Solutions for Abstract Algebra: Theory and Applications by Tom Judson

For the 2022 Annual Edition

Justin Hilyard

Contents

1 Preliminaries

1.

Suppose that

$A = \{x : x \in \mathbb{N} \text{ and } x \text{ is even}\}$,
$B = \{x : x \in \mathbb{N} \text{ and } x \text{ is prime}\}$,
$C = \{x : x \in \mathbb{N} \text{ and } x \text{ is a multiple of } 5\}$.

Describe each of the following sets.

(a) $A \cap B = \{2\}$.

(b) $B \cap C = \{5\}$.

(c) $A \cup B = \{x : x \in \mathbb{N} \text{ and } x \text{ is even or } x \text{ is prime}\}$.

(d) $A \cap (B \cup C) = \{x : x \in \mathbb{N} \text{ and } x = 2 \text{ or } x \text{ is a multiple of } 10\}$.

2.

If $A = \{a, b, c\}$, $B = \{1, 2, 3\}$, $C = \{x\}$, and $D = \emptyset$, list all of the elements in each of the following sets.

(a) $A \times B = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3), (c, 1), (c, 2), (c, 3)\}$.

(b) $B \times C = \{(1, x), (2, x), (3, x)\}$.

(c) $A \times B \times C = \{(a, 1, x), (a, 2, x), (a, 3, x), (b, 1, x), (b, 2, x), (b, 3, x),$
$(c, 1, x), (c, 2, x), (c, 3, x)\}$.

(d) $A \times D = \emptyset$.

3.

Find an example of two nonempty sets A and B for which $A \times B = B \times A$.

For any nonempty set S, let $A = B = S$.

4.

Prove $A \cup \emptyset = A$ and $A \cap \emptyset = \emptyset$.

$$\begin{aligned} A \cup \emptyset &= \{x : x \in A \vee x \in \emptyset\} \\ &= \{x : x \in A\} \\ &= A \end{aligned}$$

$$\begin{aligned} A \cap \emptyset &= \{x : x \in A \wedge x \in \emptyset\} \\ &= \{\} \\ &= \emptyset \end{aligned}$$

□

5.

Prove $A \cup B = B \cup A$ and $A \cap B = B \cap A$.

$$\begin{aligned} A \cup B &= \{x : x \in A \vee x \in B\} \\ &= \{x : x \in B \vee x \in A\} \\ &= B \cup A \end{aligned}$$

$$\begin{aligned} A \cap B &= \{x : x \in A \wedge x \in B\} \\ &= \{x : x \in B \wedge x \in A\} \\ &= B \cap A \end{aligned}$$

□

6.

Prove $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

$$\begin{aligned} A \cup (B \cap C) &= \{x : x \in A \vee x \in B \cap C\} \\ &= \{x : x \in A \vee (x \in B \wedge x \in C)\} \\ &= \{x : (x \in A \vee x \in B) \wedge (x \in A \vee x \in C)\} \\ &= \{x : x \in (A \cup B) \vee x \in (A \cup C)\} \\ &= \{x : x \in (A \cup B) \cap (A \cup C)\} \\ &= (A \cup B) \cap (A \cup C) \end{aligned}$$

□

7.

Prove $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

$$\begin{aligned} A \cap (B \cup C) &= \{x : x \in A \wedge x \in B \cup C\} \\ &= \{x : x \in A \wedge (x \in B \vee x \in C)\} \\ &= \{x : (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)\} \\ &= \{x : x \in (A \cap B) \wedge x \in (A \cap C)\} \\ &= \{x : x \in (A \cap B) \cup (A \cap C)\} \\ &= (A \cap B) \cup (A \cap C) \end{aligned}$$

□

8.

Prove $A \subset B$ if and only if $A \cap B = A$.

By definition

$$A \subset B \iff (x \in A \implies x \in B).$$

We know that $x \in B$ implies $x \in A \cap B$, and so by transitivity of implication,

$$A \subset B \iff (x \in A \implies x \in A \cap B),$$

or in other words,

$$A \subset B \iff A \subset A \cap B.$$

As we trivially have that $A \cap B \subset A$, therefore

$$A \subset B \iff A \cap B = A.$$

□

9.

Prove $(A \cap B)' = A' \cup B'$.

$$\begin{aligned} (A \cap B)' &= \{x : x \notin A \cap B\} \\ &= \{x : x \notin A \vee x \notin B\} \\ &= A' \cup B' \end{aligned}$$

□

10.

Prove $A \cup B = (A \cap B) \cup (A \setminus B) \cup (B \setminus A)$.

If $x \in A \cup B$, then either x is in both A and B, x is only in A, or x is only in B.

Therefore

$$\begin{aligned} A \cup B &= \{x : x \in A \cup B\} \\ &= \{x : x \in A \cap B \vee x \in A \setminus B \vee x \in B \setminus A\} \\ &= (A \cap B) \cup (A \setminus B) \cup (B \setminus A). \end{aligned}$$ □

11.

Prove $(A \cup B) \times C = (A \times C) \cup (B \times C)$.

$$\begin{aligned} (A \cup B) \times C &= \{(x, y) : x \in A \cup B \wedge y \in C\} \\ &= \{(x, y) : (x \in A \vee x \in B) \wedge y \in C\} \\ &= \{(x, y) : (x \in A \wedge y \in C) \vee (x \in B \wedge y \in C)\} \\ &= (A \times C) \cup (B \times C) \end{aligned}$$ □

12.

Prove $(A \cap B) \setminus B = \emptyset$.

$$\begin{aligned} (A \cap B) \setminus B &= \{x : x \in (A \cap B) \wedge x \notin B\} \\ &= \{x : x \in A \wedge x \in B \wedge x \notin B\} \\ &= \{\} \\ &= \emptyset \end{aligned}$$ □

13.

Prove $(A \cup B) \setminus B = A \setminus B$.

$$\begin{aligned} (A \cup B) \setminus B &= \{x : x \in (A \cup B) \wedge x \notin B\} \\ &= \{x : (x \in A \vee x \in B) \wedge x \notin B\} \\ &= \{x : (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin B)\} \\ &= \{x : x \in A \wedge x \notin B\} \\ &= A \setminus B \end{aligned}$$ □

14.

Prove $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

$$\begin{aligned} A \setminus (B \cup C) &= \{x : x \in A \wedge x \notin (B \cup C)\} \\ &= \{x : x \in A \wedge (x \notin B \wedge x \notin C)\} \\ &= \{x : (x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C)\} \\ &= (A \setminus B) \cap (A \setminus C) \end{aligned}$$ □

15.

Prove $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$.

$$\begin{aligned} (A \cap B) \setminus (A \cap C) &= \{x : x \in A \cap B \wedge x \notin A \cap C\} \\ &= \{x : (x \in A \wedge x \in B) \wedge (x \notin A \wedge x \notin C)\} \\ &= \{x : (x \in A \wedge x \in B \wedge x \notin A) \wedge (x \in A \wedge x \in B \wedge x \notin C)\} \\ &= \{x : x \in A \wedge x \in B \wedge x \notin C\} \\ &= \{x : x \in A \wedge x \in B \setminus C\} \\ &= A \cap (B \setminus C) \end{aligned}$$ □

16.

Prove $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$.

$$\begin{aligned} (A \setminus B) \cup (B \setminus A) &= \{x : x \in (A \setminus B) \vee x \in (B \setminus A)\} \\ &= \{x : (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\} \\ &= \{x : (x \in A \vee x \in B) \wedge (x \notin B \vee x \in B) \\ &\qquad \wedge (x \in A \vee x \notin A) \wedge (x \notin B \vee x \notin A)\} \\ &= \{x : (x \in A \vee x \in B) \wedge (x \notin B \vee x \notin A)\} \\ &= \{x : (x \in A \vee x \in B) \wedge (x \in B \wedge x \in A)'\} \\ &= \{x : x \in A \cup B \wedge x \notin A \cap B\} \\ &= (A \cup B) \setminus (A \cap B) \end{aligned}$$ □

17.

Which of the following relations $f : \mathbb{Q} \to \mathbb{Q}$ define a mapping? In each case, supply a reason why f is or is not a mapping.

(a) $f(p/q) = \frac{p+1}{p-2}$

No. $\frac{1}{3} = \frac{2}{6}$, but $f(1/3) = 2 \neq \frac{3}{4} = f(2/6)$.

(b) $f(p/q) = \frac{3p}{3q}$

Yes. For any fraction $\frac{p}{q} \in \mathbb{Q}$, the value of $f(p/q)$ reduces to simply $\frac{p}{q}$, and therefore f is the identity mapping.

(c) $f(p/q) = \frac{p+q}{q^2}$

No. $\frac{1}{3} = \frac{2}{6}$, but $f(1/3) = \frac{4}{9} \neq \frac{2}{9} = f(2/6)$.

(d) $f(p/q) = \frac{3p^2}{7q^2} - \frac{p}{q}$

Yes. Let $x = \frac{p}{q}$. Then $f(x) = \frac{3}{7}x^2 - x$, and so it follows that $f(p/q)$ isn't dependent on the representation of p/q.

18.

Determine which of the following functions are one-to-one and which are onto. If the function is not onto, determine its range.

(a) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = e^x$

Both one-to-one and onto.

(b) $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = n^2 + 3$

Neither. This function is not one-to-one —$f(n) = f(-n)$ —and the range of this function is $\{3, 4, 7, 12, \dots\} \subset \mathbb{N}$.

(c) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = \sin x$

Neither. This function is not one-to-one —$f(x) = f(x + 2\pi)$ —and the range of this function is $[-1, 1]$.

(d) $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = n^2$

Neither. This function is not one-to-one —$f(n) = f(-n)$ —and the range of this function is $\{0, 1, 4, 9, \dots\} \subset \mathbb{N}$.

19.

Let $f : A \to B$ and $g : B \to C$ be invertible mappings; that is, mappings such that f^{-1} and g^{-1} exist. Show that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Take any $a \in A$ and let $b \in B$, $c \in C$ be such that $f(a) = b$ and $g(b) = c$, or equivalently that $(g \circ f)(a) = c$. It thus follows that $(g \circ f)^{-1}(c) = a$.

Now, evaluate $(f^{-1} \circ g^{-1})(c)$. By our previous definitions, we have $f^{-1}(g^{-1}(c)) = f^{-1}(b) = a$. □

20.

Define a function $f : \mathbb{N} \to \mathbb{N}$ that is one-to-one but not onto.

$$f(n) = n + 1$$

For any two $m, n \in \mathbb{N}$, $m \neq n$ implies $m + 1 \neq n + 1$. However, there is no $n \in \mathbb{N}$ such that $f(n) = 1$.

21.

Prove the relation defined on $\mathbb{R}^2$ by $(x_1, y_1) \sim (x_2, y_2)$ if $x_1^2 + y_1^2 = x_2^2 + y_2^2$ is an equivalence relation.

Reflexivity: For any element $(x, y) \in \mathbb{R}^2$, $x^2 + y^2 = x^2 + y^2$, and so $(x, y) \sim (x, y)$.

Symmetry: For any two elements $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$ such that $(x_1, y_1) \sim (x_2, y_2)$, equivalently $x_1^2 + y_1^2 = x_2^2 + y_2^2$, then clearly we have $x_2^2 + y_2^2 = x_1^2 + y_1^2$, and so $(x_2, y_2) \sim (x_1, y_1)$.

Transitivity: For any three elements $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathbb{R}^2$ such that $(x_1, y_1) \sim (x_2, y_2)$ and $(x_2, y_2) \sim (x_3, y_3)$, equivalently $x_1^2 + y_!^2 = x_2^2 + y_2^2$ and $x_2^2 + y_2^2 = x_3^2 + y_3^2$, then clearly we have $x_1^2 + y_!^2 = x_3^2 + y_3^2$, and so $(x_1, y_1) \sim (x_3, y_3)$. □

22.

Let $f : A \to B$ and $g : B \to C$ be maps.

(a) If f and g are both one-to-one functions, show that $g \circ f$ is one-to-one.

For $a_n \in A$, let $b_n \in B$, $c_n \in C$ be such that $f(a_n) = b_n$ and $g(b_n) = c_n$). As f is a one-to-one function, $a_1 \neq a_2$ implies that $b_1 \neq b_2$. Similarly, as g is a one-to-one function, $b_1 \neq b_2$ implies that $c_1 \neq c_2$. Therefore, $a_1 \neq a_2$ implies $c_1 \neq c_2$, and so $g \circ f$ is also one-to-one.

(b) If $g \circ f$ is onto, show that g is onto.

Given that $g \circ f$ is onto, then for every $c_n \in C$ there exists some $a_n \in A$ such that $(g \circ f)(a_n) = c_n$. For every $c_n \in C$, then, it is clear that there exists $b_n \in B = f(a_n)$ such that $g(b_n) = c_n$.

(c) If $g \circ f$ is one-to-one, show that f is one-to-one.

For $a_n \in A$, let $b_n \in B$, $c_n \in C$ be such that $f(a_n) = b_n$ and $g(b_n) = c_n$). Assume that f is not one-to-one. Then there exists some $a_1, a_2 \in A$ such that $a_1 \neq a_2$ but $b_1 = b_2 = b$. As $g \circ f$ is one-to-one, we know that we must have that $c_1 \neq c_2$. However, this implies that $g(b)$ maps to distinct values c_1 and c_2, which is impossible as we know that g is a mapping. Therefore, f is one-to-one.

(d) If $g \circ f$ is one-to-one and f is onto, show that g is one-to-one.

Let $b_1, b_2 \in B$ such that $b_1 \neq b_2$. Given that f is onto and (by (c)) one-to one, we must have that for every b_n, there exists some unique a_n such that $f(a_n) = b_n$, and so we know that $a_1 \neq a_2$ must both also exist in A. As $g \circ f$ is one-to-one, we have that $a_1 \neq a_2$ implies $c_1 \neq c_2$. Therefore, $b_1 \neq b_2$ also implies that $c_1 \neq c_2$, and so g must be one-to-one.

(e) If $g \circ f$ is onto and g is one-to-one, show that f is onto.

Given that g is one-to-one and (by (b)) onto, we know that for all $b_n \in B$ there exists a unique $c_n \in C$ such that $g(b_n) = c_n$. As $(g \circ f)$ is onto, it follows that for all $c_n \in C$ there exists at least one a_n such that $(g \circ f)(a_n) = c_n$. It then follows directly that for all $b_n \in B$ there exists at least one a_n such that $f(a_n) = b_n$, and so f is onto.

23.

Define a function on the real numbers by

$$f(x) = \frac{x+1}{x-1}.$$

What are the domain and range of f? What is the inverse of f? Compute $f \circ f^{-1}$ and $f^{-1} \circ f$.

Domain: $\mathbb{R} \setminus \{1\}$

Range: $\mathbb{R} \setminus \{1\}$

$$\begin{aligned} f^{-1}: \quad y = \frac{x+1}{x-1} &\iff y(x-1) = x+1 \\ &\iff yx - y = x+1 \\ &\iff yx - x = y+1 \\ &\iff x(y-1) = y+1 \\ &\iff x = \frac{y+1}{y-1} \\ &\iff f^{-1}(x) = f(x) \end{aligned}$$

$$\begin{aligned} f \circ f^{-1} : (f \circ f^{-1})(x) &= \frac{\frac{x+1}{x-1} + 1}{\frac{x+1}{x-1} - 1} \\ &= \frac{\frac{x+1}{x-1} + \frac{x-1}{x-1}}{\frac{x+1}{x-1} - \frac{x-1}{x-1}} \\ &= \frac{\frac{2x}{x-1}}{\frac{2}{x-1}} \\ &= \frac{2x}{x-1} \cdot \frac{x-1}{2} \\ &= x \end{aligned}$$

$f^{-1} \circ f$: As $f = f^{-1}$, this is the same result as $f \circ f^{-1}$.

24.

Let $f : X \to Y$ be a map with $A_1, A_2 \subset X$ and $B_1, B_2 \subset Y$.

(a) Prove $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

Let $y \in f(A_1 \cup A_2)$. By definition, this means there is some $x \in A_1 \cup A_2$ where $f(x) = y$. It must be the case that $x \in A_1 \vee x \in A_2$, and so $f(x) \in f(A_1) \vee f(x) \in f(A_2)$. Therefore $f(x) \in f(A_1) \cup f(A_2)$, and so $f(A_1 \cup A_2) \subset f(A_1) \cup f(A_2)$.

The opposite direction follows similarly. □

(b) Prove $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$. Give an example in which equality fails.

Let $y \in f(A_1 \cap A_2)$. By definition, this means there is some $x \in A_1 \cap A_2$ where $f(x) = y$. It must be the case that $x \in A_1 \wedge x \in A_2$, and so $f(x) \in f(A_1) \wedge f(x) \in f(A_2)$. Therefore $f(x) \in f(A_1) \cap f(A_2)$, and so $f(A_1 \cup A_2) \subset f(A_1) \cup f(A_2)$.

Now, let $y \in f(A_1) \cap f(A_2)$. Therefore, $y \in f(A_1) \wedge y \in f(A_2)$. The proof of containment in the opposite direction breaks down here, however: this only establishes that there must exist some $x_1, x_2 \in X$ such that $x_1 \in A_1 \wedge x_2 \in A_2$, with no guarantee that $x_1 = x_2$ or that either element is in $A_1 \cap A_2$.

For example, let $f(x) = x^2$ for $f : \mathbb{Z} \to \mathbb{Z}$, with $A_1 = \mathbb{Z}^+$ and $A_2 = \mathbb{Z}^-$. For any $m \in \mathbb{Z}^+$ and $y = m^2$, it is certainly the case that $y \in f(\mathbb{Z}^+) \cap f(\mathbb{Z}^-)$, as $f(m) = y$ and $f(-m) = y$. However, $\mathbb{Z}^+ \cap \mathbb{Z}^- = \emptyset$, and so y could not possibly be an element of $f(\emptyset) = \emptyset$.

(Note that if f is one-to-one, then we do know that $f(x_1) = f(x_2)$ implies $x_1 = x_2$, and so we can achieve equality of sets.) □

(c) Prove $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$, where $f^{-1}(B) = \{x \in X : f(x) \in B\}$.

Let $x \in f^{-1}(B_1 \cup B_2)$. By definition, this means there is some $y \in B_1 \cup B_2$ where $f^{-1}(y) = x$. It must be the case that $y \in B_1 \vee y \in B_2$, and so $f^{-1}(y) \in f^{-1}(B_1) \vee f^{-1}(y) \in f^{-1}(B_2)$. Therefore $f^{-1}(y) \in f^{-1}(B_1) \cup f^{-1}(B_2)$, and so $f^{-1}(B_1 \cup B_2) \subset f^{-1}(B_1) \cup f^{-1}(B_2)$.

The opposite direction follows similarly. □

(d) Prove $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.

Let $x \in f^{-1}(B_1 \cap B_2)$. By definition, this means there is some $y \in B_1 \cap B_2$ where $f^{-1}(y) = x$. It must be the case that $y \in B_1 \wedge y \in B_2$, and so $x \in f^{-1}(B_1) \wedge x \in f^{-1}(B_2)$. Therefore $x \in f^{-1}(B_1) \cap f^{-1}(B_2)$, and so $f^{-1}(B_1 \cap B_2) \subset f^{-1}(B_1) \cap f^{-1}(B_2)$.

Now, let $x \in f^{-1}(B_1) \cap f^{-1}(B_2)$. Therefore, $x \in f^{-1}(B_1) \wedge x \in f^{-1}(B_2)$. In contrast to (b), we can continue further here: this implies that there must exist some $y_1, y_2 \in B$ such that $y_1 \in B_1 \wedge y_2 \in B_2$. However, as f is a mapping, we must have that $y_1 = y_2 = y$, and so $y \in B_1 \cap B_2$, and thus $x \in f^{-1}(B_1 \cap B_2)$. Therefore, $f^{-1}(B_1) \cap f^{-1}(B_2) \subset f^{-1}(B_1 \cap B_2)$.

Thus, $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$. □

(e) Prove $f^{-1}(Y \setminus B_1) = X \setminus f^{-1}(B_1)$.

Let $x \in f^{-1}(Y \setminus B_1)$. By definition, this means there is some $y \in Y \setminus B_1$ where $f^{-1}(y) = x$. Thus $y \in Y \wedge y \notin B_1$, and so $x \in X \wedge x \notin f^{-1}(B_1)$. Therefore $x \in X \setminus f^{-1}(B_1)$, and so $f^{-1}(Y \setminus B_1) \subset X \setminus f^{-1}(B_1)$.

The opposite direction follows similarly. □

25.

Determine whether or not the following relations are equivalence relations on the given set. If the relation is an equivalent relation, describe the partition given by it. If the relation is not an equivalence relation, state why it fails to be one.

(a) $x \sim y$ in $\mathbb{R}$ if $x \geq y$.

No. Take x and y such that $x > y$. Then $x \sim y$ but $y \nsim x$.

(b) $m \sim n$ in $\mathbb{Z}$ if $mn > 0$.

No. $0 \nsim 0$.

(c) $x \sim y$ in $\mathbb{R}$ if $|x - y| \leq 4$.

No. Take x, y, and z such that $x - y = 4$ and $y - z = 4$. Then $x \sim y$ and $y \sim z$, but $x - z = 8$ and so $x \nsim z$.

(d) $m \sim n$ in $\mathbb{Z}$ if $m \equiv n \pmod 6$.

Yes. All properties follow directly from the definition of a modulus class.

26.

Define a relation $\sim$ on $\mathbb{R}^2$ by stating that $(a, b) \sim (c, d)$ if and only if $a^2 + b^2 \leq c^2 + d^2$. Show that $\sim$ is reflexive and transitive by not symmetric.

Reflexivity: $a^2 + b^2 = a^2 + b^2 \implies a^2 + b^2 \leq a^2 + b^2 \implies (a, b) \sim (a, b)$.

Transitivity: If $a^2 + b^2 \leq c^2 + d^2$ and $c^2 + d^2 \leq e^2 + f^2$, then $a^2 + b^2 \leq e^2 + f^2$, and so $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$ implies $(a, b) \sim (e, f)$.

Symmetry: For any $(a, b), (c, d) \in \mathbb{R}^2$ such that $a^2 + b^2 < c^2 + d^2$, then $(a, b) \sim (c, d)$, but $(c, d) \nsim (a, b)$.

27.

Show that an $m \times n$ matrix gives rise to a well-defined map from $\mathbb{R}^n$ to $\mathbb{R}^m$.

For any arbitrary matrix $A \in \mathbb{R}^m \times \mathbb{R}^m$, define the function $f_A : \mathbb{R}^n \to \mathbb{R}^m$ such that $f_A(\vec{v}) = A\vec{v}$. As this multiplication can clearly be performed for every vector $\vec{v} \in \mathbb{R}^n$, giving a single unique vector in $\mathbb{R}^m$, we have that f_A is a well-defined map for all A.

28.

Find the error in the following argument by providing a counterexample. "The reflexive property is redundant in the axioms for an equivalence relation. If $x \sim y$, then $y \sim x$ by the symmetric property. Using the transitive property, we can deduce that $x \sim x$."

Let X be any set and let R be the empty relation on X; that is, the empty subset $\emptyset \subset X \times X$. Vacuously, R is both symmetric and transitive. However, for any $x \in X$, it is certainly not true that $(x, x) \in R$. Therefore, R is not reflexive.

29.

Define a relation on $\mathbb{R}^2 \setminus \{(0,0)\}$ by letting $(x_1, y_1) \sim (x_2, y_2)$ if there exists a nonzero real number λ such that $(x_1, y_1) = (\lambda x_2, \lambda y_2)$. Prove that $\sim$ defines an equivalence relation on $\mathbb{R}^2 \setminus \{(0,0)\}$. What are the corresponding equivalence classes?

Reflexivity: For any $(x, y) \in \mathbb{R}^2 \setminus \{(0,0)\}$, this is true for $\lambda = 1$.

Symmetry: For any $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2 \setminus \{(0,0)\}$ such that $(x_1, y_1) \sim (x_2, y_2)$, or equivalently $(x_1, y_1) = (\lambda x_2, \lambda y_2)$, we thus have that $(x_2, y_2) = \left(\frac{1}{\lambda} x_1, \frac{1}{\lambda} y_1\right)$, and so $(x_2, y_2) \sim (x_1, y_1)$.

Transitivity: For any three elements $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathbb{R}^2$ such that $(x_1, y_1) \sim (x_2, y_2)$ and $(x_2, y_2) \sim (x_3, y_3)$, we thus have that $(x_1, y_1) = (\lambda x_2, \lambda y_2)$ and $(x_2, y_2) = (\mu x_3, \mu y_3)$. Therefore, $(x_1, y_1) = (\lambda \mu x_3, \lambda \mu y_3)$, and so $(x_1, y_1) \sim (x_3, y_3)$.

Each of these equivalence classes defines a line on the plane that passes through the origin (modulo $(0,0)$).

2 The Integers

1.

Prove that

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

for $n \in \mathbb{N}$.

For $n = 1$, $1^2 = 1 = \frac{1 \cdot 2 \cdot 3}{6}$.
Assume that $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$. Then

$$\begin{aligned}
\sum_{k=1}^{n+1} k^2 &= (n+1)^2 + \sum_{k=1}^{n} n^2 \\
&= n^2 + 2n + 1 + \frac{n(n+1)(2n+1)}{6} \\
&= \frac{1}{6} \cdot (6n^2 + 12n + 6 + 2n^3 + 3n^2 + n) \\
&= \frac{1}{6} \cdot (2n^3 + 9n^2 + 13n + 6) \\
&= \frac{(n+1)(n+2)(2n+3)}{6}.
\end{aligned}$$

□

2.

Prove that

$$1^2 + 2^2 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$$

for $n \in \mathbb{N}$.

For $n = 1$, $1^2 = 1 = \frac{1 \cdot 4}{4}$.
Assume that $\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}$. Then

$$\begin{aligned}
\sum_{k=1}^{n+1} k^3 &= (n+1)^3 + \sum_{k=1}^{n} n^3 \\
&= n^3 + 3n^2 + 3n + 1 + \frac{n^2(n+1)^2}{4} \\
&= \frac{1}{4} \cdot (4n^3 + 12n^2 + 12n + 4 + n^4 + 2n^3 + n^2) \\
&= \frac{1}{4} \cdot (n^4 + 6n^3 + 13n^2 + 12n + 4) \\
&= \frac{(n+1)^2(n+2)^2}{4}.
\end{aligned}$$

□

3.

Prove that $n! > 2^n$ for $n \geq 4$.

For $n = 4$, $4! = 24 > 16 = 2^4$.

Assume that $n! > 2^n$. Then

$$\begin{aligned}
(n+1)! &= (n+1) \cdot n! \\
&> (n+1) \cdot 2^n \\
&> 2 \cdot 2^n \\
&= 2^{n+1}.
\end{aligned}$$

□

4.

Prove that

$$x + 4x + 7x + \cdots + (3n-2)x = \frac{n(3n-1)x}{2}$$

for $n \in \mathbb{N}$.

For $n = 1$, $x = \frac{1 \cdot 2 \cdot x}{2}$.
Assume that $\sum_{k=1}^{n}(3k-2)x = \frac{n(3n-1)x}{2}$. Then

$$\begin{aligned}
\sum_{k=1}^{n+1}(3k-2)x &= (3(n+1)-2)x + \sum_{k=1}^{n}(3k-2)x \\
&= (3n+1)x + \frac{n(3n-1)x}{2} \\
&= \frac{1}{2} \cdot (6n + 2 + 3n^2 - n)x \\
&= \frac{1}{2} \cdot (3n^2 + 5n + 2)x \\
&= \frac{(n+1)(3n+2)x}{2}. \\
&= \frac{(n+1)(3(n+1)-1)x}{2}.
\end{aligned}$$

□

5.

Prove that $10^{n+1} + 10^n + 1$ is divisible by 3 for $n \in \mathbb{N}$.

For $n = 1$, $10^1 + 10^1 + 1 = 111 = 3 \cdot 37$.

Assume that $3 \mid 10^{n+1} + 10^n + 1$, and so $10^{n+1} + 10^n + 1 = 3k$ for some $k \in \mathbb{N}$.

We then have that

$$\begin{aligned}
10^{n+2} + 10^{n+1} + 1 &= 10^{n+2} + 10^{n+1} + 10 - 9 \\
&= 10 \cdot (10^{n+1} + 10^n + 1) - 9 \\
&= 30k - 9 \\
&= 3 \cdot (10k - 3),
\end{aligned}$$

and so $3 \mid 10^{n+2} + 10^{n+1} + 1$. □

6.

Prove that $4 \cdot 10^{2n} + 9 \cdot 10^{2n-1} + 5$ is divisible by 99 for $n \in \mathbb{N}$.

For $n = 1$, $4 \cdot 10^2 + 9 \cdot 10 + 5 = 495 = 5 \cdot 99$.

Assume that $99 \mid 4 \cdot 10^{2n} + 9 \cdot 10^{2n-1} + 5$, and so $4 \cdot 10^{2n} + 9 \cdot 10^{2n-1} + 5 = 99k$ for some $k \in \mathbb{N}$.

We then have that

$$\begin{aligned} 4 \cdot 10^{2n+2} + 9 \cdot 10^{2n+1} + 5 &= 4 \cdot 10^{2n+2} + 9 \cdot 10^{2n+1} + 500 - 495 \\ &= 100 \cdot (4 \cdot 10^{2n} + 9 \cdot 10^{2n-1} + 5) - 495 \\ &= 9900k - 495 \\ &= 99 \cdot (100k - 5), \end{aligned}$$

and so $99 \mid 4 \cdot 10^{2n+2} + 9 \cdot 10^{2n+1} + 5$. □

7.

Show that

$$\sqrt[n]{a_1 a_2 \cdots a_n} \leq \frac{1}{n} \sum_{k=1}^{n} a_k.$$

Note that this is demonstrating that the geometric mean of a set of numbers is always at most equal to the arithmetic mean of that same set of numbers. This is a classic result known as the ***AM-GM inequality***.

For any collection S of n real numbers (not necessarily all distinct), G_S be the geometric mean $\prod_{a \in S} a^{\frac{1}{n}}$ of S and A_S be the arithmetic mean $\sum_{a \in S} \frac{a}{n}$ of S.
If $a = b$ for all $a, b \in S$, then it is clear that $G_S = A_S = a$. Thus, assume not. This means that there must exist $x, y \in S$ such that $x < A_S < y$.
Let S' be S, except x is replaced with $x' = A_S$ and y is replaced with $y' = x + y - A_S$. Clearly $x' + y' = x + y$, and so $A_{S'} = A_S$.
Further,

$$\begin{aligned} x' \cdot y' - xy &= A_S(x + y - A_S) - xy \\ &= -A_S^2 + xA_S + yA_S - xy \\ &= (A_S - x)(y - A_S), \end{aligned}$$

Given that both terms are positive (since $x < A_S < y$), it follows that $x' \cdot y' - xy > 0$, and so $x' \cdot y' > xy$. Thus, $G_{S'} > G_S$.

If S' is still not all equal values, repeat this operation. Each time, we replace one value not equal to A_S with A_S, and thus after at most $n-1$ repetitions, we will have a collection T consisting of n copies of A_S. As mentioned at the start of this proof, this means that $A_S = G_T$. At every repetition of this process the geometric mean strictly increased while the arithmetic mean remained constant, and so it must be the case that $A_S > G_S$.

Thus, for any such collection S, $A_S \geq G_S$, with $A_S = G_S$ only when all elements of S are equal. □

8.

Prove the Leibniz rule for $f^{(n)}(x)$, where $f^{(n)}$ is the nth derivative of f; that is, show that

$$(fg)^{(n)}(x) = \sum_{k=0}^{n} \binom{n}{k} f^{(k)}(x) g^{(n-k)}(x).$$

9.

Use induction to prove that $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$ for $n \in \mathbb{N}$.

For $n = 1$, this is clear: $1 + 2 = 3 = 2^2 - 1$.

Assume for n. Then we have that

$$\begin{aligned} 1 + 2 + 2^2 \cdots + 2^n + 2^{n+1} &= (2^{n+1} - 1) + 2^{n+1} \\ &= 2 \cdot 2^{n+1} - 1 \\ &= 2^{n+2} - 1. \end{aligned}$$

□

10.

Prove that

$$\frac{1}{2} + \frac{1}{6} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$$

for $n \in \mathbb{N}$.

For $n = 1$, this is obvious.

Assume for n. Then we have that

$$\begin{aligned}\frac{1}{2}+\frac{1}{6}+\cdots+\frac{1}{n(n+1)}+\frac{1}{(n+1)(n+2)} &= \frac{n}{n+1}+\frac{1}{(n+1)(n+2)}\\ &= \frac{n(n+2)+1}{(n+1)(n+2)}\\ &= \frac{n^2+2n+1}{(n+1)(n+2)}\\ &= \frac{(n+1)^2}{(n+1)(n+2)}\\ &= \frac{n+1}{n+2}.\end{aligned}$$

□

11.

if x is a nonnegative real number, then show that $(1+x)^n-1 \geq nx$ for $n = 0, 1, 2, \ldots$.

For $n = 0$, this is obvious.

Assume for n. Then we have that

$$\begin{aligned}(1+x)^{n+1}-1 &= (1+x)\cdot(1+x)^n-(1+x)+x\\ &= (1+x)\cdot((1+x)^n-1)+x\\ &\geq (1+x)(nx)+x\\ &= nx^2+nx+x\\ &= nx^2+(n+1)x\\ &\geq (n+1)x.\end{aligned}$$

□

12. Power Sets.

Let X be a set. Define the ***power set*** of X, denoted $\mathcal{P}(X)$, to be the set of all subsets of X. For example,

$$\mathcal{P}(\{a,b\}) = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}.$$

For every positive integer n, show that a set with exactly n elements has a power set with exactly 2^n elements.

This can be proved both inductively and directly.

12.1 Inductive proof

For $n = 0$, $X = \emptyset$, and there is only one subset of $\emptyset$: $\emptyset$ itself. Thus $\mathcal{P}(X)$ has exactly $2^0 = 1$ element.

Assume for n. Let $S = \{s_1, s_2, \ldots, s_{n+1}\}$ be any set of $n+1$ elements and $T = \{s_1, s_2, \ldots, s_n\}$. By assumption, we know that $\mathcal{P}(T)$ has 2^n elements.

We can see that $S = T \cup \{s_{n+1}\}$. Thus, every subset $T' \subset T$ corresponds to exactly two subsets in S: T' itself and $T' \cup \{s_{n+1}\}$. Therefore, $\mathcal{P}(S)$ must have twice as many elements as $\mathcal{P}(T)$, and so must have 2^{n+1} elements. □

12.2 Direct proof

For any set S with n elements, every subset $S' \subset S$ is constructed by making a choice for every element $s \in S$ whether or not to include it. Every distinct set of choices corresponds to a specific subset and vice versa. Therefore, $\mathcal{P}(S)$ has as many elements as the number of ways of making a yes/no choice for every element $s \in S$; in other words, 2^n elements. □

13.

Prove that the two principles of mathematical induction stated in Section 2.1 are equivalent.

Assume the first principle: Given some statement $S(n)$ about integers $n \in \mathbb{N}$ and some integer n_0 such that $S(n_0)$ is true, if for all integers $k \geq n_0$, $S(k)$ implies $S(k+1)$, then $S(n)$ is true for all integers $n \geq n_0$.

Let $S(n)$ be a statement such that for some integer n_0, $S(n_0), S(n_0+1), \ldots, S(k)$ implies $S(k+1)$ for all $k \geq n_0$. Specifically then, $S(k)$ implies $S(k+1)$ for all such k, and so $S(n)$ is true for all integers $n \geq n_0$. Thus the second principle is true.

Assume the second principle: Given some statement $S(n)$ about integers $n \in \mathbb{N}$ and some integer n_0 such that $S(n_0)$ is true, if for all integers $k \geq n_0$, $S(n_0), S(n_0+1), \ldots, S(k)$ implies $S(k+1)$, then $S(n)$ is true for all integers $n \geq n_0$.

Let $S(n)$ be a statement such that for some integer n_0, $S(k)$ implies $S(k+1)$ for all $k \geq n_0$. Select some particular k. We know that $S(n_0)$ implies $S(n_0+1)$, $S(n_0+1)$ implies $S(n_0+2)$, and so on up to $S(k-1)$ implies $S(k)$. Therefore if the statement is true for $S(n_0)$, it is true for all statements $S(n_0)$ through $S(k)$, and so by assumption it must be that $S(n)$ is true for all integers $n \geq n_0$. Thus the first principle is true.

Therefore, the first principle and the second principle are equivalent. □

14.

Show that the Principle of Well-Ordering for the natural numbers implies that 1 is the smallest natural number. Use this result to show that the Principle of Well-Ordering implies the Principle of Mathematical Induction; that is, show that if $S \subset \mathbb{N}$ such that $1 \in S$ and $n+1 \in S$ whenever $n \in S$, then $S = \mathbb{N}$.

15.

For each of the following pairs of numbers a and b, calculate $\gcd(a,b)$ and find integers r and s such that $\gcd(a,b) = ra + sb$.

16.

Let a and b be nonzero integers. If there exist integers r and s such that $ar + bs = 1$, show that a and b are relatively prime.

---

17. Fibonacci Numbers

The Fibonacci numbers are

$$1, 1, 2, 3, 5, 8, 13, 21, \ldots.$$

We can define them inductively by $f_1 = 1$, $f_2 = 1$, and $f_{n+2} = f_{n+1} + f_n$ for $n \in \mathbb{N}$.

(a) Prove that $f_n < 2^n$.

For $n = 1$, $1 < 2$, and for $n = 2$, $1 < 4$. (We must show two base cases, as the definition for a Fibonacci number is dependent on the previous two numbers.)

Assume for n.

$$\begin{aligned} f_{n+1} &= f_n + f_{n-1} \\ &< 2^n + 2^{n-1} \\ &< 2^{n+1} \end{aligned}$$

□

(b) Prove that $f_{n+1}f_{n-1} = f_n^2 + (-1)^n, n \geq 2$.

As a note, this result (usually phrased $f_{n+1}f_{n-1} - f_n^2 = (-1)^n$) is known as ***Cassini's identity***, or ***Simson's identity***.

The result is more straight-forward to derive starting from this form, and so the proof will proceed using it instead.

For $n = 2$, $f_3 f_1 - f_2 = 2 \cdot 1 - 1 = 1$.

Assume for n.

$$\begin{aligned} f_{n+2}f_n - f_{n+1}^2 &= (f_{n+1} + f_n)f_n - f_{n+1}^2 \\ &= f_{n+1}f_n + f_n^2 - f_{n+1}^2 \\ &= f_n^2 + f_{n+1}f_n - f_{n+1}^2 \\ &= f_n^2 - f_{n+1}(f_{n+1} - f_n) \\ &= f_n^2 - f_{n+1}f_{n-1} \\ &= f_n^2 - f_n^2 - (-1)^n \\ &= -(-1)^n \\ &= (-1)^{n+1}. \end{aligned}$$

□

(c) Prove that $f_n = \left[\left(1+\sqrt{5}\right)^n - \left(1-\sqrt{5}\right)^n\right]/2^n\sqrt{5}$.

As a note, this formula is known as ***Binet's formula***. Though it was not first derived via the following inductive proof, it is fairly easy to prove inductively.

For convenience of calculation, we rewrite this function as

$$\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right].$$

For $n = 1$, we have

$$\begin{aligned}\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^1 - \left(\frac{1-\sqrt{5}}{2}\right)^1\right] &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}\right)\\ &= \frac{1}{\sqrt{5}}\left(\frac{(1+\sqrt{5})-(1-\sqrt{5})}{2}\right)\\ &= \frac{1}{\sqrt{5}}\left(\frac{2\sqrt{5}}{2}\right)\\ &= 1.\end{aligned}$$

Now, assume Binet's formula holds for all integers from 1 to n. In this proof, we will need the interesting fact that $(1\pm\sqrt{5})/2 + 1 = \left(\left(1\pm\sqrt{5}\right)/2\right)^2$, which we will first demonstrate.

$$\begin{aligned}\left(\frac{1\pm\sqrt{5}}{2}\right)^2 &= \frac{1}{4}\left(1\pm\sqrt{5}\right)^2\\ &= \frac{1}{4}(1\pm 2\sqrt{5}+5)\\ &= \frac{6\pm 2\sqrt{5}}{4}\\ &= \frac{3\pm\sqrt{5}}{2}\\ &= \frac{1\pm\sqrt{5}}{2}+1.\end{aligned}$$

Deriving this proof is far easier starting from f_{n+1} and ending at Binet's formula for $n+1$, so we will proceed thusly.

$$\begin{aligned}
f_{n+1} &= f_n + f_{n-1} \\
&= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right] \\
&\qquad + \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\right] \\
&= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right. \\
&\qquad \left. + \left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\right] \\
&= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1+\sqrt{5}}{2}\right)^{n-1}\right. \\
&\qquad \left. - \left(\frac{1-\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\right] \\
&= \frac{1}{\sqrt{5}}\left[\left(\left[\frac{1+\sqrt{5}}{2}\right]^n + \left[\frac{1+\sqrt{5}}{2}\right]^{n-1}\right)\right. \\
&\qquad \left. - \left(\left[\frac{1-\sqrt{5}}{2}\right]^n + \left[\frac{1-\sqrt{5}}{2}\right]^{n-1}\right)\right] \\
&= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n-1}\left(\frac{1+\sqrt{5}}{2}+1\right)\right. \\
&\qquad \left. - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\left(\frac{1-\sqrt{5}}{2}+1\right)\right] \\
&= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n-1}\left(\frac{1+\sqrt{5}}{2}\right)^2\right. \\
&\qquad \left. - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\left(\frac{1-\sqrt{5}}{2}\right)^2\right] \\
&= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right].
\end{aligned}$$

□

(d) Show that $\phi = \lim_{n\to\infty} f_{n+1}/f_n = \left(\sqrt{5}+1\right)/2$. The constant ϕ is known as the ***golden ratio***.

This is relatively straightforward algebra. Define ϕ as above, and define ψ as $(1-\sqrt{5})/2$. Note that $|\psi/\phi| < 1$.

$$\begin{aligned}
\lim_{n\to\infty} \frac{f_{n+1}}{f_n} &= \lim_{n\to\infty} \frac{\left[\left(1+\sqrt{5}\right)^{n+1} - \left(1-\sqrt{5}\right)^{n+1}\right]/2^{n+1}\sqrt{5}}{\left[\left(1+\sqrt{5}\right)^{n} - \left(1-\sqrt{5}\right)^{n}\right]/2^{n}\sqrt{5}} \\
&= \lim_{n\to\infty} \frac{\phi^{n+1} - \psi^{n+1}}{\phi^n - \psi^n} \\
&= \frac{\phi^{n+1}}{\phi^n} \cdot \lim_{n\to\infty} \frac{1-(\psi/\phi)^{n+1}}{1-(\psi/\phi)^n} \\
&= \phi \cdot \lim_{n\to\infty} \frac{1-(\psi/\phi)^{n+1}}{1-(\psi/\phi)^n} \\
&= \phi.
\end{aligned}$$

□

18.

Let a and b be integers such that $\gcd(a,b) = 1$. Let r and s be integers such that $ar + bs = 1$. Prove that

$$\gcd(a,s) = \gcd(r,b) = \gcd(r,s) = 1.$$

19.

Let $x, y \in \mathbb{N}$ be relatively prime. If xy is a perfect square, prove that x and y must both be perfect squares.

20.

Using the division algorithm, show that every perfect square is of the form $4k$ or $4k+1$ for some nonnegative integer k.

21.

Suppose that a, b, r, s are pairwise relatively prime and that

$$a^2 + b^2 = r^2$$
$$a^2 - b^2 = s^2.$$

Prove that a, r, and s are odd and b is even.

22.

Let $n \in \mathbb{N}$. Use the division algorithm to prove that every integer is congruent mod n to precisely one of the integers $0, 1, \ldots, n-1$. Conclude that if r is an integer, then there is exactly one s in $\mathbb{Z}$ such that $0 \leq s < n$ and $[r] = [s]$. Hence, the integers are indeed partitioned by congruence mod n.

23.

Define the ***least common multiple*** of two nonzero integers a and b, denoted by $\text{lcm}(a, b)$, to be the nonnegative integer m such that both a and b divide m, and if a and b divide any other integer n, then m also divided n. Prove there exists a unique least common multiple for any two integers a and b.

24.

If $d = \gcd(a, b)$ and $m = \text{lcm}(a, b)$, prove that $dm = |ab|$.

25.

Show that $\text{lcm}(a, b) = ab$ if and only if $\gcd(a, b) = 1$.

26.

Prove that $\gcd(a, c) = \gcd(b, c) = 1$ if and only if $\gcd(ab, c) = 1$ for integers a, b, and c.

27.

Let $a, b, c \in \mathbb{Z}$. Prove that if $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Without loss of generality, let p be any prime factor of a. Since $a \mid bc$, we must have that $p \mid bc$, and so by the Fundamental Theorem of Arithmetic, p must be a prime factor of bc. However, $a \nmid b$, and so $p \nmid b$. Therefore, p is not a prime factor of b, and so p must be a prime factor of c.

Let $m, n \in \mathbb{Z}$ be such that $pm = a$ and $an = pmn = c$. Now, repeat the previous argument, replacing a with m and c with mn. As any prime factorization has only a finite number of elements, repeating this argument will eventually terminate once all prime factors of a are exhausted. Therefore, all prime factors of a are also prime factors of c, and so $a \mid c$.

28.

Let $p \geq 2$. Prove that if $2^p - 1$ is prime, then p must also be prime.

29.

Prove that there are an infinite number of primes of the form $6n + 5$.

30.

Prove that there are an infinite number of primes of the form $4n - 1$.

31.

Using the fact that 2 is prime, show that there do not exist integers p and q such that $p^2 = 2q^2$. Demonstrate that therefore $\sqrt{2}$ cannot be a rational number.

Assume otherwise, and further, assume that they are such that the fraction $\frac{p}{q} = \sqrt{2}$ is in least terms. As $p^2 = 2q^2$, it must be the case that $2 \mid p^2$, and so 2 is a prime factor of p^2. This is only possible if 2 is also a prime factor of p, and so it follows that $2 \mid p$.

Let m be such that $p = 2m$, and so $4m^2 = 2q^2$, or $2m^2 = q^2$. By the same argument as with p, it thus follows that $2 \mid q$. Let n be such that $q = 2n$. Then $2m^2 = 4n^2$, or $m^2 = 2n^2$, and so $\frac{m}{n} = \sqrt{2}$. However, we had previously taken p and q such that $\frac{p}{q} = \sqrt{2}$ was in least terms; contradiction.

Therefore, it must be that $\sqrt{2}$ is irrational. □