Discrete Mathematics

MATH1064, Lecture 17

Jonathan Spreer

The principle of mathematical induction

Let $P(n)$ be a predicate that is defined for all integers $n \geq a$, $a \in N$.
Suppose:

1. $P(a)$ is true;
2. For all integers $n \geq a$, $P(n) \rightarrow P(n+1)$.

Then $P(n)$ is true for all integers $n \geq a$.

Think of an infinite train, with the engine numbered a and the other carriages numbered $a+1$, $a+2$, $a+3$, $\ldots$ to infinity.

Suppose:

1. $P(a)$: The engine moves.
2. $P(n) \rightarrow P(n+1)$: Each carriage pulls the one behind it.

Then the entire train moves.

Note: we never directly prove that $P(n)$ is true $(n \neq a)$.

Example: Stamps

Question:
Which values can we make using only 3¢ and/or 5¢ stamps?

1. **Exploration!**
2. **Conjecture:** We can make 3, 5, 6, and all $n \geq 8$.
3. **Observation:** We can add one to the total value, by:
   - replacing 5 with $3 + 3$; or
   - replacing $3 + 3 + 3$ with $5 + 5$.

4. Proving our conjecture: Let $P(n)$ be the predicate "we can form n¢ using only 3¢ and/or 5¢ stamps".

We can prove $P(3)$, $P(5)$, $P(6)$ and $P(8)$ directly:

$$3 = 3, \quad 5 = 5, \quad 6 = 3 + 3, \quad 8 = 5 + 3$$

Hopefully we can use our observation to obtain $P(n)$ for all $n \geq 8$!

Proposition

$P(n)$ is true for all integers $n \geq 8$.

Proof: We know that $P(8)$ is true, from the previous slide.
We will now prove that $P(n) \rightarrow P(n+1)$ for all $n \geq 8$.

Suppose $n \geq 8$ and $P(n)$ is true; that is,
assume we have formed n¢ from 3¢ and/or 5¢ stamps.

- If we do not use any 5¢ stamps to form n¢, then since $n \geq 8$ it follows that we have at least three 3¢ stamps.
  Replace $3+3+3$ with $5+5$, and we obtain $(n+1)$¢.
- Otherwise, we do use a 5¢ stamp.
  Replace 5 with $3+3$, and we obtain $(n+1)$¢.

So:

- $P(8)$ is true (previous slide);
- $P(n) \rightarrow P(n+1)$ for all integers $n \geq 8$ (above).

By mathematical induction, $P(n)$ is true for all integers $n \geq 8$! □

How to use mathematical induction

To prove $P(n)$ for all integers $n \geq a$, you need to:

1. Prove $P(a)$.
   This is called the basis step.
2. Prove that $P(n) \to P(n+1)$ for all integers $n \geq a$.
   Here you must:
   - assume $P(n)$ is true for some particular but arbitrary $n \geq a$;
   - using this, show that $P(n+1)$ is also true.

   This is called the inductive step.
   The assumption that $P(n)$ is true is called the inductive hypothesis.

Example: Gauss (yet again)

Theorem

For all $n \in \mathbb{N}$, $n \geq 1$, $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

We will reprove this using induction.

Proof: Let $P(n)$ be the proposition: $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Basis step: Setting $n = 1$, we see that $\sum_{i=1}^{1} i = 1 = \frac{1 \cdot 2}{2}$.

Therefore $P(1)$ is true.

Observation: $\sum_{i=1}^{n+1} i = \left(\sum_{i=1}^{n} i \right) + (n+1)$.

This gives us a way to link $P(n)$ with $P(n+1)$!

Inductive step: Assume that $P(n)$ is true for some $n \geq 1$.
We aim to show that $P(n+1)$. That is, we must prove:

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

From our earlier observation, the left hand side expands to:

$$\sum_{i=1}^{n+1} i = \left(\sum_{i=1}^{n} i\right) + (n+1) = \frac{n(n+1)}{2} + (n+1),$$

by our inductive hypothesis. Therefore:

$$\sum_{i=1}^{n+1} i = \frac{n(n+1)}{2} + (n+1) = (n+1)\left(\frac{n}{2} + 1\right) = (n+1) \cdot \frac{(n+2)}{2},$$

and so $P(n+1)$ is true.

In summary, we have shown that:

- $P(1)$ is true;
- $P(n) \to P(n+1)$ for all integers $n \geq 1$.

Therefore, by mathematical induction, $P(n)$ is true for all integers $n \geq 1$.

That is: $\displaystyle\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ for all $n \in \mathbb{N}$. $\square$

Example: Divisibility

Proposition

For all $n \in \mathbb{N}$, $3 \mid (2^{2n} - 1)$.

Proof. Let $P(n)$ be the predicate "$3 \mid (2^{2n} - 1)$".

Basis step: $3 \mid (2^{2 \cdot 0} - 1) = 0$, and so $P(0)$ is true.

Inductive step: Assume $P(n)$; that is, assume that $3 \mid (2^{2n} - 1)$. Our task is to prove that $3 \mid (2^{2(n+1)} - 1)$.

We have: $2^{2(n+1)} - 1 = 2^{2n+2} - 1 = 4 \cdot 2^{2n} - 1 = 4(2^{2n} - 1) + 3$.

But $2^{2n} - 1 = 3k$ for some $k \in \mathbb{Z}$, by the inductive hypothesis.

Therefore $2^{2(n+1)} - 1 = 4 \cdot 3k + 3 = 3(4k + 1)$,
and so $3 \mid (2^{2(n+1)} - 1)$ as required.

We have shown $P(0)$ is true and $P(n) \to P(n+1)$, and so by mathematical induction, $P(n)$ is true for all $n \in \mathbb{N}$. $\square$

Example: Divisibility

There are often several different ways to prove a theorem!

Proposition

For all $n \in \mathbb{N}$, $3 \mid (2^{2n} - 1)$.

A cautionary tale

Theorem

All numbers are equal.

Proof. Let $P(n)$ be the predicate: "For any collection of n numbers $x_1, x_2, \ldots, x_n$, it is always true that $x_1 = x_2 = \ldots = x_n$."

Basis step: $P(1)$ is clearly true—the collection is just x_1.

Inductive step: Suppose that $P(n)$ is true, and consider a collection of $n+1$ numbers $x_1, \ldots, x_{n+1}$.

The sub-collection $x_1, \ldots, x_n$ contains n numbers, and so $x_1 = \ldots = x_n$ by the inductive hypothesis.

The sub-collection $x_2, \ldots, x_{n+1}$ also contains n numbers, and so $x_2 = \ldots = x_{n+1}$ by the inductive hypothesis.

Therefore $x_1 = x_2 = \ldots = x_n = x_{n+1}$, and $P(n+1)$ is true.

By mathematical induction, $P(n)$ is true for all $n \in \mathbb{N}$! $\square$

A cautionary tale

What was wrong with that proof?

The inductive step fails for $n = 1$ (and only for $n = 1$)!

- For $n = 1$, we apply the inductive hypothesis to the collection x_1, and again to the collection x_2.
- These two collections do not overlap, and so we cannot conclude that $x_1 = x_2$.