Problem Set 2 Solutions

Problem 1. Prove by induction that $n^5 - n$ is a multiple of 5 for every integer n.

Let $P(n) =$ "$n^5 - n$ is divisible by 5"

Proof: By cases.

1. **Case 1:** $n \geq 0$. Proof by induction.
   Base Case: $n = 0$. $P(0)$ is true since $0^5 - 0 = 0$ is divisible by 5.
   Inductive Hypothesis: For $n = k$ assume $P(n = k)$ is true, that is, "$k^5 - k$ is divisible by 5"
   Inductive Step: For $n = k + 1$ prove P(n=k+1):

$$\begin{aligned}(k+1)^5 - (k+1) &= (k^5 + 5k^4 + 10k^3 + 10k^2 + 5k + 1) - (k+1) \\ &= (k^5 - k) + (5k^4 + 10k^3 + 10k^2 + 5k) \\ &= (k^5 - k) + 5(k^4 + 2k^3 + 2k^2 + k)\end{aligned}$$

   This sum is also divisible by 5 since both terms in the sum are divisible by 5. The first term is divisible by 5 by the inductive hypothesis and the second term is a multiple of 5.

2. **Case 2:** $n \leq 0$. Proof by induction.
   Base Case: $n = 0$. $P(0)$ is true since $0^5 - 0 = 0$ is divisible by 5.
   Inductive Hypothesis: For $n = k$ assume $P(n = k)$ is true, that is, "$k^5 - k$ is divisible by 5"
   Inductive Step: For $n = k - 1$ prove P(n=k-1):

$$\begin{aligned}(k-1)^5 - (k-1) &= (k^5 - 5k^4 + 10k^3 - 10k^2 + 5k - 1) - (k-1) \\ &= (k^5 - k) + (-5k^4 + 10k^3 - 10k^2 + 5k) \\ &= (k^5 - k) + 5(-k^4 + 2k^3 - 2k^2 + k)\end{aligned}$$

   This sum is also divisible by 5 since both terms in the sum are divisible by 5. The first term is divisible by 5 by the inductive hypothesis and the second term is a multiple of 5.

NOTE: The proof by cases could have been embedded in the inductive step.

Problem 2. Determine and prove which Fibonacci numbers are divisible by 3.

Notice that f_8 and f_9 are the same , modulo 3, as f_0 and f_1. The sequence of "f_n mod 3" numbers repeats after this point. Therefore, the pattern has period 8. Note, also, that for $n \equiv 0$ or $4 \pmod 8$, f_n is divisible by 3.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
f_n	0	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610	987
f_n mod 3	0	1	1	2	0	2	2	1	0	1	1	2	0	2	2	1	0
n mod 8	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0

Figure 1: Problem 2

We can formulate a definition for f_n divisible by 3 as follows:

$$\begin{aligned}
f_n &\equiv 0 \pmod 3 \text{ if } n \equiv 0 \text{ or } 4 \pmod 8 \\
f_n &\equiv 1 \pmod 3 \text{ if } n \equiv 1, 2 \text{ or } 7 \pmod 8 \\
f_n &\equiv 2 \pmod 3 \text{ if } n \equiv 3, 5 \text{ or } 6 \pmod 8
\end{aligned}$$

Proof: Prove the above conjecture by strong induction:

Base Case: There are two bases cases $n = 0$ and $n = 1$.
The conjecture is true for $n = 0$ since $n \equiv 0 \pmod 8$ and $f_0 \equiv 0 \pmod 3$.
The conjecture is true for $n = 1$ since $n \equiv 1 \pmod 8$ and $f_1 \equiv 1 \pmod 3$.

Inductive Hypothesis: Assume the conjecture is true for all values $\leq n$.

Inductive Step: Prove the conjecture for $(n + 1)$. There are eight cases depending on the value of $(n + 1)$ mod 8. We will carry out one of them; the other seven cases are similar.

Case 1: $(n + 1) \equiv 1 \pmod 8$ similar to case 5.

Case 2: $(n + 1) \equiv 2 \pmod 8$ similar to case 5.

Case 3: $(n + 1) \equiv 3 \pmod 8$ similar to case 5.

Case 4: $(n + 1) \equiv 4 \pmod 8$ similar to case 5.

Case 5: $(n + 1) \equiv 5 \pmod 8$

$$\begin{array}{rcll} f_{n+1} & = & f_n + f_{n-1} & \text{by the definition of Fibonacci numbers} \\ & = & f_{n\equiv 4 \pmod 8} + f_{(n-1)\equiv 3 \pmod 8} & \text{since } (n+1) \equiv 5 \pmod 8 \\ & & & \text{then } n \equiv 4 \pmod 8 \text{ and } (n-1) \equiv 3 \pmod 8 \\ & = & 0 + 2 \pmod 3 & \text{by the inductive hypothesis,} \\ & & & f_n \equiv 0 \pmod 3 \text{ and } f_{n-1} \equiv 2 \pmod 3 \\ & = & 2 \pmod 3 & \text{as desired.} \end{array}$$

Case 6: $(n+1) \equiv 6 \pmod 8$ similar to case 5.

Case 7: $(n+1) \equiv 7 \pmod 8$ similar to case 5.

Case 8: $(n+1) \equiv 0 \pmod 8$ similar to case 5.

Problem 3. Find a formula for

$$\frac{1}{1*2} + \frac{1}{2*3} + \frac{1}{3*4} + \ldots + \frac{1}{n(n+1)}$$

by examining the values of this expression for small values of n. Use mathematical induction to prove your result.

Prove that $\frac{1}{1*2} + \frac{1}{2*3} + ... + \frac{1}{n*(n+1)} = \frac{n}{n+1}$.

Proof by induction.
Let $P(n)$ be "$\frac{1}{1*2} + \frac{1}{2*3} + ... + \frac{1}{n*(n+1)} = \frac{n}{n+1}$."

Base Case: $n = 1$. $P(1)$ is true since $\frac{1}{1*2} = \frac{1}{(1+1)}$.

Inductive Hypothesis (I.H.): For $n = k$ assume $P(n = k)$ is true, that is, $\frac{1}{1*2} + \frac{1}{2*3} + ... + \frac{1}{k*(k+1)} = \frac{k}{k+1}$.

Inductive Step: For $n = k+1$ prove $P(n = k+1)$:

$$\begin{array}{rcll} \frac{1}{1*2} + \frac{1}{2*3} + ... + \frac{1}{(k+1)*((k+1)+1)} & = & \frac{1}{1*2} + \frac{1}{2*3} + ... \frac{1}{k*(k+1)} + \frac{1}{(k+1)*((k+1)+1)} & \\ & = & \frac{k}{k+1} + \frac{1}{(k+1)*((k+1)+1)} & \text{true by } \textbf{I.H.} \\ & = & \frac{k*(k+2)}{(k+1)*(k+2)} + \frac{1}{(k+1)*(k+2)} & \\ & = & \frac{k^2+2k+1}{(k+1)(k+2)} & \\ & = & \frac{(k+1)^2}{(k+1)(k+2)} & \end{array}$$

$$= \frac{k+1}{k+2}$$
$$= \frac{k+1}{(k+1)+1}$$

Problem 4. Use mathematical induction to prove that $\forall n \geq 4$, $n^2 < n!$.
Prove that $\forall n \geq 4$ $n^2 < n!$.

Proof by induction.

Base Case: True for $n = 4$ since $16 < 24$.

Inductive Hypothesis (I.H.): For $n = k$ assume $n^2 < n!$ is true.

Inductive Step: Prove for $n = k + 1$:

$$\begin{array}{rcll}
(n+1)^2 & = & n^2 + 2n + 1 & \\
& < & n! + 2n + 1 & \text{true by } \textbf{I.H.} \\
& < & n! + 2n + n = n! + 3n & \text{a valid upper bound } 1 < n \\
& < & n! + n * n = n! + n * n * 1 & \text{a valid upper bound } 3 < n \\
& < & n! + n * n^2 & \text{a valid upper bound } 1 < n \\
& < & n! + n * n! & \text{true by } \textbf{I.H.} \\
& = & (n+1)n! & \\
& = & (n+1)! &
\end{array}$$

Problem 5. Define a new propositional operator $\oplus$ as follows: for propositions p and q, $p \oplus q$ is true if exactly one of p and q is true.

(a) Write $p \oplus q$ in terms of the standard operators $\vee, \wedge, \neg$.

(b) Let $P_1, \ldots, P_n$ be n propositions and Q_n the proposition $P_1 \oplus P_2 \oplus \cdots \oplus P_n$. Prove by induction on n that Q_n is true if and only if the number of true propositions among $P_1, \ldots, P_n$ is odd.

(c) $p \otimes q = (p \vee q) \wedge \neg(p \wedge q)$

(d) *Proof by induction on n.*

Let S(n) = "Q_n is true $\iff$ the number of true propositions $P_1 \ldots P_n$ is odd.

Notation: Q_n is true(false) can also be written as $Q_n = 1(0)$.

Base Case: $S(n)$ is true for $n = 1$. Since $Q_1 = P_1$, Q_1 is made up of an odd number of propositions P, and Q_1 is true $\iff$ P_1 is true.

$S(n)$ is true for $n = 2$. Since $Q_2 = P_1 \otimes P_2 = (P_1 \vee P_2) \wedge \neg(P_1 \wedge P_2)$ one can trivially fill in the truth table to show that $S(2)$ is true.

p	q	(p ∨ q) ∧ ¬ (p ∧ q)
0	0	0
0	1	1
1	0	1
1	1	0

Figure 2: Problem 5

Inductive Hypothesis (I.H.): For n assume that "Q_n is true $\Longleftrightarrow$ the number of true propositions $P_1 ... P_n$ is odd", ie. that $S(n)$ is true.

Inductive Step: Prove $S(n+1)$

$$\begin{aligned} Q_{n+1} &= P_1 \otimes P_2 \otimes ... \otimes P_n \otimes P_{n+1} \\ &= Q_n \otimes P_{n+1} \end{aligned}$$

We have now reverted to a $n = 2$ scenario where there are 4 cases as seen in Figure 2.

Proof by cases:

Case 1: $Q_n = 0$ and $P_{n+1} = 0$.

Thus Q_{n+1} is False. Q_{n+1} also has an even number of true propositions since Q_n has an even number of true propositions (true by **I.H.**).

Case 2: $Q_n = 0$ and $P_{n+1} = 1$.

Thus Q_{n+1} is true. A true P_{n+1} plus an even number of true propositions in Q_n (true by **I.H.**) equals an odd number of true propositions for Q_{n+1}.

Case 3: $Q_n = 1$ and $P_{n+1} = 0$.

Thus Q_{n+1} is true. A false P_{n+1} plus an odd number of true propositions in Q_n (true by **I.H.**) equals an odd number of true propositions for Q_{n+1}.

Case 4: $Q_n = 1$ and $P_{n+1} = 1$.

Thus Q_{n+1} is false. A true P_{n+1} plus an odd number of true propositions in Q_n (true by **I.H.**) equals an even number of true propositions for Q_{n+1}.

Therefore, Q_{n+1} is true $\Longleftrightarrow$ an odd number of $P_1 ... P_{n+1}$ are true

Problem 6. What are the fallacies in the following arguments? Don't just explain why the claim is wrong; rather, explain how the argument violates the notion of correct proofs.

(a) Claim: Every integer is nonnegative. Proof: 0 is nonnegative. Assuming n is nonnegative, $n + 1$ is certainly nonnegative.

(b) Claim: Every natural number is a prime or a perfect square. Proof: as the inductive hypothesis, use $P(n)$ ="every number less than or equal to n is a prime or a perfect square." $P(1)$ is certainly true. Now consider n. If n is prime we are done. Otherwise, n can be factored as $n = rs$ with r and s less than or equal to $n - 1$. By the inductive hypothesis, r and s are perfect squares, $r = u^2$ and $v = s^2$. Then $n = rs = u^2v^2 = (uv)^2$.

(c) Claim: no quantity of homework problems is too many. Proof: Base case: Clearly 0 homework problems is not too many. Inductive step: if n homework problems are not too many, then certainly $n + 1$ homework problems is not too many.

(d) The claim is for all integers but the proof only checks the natural numbers.

(e) The proof does not consider the case when r and/or s are primes. It also neglects to prove anything about zero.

(f) "Too many" is an ill-defined relation. **OR** asserting the conclusion.

Problem 7. Using only the Peano Axioms, prove

$$\neg(\exists x, y)(x = y' \wedge y = x')$$

(recall that x' is the successor of x).

Peano's Axioms define the natural numbers $\mathbb{N}$. We use two primitive symbols: 0 and $'$ (successor).

1. $0 \in \mathbb{N}$
2. $(\forall x \in \mathbb{N}),\ x' \in \mathbb{N}$
3. $\forall x, y \in \mathbb{N},\ x' = y' \Longrightarrow x = y$ (no two numbers have same successor)
4. $\neg \exists x \in \mathbb{N}$ such that $0 = x'$ (equivalently, $\forall x \in \mathbb{N}, x' \neq 0$)
5. (Induction) $\forall S \subseteq \mathbb{N}$, if $0 \in S$ and $\forall x \in \mathbb{N}, (x \in S \Longrightarrow x' \in S)$, then $S = \mathbb{N}$.

Theorem Prove $\neg(\exists x, y)(x = y' \wedge y = x')$.

Proof

$\neg(\exists x, y)(x = y' \wedge y = x') \iff (\forall x, y)\neg(x = y' \wedge y = x')$.

Substituting $y = x'$ into $x = y'$, then $(x = y' \wedge y = x') \Longrightarrow (x = (x')')$.

The contrapositive of the above is $\neg(x = (x')') \Longrightarrow \neg(x = y' \wedge y = x')$. Thus,

$(\forall x, y)\neg(x = y' \wedge y = x') \iff (\forall x)\neg(x = (x')')$.

Let $S = \{x \mid x \neq (x')'\}$. Must show $S = \mathbb{N}$.

Basis Step $0 \in S$, since $0 \neq x''$ by the 4 Axiom.

Inductive Step: Assume $x \in S$.

$$\begin{aligned} x \in S &\implies x \neq x'' \\ &\implies x' \neq x''' \\ &\implies x' \in S \end{aligned}$$

(In the second implication we apply the contrapositive of axiom 3, taking $y = x''$).

Thus (by the syllogism inference rule and universal generalization) $x \in S \implies x' \in S$. Thus, by the induction axiom, $S = \mathbb{N}$.

Problem 8. Give a recursive definition of multiplication of natural numbers in terms of addition. Using standard facts about addition (associativity, commutativity, etc) as axioms, prove that $x(y + z) = xy + xz$ and $(x + y)z = xz + yz$.

Axioms of addition:

- $n + k' = (n + k)'$
- $(x + y) + z = x + (y + z)$
- $n + 0 = n$ (implicit universal quantification)

We define multiplication:

- $n * 0 = 0$ (implicit universal quantification)
- $n * k' = n * k + n$

This is a *recursive* definition: it lets us compute $n * k$ for any n, k. For example,

$$\begin{aligned} 3 * 2 &= 3 * 1 + 3 \\ &= (3 * 1) + 3 \\ &= (3 * 0 + 3) + 3 \\ &= (0 + 3) + 3 \\ &= (3) + 3 \\ &= 3 + 2' \\ &= (3 + 1')' \\ &= (3 + 1)')' \\ &= (3 + 0')')' \\ &= ((3 + 0)')')' \\ &= (3')')' \\ &= (4')' \\ &= 5' \\ &= 6. \end{aligned}$$

Theorem: $x(y+z) = xy + xz$.

Proof: Let $S = \{z|\forall(x,y)\ x(y+z) = xy + xz\}$. Must show $S = \mathbb{N}$. (By induction on z.)
Basis Step: $0 \in S$ (means true for $z = 0$) since,

$$\begin{aligned} x(y+0) &= x(y) \text{ axiom 3 of addition} \\ &= xy + 0 \text{ axiom 3 of addition} \\ &= xy + x0 \text{ definition 1 of multiplication} \end{aligned}$$

Inductive Hypothesis (I.H.): Suppose $z \in S$. (Assume that $x(y+z) = xy + xz$ is true for z.)

Inductive Step: Prove for (z'):

$$\begin{aligned} x(y+(z')) &= x((y+z)') \text{ by axiom 1 of addition} \\ &= x(y+z) + x \text{ by definition 2 of multiplication} \\ &= xy + xz + x \text{ by } \textbf{I.H.} \\ &= xy + x(z') \text{ definition 2 of multiplication} \end{aligned}$$

Theorem: $(x+y)z = xz + yz$.

Proof: Let $S = \{z|\forall(x,y)\ (x+y)z = xz + yz\}$. Must show $S = \mathbb{N}$. (By induction on z.)
Basis Step: $0 \in S$ (means true for $z = 0$) since,

$$\begin{aligned} (x+y)*0 &= 0 \text{ by definition 1 of multiplication} \\ &= 0 + 0 \text{ axiom 3 of addition} \\ &= x0 + y0 \text{ definition 1 of multiplication} \end{aligned}$$

Inductive Hypothesis (I.H.): Assume $z \in S$ (Assume that $(x+y)z = xz + yz$ is true for z.)

Inductive Step: Prove for (z'):

$$\begin{aligned} (x+y)*(z') &= (x+y)z + (x+y) \text{ by definition 2 of multiplication} \\ &= xz + yz + x + y \text{ by } \textbf{I.H.} \\ &= x(z') + y(z') \text{ definition 2 of multiplication} \end{aligned}$$

Problem 9. A disgraceful disease strikes a monastery. The monks are informed that at least one of them has the disease. All monks are ordered to leave the monastery as soon that they are certain that they are infected. The disease demonstrates itself by a mark on the forehead (all sick people get the mark). Unfortunately in this monastery there are no mirrors and the monks are not allowed any form of communication. Monks gather to pray every morning so they can all see each other. If they become certain that they are infected they depart during that night.

Proof. Let m be the number of infected monks. We know that $m \geq 1$. We claim that all and only the infected monks will leave, and they will leave the night of the m^{th} day. More formally, we will prove by strong induction on n the following statement: the night of the n^{th} day monk M will depart if and only if M is infected and the number of infected monks m is equal to n.

Base Case (n=1): We distinguish three cases:

- If monk M is sick, and the number of infected monks is $m = 1$, M is the only infected monk and he cannot see any monk with the mark on the forehead. Since he knows that at least one monk is infected, he will be certain that he is infected and will depart during the night of the first day.
- If monk M is sick, but the number of infected monks is $m > 1$, M can see $m - 1 \geq 1$ monks with the mark on the forehead. Since, as far as M knows, the number of infected monks could be $m - 1$ as well as m, he does not know if he is infected or not, and therefore he won't leave.
- If monk M is not sick, he can see m monks with the mark on the forehead. Since, as far as M knows, the number of infected monks could be m as well as $m + 1$, he does not know if he is infected or not, and therefore he won't leave.

Inductive Case ($n \geq 2$): If $m < n$ then by induction hypothesis the infected monks departed the monastery on the m^{th} day, and all remaining monks will know that they are not infected and will stay in the monastery on the n^{th} day. Otherwise, $m \geq n$ and no monk departed the monastry before the n^{th} day. Since the monks are rational, on the n^{th} day they will know that the number of infected monks is at least n and that all monks are aware of that.

We now distinguish three cases:

- If monk M is sick, and the number of infected monks is $m = n$, M will know he is infected because he can see only $m - 1$ monks with the mark on the forehead. So, he will depart the monastry that same night.
- If monk M is sick, but the number of infected monks is $m > n$, M can see $m - 1 \geq n$ monks with the mark on the forehead. Since, as far as M knows, the number of infected monks could be $m - 1$ as well as m, he does not know if he is infected or not, and therefore he won't depart the monastry on that night.
- If monk M is not sick, he can see m monks with the mark on the forehead. Since, as far as M knows, the number of infected monks could be m as well as $m + 1$, he does not know if he is infected or not, and therefore he won't depart the monastry on that night.