



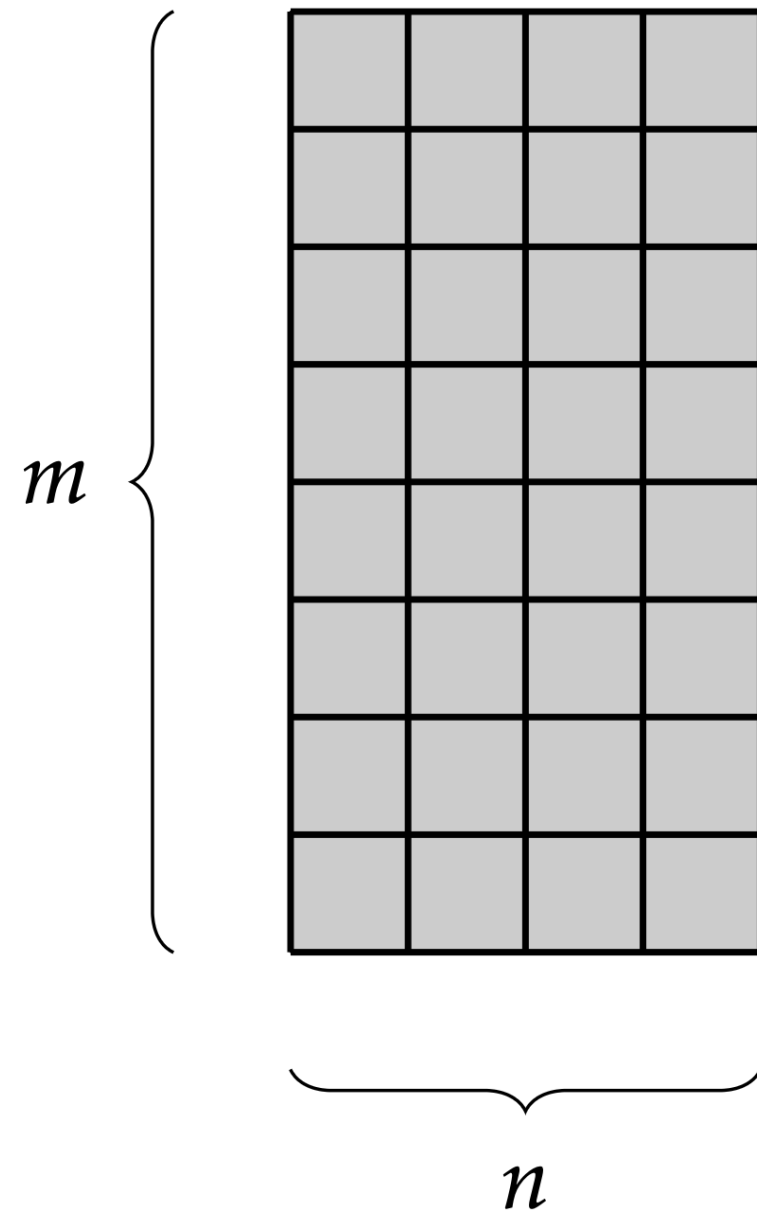
Middlebury

CSCI 200: Math Foundations of Computing

Spring 2026

Lecture 7M: Strong Induction

Goals for today.

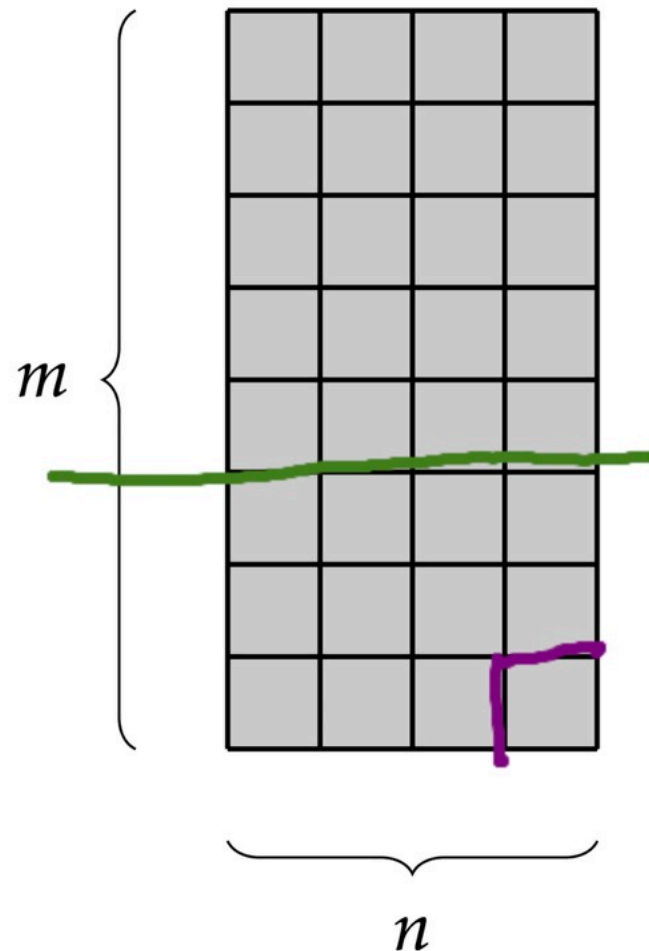


- Practice some more with proofs by induction.
- Identify when multiple base cases are needed in a proof by induction.
- Identify when strong induction is needed.
- Prove correctness and/or a property about an algorithm using induction.

How many "breaks" to break up $m \times n$ chocolate bar into individual squares?

Theorem: An $m \times n$ chocolate bar requires $mn - 1$ breaks to break it up into individual squares.

Prove that it takes $mn - 1$ "breaks" to break up the $m \times n$ chocolate bar into individual squares.



Proof. We use a proof by induction on the total number of squares in the chocolate bar. Let $p(k)$ be the predicate that a chocolate bar with k squares requires $k - 1$ breaks to split the bar into individual squares.

- **Base case:** For $k = 1$, no breaks are needed to split the chocolate bar, and the formula $1 - 1 = 0$ is verified.
- **Inductive step:** Suppose $p(k)$ is true. This means that a chocolate bar with k squares requires $k - 1$ splits to break it up into individual squares. We must show that a chocolate bar with $k + 1$ squares requires k breaks.

need to remove a square



STUCK :-)

The Principle of Strong Induction

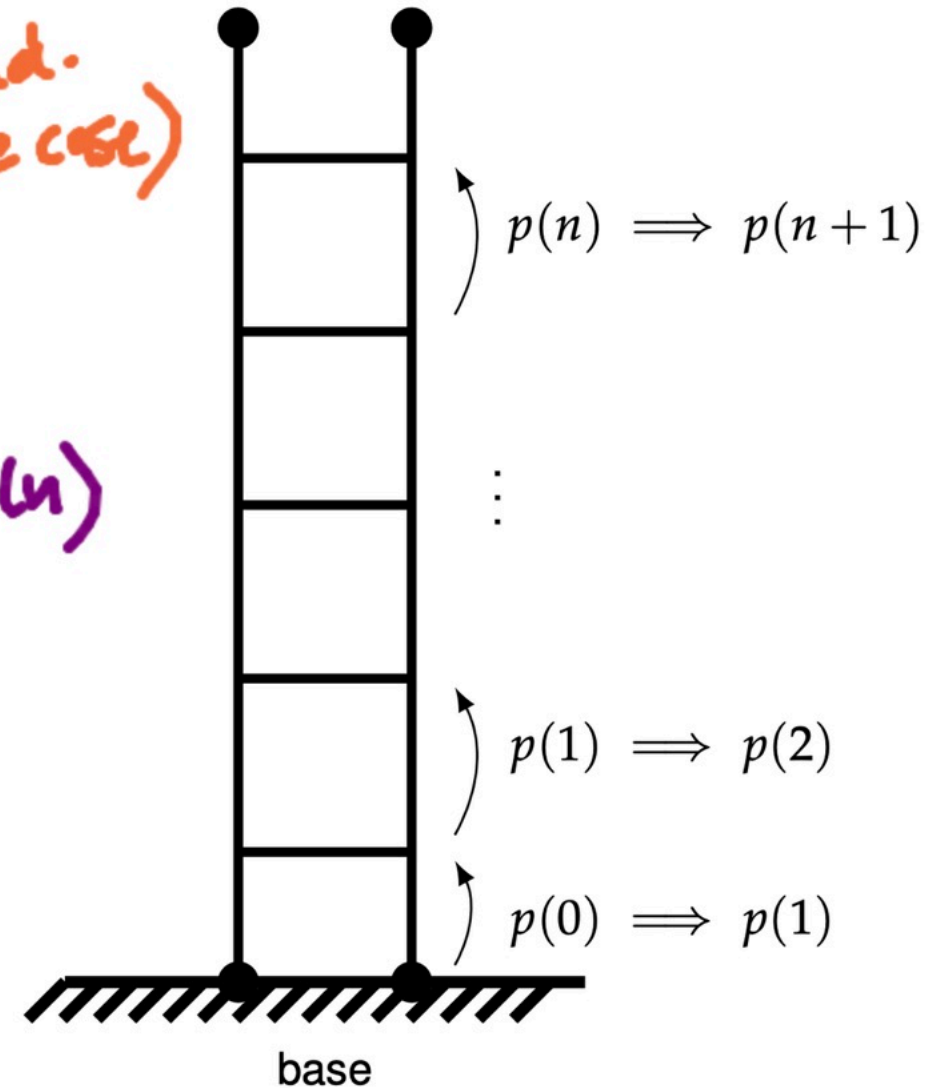
Let P be a predicate.
if $P(0)$ true ↗ whatever lowest value of ind. var. is (base case)

and

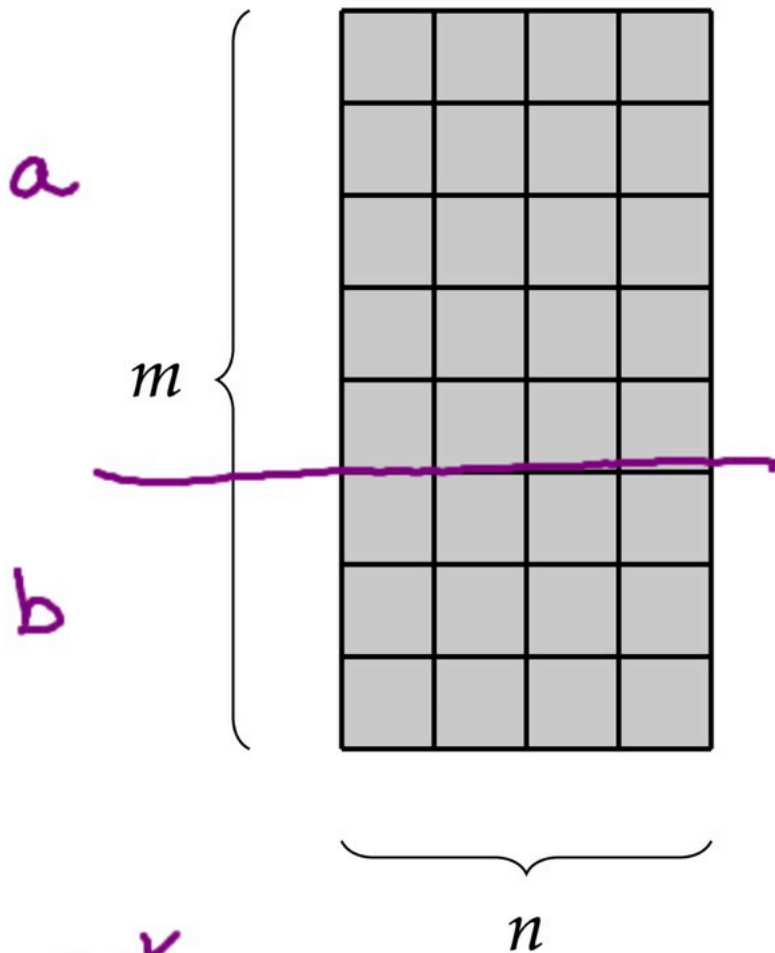
$$P(0) \wedge P(1) \wedge P(2) \wedge \dots \wedge P(n-1) \wedge P(n)$$

→ $P(n+1)$
(implies)

then $P(n)$ is true for all n .



Prove that it takes $mn - 1$ "breaks" to break up the $m \times n$ chocolate bar into individual squares.



Proof. We use a proof by strong induction on the total number of squares in the chocolate bar. Let $p(k)$ be the predicate that a chocolate bar with k squares requires $k - 1$ breaks to split the bar into individual squares.

- **Base case:** For $k = 1$, no breaks are needed to split the chocolate bar, and the formula $1 - 1 = 0$ is verified.
- **Inductive step:** Suppose $p(1) \wedge p(2) \wedge \dots \wedge p(k)$ are true. This means that a chocolate bar with $1 \leq s \leq k$ squares requires $s - 1$ splits to break it into individual squares. We must show that a chocolate bar with $k + 1$ squares requires k breaks to break it into individual squares.

Starting with a $k+1$ square bar, break it into 2 subbars with a and b squares, respectively. Then $a+b = k+1$. By assumption, then the a -bar requires $a-1$ splits, and the b -bar requires $b-1$ splits. The total number of splits is $(a-1) + (b-1) + 1 = a+b-1 = k+1-1 = k$ splits, verifying $p(k+1)$ is true.

$$1 \leq a \leq k$$

$$1 \leq b \leq k$$

of splits is $(a-1) + (b-1) + 1 = a+b-1 = k+1-1 = k$ splits, verifying $p(k+1)$ is true.

Therefore, by strong induction on k , $p(k)$ is true for all $k \geq 1$.

Example 2: Prove that every integer greater than 1 is either prime or a product of primes.

p.o.p.

Proof. We will use a proof by strong induction on integers $n > 1$. Let the induction hypothesis be $p(n)$:

$p(n)$ is a predicate \rightarrow

A. "an integer greater than 1 is either prime or a product of primes" $\rightarrow p(n) \checkmark$

B. "all integers greater than 1 are either prime or a product of primes" \times

C. Both A and B are valid.

• **Base case:** For $n = 2$ we have that 2 is a prime number.

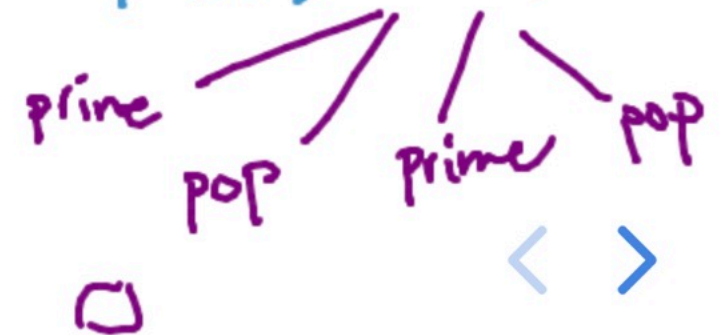
• **Inductive step:** Let $n \geq 2$ and assume that $p(2) \wedge p(3) \wedge \dots \wedge p(n)$ are true. We need to show that $(n+1)$ is either a prime number or a product of primes.

Two cases: $(n+1)$ is ① prime or ② not prime.

Case 1: Suppose $(n+1)$ is a prime, $p(n+1)$ true.

Case 2: Suppose $(n+1)$ is not prime. Then $(n+1) = k \cdot m$ for some $k, m \in \mathbb{Z}$. By our assumption k is either prime or a p.o.p. and m is either prime or a p.o.p. Therefore, $(n+1) = k \cdot m$ is always a p.o.p.

Therefore, by strong induction on n , $p(n)$ is true for all $n > 1$.



Example 3: Recurrence relations.

Consider the following recurrence relation:

$$F(n) = 4F(n-1) - 4F(n-2), \quad F(0) = 1, \quad F(1) = 0.$$

We want a "closed-form" expression for $F(n)$ that doesn't depend on $F(n-1)$, $F(n-2)$, etc. Prove that $F(n) = 2^n(1-n)$ for all $n \geq 0$.

$$2^n(1-n)$$

Proof. We use strong induction on the integer n . Let the induction hypothesis be $p(n) : "F(n) = 2^n(1-n)"$.

• **Base cases:**

- For $n = 0$, $F(0) = 2^0(1-0) = 1$
- For $n = 1$, $F(1) = 2^1(1-1) = 0$

• **Inductive step:** Assume $p(0) \wedge p(1) \wedge \dots \wedge p(n)$ are true. That is, $F(k) = 2^k(1-k)$ for $0 \leq k \leq n$. We need to show that $F(n+1) = -2^{n+1}n$. *Start with the recurrence relation:*

$$F(n+1) = 2^{n+1} \left(1 - (n+1) \right) = 2^{n+1}(-n) = -n \cdot 2^{n+1}$$

$$\begin{aligned} F(n+1) &= 4F(n+1-1) - 4F(n+1-2) = 4F(n) - 4F(n-1) \\ &= 4 \cdot 2^n(1-n) - 4 \cdot 2^{n-1}(1-(n-1)) \\ &= 4 \cdot 2^n - n \cdot 4 \cdot 2^n - 2 \cdot 2^n(2-n) \\ &= 4 \cdot 2^n - n \cdot 4 \cdot 2^n - 2 \cdot 2^n(2-n) \\ &= 4 \cdot 2^n - n \cdot 4 \cdot 2^n - 4 \cdot 2^n + 2 \cdot n \cdot 2^n \\ &= -2 \cdot n \cdot 2^n \\ &= -n \cdot 2^{n+1} \end{aligned}$$

by assumption

Therefore... \square

