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 $0 \leq y < 33$.

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. 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.

3. Divisibility by Induction

Prove that $9 \mid n^3 + (n+1)^3 + (n+2)^3$ for all $n > 1$ by induction.

Solution:

Let $P(n)$ be "$9 \mid n^3 + (n+1)^3 + (n+2)^3$". We will prove $P(n)$ for all integers $n > 1$ by induction.

Base Case $(n = 2)$**:** $2^3 + (2+1)^3 + (2+2)^3 = 8 + 27 + 64 = 99 = 9 \cdot 11$, so $9 \mid 2^3 + (2+1)^3 + (2+2)^3$.

Induction Hypothesis: Assume that $9 \mid j^3 + (j+1)^3 + (j+2)^3$ for an arbitrary integer $j > 1$. Note that this is equivalent to assuming that $j^3 + (j+1)^3 + (j+2)^3 = 9k$ for some integer k.

Induction Step: Goal: Show $9 \mid (j+1)^3 + (j+2)^3 + (j+3)^3$

$$
\begin{aligned}
(j+1)^3 + (j+2)^3 + (j+3)^3 &= (j+3)^3 + 9k - j^3 \text{ for some integer } k && \text{[Induction Hypothesis]} \\
&= j^3 + 9j^2 + 27j + 27 + 9k - j^3 \\
&= 9j^2 + 27j + 27 + 9k \\
&= 9(j^2 + 3j + 3 + k)
\end{aligned}
$$

So $9 \mid (j+1)^3 + (j+2)^3 + (j+3)^3$, which is $P(j+1)$.

Conclusion: $P(n)$ holds for all integers $n > 1$ 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.