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

Solution: Base Case: $n = 1$. $1^3 - 1 = 0$, 0 is divisible by 3.

Assume that for $n \leq k$, where $k \geq 1$, $k^3 - k$ is divisible by 3.
Now consider $n = k+1$. We want to show that $(k+1)^3 - (k+1)$ is also divisible by 3.

$$(k+1)^3 - (k+1) = k^3 + 3k^2 + 3k + 1 - k - 1 = k^3 + 3k^2 + 2k = (k^3 - k) + 3k^2 + 3k$$

By the Inductive Hypothesis, we know the part in parentheses is divisible by 3 and the rest has a factor of 3, so the whole term is divisible by 3.

2 Make It Stronger

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.)

Solution: Before starting the proof, writing out the first few powers reveals a telling pattern:

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^1 = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2x \\ 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 3x \\ 0 & 1 \end{pmatrix}$$

It appears (and we shall soon prove) that the upper left and lower right entries are always 1, the lower left entry is always 0, and the upper right entry is xn. We shall take this to be our inductive hypothesis.

Proof: We prove that

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

This claim clearly also proves the original claim in the question, since all elements of this matrix are $\leq xn$ (since $x \geq 1$). Hence, we prove this stronger claim.

- Base case (n=1): $P(1)$ asserts that $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^1 = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$. The base case is true.
- Inductive Hypothesis: Assume for arbitrary $k \geq 1$, $P(k)$ is correct: $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^k = \begin{pmatrix} 1 & xk \\ 0 & 1 \end{pmatrix}$.
- Inductive Step: Prove the statement for $n = k+1$,

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

By the principle of induction, our proposition is therefore true for all $n \geq 1$, so all entries in the matrix will be less than or equal to xn.

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 $c_k \in \{0, 1\}$.

Solution:

Prove by strong induction on n. (Note that this is the first time students will have seen strong induction, so it is important that this problem be done in an interactive way that shows them how simple induction gets stuck.)

The key insight here is that if n is divisible by 2, then it is easy to get a bit string representation of $(n+1)$ from that of n. However, if n is not divisible by 2, then $(n+1)$ will be, and its binary representation will be more easily derived from that of $(n+1)/2$. More formally:

- Base Case: $n = 1$ can be written as 1×2^0.
- Inductive Step: Assume that the statement is true for all $1 \leq m \leq n$, where n is arbitrary. Now, we need to consider $n+1$. If $n+1$ is divisible by 2, then we can apply our inductive hypothesis to $(n+1)/2$ and use its representation to express $n+1$ in the desired form.

$$(n+1)/2 = c_k \cdot 2^k + c_{k-1} \cdot 2^{k-1} + \cdots + c_1 \cdot 2^1 + c_0 \cdot 2^0$$
$$n+1 = 2 \cdot (n+1)/2 = c_k \cdot 2^{k+1} + c_{k-1} \cdot 2^k + \cdots + c_1 \cdot 2^2 + c_0 \cdot 2^1 + 0 \cdot 2^0.$$

Otherwise, n must be divisible by 2 and thus have $c_0 = 0$. We can obtain the representation of $n+1$ from n as follows:

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

Therefore, the statement is true.

Note: In proofs using simple induction, we only use $P(n)$ in order to prove $P(n+1)$. Simple induction gets stuck here because in order to prove $P(n+1)$ in the inductive step, we need to assume more than just $P(n)$. This is because it is not immediately clear how to get a representation for $P(n+1)$ using just $P(n)$, particularly in the case that $n+1$ is divisible by 2. As a result, we assume the statement to be true for all of $1,2,\ldots,n$ in order to prove it for $P(n+1)$.

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 $A = \{a - qb | q \in \mathbb{Z} \wedge a - qb \geq 0\}$. 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

Solution:

(a) If $a \geq 0$, then we can take $q = 0$ and see that $a = a - 0 * b \in A$. If $a < 0$, then we can take $q = ab$. We see that $a - ab^2 = a(1 - b^2)$. Note that $b^2 > 0$, as $b \neq 0$, so $1 - b^2$ is 0 or negative, which means $a(1 - b^2) \geq 0$

(b) Since A is non-empty and a subset of $\mathbb{N}$, let r be the smallest element in $\mathbb{N}$. By definition of A, there is a $q \in \mathbb{Z}$ such that $r = a - qb$, and $r \geq 0$. To show that $0 \leq r < |b|$, we suppose, by contradiction, that $r \geq |b|$. However, this means that $r - |b| = a - qb - |b| = a - (q \pm 1)b \geq 0$, contradicting the fact that r is the smallest element of A.

(c) Suppose by contradiction that there is another q' and r' such that $a = q'b + r'$, and $0 \leq r' < b$. Without loss of generality, suppose that $r > r'$. Since $a = qb + r = q'b + r'$, we have that $r - r' = b(q - q')$. Since $0 \leq r' < r < |b|$, we have that $r - r' < |b|$. However, this is a contradiction because $r - r' = b(q - q')$ implies that b divdes $r - r'$.