PROOF PORTFOLIO - SPRING 2023

BERNICE YUAN

1. DIRECT PROOF

The sum of the squares of two consecutive integers is odd.

Proof. Let x and y be two consecutive integers. By the definition of consecutive integers, we know that $y = x + 1$. We can substitute this into the equation $x^2 + y^2$, which gives us

$$x^2 + (x + 1)^2 = 2x^2 + 2x + 1 = 2(x^2 + x) + 1$$

Since $x \in \mathbb{Z}$, $x^2 + x \in \mathbb{Z}$. Thus, the sum of the squares of x and y is always an odd number. So, the statement proved. $\square$

Date: April 26, 2023.

2. CONTRAPOSITIVE PROOF

Let $a, b \in \mathbb{Z}$. Prove that if $a^2(b^2 - 2b)$ is odd, then a and b are odd.

Proof. We will prove by the contrapositive:
If either a or b is even, then $a^2(b^2 - 2b)$ is even.
Suppose $a, b \in \mathbb{Z}$, and a or b is even.
First, assume that a is even. Then we can write $a = 2k$ for some $k \in \mathbb{Z}$. Substituting this into $a^2(b^2 - 2b)$, we get:

$$a^2(b^2 - 2b) = (2k)^2(b^2 - 2b) = 4k^2(b^2 - 2b) = 2(2k^2)(b^2 - 2b)$$

Since $(2k^2)(b^2 - 2b) \in \mathbb{Z}$, by definition of even, $a^2(b^2 - 2b)$ is even.
Next, assume that b is even. Then we can write $b = 2m$ for some $m \in \mathbb{Z}$. Substituting this into $a^2(b^2 - 2b)$, we get:

$$a^2(b^2 - 2b) = a^2(4m^2 - 4m) = 2(a^2)(2m^2 - 2m)$$

Since $(a^2)(2m^2 - 2m) \in \mathbb{Z}$, again, by definition of even, $a^2(b^2 - 2b)$ is even.
Therefore, if a or b is even, then $a^2(b^2 - 2b)$ is even. This completes the proof by contrapositive, which shows that if $a^2(b^2 - 2b)$ is odd, then a and b are odd. $\square$

Prove that any real-valued solution to $x^3 + x = 1$ must be irrational.

Proof. Assume, for the sake of contradiction, that there exists a real-valued solution of $x^3+x = 1$ that is rational. Then there exists integers p and q with $q \neq 0$, such that $x = \frac{p}{q}$ and $\frac{p^3}{q^3} + \frac{p}{q} = 1$. We may assume that p, q have no common factors. Times both sides with q^3, we have $p^3 + q^2p = q^3$.
Case (a): Suppose p, q are both even integers;
Since p and q are both even, p and q are both divisible by 2, this case is impossible.
Case (b): Suppose p, q are both odd integers;
Let $p = 2m + 1, q = 2n + 1$ for some $m, n \in \mathbb{Z}$. Then

$$\begin{aligned} p^3 + q^2p &= (2m + 1)^3 + (2n + 1)^2(2m + 1) \\ &= 2(2m + 1)(2m^2 + 2m + 2n^2 + 2n + 1) \end{aligned}$$

$$\begin{aligned} q^3 &= (2n + 1)^3 \\ &= 8n^3 + 12n^2 + 6n + 1 \\ &= 2(4n^3 + 6n^2 + 3n) + 1 \end{aligned}$$

Since $(2m+1)(2m^2+2m+2n^2+2n+1) \in \mathbb{Z}$ and $4n^3+6n^2+3n \in \mathbb{Z}$, $p^3 + q^2p$ is even and q^3 is odd. Therefore, we have a contradiction.
Case (c): Suppose p is even and q is odd;
Let $p = 2m, q = 2n + 1$ for some $m, n \in \mathbb{Z}$. Then

$$\begin{aligned} p^3 + q^2p &= (2m)^3 + (2n + 1)^2(2m) \\ &= 2(4m^3 + 4mn^2 + 4mn + m) \end{aligned}$$

$$\begin{aligned} q^3 &= (2n + 1)^3 \\ &= 2(4n^3 + 6n^2 + 3n) + 1 \end{aligned}$$

Since $4m^3 + 4mn^2 + 4mn + m \in \mathbb{Z}$ and $4n^3 + 6n^2 + 3n \in \mathbb{Z}$, $p^3 + q^2p$ is even and q^3 is odd. Therefore, we have a contradiction.
Case (d): Suppose p is odd and q is even.
Let $p = 2m + 1, q = 2n$ for some $m, n \in \mathbb{Z}$. Then

$$\begin{aligned} p^3 + q^2p &= (2m + 1)^3 + (2n)^2(2m + 1) \\ &= 2(4m^3 + 6m^2 + 3m + 4mn^2 + 2n^2) + 1 \end{aligned}$$

$$
\begin{aligned}
q^3 &= (2n)^3 \\
&= 2(4n^3)
\end{aligned}
$$

Since $4m^3 + 6m^2 + 3m + 2mn^2 + 2n^2 \in \mathbb{Z}$ and $4n^3 \in \mathbb{Z}$, $p^3 + q^2 p$ is odd and q^3 is even. Therefore, we have a contradiction.

We have contradictions for every case, so the real-valued solution to $x^3 + x = 1$ must be irrational. $\square$

4. If and only if (equivalence) proof

Let A, B, and C be sets. Prove that $(A \cap B) \cup C = A \cap (B \cup C)$ if and only if $C \subseteq A$.

Proof. Suppose A, B, C are sets.
($\Rightarrow$) Assume that $(A \cap B) \cup C = A \cap (B \cup C)$, we want to show that $C \subseteq A$. Take an element $x \in C$. Since $x \in C$, we know that $x \in (A \cap B) \cup C$. Since $(A \cap B) \cup C = A \cap (B \cup C)$, we know that $x \in A \cap (B \cup C)$. This means $x \in A$ and $x \in (B \cup C)$. So, for every element $x \in C$, we have $x \in A$, and hence $C \subseteq A$.

($\Leftarrow$) Assume that $C \subseteq A$. Now, let's show that $(A \cap B) \cup C = A \cap (B \cup C)$.

We will prove this by showing the following two inclusions:

1. $(A \cap B) \cup C \subseteq A \cap (B \cup C)$
2. $A \cap (B \cup C) \subseteq (A \cap B) \cup C$

1. Let $x \in (A \cap B) \cup C$. Then, either $x \in (A \cap B)$ or $x \in C$.

If $x \in (A \cap B)$, then $x \in A$ and $x \in B$. Since $x \in A$, we have $x \in A \cap (B \cup C)$ because $x \in B \cup C$ (as $x \in B$). If $x \in C$, then $x \in A$ (since $C \subseteq A$) and $x \in B \cup C$ (since $x \in C$). So, $x \in A \cap (B \cup C)$. In both cases, we have $x \in A \cap (B \cup C)$. Thus, $(A \cap B) \cup C \subseteq A \cap (B \cup C)$.

2. Let $x \in A \cap (B \cup C)$. Then, $x \in A$ and $x \in (B \cup C)$. If $x \in B$, then $x \in A$ and $x \in B$, so $x \in A \cap B$. Thus, $x \in (A \cap B) \cup C$. If $x \in C$, then $x \in (A \cap B) \cup C$ by definition of union.

In both cases, we have $x \in (A \cap B) \cup C$. Thus, $A \cap (B \cup C) \subseteq (A \cap B) \cup C$.
Therefore, we can conclude that $(A \cap B) \cup C = A \cap (B \cup C)$ if and only if $C \subseteq A$. $\square$

5. A PROOF INVOLVING SETS

Let A, B sets inside a fixed universe U. Prove that $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$.

Proof. Let $x \in \overline{A \cap B}$, by definition of complement, $x \notin (A \cap B)$. Then, $x \notin A$ or $x \notin B$.
Without loss of generality, we assume $x \notin A$, then $x \in \overline{A}$. Since $\overline{A} \subseteq \overline{A} \cup \overline{B}$, $x \in \overline{A} \cup \overline{B}$. $\square$

6. An induction proof

Prove the following by induction: For all $n \in \mathbb{N}$
$1 + 3 + 5 + ... + (2n - 1) = n^2$

Proof. Let $n \in \mathbb{N}$, Let $P(n)$ be the statement that

$$1 + 3 + 5 + ... + (2n - 1) = n^2$$

Base case: Suppose $n = 1$. Take note that $1 = 1^2$. So $P(1)$ is true.
Inductive step: Now suppose that $P(k)$ is true for some $k \geq 1$, so that

$$1 + 3 + 5 + ... + (2k - 1) = k^2$$

We'll show that $P(k + 1)$ is true.
We want to show that

$$1 + 3 + 5 + ... + (2k - 1) + (2(k + 1) - 1) = (k + 1)^2$$

Adding $(2(k+1)-1)$ to both sides of the induction hypothesis, we get:

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

So $P(k + 1)$ is true. We've shown that $P(1)$ is true and $\forall k \geq 1$, $P(k) \Rightarrow P(k+1)$. So by the principle of mathematical induction, $P(n)$ holds for $n \in \mathbb{N}$. $\square$

7. PROOF A RELATION IS AN EQUIVALENCE RELATION

Consider the relation R on $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ defined by $(a, b)R(c, d)$ if $a^b = c^d$. Show that R is an equivalence equation.

Proof. Let the relation R on $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ defined by $(a, b)R(c, d)$ if $a^b = c^d$. We will show that R is an equivalence equation.
Reflexive: Let $(a, b) \in \mathbb{N}^2$, since $a^b = a^b$, R is reflexive.
Symmetric: Let $(a, b), (c, d) \in \mathbb{N}^2$, such that $(a, b)R(c, d)$. So we have $a^b = c^d$. Since $c^d = a^b$, we have $(c, d)R(a, b)$. Thus it's symmetric.
Transitive: Let $(a, b), (c, d), (e, f) \in \mathbb{N}^2$ such that $(a, b)R(c, d)$, $(c, d)R(e, f)$. Then we have $a^b = c^d, c^d = e^f$. Hence we have the equation that $a^b = c^d = e^f$. Since $a^b = e^f$, $(a, b)R(e, f)$. So it's transitive.
As we've shown that R is reflexive, symmetric, and transitive, R is an equivalence relation. $\square$

8. INJECTIVITY OR SURJECTIVITY OF A FUNCTION

Let A, B and C be sets, and let $f : A \to B, g : B \to C$ be functions. Prove or disprove each of the following:

(1) If $g \circ f$ is an injection, then g is an injection.

Disprove. Let $A = \{1\}, B = \{1, 2\}, C = \{1\}$, and $f : A \to B$ by $f(1) = 1$ and $g : B \to C$ by $g(1) = g(2) = 1$. Then $g \circ f : A \to C$ is defined by $(g \circ f)(1) = 1$. This map is a bijection from $A = \{1\}$ to $C = \{1\}$, so is injective and surjective. However, g is not injective, since $g(1) = g(2) = 1$. $\square$

(2) If $g \circ f$ is a surjection, then f is a surjection.

Disprove. Using the same example in (1), $g \circ f$ is surjective, but f is not surjective since $2 \notin f(A) = \{1\}$. $\square$

(3) If $g \circ f$ is a surjection, then g is a surjection.

Proof. Suppose $g \circ f$ is surjective. Let $c \in C$. Then since $g \circ f$ is surjective, $\exists a \in A$ such that $(gf)(a) = g(f(a)) = c$. Therefore if we let $b = f(a) \in B$, then $g(b) = c$. Thus g is surjective. $\square$

9. AN EPSILON-DELTA PROOF

Prove using the $\epsilon - \delta$ definition of continuity that $f(x) = 2x^2 + 1$ is continuous at $x = 2$.

Proof. We want to show that $\forall \epsilon > 0$, $\exists \delta > 0$ such that if $|x-2| < \delta$, then $|f(x) - f(2)| < \epsilon$.
Let $\epsilon > 0$ be given: choose $\delta = min\{2, \frac{\epsilon}{12}\}$. Take note that $\delta \leq 2$ and $\delta \leq \frac{\epsilon}{12}$. Suppose $x \in R$ such that $|x-2| < \delta$. Note that since $\delta \leq 2$, we have $|x-2| < \delta \leq 2$. So $-2 < x-2 < 2$, which is $0 < x < 4$. Thus, $2 < x+2 < 6$, or $|x+2| < 6$.
Then

$$\begin{aligned}
|f(x) - f(2)| &= |2x^2 + 1 - (2 \times 2^2 + 1)| \\
&= |2x^2 - 8| \\
&= 2|x^2 - 4| \\
&= 2|x+2||x-2| \\
&< 12|x-2| \\
&< 12\delta \\
&= 12 \times min\{2, \frac{\epsilon}{12}\} \\
&\leq 12 \times \frac{\epsilon}{12} \\
&= \epsilon
\end{aligned}$$

Since $\epsilon > 0$ is arbitrary, we've shown that $\forall \epsilon > 0, \exists \delta = min\{2, \frac{\epsilon}{12}\}$ such that if $|x-2| < \delta$, then $|f(x) - f(2)| < \epsilon$. So f is continuous at $x = 2$. ∎

Given any 4 integers, there is a pair of numbers whose difference is divisible by 3.

Proof. Let set S be a set with any 4 integers.
We want to show that $\exists a, b \in S$ such that $a \equiv b \ mod\ 3$.
$\forall s \in S$, we can write $s = 3k + r$ where $k \in \mathbb{Z}$ and $r \in \{0, 1, 2\}$. There are exactly 3 possibilities for r. However there are 4 integers in S. So by the Pigeonhole Principle, $\exists a, b \in S$ such that $a = 3k + r, b = 3l + r$ where $k, l \in \mathbb{Z}$ and $r \in \{0, 1, 2\}$. Then $a - b = 3k + r - 3l - r = 3(k - l)$. Since $(k - l) \in \mathbb{Z}$, $3|(a - b)$. So $a \equiv b \ mod\ 3$. $\square$