Before Section

Wednesday

→ Strong Induction → Induction
→ proof techniques
→ strengthening → cases →
→ practice

Yesterday Questions

(1) Induction + Strong

Recursion !

think defining recursive algorithm
construct some $\underline{n=k+1}$ from all $n \leq k$ parts

strong → weak induction
part prove $n = k+1$
use only $(n = k)$
$P(k+1)$ using $P(k)$

Strong Induction
→ prove for a set of number
$n \in N$
~~0~~ 1 . . . . . .

construct a solution for
$n=1$ $P(n=1)$ holds
↓ math show
$P(n=2)$
↓
⋮
$P(n=k)$

recursion
base
how to construct
$n=k$ using parts lower

CS 70 Discrete Mathematics and Probability Theory
Summer 2021 **DIS 1C**

1 Divisibility Induction

Prove that for all $n \in \mathbb{N}$ with $n \geq 1$, the number $n^3 - n$ is divisible by 3. (**Hint**: recall the binomial expansion $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$)

$n=1$ BC

$n = k$ Assume → try base case first

$n = k+1$ Prove

IH $k+1$ holds $n=k$ $k^3 - k = 3m$ $m \in \mathbb{Z}$

$n^3 - n \longrightarrow (k+1)^3 - (k+1)$ → $k^3 + 3k^2 + 3k + 1 - k - 1$

$3m + 3k^2 + 3k$ → $3(m + k^2 + k)$ → 3

2 Make It Stronger

→ not induction

Let $x \geq 1$ be a real number. Use induction to prove that for all positive integers n, all of the entries in the matrix

$n \in \mathbb{Z}^+ \to 1 2 \ldots$

$$\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^n\right)$$

are $\leq xn$. (Hint 1: Find a way to strengthen the inductive hypothesis! Hint 2: Try writing out the first few powers.)

$\forall n \in \mathbb{Z}^+$ $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

→ $a \wedge b \wedge c \wedge d \leq xn$

st

$n=1$ $\begin{matrix} 1 & x \\ 0 & 1 \end{matrix}$

$n=2$ $\begin{matrix} 1 & 2x \\ 0 & 1 \end{matrix}$

$n=3$ $\begin{pmatrix} 1 & 3x \\ 0 & 1 \end{pmatrix}$ → Prove pattern

$n=n$ $\begin{bmatrix} 1 & xn \\ 0 & 1 \end{bmatrix}$ → all $\leq xn$ → format of any $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^n$

same thing logically equiv

→ all entries $\leq xn$

3 Binary Numbers

Prove that every positive integer n can be written in binary. In other words, prove that we can write

$\equiv$ written in binary → multiples of two sum →

$$n = c_k \cdot 2^k + c_{k-1} \cdot 2^{k-1} + \cdots + c_1 \cdot 2^1 + c_0 \cdot 2^0,$$

where $k \in \mathbb{N}$ and $c_k \in \{0, 1\}$.

try weak induction → then try strong induction → more access

$c_k \in \{0,1\}$ $0 \cdot 2^3$

$7 \to 0111 \to c_2 2^2 + c_1 \cdot 2^1 + c_0 \cdot 2^0 = 7$ → $4+2+1$

$c_3 = 0$ $c_2 = 1$ $c_1 = 1$ $c_0 = 1$

→ Base Case

→ $n = 1$

in binary $= 1$ $c_0 = 1$

Answers

Prove $n \in \mathbb{N}$, $n \geq 1$

1) Divisibility Induction $3 \mid n^3 - n$

Solution

① Base Case → $n = 1$

$1^3 - 1 = 0$ $\quad 3 \mid 0$ $\quad n = k$ holds

power of induction

② Induction Step → $\forall$ $n \leq k$ $\quad k \geq 1$

assume or stronger

not necessary

$[3 \mid k^3 - k]$

show $n = k+1$ holds

$(k+1)^3 - (k+1)$ expand

$= k^3 + 3k^2 \ldots$

$(k^3 - k) + 3k^2 + 3k$

by assumption

$3 \mid 3k^2$

$3k$

2 Make it Stronger

$x \geq 1$ prove $\forall n \in \mathbb{Z}^+$

$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^n$ (all entries $\leq xn$)

① try a few

all entries $\leq$ \

$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^1$ ← 1st power $= \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ $\quad n = 1$

$1 \cdot 1 + x \cdot 0$ $\quad x + x$

$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^2 \to \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2x \\ 0 & 1 \end{pmatrix}$ $\quad n = 2$

$1 \cdot 0 + 0 \cdot 1$ $\quad x \cdot 0 + 1$

$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^3 \to \begin{pmatrix} 1 & 2x \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \begin{bmatrix} 1 \cdot 1 + 2x \cdot 0 & x \cdot 1 + 2x \cdot 1 \\ 1 \cdot 0 + 0 \cdot 1 & 0 \cdot x + 1 \cdot 1 \end{bmatrix}$

$\begin{pmatrix} 1 & 3x \\ 0 & 1 \end{pmatrix}$ $\quad n = 3$

prove stronger

any $n \in \mathbb{Z}^+$

$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & xn \\ 0 & 1 \end{pmatrix}$

Base $n = 1$ $\quad P(1)$ $\quad \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^1 = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$

Induction Case

Assume $n = k$ holds → $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^k = \begin{pmatrix} 1 & xk \\ 0 & 1 \end{pmatrix}$

Prove $n = k+1$

$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^{k+1} \longrightarrow \begin{pmatrix} 1 & xk \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & x(k+1) \\ 0 & 1 \end{pmatrix}$

stronger statement

prev statement

tr

Prove

3 Binary Numbers

(can write $\forall n \in \mathbb{Z}^+$ as a binary)

decimal $\rightarrow$ binary

Two ways
1. "functional form"
2. "hardware algorithm form"

2 ways: strong induction

Assume anything $< k+1$ holds

1. Based on cases
   - (a) $2 \mid k+1$ — $n = k+1$, use $(k+1)/2$ $\rightarrow$ $\exists$ binary rep, then shift bits
   - b) $2 \nmid k+1$ $\Rightarrow$ $2 \mid k$ — use 2^1, use * and add 1 to last bit

$\downarrow 3-1$, $2 \mid 2$

$\exists$ bin: $\frac{k+1}{2} \rightarrow$ bit shift oper, $k+1$ binary

any binary # $\cdot$ 2 $\rightarrow$ shift bits right $\rightarrow$ last bit $= 0$ $\rightarrow$ $k+1$ $\rightarrow$ bin rep $+1$

for k

$n=1$	1
$n=2$	10
$n=k$	
$k=1$	1
$k=2$	10

last bit 0

2. Hardware algo

$7 \rightarrow 111$

$3 \rightarrow 1\textcircled{0} \leftarrow$ last 1

B C] $n=1$ $1 \times 2^0 \rightarrow$

Induc Step

Assume holds $\forall k < n$

2^m largest power st $n \geq 2^m \Rightarrow n < 2^{m+1}$

2^m — n — 2^{m+1}

$n - 2^m < 2^{m+1} - 2^m$

$= n - 2^m \geq 0$

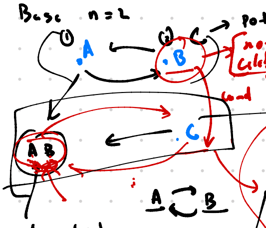
and $n - 2^m < n < 2^{m+1}$ $\Rightarrow n - 2^m < 2^m$ $\rightarrow$ highest power 2^{m-1}

$\Rightarrow$ has a binary rep by def

$n - 2^m = c_{m-1} 2^{m-1} \cdots c_0 \cdot 2^0$

$n = 2^m + c_{m-1} 2^{m-1} \cdots c_0 \cdot 2^0$

constructed solved



$B \rightarrow A$ — B knows A

$B \rightarrow$ cand

$B \rightarrow A$	~~F~~ T
$A \rightarrow B$	T

(A B C) B

$A \rightarrow C$

$B \rightarrow C$

$\boxed{C \rightarrow A}$ T — cont

$\boxed{C \rightarrow B}$ T

Celeb F

$C \rightarrow A \Rightarrow C \rightarrow B$

$C \rightarrow A$ T — C cont celeb

$(3n - 4)$

③ $\rightarrow$ fact # question — 3 factor # quests

n people $\rightarrow$ all n

4) celeb any pair A and B → ask q

3n − 4 questions max

find celeb C st C has no one he knows

BC n = 2 wlog if: A knows B and B does not know A

B is celeb else: B not celeb

if A → B A ≠ C B = cand
if B → A B ≠ C A = cand

n = k+1 assume n = k we know celeb or not

1) n = k celeb C
compare with new guy A
A → C T
C → A F
if this C is celeb
if not C not celeb

n=3 1 check + 1 check + 2
$\frac{3-1}{2(n-1)}$ = 3(n−1) → 3n − 3

Sol

BC n = 0 0 checks no celeb cand
n = 1 → 0 checks
n = 2 → 1 checks
BC n=2 k−1
n = k k−2 checks k−1−2

prove n = k assume n = k − 1 know if there is a celeb or not

2 Eliminate recursively → 2

① if there are ~~no celeb~~ n = k−1 candidates → new person is celeb → [check everyone later]

∃ celeb cand → n=k−1

② a n = k−1 celeb candidate knows new person ⇒ new person is celeb

b n = k−1 new person knows celeb candidate ⇒ celeb candidate → [check only] otw → new person

Outputs potential celeb → not self
→ check with 2(n−1) checks
everyone knows
know no one

3n − 4 → check n
3n 3(n−1) −1
n−4 n − 2 more checks
3n − 4
for n n have