Section 07: Solutions

1. Midterm Review: Translation

Let your domain of discourse be all coffee drinks. You should use the following predicates:

- $\texttt{soy}(x)$ is true iff x contains soy milk.
- $\texttt{whole}(x)$ is true iff x contains whole milk.
- $\texttt{sugar}(x)$ is true iff x contains sugar
- $\texttt{decaf}(x)$ is true iff x is not caffeinated.
- $\texttt{vegan}(x)$ is true iff x is vegan.
- $\texttt{RobbieLikes}(x)$ is true iff Robbie likes the drink x.

Translate each of the following statements into predicate logic. You may use quantifiers, the predicates above, and usual math connectors like $=$ and $\neq$.

(a) Coffee drinks with whole milk are not vegan. **Solution:**

$\forall x(\texttt{whole}(x) \rightarrow \neg\,\texttt{vegan}(x))$.

(b) Robbie only likes one coffee drink, and that drink is not vegan. **Solution:**

$\exists x \forall y(\texttt{RobbieLikes}(x) \wedge \neg\,\texttt{Vegan}(x) \wedge [\texttt{RobbieLikes}(y) \rightarrow x = y])$

OR $\exists x(\texttt{RobbieLikes}(x) \wedge \neg\,\texttt{Vegan}(x) \wedge \forall y[\texttt{RobbieLikes}(y) \rightarrow x = y])$

(c) There is a drink that has both sugar and soy milk. **Solution:**

$\exists x(\texttt{sugar}(x) \wedge \texttt{soy}(x))$

Translate the following symbolic logic statement into a (natural) English sentence. Take advantage of domain restriction.

$$\forall x([\texttt{decaf}(x) \wedge \texttt{RobbieLikes}(x)] \rightarrow \texttt{sugar}(x))$$

Solution:

Every decaf drink that Robbie likes has sugar.

Statements like "For every decaf drink, if Robbie likes it then it has sugar" are equivalent, but only partially take advantage of domain restriction.

2. Midterm Review: Number Theory

Let p be a prime number at least 3, and let x be an integer such that $x^2 \bmod p = 1$.

(a) Show that if an integer y satisfies $y \equiv 1 \pmod p$, then $y^2 \equiv 1 \pmod p$. (this proof will be short!) (Try to do this without using the theorem "Raising Congruences To A Power")
Solution:

Let y be an arbitrary integer and suppose $y \equiv 1 \pmod p$. We can multiply congruences, so multiplying this congruence by itself we get $y^2 \equiv 1^2 \pmod p$. Since y is arbitrary, the claim holds.

(b) Repeat part (a), but don't use any theorems from the Number Theory Reference Sheet. That is, show the claim directly from the definitions.

Solution:

Suppose $x \equiv 1 \pmod p$. By the definition of Congruences, $p \mid (x-1)$. Therefore, by the definition of divides, there exists an integer k such that

$$pk = (x-1)$$

By multiplying both sides of pk = (x - 1) by (x + 1) and re-arranging the equation, we have

$$pk(x+1) = (x-1)(x+1)$$
$$p(k(x+1)) = (x-1)(x+1)$$

Since $(x-1)(x+1) = x^2-1$, by replacing $(x-1)(x+1)$ with x^2-1, we have

$$p(k(x+1)) = x^2 - 1$$

Note that since k and x are integers, (k (x + 1)) is also an integer. Therefore, by the definition of divides $p \mid x^2 - 1$.
Hence, by the definition of Congruences, $x^2 \equiv 1 \pmod p$.

(c) From part (a), we can see that $x \bmod p$ can equal 1. Show that for any integer x, if $x^2 \equiv 1 \pmod p$, then $x \equiv 1 \pmod p$ or $x \equiv -1 \pmod p$. That is, show that the only value $x \bmod p$ can take other than 1 is $p-1$.
Hint: Suppose you have an x such that $x^2 \equiv 1 \pmod p$ and use the fact that $x^2 - 1 = (x-1)(x+1)$
Hint: You may the following theorem without proof: if p is prime and $p \mid (ab)$ then $p \mid a$ or $p \mid b$.

Solution:

Suppose $x^2 \equiv 1 \pmod p$. By the definition of Congruences,

$$p \mid x^2 - 1$$

Since $(x-1)(x+1) = x^2-1$, by replacing x^2-1 with $(x-1)(x+1)$, we have

$$p \mid (x-1)(x+1)$$

Note that for an integer p if p is a prime number and $p \mid (ab)$, then $p \mid a$ or $p \mid b$. In this case, since p is a prime number, by applying the rule, we have $p \mid (x-1)$ or $p \mid (x+1)$.
Therefore, by the definition of Congruences, we have $x \equiv 1 \pmod p$ or $x \equiv -1 \pmod p$.

3. Midterm Review: Induction

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 $\mathsf{P}(n)$ 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.

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

Inductive 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 inductive 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.

Conclusion: $P(n)$ for all integers $n \geq 0$ by the principle of induction.

4. 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.

5. 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.

6. Walk the Dawgs

Suppose a dog walker takes care of $n \geq 12$ dogs. The dog walker is not a strong person, and will walk dogs in groups of 3 or 7 at a time (every dog gets walked exactly once). Prove the dog walker can always split the n dogs into groups of 3 or 7.

Solution:

Let $P(n)$ be "a group with n dogs can be split into groups of 3 or 7 dogs." We will prove $P(n)$ for all natural numbers $n \geq 12$ by strong induction.

Base Cases $n = 12, 13, 14,$ **or** 15**:** $12 = 3 + 3 + 3 + 3$, $13 = 3 + 7 + 3$, $14 = 7 + 7$, So $P(12)$, $P(13)$, and $P(14)$ hold.

Inductive Hypothesis: Assume that $P(12), \ldots, P(k)$ hold for some arbitrary $k \geq 14$.

Inductive Step: $\boxed{\text{Goal: Show } k+1 \text{ dogs can be split into groups of size 3 or 7.}}$

We first form one group of 3 dogs. Then we can divide the remaining $k-2$ dogs into groups of 3 or 7 by the assumption $P(k-2)$. (Note that $k \geq 14$ and so $k-2 \geq 12$; thus, $P(k-2)$ is among our assumptions $P(12), \ldots, P(k)$.)

Conclusion: $P(n)$ holds for all integers $n \geq 12$ by by principle of strong induction.