0: Your Average Induction

Let A be an arbitrary, non-empty list[int], and let n = len(A).

Prove that `average(A, n)` $= \sum_{i=0}^{n-1} \frac{A_i}{n}$**, where** $A_i = A[i]$ **for** $0 \leq i < n$ **for all** $n \geq 1$**.**

We start this proof by converting the code function to a mathematical function. Then, we'll proceed by induction. `average(A, b)`is equivalent to the following function definition:

$$f(n) = \frac{(n-1) * f(n-1) + g_{n-1}}{n}$$

with initial value $f(1) = g_0$. The definition above follows from making each element in `A` an array of g values (i.e. `A` $= [g_0, g_1, g_2, \cdots, g_n]$) and rewriting the recursion in the function as a recursive mathematical function. The initial condition was set by the base case of `average(A, n)`.

Let $P(n)$ be "$f(n) = \sum_{i=0}^{n-1} \frac{g_i}{n}$". We prove $P(n)$ for all $n \in \mathbb{N}$ by induction on n.

Base Case ($n = 1$): $f(1) = g_0 = \frac{g_0}{1} = \sum_{i=0}^{0} \frac{g_i}{1}$. So, $P(0)$ is true.

Inductive Hypothesis: Suppose that $P(k)$ is true for some $k \in \mathbb{N}$.

Induction Step: We want to show that $P(k+1)$ is true.

$$\begin{aligned}
f(k+1) &= \frac{k * f(k) + g_k}{k+1} && \text{[left side of } P(k+1)\text{]} \\
&= \frac{k * \sum_{i=0}^{k-1} \frac{g_i}{k} + g_k}{k+1} && \text{[by I.H.]} \\
&= \frac{k * \frac{1}{k} \sum_{i=0}^{k-1} g_i + g_k}{k+1} \\
&= \frac{\sum_{i=0}^{k-1} g_i + g_k}{k+1} \\
&= \frac{(g_0 + g_1 + g_2 + \cdots + g_{k-1}) + g_k}{k+1} \\
&= \frac{1}{k+1} \sum_{i=0}^{k} g_i \\
&= \sum_{i=0}^{k} \frac{g_i}{k+1}
\end{aligned}$$

So, $P(k) \Rightarrow P(k+1)$ for all $k \in \mathbb{N}$. It follows that $P(n)$ is true for all $n \in \mathbb{N}$ by induction.

1: No, You're Being Irrational

Prove that $\sqrt{2} + \sqrt{5}$ is irrational. You may use the fact that $\sqrt{2}$ is irrational, but you don't have to.

We proceed by performing a proof by contradiction. Assume that $\sqrt{2} + \sqrt{5}$ is rational. By the definition of the rational numbers, there exists an $a, b \in \mathbb{N}, b \neq 0$ such that $\sqrt{2} + \sqrt{5} = \frac{a}{b}$.

We perform the following calculations:

$$\begin{aligned}
\sqrt{2} + \sqrt{5} &= \frac{a}{b} && \text{[defintion of rational numbers]} \\
\sqrt{5} &= \frac{a}{b} - \sqrt{2} \\
5 &= \frac{a^2}{b^2} - 2\sqrt{2}\frac{a}{b} + 2 \\
2\sqrt{2}\frac{a}{b} &= \frac{a^2}{b^2} - 3 \\
\sqrt{2} &= \frac{a}{2b} - \frac{3b}{2a} \\
\sqrt{2} &= \frac{2a^2 - 6b^2}{4ab}
\end{aligned}$$

Since $\sqrt{2} + \sqrt{5}$ is strictly positive, we know that $a \neq 0$, and by our use of the definition of rational numbers, we know that $b \neq 0$. As such, $4ab \neq 0$. Since $a, b \in \mathbb{N}$, $4ab \in \mathbb{N}$ and $2a^2 - 6b^2 \in \mathbb{N}$. Since we wrote $\sqrt{2}$ as the quotient of two integers, and the denominator is not zero, the defintion of a rational number is satisfied implying that $\sqrt{2}$ is a rational number. This contradicts the fact that $\sqrt{2}$ is irrational, so by contradiction, our orriginal assumption was incorrect.

Therefore, $\sqrt{2} + \sqrt{5}$ is irrational.

2: Prime Examples

Prove that for any prime $p > 3$, either $p \equiv_6 1$ or $p \equiv_6 5$.

We prove the statement by proving the contrapositive which states that for any composite $p > 3$ if $p \not\equiv_6 1$ or $p \not\equiv_6 5$. Since $\equiv_6$ can only return a $0, 1, 2, 3, 4,$ or a 5, we can investigate each case (excluding 1 and 5 by our claim) and show that p is composite.

- $p \equiv_6 0$

$$\begin{aligned} 6|(p-0) & \qquad\qquad [\text{definition of } \equiv_m] \\ 6|p & \end{aligned}$$

  By the definition of a factor, 6 is a factor of p. Since there are factors of p other than 1 and p, p is composite.

- $p \equiv_6 2$

$$\begin{aligned} 6|(p-2) & \qquad [\text{definition of } \equiv_m] \\ (p-2) = 6k & \qquad [\text{for some } k \in \mathbb{Z} \text{ by defintion of } |\ ] \\ p = 6k+2 & \\ p = 2*(3k+1) \Rightarrow 2|p & \qquad [\text{definition of } |] \end{aligned}$$

  By the definition of a factor, 2 is a factor of p. Since there are factors of p other than 1 and p, p is composite.

- $p \equiv_6 3$

$$\begin{aligned} 6|(p-3) & \qquad [\text{definition of } \equiv_m] \\ (p-3) = 6k & \qquad [\text{for some } k \in \mathbb{Z} \text{ by defintion of } |\ ] \\ p = 6k+3 & \\ p = 3*(2k+1) \Rightarrow 3|p & \qquad [\text{definition of } |\ ] \end{aligned}$$

  By the definition of a factor, 3 is a factor of p. Since there are factors of p other than 1 and p, p is composite.

- $p \equiv_6 4$

$$\begin{aligned} 6|(p-4) & \qquad [\text{definition of } \equiv_m] \\ (p-4) = 6k & \qquad [\text{for some } k \in \mathbb{Z} \text{ by defintion of } |\ ] \\ p = 6k+4 & \\ p = 2*(3k+2) \Rightarrow 4|p & \qquad [\text{definition of } |\ ] \end{aligned}$$

  By the definition of a factor, 4 is a factor of p. Since there are factors of p other than 1 and p, p is composite.

As such, we have proved the contrapositive and thus the original statement.