CSE 311: Foundations of Computing I

Section 6: Induction Solutions

1. Extended Euclidean Algorithm

(a) Find the multiplicative inverse y of 7 mod 33. That is, find y such that $7y \equiv 1 \pmod{33}$. You should use the extended Euclidean Algorithm. Your answer should be in the range $0 \le y < 33$.

Solution:

First, we find the gcd:

$$\begin{aligned}
\gcd(33,7) &= \gcd(7,5) & 33 &= \boxed{7} \bullet 4 + 5 & (1)\\
&= \gcd(5,2) & 7 &= \boxed{5} \bullet 1 + 2 & (2)\\
&= \gcd(2,1) & 5 &= \boxed{2} \bullet 2 + 1 & (3)\\
&= \gcd(1,0) & 2 &= 1 \bullet 2 + 0 & (4)\\
&= 1 & & & (5)
\end{aligned}$$

Next, we re-arrange equations (1) - (3) by solving for the remainder:

$$\begin{aligned}
1 &= 5 - \boxed{2} \bullet 2 & (6)\\
2 &= 7 - \boxed{5} \bullet 1 & (7)\\
5 &= 33 - \boxed{7} \bullet 4 & (8)\\
& & (9)
\end{aligned}$$

Now, we backward substitute into the boxed numbers using the equations:

$$\begin{aligned}
1 &= 5 - \boxed{2} \bullet 2\\
&= 5 - (7 - \boxed{5} \bullet 1) \bullet 2\\
&= 3 \bullet \boxed{5} - 7 \bullet 2\\
&= 3 \bullet (33 - \boxed{7} \bullet 4) - 7 \bullet 2\\
&= 33 \bullet 3 + 7 \bullet -14
\end{aligned}$$

So, $1 = 33 \bullet 3 + \boxed{7} \bullet -14$. Thus, $33 - 14 = 19$ is the multiplicative inverse of 7 mod 33.

(b) Now, solve $7z \equiv 2 \pmod{33}$.

Solution:

If z is a solution to that equation, then multiplying both sides by 19, we have $z = 1z \equiv 19 \cdot 7z \equiv 19 \cdot 2 \equiv 5 \pmod{33}$. Hence, every solution must be of the form $z = 5 + 33k$ for some $k \in \mathbb{Z}$.

Furthermore, we can see that every number of this form is a solution since $(7(5 + 33k)) \bmod 33 = (35 + 7 \cdot 33k) \bmod 33 = 35 \bmod 33 = 2 = 2 \bmod 33$.

2. Induction with Sums: Equality

For any $n \in \mathbb{N}$, define S_n to be the sum of the squares of the first n positive integers, or

$$S_n = \sum_{i=1}^{n} i^2.$$

For all $n \in \mathbb{N}$, prove that $S_n = \frac{1}{6}n(n+1)(2n+1)$.

Solution:

Let $\mathsf{P}(n)$ be the statement "$S_n = \frac{1}{6}n(n+1)(2n+1)$" defined for all $n \in \mathbb{N}$. We prove that $\mathsf{P}(n)$ is true for all $n \in \mathbb{N}$ by induction on n.

Base Case. When $n = 0$, we know the sum of the squares of the first n positive integers is the sum of no terms, so we have a sum of 0. Thus, $S_0 = 0$. Since $\frac{1}{6}(0)(0+1)((2)(0)+1) = 0$, we know that $\mathsf{P}(0)$ is true.

Induction Hypothesis. Suppose that $\mathsf{P}(k)$ is true for an arbitrary $k \in \mathbb{N}$.

Induction Step. Examining S_{k+1}, we see that

$$S_{k+1} = \sum_{i=1}^{k+1} i^2 = \sum_{i=1}^{k} i^2 + (k+1)^2 = S_k + (k+1)^2.$$

By the induction hypothesis, we know that $S_k = \frac{1}{6}k(k+1)(2k+1)$. Therefore, we can substitute and rewrite the expression as follows:

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

Thus, we can conclude that $\mathsf{P}(k+1)$ is true.

Therefore, because the base case and induction step hold, $\mathsf{P}(n)$ is true for all $n \in \mathbb{N}$ by induction.

3. A Strict Inequality

Prove that $6n + 6 < 2^n$ for all $n \geq 6$.

Solution:

Let $P(n)$ be "$6n + 6 < 2^n$". We will prove $P(n)$ for all integers $n \geq 6$ by induction.

Base Case $(n = 6)$**:** $6 \cdot 6 + 6 = 42 < 64 = 2^6$, so $P(6)$ holds.

Induction Hypothesis: Assume that $6j + 6 < 2^j$ for an arbitrary integer $j \geq 6$.

Induction Step: Goal: Show $6(j + 1) + 6 < 2^{j+1}$

$$\begin{aligned}
6(j+1) + 6 &= 6j + 6 + 6 \\
&< 2^j + 6 && \text{[Induction Hypothesis]} \\
&< 2^j + 2^j && \text{[Since } 2^j > 6\text{, since } j \geq 6\text{]} \\
&< 2 \cdot 2^j \\
&< 2^{j+1},
\end{aligned}$$

which shows that $P(j + 1)$ is true.

Conclusion: $P(n)$ holds for all integers $n \geq 6$ by induction.

4. Another Inequality

Prove that, for all integers $n \geq 1$, if you have numbers $a_1, \cdots, a_n$ and $b_1, \cdots, b_n$, with $\forall i \in [n].\ a_i \leq b_i$, then:

$$\sum_{i=1}^{n} a_i \leq \sum_{i=1}^{n} b_i$$

Solution:

Let P(n) be the statement "if $a_1 \leq b_1$, $a_2 \leq b_2$, $\ldots$, $a_n \leq b_n$, then $\sum_{i=1}^{n} a_i \leq \sum_{i=1}^{n} b_i$". We prove that P($n$) is true for all integers $n \geq 1$ by induction on n:

Base Case ($n = 1$). Suppose $a_1 \leq b_1$. Using the definition of summation, we can see that

$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{1} a_i = a_1 \leq b_1 = \sum_{i=1}^{1} b_i = \sum_{i=1}^{n} b_i,$$

so the claim is true for $n = 1$.

Induction Hypothesis. Suppose that $P(k)$ holds for an arbitrary integer $k \geq 1$.

Induction Step. Suppose that $a_1 \leq b_1$, $a_2 \leq b_2$, $\ldots$, $a_{k+1} \leq b_{k+1}$. Then, we can calculate

$$\begin{aligned}
\sum_{i=1}^{k+1} a_i &= \sum_{i=1}^{k} a_i + a_{k+1} && \text{[Splitting the summation]} \\
&\leq \sum_{i=1}^{k} b_i + a_{k+1} && \text{[By IH]} \\
&\leq \sum_{i=1}^{k} b_i + b_{k+1} && \text{[By Assumption]} \\
&\leq \sum_{i=1}^{k+1} b_i && \text{[Algebra]}
\end{aligned}$$

This shows $P(k+1)$.

Therefore, we have shown the claim for all $n \in \mathbb{N}$ by induction.