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 $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$)

2 Make It Stronger

$\begin{bmatrix}1 & 5\\0 & 1\end{bmatrix}^3 = \begin{bmatrix}1 & 2\\0 & 2\end{bmatrix}\begin{bmatrix}1 & 2\\0 & 2\end{bmatrix}\begin{bmatrix}1 & 2\\0 & 2\end{bmatrix}$

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

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

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

$= 2\times 2$ $\begin{bmatrix}1 & 4\\0 & 1\end{bmatrix}^3 = \begin{bmatrix}1 & 4\\0 & 1\end{bmatrix}\begin{bmatrix}1 & 4\\0 & 1\end{bmatrix}\begin{bmatrix}1 & 4\\0 & 1\end{bmatrix}$

2×2 2×2

$\begin{bmatrix}1 & 4\\0 & 1\end{bmatrix}\begin{bmatrix}1 & 4\\0 & 1\end{bmatrix}$

$= \begin{bmatrix}1 & 8\\0 & 1\end{bmatrix}\begin{bmatrix}1 & 4\\0 & 1\end{bmatrix}$

$= \begin{bmatrix}1 & 8\\ & \end{bmatrix}$ $1\times 4 + 4\times 1 = 8$

$= \begin{bmatrix}1 & 12\\0 & 1\end{bmatrix} = \begin{bmatrix}1 & 3\cdot 4\\0 & 1\end{bmatrix}$

3 Binary Numbers

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

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

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

4 Division Algorithm

Let $a, b \in \mathbb{Z}$, $b \neq 0$. In this problem, we will prove, using the WOP, that there exists unique integers q, r such that $0 \leq r < |b|$ and $a = qb + r$. Here, q is called the *quotient* and r is called the *remainder*.

(a) Let $A = \{\overset{r}{a - qb} \mid q \in \mathbb{Z} \wedge \overset{r \geq 0}{a - qb \geq 0}\}$. Show that A is non-empty (keep in mind that we must consider the case where a is negative)

(b) Use the WOP to show that there exists $q, r \in \mathbb{Z}$ such that $a = qb + r$, and $0 \leq r < r$.

(c) Show that the q and r from part b are unique

$q' \neq q \quad r' \neq r \rightsquigarrow q' = q$

$r' = r$

(a) Given a, b, find $q \in \mathbb{Z} : a - qb \in A$

$a - qb \geq 0$

$q = 0$, if $a \geq 0$

if $a < 0$, $q = ab$

$a - qb$

$= a - abb$

$= a - ab^2$

$= \underset{\underset{0}{\wedge}}{a}\boxed{(1 - \underset{\underset{1}{\geq}}{b^2})} \leq 0$

≥ 0

$a = 15$
$b = 3$

$a = \underset{q}{5} \times \underset{b}{3} + \underset{r}{0}$

$a = 16$
$b = 7$

$a = \underset{q}{2} \times \underset{b}{7} + \underset{r}{2}$

$= 1 \times 7 + \underset{r \geq 7}{9}$

$a = 17$

$b = 7$

$A = \{3, 10, \underset{q=0}{\underline{17}}, 24, \ldots\}$

$A = \{\overset{q=3}{4}, \overset{q=4}{11}, \ldots\}$

$-17 + q7$

```
int a = 17
int b = 7
print(17/7) ~ 2      <- q
print(17%7) ~ 3      <- r
```

$\underset{a}{17} = \underset{q}{2} \times \underset{b}{7} + \underset{r}{3}$

$1 \times 7 + \underline{10}$

$17 - 1 \times 7 = 10$

$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}^3 = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1\times 1 + x\times 0 & 1\times x + x\times 1 \\ 0\times 1 + 1\times 0 & 0\times x + 1\times 1 \end{bmatrix}\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$$

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

$$= \begin{bmatrix} 1 & 3x \\ 0 & 1 \end{bmatrix}$$

IH: $\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}^k = \begin{bmatrix} 1 & kx \\ 0 & 1 \end{bmatrix}$ all elts $\leq kx$

IS: $\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}^{k+1}$

$$= \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}^k \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & kx \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & (k+1)x \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}^k = \begin{bmatrix} kx & 0 \\ 0 & kx \end{bmatrix}$$

$$\begin{bmatrix} kx & 0 \\ 0 & kx \end{bmatrix}\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} kx & kx^2 \\ 0 & kx \end{bmatrix}$$

Notice that all elts are $\leq (k+1)x$ ∎