Review Sheet for Test 3

These problems are provided to help you study. The presence of a problem on this handout does not imply that there *will* be a similar problem on the test. And the absence of a topic does not imply that it *won't* appear on the test.

1. Let n be a positive integer, and let A_1, A_2, ..., A_n, and B be sets. Prove that

$$B - \bigcup_{i=1}^{n} A_i = \bigcap_{i=1}^{n} (B - A_i).$$

2. Consider the set

$$S = \bigcup_{n=0}^{\infty} \left(\frac{1}{2^n}, 1 \right].$$

Write S as a single interval in the real line and prove that your result is correct.

3. Prove that

$$\bigcap_{n=1}^{\infty} \left[0, 1 + \frac{1}{n} \right] = [0, 1].$$

4. Prove that

$$\left(0, 2 - \frac{1}{1} \right) \cup \left(0, 2 - \frac{1}{2} \right) \cup \left(0, 2 - \frac{1}{3} \right) \cup \left(0, 2 - \frac{1}{4} \right) \cup \ldots = (0, 2).$$

5. Define a relation $\sim$ on $\mathbb{R}$ by

$$x \sim y \quad \text{means} \quad |x + y| \geq 2.$$

Consider each axiom for an equivalence relation. If the axiom holds, prove it; if the axiom fails, give a counterexample.

6. Define a relation $\sim$ on $\mathbb{R}^2$ by

$$(a, b) \sim (c, d) \quad \text{means} \quad a + c = 2(b + d).$$

Consider each axiom for an equivalence relation. If the axiom holds, prove it; if the axiom fails, give a counterexample.

7. Let $X = \{0, 1, 2, 3\}$. A equivalence relation is defined on $X \times X$ by

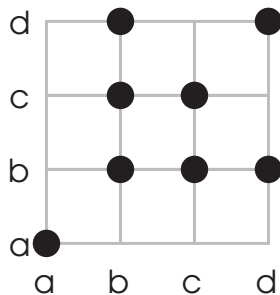$$(a, b) \sim (c, d) \leftrightarrow a + b = c + d \pmod{4}.$$

List the elements of the equivalence classes of $\sim$ under this relation.

8. For each positive integer n, define a subset of $\mathbb{R}$ by

$$S_n = \{x \in \mathbb{R} \mid |x| \leq n\}.$$

Consider each axiom for a partition. If the axiom holds, prove it; if the axiom fails, give a counterexample.

9. Consider the relation $\sim$ on $S = \{a, b, c, d\}$ whose graph is shown below. Is $\sim$ an equivalence relation?

10. A relation is defined on $\mathbb{R}^2$ by

$$(a, b) \sim (c, d) \quad \text{if and only if} \quad |a - d| = |b - c|.$$

Check *each* axiom for an equivalence relation. If the axiom holds, prove it. If the axiom does not hold, give a specific counterexample.

11. Prove that if n is a prime number and $n > 2$, then $n = 1 \pmod 4$ or $n = 3 \pmod 4$.

12. Prove that if $n \in \mathbb{Z}$, then $(3n^2 + 7n + 4, n + 2)$ is either 1 or 2. Show by specific example that both cases can occur.

13. Compute $(1121, 487)$. (Don't factor the numbers!)

14. Prove that if $n \in \mathbb{Z}$, then $(3n + 4, 4n + 5) = 1$.

15. (a) Let m and n be integers. Prove that

$$(m, n) = (m - n, n).$$

(b) Prove that if $a \in \mathbb{Z}$, then $(a^2 + 2a + 1, a + 2) = 1$.

16. Show that if $n \in \mathbb{Z}$, then $3n^2 + 4n + 1$ does not leave a remainder of 2 when it is divided by 5.

17. (a) Find $5^{-1} \pmod 7$.

(b) Show that 8 does not have a multiplicative inverse mod 10.

18. Let m and n be integers, and suppose $m \mid n$. Prove that $a = b \pmod n$ implies $a = b \pmod m$.

19. Suppose $a = b \pmod n$. Is it necessarily true that $3^a = 3^b \pmod n$?

20. Prove that if $n \in \mathbb{Z}$, then $n^2 + 4n + 1$ is not divisible by 5.

21. The following functions take real numbers as inputs and produce real numbers as outputs. Taking the domain to be the largest set of valid inputs, find the domain and the range for each function.

(a) $f(x) = 2x^4$.

(b) $g(x) = \dfrac{x - 1}{x - 1}$.

(c) $f(x) = \dfrac{2x}{x - 1}$.

22. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = x^3 + 10$. Prove directly using the definition that f is injective.

23. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = x^2 + \cos x$. Prove that f is not injective.

24. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = 2e^x + 4x^3 + 1$. Prove that f is injective.

25. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = 4 - 3x^5$. Prove that directly using the definition that f is surjective.

26. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = x^3 + \sin x$. Prove that f is surjective.

27. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = 2^x - 5$. Prove that f is injective. Is f surjective?

28. Define $f : \mathbb{R}^2 \to \mathbb{R}$ by $f(x, y) = x^2 + 2y$. Prove that f is *not* injective, but that f is surjective.

29. Define $f : \mathbb{R} \to \mathbb{R}^2$ by $f(x) = (x + 1, -3x)$. Prove that f is injective, but is *not* surjective.

30. Define $f : \mathbb{R}^2 \to \mathbb{R}^2$ by
$$f(x, y) = (|x| + y, 17y).$$

Is f surjective? Why or why not?

31. Define $f : \mathbb{R}^2 \to \mathbb{R}^2$ by
$$f(x, y) = (x + y, x^3 + 1).$$

Prove that f is bijective by constructing an inverse.

32. Define $f : \mathbb{R}^2 \to \mathbb{R}^2$ by
$$f(x, y) = (x - 10, y + e^x).$$

Prove that f is bijective by constructing an inverse.

33. Let $f : X \to Y$ and $g : Y \to Z$ be functions. Suppose f and g are injective. Prove that the composite $g \circ f$ is injective.

34. Give a specific example of sets X, Y, and Z and functions $f : X \to Y$ and $g : Y \to Z$ such that g is surjective, but the composite $g \circ f$ is not.

35. Prove that the following sets have the same cardinality by constructing a bijection from A to B:
$$A = \mathbb{Z}^{\geq 0} = \{0, 1, 2, 3, \ldots\} \quad \text{and} \quad B = 2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}.$$

36. Prove that $[1, 5]$ has the same cardinality as $[-2, 6]$ by constructing a bijection from $[1, 5]$ to $[-2, 6]$.

37. Prove that $[-3, 5)$ has the same cardinality as $(7, 23]$ by constructing a bijection from $[-3, 5)$ to $(7, 23]$.

Solutions to the Review Sheet for Test 3

1. Let n be a positive integer, and let A_1, A_2, ..., A_n, and B be sets. Prove that
$$B - \bigcup_{i=1}^{n} A_i = \bigcap_{i=1}^{n} (B - A_i).$$

For $n = 1$,
$$B - \bigcup_{i=1}^{n} A_i = B - A_1, \quad \text{while} \quad \bigcap_{i=1}^{n} (B - A_i) = B - A_1.$$

The result is true for $n = 1$.

The induction step will also need the result for $n = 2$, so I'll prove it here. For $n = 2$, the result says that
$$B - (A_1 \cup A_2) = (B - A_1) \cap (B - A_2).$$

$$
\begin{array}{llr}
x \in [B - (A_1 \cup A_2)] & \leftrightarrow \quad x \in B \wedge x \notin (A_1 \cup A_2) & \text{Definition of complement} \\
& \leftrightarrow \quad x \in B \wedge \neg[x \in (A_1 \cup A_2)] & \text{Definition of } \notin \\
& \leftrightarrow \quad x \in B \wedge \neg(x \in A_1 \vee x \in A_2) & \text{Definition of } \cup \\
& \leftrightarrow \quad x \in B \wedge [\neg(x \in A_1) \wedge \neg(x \in A_2)] & \text{DeMorgan's law} \\
& \leftrightarrow \quad x \in B \wedge \neg(x \in A_1) \wedge x \in B \wedge \neg(x \in A_2) & (P \wedge P) \leftrightarrow P \\
& \leftrightarrow \quad [x \in B \wedge \neg(x \in A_1)] \wedge [x \in B \wedge \neg(x \in A_2)] & \text{Grouping} \\
& \leftrightarrow \quad (x \in B \wedge x \notin A_1) \wedge (x \in B \wedge x \notin A_2) & \text{Definition of } \notin \\
& \leftrightarrow \quad x \in (B - A_1) \wedge x \in (B - A_2) & \text{Definition of complement} \\
& \leftrightarrow \quad x \in [(B - A_1) \cap (B - A_2)] & \text{Definition of } \cap
\end{array}
$$

Now I'll prove the general result by induction. Take $n > 2$, and suppose the result is true for $n - 1$. This means that
$$B - \bigcup_{i=1}^{n-1} A_i = \bigcap_{i=1}^{n-1} (B - A_i).$$

I want to prove that
$$B - \bigcup_{i=1}^{n} A_i = \bigcap_{i=1}^{n} (B - A_i).$$

The proof proceeds in the usual way by "splitting off" the $n - 1$ piece and applying the induction hypothesis:
$$B - \bigcup_{i=1}^{n} A_i = B - \left(\bigcup_{i=1}^{n-1} A_i \cup A_n \right) = \left(B - \bigcup_{i=1}^{n-1} A_i \right) \cap (B - A_n) =$$

$$\bigcap_{i=1}^{n-1} (B - A_i) \cap (B - A_n) = \bigcap_{i=1}^{n} (B - A_i).$$

(Notice that the second equality used the result for $n = 2$, which is why I needed to prove it first.) I've proved the result for n; hence, the result is true for all $n \geq 1$ by induction. □

---

2. Consider the set
$$S = \bigcup_{n=0}^{\infty} \left(\frac{1}{2^n}, 1 \right].$$

Write S as a single interval in the real line and prove that your result is correct.

I'll show that $S = (0, 1]$.

First, notice that $\left(\frac{1}{2^n}, 1 \right] \subset (0, 1]$ for all $n \geq 0$, since $\frac{1}{2^n} > 0$. This implies that $S = \bigcup_{n=0}^{\infty} \left(\frac{1}{2^n}, 1 \right] \subset (0, 1]$.

Next, I'll show that $(0, 1] \subset S$. Take $x \in (0, 1]$, so $0 < x \leq 1$.

Note that
$$\lim_{n \to \infty} \frac{1}{2^n} = 0.$$

In the limit definition, let $\epsilon = x$. Then there is a number M such that for $n > M$,
$$\epsilon = x > \left| \frac{1}{2^n} - 0 \right| = \frac{1}{2^n}.$$

4

Then $\dfrac{1}{2^n} < x \le 1$, so $x \in \left(\dfrac{1}{2^n}, 1\right]$. Hence, $x \in \displaystyle\bigcup_{n=0}^{\infty} \left(\dfrac{1}{2^n}, 1\right] = S$. This proves that $(0, 1] \subset S$.

Since $(0, 1] \subset S$ and $S \subset (0, 1]$, it follows that $S = (0, 1]$. $\square$

---

3. Prove that

$$\bigcap_{n=1}^{\infty} \left[0, 1 + \frac{1}{n}\right] = [0, 1].$$

Let $x \in [0, 1]$, so $0 \le x \le 1$. Note that for $n \ge 1$, I have $1 < 1 + \dfrac{1}{n}$. Hence, $0 \le x \le 1 + \dfrac{1}{n}$ for $n \ge 1$,

and $x \in \left[0, 1 + \dfrac{1}{n}\right]$ for $n \ge 1$. Therefore, $x \in \displaystyle\bigcap_{n=1}^{\infty} \left[0, 1 + \dfrac{1}{n}\right]$. This proves that $[0, 1] \subset \displaystyle\bigcap_{n=1}^{\infty} \left[0, 1 + \dfrac{1}{n}\right]$.

Conversely, let $x \in \displaystyle\bigcap_{n=1}^{\infty} \left[0, 1 + \dfrac{1}{n}\right]$. This means that $x \in \left[0, 1 + \dfrac{1}{n}\right]$ for all $n \ge 1$, so $0 \le x \le 1 + \dfrac{1}{n}$ for all $n \ge 1$.

Suppose $x > 1$. I have

$$\lim_{n \to \infty} \left(1 + \frac{1}{n}\right) = 1.$$

In the limit definition, let $\epsilon = x - 1$. Then there is a number M such that if $n > M$,

$$\epsilon = x - 1 > \left|1 + \frac{1}{n} - 1\right| = \frac{1}{n}.$$

Hence, for $n > M$,

$$x > 1 + \frac{1}{n}.$$

This contradicts $0 \le x \le 1 + \dfrac{1}{n}$ for all $n \ge 1$.

It follows that $x \le 1$. Since $0 \le x$, I have $0 \le x \le 1$, and hence $x \in [0, 1]$. Thus, $\displaystyle\bigcap_{n=1}^{\infty} \left[0, 1 + \dfrac{1}{n}\right] \subset [0, 1]$.

This proves that $\displaystyle\bigcap_{n=1}^{\infty} \left[0, 1 + \dfrac{1}{n}\right] = [0, 1]$. $\square$

---

4. Prove that

$$\left(0, 2 - \frac{1}{1}\right) \cup \left(0, 2 - \frac{1}{2}\right) \cup \left(0, 2 - \frac{1}{3}\right) \cup \left(0, 2 - \frac{1}{4}\right) \cup \ldots = (0, 2).$$

The union on the left is $\displaystyle\bigcup_{n=1}^{\infty} \left(0, 2 - \dfrac{1}{n}\right)$.

Let $x \in \displaystyle\bigcup_{n=1}^{\infty} \left(0, 2 - \dfrac{1}{n}\right)$. Then for some $n \ge 1$, I have $x \in \left(0, 2 - \dfrac{1}{n}\right)$. This means that

$$0 < x < 2 - \frac{1}{n} < 2.$$

Hence, $x \in (0, 2)$. This proves that $\displaystyle\bigcup_{n=1}^{\infty} \left(0, 2 - \dfrac{1}{n}\right) \subset (0, 2)$.

5

Conversely, suppose $x \in (0, 2)$, so $0 < x < 2$. Now

$$\lim_{n \to \infty} \left(2 - \frac{1}{n}\right) = 2.$$

In the limit definition, let $\epsilon = 2 - x$. Then there is a number M such that if $n > M$,

$$\epsilon = 2 - x > \left|2 - \frac{1}{n} - 2\right| = \frac{1}{n}.$$

Thus, for $n > M$ I have

$$2 - x > \frac{1}{n}$$

$$2 - \frac{1}{n} > x$$

This implies that

$$0 < x < 2 - \frac{1}{n}, \quad \text{so} \quad x \in \left(0, 2 - \frac{1}{n}\right).$$

Therefore, $x \in \bigcup_{n=1}^{\infty} \left(0, 2 - \frac{1}{n}\right)$. This proves that $(0, 2) \subset \bigcup_{n=1}^{\infty} \left(0, 2 - \frac{1}{n}\right)$.

Hence, $\bigcup_{n=1}^{\infty} \left(0, 2 - \frac{1}{n}\right) = (0, 2)$. □

---

5. Define a relation $\sim$ on $\mathbb{R}$ by

$$x \sim y \quad \text{means} \quad |x + y| \geq 2.$$

Consider each axiom for an equivalence relation. If the axiom holds, prove it; if the axiom fails, give a counterexample.

Reflexivity does not hold: For example, $|0 + 0| = 0 \not\geq 2$, so $0 \not\sim 0$.

If $x \sim y$, then $|x + y| \geq 2$. Hence, $|y + x| \geq 2$, and so $y \sim x$. Therefore, symmetry holds.

Transitivity does not hold. For example, $0.5 \sim 2$, since $|0.5 + 2| = 2.5 \geq 2$; $2 \sim 0.5$, since $|2 + 0.5| = 2.5 \geq 2$. However, $0.5 \not\sim 0.5$, since $|0.5 + 0.5| = 1 \not\geq 2$. □

---

6. Define a relation $\sim$ on $\mathbb{R}^2$ by

$$(a, b) \sim (c, d) \quad \text{means} \quad a + c = 2(b + d).$$

Consider each axiom for an equivalence relation. If the axiom holds, prove it; if the axiom fails, give a counterexample.

$1 + 1 = 2$, but $2(0 + 0) = 0$. Therefore,

$$(1 + 1 \neq 2(0 + 0)), \quad \text{so} \quad (1, 0) \not\sim (1, 0).$$

The relation is not reflexive.

Suppose $(a, b) \sim (c, d)$. Then

$$a + c = 2(b + d), \quad \text{so} \quad c + a = 2(d + b).$$

Therefore, $(c, d) \sim (a, b)$. Hence, the relation is symmetric.

$(3, 1) \sim (5, 3)$, since
$$3 + 5 = 8 \quad \text{and} \quad 2(1 + 3) = 8.$$

$(5, 3) \sim (15, 7)$, since
$$5 + 15 = 20 \quad \text{and} \quad 2(3 + 7) = 20.$$

However, $(3, 1) \not\sim (15, 7)$, since
$$3 + 15 = 18, \quad \text{but} \quad 2(1 + 7) = 16.$$

Therefore, the relation is not transitive. □

---

7. Let $X = \{0, 1, 2, 3\}$. A equivalence relation is defined on $X \times X$ by
$$(a, b) \sim (c, d) \leftrightarrow a + b = c + d \pmod{4}.$$

List the elements of the equivalence classes of $\sim$ under this relation.

There are 16 points in $X \times X$:

$$
\begin{array}{cccc}
\bullet & \bullet & \bullet & \bullet \\
(0,3) & (1,3) & (2,3) & (3,3) \\[6pt]
\bullet & \bullet & \bullet & \bullet \\
(0,2) & (1,2) & (2,2) & (3,2) \\[6pt]
\bullet & \bullet & \bullet & \bullet \\
(0,1) & (1,1) & (2,1) & (3,1) \\[6pt]
\bullet & \bullet & \bullet & \bullet \\
(0,0) & (1,0) & (2,0) & (3,0)
\end{array}
$$

Two points are in the same equivalence class if the sums of their components are equal mod 4. For example, $(1, 1) \sim (3, 3)$, because
$$1 + 1 = 2 \pmod{4} \quad \text{and} \quad 3 + 3 = 2 \pmod{4}.$$

The four equivalence classes are:
$$\{(0, 0), \ (1, 3), \ (2, 2), \ (3, 1)\},$$
$$\{(0, 1), \ (1, 0), \ (2, 3), \ (3, 2)\},$$
$$\{(0, 2), \ (1, 1), \ (2, 0), \ (3, 3)\},$$
$$\{(0, 3), \ (1, 2), \ (2, 1), \ (3, 0)\}. \quad □$$

---

8. For each positive integer n, define a subset of $\mathbb{R}$ by
$$S_n = \{x \in \mathbb{R} \mid |x| \le n\}.$$

Consider each axiom for a partition. If the axiom holds, prove it; if the axiom fails, give a counterexample.

If x is a real number, there is a positive integer n such that $n \ge |x|$ — and hence, $x \in S_n$. Every point of $\mathbb{R}$ is in one of the S_n's.

On the other hand, $|0| = 0 \leq n$ for every positive integer n, so $0 \in S_n$ for all n. There are points which are in more than one S_n — in fact, in infinitely many of the S_n's.

Thus, the S_n's do not form a partition of $\mathbb{R}$. ◻

---

9. Consider the relation $\sim$ on $S = \{a, b, c, d\}$ whose graph is shown below. Is $\sim$ an equivalence relation?
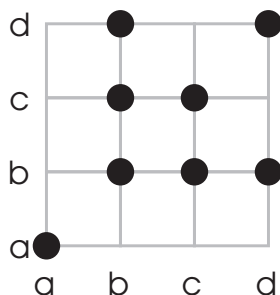
The relation is reflexive (all the diagonal points are filled in) and symmetric (the graph is symmetric about the diagonal). However, it isn't transitive: $c \sim b$ and $b \sim d$, but $c \not\sim d$. Therefore, the relation is not an equivalence relation. ◻

---

10. A relation is defined on $\mathbb{R}^2$ by

$$(a, b) \sim (c, d) \quad \text{if and only if} \quad |a - d| = |b - c|.$$

Check *each* axiom for an equivalence relation. If the axiom holds, prove it. If the axiom does not hold, give a specific counterexample.

It may be helpful if you label the pairs by position:

$$(\text{first}, \text{second}) \sim (\text{third}, \text{fourth}) \quad \text{if and only if} \quad |\text{first} - \text{fourth}| = |\text{second} - \text{third}|.$$

Also, remember that
$$|x - y| = |y - x|.$$

Let $(a, b) \in \mathbb{R}^2$. Since $|a - b| = |b - a|$, it follows that $(a, b) \sim (a, b)$. Hence, $\sim$ is reflexive.
Suppose $(a, b), (c, d) \in \mathbb{R}^2$ and $(a, b) \sim (c, d)$. Then

$$|a - d| = |b - c|$$
$$|d - a| = |c - b|$$
$$|c - b| = |d - a|$$

Therefore, $(c, d) \sim (a, b)$. Hence, $\sim$ is symmetric.
Note that
$$(1, 0) \sim (-1, 0), \quad \text{since} \quad |1 - 0| = |0 - (-1)|,$$
$$(-1, 0) \sim (1, -2), \quad \text{since} \quad |-1 - (-2)| = |0 - 1|.$$

However, $(1, 0) \not\sim (1, -2)$, because

$$|1 - (-2)| = 3, \quad \text{but} \quad |0 - 1| = 1.$$

Therefore, $\sim$ is not transitive. ◻

11. Prove that if n is a prime number and $n > 2$, then $n = 1 \pmod 4$ or $n = 3 \pmod 4$.

Every integer is congruent mod 4 to 0, 1, 2, or 3.

Suppose n is prime and $n > 2$. Since n is an integer, n is congruent mod 4 to 0, 1, 2, or 3.

Suppose $n = 0 \pmod 4$. Then $4 \mid n$, contradicting the fact that n is prime.

Suppose $n = 2 mod 4$. Then $n = 4k + 2$, where $k \in \mathbb{Z}$. Thus, $n = 2(2k + 1)$, so n is even. Since $n > 2$, this contradicts the fact that n is prime.

It follows that $n = 1 \pmod 4$ or $n = 3 \pmod 4$. Both cases can occur, since $5 = 1 \pmod 4$ and $7 = 3 \pmod 4$ (for example). □

12. Prove that if $n \in \mathbb{Z}$, then $(3n^2 + 7n + 4, n + 2)$ is either 1 or 2. Show by specific example that both cases can occur.

Dividing $3n^2 + 7n + 4$ by $n + 2$, I have

$$3n^2 + 7n + 4 = (3n + 1)(n + 2) + 2, \quad \text{or} \quad (3n^2 + 7n + 4) - (3n + 1)(n + 2) = 2.$$

Now $(3n^2+7n+4, n+2)$ divides both $3n^2+7n+4$ and $n+2$, so it divides $(3n^2+7n+4)-(3n+1)(n+2) = 2$. But the only positive integers which divide 2 are 1 and 2. Hence, $(3n^2 + 7n + 4, n + 2)$ is either 1 or 2.

If $n = 1$, I have $3n^2 + 7n + 4 = 14$ and $n + 2 = 3$, and $(14, 3) = 1$.

If $n = 2$, I have $3n^2 + 7n + 4 = 30$ and $n + 2 = 4$, and $(30, 4) = 2$.

These examples show that both cases can occur. □

13. Compute $(1121, 487)$. (Don't factor the numbers!)

1121	-
487	2
147	3
46	3
9	5
1	9

Hence, $(1121, 487) = 1$. □

14. Prove that if $n \in \mathbb{Z}$, then $(3n + 4, 4n + 5) = 1$.

$(3n + 4, 4n + 5) \mid 3n + 4$ and $(3n + 4, 4n + 5) \mid 4n + 5$, so

$$(3n + 4, 4n + 5) \mid 4(3n + 4) - 3(4n + 5) = 1.$$

Since $(3n + 4, 4n + 5) \geq 1$, it follows that $(3n + 4, 4n + 5) = 1$. □

In general, if a linear combination of two integers is equal to 1, the two integers are relatively prime (their greatest common divisor is 1).

15. (a) Let m and n be integers. Prove that

$$(m, n) = (m - n, n).$$

(b) Prove that if $a \in \mathbb{Z}$, then $(a^2 + 2a + 1, a + 2) = 1$.

(a) First, $(m, n) \mid m$ and $(m, n) \mid n$. So $(m, n) \mid m - n$. Since (m, n) divides both $m - n$ and n, it's a common divisor of $m - n$ and n. Therefore, it must be less than or equal to the *greatest* common divisor of $m - n$ and n; that is,

$$(m, n) \le (m - n, n).$$

Similarly, $(m - n, n) \mid m - n$ and $(m - n, n) \mid n$. So

$$(m - n, n) \mid (m - n) + n = m.$$

Since $(m - n, n)$ divides both m and n, it's a common divisor of m and n. Therefore, it must be less than or equal to the *greatest* common divisor of m and n; that is,

$$(m - n, n) \le (m, n).$$

The two inequalities I've proved combine to show that $(m, n) = (m - n, n)$. ◻

In words, the result of (a) says that the greatest common divisor of two numbers doesn't change if you replace the first number with the first number minus the second number. This provides a way of "simplifying" a greatest common divisor expression.

(b) Using the result of (a), I have

$$(a^2 + 2a + 1, a + 2) = (a^2 + 2a + 1 - a(a + 2), a + 2) = (a^2 + 2a + 1 - a^2 - 2a, a + 2) = (1, a + 2).$$

Now $(1, a + 2) \mid 1$, so $(1, a + 2) = 1$. Therefore, $(a^2 + 2a + 1, a + 2) = 1$. ◻

---

16. Show that if $n \in \mathbb{Z}$, then $3n^2 + 4n + 1$ does not leave a remainder of 2 when it is divided by 5.

Consider n mod 5. There are 5 cases:

n	0	1	2	3	4
$3n^2 + 4n + 1$	1	3	1	0	0

As the table shows, $3n^2 + 4n + 1 \ne 2 \pmod 5$. Therefore, $3n^2 + 4n + 1$ does not leave a remainder of 2 when it is divided by 5. ◻

---

17. (a) Find $5^{-1} \pmod 7$.

(b) Show that 8 does not have a multiplicative inverse mod 10.

(a) By trial and error, you can show that $5 \cdot 3 = 1 \pmod 7$. Therefore, $5^{-1} = 3 \pmod 7$. ◻

(b) Suppose $8x = 1 \pmod{10}$ for some x (so that $x = 8^{-1} \pmod{10}$). Multiplying both sides by 5, I get

$$5 \cdot 8x = 5 \cdot 1 \pmod{10}$$
$$0 = 5 \pmod{10}$$

This contradiction shows that 8 does not have a multiplicative inverse mod 10. ◻

10

18. Let m and n be integers, and suppose $m \mid n$. Prove that $a = b \pmod{n}$ implies $a = b \pmod{m}$.

Since $m \mid n$, I have $mp = n$ for some integer p. If $a = b \pmod{n}$, then $a - b = kn$ for some integer k. Substituting yields $a - b = kmp = (kp)m$; this means that $a = b \pmod{m}$, which is what I wanted to prove. $\square$

---

19. Suppose $a = b \pmod{n}$. Is it necessarily true that $3^a = 3^b \pmod{n}$?

No. $2 = 7 \pmod 5$, but $3^2 = 4 \pmod 5$, while $3^7 = 2 \pmod 5$. $\square$

---

20. Prove that if $n \in \mathbb{Z}$, then $n^2 + 4n + 1$ is not divisible by 5.

If $n \in \mathbb{Z}$, then n is congruent mod 5 to 0, 1, 2, 3, or 4. Take cases:

$n \pmod 5$	0	1	2	3	4
$n^2 + 4n + 1 \pmod 5$	1	1	3	2	3

Since $n^2 + 4n + 1 \neq 0 \pmod 5$, it follows that $5 \nmid n^2 + 4n + 1$ for all $n \in \mathbb{Z}$. $\square$

---

21. The following functions take real numbers as inputs and produce real numbers as outputs. Taking the domain to be the largest set of valid inputs, find the domain and the range for each function.

(a) $f(x) = 2x^4$.

(b) $g(x) = \dfrac{x - 1}{x - 1}$.

(c) $f(x) = \dfrac{2x}{x - 1}$.

(a) The domain is $\mathbb{R}$.
    An even power can't be negative, so $2x^4 \geq 0$. On the other hand, if $y \geq 0$, then

$$f\left(\sqrt[4]{\frac{y}{2}}\right) = 2\left(\sqrt[4]{\frac{y}{2}}\right)^4 = 2 \cdot \frac{y}{2} = y.$$

Therefore, every $y \geq 0$ is an output of f, and the range is $y \geq 0$. $\square$

(b) The domain is $x \neq 1$. (Note that plugging 1 into $\dfrac{x - 1}{x - 1}$ gives $\dfrac{0}{0}$, which is undefined.)
    The range is $y = 1$, since if $x \neq 1$,

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

(c) The domain is $x \neq 1$.
    Note that $\displaystyle\lim_{x \to \pm\infty} \frac{2x}{x - 1} = 2$. This suggests that the range is $y \neq 2$.
    First, I'll show that $y = 2$ *is not* in the range. Suppose it is. Then for some x, I have $f(x) = 2$. So

$$\frac{2x}{x - 1} = 2$$
$$2x = 2(x - 1)$$
$$2x = 2x - 2$$
$$0 = -2$$

11

This contradiction shows that there is no such x, so $y = 2$ is not in the range.

Next, I'll show if $y \neq 2$, then y *is* in the range. Since $y \neq 2$, the quantity $\dfrac{y}{y-2}$ is defined. (I found it by setting $y = f(x) = \dfrac{2x}{x-1}$ and solving for x.) Moreover,

$$f\left(\frac{y}{y-2}\right) = \frac{2 \cdot \dfrac{y}{y-2}}{\dfrac{y}{y-2} - 1} = \frac{2y}{y - (y-2)} = \frac{2y}{2} = y.$$

This proves that y is in the range.

Therefore, the range of f is $y \neq 2$. □

---

22. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = x^3 + 10$. Prove directly using the definition that f is injective.

$$f(a) = f(b)$$
$$a^3 + 10 = b^3 + 10$$
$$a^3 = b^3$$
$$a = b \quad \square$$

---

23. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = x^2 + \cos x$. Prove that f is not injective.

$$f(\pi) = \pi^2 + \cos \pi = \pi^2 - 1.$$
$$f(-\pi) = (-\pi)^2 + \cos(-\pi) = \pi^2 - 1.$$

Thus, $f(\pi) = f(-\pi)$, but $\pi \neq -\pi$. Hence, f is not injective. □

---

24. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = 2e^x + 4x^3 + 1$. Prove that f is injective.

It would be difficult to do this directly. Instead, use derivatives:

$$f'(x) = 2e^x + 12x^2 > 0 \quad \text{for all} \quad x.$$

Hence, f increases for all x, and hence f is injective. □

---

25. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = 4 - 3x^5$. Prove that directly using the definition that f is surjective.

Let $y \in \mathbb{R}$. Then

$$f\left(\sqrt[5]{\frac{4}{3} - \frac{1}{3}y}\right) = 4 - 3[\sqrt[5]{\frac{4}{3} - \frac{1}{3}y}]^5 = 4 - 3\left(\frac{4}{3} - \frac{1}{3}y\right) =$$

$$4 - 4 + y = y.$$

Hence, f is surjective. □

---

26. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = x^3 + \sin x$. Prove that f is surjective.

Let $y \in \mathbb{R}$. I must show that there is an $x \in \mathbb{R}$ such that $f(x) = y$.
Note that f is continuous, and

$$\lim_{x \to \infty} (x^3 + \sin x) = +\infty \quad \text{and} \quad \lim_{x \to -\infty} (x^3 + \sin x) = -\infty.$$

Hence, there are numbers c and d such that

$$f(c) < y < f(d).$$

By the Intermediate Value Theorem, there is a number x such that $c \le x \le d$ and $f(x) = y$.
Therefore, f is surjective. $\square$

---

27. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = 2^x - 5$. Prove that f is injective. Is f surjective?

Suppose $f(a) = f(b)$. Then
$$2^a - 5 = 2^b - 5$$
$$2^a = 2^b$$
$$\log_2 2^a = \log_2 2^b$$
$$a = b$$

Therefore, f is injective.
However, f is not surjective. For example, I'll show that there is no $x \in \mathbb{R}$ such that $f(x) = -6$. For if $f(x) = -6$, then
$$2^x - 5 = -6$$
$$2^x = -1$$

The last equation is a contradiction, since $2^x > 0$ for all x. $\square$

---

28. Define $f : \mathbb{R}^2 \to \mathbb{R}$ by $f(x, y) = x^2 + 2y$. Prove that f is *not* injective, but that f is surjective.

First, $f(0, 0) = 0$ and $f(2, -2) = 0$, but $(0, 0) \ne (2, -2)$. Since different inputs can give the same output, f is not injective.
To show that f is surjective, let $z \in \mathbb{R}$. I have to find an input (x, y) such that $f(x, y) = z$. There are many that work; here's one:
$$f\left(0, \frac{z}{2}\right) = 0^2 + 2 \cdot \frac{z}{2} = z.$$

Hence, f is surjective. $\square$

---

29. Define $f : \mathbb{R} \to \mathbb{R}^2$ by $f(x) = (x + 1, -3x)$. Prove that f is injective, but is *not* surjective.

First, suppose $f(a) = f(b)$. Then

$$(a + 1, -3a) = (b + 1, -3b).$$

Equate the first components to get $a + 1 = b + 1$. Subtracting 1 from both sides, I get $a = b$. Therefore, f is injective.
On the other hand, I'll show that there is no input x such that $f(x) = (3, 12)$. Suppose on the contrary that $f(x) = (3, 12)$, so $(x + 1, -3x) = (3, 12)$. Equating the first components, I get $x + 1 = 3$, so $x = 2$. But

13

equating the second components, I get $-3x = 12$, so $x = -4$. Since x can't be 2 and -4 simultaneously, this is a contradiction, and there is no such x. Hence, f is not surjective. $\square$

---

30. Define $f : \mathbb{R}^2 \to \mathbb{R}^2$ by

$$f(x, y) = (|x| + y, 17y).$$

Is f surjective? Why or why not?

Suppose $f(x, y) = (-1, 0)$. Then

$$(|x| + y, 17y) = (-1, 0).$$

Equating the second components, I get $17y = 0$, so $y = 0$. Equating the first components and plugging in $y = 0$, I get

$$|x| + y = -1, \quad |x| + 0 = -1, \quad |x| = -1.$$

The last equation has no solutions.

Therefore, there is no pair $(x, y) \in \mathbb{R}^2$ such that $f(x, y) = (-1, 0)$, and hence f is not surjective. $\square$

---

31. Define $f : \mathbb{R}^2 \to \mathbb{R}^2$ by

$$f(x, y) = (x + y, x^3 + 1).$$

Prove that f is bijective by constructing an inverse.

First, I'll work backwards to guess the inverse. If $f(x, y) = (a, b)$, then $(x, y) = f^{-1}(a, b)$. So I'll set $f(x, y) = (a, b)$ and solve for x and y:

$$(x + y, x^3 + 1) = (a, b), \quad x + y = a \quad \text{and} \quad x^3 + 1 = b.$$

$x^3 + 1 = b$ gives $x^3 = b - 1$, so $x = (b - 1)^{1/3}$. Then

$$x + y = a, \quad \text{so} \quad (b - 1)^{1/3} + y = a, \quad \text{and} \quad y = a - (b - 1)^{1/3}.$$

Thus, I'll define $f^{-1} : \mathbb{R}^2 \to \mathbb{R}^2$ by

$$f^{-1}(a, b) = \left((b - 1)^{1/3}, a - (b - 1)^{1/3} \right).$$

Next, I'll check that the inverse actually works. (This is the actual proof.)

$$f\left(f^{-1}(a, b) \right) = f\left((b - 1)^{1/3}, a - (b - 1)^{1/3} \right) = \left((b - 1)^{1/3} + a - (b - 1)^{1/3}, \left((b - 1)^{1/3} \right)^3 + 1 \right) =$$

$$(a, b - 1 + 1) = (a, b).$$

$$f^{-1}\left(f(x, y) \right) = f^{-1}\left(x + y, x^3 + 1 \right) = \left(\left((x^3 + 1) - 1 \right)^{1/3}, x + y - \left(x^3 + 1 - 1 \right)^{1/3} \right) =$$

$$\left((x^3)^{1/3}, x + y - (x^3)^{1/3} \right) = (x, x + y - x) = (x, y).$$

Therefore, f and f^{-1} are inverses, and f is bijective. $\square$

---

32. Define $f : \mathbb{R}^2 \to \mathbb{R}^2$ by

$$f(x, y) = (x - 10, y + e^x).$$

Prove that f is bijective by constructing an inverse.

I'll work backwards to guess the inverse, then confirm my guess. If $f(x, y) = (a, b)$, then $(x, y) = f^{-1}(a, b)$. So I'll set $f(x, y) = (a, b)$ and solve for x and y:

$$(x - 10, y + e^x) = (a, b), \quad x - 10 = a \quad \text{and} \quad y + e^x = b.$$

$x - 10 = a$ gives $x = a + 10$. Then

$$y + e^x = b, \quad \text{so} \quad y + e^{(a+10)} = b, \quad \text{and} \quad y = b - e^{(a+10)}.$$

Thus, I'll define $f^{-1} : \mathbb{R}^2 \to \mathbb{R}^2$ by

$$f^{-1}(a, b) = \left(a + 10, b - e^{(a+10)} \right).$$

Next, I'll check that the inverse actually works. (This is the actual proof.)

$$f\left(f^{-1}(a, b)\right) = f\left(a + 10, b - e^{(a+10)}\right) = \left((a + 10) - 10, (b - e^{(a+10)}) + e^{(a+10)}\right) = (a, b).$$

$$f^{-1}\left(f(x, y)\right) = f^{-1}\left(x - 10, y + e^x\right) = \left((x - 10) + 10, (y + e^x) - e^{(x-10+10)}\right) =$$

$$(x, y + e^x - e^x) = (x, y).$$

Therefore, f and f^{-1} are inverses, and f is bijective. ◻

---

33. Let $f : X \to Y$ and $g : Y \to Z$ be functions. Suppose f and g are injective. Prove that the composite $g \circ f$ is injective.

Suppose that $(g \circ f)(a) = (g \circ f)(b)$. I must show $a = b$. I have

$$\begin{array}{rll}
(g \circ f)(a) & = (g \circ f)(b) & \\
g(f(a)) & = g(f(b)) & \text{(Definition of composite)} \\
f(a) & = f(b) & \text{(g is injective)} \\
a & = b & \text{(f is injective)}
\end{array}$$

Therefore, $g \circ f$ is injective. ◻

---

34. Give a specific example of sets X, Y, and Z and functions $f : X \to Y$ and $g : Y \to Z$ such that g is surjective, but the composite $g \circ f$ is not.

Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$. Let $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = x^3$.
g is surjective, because if $y \in \mathbb{R}$, then

$$g(\sqrt[3]{y}) = (\sqrt[3]{y})^3 = y.$$

However, $g \circ f$ is not surjective. In fact,

$$(g \circ f)(x) = g(f(x)) = g(x^2) = x^6.$$

But since x^6 is an even power, it's always nonnegative. Therefore, there is no $x \in \mathbb{R}$ such that $(g \circ f)(x) = x^6 = -1$. ◻

---

35. Prove that the following sets have the same cardinality by constructing a bijection from A to B:

$$A = \mathbb{Z}^{\geq 0} = \{0, 1, 2, 3, \ldots\} \quad \text{and} \quad B = 2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}.$$

Define $f : A \to B$ by

$$f(n) = \begin{cases} 0 & \text{if } n = 0 \\ n & \text{if } n \text{ is even} \\ -n - 1 & \text{if } n \text{ is odd} \end{cases}.$$

Note that $f(n)$ is even for all $n \in A$. (In the third case, if n is odd, then $-n$ is odd, so $-n - 1$ is even.) In words, f sends 0 to 0, positive even numbers to themselves, and positive odd numbers to negative even numbers.

Define $g : B \to A$ by

$$g(n) = \begin{cases} 0 & \text{if } n = 0 \\ n & \text{if } n > 0 \\ -n - 1 & \text{if } n < 0 \end{cases}.$$

Note that $g(n) \geq 0$ for all $n \in B$.

I'll show that f and g are inverses.

First, let $n \in A$. I must show $g(f(n)) = n$. There are 3 cases.

If $n = 0$, then

$$g(f(0)) = g(0) = 0.$$

If $n > 0$ and n is even, then

$$g(f(n)) = g(n) = n.$$

Finally, if $n > 0$ and n is odd, then

$$g(f(n)) = g(-n - 1) = -(-n - 1) - 1 = n + 1 - 1 = n.$$

Thus, in all cases $g(f(n)) = n$.

Next, let $n \in B$. I must show that $f(g(n)) = n$. There are 3 cases.

If $n = 0$, then

$$f(g(0)) = f(0) = 0.$$

If $n > 0$ and n is even, then

$$f(g(n)) = f(n) = n.$$

If $n < 0$ and n is even, then $-n - 1$ is positive and odd. Hence,

$$f(g(n)) = f(-n - 1) = -(-n - 1) - 1 = n + 1 - 1 = n.$$

Thus, in all cases $f(g(n)) = n$.

Therefore, f and g are inverses. Hence, f is bijective. This proves that $|A| = |B|$. $\square$

---

36. Prove that $[1, 5]$ has the same cardinality as $[-2, 6]$ by constructing a bijection from $[1, 5]$ to $[-2, 6]$.

Define $f : [1, 5] \to [-2, 6]$ by

$$f(x) = 2x - 4.$$

First, I have to show that f takes $[1, 5]$ into $[-2, 6]$. Suppose that $x \in [1, 5]$, so $1 \leq x \leq 5$. Then

$$2 \leq 2x \leq 10, \quad \text{so} \quad -2 \leq 2x - 4 \leq 6.$$

Thus, $f(x) \in [-2, 6]$.

Next, I'll show that f is bijective. I'll do this by constructing the inverse. Set $y = 2x - 4$. Swapping x and y gives $x = 2y - 4$. Solving for y, I get

$$x = 2y - 4, \quad 2y = x + 4, \quad y = \frac{1}{2}(x + 4).$$

Thus, $f^{-1}(x) = \frac{1}{2}(x + 4)$. Note that if $x \in [-2, 6]$, then $-2 \le x \le 6$. Hence,

$$2 \le x + 4 \le 10, \quad 1 \le \frac{1}{2}(x + 4) \le 5.$$

Thus, $f^{-1}(x) \in [1, 5]$, and f^{-1} takes $[-2, 6]$ into $[1, 5]$.
Check that the functions *are* inverses:

$$f\left(f^{-1}(x)\right) = f\left(\frac{1}{2}(x + 4)\right) = 2 \cdot \frac{1}{2}(x + 4) - 4 = x + 4 - 4 = x,$$

$$f^{-1}\left(f(x)\right) = f^{-1}(2x - 4) = \frac{1}{2}((2x - 4) + 4) = \frac{1}{2}(2x) = x.$$

Thus, f and f^{-1} are inverses, f is bijective, that $||[1, 5]|| = ||[-2, 6]||$. $\square$

---

37. Prove that $[-3, 5)$ has the same cardinality as $(7, 23]$ by constructing a bijection from $[-3, 5)$ to $(7, 23]$.

Define $f : [-3, 5) \to (7, 23]$ by
$$f(x) = -2x + 17.$$

Note that if $x \in (-3, 5]$, then
$$-3 < x \le 5$$
$$6 > -2x \ge -10$$
$$23 > -2x + 17 \ge 7$$
$$23 > f(x) \ge 7$$

Hence, $f(x) \in (7, 23]$.
Define $g : (7, 23] \to [-3, 5)$ by
$$g(x) = -\frac{1}{2}(x - 17).$$

If $x \in (7, 23]$, then
$$7 < x \le 23$$
$$-10 < x - 17 \le 6$$
$$5 > -\frac{1}{2}(x - 17) \ge -3$$
$$5 > g(x) \ge -3$$

Hence, $g(x) \in [-3, 5)$.
I'll check that f and g are inverses.

$$f[g(x)] = f\left(-\frac{1}{2}(x - 17)\right) = (-2) \cdot -\frac{1}{2}(x - 17) + 17 = (x - 17) + 17 = x.$$

$$g[f(x)] = g(-2x + 17) = -\frac{1}{2}\left[(-2x + 17) - 17\right] = -\frac{1}{2}(-2x) = x.$$

Hence, f and g are inverses. Therefore, f is bijective. Thus, $||[-3, 5)|| = |(7, 23]|$. $\square$

A very dangerous state of mind: thinking one understands. - Paul Valéry