Section 05: Solutions

1. GCD

(a) Calculate gcd(100, 50).

Solution:

50

(b) Calculate gcd(17, 31).

Solution:

1

(c) Find the multiplicative inverse of $6 \pmod 7$.

Solution:

6

(d) Does 49 have an multiplicative inverse $\pmod 7$?

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. Mod Review

(a) Prove that if $n \mid m$, where n and m are integers greater than 1, and if $a \equiv b \pmod m$, where a and b are integers, then $a \equiv b \pmod n$. **Solution:**

Let n, m, a, and b be arbitrary integers.
Suppose $n \mid m$ with $n, m > 1$, and $a \equiv b \pmod m$. By definition of divides, we have $m = kn$ for some $k \in \mathbb{Z}$. By definition of congruence, we have $m \mid b - a$, which means that $b - a = mj$ for some $j \in \mathbb{Z}$. Combining the two equations, we see that $b - a = (knj) = n(kj)$. By the definition of divides, $n \mid (b - a)$ By definition of congruence, we have $a \equiv b \pmod n$, as required. Since n and m were arbitrary, the claim holds.

3. Modular Multiplication

Write an English proof to prove that for an integer $m > 0$ and any integers a, b, c, d, if $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then $ac \equiv bd \pmod m$.

Solution:

Let $m > 0$, a, b, c, d be arbitrary integers. Assume that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then by definition of mod, $m \mid (a-b)$ and $m \mid (c-d)$. Then by definition of divides, there exists some integer k such that $a - b = mk$, and there exists some integer j such that $c - d = mj$. Then $a = b + mk$ and $c = d + mj$. So, multiplying, $ac = (b+mk)(d+mj) = bd + mkd + mjb + m^2jk = bd + m(kd + jb + mjk)$. Subtracting bd from both sides, $ac - bd = m(kd + jb + mjk)$. By definition of divides, $m \mid ac - bd$. Then by definition of congruence, $ac \equiv bd \pmod{m}$.

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

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

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

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

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

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

$$\begin{aligned}
0^3 + 1^3 + \cdots (k+1)^3 &= (0^3 + 1^3 + \cdots + k^3) + (k+1)^3 && \text{[Associativity7]}\\
&= (0 + 1 + \cdots + k)^2 + (k+1)^3 && \text{[Inductive Hypothesis]}\\
&= \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3 && \text{[Part (a)]}\\
&= (k+1)^2 \left(\frac{k^2}{2^2} + (k+1)\right) && \text{[Factor } (k+1)^2\text{]}\\
&= (k+1)^2 \left(\frac{k^2 + 4k + 4}{4}\right) && \text{[Add via common denominator]}\\
&= (k+1)^2 \left(\frac{(k+2)^2}{4}\right) && \text{[Factor numerator]}\\
&= \left(\frac{(k+1)(k+2)}{2}\right)^2 && \text{[Take out the square]}\\
&= (0 + 1 + \cdots + (k+1))^2 && \text{[Part (a)]}
\end{aligned}$$

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

5. Induction with Mod

Prove that the equivalence $4^n \equiv 1(\text{mod } 3)$ holds for all $n \in \mathbb{N}$ by induction
Solution:

Let $P(n)$ be "$4^n \equiv 1(\text{mod } 3)$". We will prove $P(n)$ for all integers $n \in \mathbb{N}$ by induction.
From the definition of modular equivalence, it follows that $3 \mid (4^n - 1)$
And from the definition of divides, we see that $4^n - 1 = 3k$ or $4^n = 3k + 1$ for some integer k

Base Case $(n = 0)$**:** $4^0 = 1 = 0 + 1 = 3(0) + 1$, so $P(0)$ holds.

Induction Hypothesis: Assume that $4^j \equiv 1(\text{mod } 3)$ for an arbitrary integer $j \geq 0$.
Note that this is equivalent to assuming that $4^j - 1 = 3k$ or $4^j = 3k + 1$ for some integer k by the definition of divides and modular equivalence.

Induction Step: $\boxed{\text{Goal: Show } 4^{(j+1)} \equiv 1(\text{mod } 3)}$

$$\begin{aligned}
4^{(j+1)} &= 4^j \cdot 4\\
&= (3t + 1) \cdot 4 \text{ for some integer } t && \text{[Induction Hypothesis]}\\
&= 12t + 4\\
&= 3(4t) + 3 + 1\\
&= 3(4t + 1) + 1
\end{aligned}$$

Since t is an integer, $4t + 1$ is also an integer so we got $3k + 1$ for some integer k.
This demonstrates that $4^{(j+1)} = 3k + 1$ holds which shows,
$4^{(j+1)} \equiv 1(\text{mod } 3)$ for an arbitrary integer j by the definition of divides and modular equivalence.

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

6. 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: $\boxed{\text{Goal: Show } 9 \mid (j+1)^3 + (j+2)^3 + (j+3)^3}$

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

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.

7. 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: $\boxed{\text{Goal: Show } 6(k+1) + 6 < 2^{k+1}}$

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

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.

8. Cantelli's Rabbits

Xavier Cantelli owns some rabbits. The number of rabbits he has in any given year is described by the function f:

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

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 $P(0) \land P(1) \land \ldots P(k)$ 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.

9. 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.