

When we talked about number theory, many of our proofs ended up relying on mathematical induction or, in another guiese, the least number principle.

Previously in Math 321

When we talked about number theory, many of our proofs ended up relying on mathematical induction or, in another guiese, the least number principle.

- All over mathematics it is common to use proofs by induction, so let's discuss induction in more detail.

Previously in Math 321

When we talked about number theory, many of our proofs ended up relying on mathematical induction or, in another guiese, the least number principle.

- All over mathematics it is common to use proofs by induction, so let's discuss induction in more detail.
- Also, induction is a fundamental property about the natural numbers, a principle which underlies other facts about the natural numbers.

The least number principle

- If there is a natural number with a property, there is a smallest natural number with that property.

The least number principle

- If there is a natural number with a property, there is a smallest natural number with that property.
- If $X \subseteq \mathbb{N}$ is nonempty, then X has a smallest element.

The least number principle

- If there is a natural number with a property, there is a smallest natural number with that property.
- If $X \subseteq \mathbb{N}$ is nonempty, then X has a smallest element.

You don't have to start counting from 0 for this; it's still true if you say "positive integer" instead of "natural number", or even "integer $> k$" instead of "natural number".

A simple example

Theorem

For any finite list $n_1, n_2, \ldots, n_k$ of integers, there is a smallest natural number which is a multiple of all of them, called their least common multiple.

A simple example

Theorem

For any finite list $n_1, n_2, \ldots, n_k$ of integers, there is a smallest natural number which is a multiple of all of them, called their least common multiple.

Proof.

Observe that $|n_1 n_2 \cdots n_k|$ is a natural number which is a common multiple of all these n_i. So there is a smallest common multiple. □

A simple example

Theorem

For any finite list $n_1, n_2, \ldots, n_k$ of integers, there is a smallest natural number which is a multiple of all of them, called their least common multiple.

Proof.

Observe that $|n_1 n_2 \cdots n_k|$ is a natural number which is a common multiple of all these n_i. So there is a smallest common multiple. □

I won't prove it, but in fact there is a formula for the least common multiple:

$$\operatorname{lcm}(n_1, n_2, \ldots, n_k) = \frac{|n_1 n_2 \cdots n_k|}{\gcd(n_1, n_2, \ldots, n_k)},$$

where $\gcd(\cdots)$ is the greatest common divisor.

Mathematical induction

- Let $P(n)$ be a predicate about natural numbers. If for each n we have that $P(k)$ for all $k < n$ implies $P(n)$, then $P(n)$ is true for every $n \in \mathbb{N}$.
- Suppose $X \subseteq \mathbb{N}$ is a set of natural numbers. If for each n we have that $k \in X$ for all $k < n$ implies $n \in X$, then $X = \mathbb{N}$.

Mathematical induction

- Let $P(n)$ be a predicate about natural numbers. If for each n we have that $P(k)$ for all $k < n$ implies $P(n)$, then $P(n)$ is true for every $n \in \mathbb{N}$.
- Suppose $X \subseteq \mathbb{N}$ is a set of natural numbers. If for each n we have that $k \in X$ for all $k < n$ implies $n \in X$, then $X = \mathbb{N}$.

Note that the statement about each n is itself an if-then statement (just phrased in different language).

Mathematical induction

- Let $P(n)$ be a predicate about natural numbers. If for each n we have that $P(k)$ for all $k < n$ implies $P(n)$, then $P(n)$ is true for every $n \in \mathbb{N}$.
- Suppose $X \subseteq \mathbb{N}$ is a set of natural numbers. If for each n we have that $k \in X$ for all $k < n$ implies $n \in X$, then $X = \mathbb{N}$.

Note that the statement about each n is itself an if-then statement (just phrased in different language). One way to think about induction is that it allows you to use extra information to prove something about all natural numbers.

Mathematical induction

- Let $P(n)$ be a predicate about natural numbers. If for each n we have that $P(k)$ for all $k < n$ implies $P(n)$, then $P(n)$ is true for every $n \in \mathbb{N}$.
- Suppose $X \subseteq \mathbb{N}$ is a set of natural numbers. If for each n we have that $k \in X$ for all $k < n$ implies $n \in X$, then $X = \mathbb{N}$.

Note that the statement about each n is itself an if-then statement (just phrased in different language). One way to think about induction is that it allows you to use extra information to prove something about all natural numbers.

- (Direct proof) Consider an arbitrary n and prove $P(n)$.
- (Inductive proof) Consider an arbitrary n, assume $P(k)$ for all $k < n$, and then prove $P(n)$.

An example we've seen before

Theorem (Fundamental theorem of arithmetic, existence)

Every positive integer can be expressed as a product of primes.

An example we've seen before

Theorem (Fundamental theorem of arithmetic, existence)

Every positive integer can be expressed as a product of primes.

Proof.

We prove this by induction. The case $n = 1$ is trivial, so consider the $n > 1$ case. Assume that we have the result for all $k < n$. There are now two cases. If n is prime, then its prime factorization is $n = n$, so we are trivially done. Otherwise, n is a product of two smaller positive integers, say $n = ab$. By indctive hypothesis, a and b each have prime factorizations. Multiplying together their factorizations gives a prime factorization for n. □

An example we've seen before

Theorem (Fundamental theorem of arithmetic, existence)

Every positive integer can be expressed as a product of primes.

Proof.

We prove this by induction. The case $n = 1$ is trivial, so consider the $n > 1$ case. Assume that we have the result for all $k < n$. There are now two cases. If n is prime, then its prime factorization is $n = n$, so we are trivially done. Otherwise, n is a product of two smaller positive integers, say $n = ab$. By indctive hypothesis, a and b each have prime factorizations. Multiplying together their factorizations gives a prime factorization for n. □

One way to think of this is, we reduced the problem of finding a prime factorization for n to finding a prime factorization for smaller numbers. If we can reduce a problem to a smaller problem, then induction says that's always enough to find a solution.

Different looks at the same phenomenon

Theorem

The least number principle and induction are equivalent.

Different looks at the same phenomenon

Theorem

The least number principle and induction are equivalent.

Proof that LNP $\rightarrow$ induction.

$\square$

Different looks at the same phenomenon

Theorem

The least number principle and induction are equivalent.

Proof that induction $\to$ LNP.

$\square$

Yet another way to formulate this phenomenon

Here's yet another way to formulate induction:

- There is no infinite strictly decreasing sequence of natural numbers. In other words, if you have an infinite descending sequence

$$n_1 \geq n_2 \geq \cdots \geq n_k \geq \cdots$$

of natural numbers, then the sequence is eventually constant—for all large enough k, the values n_k must all be the same.

An application: computing the gcd

Lemma

Let a and b be positive integers, and suppose $b = aq + r$ is the Euclidean division for b divided by a. Then,

$$\gcd(a, b) = \gcd(a, r).$$

An application: computing the gcd

Lemma

Let a and b be positive integers, and suppose $b = aq + r$ is the Euclidean division for b divided by a. Then,

$$\gcd(a, b) = \gcd(a, r).$$

Since $r < b$, this says that we can replace a calculation of the gcd of two integers with two smaller integers. Since we are counting down in the integers, we have to eventually hit 0, in which case we use $\gcd(x, 0) = x$ to get the answer.

An application: computing the gcd

Lemma

Let a and b be positive integers, and suppose $b = aq + r$ is the Euclidean division for b divided by a. Then,

$$\gcd(a, b) = \gcd(a, r).$$

Since $r < b$, this says that we can replace a calculation of the gcd of two integers with two smaller integers. Since we are counting down in the integers, we have to eventually hit 0, in which case we use $\gcd(x, 0) = x$ to get the answer.

Proof.

An application: computing the gcd

Lemma

Let a and b be positive integers, and suppose $b = aq + r$ is the Euclidean division for b divided by a. Then,

$$\gcd(a, b) = \gcd(a, r).$$

Since $r < b$, this says that we can replace a calculation of the gcd of two integers with two smaller integers. Since we are counting down in the integers, we have to eventually hit 0, in which case we use $\gcd(x, 0) = x$ to get the answer.

Proof.

Homework :) □

A convenient form for induction

Mathematical induction can also be formulated as, what the book calls common induction:

- Let $X \subseteq \mathbb{N}$ be a set of natural numbers. If $0 \in X$ and if $n \in X$ implies $n + 1 \in X$ for all n, then $X = \mathbb{N}$.

A convenient form for induction

Mathematical induction can also be formulated as, what the book calls common induction:

- Let $X \subseteq \mathbb{N}$ be a set of natural numbers. If $0 \in X$ and if $n \in X$ implies $n + 1 \in X$ for all n, then $X = \mathbb{N}$.

This gives rise the following strategy for proving some predicate $P(n)$ holds for all natural numbers n:

1. (Base case) First prove $P(0)$. This is often, though not always, trivial.
2. (Inductive step) Then prove if $P(k)$ then $P(k + 1)$.

An example

Theorem

For any natural number n,

$$\sum_{i=0}^{n} i = 0 + 1 + \cdots + n = \frac{n(n+1)}{2}.$$

An example

Theorem

For any natural number n,

$$\sum_{i=0}^{n} i = 0 + 1 + \cdots + n = \frac{n(n+1)}{2}.$$

Proof.

(Base case)

An example

Theorem

For any natural number n,

$$\sum_{i=0}^{n} i = 0 + 1 + \cdots + n = \frac{n(n+1)}{2}.$$

Proof.

(Base case) $0 = 0 \cdot 1/2$.

An example

Theorem

For any natural number n,

$$\sum_{i=0}^{n} i = 0 + 1 + \cdots + n = \frac{n(n+1)}{2}.$$

Proof.

(Base case) $0 = 0 \cdot 1/2$.
(Inductive step) Assume that $\sum_{i=0}^{k} i = k(k+1)/2$. Then, by inductive hypothesis,

$$\sum_{i=0}^{k+1} i = \left(\sum_{i=0}^{k}\right) + (k+1) = k(k+1)/2 + (k+1).$$

Some algebra gives that this is $\frac{k^2+3k+2}{2} = \frac{(k+1)(k+2)}{2}$.

An example

Theorem

For any natural number n,

$$\sum_{i=0}^{n} i = 0 + 1 + \cdots + n = \frac{n(n+1)}{2}.$$

Proof.

(Base case) $0 = 0 \cdot 1/2$.
(Inductive step) Assume that $\sum_{i=0}^{k} i = k(k+1)/2$. Then, by inductive hypothesis,

$$\sum_{i=0}^{k+1} i = \left(\sum_{i=0}^{k}\right) + (k+1) = k(k+1)/2 + (k+1).$$

Some algebra gives that this is $\frac{k^2+3k+2}{2} = \frac{(k+1)(k+2)}{2}$. □