CS 70 Spring 2020 — Discrete Mathematics and Probability Theory — DIS 1A

1 Induction

Prove the following using induction:

(a) For all integers $n > 2$, $2^n > 2n+1$.

(b) For all positive integers n, $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

(c) For all positive integers n, $\frac{5}{4} \cdot 8^n + 3^{3n-1}$ is divisible by 19.

Solution:

(a) The inequality is true for $n = 3$ because $8 > 7$. Let the inequality be true for $n = k$, such that $2^k > 2k+1$. Then,

$$2^{k+1} = 2 \cdot 2^k > 2 \cdot (2k+1) = 4k+2$$

We know $2k > 1$ because k is a positive integer. Thus:

$$4k+2 = 2k+2k+2 > 2k+1+2 = 2k+3 = 2(k+1)+1$$

We've shown that $2^{k+1} > 2(k+1)+1$, which completes the inductive step.

(b) We can verify that the statement is true for $n = 1$. Assume the statement holds for $n = k$, so that

$$\sum_{i=1}^{k} i^2 = \frac{k(k+1)(2k+1)}{6}.$$

Then we can write

$$\begin{aligned}
\sum_{i=1}^{k+1} i^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\
&= (k+1)\left(\frac{k(2k+1)}{6} + (k+1)\right) \\
&= (k+1)\left(\frac{2k^2+k+6k+6}{6}\right) \\
&= (k+1)\left(\frac{2k^2+7k+6}{6}\right) \\
&= (k+1)\left(\frac{(2k+3)(k+2)}{6}\right) \\
&= \frac{(k+1)(2(k+1)+1)((k+1)+1)}{6},
\end{aligned}$$

as desired. Since we've shown that the statement holds for $n = k+1$, our proof is complete.

(c) For $n = 1$, the statement is "$10+9$ is divisible by 19", which is true. Assume that the statement holds for $n = k$, such that $\frac{5}{4} \cdot 8^k + 3^{3k-1}$ is divisible by 19. Then,

$$\begin{aligned}
\frac{5}{4} \cdot 8^{k+1} + 3^{3(k+1)-1} &= \frac{5}{4} \cdot 8 \cdot 8^k + 3^{3k+2} \\
&= 8 \cdot \frac{5}{4} \cdot 8^k + 3^3 \cdot 3^{3k-1} \\
&= 8 \cdot \frac{5}{4} \cdot 8^k + 8 \cdot 3^{3k-1} + 19 \cdot 3^{3k-1} \\
&= 8\left(\frac{5}{4} \cdot 8^k + 3^{3k-1}\right) + 19 \cdot 3^{3k-1}
\end{aligned}$$

The first term is divisible by the inductive hypothesis, and the second term is clearly divisible by 19. This completes our proof, as we've shown the statement holds for $k+1$.

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.

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: It is actually possible to do this problem with standard induction, but the solution is much more complicated. One can appeal to the mechanics of binary addition to show how $P(n+1)$ follows from $P(n)$, but formally proving that works requires some care.