Updated April 19, 2018.

Problem 1

Problem Statement

Let a be any integer and let b and c be odd integers. Prove that $ab + ac$ is an even integer.

Common Feedback

- Avoid the word "prove" in the statement of your proposition. Use a conditional statement, as in the solution below.

Solution (from Seth McRobert)

Proposition. *If b and c are odd integers and a is any integer, then $ac+ab$ is an even integer.*

Proof. Since b and c are odd integers, there exists some integers m and n such that $b = 2m + 1$ and $c = 2n + 1$.

$$\begin{aligned} ab + ac &= a(b + c) \\ &= a((2m + 1) + (2n + 1)) \\ &= a(2m + 2n + 2) \\ &= 2a(m + n + 1) \end{aligned}$$

By the closure of the integers under multiplication and addition, we know that $a(m + n + 1)$ is an integer. Call this integer p, so that we have $ab + ac = 2p$. Therefore, $ab + ac$ is even.

□

Problem 2

Problem Statement

Definition. *We say an integer k **divides** another integer n provided we can write $n = km$ for some integer m. (For example, 3 divides 15 since $15 = 3 \cdot 5$.)*

Part A

The following proposition is true. You do not need to prove it.

Proposition. *If a divides b and a divides c, then a divides $b + c$.*

Write the inverse, converse, and contrapositive of this proposition. Which of these is equivalent to the original proposition? For the others, provide a specific example of a, b, and c where the statement fails to be true.

Part B

Show that the following statement is not true in general by writing its negation and giving a specific exmaple where the negation is true.

If a divides bc, then a divides b or a divides c.

Common Feedback

- Be aware of instances where DeMorgan's law is needed in negations. For example, when writing the inverse in Part A, we encounter $\neg((a \mid b) \wedge (a \mid c))$, which is logically equivalent to $(a \nmid b) \vee (a \nmid c)$ by DeMorgan.
- The negation of a conditional statement is not another conditional statement. To negate a conditional statement, we want to show that the hypothesis holds **and** the conclusion does not. For Part B, we could write symbolically:

$$\begin{aligned} \neg(P \to (Q \vee R)) &\equiv P \wedge \neg(Q \vee R) \\ &= P \wedge \neg Q \wedge \neg R \end{aligned}$$

Solution (from JP Miranda)

Part A

Proposition. *If a divides b and a divides c, then a divides $b + c$.*

Inverse. *If a does not divide b or a does not divide c, then a does not divide $b + c$.*

An example that falsifies the inverse would be if $a = 8$, $b = 7$, and $c = 9$, where a does not divide b and a does not divide c, but a divides $b + c$.

Converse. *If a divides $b + c$, then a divides b and a divides c.*

An example that falsifies the inverse would be if $a = 8$, $b = 7$, and $c = 9$, where a divides $b + c$, but a does not divide b and a does not divide c.

Contrapositive. *If a does not divide $b + c$, then a does not divide b or a does not divide c.*

The contrapositive is equivalent to the original proposition.

Part B

Proposition. *If a divides bc, then a divides b or a divides c.*

Negation. *a divides bc and a does not divide b and a does not divide c.*

An specific case where the negation is true would be if $a = 15$, $b = 5$, and $c = 6$, where a divides bc and a does not divide b and a does not divide c.

Problem 3

Complete exercise # 11 from Section 2.4 in the text.

Common Feedback

- The phrase "such that" follows "there exists", but not "for all". See the third item in the solution for an example.

Solution (from Seth McRobert)

- A function f is continuous at the real number a provided that $(\forall \epsilon \in \mathbb{R})(\epsilon > 0)(\exists \delta \in \mathbb{R})(\delta > 0)(|x - a| < \delta \to |f(x) - f(a)| < \epsilon)$.
- A function f is not continuous at the real number a provided that $(\exists \epsilon \in \mathbb{R})(\epsilon > 0)(\forall \delta \in \mathbb{R})(\delta > 0)(|x - a| < \delta \wedge |f(x) - f(a)| \geq \epsilon)$.
- There is a real number $\epsilon > 0$ such that for all real numbers $\delta > 0$, it is true that $|x - a| < \delta$ and $|f(x) - f(a)| \geq \epsilon$.

Problem 4

Prove the following statement by contraposition (see exercise # 9 from Section 3.2 in the text for more details):

Let $x \in \mathbb{R}$. If x is irrational, then $\sqrt{x}$ is irrational.

Common Feedback

- Whenever possible, try to avoid making changes to both sides of an equation when carrying out a long string of algebraic manipulations.
- Use `\left(` and `\right)` to get parentheses that stretch to fit your symbols (such as around a fraction).

Solution (from Caitlynn Croner)

Proposition. *Let $x \in \mathbb{R}$. If x is irrational, then $\sqrt{x}$ is irrational.*

Proof. If we take the contrapositive of the proposition we have, if $\sqrt{x}$ is rational, then x is rational. If x is rational we can substitute some integers m/n for x.

$$\sqrt{x} = \frac{m}{n}$$

We can square both sides to eliminate the square root.

$$\begin{aligned}(\sqrt{x})^2 &= \left(\frac{m}{n}\right)^2 \\ &= \frac{m^2}{n^2}\end{aligned}$$

By closure of integers under multiplication we know that m^2 and n^2 are integers. Therefore, x is a rational number. Since the contrapositive of the proposition is true the proposition itself must also be true. □

Problem 5

Prove the following statement by construction:

> Let $p, q \in \mathbb{Q}$ with $p < q$. There exists a rational number x such that $p < x < q$.

Common Feedback

- The value of x you construct must satisfy $p < x < q$ for *every* choice of p and q.
- You should verify two key facts about the x you construct: x is rational and $p < x < q$.

Solution (from Austin Mohr)

Proposition. *Let $p, q \in \mathbb{Q}$ with $p < q$. There exists a rational number x such that $p < x < q$.*

Proof. Define $x = \frac{1}{2}(p+q)$. We first show that x is indeed a rational number. Since p and q are both rational, we may write $p = \frac{j}{k}$ and $q = \frac{m}{n}$ with $j, k, m, n \in \mathbb{Z}$ and $k, n \neq 0$. Now,

$$\begin{aligned}x &= \frac{1}{2}(p+q) \\ &= \frac{1}{2}\left(\frac{j}{k} + \frac{m}{n}\right) \\ &= \frac{1}{2} \cdot \frac{jn+mk}{kn} \\ &= \frac{jn+mk}{2kn}.\end{aligned}$$

By the closure of integers under addition and multipication, we know that $jn+mk, 2kn \in \mathbb{Z}$. Moreover, since $k, n \neq 0$, we know $kn \neq 0$. Hence, x is a rational number.

It remains to show $p < x < q$. First, observe

$$\begin{aligned}x &= \frac{1}{2}(p+q) \\ &> \frac{1}{2}(p+p) \\ &= p.\end{aligned}$$

Similarly,

$$\begin{aligned} x &= \frac{1}{2}(p+q) \\ &< \frac{1}{2}(q+q) \\ &= q. \end{aligned}$$

Taken together, we have $p < x < q$, as desired. □

Problem 6

Prove the following statement by contradiction. (Hint: $\sin^2\theta + \cos^2\theta = 1$)

> For each real number θ, if $0 < \theta < \frac{\pi}{2}$, then $\sin\theta + \cos\theta > 1$.

Common Feedback

- Whenever possible, try to avoid making changes to both sides of an equation when carrying out a long string of algebraic manipulations.
- Use `\sin` and `\cos` for sine and cosine.
- The negation of $\sin\theta + \cos\theta > 1$ is $\sin\theta + \cos\theta \leq 1$, so your proof should start something like the following: Suppose $0 \leq \theta \leq \frac{\pi}{2}$ and suppose, for contradiction, that $\sin\theta + \cos\theta \leq 1$.

Solution (from Austin Mohr)

Proposition. *For each real number θ, if $0 < \theta < \frac{\pi}{2}$, then $\sin\theta + \cos\theta > 1$.*

Proof. Suppose, for contradiction, there is a real number α such that $0 < \alpha < \frac{\pi}{2}$, yet $\sin\alpha + \cos\alpha \leq 1$. Since $\sin\alpha + \cos\alpha$ is positive for all α in the specified domain, we may square both sides of the previous inequality to obtain $(\sin\alpha + \cos\alpha)^2 \leq 1$. Now,

$$\begin{aligned} (\sin\alpha + \cos\alpha)^2 &= \sin^2\alpha + 2\sin\alpha\cos\alpha + \cos^2\alpha \\ &= 1 + 2\sin\alpha\cos\alpha \\ &> 1, \end{aligned}$$

since $2\sin\alpha\cos\alpha$ is strictly positive. The preceding derivation contradicts the fact that $(\sin\alpha + \cos\alpha)^2 \leq 1$, so our initial assumption is false. Therefore, for each real number θ, if $0 < \theta < \frac{\pi}{2}$, then $\sin\theta + \cos\theta > 1$. □

Problem 7

Prove the following statement by case analysis.

> For each integer n, if $n \not\equiv 0 \pmod 7$, then $n^2 \not\equiv 0 \pmod 7$.

Common Feedback

- Exit math mode or use `\text{}` to get the appropriate spacing in front of "(mod 7)". For example: `$n \equiv 1$ (mod 7)` or `$n \equiv 1 \text{ (mod 7)}$`
- The six cases can be analyzed all at once quite elegantly (see Chong's solution).

Solution (from Chong Lok)

Theorem. *For each integer n, if $n \not\equiv 0$ (mod 7), then $n^2 \not\equiv 0$.*

Proof. If $n \not\equiv 0 \pmod 7$, then $n = 7k + r$, where $k \in \mathbb{Z}$, $r \in \{1, 2, 3, 4, 5, 6\}$. Now,

$$\begin{aligned} n^2 &= (7k + r)^2 \\ &= 49k^2 + 14kr + r^2 \\ &= 7(k^2 + 2kr) + r^2. \end{aligned}$$

Thus, we have $n^2 = 7a + b$, where $a \in \mathbb{Z}$ and $b \in \{1, 4, 9, 16, 25, 36\}$. Since none of the possible values for b is divisible by 7, it follows that n^2 is not divisible by 7. In other words, $n^2 \not\equiv 0 \pmod 7$. □

Problem 8

Prove the following statement by induction.

> The congruence $4^n \equiv 1 \pmod 3$ holds for each natural number n.

Common Feedback

- The correct inductive hypothesis is: Suppose there exists a natural number k such that $4^k \equiv 1 \pmod 3$.
- Be very careful of question-begging in induction proofs. We can write $4^k + 1 = 3\ell$ for some ℓ because we really are taking that as a hypothesis. We *cannot* start our inductive step with $4^{k+1} + 1 = 3m$ for some m because that's the very thing we are trying to *prove*.

Solution (from Caitlynn Croner)

Proposition. *The congruence $4^n \equiv 1$ (mod 3) holds for each natural number n.*

Proof. Base case: When $n = 1$, observe that $4^1 - 1 = 3$ and $3|3$.

For induction, suppose $4^k \equiv 1 \pmod 3$. We can show that $4^{k+1} \equiv 1 \pmod 3$. Since $4^k - 1$ is divisible by 3 we can write it as a multiple of 3. The expression can be written as

$$4^k - 1 = 3n$$

for some integer n. Next we multiply both sides by 4.

$$4^{k+1} - 4 = 12n$$
$$4^{k+1} - 1 = 12n - 3$$
$$4^{k+1} - 1 = 3(4n - 1)$$

By closure of integers under multiplication and addition $4n-1$ is an integer. Clearly we can see that 4^{k+1} is a multiple of 3 and is therefore divisible by 3. □

Problem 9

Let $a_1 = a_2 = a_3 = 1$ and define $a_n = a_{n-1} + a_{n-2} + a_{n-3}$ for each natural number $n \geq 4$. Prove (by strong induction) that $a_n \leq 2^{n-2}$ for each natural number $n \geq 2$.

Common Feedback

- The correct strong inductive hypothesis is: Suppose there exists a natural number k such that $a_n \leq 2^{n-2}$ for all natural numbers $2 \leq n \leq k$. (A less formal, but perhaps more transparent, version is: Suppose there exists a natural number k such that $a_2 \leq 2^0, a_3 \leq 2^1, \ldots, a_k \leq 2^{k-2}$.)
- You need three base cases ($n = 2, 3, 4$) since the recurrence relation reaches back three steps.

Solution (from Katie Stanzel)

Theorem. *Let $a_1 = a_2 = a_3 = 1$ and define $a_n = a_{n\text{-}1} + a_{n\text{-}2} + a_{n\text{-}3}$ for each natural number $n \geq 4$. Prove that $a_n \leq 2^{n-2}$ for each natural number $n \geq 2$.*

Proof. We will prove this theorem by strong induction.

Base Case: We aim to show that $a_n \leq 2^{n-2}$ is true for $n = 2, 3, 4$. Observe,

$$\begin{aligned}
\mathbf{n = 2}\\
a_2 &\leq 2^{2-2}\\
1 &\leq 1.\\
\mathbf{n = 3}\\
a_3 &\leq 2^{3-2}\\
1 &\leq 2.\\
\mathbf{n = 4}\\
a_4 &\leq 2^{4-2}\\
1+1+1 &\leq 4\\
3 &\leq 4.
\end{aligned}$$

Thus, $a_{\text{n}} \leq 2^{n-2}$ is true for $n = 2, 3, 4$.

Strong Induction: For all $n \leq k$, where $k \in \mathbb{N}$, we may assume $a_{\text{n}} \leq 2^{n-2}$. We aim to show that $a_{\text{k+1}} \leq 2^{k-1}$. Observe,

$$\begin{aligned}
&a_{\text{k+1}} \leq a_{\text{k}} + a_{\text{k-1}} + a_{\text{k-2}}\\
&\leq 2^{k-2} + 2^{k-3} + 2^{k-4}\\
&\leq 2^k(2^{-2} + 2^{-3} + 2^{-4})\\
&\leq 2^k(\frac{1}{4} + \frac{1}{8} + \frac{1}{16})\\
&\leq 2^k(\frac{7}{16})\\
&\leq 2^k(\frac{1}{2})\\
&\leq 2^{k-1}
\end{aligned}$$

Therefore, it is true that $a_{\text{n}} \leq 2^{n-2}$ for each natural number $n \geq 2$.

□

Problem 10

Prove that $(A \cap B) - C = (A - C) \cap (B - C)$ for all sets A, B, and C.

Common Feedback

- Break this proof into two parts: $(A \cap B) - C \subseteq (A - C) \cap (B - C)$ and $(A - C) \cap (B - C) \subseteq (A \cap B) - C$. Alternatively, you can use set identities, in which case you establishing equality throughout the proof.

Solution (from Jessica Belfiore)

Proposition. *Prove that* $(A \cap B) - C = (A - C) \cap (B - C)$ *for all sets* A, B, *and* C.

Proof. Case 1: First we show $(A \cap B) - C \subseteq (A - C) \cap (B - C)$. Choose $x \in (A \cap B) - C$. If follows that, $x \in A$ and $x \in B$ but $x \notin C$. Since $x \notin C$, we are left with $x \in A$ and $x \in B$. By the definition of difference of sets, we know that $(A - C) \cap (B - C)$ says that $x \in A$ and $x \notin C$ and $x \in B$ and $x \notin C$. Therefore, both sides are left with $x \in A$ and $x \in B$. So, $(A \cap B) - C \subseteq (A - C) \cap (B - C)$.

Case 2: Show $(A - C) \cap (B - C) \subseteq (A \cap B) - C$. Choose $x \in (A - C) \cap (B - C)$. It follows that, $x \in A$ and $x \notin C$ and $x \in B$ and $x \notin C$. Since $x \notin C$, we are left with $x \in A$ and $x \in B$. By the definition of difference of sets, we know that $(A \cap B) - C$ says that $x \in A$ and B and $x \notin C$. Therefore, both sides are left with $x \in A$ and $x \in B$. So, $(A - C) \cap (B - C) \subseteq (A \cap B) - C$. □

Problem 11

Decide whether each of the following functions is injective and/or surjective. Justify your claims.

- $f : \mathbb{Z} \to \mathbb{Z}$
  $f(n) = 3n + 1$
- $g : \mathbb{R} \to (0, 1]$
  $g(x) = e^{-x^2}$

Common Feedback

- Use the formal definitions of injective and surjective in these proofs.
- Be careful to argue that any values you define actually belong to the domain or codomain, as appropriate. In this example, $\sqrt{-\ln y}$ is not obviously real until you look closely at the codomain.

Solution (from Austin Mohr)

The function f is an injection:

$$\begin{aligned} f(n_1) &= f(n_2) \\ 3n_1 + 1 &= 3n_2 + 1 \\ 3n_1 &= 3n_2 \\ n_1 &= n_2 \end{aligned}$$

It is not a surjection, however. Observe, for example, that $f(0) = 1$ and $f(1) = 4$. Since f is strictly increasing, it will never have 2 or 3 as outputs.

The function g is not an injection. Observe, for example, that $g(1) = g(-1) = e^{-1}$. It is a surjection, however. To see this, let $y \in (0, 1]$ be given and consider $x = \sqrt{-\ln y}$. Note that x is a real number, since $-\ln y$ is non-negative for $y \in (0, 1]$. Now,

$$\begin{aligned} g(x) &= e^{-(\sqrt{-\ln y})^2} \\ &= e^{--\ln y} \\ &= e^{\ln y} \\ &= y. \end{aligned}$$