Homework 1 Due Thurs 10/7 @ 11:59pm

Antonio's OO (in person: directly after class
virtual: on demand tomorrow)

Lecture 7
10/5

Last Time: principle of mathematical induction
ordinary induction examples

Today: Strong Induction

Strong Induction

Idea: Intuitively we thought of Induction as 'knocking over dominoes' via a chain of implications $\to P(k-1) \to P(k) \to P(k+1) \to$

At the point where the 100^{th} domino is next to fall, not just we know that the first 99 dominoes have fallen, not just the 99^{th}.

Likewise when proving a sequence of statements $S_1, S_2, S_3, \ldots$ instead of just assuming that S_k true in order to prove S_{k+1}, why not assume that $S_1, S_2, \ldots, S_k$ are all true in order to prove S_{k+1}? Strong Induction uses this information.

Principle of Strong Induction

Consider a sequence of mathematical statements $S_1, S_2, S_3, \ldots$.

- Suppose S_1 true and
- Suppose $\forall k \in \mathbb{N}$, if $S_1, S_2, \ldots, S_k$ true then S_{k+1} true,

then S_n true for all $n \in \mathbb{N}$.

Ex: Regular Induction

$S_1 \to S_2 \to \cdots \to S_k \to S_{k+1}$

Strong Induction

$S_1 \to S_2 \to S_3 \cdots \to S_{k+1}$

Strong Induction Outline

Base Case: (show P_1 true $\Rightarrow$ we called it S_1)

Inductive Hypothesis: Assume $S_1, S_2, \ldots, S_k$ are all true
as opposed to ordinary induction where we just assume S_k true

Inductive Step: prove $(S_1, \ldots, S_k) \rightarrow S_{k+1}$ is true

Ex Fundamental Thm of Arithmetic

Every integer $n \geq 2$ is either a prime or can be (uniquely) represented as a product of primes

Let's try to prove the existence of a prime factorization for all $n \geq 2$
(we'll use some results about divisibility to prove uniqueness)

A First Try (using ordinary induction)

Base Case: when $n = 2 \Rightarrow 2$ is prime ✓

Inductive Hypothesis: Let $k \geq 2$, suppose k can be written as a product of primes

$$K = \prod_{i=1}^{l} p_i^{e_i}$$

Inductive step: Show that $K+1$ can also be written as a product of primes.

Case i) $K+1$ is prime $\Rightarrow$ we're done

Case ii) $K+1$ is composite $\Rightarrow$ $\exists\, a, b$ s.t. $2 \leq a \leq b \leq K+1$
such that ~~$K \leq a \leq b$~~ $K+1 = a \cdot b$

I want to say that a and b can be written as a product of primes and so their product by def is a product of primes

$\Rightarrow$ Knowing that K can be written as a product of primes does not tell us about $K+1$; we need $P(a)\ P(b) \rightarrow P(k) \not\rightarrow P(K+1)$

A Second Attempt

Base Case $(n=2)$ $\Rightarrow$ prime ✓

Inductive Hypothesis: Suppose $2, 3, 4, \ldots, k$ can all be written as a product of primes.

Inductive Step: Need to show $k+1$ can be written as a product of primes

Case I) $k+1$ prime $\Rightarrow$ we're done

Case II) $k+1$ composite $\Rightarrow$ $\exists\, a, b$ s.t. $2 \leq a \leq b \leq k+1$ such that $k+1 = a \cdot b$

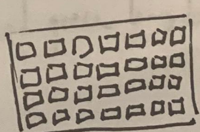
By I.H. a can be written as a product of primes $a = (p_1 \cdots p_m)$

b " " " " " " " $b = (q_1 \cdots q_\ell)$

Therefore $k+1 = (p_1 \cdots p_m)(q_1 \cdots q_\ell)$ which is a product of primes $\square$

Below we give a proof of Uniqueness of the prime factorization in the Fundamental Thm of Arithmetic, let's look at one more example of strong induction.

- Uniqueness proof involves some lemmas about divisibility

Ex:  4×7 bar

Proposition on Chocolate Bars

Suppose you have a chocolate bar (an $m \times n$ grid of squares). The entire bar (or any smaller rectangular piece of the bar) can be broken along vertical/horizontal lines separating squares.

Question: is the # breaks to break bar into 1×1 squares always the same?

Claim: # breaks = $m \cdot n - 1$

How can I prove this?

Induction

Q: what should I consider for my base case

Base: 1x1 square requires $1 \times 1 - 1 = 0$ breaks ✓

Q: what should I consider for IH?

IH: Assume all bars with at most k squares satisfy result?

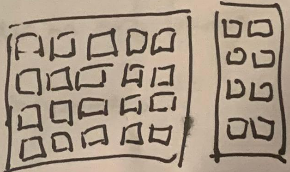
Problem: Thinking in terms of a single variable makes it difficult to apply the claim, since claim stated for an mxn grid.

Can I reword my IH to think in terms of mxn?

$\Longrightarrow$ IH: All chocolate bars with fewer than mxn squares satisfy the proposition.

Inductive Step: prove that mxn bar satisfies proposition.

Idea: Many ways to break a chocolate bar, here is one



How will I setup the algebra here?

Suppose first piece has a squares, second piece has b squares.

$\Longrightarrow a+b = m \cdot n$

Since both have fewer than $m \cdot n$ squares, can apply IH to each

$\Longrightarrow$ bar with a squares can be completely broken up with a-1 breaks

" " " b-1 "

b "

⇒ Combined, this tells us how many breaks for the original bar

Q: Do we need strong induction here?

⟹ Again, with reg. induction, we are permitted to use only k^{th} case to prove $k+1$

⟹ Breaking a bar of $k+1$ squares is not ~~possible~~ guaranteed to produce a bar of k squares.

Typically, first break produces two bars with fewer than k pieces

Proof

Base Case: Chocolate Bar w/ one piece 1×1 bar

$1-1=0$ breaks ✓

$=k-1$ ✓

IH: Let $k\in\mathbb{N}$, assume all bars w/ at most k squares satisfy proposition.

Induction Step: Consider any bar w/ $k+1$ squares. Suppose it has dimensions $m\times n$. Any seq of breaks begins w/ a first break, which breaks bar into two smaller bars. Consider an arbitrary first break, suppose two smaller bars have a, b squares

$\Rightarrow a+b=m\cdot n$ (b/c squares must add up)

by IH: bar w/ a squares requires $a-1$ breaks, b squares... $b-1$ breaks

$\Rightarrow$ To break $m\cdot n$ bar, must make first break followed by $(a-1)+(b-1)$ additional breaks. Total # of breaks is then

$1+(a-1)+(b-1)=(a+b)-1=m\cdot n-1$ ✓

By Strong Induction a chocolate bar of any size requires one less break than its # squares to break into ind. pi[illegible]

Fundamental Thm of Arithmetic

$\forall n \geq 2$, $n = p_1^{a_1} \cdots p_k^{a_k}$ where p_i prime, $a_i \in \mathbb{N}$ and this is unique up to reordering.

Lemma 1 if $p|ab$ then $p|a$ or $p|b$ (with p prime) $a, b \in \mathbb{N}$ (Euclid's Lemma)

Proof

We will show if $p \nmid a$ then $p|b$ or similarly if $p \nmid b$ then $p|a$

p does not divide one, then it must divide the other.

Suppose $p \nmid a$, then since p is prime $\gcd(p,a)=1$

Since $GCD(a,p)=1$, $\exists\, x,y \in \mathbb{Z}$ s.t. $ax+py=1$

Remark: we can find the numbers x and y with Extended Euclidean Algorithm

Since $p|ab$, $\exists\, d \in \mathbb{Z}$ s.t. $p \cdot d = ab$

$\Rightarrow$ We have two equations, lets combine them. The proposition involves an ab term so lets try to get that

$\underline{ab}x + pby = b$, $p \cdot d = ab$

$p \cdot dx + p \cdot by = b$

$p(dx + by) = b$ by def we found a multiple of p equal to b

so $p|b$ $\square$

Lemma 2: if $p | a_1 \cdot a_2 \cdots a_n$ then $p | a_i$ for some $1 \leq i \leq n$ (p prime)
(Euclid's Lemma was the case when $n=2$)

We can generalize w/ Induction

Base Case: $(n=2)$

By Euclid's Lemma if $p | a_1 \cdot a_2$ then $p | a_1$ or $p | a_2$

Induction Hypothesis:

Suppose if $p | a_1 \cdots a_k$ then $p | a_i$ for some $1 \leq i \leq k$

Induction Step: Suppose $p | a_1 \cdots a_k \cdot a_{k+1}$

$\Rightarrow p | (a_1 \cdots a_k) \cdot a_{k+1}$

by Euclid's Lemma again

we know $p | (a_1 \cdots a_k)$ or $p | a_{k+1}$

by IH $p | a_i$ for $1 \leq i \leq k$ or $p | a_{k+1} \Rightarrow p | a_i$ for $1 \leq i \leq k+1$ $\square$

roof (Fundamental Thm of Arithmetic)

Can also prove existence of prime factorization via contradiction.

$\Rightarrow$ Suppose $\exists$ a natural number that cannot be represented as a product of primes

Let M be the smallest such number. Observe M must be composite.

1) if M is prime,
$M = p^1$ which is a contradiction

Case 2) M is composite.

$M = a \cdot b$ where a & $1 < a, b <$
Since a, b both smaller than M $a,$
we can write