Section 06: Solutions

1. GCD

(a) Calculate gcd(100, 50).

Solution:

50

(b) Calculate gcd(17, 31).

Solution:

1

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

Solution:

6

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

Solution:

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 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 $7z \equiv 2 (\text{mod } 33)$ for all of its integer solutions z.

Solution:

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. A Horse of a Different Color

Did you know that all dogs are named Dubs? It's true. Maybe. Let's prove it by induction. The key is talking about groups of dogs, where every dog has the same name.

Let $P(i)$ mean "all groups of i dogs have the same name." We prove $\forall n\ P(n)$ by induction on n.

Base Case: $P(1)$ Take an arbitrary group of one dog, all dogs in that group all have the same name (there's only the one, so it has the same name as itself).

Inductive Hypothesis: Suppose $P(k)$ holds for some arbitrary k.

Inductive Step: Consider an arbitrary group of $k+1$ dogs. Arbitrarily select a dog, D, and remove it from the group. What remains is a group of k dogs. By inductive hypothesis, all k of those dogs have the same name. Add D back to the group, and remove some other dog D'. We have a (different) group of k dogs, so the inductive hypothesis applies again, and every dog in that group also shares the same name. All $k+1$ dogs appeared in at least one of the two groups, and our groups overlapped, so all of our $k+1$ dogs have the same name, as required.

Conclusion: We conclude $P(n)$ holds for all n by the principle of induction.

Recalling that Dubs is a dog, we have that every dog must have the same name as him, so every dog is named Dubs.

This proof cannot be correct (the proposed claim is false). Where is the bug?

Solution:

The bug is in the final sentence of the inductive step. We claimed that the groups overlapped, i.e. that some dog was in both of them. That's true for large k, but not when $k+1=2$. When $k=2$, D is in a group by itself, and D' was in a group by itself. The inductive hypothesis holds (D has the only name in its subgroup, and D' has the only name in its subgroup) but returning to the full group $\{D, D'\}$ we cannot conclude that they share a name.

From there everything unravels. $P(1) \not\Rightarrow P(2)$, so we cannot use the principle of induction. It turns out this is the **only** bug in the proof. The argument in the inductive step is correct as long as $k+1 > 2$. But that implication is always vacuous, since $P(2)$ is false.

4. Induction with Equality

(a) Show using induction that $0+1+2+\cdots+n = \frac{n(n+1)}{2}$ for all $n \in \mathbb{N}$.

Solution:

For $n \in \mathbb{N}$ let $P(n)$ be "$0+1+\cdots+n = \frac{n(n+1)}{2}$". We show $P(n)$ for all $n \in \mathbb{N}$ by induction on n.

Base Case: We have $0 = \frac{0(0+1)}{2}$ which is $P(0)$ so the base case holds.

Inductive Hypothesis: Suppose $P(k)$ holds for some arbitrary integer $k \geq 0$.

Inductive Step: $\boxed{\text{Goal: Show } 0+1+\cdots+(k+1) = \frac{(k+1)(k+2)}{2}}$.

We have

$$\begin{aligned}
0+1+\cdots+k+(k+1) &= (0+1+\cdots+k)+(k+1) \\
&= \frac{k(k+1)}{2} + (k+1) && \text{[Inductive Hypothesis]} \\
&= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\
&= \frac{k(k+1)+2(k+1)}{2} \\
&= \frac{(k+1)(k+2)}{2} && \text{[Factor out } (k+1)\text{]}
\end{aligned}$$

This proves $P(k+1)$.

Conclusion: $P(n)$ holds for all $n \in \mathbb{N}$ by the principle of induction.

(b) Define the triangle numbers as $\triangle_n = 1 + 2 + \cdots + n$, where $n \in \mathbb{N}$. In part (a) we showed $\triangle_n = \frac{n(n+1)}{2}$. 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 $P(n)$ be the statement:

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

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

Base Case. $0^3 = 0^2$, so $P(0)$ holds.

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

Inductive Step. We show $P(k+1)$:

$$\begin{aligned}
0^3 + 1^3 + \cdots (k+1)^3 &= (0^3 + 1^3 + \cdots + k^3) + (k+1)^3 && \text{[Associativity]} \\
&= (0 + 1 + \cdots + k)^2 + (k+1)^3 && \text{[Inductive Hypothesis]} \\
&= \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3 && \text{[Part (a)]} \\
&= (k+1)^2 \left(\frac{k^2}{2^2} + (k+1)\right) && \text{[Factor } (k+1)^2\text{]} \\
&= (k+1)^2 \left(\frac{k^2 + 4k + 4}{4}\right) && \text{[Add via common denominator]} \\
&= (k+1)^2 \left(\frac{(k+2)^2}{4}\right) && \text{[Factor numerator]} \\
&= \left(\frac{(k+1)(k+2)}{2}\right)^2 && \text{[Take out the square]} \\
&= (0 + 1 + \cdots + (k+1))^2 && \text{[Part (a)]}
\end{aligned}$$

Conclusion: $P(n)$ is true for all $n \in \mathbb{N}$ by the principle of induction.

5. Induction with Divides

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 $9 \mid 2^3 + (2+1)^3 + (2+2)^3$, so $P(2)$ holds.

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 by the definition of divides.

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

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

Since j is an integer, $j^2 + 3j + 3 + k$ is also an integer. Therefore, by the definition of divides, $9 \mid (j+1)^3 + (j+2)^3 + (j+3)^3$, so $P(j) \to P(j+1)$ for an arbitrary integer $j > 1$.

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

6. Induction with 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 on n

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

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

Inductive Step: Goal: Show $6(k+1) + 6 < 2^{k+1}$

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

So $P(k) \to P(k+1)$ for an arbitrary integer $k \geq 6$.

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

7. Induction with Formulas

These problems are a little more difficult and abstract. Try making sure you can do all the other problems before trying these ones.

(a) (i) Show that given two sets A and B that $\overline{A \cup B} = \overline{A} \cap \overline{B}$. (Don't use induction.)

Solution:

Let x be arbitrary. Then,

$$\begin{aligned} x \in \overline{A \cup B} &\equiv \neg(x \in A \cup B) && \text{[Definition of complement]} \\ &\equiv \neg(x \in A \vee x \in B) && \text{[Definition of union]} \\ &\equiv \neg(x \in A) \wedge \neg(x \in B) && \text{[De Morgan's Laws]} \\ &\equiv x \in \overline{A} \wedge x \in \overline{B} && \text{[Definition of complement]} \\ &\equiv x \in (\overline{A} \cap \overline{B}) && \text{[Definition of intersection]} \end{aligned}$$

Since x was arbitrary we have that $x \in \overline{A \cup B}$ if and only if $x \in \overline{A} \cap \overline{B}$ for all x. By the definition of set equality we've shown,

$$\overline{A \cup B} = \overline{A} \cap \overline{B}.$$

(ii) Show using induction that for an integer $n \geq 2$, given n sets $A_1, A_2, \ldots, A_{n-1}, A_n$ that

$$\overline{A_1 \cup A_2 \cup \cdots \cup A_{n-1} \cup A_n} = \overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_{n-1}} \cap \overline{A_n}$$

Solution:

Let $P(n)$ be "given n sets $A_1, A_2, \ldots, A_{n-1}, A_n$ it holds that $\overline{A_1 \cup A_2 \cup \cdots \cup A_n} = \overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_{n-1}} \cap \overline{A_n}$." We show $P(n)$ for all integers $n \geq 2$ by induction on n.

Base Case: $P(2)$ says that for two sets A_1 and A_2 that $\overline{A_1 \cup A_2} = \overline{A_1} \cap \overline{A_2}$, which is exactly part (a) so $P(2)$ holds.

Inductive Hypothesis: Suppose that $P(k)$ holds for some arbitrary integer $k \geq 2$.

Inductive Step: Let $A_1, A_2, \ldots, A_k, A_{k+1}$ be sets. Then by part (a) we have,

$$\overline{(A_1 \cup A_2 \cup \cdots \cup A_k) \cup A_{k+1}} = \overline{A_1 \cup A_2 \cup \cdots \cup A_k} \cap \overline{A_{k+1}}.$$

By the inductive hypothesis we have $\overline{A_1 \cup A_2 \cup \cdots A_k} = \overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_k}$. Thus,

$$\overline{A_1 \cup A_2 \cup \cdots \cup A_k} \cap \overline{A_{k+1}} = (\overline{A_1} \cap \overline{A_2} \cap \cdots \overline{A_k}) \cap \overline{A_{k+1}}.$$

We've now shown

$$\overline{A_1 \cup A_2 \cup \cdots \cup A_k \cup A_{k+1}} = \overline{A_1} \cap \overline{A_2} \cap \cdots \overline{A_k} \cap \overline{A_{k+1}}.$$

which is exactly $P(k+1)$.

Conclusion $P(n)$ holds for all integers $n \geq 2$ by the principle of induction.

(b) (i) Show that given any integers a, b, and c, if $c \mid a$ and $c \mid b$, then $c \mid (a + b)$. (Don't use induction.)

Solution:

Let a, b, and c be arbitrary integers and suppose that $c \mid a$ and $c \mid b$. Then by definition there exist integers j and k such that $a = jc$ and $b = kc$. Then $a + b = jc + kc = (j + k)c$. Since $j + k$ is an integer, by definition we have $c \mid (a + b)$.

(ii) Show using induction that for any integer $n \geq 2$, given n numbers $a_1, a_2, \ldots, a_{n-1}, a_n$, for any integer c such that $c \mid a_i$ for $i = 1, 2, \ldots, n$, that

$$c \mid (a_1 + a_2 + \cdots + a_{n-1} + a_n).$$

In other words, if a number divides each term in a sum then that number divides the sum.

Solution:

Let $P(n)$ be "given n numbers $a_1, a_2, \ldots, a_{n-1}, a_n$, for any integer c such that $c \mid a_i$ for $i = 1, 2, \ldots, n$, it holds that $c \mid (a_1 + a_2 + \cdots + a_n)$." We show $P(n)$ holds for all integer $n \geq 2$ by induction on n.

Base Case: $P(2)$ says that given two integers a_1 and a_2, for any integer c such that $c \mid a_1$ and $c \mid a_2$ it holds that $c \mid (a_1 + a_2)$. This is exactly part (a) so $P(2)$ holds.

Inductive Hypothesis: Suppose that $P(k)$ holds for some arbitrary integer $k \geq 2$.

Inductive Step: Let $a_1, a_2, \ldots, a_k, a_{k+1}$ be $k + 1$ integers. Let c be arbitrary and suppose that $c \mid a_i$ for $i = 1, 2, \ldots, k + 1$. Then we can write

$$a_1 + a_2 + \cdots + a_k + a_{k+1} = (a_1 + a_2 + \cdots + a_k) + a_{k+1}.$$

The sum $a_1 + a_2 + \cdots + a_k$ has k terms and c divides all of them, meaning we can apply the inductive hypothesis. It says that $c \mid (a_1 + a_2 + \cdots + a_k)$. Since $c \mid (a_1 + a_2 + \cdots + a_k)$ and $c \mid a_{k+1}$, by part (a) we have,

$$c \mid (a_1 + a_2 + \cdots + a_k + a_{k+1}).$$

This shows $P(k + 1)$.

Conclusion: $P(n)$ holds for all integers $n \geq 2$ by induction the principle of induction.

8. Cantelli's Rabbits

Xavier Cantelli owns some rabbits. The number of rabbits he has in year n is described by the function $f(n)$:

$$\begin{aligned} f(0) &= 0 \\ f(1) &= 1 \\ f(n) &= 2f(n-1) - f(n-2) \text{ for } n \geq 2 \end{aligned}$$

Determine, with proof, the number, $f(n)$, of rabbits that Cantelli owns in year n. That is, construct a formula for $f(n)$ and prove its correctness.

Solution:

Let $P(n)$ be "$f(n) = n$". We prove that $P(n)$ is true for all $n \in \mathbb{N}$ by strong induction on n.

Base Cases $(n = 0, n = 1)$**:** $f(0) = 0$ and $f(1) = 1$ by definition.

Inductive Hypothesis: Assume that $P(0) \wedge P(1) \wedge \ldots P(k)$ hold for some arbitrary $k \geq 1$.

Inductive Step: We show $P(k+1)$:

$$\begin{aligned} f(k+1) &= 2f(k) - f(k-1) && \text{[Definition of } f\text{]} \\ &= 2(k) - (k-1) && \text{[Induction Hypothesis]} \\ &= k+1 && \text{[Algebra]} \end{aligned}$$

Conclusion: $P(n)$ is true for all $n \in \mathbb{N}$ by principle of strong induction.