CSE 311: Foundations of Computing I

Section 5: Number Theory and Induction Solutions

1. GCD

(a) Calculate gcd(100, 50).

(b) Calculate gcd(17, 31).

(c) Find the multiplicative inverse of 6 modulo 7.

(d) Does 49 have an multiplicative inverse modulo 7?

Solution:

a) 50

b) 1

c) 6

d) It does not. Intuitively, this is because 49x for any x is going to be 0 mod 7, which means it can never be 1.

2. Extended Euclidean Algorithm

(a) Find the multiplicative inverse y of $7 \bmod 33$. 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 $0 \leq y < 33$.

(b) Now, solve $7z \equiv 2 (\bmod 33)$ for all of its integer solutions z.

Solution:

Part (a) 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.

Part (b) If $7y \equiv 1 (\text{mod } 33)$, then

$$2 \cdot 7y \equiv 2 (\text{mod } 33).$$

So, $z \equiv 2 \times 19 (\text{mod } 33) \equiv 5 (\text{mod } 33)$. This means that the set of solutions is $\{5 + 33k \mid k \in \mathbb{Z}\}$.

3. Induction

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

$$S_n = 1^2 + 2^2 + \cdots + n^2.$$

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

Solution:

Let 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 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 P$(0)$ is true.

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

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

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

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 P$(k+1)$ is true.

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

(b) Define the triangle numbers as $\triangle_n = 1+2+\cdots+n$, where $n \in \mathbb{N}$. We showed in lecture that $\triangle_n = \frac{n(n+1)}{2}$. Prove the following equality for all $n \in \mathbb{N}$:

$$0^3 + 1^3 + \cdots + n^3 = \triangle_n^2$$

Solution:

First, note that $\triangle_n = (0+1+2+\cdots+n)$. So, we are trying to prove $(0^3+1^3+\cdots+n^3) = (0+1+\cdots+n)^2$. Let $\mathsf{P}(n)$ be the statement:

$$0^3 + 1^3 + \cdots + n^3 = (0 + 1 + \cdots + n)^2.$$

We prove that $\mathsf{P}(n)$ is true for all $n \in \mathbb{N}$ by induction on n.

Base Case. $0^3 = 0^2$, so $\mathsf{P}(0)$ holds.

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

Induction Step. We show $\mathsf{P}(k+1)$:

$$\begin{aligned}
0^3 + 1^3 + \cdots (k+1)^3 &= (0^3 + 1^3 + \cdots + k^3) + (k+1)^3 && \text{[Associativity]} \\
&= (0 + 1 + \cdots + k)^2 + (k+1)^3 && \text{[by Induction Hypothesis]} \\
&= \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3 && \text{[Substitution from note/class]} \\
&= (k+1)^2 \left(\frac{k^2}{2^2} + (k+1)\right) && \text{[Factor } (k+1)^2\text{]} \\
&= (k+1)^2 \left(\frac{k^2 + 4k + 4}{4}\right) && \text{[Add via common denominator]} \\
&= (k+1)^2 \left(\frac{(k+2)^2}{4}\right) && \text{[Factor numerator]} \\
&= \left(\frac{(k+1)(k+2)}{2}\right)^2 && \text{[Take out the square]} \\
&= (0 + 1 + \cdots + (k+1))^2 && \text{[Substitution from note/class]}
\end{aligned}$$

Therefore, $\mathsf{P}(n)$ is true for all $n \in \mathbb{N}$ by induction.

(c) Prove for all $n \in \mathbb{N}$ that if you have two groups of numbers, $a_1, \cdots, a_n$ and $b_1, \cdots, b_n$, such that $\forall (i \in [n]).\ a_i \le b_i$, then it must be that:

$$a_1 + \cdots + a_n \le b_1 + \cdots + b_n$$

Solution:

Let $P(n)$ be that "$a_1 + \cdots + a_n \le b_1 + \cdots + b_n$ for all groups of numbers such that $\forall (i \in [n]).\ a_i \le b_i$". We prove this by induction on n:

Base Case ($n = 0$). In this case there are 0 terms on both sides so the sums on both sides are 0. So the claim is true for $n = 0$.

Induction Hypothesis. Suppose for some arbitrary $k \in \mathbb{N}$ that $a_1 + \cdots a_k \le b_1 + \cdots b_k$ for all groups of numbers $a_1, \cdots, a_k$ and $b_1, \cdots, b_k$ such that $a_i \le b_i$ for all $i \in [k]$

Induction Step. Let the groups of numbers $a_1, \cdots, a_{k+1}$ and $b_1, \cdots, b_{k+1}$ be two groups such that $a_i \le b_i$ for all $i \in [k+1]$.

Note that

$$\begin{aligned}
a_1 + \cdots + a_{k+1} &= (a_1 + \cdots + a_k) + a_{k+1} && \text{[Splitting the summation]} \\
&\leq (b_1 + \cdots + b_k) + a_{k+1} && \text{[By IH]} \\
&\leq (b_1 + \cdots + b_k) + b_{k+1} && \text{[By Assumption]} \\
&\leq b_1 + \cdots + b_{k+1} && \text{[Algebra]}
\end{aligned}$$

Thus we have shown that if the claim is true for k, it is true for $k+1$.

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

4. Casting Out Nines

(a) Suppose that $a \equiv b \pmod{m}$. Prove by induction that for every integer $n \geq 1$, $a^n \equiv b^n \pmod{m}$.

Solution:

Let $\mathsf{P}(n)$ be the statement "$a^n \equiv b^n \pmod{m}$". We prove that $\mathsf{P}(n)$ is true for all integers $n \geq 1$ by induction.

Base Case. $(n = 1)$ We have $a^1 = a$ and $b^1 = b$, so we have $a^1 \equiv b^1 \pmod{m}$ by our assumption that $a \equiv b \pmod{m}$ and hence $\mathsf{P}(1)$ is true.

Induction Hypothesis. Suppose that $\mathsf{P}(k)$ is true for some arbitrary integer $k \geq 1$.

Induction Step. We need to prove that $a^{k+1} \equiv b^{k+1} \pmod{m}$. By the inductive hypothesis we have $a^k \equiv b^k \pmod{m}$ and by the assumption we have $a \equiv b \pmod{m}$. Using the multiplicative property of mods we have $a^k \cdot a \equiv b^k \cdot b \pmod{m}$. But this is just $a^{k+1} \equiv b^{k+1} \pmod{m}$.

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

Therefore, by induction $P(n)$ is true for all integers $n \geq 1$.

(b) Let $K \in \mathbb{N}$. Prove that if $K \equiv 0 \pmod{9}$, then the sum of the digits of K is a multiple of 9.

Solution:

Write $K = (d_m d_{m-1} \cdots d_1 d_0)_{10}$ where $d_0, \ldots, d_m$ are the base-10 digits of K. Then $K = \sum_{i=0}^{m} d_i 10^i$ by definition. We show that $K \equiv \sum_{i=0}^{m} d_i \pmod{9}$: Now $10 \equiv 1 \pmod{9}$ and so by part (a) we know that $10^i \equiv 1^i \pmod{9}$ for $i \geq 1$ which is just $10^i \equiv 1 \pmod{9}$. We also have $10^0 = 1$. Therefore, for any $i = 0, \ldots, m$ by the multiplicative property modulo 9, we have $d_i 10^i \equiv d_i \pmod{9}$. We then apply the sum property modulo 9 to derive that $\sum_{i=0}^{m} d_i 10^i \equiv \sum_{i=0}^{m} d_i \pmod{9}$. The left-hand quantity is just K by definition so we have $K \equiv \sum_{i=0}^{m} d_i \pmod{9}$.

In particular, since $K \equiv 0 \pmod{9}$ by assumption, we have $\sum_{i=0}^{m} d_i \equiv 0 \pmod{9}$ and hence 9 divides the sum of the digits of K which is what we wanted to prove.