

PS1-1

Set-builder to roster notation.

- $\{x : x \text{ is a multiple of 7 and } 0 < x < 50\}$.
Solution. $\{7, 14, 21, 28, 35, 42, 49\}$.
- $\{x + y : x \in \mathbb{N}, y \in \mathbb{N}, \text{ and } xy = 12\}$.
Solution. $\{7, 8, 13\}$.
- $\{S : S \subseteq \{1, 2, 3, 4\} \text{ and } |S| \text{ is odd}\}$.
Solution. $\{\{1\}, \{2\}, \{3\}, \{4\}, \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}\}$.

PS1-2^{HW}

More set-builder to roster notation.

- $\{x^3 : x \in \mathbb{Z} \text{ and } x^2 < 20\}$ [2 points]
Solution. $\{-64, -27, -8, -1, 0, 1, 8, 27, 64\}$.
- $\{x \in \mathbb{R} : x = x^2\}$. [2 points]
Solution. $\{0, 1\}$.
- $\{S : \{1, 2\} \subseteq S \subseteq \{1, 2, 3, 4\}\}$ [2 points]
Solution. $\{\{1, 2\}, \{1, 2, 3\}, \{1, 2, 4\}, \{1, 2, 3, 4\}\}$.
- $\{S \subseteq \{1, 2, 3, 4\} : S \text{ is disjoint from } \{2, 3\}\}$ [2 points]
Solution. $\{\emptyset, \{1\}, \{4\}, \{1, 4\}\}$.

PS1-3

Let $A = \{1, 2, 3, 4, 5, 6\}$, $B = \{2, 4, 6, 8, 10\}$, and $C = \{0, 1, 5, 6, 9\}$.

- What is $A \cup B$? What is $(A \cup B) \cup C$?
Solution. $A \cup B = \{1, 2, 3, 4, 5, 6, 8, 10\}$; $(A \cup B) \cup C = \{0, 1, 2, 3, 4, 5, 6, 8, 9, 10\}$.
- What is $B \cup C$? What is $A \cup (B \cup C)$?
Solution. $B \cup C = \{0, 1, 2, 4, 5, 6, 8, 9, 10\}$; $A \cup (B \cup C) = \{0, 1, 2, 3, 4, 5, 6, 8, 9, 10\}$.
- What is $A \cap B \cap C$?
Solution. $\{6\}$.
- Verify by direct computation that $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.
Solution. We computed $A \cup B$ above. Using that, $(A \cup B) \cap C = \{1, 5, 6\}$.
Further, $A \cap C = \{1, 5, 6\}$ and $B \cap C = \{6\}$. So, $(A \cap C) \cup (B \cap C) = \{1, 5, 6\}$.
Hence, $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.
- What is $A - B$? What is $B - C$?
Solution. $A - B = \{1, 3, 5\}$; $B - C = \{2, 4, 8, 10\}$.
- What is $(A - B) - C$? What is $A - (B - C)$?
Solution. $(A - B) - C = \{3\}$; $A - (B - C) = \{1, 3, 5, 6\}$.
- Verify by direct computation that $(A - B) - C = A - (B \cup C)$.
Solution. We already know $(A - B) - C = \{3\}$.
Further, $B \cup C = \{0, 1, 2, 4, 5, 6, 8, 9, 10\}$ and so, $A - (B \cup C) = \{3\}$.
Hence, $(A - B) - C = A - (B \cup C)$.
- Verify by direct computation that $A - (B - C) = (A - B) \cup (A \cap B \cap C)$.
Solution. We already know $A - (B - C) = \{1, 3, 5, 6\}$.
Further, $A - B = \{1, 3, 5\}$ and $A \cap B \cap C = \{6\}$. So, $(A - B) \cup (A \cap B \cap C) = \{1, 3, 5, 6\}$.
Hence, $A - (B - C) = (A - B) \cup (A \cap B \cap C)$.

i. What is $(A \cap B) \times (B - C)$?

Solution. $\{(2, 2), (2, 4), (2, 8), (2, 10), (4, 2), (4, 4), (4, 8), (4, 10), (6, 2), (6, 4), (6, 8), (6, 10)\}$.

j. Verify by direct computation that $A \cup B \cup C = (A - B) \cup (B - C) \cup (C - A) \cup (A \cap B \cap C)$.

Solution. We already computed $A \cup B \cup C = \{0, 1, 2, 3, 4, 5, 6, 8, 9, 10\}$ above.

Now, $A - B = \{1, 3, 5\}$; $B - C = \{2, 4, 8, 10\}$; $C - A = \{0, 9\}$; $A \cap B \cap C = \{6\}$.

So, $(A - B) \cup (B - C) \cup (C - A) \cup (A \cap B \cap C) = \{0, 1, 2, 3, 4, 5, 6, 8, 9, 10\}$.

Hence, $A \cup B \cup C = (A - B) \cup (B - C) \cup (C - A) \cup (A \cap B \cap C)$.

PS1-4

Let A , B , and C be arbitrary sets. Prove each of the following.

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

Solution. Consider an arbitrary element $(x, y) \in A \times (B \cup C)$.

Then $x \in A$ and $y \in B \cup C$, i.e., $y \in B$ or $y \in C$. Thus, $(x, y) \in A \times B$ or $(x, y) \in A \times C$.

So, $(x, y) \in (A \times B) \cup (A \times C)$. Hence, $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$ (i)

Again, consider any $(x, y) \in (A \times B) \cup (A \times C)$.

Then $(x, y) \in A \times B$ or $(x, y) \in A \times C$. Thus, $x \in A$ and $y \in B$ or $y \in C$, i.e. $y \in B \cup C$.

So, $(x, y) \in A \times (B \cup C)$. Hence, $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$ (ii)

Thus, from (i) and (ii), $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

b. $(A - C) \cap (C - B) = \emptyset$.

Solution. Consider an arbitrary $x \in A - C$. Then $x \in A$ and $x \notin C$.

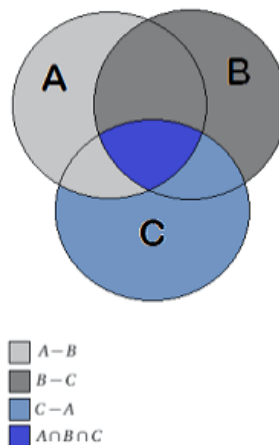
Now, $C - B = \{y : y \in C \text{ and } y \notin B\}$. Thus $x \notin C - B$.

Hence, $(A - C) \cap (C - B) = \emptyset$.

c. $A \cup B \cup C = (A - B) \cup (B - C) \cup (C - A) \cup (A \cap B \cap C)$.

◁ It may help to draw a Venn diagram.

Solution. The following Venn diagram can help us in proving this.



Part (i) Consider any $x \in (A - B) \cup (B - C) \cup (C - A) \cup (A \cap B \cap C)$.

Then $x \in A - B$ or $x \in B - C$ or $x \in C - A$ or $x \in A \cap B \cap C$.

In the first three cases, we have (respectively) $x \in A$ or $x \in B$ or $x \in C$. In the fourth case, we have all three things: $x \in A$, $x \in B$, and $x \in C$.

Thus, in any case, at least one of the following holds: $x \in A$, $x \in B$, or $x \in C$. Hence, $x \in A \cup B \cup C = \text{LHS}$.

This proves that $\text{RHS} \subseteq \text{LHS}$.

Part (ii) Now consider any $x \in A \cup B \cup C$. Then $x \in A$ or $x \in B$ or $x \in C$.

Case 1. x belongs to all three of A , B , and C .

Then, $x \in A \cap B \cap C$. Therefore, $x \in (A - B) \cup (B - C) \cup (C - A) \cup (A \cap B \cap C)$.

Case 2. There is at least one set among A, B , and C to which x does not belong.

Without loss of generality, suppose that $x \notin B$. We now have two subcases.

Case 2.1. x doesn't belong to A .

In this case, $x \notin A$ and $x \notin B$, so we must have $x \in C$. So $x \in C - A$.

Therefore, $x \in (A - B) \cup (B - C) \cup (C - A) \cup (A \cap B \cap C)$.

Case 2.2. x does belong to A .

In this case, $x \in A$ and $x \notin B$, so we must have $x \in A - B$.

Therefore, $x \in (A - B) \cup (B - C) \cup (C - A) \cup (A \cap B \cap C)$.

Thus, in every case, $x \in \text{RHS}$, so $\text{LHS} \subseteq \text{RHS}$.

PS1-5^{HW}

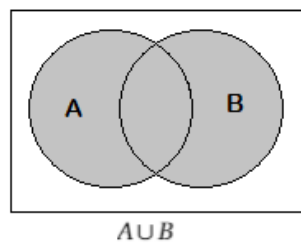
Proofs of set equalities.

- a. Proof that $\overline{A \cup B} = \bar{A} \cap \bar{B}$.

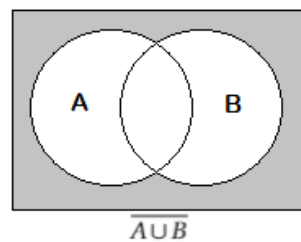
[4 points]

Solution.

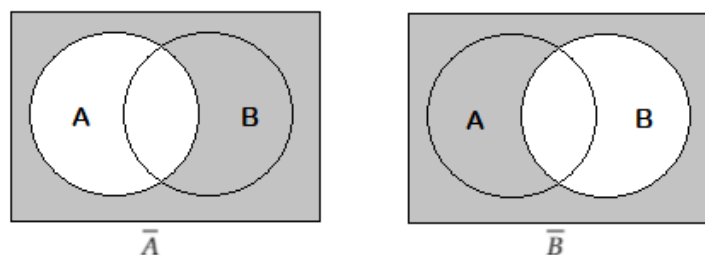
The Venn diagram for $A \cup B$ is given by the following figure:



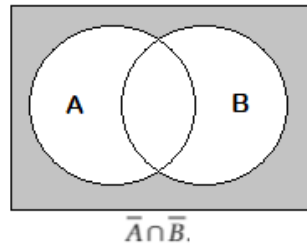
Hence, the Venn diagram for $\overline{A \cup B}$ is:



Again, the Venn diagrams for \bar{A} and \bar{B} are:



Hence, the Venn diagram for $\bar{A} \cap \bar{B}$ is given by:



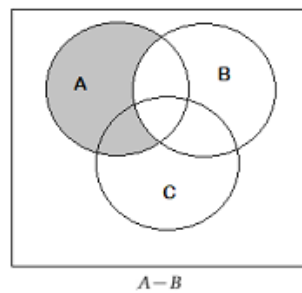
So we see that the diagrams for $\overline{A \cup B}$ and $\bar{A} \cap \bar{B}$ are the same. Hence $\overline{A \cup B} = \bar{A} \cap \bar{B}$

- b. Similarly, prove that $(A - B) - C = (A - C) - (B - C)$.

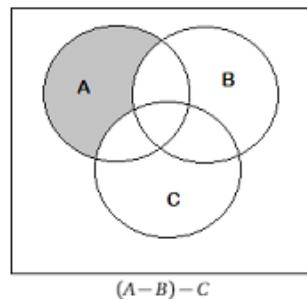
[4 points]

Solution.

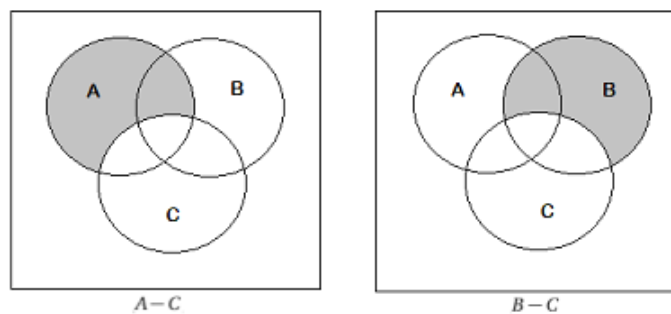
The Venn diagram for $A - B$ is given by:



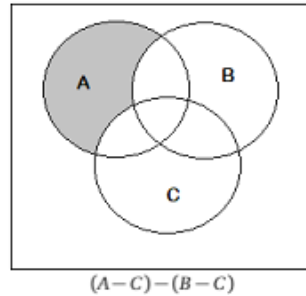
So, the Venn diagram for $(A - B) - C$ is:



Again, the Venn diagrams for $A - C$ and $B - C$ are:



Thus, the Venn diagram for $(A - C) - (B - C)$ is given by:



So we see that the Venn diagrams for $(A - B) - C$ and $(A - C) - (B - C)$ are the same. Hence, $(A - B) - C = (A - C) - (B - C)$.

- c. Algebra-style proof that $(A \cap B) \cup (A \cap \bar{B}) = A$. [4 points]

Solution. Consider an arbitrary $x \in A$.

If $x \in B$, then $x \in A \cap B$.

Otherwise, $x \notin B$, so $x \in \bar{B}$ and so $x \in A \cap \bar{B}$.

Combining the above two conclusions, $x \in (A \cap B) \cup (A \cap \bar{B})$.

Thus, $A \subseteq (A \cap B) \cup (A \cap \bar{B})$ (i)

Now consider an arbitrary $x \in (A \cap B) \cup (A \cap \bar{B})$.

Then $x \in A \cap B$ or $x \in A \cap \bar{B}$.

In the former case, $x \in A$ and $x \in B$. In the latter case, $x \in A$ and $x \in \bar{B}$.

In either case, $x \in A$.

Thus, $(A \cap B) \cup (A \cap \bar{B}) \subseteq A$ (ii)

Combining (i) and (ii), $(A \cap B) \cup (A \cap \bar{B}) = A$.

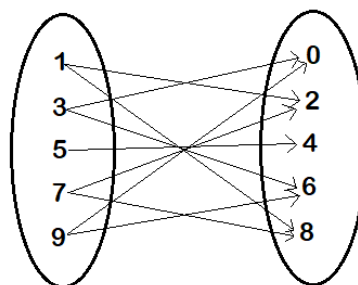
PS1-6^{HW}

The “completes” relation.

[3 points]

Solution. As a set, the relation is $\{(1, 2), (1, 8), (3, 0), (3, 6), (5, 4), (7, 2), (7, 8), (9, 0), (9, 6)\}$.

Below is a pictorial representation.



PS1-7

Are these relations (a) symmetric; (b) transitive?

- a. The relation “divides”, on \mathbb{N} (“ m divides n ” means “ n/m is an integer”).

Solution. This relation is

(a) NOT symmetric [Reason: 1 divides 2, but 2 does not divide 1.]

(b) transitive

- b. The relation “is disjoint from”, on $\mathcal{P}(\mathbb{Z})$.

Solution. This relation is

- (a) symmetric
- (b) NOT transitive [Reason: $\{1\}$ disj from $\{2\}$, and $\{2\}$ disj from $\{1\}$, but $\{1\}$ is not disjoint from $\{1\}$.]

- c. The relation “is no larger than”, on $\mathcal{P}(\mathbb{Z})$. We say that A is no larger than B when one of the following holds:

- A and B are both finite sets, and $|A| \leq |B|$.
- A is a finite set and B is an infinite set.
- A and B are both infinite sets.

Solution. This relation is:

- (a) NOT symmetric [Reason: $(\{1\}, \{1, 2\}) \in$ “is no larger than”, but $(\{1, 2\}, \{1\}) \notin$ “is no larger than”.]
- (b) transitive

PS1-8^{HW}

Same instructions as the previous problem, **PS1-7**.

- a. The relation “is a subset of”, on $\mathcal{P}(\mathbb{Z})$. [4 points]

Solution. This relation is:

- (a) NOT symmetric [Reason: $\{1\}$ is a subset of $\{1, 2\}$ but $\{1, 2\}$ is not a subset of $\{1\}$.]
- (b) transitive

- b. $\{(m, n) \in \mathbb{N} \times \mathbb{N} : \text{the sum of the digits of } m \text{ equals the sum of the digits of } n\}$. [4 points]

Solution. This relation is (a) symmetric, (b) transitive.

- c. The relation “overlapped” on the set of all US presidents. [4 points]

Solution. This relation is:

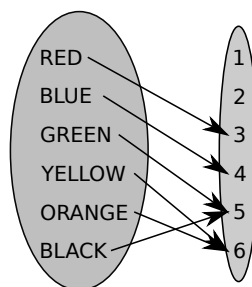
- (a) symmetric
- (b) NOT transitive [Reason: George Washington overlapped Thomas Jefferson and Thomas Jefferson overlapped Abraham Lincoln, but Washington did not overlap Lincoln.]

PS1-9

Let $S = \{\text{“RED”}, \text{“BLUE”}, \text{“GREEN”}, \text{“YELLOW”}, \text{“ORANGE”}, \text{“BLACK”}\}$ and $T = \{1, 2, 3, 4, 5, 6\}$. Consider the function $\text{len} : S \rightarrow T$ given by $\text{len}(s) = \text{the length of the string } s$ (as in the Python programming language).

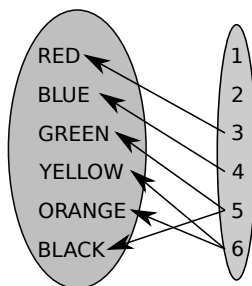
- a. Describe the “len” function pictorially, using arrows, as done in class.

Solution.



- b. Reverse the directions of all the arrows in your picture. Does this new picture represent a function $g : T \rightarrow S$. If not, why not?

Solution.



No: functions associate exactly one value (output) with each argument (input). In the picture above, there are multiple arrows leaving elements 5 and 6. Also, there are no arrows leaving elements 1 and 2.

PS1-10 Prove: if $S_1, S_2 \subseteq A$, then $f(S_1 \cup S_2) = f(S_1) \cup f(S_2)$.

Solution. Consider an arbitrary element $y \in f(S_1 \cup S_2)$.

Then $y = f(x)$ for some $x \in S_1 \cup S_2$, i.e., $x \in S_1$ or $x \in S_2$. In the former case, $y = f(x) \in f(S_1)$. In the latter case, $y = f(x) \in f(S_2)$. Overall, $y \in f(S_1) \cup f(S_2)$. Thus, $\text{LHS} \subseteq \text{RHS}$.

Next, consider an arbitrary element $y \in f(S_1) \cup f(S_2)$. Then $y \in f(S_1)$ or $y \in f(S_2)$.

In the former case, $y = f(x)$ for some $x \in S_1 \subseteq S_1 \cup S_2$. In the latter case, $y = f(x)$ for some $x \in S_2 \subseteq S_1 \cup S_2$. Thus, in each case, $y \in f(S_1 \cup S_2)$. Thus, $\text{RHS} \subseteq \text{LHS}$.

PS1-11

The functions $f, g: \mathbb{R} \rightarrow \mathbb{R}$ are given by the formulas $f(x) = x^2 + 1$ and $g(x) = x + 2$. Find $f \circ g$ and $g \circ f$.

Solution. $(f \circ g)(x) = x^2 + 4x + 5$; $(g \circ f)(x) = x^2 + 3$

PS1-12^{HW}

The functions $f, \text{id}: \mathbb{R} \rightarrow \mathbb{R}$ are given by the formulas $f(x) = x^3 + 7$ and $\text{id}(x) = x$.

a. Find a function $g: \mathbb{R} \rightarrow \mathbb{R}$ such that $f \circ g = \text{id}$. [2 points]

Solution. Pick an arbitrary $x \in \mathbb{R}$ and let $y = g(x)$.

Then $f(y) = f(g(x)) = x$, since $f \circ g = \text{id}$. Thus, $y^3 + 7 = x$, which implies $y = \sqrt[3]{x-7}$.

We conclude that the required function $g: \mathbb{R} \rightarrow \mathbb{R}$ is given by $g(x) = \sqrt[3]{x-7}$.

(Note that this g is a well-defined function from \mathbb{R} to \mathbb{R} since every real number has a unique real cube root.)

b. For the function g you found above, find $g \circ f$. [2 points]

Solution. We compute: $(g \circ f)(x) = g(f(x)) = \sqrt[3]{f(x)-7} = \sqrt[3]{x^3+7-7} = x$.

Hence, $g \circ f = \text{id}$.

Solution for PS2-1.

- a. $\forall y \in B$, because f is surjective, $\exists x \in A$, such that $f(x) = y$, i.e. $(y, x) \in f^{-1}$. And because f is injective, there is only one $x \in A$, such that $f(x) = y$, i.e. $(y, x) \in f^{-1}$. In conclusion, $\forall y \in B$, there is one and only one $x \in A$, such that $(y, x) \in f^{-1}$. Therefore, f^{-1} is a function.
- b. **First**, we will prove that f is surjective. That is, we will prove $\forall y \in B \exists x \in A (f(x) = y)$.
Consider an arbitrary $y \in B$.
Since f^{-1} is a function, according to the definition of a function, $\exists x \in A ((y, x) \in f^{-1})$.
By the definition of the relation f^{-1} , this means $f(x) = y$.
Second, we will prove that f is injective. That is, we will prove $\forall x_1, x_2 \in A (f(x_1) = f(x_2) \implies x_1 = x_2)$.
Consider arbitrary elements $x_1, x_2 \in A$. Suppose that $f(x_1) = f(x_2)$. We will now show that $x_1 = x_2$.
Define $y = f(x_1) = f(x_2)$.
By the definition of the relation f^{-1} , we have $(y, x_1) \in f^{-1}$ and $(y, x_2) \in f^{-1}$.
Since f^{-1} is a function, for each y there must be at most one x so that $(y, x) \in f^{-1}$. It follows that $x_1 = x_2$.

Solution for PS2-2.

- a. Consider an arbitrary element $y \in f(S_1 \cup S_2)$. Then $y = f(x)$ for some $x \in S_1 \cup S_2$, i.e. $x \in S_1$ or $x \in S_2$. If $x \in S_1$, $f(x) = y \in f(S_1)$, or, if $x \in S_2$, $f(x) = y \in f(S_2)$. So, in any case, $y \in f(S_1)$ or $y \in f(S_2)$. Hence $y \in f(S_1) \cup f(S_2)$. Thus, $f(S_1 \cup S_2) \subseteq f(S_1) \cup f(S_2) \dots$
Again, consider an arbitrary element $y \in f(S_1) \cup f(S_2)$. Then $y \in f(S_1)$ or $y \in f(S_2)$. If $y \in f(S_1)$, then $y = f(x)$ for some $x \in S_1$, or, if $y \in f(S_2)$, then $y = f(x)$ for some $x \in S_2$. So, in any case, $y = f(x)$ for some $x \in S_1$ or $x \in S_2$, i.e. $x \in S_1 \cup S_2$. Hence, $y \in f(S_1 \cup S_2)$. Thus, $f(S_1) \cup f(S_2) \subseteq f(S_1 \cup S_2) \dots$
- b. Consider an arbitrary element $x \in f^{-1}(T_1 \cup T_2)$. Then $f(x) \in T_1 \cup T_2$, i.e. $f(x) \in T_1$ or $f(x) \in T_2$. If $f(x) \in T_1$, $x \in f^{-1}(T_1)$, or, if $f(x) \in T_2$, $x \in f^{-1}(T_2)$. So, in any case, $x \in f^{-1}(T_1)$ or $x \in f^{-1}(T_2)$ i.e. $x \in f^{-1}(T_1) \cup f^{-1}(T_2)$. Thus, $f^{-1}(T_1 \cup T_2) \subseteq f^{-1}(T_1) \cup f^{-1}(T_2) \dots$
Again, consider an arbitrary element $x \in f^{-1}(T_1) \cup f^{-1}(T_2)$. Then $x \in f^{-1}(T_1)$ or $x \in f^{-1}(T_2)$. If $x \in f^{-1}(T_1)$, then $f(x) \in T_1$, or, if $x \in f^{-1}(T_2)$, then $f(x) \in T_2$. So, in any case, $f(x) \in T_1$ or $f(x) \in T_2$, i.e. $f(x) \in T_1 \cup T_2$. Hence, $x \in f^{-1}(T_1 \cup T_2)$. Thus, $f^{-1}(T_1) \cup f^{-1}(T_2) \subseteq f^{-1}(T_1 \cup T_2) \dots$

Solution for PS2-3.

- a. To prove $f \circ g$ is injective, assume x_1, x_2 are such that $f(g(x_1)) = f(g(x_2))$; since f is injective, it follows $g(x_1) = g(x_2)$, and then since g is injective, $x_1 = x_2$.
To prove surjectivity, consider any $x \in C$; then since f is surjective, $\exists y \in B$ s.t. $f(y) = x$. Next, since g is surjective, $\exists z \in A$ s.t. $g(z) = y$. Overall, we've found an element $z \in A$ s.t. $(f \circ g)(z) = f(g(z)) = x$.
- b. To show that $g^{-1} \circ f^{-1}$ is the inverse of $f \circ g$ (already knowing that such an inverse exists), it suffices to verify that $(f \circ g)((g^{-1} \circ f^{-1})(x)) = x$ for all $x \in C$, i.e., that $g^{-1} \circ f^{-1}$ behaves identically to the actual inverse on its domain. Verification follows since

$$(f \circ g)((g^{-1} \circ f^{-1})(x)) = f(g(g^{-1}(f^{-1}(x)))) = f(f^{-1}(x)) = x.$$

Solution for PS2-4.

To solve this problem, it will help to prove a little lemma first.

Lemma 1. Let S and C be sets with $C \subseteq S$. Then $S - (S - C) = C$.

Proof. Using the definitions of the basic set operations,

$$\begin{aligned}
 S - (S - C) &= \{x : x \in S \wedge x \notin S - C\} &> \text{definition of set difference} \\
 &= \{x : x \in S \wedge \neg(x \in S \wedge x \notin C)\} &> \text{definition of set difference} \\
 &= \{x : x \in S \wedge (x \notin S \vee x \in C)\} &> \text{de Morgan's law} \\
 &= \{x : x \in S \wedge x \in C\} \\
 &= S \cap C &> \text{definition of intersection} \\
 &= C. &> \text{because } C \subseteq S \quad \square
 \end{aligned}$$

First, we will prove that g is surjective. That is, we will prove $\forall B \subseteq S \exists A \subseteq S (g(A) = B)$.

Consider an arbitrary $B \subseteq S$.

Define $A := S - B$. Then, by Lemma 1, $g(A) = S - (S - B) = B$.

Thus, we have proved the existence of an A such that $g(A) = B$.

Second, we will prove that g is injective. That is, we will prove $\forall A_1, A_2 \subseteq S (g(A_1) = g(A_2) \implies A_1 = A_2)$.

Consider arbitrary $A_1, A_2 \subseteq S$. Suppose that $g(A_1) = g(A_2)$. We will now show that $A_1 = A_2$.

We have

$$\begin{aligned}
 A_1 &= S - (S - A_1) &> \text{by Lemma 1} \\
 &= S - g(A_1) &> \text{definition of } g \\
 &= S - g(A_2) &> \text{by our assumption} \\
 &= S - (S - A_2) &> \text{definition of } g \\
 &= A_2. &> \text{by Lemma 1}
 \end{aligned}$$

Solution for PS2-5. Because S is nonempty, $\exists a \in S$. We construct h as follows:

$$h(A) = \begin{cases} A \cup \{a\}, & \text{if } a \notin A \\ A - \{a\}, & \text{if } a \in A. \end{cases}$$

Note that $|h(A)| = |A| \pm 1$. So, if $A \in \mathcal{P}^{\text{odd}}(S)$, then $h(A) \in \mathcal{P}^{\text{even}}(S)$. Thus, h is indeed a *function* of the form $h: \mathcal{P}^{\text{odd}}(S) \rightarrow \mathcal{P}^{\text{even}}(S)$.

Now, we prove that h is a *bijection*. As usual, the proof has two parts.

First, we prove that h is surjective.

Consider an arbitrary $B \in \mathcal{P}^{\text{even}}(S)$. Either $a \in B$ or $a \notin B$.

If $a \in B$, then $B - \{a\} \in \mathcal{P}^{\text{odd}}(S)$ and $h(B - \{a\}) = (B - \{a\}) \cup \{a\} = B$.

If $a \notin B$, then $B \cup \{a\} \in \mathcal{P}^{\text{odd}}(S)$ and $h(B \cup \{a\}) = (B \cup \{a\}) - \{a\} = B$.

We have shown that in either case, $\exists A \in \mathcal{P}^{\text{odd}}(S)$ such that $h(A) = B$. Therefore, h is surjective.

Second, we prove that h is injective.

Consider arbitrary sets $A_1, A_2 \in \mathcal{P}^{\text{odd}}(S)$ and suppose that $h(A_1) = h(A_2)$. We will prove that $A_1 = A_2$.

For this, we will show that $A_1 \subseteq A_2$ and $A_2 \subseteq A_1$. Actually, it suffices to prove the first of these; the second then follows by symmetry.

So, consider an arbitrary $x \in A_1$. Either $x \neq a$ or $x = a$.

- If $x \neq a$, then $x \in A_1 \cup \{a\}$ and $x \in A_1 - \{a\}$. Examining the definition of h , we see that $x \in h(A_1)$. By our assumption, $x \in h(A_2)$. So, either $x \in A_2 \cup \{a\}$ or $x \in A_2 - \{a\}$. Using $x \neq a$ again, we have $x \in A_2$.
- If $x = a$, then $a \in A_1$ and so $h(A_1) = A_1 - \{a\}$. So, $a \notin h(A_1)$. By our assumption, $a \notin h(A_2)$. Examining the definition of h , we get $h(A_2) = A_2 - \{a\}$ and $a \in A_2$. Since $x = a$, we have $x \in A_2$.

We have shown that in either case, $x \in A_2$. Thus $A_1 \subseteq A_2$. As observed earlier, this proves that h is injective.

Alternative proof of bijectivity. We could instead appeal to h^{-1} . We will show that h is its own inverse! That is, $h^{-1} = h$. Since h is a function, this means that h^{-1} is a function, which implies that h is a bijection.

To prove that $h^{-1} = h$, we will show that $\forall A \in \mathcal{P}^{\text{odd}}(S)$ we have $h(h(A)) = A$. For this, consider an arbitrary $A \in \mathcal{P}^{\text{odd}}(S)$. Either $a \in A$ or $a \notin A$.

- If $a \in A$, then $h(h(A)) = h(A - \{a\}) = (A - \{a\}) \cup \{a\} = A$.
- If $a \notin A$, then $h(h(A)) = h(A \cup \{a\}) = (A \cup \{a\}) - \{a\} = A$.

In either case, $h(h(A)) = A$, and we are done.

Solution for PS2-6.

- Suppose that $|A| = m$. Let a_1, \dots, a_m be the elements of A . Since f is a surjection, $(f(a_1), \dots, f(a_m))$ is a listing of *all* the elements of B , possibly with some repetitions. Therefore $|B| \leq m$.
- Since g is an injection, the elements in the list $(g(a_1), \dots, g(a_m))$ are *distinct*. Since B contains at least these m distinct elements, $|B| \geq m$.
- Combining parts (a) and (b), we get $|A| = |B| = m$.
Now, if $(f(a_1), \dots, f(a_m))$ has repetitions, then $|B| < m$, a contradiction. So $f(a_1), \dots, f(a_m)$ are all distinct and hence f is an injection. Therefore, f is a bijection.
Again, if the list $(g(a_1), \dots, g(a_m))$ does not cover all elements of B , then $|B| > m$, a contradiction. Hence, $(g(a_1), \dots, g(a_m))$ is a listing of all elements of B and so g is a surjection. Therefore, g is a bijection.

Solution for PS2-7. Let

$$g(n) = \begin{cases} -2n, & \text{if } n \leq 0 \\ 2n-1, & \text{if } n > 0 \end{cases}$$

To verify that $f \circ g = \text{id}_{\mathbb{Z}}$, consider the cases where an input n is positive/negative.

$$\text{For } n \geq 0, \quad f(g(n)) = f(2n-1) = (2n-1+1)/2 = n.$$

$$\text{For } n < 0, \quad f(g(n)) = f(-2n) = -2n/2 = n.$$

To verify that $g \circ f = \text{id}_{\mathbb{N}}$, consider the cases where an input m is even/odd.

$$\text{When } m \text{ is even, } g(f(m)) = g(-m/2) = -2(-m)/2 = m,$$

$$\text{When } m \text{ is odd, } g(f(m)) = g((m+1)/2) = 2 \cdot ((m+1)/2) - 1 = (m+1) - 1 = m.$$

When $f \circ g = \text{id}_{\mathbb{Z}}$ (we say that f has g as a right inverse), f is surjective. This is because for each $x \in \mathbb{Z}$, we have the element $g(x) \in \mathbb{N}$ for which $f(g(x)) = \text{id}_{\mathbb{Z}}(x) = x$.

When $g \circ f = \text{id}_{\mathbb{N}}$ (we say that f has g as a left inverse), f is injective. This is because for all $x, x' \in \mathbb{N}$, if $f(x) = f(x')$, then applying g to both sides, $g(f(x)) = g(f(x'))$, so $x = x'$.

When both conditions hold, f is surjective and injective, hence bijective.

Solution for PS2-8. As $f(A)$ is a subset of \mathbb{N} , $f(A)$ is countable. Letting g be f with codomain restricted to $f(A)$, g is an injection (just like f is), and a surjection (since its codomain is its range). As g is a bijection, A is countable iff $g(A)$ is, and since $g(A) = f(A)$ is a subset of \mathbb{N} , it follows both $g(A)$ and A are countable.

Solution for PS2-9. Consider $f(x, y) = (x + y + 1)^2 + (x - y)$, which maps pairs in $\mathbb{N} \times \mathbb{N}$ to the set of odd positive integers. It is only necessary to show that f is injective, as then by ?? it would follow $\mathbb{N} \times \mathbb{N}$ is countable.

To do this, assume to the contrary that there are two distinct pairs (x, y) and (x', y') in $\mathbb{N} \times \mathbb{N}$, for which $f(x, y) = f(x', y')$. Expanding the definition of f and rearranging yields $(x + y + 1)^2 - (x' + y' + 1)^2 = (x - y) - (x' - y')$. Factoring the left hand side gives

$$(x - x' + y - y')(x + x' + y + y' + 2) = (x - x' - y + y'). \quad (1)$$

Since x, x', y, y' are all nonnegative, $(x + x' + y + y' + 2) > (x - x' - y + y')$, so that in Eq. 1 either $(x - x' + y - y')$ is zero, or else the left side has a larger absolute value than the right, breaking the equality. Consequently,

$$\begin{aligned} x - x' + y - y' &= 0, \text{ and} \\ x - x' - y + y' &= 0. \end{aligned}$$

Solving this linear system gives $x = x'$ and $y = y'$, contradicting the initial assumption that $(x, y) \neq (x', y')$.

Solution for PS2-10. Define the *weight* of a finite-length list

$$w((a_1, \dots, a_\ell)) = \ell + \sum_{i=1}^{\ell} |a_i|.$$

There are finitely many lists with a given weight. Since list weights are in \mathbb{N} , we can enumerate all elements of \mathbb{N}^* by first listing the elements of weight 0, then those of weight 1, and so on (each element $e \in \mathbb{N}^*$ will be in the $w(e)$ th enumerated group). As \mathbb{N}^* can be enumerated, it is countable.

Solution for PS3-1.

- $(2m) + (2n) = 2(m + n)$, which is even.
- $(2m + 1) + (2n + 1) = 2(m + n + 1)$, which is even.
- $(2m + 1) + (2n) = 2(m + n) + 1$, which is odd.
- $(2m) \cdot (n) = 2(mn)$, which is even.
- $(2m + 1) \cdot (2n + 1) = 2(2mn + m + n) + 1$, which is odd.

Solution for PS3-2.

- Since $3^b = 3^d$, we can simplify the equation to $2^a = 2^c$, which makes $a = c$. Thus, $(a, b) = (c, d)$.
- Rearranging the equation, $2^{a-c} = 3^{d-b}$. So let $p = a - c, q = d - b$. By assumption, $q > 0$, so $q \in \mathbb{N}$.
- Each time we multiply an odd integer by three, the result must be odd. Since 3^q is obtained by starting with one (an odd integer) and multiplying by three q times, the final result must be odd.
- We have that $2^p = 3^q$, which is odd. If $p < 0$, $2p$ is not even an integer. If $p > 0$, $2^p = 2 \times 2^{p-1}$, which is two times an integer, so it is even. The only way that 2^p can be odd is if $p = 0$.
- Since $p = a - c = 0$, we have $a = c$. Thus, $2^a = 2^c$ and the original equation simplifies to $3^b = 3^d$, which implies $b = d$. Thus, $(a, b) = (c, d)$.
- We have shown that $f(a, b) = f(c, d) \implies (a, b) = (c, d)$, so by definition, f is injective.

Solution for PS3-3. If A is countable, then we know there exists an injection $g : A \rightarrow \mathbb{N}$ by the definition of countability. If B is a subset of A we can define a function $f : B \rightarrow \mathbb{N}$ with $f(x) = g(x)$. To prove that B is countable we will show that f is an injection.

Let x_1 and x_2 be any two elements of B . If $f(x_1) = f(x_2)$, then $g(x_1) = g(x_2)$. But g is injective, so this implies $x_1 = x_2$. Therefore f is also injective.

Solution for PS3-4.

- If A and B are both countable then there are injections $g : A \rightarrow \mathbb{N}$ and $h : B \rightarrow \mathbb{N}$. We can define a function $f : (A \cup B) \rightarrow \mathbb{N}$ by the following:

$$f(x) = \begin{cases} 2g(x) + 1, & \text{if } x \in A, \\ 2h(x), & \text{otherwise (i.e., } x \in (B - A)). \end{cases}$$

We can show this function is an injection. Let x_1, x_2 be elements of $A \cup B$ with $f(x_1) = f(x_2)$. Either $f(x_1)$ will be odd, or it will be even.

If $f(x_1)$ is odd, then $f(x_1) = 2g(x_1) + 1$ (note that $2h(x)$ can never be odd because $h(x)$ is a natural number). Similarly, $f(x_2)$ is odd (it is equal to $f(x_1)$ after all) so we have $f(x_2) = 2g(x_2) + 1$. This means $2g(x_1) + 1 = 2g(x_2) + 1$ which implies $g(x_1) = g(x_2)$. But we know g is an injective function, so $x_1 = x_2$.

If $f(x_1)$ is even, then $f(x_1) = 2h(x_1)$ (again note that $2g(x) + 1$ can never be even because $g(x)$ is a natural number). We also know $f(x_2)$ is even so it equals $2h(x_2)$, therefore $2h(x_1) = 2h(x_2)$. This in turn implies $h(x_1) = h(x_2)$. We know h is an injection so $x_1 = x_2$.

So in either case we know if $f(x_1) = f(x_2)$ then $x_1 = x_2$. Therefore f is an injective function from $A \cup B$ to \mathbb{N} and there $A \cup B$ must be countable.

- If A and B are both countable then there are injections $g : A \rightarrow \mathbb{N}$ and $h : B \rightarrow \mathbb{N}$. As in part a, we can define a function $f : (A \times B) \rightarrow \mathbb{N}$ by $f(a, b) = 2^{g(a)}3^{h(b)}$. As before we can prove this is an injection.
Let $f(a_1, b_1) = f(a_2, b_2)$, so $2^{g(a_1)}3^{h(b_1)} = 2^{g(a_2)}3^{h(b_2)}$. From the uniqueness of prime factorization we know that this implies $g(a_1) = g(a_2)$ and $h(a_1) = h(a_2)$. But g and h are both injections so $a_1 = a_2$ and $b_1 = b_2$. This means the ordered pairs (a_1, b_1) and (a_2, b_2) are equal to each other. Therefore f is an injective function and $A \times B$ is countable.

Solution for PS3-5. Let's repeatedly invoke the fact " A and B countable $\implies A \times B$ countable".

Using it with $A = \mathbb{N}$ and $B = \mathbb{N}$ tells us that $\mathbb{N} \times \mathbb{N}$ is countable.

Now, using it with $A = \mathbb{N} \times \mathbb{N}$ and $B = \mathbb{N}$ tells us that $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ is countable.

Next, using it with $A = \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ and $B = \mathbb{N}$ tells us that $\mathbb{N} \times \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ is countable.

Finally, using it with $A = \mathbb{N} \times \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ and $B = \mathbb{N}$ tells us that $\mathbb{N} \times \mathbb{N} \times \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ is countable.

Solution for PS3-6. Since A is infinite, there exists some element $a_0 \in A$.

Since A is infinite, it has at least two elements, so there exists some element $a_1 \in A$ distinct from a_0 .

Since A is infinite, it has at least three elements, so there exists some element $a_3 \in A$ distinct from a_0, a_1 .

Since A is infinite, it has at least four elements, so there exists some element $a_4 \in A$ distinct from a_0, a_1, a_2 .

Proceeding in this fashion, for each $n \in \mathbb{N}$ we have an element a_n distinct from all elements a_m where $m < n$.

Now define a function $f : A \rightarrow \mathbb{N}$ as follows.

$$f(x) = \begin{cases} n, & \text{if } x = a_n \text{ for some } n \in \mathbb{N}, \\ 0, & \text{otherwise (i.e., } x \text{ is not in the list } (a_0, a_1, a_2, \dots)). \end{cases}$$

This function is surjective because, given any $n \in \mathbb{N}$, there exists the element $a_n \in A$ for which $f(a_n) = n$.

Solution for PS3-7. Since S is finite, given any particular length ℓ , there are only a finite number of ℓ -length strings in S^* . (To be precise, there are $|S|^\ell$ such strings, though we don't need this fact.) Therefore, we can list all the elements of S^* as follows:

empty string, followed by
all strings of length 1 in some arbitrary order, followed by
all strings of length 2 in some arbitrary order, followed by
all strings of length 3 in some arbitrary order, followed by

This listing implicitly defines a bijection $f : \mathbb{N} \rightarrow S^*$, proving that S^* is countable.

Solution for PS3-8. Every Python program is just a string over a certain alphabet: say, the alphabet of all Unicode characters.

Thus, the set of all Python programs is a subset of a countable set, so it is itself a countable set.

Solution for PS3-9. Let $I = (0, 1)$. We define $f(x, y)$ as follows, for $(x, y) \in I \times I$. Let

$$\begin{aligned} x &= 0.a_1a_2a_3\cdots, \\ y &= 0.b_1b_2b_3\cdots \end{aligned}$$

be the unique decimal representations of x and y , as defined in class. Now construct the number

$$z = 0.a_1b_1a_2b_2a_3b_3\cdots.$$

The sequence of digits in this definition of z has infinitely many non-9s, so it is a legit decimal representation of a real number in I . Set $f(x, y) = z$.

Students: You should write up a formal proof that f is indeed an injection.

Solution for PS3-10. Consider the function $g : (0, 1] \rightarrow (0, 1)$ defined by:

$$g(x) = \begin{cases} \frac{x}{2}, & \text{if } \exists n \in \mathbb{Z} \text{ such that } x = 2^{-n}, \\ x, & \text{otherwise.} \end{cases}$$

To prove this is a bijection we will construct an inverse function. Define $h(x) : (0, 1) \rightarrow (0, 1]$ to be:

$$h(x) = \begin{cases} 2x, & \text{if } \exists n \in \mathbb{Z} \text{ such that } x = 2^{-n}, \\ x, & \text{otherwise.} \end{cases}$$

To prove that g and h are inverses of each other (which, in turn, shows that g is a bijection) we must show that $g \circ h = \text{id}_{(0,1)}$ and $h \circ g = \text{id}_{(0,1]}$.

To show $g \circ h = \text{id}_{(0,1)}$, let x be any element of $(0, 1)$. We must show $g(h(x)) = x$. If $x = 2^{-n}$ for some integer n , then $g(h(x)) = g(2x)$, but $2x = 2^{1-n}$ and $(n-1)$ is an integer, so $g(2x) = \frac{2x}{2} = x$. If instead $x \neq 2^{-n}$ for every integer n , we have $g(h(x)) = g(x) = x$. In either case $g(h(x)) = x$ so $g \circ h = \text{id}_{(0,1)}$.

Similarly To show $h \circ g = \text{id}_{(0,1]}$, we let $x \in (0, 1]$. Once again we have two cases either $x = 2^{-n}$ for some integer n , or $x \neq 2^{-n}$ for every integer n . In the former case, $h(g(x)) = h(\frac{x}{2})$. However $\frac{x}{2} = 2^{-(n+1)}$ and $(n+1)$ is an integer so $h(\frac{x}{2}) = 2 \cdot \frac{x}{2} = x$. In the latter case $h(g(x)) = h(x) = x$. Therefore $h(g(x))$ is always x and $h \circ g = \text{id}_{(0,1]}$.

So g and h are inverse functions of each other. Because g is a function with an inverse function it must be a bijection.

Solution for PS4-1.

Number	Positive divisors	Prime?
12	1, 2, 3, 4, 6, 12	No
15	1, 3, 5, 15	No
29	1, 29	Yes
64	1, 2, 4, 8, 16, 32, 64	No
72	1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72	No
73	1, 73	Yes
75	1, 3, 5, 15, 25, 75	No

Solution for PS4-2. We claim that $n \in \mathbb{N}^+$ has an odd number of positive divisors iff n is a perfect square. Informally, this is because the positive divisors of n can be grouped into pairs of the form $\{d, n/d\}$, so there must be an even number of such divisors in total *except* when one of these “pairs” is in fact a singleton set, which happens when $d = n/d$ for some d , i.e., $n = d^2$.

Here is the formal proof. Let

$$A = \{d \in \mathbb{N}^+ : d \mid n \text{ and } d < \sqrt{n}\},$$

$$B = \{d \in \mathbb{N}^+ : d \mid n \text{ and } d > \sqrt{n}\},$$

$$D = \{d \in \mathbb{N}^+ : d \mid n\}.$$

The function $f : A \rightarrow B$ given by $f(a) = n/a$ is a bijection from A to B , because its inverse is the function $g : B \rightarrow A$ given by $g(b) = n/b$. Therefore, $|A| = |B|$. If \sqrt{n} is not an integer, then $D = A \cup B$, so $|D| = |A| + |B| = 2|A|$, which is even. If \sqrt{n} is an integer, then $D = A \cup B \cup \{\sqrt{n}\}$, so $|D| = |A| + |B| + 1 = 2|A| + 1$, which is odd. This completes the proof of our claim.

Using our claim, the desired set of integers is $\{1, 4, 9, 16, 25, 36, 49, 64, 81, 100\}$.

Solution for PS4-3. For \mathbb{Z}_{11} :

\otimes	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

For \mathbb{Z}_{12} :

\otimes	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

Observe that in the table for \mathbb{Z}_{11} , the zero entries are confined to the zero row and the zero column, whereas in the table for \mathbb{Z}_{12} , there are some zero entries in addition to these “obvious” ones. In fact, for each $x \in \mathbb{Z}_{12}$ that is not relatively prime to 12, there is at least one zero entry in the row/column for x .

Solution for PS4-4. Using the definition of congruence, $d \mid a - b$ and $d \mid x - y$.

Therefore, $d \mid (a - b) + (x - y) = (a + x) - (b + y)$, i.e., $a + x \equiv b + y \pmod{d}$.

Further, $d \mid (a - b)x$ and $d \mid b(x - y)$. Therefore, $d \mid (a - b)x + b(x - y) = ax - by$, i.e., $ax \equiv by \pmod{d}$.

Solution for PS4-5. Using the result of PS4-4, if $a \equiv b \pmod{d}$, then $a^2 \equiv b^2 \pmod{d}$. Using the same result again, $a^3 \equiv b^3 \pmod{d}$. Proceeding in this way, $a^n \equiv b^n \pmod{d}$ for all $n \in \mathbb{N}^+$.

Now take $d = a - b$. Trivially, $d \mid a - b$, so $a \equiv b \pmod{d}$. Therefore, $a^n \equiv b^n \pmod{d}$, which means $d \mid a^n - b^n$.

Solution for PS4-6. Take $d = a + b$. Then $a \equiv -b \pmod{d}$.

As in PS4-5, $a^n \equiv (-b)^n \pmod{d}$. Since n is odd, $(-1)^n = -1$. Therefore, $(-b)^n = (-1)^n b^n = -b^n$. We conclude that $a^n \equiv -b^n \pmod{d}$, so $d \mid a^n + b^n$.

Solution for PS4-7. Start by observing that $2^4 = 16 \equiv -1 \pmod{17}$. Therefore, powers of 2^4 are going to be easy to figure out. We use this to simplify:

$$2^{2019} = 2^{4 \times 504 + 3} = 16^{504} \times 2^3 \equiv (-1)^{504} \times 8 = 8 \pmod{17}.$$

Solution for PS4-8. Let n^2 be a perfect square. To reason about the last digit of n^2 , we consider arithmetic modulo 10. To reduce the number of cases to consider, we further use $9 \equiv -1 \pmod{10}$ and so on.

- If $n \equiv 0 \pmod{10}$, then $n^2 \equiv 0 \pmod{10}$.
- If $n \equiv \pm 1 \pmod{10}$, then $n^2 \equiv 1 \pmod{10}$.
- If $n \equiv \pm 2 \pmod{10}$, then $n^2 \equiv 4 \pmod{10}$.
- If $n \equiv \pm 3 \pmod{10}$, then $n^2 \equiv 9 \pmod{10}$.
- If $n \equiv \pm 4 \pmod{10}$, then $n^2 \equiv 16 \equiv 6 \pmod{10}$.
- If $n \equiv 5 \pmod{10}$, then $n^2 \equiv 25 \equiv 5 \pmod{10}$.

It follows that $n^2 \not\equiv 7 \pmod{10}$.

Alternate Solution for PS4-8. Let n^2 be a perfect square. If the last digit of n^2 is 7, then $n^2 \equiv 2 \pmod{5}$. However, the following exhaustive list of cases shows that this is not possible.

- If $n \equiv 0 \pmod{5}$, then $n^2 \equiv 0 \pmod{5}$.
- If $n \equiv \pm 1 \pmod{5}$, then $n^2 \equiv 1 \pmod{5}$.
- If $n \equiv \pm 2 \pmod{5}$, then $n^2 \equiv 4 \pmod{5}$.

Solution for PS4-9. Given that decimal representation, the value of n is given by

$$n = 10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10^2 a_2 + 10 a_1 + a_0 = \sum_{j=0}^k 10^j a_j.$$

Now $10 \equiv 1 \pmod{3}$, therefore $10^j \equiv 1^j = 1 \pmod{3}$ for each j . Using this in the above equation, we obtain $n \equiv \sum_{j=0}^k a_j \pmod{3}$, as desired.

Solution for PS4-10. Let $n = m(m+1)(m+2)$ be the product of three consecutive integers. Then, modulo 3, the integers m , $m+1$, and $m+2$ are congruent to 0, 1, and 2 in some order. Therefore $n \equiv 0 \times 1 \times 2 = 0 \pmod{3}$, i.e., $n = 3k$ for some integer k .

At least one of m , $m+1$, and $m+2$ is even. Therefore, n is even. If k were odd, then $n = 3k$ would have been odd. Therefore, k is even. Let $k = 2\ell$ for some integer ℓ . Then $n = 3 \cdot 2\ell = 6\ell$, which is divisible by 6.

Note: It's not enough to say that n is divisible by 2 and by 3, *therefore* it is divisible by 6. That “therefore” needs to be justified.

Solution for PS5-1.

- a. By repeated application of “Theorem 6” from the lecture notes,

$$\begin{aligned}\gcd(13631, 8213) &= \gcd(8213, 13631 \bmod 8213) \\ &= \gcd(5418, 8213 \bmod 5418) \\ &= \gcd(2795, 5418 \bmod 2795) \\ &= \gcd(2623, 2795 \bmod 2623) \\ &= \gcd(172, 2623 \bmod 172) \\ &= \gcd(43, 172 \bmod 43) \\ &= \gcd(43, 0) = 43.\end{aligned}$$

- b. Using the Extended Euclidean Algorithm,

$\begin{aligned}43 &= 1 \cdot 43 + 0 \cdot 0 \\ &= 0 \cdot 172 + 1 \cdot 43 \\ &= 1 \cdot 2623 - 15 \cdot 172 \\ &= -15 \cdot 2795 + 16 \cdot 2623 \\ &= 16 \cdot 5418 - 31 \cdot 2795 \\ &= -31 \cdot 8213 + 47 \cdot 5418 \\ &= 47 \cdot 13631 - 78 \cdot 8213\end{aligned}$	<p style="text-align: right;">Base case, $k_0 = 1; \ell_0 = 0$</p> $\begin{aligned}k_1 &= \ell_1 = 0; \ell_1 = k_0 - \lfloor a_1/b_1 \rfloor \cdot \ell_0 = 1 - \lfloor 172/43 \rfloor \cdot 0 \\ k_2 &= 1; \ell_2 = 0 - \lfloor 2623/172 \rfloor \cdot 1 \\ k_3 &= -15; \ell_3 = 1 - \lfloor 2795/2623 \rfloor \cdot (-15) \\ k_4 &= 16; \ell_4 = -15 - \lfloor 5418/2795 \rfloor \cdot 16 \\ k_5 &= -31; \ell_5 = 16 - \lfloor 8213/5418 \rfloor \cdot (-31) \\ k_6 &= 47; \ell_6 = -31 - \lfloor 13631/8213 \rfloor \cdot 47\end{aligned}$
--	--

we find $k = 47, \ell = -78$.

- c. Consider $k = 47 - 8213/43 = -144$, and $\ell = -78 + 13631/43 = 239$.

Solution for PS5-2.

- a. False. Take $a = 2, b = 6$, and $c = 3$.
- b. True. This is because $d \mid c \iff d^n \mid c^n$. The reverse implication isn’t straightforward, but can be proved using the Unique Factorization Theorem.
- c. True. If $d = \gcd(b, c)$, then clearly ad is a common divisor of ab and ac . On the other hand, by LCT, $\exists k, \ell \in \mathbb{Z}$ such that $d = kb + \ell c$, so $ad = kab + \ell ac$, whence $\gcd(ab, ac) \mid ad$.
- d. False. Take $a = 2, b = 4$.
- e. True. If $ka + \ell b = 1$, then $\ell^2 b^2 = (1 - ka)^2 = k^2 a^2 - 2ka + 1$. Therefore, $(2k - k^2 a)a + \ell^2 b^2 = 1$.
- f. True. The given condition implies $g := \gcd(a, b) \geq 3$. Clearly, $\gcd(a^2, b^2) \geq g \geq 3$. Had 2 been an IntLC of a^2 and b^2 , we would have had $\gcd(a^2, b^2) \mid 2$.

Solution for PS5-3.

- a. The code doesn’t handle negative numbers correctly. Calling `egcd(9, -6)` returns $(-3, 1, 2)$. However, by definition $\gcd(9, -6) = 3$, not -3 .
- b.

```
def egcd(a, b):
    if b < 0:
        g, k, l = egcd(a, -b)
        return (g, k, -l)
    elif a < 0:
        g, k, l = egcd(-a, b)
```

```

    return (g, -k, 1)
elif b == 0:
    return (a, 1, 0)
else:
    g, k, l = egcd(b, a % b)
    return (g, l, k - (a // b) * l)

```

Solution for PS5-4.

- a. Assume that a good call $\text{egcd}(a, b)$ is made, so that $0 \neq a \geq b \geq 0$. If it makes an immediate recursive call, $b \neq 0$. The new call is $\text{egcd}(b, r)$, where $r = a \bmod b$. By definition of the “mod” operation, $r < b$. Therefore, $0 \neq b \geq r \geq 0$, i.e., the new call is good. Furthermore, the size of the new call is

$$b + r < b + b \leq b + a = s.$$

- b. Consider the sequence of sizes of all recursive calls that result from an initial good call to egcd . By the above results, these recursive calls are all good, so the sizes are all natural numbers, and the sequence is decreasing. The sequence cannot be infinite (the sizes cannot decrease forever), so it eventually terminates, i.e., there is eventually a call to egcd that does not result in further recursion.

Solution for PS5-6.

- a. Let $m = \text{lcm}(a, b)$. Being a positive multiple of a , m must equal ax for some $x \in \mathbb{N}^+$. Similarly, $m = by$ for some $y \in \mathbb{N}^+$. Now suppose that $\text{gcd}(x, y) = z > 1$. Then x/z and y/z are both integers and so

$$\frac{ax}{z} = \frac{by}{z} = \frac{m}{z} < m$$

is a common multiple of a and b that is smaller than m , a contradiction.

- b. By LCT, $\exists k, \ell \in \mathbb{Z}$ such that $1 = kx + \ell y$. Therefore, $a/y = kax/y + \ell ay/y = kb + \ell a$.
c. Since $d := \text{gcd}(a, b)$ must divide every IntLC of a and b , in particular, $d \mid a/y$.
d. Since $a/y \in \mathbb{Z}$, it is obviously a divisor of a . Further, $b/(a/y) = by/a = x \in \mathbb{Z}$, so a/y divides b as well.
e. Since a/y is one particular common divisor of a and b , the *greatest* common divisor $d \geq a/y$. But we also showed that $d \mid a/y$. Therefore, $d = a/y$.
f. A simple calculation: $\text{gcd}(a, b) \cdot \text{lcm}(a, b) = dm = (a/y)(by) = ab$.

Solution for PS5-7.

- a. The only divisors of p are 1 and itself. Of these, only 1 is a divisor of b , since $0 < b < p$. Therefore, $\text{gcd}(b, p) = 1$. By the Inverse Existence Theorem, b has an inverse modulo p .
b. Let $a = b^{-1}$. We claim that the function f_a is the inverse of f_b . Indeed,

$$f_a(f_b(x)) = f_a(bx \bmod p) = (a(bx \bmod p) \bmod p) = abx \bmod p = x,$$

so $f_a \circ f_b = \text{id}_{\mathbb{Z}_p}$. Similarly, $f_b \circ f_a = \text{id}_{\mathbb{Z}_p}$. By results from earlier in the course, f_b is a bijection.

Solution for PS5-8. The fact to be shown follows from its contrapositive, the statement that if n is not even, then n^2 is not even. This statement is precisely PS3-1e, the fact that the product of two odd numbers is odd.

- a. Assume, to the contrary, that $\sqrt{2} = u/v$, in lowest terms, for some $u, v \in \mathbb{N}^+$. Then $u^2 = 2v^2$, which is even. Therefore, u is even. Let $u = 2w$, where $w \in \mathbb{N}^+$. We get

$$(2w)^2 = 2v^2, \quad \text{i.e., } v^2 = 2w^2,$$

which is even. Therefore, v is even. Since u and v are both even, the expression u/v is not in lowest terms, a contradiction.

- b. Suppose that $p \mid n^2 = n \cdot n$. Applying Euclid's Lemma (the "consequently" portion), we directly get $p \mid n$.
- c. Let p be an arbitrary prime. Assume, to the contrary, that $\sqrt{p} = u/v$, in lowest terms, for some $u, v \in \mathbb{N}^+$. Then $u^2 = pv^2$, so $p \mid u^2$, so $p \mid u$ (by the previous part). Let $u = pw$, where $w \in \mathbb{N}^+$. We get

$$(pw)^2 = pv^2, \quad \text{i.e., } v^2 = pw^2,$$

which means $p \mid v^2$. Therefore, $p \mid v$. Since p divides both u and v , the expression u/v is not in lowest terms, a contradiction.

- d. Suppose that $p \mid n^2 = n \cdot n$. Applying Euclid's lemma (the "consequently" portion), we directly get $p \mid n$.
- e. Let p be an arbitrary prime and $a \in \mathbb{Z}$. By repeatedly using Euclid's Lemma, we get that

$$\begin{aligned} p \mid a^n = a \cdot a^{n-1} &\implies \text{either } p \mid a \text{ or } p \mid a^{n-1} = a \cdot a^{n-2} \\ &\implies \text{either } p \mid a \text{ or } p \mid a^{n-2} = a \cdot a^{n-3} \\ &\implies \dots \\ &\implies \text{either } p \mid a \text{ or } p \mid a. \end{aligned}$$

In short, $p \mid a^n \implies p \mid a$.

Now let n be an arbitrary integer ≥ 2 . Assume, to the contrary, that $p^{1/n} = u/v$, in lowest terms, for some $u, v \in \mathbb{N}^+$. Then $u^n = pv^n$, so $p \mid u^n$, so $p \mid u$ (by the above). Let $u = pw$, where $w \in \mathbb{N}^+$. We get

$$(pw)^n = pv^n, \quad \text{i.e., } v^n = p^{n-1}w^n.$$

Since $n \geq 2$, this means $p \mid v^n$. Therefore, $p \mid v$. Since p divides both u and v , the expression u/v is not in lowest terms, a contradiction.

Solution for PS5-9.

- a. The numbers 1 and $p-1$ (which are distinct because $p \geq 3$) are self-inverses, because $1^2 \equiv 1 \pmod{p}$ and $(p-1)^2 \equiv (-1)^2 \equiv 1 \pmod{p}$. To show that there are no others, suppose $a \in \mathbb{Z}_p$ is a self-inverse, so $a^2 \equiv 1 \pmod{p}$. By the definition of congruence,

$$p \mid a^2 - 1 = (a-1)(a+1).$$

By Euclid's Lemma, either $p \mid a-1$ or $p \mid a+1$, i.e., either $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$.

- b. We can solve this by exhaustive case analysis, but let's be cleverer. Reasoning as above, 1 and 14 are clearly self-inverses. Further, if $a^2 \equiv 1 \pmod{15}$, then

$$15 \mid a^2 - 1 = (a-1)(a+1) \implies 5 \mid (a-1)(a+1).$$

So $a \equiv \pm 1 \pmod{5}$. Besides 1 and 14, the only other values in \mathbb{Z}_{15} satisfying this are 4, 6, 9, and 11. But by analogous reasoning, $a \equiv \pm 1 \pmod{3}$, so we can eliminate 6 and 9. Finally, $4^2 \equiv 11^2 \equiv 1 \pmod{15}$.

Thus, there are exactly four self-inverses modulo 15: they are 1, 4, 11, and 14.

Solution for PS6-1. When $\gcd(a, m) \neq 1$, the number a has no inverse modulo m , nor can any positive power of a be congruent to 1 modulo m .

I used the 'egcd' Python function from the lecture notes to compute GCDs and, as a result, inverses when they exist. For the powers, I used some trial and error.

number	inverse	power congruent to 1
1	1	$1^1 \equiv 1$
10	\nexists	\nexists
13	7	$13^4 \equiv 1$
19	19	$19^2 \equiv 1$
27	\nexists	\nexists
29	29	$29^2 \equiv 1$

Solution for PS6-2. Let $n = q(p-1) + r$, where $q, r \in \mathbb{Z}$ and $0 \leq r < p-1$. By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$. Therefore,

$$a^n = (a^{p-1})^q \cdot a^r \equiv 1^q a^r = a^{n \bmod (p-1)} \pmod{p}.$$

Solution for PS6-3. Suppose that $a, b \in \mathbb{Z}_m^*$ and $c = ab \bmod m$. We must show that $c \in \mathbb{Z}_m^*$.

By the Inverse Existence Theorem, a^{-1} and b^{-1} exist. Therefore,

$$c \cdot (b^{-1}a^{-1}) = ab b^{-1}a^{-1} \equiv 1 \pmod{m},$$

so c^{-1} exists. By the Inverse Existence Theorem, $\gcd(c, m) = 1$, so $c \in \mathbb{Z}_m^*$.

Solution for PS6-4.

- a. First, check that f_a is indeed a function from \mathbb{Z}_m^* to \mathbb{Z}_m^* . Of course, for any $m \in \mathbb{Z}_m^*$, $ax \bmod m$ is a unique defined value in \mathbb{Z}_m ; the only question is whether it lies in \mathbb{Z}_m^* . By the result of **PS6-3**, it does.

To prove that f_a is a *bijection*, we demonstrate that it has an inverse function. By the Inverse Existence Theorem, $\exists b \in \mathbb{Z}_m^*$ such that $ab \equiv 1 \pmod{m}$. Now, for all $x \in \mathbb{Z}_m^*$,

$$f_b(f_a(x)) = b(ax \bmod m) \bmod m = bax \bmod m = x,$$

so $f_b \circ f_a = \text{id}$. Similarly, $f_a \circ f_b = \text{id}$. This completes the proof.

- b. Let $L = (b_1, b_2, \dots, b_{\phi(m)})$ be a list of all the elements of \mathbb{Z}_m^* . By the previous part, the list

$$L' = (ab_1 \bmod m, ab_2 \bmod m, \dots, ab_{\phi(m)} \bmod m)$$

consists of the same elements as L , but perhaps in a different order. Comparing the products of the elements in each list,

$$b_1 b_2 \cdots b_{\phi(m)} \equiv a^{\phi(m)} b_1 b_2 \cdots b_{\phi(m)} \pmod{m}.$$

By the Inverse Existence Theorem, each b_i has an inverse b_i^{-1} . Multiplying both sides by $b_1^{-1} b_2^{-1} \cdots b_{\phi(m)}^{-1}$ gives $1 \equiv a^{\phi(m)} \pmod{m}$.

- c. When m is a prime, every nonzero number in \mathbb{Z}_m is coprime to m , so $\mathbb{Z}_m^* = \{1, 2, \dots, m-1\}$ and $\phi(m) = m-1$. The congruence now reads $a^{m-1} \equiv 1 \pmod{m}$, which is exactly Fermat's Little Theorem.

Solution for PS6-5.

- a. By definition, $P_{m,a}$ is an infinite sequence, but all its elements lie in the finite set \mathbb{Z}_m^* . Therefore, there must be a repetition in the sequence. Let $i < j$ be two positions such that $a^i \bmod m = a^j \bmod m$. By the Inverse Existence Theorem, a has an inverse b modulo m . So,

$$a^i \equiv a^j \pmod{m} \implies b^i a^i \equiv b^i a^j \pmod{m} \implies 1 \equiv a^{j-i} \pmod{m}.$$

Thus, 1 reappears in the sequence at position $j - i$.

- b. Let k be the smallest positive index at which 1 appears in $P_{m,a}$. Then $a^k \equiv 1 \pmod{m}$. For any index $\ell > k$, let $\ell = qk + r$ with $q, r \in \mathbb{N}$ and $0 \leq r < k$. Then

$$a^\ell = (a^k)^q \cdot a^r \equiv 1^q a^r = a^r \pmod{m}.$$

Therefore, $P_{m,a}$ consists of the block $(a^0 \bmod m, \dots, a^{k-1} \bmod m)$ repeated infinitely often.

- c. Let's look more closely at the argument in Part a. If we consider the first $m + 1$ elements in the sequence, there must already be a repetition because the elements come from a set of size $\leq m$. Therefore, we can enforce $0 \leq i < j \leq m$ in that argument.

Thus, 1 reappears at position $j - i \leq m$. So the value of k in the previous part—which is the period—is $\leq m$.

- d. Look even more closely at the argument above. The elements in the sequence in fact come from the set \mathbb{Z}_m^* , whose cardinality is $\phi(m) \leq m - 1$. Therefore, $k \leq m - 1$. In particular, the period cannot be m .

Note: With a little more effort, you can in fact show that $k \mid \phi(m)$, so the period must be a divisor of $\phi(m)$.

Alternate Solution for PS6-5.

- a. Since $a \in \mathbb{Z}_m^*$, by Euler's Theorem, $a^{\phi(m)} \equiv 1 \pmod{m}$. Since $\phi(m) > 0$, we see that 1 reappears in the sequence at position $\phi(m)$.
- b. Same as above.
- c. The period is clearly at most $\phi(m)$. Since $\mathbb{Z}_m^* \subset \mathbb{Z}_m$, it follows that $\phi(m) < m$. So the period is $\leq m$.
- d. Of course, we've in fact shown that the period is $< m$. In particular, it can't be m .

Solution for PS6-6. Consider an arbitrary $a \in \mathbb{Z}_{pq}$. The positive divisors of pq are 1, p , q , and pq . So $\gcd(a, pq)$ must be one of these four numbers. Let's count how many numbers a lead to each of these GCDs.

Case 1: $\gcd(a, pq) = 1$. Then $a \in \mathbb{Z}_{pq}^*$. By definition, there are $\phi(pq)$ such numbers a .

Case 2: $\gcd(a, pq) = pq$. Since $a < pq$, this means $a = pq$, i.e., there is exactly one possibility for a .

Case 3: $\gcd(a, pq) = p$. Then $p \mid a$ and $a < pq$, so $a \in \{p, 2p, 3p, \dots, (q-1)p\}$, i.e., $q-1$ possibilities for a .

Case 4: $\gcd(a, pq) = q$. Analogously, there are $p-1$ possibilities for a in this case.

Since there is no overlap between the cases and there are $|\mathbb{Z}_{pq}| = pq$ total possibilities for a , we obtain

$$pq = \phi(pq) + 1 + (q-1) + (p-1).$$

Solving for $\phi(pq)$ gives $\phi(pq) = pq - p - q + 1 = (p-1)(q-1)$.

Solution for PS6-7.

- a. We work modulo p . Imagine drawing an arrow from each $a \in \mathbb{Z}_p^*$ to a^{-1} . Then the arrow from a^{-1} will point to $(a^{-1})^{-1} = a$. We can then pair off a and a^{-1} . If we consider any other element $b \notin \{a, a^{-1}\}$, then $\{b, b^{-1}\}$ will be another pair disjoint from $\{a, a^{-1}\}$.
There is a catch: a might equal a^{-1} sometimes! But by PS5-9^{HW}, this only happens for $a = 1$ and $a = p-1$. So the argument above works for all $a \in S$.
- b. Consider the modulo- p product Q of all numbers in S . We can rearrange the product to place each $a \in S$ adjacent to its partner $a^{-1} \in S$. The product within each pair is 1 modulo p . Therefore, so is the overall product, i.e., $Q \equiv 1 \pmod{p}$. Therefore,

$$(p-1)! = 1 \times Q \times (p-1) \equiv 1 \times 1 \times (-1) \equiv -1 \pmod{p}.$$

- c. By the definition of congruence, the last statement above can be rewritten as $p \mid (p-1)! + 1$.

Solution for PS6-8. Since m is composite, we can write $m = ab$ where $2 \leq a \leq m-1$ and $2 \leq b \leq m-1$. Consider the list of factors $L = (1, 2, \dots, m-1)$ whose product equals $(m-1)!$. Three cases arise.

Case 1: $a \neq b$. In this case both a and b appear in L . Therefore $m = ab \mid (m-1)!$, whence $m \nmid (m-1)! + 1$.

Case 2: $a = b > 2$. In this case, $m = a^2 > 2a$, so a and $2a$ both appear in L . Thus, $m = a^2 \mid (m-1)!$, as before.

Case 3: $a = b = 2$. Then $m = 4$ and we check directly that $4 \nmid 3! + 1 = 7$.

Solution for PS6-9.

- a. By the GCD Linear Combination Theorem (LCT), $\exists k, \ell \in \mathbb{Z}$ such that $\gcd(a, b) = ka + \ell b$. By PS5-6^{HW},

$$\frac{n}{\text{lcm}(a, b)} = \frac{n \cdot \gcd(a, b)}{ab} = \frac{n(ka + \ell b)}{ab} = \frac{kn}{b} + \frac{\ell n}{a} \in \mathbb{Z},$$

since $b \mid n$ and $a \mid n$.

- b. From the given info,

- $\gcd(p_1, p_2) = 1$, so n is divisible by $\text{lcm}(p_1, p_2) = p_1 p_2$;
- $\gcd(p_1 p_2, p_3) = 1$, so n is divisible by $\text{lcm}(p_1 p_2, p_3) = p_1 p_2 p_3$;
- and so on.

Note: Once we study mathematical induction, we'll learn a better way to write this type of proof formally.

Solution for PS6-10. We first work out the factorization $2730 = 2 \times 3 \times 5 \times 7 \times 13$. By the previous result, it suffices to show that each of these prime factors divides $n^{13} - n$.

Consider each $p \in \{2, 3, 5, 7, 13\}$. If $p \mid n$ then $p \mid n^{13}$ as well, so $p \mid n^{13} - n$. Otherwise, if $p \nmid n$, we apply Fermat's Little Theorem:

- For $p = 2$, we have $n^{13} \equiv 1^{13} \equiv 1 \equiv n \pmod{2}$.
- For $p = 3$, we have $n^{13} = (n^2)^6 \cdot n \equiv 1^6 \cdot n \equiv n \pmod{3}$.
- For $p = 5$, we have $n^{13} = (n^4)^3 \cdot n \equiv 1^3 \cdot n \equiv n \pmod{5}$.
- For $p = 7$, we have $n^{13} = (n^6)^2 \cdot n \equiv 1^2 \cdot n \equiv n \pmod{7}$.
- For $p = 13$, we have $n^{13} \equiv n \pmod{13}$.

Solution for PS7-1.

- a. If $M = 0$, clearly $M' = 0$. Else, since $ed \equiv 1 \pmod{P-1}$, write $ed = k(P-1) + 1$ where $k \in \mathbb{N}$. We compute

$$M' \equiv C^d \equiv M^{ed} = (M^{P-1})^k \cdot M \equiv 1^k M = M \pmod{P},$$

where the last congruence is because of Fermat's Little Theorem. Since $M, M' \in \mathbb{Z}_p$, $M = M'$.

- b. Dr. Speedy's "cryptosystem" is not secure at all! Anyone can use the Extended GCD Algorithm to compute d from e and P (which are both public) and then cheerfully decrypt any message to Bob that they can intercept.

Solution for PS7-2. Suppose that $N = pq$, where p and q are distinct primes. Using the result of a previous class exercise, $\phi(N) = \phi(pq) = (p-1)(q-1) = N - p - q + 1$.

Therefore, $q = N - \phi(N) + 1 - p$. Substituting this expression for q in $N = pq$, we obtain

$$\begin{aligned} p(N - \phi(N) + 1 - p) &= N, \\ \text{i.e., } p^2 + (\phi(N) - N - 1)p + N &= 0. \end{aligned}$$

Run algorithm \mathcal{A} to obtain $\phi(N)$. We now know all the coefficients in this quadratic equation for p . Solving it, we obtain p . Then we obtain $q = N/p$.

Solution for PS7-3. One can verify that the Decryption Theorem for RSA still holds with 10-prime RSA, so Dr. Tricky's idea is not immediately flawed.

For regular, 2-prime RSA, with public key (N_2, e_2) , and private key d , the time needed to perform encryption and decryption is given by the time needed for modular exponentiation. This mainly depends on the number of bits needed to express N_2 and e_2 . Given the value of N_2 , the value of e_2 is essentially unrestrained; it must only be coprime to $\phi(N)$. For 10-prime RSA, and a modulus N_{10} with the same number of bits as N_2 , because only a small fraction of numbers are not coprime to N_{10} , one can pick an encryption exponent e_1 almost exactly equal to e_2 . As a result, for the same key size, encryption and decryption procedures do not differ significantly between 2-prime and 10-prime RSA.

On the other hand, for the same key size (number of bits of N_2 and N_{10}), the time to factor the modulus can differ significantly for 10-prime RSA. Here we consider the brute force factoring algorithm, that checks divisibility by every number $\leq \sqrt{n}$. Better algorithms, like the General Number Field Sieve or the Elliptic-Curve Factorization Method, are more efficient, but their runtime analysis is more complicated. Write the factors of N_2 and N_{10} in increasing order, so that $N_2 = p_1 \cdot p_2$, and $N_{10} = q_1 \cdot q_2 \cdot q_3 \cdots q_{10}$, with $p_1 < p_2$, and $q_1 < q_2 < \dots < q_{10}$. Then brute force factorization of N_2 requires time $O(p_1)$ to discover the smaller factor; while factoring N_{10} requires time $O(q_1 + q_2 + \dots + q_9) = O(q_9)$ to discover the 9 smallest factors.

To make breaking 2-prime RSA difficult, p_1 and p_2 are chosen roughly equal in size, so that $p_1 \approx \sqrt{N_2}$, and it takes $O(\sqrt{N_2})$ time to brute-force factor N_2 . To make breaking 10-prime RSA hard, q_9 should be as large as possible. This can be done by setting $q_1 = 2$, $q_2 = 3$, $q_3 = 5$, and picking q_9 and q_{10} both $\approx \sqrt{N_{10}}$, in which case the time to factor N_{10} is a constant multiple of that for N_2 . There isn't any reason to prefer 10-prime RSA over 2-prime RSA.

If the prime factors of N_{10} are all roughly the same size, then $q_1 \approx q_2 \approx \dots \approx q_{10} \approx N_{10}^{1/10}$, and it only takes $O(N_{10}^{1/10})$ time to break Dr. Tricky's method, which is far less than $O(\sqrt{N_2})$.

Solution for PS7-4.

- a. When we call `modpow_bad(a, k, n)`, it results in k calls to `modmult`. Since k is a 1024-bit integer, the value of k could be as large as $2^{1024} - 1$ and is typically greater than 2^{1000} . Even if each call to `modmult` takes just one nanosecond, the time spent by `modpow_bad` would be orders of magnitude greater than the age of the universe!

- b. By repeated squaring, compute $a \rightarrow a^2 \rightarrow a^4 \rightarrow a^8 \rightarrow a^{16} \rightarrow a^{32} \rightarrow a^{64}$ (all computations modulo n). Then combine the results like this: $a \cdot a^2 \cdot a^{16} \cdot a^{64} = a^{1+2+16+64} = a^{83}$ (again, modulo n).
- c. If n is even, let $n = 2k$. Then $x^n = x^{2k} = (x^2)^k = (x^2)^{\lfloor n/2 \rfloor}$.
If n is odd, let $n = 2k + 1$. Then $x^n = x^{2k+1} = x \cdot (x^2)^k = x \cdot (x^2)^{\lfloor n/2 \rfloor}$.
- d. The equation in the previous part shows how raising to the power n can be reduced to raising to the power $\lfloor n/2 \rfloor$, provided we first compute the square. We can translate this directly into the following recursive implementation.

```
def modpow(a, k, n):
    """compute a**k modulo n quickly, assuming k >= 0, n > 0"""
    if k == 0:
        return 1
    square = modmult(a, a, n)
    temp = modpow(square, k // 2, n)
    if k % 2 == 0:
        return temp
    else:
        return modmult(a, temp, n)
```

- e. When I ran the above code on the given numbers, it “instantly” returned 4808550559.

Solution for PS7-5.

- a. Since $\gcd(m, n) = 1$, by **PS5-6**^{HW}, $\text{lcm}(m, n) = mn$. Therefore, by **PS6-9**, if $m \mid s$ and $n \mid s$, then $mn \mid s$. Now, to prove what’s asked for, take $s = x - y$.
- b. Suppose that $f(x) = f(y)$. Then $(x \bmod m, x \bmod n) = (y \bmod m, y \bmod n)$. In other words, $x \equiv y \pmod{m}$ and $x \equiv y \pmod{n}$. Therefore, by the previous part, $x \equiv y \pmod{mn}$. Since both x and y belong to \mathbb{Z}_{mn} , this forces $x = y$.
- c. Since f is injective, $|\text{Range}(f)| = |\text{Domain}(f)| = |\mathbb{Z}_{mn}| = mn$. However, $|\text{Codomain}(f)| = |\mathbb{Z}_m \times \mathbb{Z}_n| = mn$ as well. Therefore, $\text{Range}(f) = \text{Codomain}(f)$, which makes f surjective.
- d. By the previous two parts, f is bijective. Therefore, for each $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$, there is one and only one value $x \in \mathbb{Z}_{mn}$ such that $f(x) = (a, b)$. This value, which is precisely $f^{-1}(a, b)$, is the unique solution to the system of congruences.

Solution for PS7-6.

- a. We already know from **PS7-5** that f is injective on the full domain \mathbb{Z}_{mn} . Therefore, we only need to show that $x \in \mathbb{Z}_{mn}^* \iff f(x) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*$. This is logically equivalent to $x \notin \mathbb{Z}_{mn}^* \iff f(x) \notin \mathbb{Z}_m^* \times \mathbb{Z}_n^*$, so we’ll prove the latter instead.

Suppose that $x \notin \mathbb{Z}_{mn}^*$. Then $\gcd(x, mn) = d > 1$. Let p be a prime divisor of d . Then $p \mid x$ and $p \mid mn$. By Euclid’s Lemma, either $p \mid m$ or $p \mid n$. Assume WLOG that $p \mid m$. Let $f(x) = (a, b)$. Then

$$\gcd(a, m) = \gcd(x \bmod m, m) = \gcd(x, m) \geq p > 1,$$

whence $a \notin \mathbb{Z}_m^*$, implying $f(x) \notin \mathbb{Z}_m^* \times \mathbb{Z}_n^*$.

On the other hand, suppose that $f(x) = (a, b) \notin \mathbb{Z}_m^* \times \mathbb{Z}_n^*$. Assume WLOG that $a \notin \mathbb{Z}_m^*$. Then $\gcd(a, m) = d > 1$. Therefore,

$$\gcd(x, mn) \geq \gcd(x, m) = \gcd(x \bmod m, m) = \gcd(a, m) = d > 1,$$

whence $x \notin \mathbb{Z}_{mn}^*$.

- b. The existence of a bijection from finite set A to finite set B implies $|A| = |B|$. Therefore, $\phi(mn) = \phi(m)\phi(n)$. In the language of Unit 8, we are using the bijection principle and the product principle.

Solution for PS7-7.

- a. A square root of unity modulo m is exactly the same thing as a self-inverse modulo m . If m were prime, as shown in **PS5-9^{HW}**, it would have had only two such square roots: 1 and $m - 1$.
- b. By definition, $b^2 \equiv 1 \pmod{m}$, so $m \mid b^2 - 1 = (b - 1)(b + 1)$. Let p be a prime divisor of m . Then $p \mid (b - 1)(b + 1)$, so by Euclid's Lemma, either $p \mid b - 1$ or $p \mid b + 1$. Since $b \neq 1$, $b \neq m - 1$, and $m \geq 3$, we have $1 \leq b - 1 < b + 1 < m$.
- Suppose that $p \mid b - 1$. Then $\gcd(m, b - 1) \geq p > 1$. Also, $\gcd(m, b - 1) \leq b - 1 < m$. Therefore $\gcd(m, b - 1)$ is a nontrivial divisor of m .
- Suppose that $p \mid b + 1$. Then $\gcd(m, b + 1) \geq p > 1$. Also, $\gcd(m, b + 1) \leq b + 1 < m$. Therefore $\gcd(m, b + 1)$ is a nontrivial divisor of m .

Solution for PS8-1.

- a. $27 \times 37 = 999$, by the product principle.
- b. $52 \times 51 = 2652$, by the generalized product principle.
- c. $\lfloor 1000/3 \rfloor + \lfloor 1000/5 \rfloor - \lfloor 1000/15 \rfloor = 467$, by the generalized sum principle.

Solution for PS8-2.

- a. Let C be the set of ways in which we can answer a single question on the test. Then the set of choices for the entire test is C^{10} . So we apply the product principle.
 - (a) In this case, $|C| = 4$, so the number of ways is $4^{10} = 1\,048\,576$.
 - (b) Here $|C| = 5$ —one of the choices is to leave an answer blank—so the number of ways is $5^{10} = 9\,765\,625$.
- b. Consider natural numbers below 10^9 , padded up to nine digits by adding zeros as needed. Let

$$\begin{aligned} S &= \{0, 1, 2, \dots, 10^9 - 1\}, \\ A &= \{n \in S : n\text{'s padded decimal representation contains a '1'}\}, \\ B &= \{n \in S : n\text{'s padded decimal representation does not contain a '1'}\}. \end{aligned}$$

Every number in B can be thought of as a sequence of 9 characters, with each character drawn from $\{0, 2, 3, 4, 5, 6, 7, 8, 9\}$, a set of size 9. By the product principle, $|B| = 9^9$.

Since $A \cap B = \emptyset$, by the sum principle, $|S| = |A| + |B|$. Therefore, $|A| = |S| - |B| = 10^9 - 9^9$.

The question asks about numbers in the set $(S - \{0\}) \cup \{10^9\}$. The number 0 does not contain the digit '1', so there's nothing to take away, but the number 10^9 does contain the digit '1', so we need to add one to this figure. This gives a final answer of

$$10^9 - 9^9 + 1 = 612\,579\,512.$$

Solution for PS8-3. Let a_k denote the sum of all multiples of k between 1 and 1000. Repeatedly using the basic summation formula $1 + 2 + \dots + n = n(n+1)/2$, we obtain

$$\begin{aligned} a_3 &= 3 + 6 + \dots + 999 = 3(1 + 2 + \dots + 333) = 3 \times \frac{333 \times 334}{2} = 166\,833; \\ a_5 &= 5 + 10 + \dots + 1000 = 5(1 + 2 + \dots + 200) = 5 \times \frac{200 \times 201}{2} = 100\,500; \\ a_{15} &= 15 + 30 + \dots + 990 = 15(1 + 2 + \dots + 66) = 15 \times \frac{66 \times 67}{2} = 33\,165. \end{aligned}$$

The desired answer is $a_3 + a_5 - a_{15} = 166\,833 + 100\,500 - 33\,165 = 234\,168$. We subtracted a_{15} because numbers which are multiple of both 3 and 5—i.e., multiples of $\text{lcm}(3, 5) = 15$ —are included twice when we write $a_3 + a_5$.

Solution for PS8-4. Using the sum principle, it's $62^6 + 62^7 + 62^8 - 52^6 - 52^7 - 52^8 = 167\,410\,949\,583\,040$.

Solution for PS8-5. Let $s(n) := n^6 + n^7 + n^8$; this is the number of six-to-eight character strings where each character is drawn from a set of size n .

By the generalized sum principle, the desired answer is $s(62) - s(52) - 2s(36) + s(10) + 2s(26)$.

Solution for PS8-6.

- a. For any arbitrary choices of x and y , we can always choose z in such a way that $x + y + z$ is even. More precisely, if $x + y$ is odd then we choose z to be odd, else we choose z to be even. Thus, choosing a 3-tuple $(x, y, z) \in T$ can be seen as making the following sequence of choices:
 - Choose x freely from D . There are 10 choices.
 - Choose y freely from D . There are 10 choices.

- Choose z from $\{1, 3, 5, 7, 9\}$ if $x + y$ is odd; else choose z from $\{0, 2, 4, 6, 8\}$. There are exactly 5 choices in each case.

Thus, by the generalized product principle, $|T| = 10 \times 10 \times 5 = 500$.

- b. Let the n digits be x_1, x_2, \dots, x_n (from left to right). Then we want to find number of choices for x_1, \dots, x_n such that $1 \leq x_1 \leq 9$; for each $i \in \{2, 3, \dots, n\}$, $0 \leq x_i \leq 9$; and $x_1 + x_2 + \dots + x_n$ is even.

Now, for any arbitrary choices of x_1, \dots, x_{n-1} , we can always choose x_n in such a way that $x_1 + x_2 + \dots + x_n$ is even. More precisely, if $x_1 + \dots + x_{n-1}$ is odd, then we choose x_n to be odd, else we choose x_n to be even. Hence for each list of choices of x_1, \dots, x_{n-1} , there are exactly 5 choices of x_n such that $x_1 + x_2 + \dots + x_n$ is even. By the generalized product principle, the total number of choices for all the digits is

$$9 \times 10^{n-2} \times 5 = 45 \times 10^{n-2},$$

since there are 9 choices for x_1 , and 10 choices for each of x_2, \dots, x_{n-1} .

Alternate Solution for PS8-6.

- a. Let $A = \{1, 3, 5, 7, 9\}$ be the set of odd digits and let $B = \{0, 2, 4, 6, 8\}$ be the set of even digits. We break T into four pairwise disjoint subsets, each of which is a Cartesian product. So the product principle applies to each subset.
- $T_1 = \{(x, y, z) \in D^3 : x, y, \text{ and } z \text{ are even}\} = B \times B \times B$. Then $|T_1| = |B| \times |B| \times |B| = 5 \times 5 \times 5 = 125$.
 - $T_2 = \{(x, y, z) \in D^3 : x \text{ and } y \text{ are odd, } z \text{ is even}\} = A \times A \times B$. Then $|T_2| = |A| \times |A| \times |B| = 125$.
 - $T_3 = \{(x, y, z) \in D^3 : x \text{ and } z \text{ are odd, } y \text{ is even}\} = A \times B \times A$. Then $|T_3| = 125$ as well.
 - $T_4 = \{(x, y, z) \in D^3 : y \text{ and } z \text{ are odd, } x \text{ is even}\} = B \times A \times A$. Then $|T_4| = 125$ as well.
- b. Same as above.

Solution for PS8-7.

- a. $4 \times 3 \times 2 \times 1 = 4! = 24$, by the generalized product principle.
- b. $n!$, by the generalized product principle.

Solution for PS8-8.

- a. If we color one of the 1s red, and the other black, then we have four distinct symbols, leading to $4! = 24$ permutations.
- Now consider the function f that maps a colored permutation to an ordinary (uncolored) permutation of $(1, 1, 4, 9)$ by “removing the colors.” This f is a 2-to-1 correspondence. So, by the division principle, the number of permutations of $(1, 1, 4, 9)$ is $24/2 = 12$.
- b. We can either reason directly, or follow the steps of Problem 15.27 (“The Tao of BOOKKEEPER”) from the [LLM] book. Then we apply similar logic to the word “CONDESCENDENCE”. This 14-letter word has 3 Cs, 3 Ns, 2 Ds, 4 Es, 1 O, and 1 S. Therefore, it has

$$\frac{14!}{3! \cdot 3! \cdot 2! \cdot 4! \cdot 1! \cdot 1!} = 50450400$$

anagrams.

Solution for PS8-9.

- a. 2^{mn} , since each relation is just a subset of $A \times B$.
- b. n^m , by the generalized product principle (choosing a function means making a sequence of $|A|$ choices).
- c. $n(n-1) \cdots (n-m+1)$, by the generalized product principle. Note that this equals 0 when $m > n$.
- d. If $m = n$ then $n!$, else 0.

Solution for PS8-10. For a palindrome of length n , where n is even, we can arbitrarily choose the first $n/2$ bits and then the last $n/2$ bits are automatically fixed. Thus, there are 2 choices for each of the first $n/2$ bits, and then 1 choice for each remaining bit. This leads to $2^{n/2}$ possible palindromes.

If n is odd, then we can arbitrarily choose the first $(n+1)/2$ bits and then the last $(n-1)/2$ bits are automatically fixed. As before, this leads to $2^{(n+1)/2}$ possible palindromes.

We can combine these two cases and say that the number of n -bit palindromes for any natural number n is $2^{\lceil n/2 \rceil}$.

Solution for PS8-11.

- a. $\binom{13}{10}$. This is pretty much the definition of “ n choose k .”
- b. $13 \times 12 \times \cdots \times 4 = \frac{13!}{3!}$, by the generalized product principle.
- c. $\binom{13}{10} - \binom{11}{10}$, subtracting off sets of 10 players chosen solely from the 11 students.

Solution for PS8-12.

- a. $\binom{10}{4}$, since this amounts to choosing the 4 locations (out of 10) where the 1s will occur.
- b. $\binom{10}{1} + \binom{10}{2} + \binom{10}{3} + \binom{10}{4}$, by applying the previous observation four times.
- c. $\binom{10}{4} + \binom{10}{5} + \binom{10}{6} + \binom{10}{7} + \binom{10}{8} + \binom{10}{9} + \binom{10}{10}$, along similar lines.
- d. $\binom{10}{5}$, along similar lines.

Solution for PS8-13.

- a. 5040.
- b. 1440.
- c. 240.
- d. 2640.

Solution for PS9-1. Let $P(n)$ be the statement “ $\sum_{i=1}^n (2i - 1) = n^2$.” We shall prove by induction on n that $\forall n \in \mathbb{N} : P(n)$.

Base case. $P(0)$ states “ $0 = 0^2$.” This is obviously true.

Induction step. Assume that $P(k)$ is true for some $k \geq 0$. Then

$$\begin{aligned} \sum_{i=1}^{k+1} (2i - 1) &= \left(\sum_{i=1}^k (2i - 1) \right) + (2(k+1) - 1) \\ &= k^2 + (2(k+1) - 1) &< \text{by the induction hypothesis} \\ &= k^2 + 2k + 1 \\ &= (k+1)^2. \end{aligned}$$

Therefore, $P(k+1)$ is true. We have shown that $P(k) \implies P(k+1)$.

Thus, by the principle of mathematical induction, the proof is complete.

Solution for PS9-2. Let $P(n)$ be the given statement. We shall prove it for all $n \in \mathbb{N}$ by induction on n .

Base case. $P(0)$ states “ $0 = 1! - 1$.” This is obviously true.

Induction step. Assume that $P(k)$ is true for some $k \geq 0$. Then

$$\begin{aligned} \sum_{j=1}^{k+1} j \cdot j! &= \left(\sum_{j=1}^k j \cdot j! \right) + (k+1) \cdot (k+1)! \\ &= (k+1)! - 1 + (k+1) \cdot (k+1)! &< \text{by the induction hypothesis} \\ &= (k+1)! \cdot (1 + (k+1)) - 1 \\ &= (k+2)! - 1. \end{aligned}$$

Therefore, $P(k+1)$ is true. We have shown that $P(k) \implies P(k+1)$.

Thus, by the principle of mathematical induction, the proof is complete.

Solution for PS9-3. Fix a *particular*, though arbitrary, real number $x \in \mathbb{R} - \{1\}$.

(This is an important step! From here on, for the rest of this proof, x is no longer a variable.)

Let $P_x(n)$ be the following statement:

$$1 + x + x^2 + \cdots + x^n = \frac{x^{n+1} - 1}{x - 1}.$$

We shall prove by induction on n that $\forall n \in \mathbb{N} : P_x(n)$.

Base case. $P_x(0)$ states “ $1 = (x - 1)/(x - 1)$.” This is obviously true.

Induction step. Assume that $P_x(k)$ is true for some $k \geq 0$. Then

$$\begin{aligned} 1 + x + x^2 + \cdots + x^{k+1} &= (1 + x + x^2 + \cdots + x^k) + x^{k+1} \\ &= \frac{x^{k+1} - 1}{x - 1} + x^{k+1} &< \text{by the induction hypothesis} \\ &= \frac{x^{k+1} - 1 + x^{k+2} - x^{k+1}}{x - 1} \\ &= \frac{x^{k+2} - 1}{x - 1} + x^{k+1}. \end{aligned}$$

Therefore, $P_x(k+1)$ is true. We have shown that $P_x(k) \implies P_x(k+1)$.

Thus, by the principle of mathematical induction, we’ve proved that $\forall n \in \mathbb{N} : P_x(n)$.

Since we did this for an arbitrary choice of x , we’ve in fact shown that $\forall x \in \mathbb{R} - \{1\} \forall n \in \mathbb{N} : P_x(n)$.

Solution for PS9-4. Let $P(n)$ be the statement “ $3 \mid n^3 + 2n$.” We shall prove it for all $n \in \mathbb{N}$ by induction on n .

Base case. $P(0)$ states “ $3 \mid 0^3 + 2 \times 0$,” i.e., “ $3 \mid 0$.” This is obviously true.

Induction step. Assume that $P(k)$ is true for some $k \geq 0$. This implies $k^3 + 2k = 3m$, for some $m \in \mathbb{N}$. Notice that

$$(k+1)^3 + 2(k+1) = k^3 + 3k^2 + 3k + 1 + 2(k+1) = (k^3 + 2k) + 3(k^2 + k + 1) = 3(m + k^2 + k + 1).$$

Therefore, $3 \mid (k+1)^3 + 2(k+1)$, i.e., $P(k+1)$ is true. We have shown that $P(k) \implies P(k+1)$.

Thus, by the principle of mathematical induction, the proof is complete.

Solution for PS9-5. Let $P(n)$ be the statement “ $5 \mid 8^n - 3^n$.” We shall prove it for all $n \in \mathbb{N}$ by induction on n .

Base case. $P(0)$ states “ $5 \mid 8^0 - 3^0$,” i.e., “ $5 \mid 1 - 1 = 0$.” This is obviously true.

Induction step. Assume that $P(k)$ is true for some $k \geq 0$. This implies $8^k - 3^k = 5m$, for some $m \in \mathbb{N}$. Notice that

$$8^{k+1} - 3^{k+1} = 8 \cdot 8^k - 3 \cdot 8^k + 3 \cdot 8^k - 3 \cdot 3^k = 5 \cdot 8^k + 3 \cdot 5m = 5(8^k + 3m).$$

Therefore, $5 \mid 8^{k+1} - 3^{k+1}$, i.e., $P(k+1)$ is true. We have shown that $P(k) \implies P(k+1)$.

Thus, by the principle of mathematical induction, the proof is complete.

Solution for PS9-6.

a. Let $P(n)$ denote the statement “ $2^n \geq n^3$ ”. We shall prove that $P(n)$ holds for all $n \geq 10$, by induction on n .

Base case ($n = 10$). The following shows that the base case, i.e., $P(10)$, holds.

$$2^{10} = 1024 > 1000 = 10^3.$$

Induction step ($n \geq 10$). Assume that $P(k)$ is true for some $k \geq 10$. Then

$$\begin{aligned} 2^{k+1} &= 2 \cdot 2^k \\ &\geq 2k^3 && \text{by the induction hypothesis} \\ &= k^3 + k^3 \\ &\geq k^3 + 10k^2 && \text{since } k \geq 10 \\ &\geq k^3 + 3k^2 + 7k && \text{since } k^2 \geq k \\ &\geq k^3 + 3k^2 + 3k + 1 && \text{since } 4k \geq 1 \\ &= (k+1)^3, \end{aligned}$$

which is $P(k+1)$. This proves that $P(k) \implies P(k+1)$ for all $k \geq 10$.

Thus, by the principle of mathematical induction, the proof is complete.

b. Consider the following for $n > 1$.

$$\begin{aligned} \frac{1}{n} - \frac{1}{(n+1)^2} &= \frac{(n+1)^2 - n}{n(n+1)^2} = \frac{n^2 + 2n + 1 - n}{n(n+1)^2} \\ &= \frac{n^2 + n + 1}{n(n+1)^2} \\ &> \frac{n^2 + n}{n(n+1)^2} && \text{this is strictly greater because numerator is 1 less here,} \\ &= \frac{n(n+1)}{n(n+1)^2} \\ &= \frac{1}{n+1}. \end{aligned}$$

Hence, $\frac{1}{n} - \frac{1}{(n+1)^2} > \frac{1}{n+1}$, and multiplying by -1 we get the reverse inequality,

$$-\left(\frac{1}{n} - \frac{1}{(n+1)^2}\right) < -\frac{1}{n+1}. \quad (1)$$

Let $P(n)$ denote the statement

$$\text{“} \sum_{i=1}^n \frac{1}{i^2} < 2 - \frac{1}{n} \text{.”}$$

We shall prove that $P(n)$ holds for all $n > 1$, by induction on n .

Base case ($n = 2$). The following shows that the base case, i.e., $P(2)$, holds.

$$\sum_{i=1}^2 \frac{1}{i^2} = \frac{1}{1} + \frac{1}{4} = \frac{5}{4} < \frac{6}{4} = 2 - \frac{1}{2}.$$

Induction step ($n \geq 2$). Assume $P(k)$ is true for some $k \geq 2$. Then

$$\begin{aligned} \sum_{i=1}^{k+1} \frac{1}{i^2} &= \sum_{i=1}^k \frac{1}{i^2} + \frac{1}{(k+1)^2} \\ &< 2 - \frac{1}{k} + \frac{1}{(k+1)^2} && \text{by induction hypothesis,} \\ &= 2 - \left(\frac{1}{k} - \frac{1}{(k+1)^2}\right) && \text{rearranging,} \\ &< 2 - \frac{1}{k+1} && \text{by (1),} \end{aligned}$$

which is $P(k+1)$. This proves that $P(k) \implies P(k+1)$ for all $k \geq 2$.

Thus, by the principle of mathematical induction, the proof is complete.

Solution for PS9-7. For this problem, we’re given that the basic sum principle holds. Let $P(n)$ be the statement of the extended sum principle, i.e., the statement

$$\text{“If the sets } A_1, A_2, \dots, A_n \text{ are pairwise disjoint, then } |A_1 \cup A_2 \cup \dots \cup A_n| = |A_1| + |A_2| + \dots + |A_n| \text{.”}$$

We shall prove it for all $n \geq 2$ by induction on n .

Base case. $P(2)$ is the basic sum principle, which does hold (we’re given this).

Induction step. Assume that $P(k)$ is true for some $k \geq 2$. Towards proving $P(k+1)$, consider arbitrary pairwise disjoint sets A_1, A_2, \dots, A_{k+1} . Let $C = A_1 \cup A_2 \cup \dots \cup A_{k+1}$ and $B = A_1 \cup A_2 \cup \dots \cup A_k$.

Since A_{k+1} has no elements in common with any of A_1, A_2, \dots, A_k , it has no elements in common with their union either. In other words, $B \cap A_{k+1} = \emptyset$. Therefore,

$$\begin{aligned} |C| &= |B \cup A_{k+1}| \\ &= |B| + |A_{k+1}| && = (k+1)! - 1 + (k+1) \cdot (k+1)! && \triangleleft \text{by the induction hypothesis} \\ &= (k+1)! \cdot (1 + (k+1)) - 1 \\ &= (k+2)! - 1. \end{aligned}$$

Since $P(k)$ is true (this is the induction hypothesis), B is a countable set. Now $C = B \times A_{k+1}$ and we have proved earlier that the Cartesian product of two countable sets is countable. Therefore, C is countable, establishing $P(k+1)$.

Thus, by the principle of mathematical induction, the proof is complete.

Solution for PS9-8. Let $P(n)$ be the statement

“For all sets A_1, A_2, \dots, A_n , if each A_i is countable, then so is $A_1 \times A_2 \times \dots \times A_n$.”

We shall prove it for all $n \in \mathbb{N}^+$ by induction on n .

Base case. $P(1)$ states “For all sets A_1 , if A_1 is countable, then so is A_1 .” This is obviously true.

Induction step. Assume that $P(k)$ is true for some $k \in \mathbb{N}^+$. Towards proving $P(k+1)$, consider arbitrary sets A_1, A_2, \dots, A_{k+1} such that each A_i is countable, and let $C = A_1 \times A_2 \times \dots \times A_{k+1}$. Let $B = A_1 \times A_2 \times \dots \times A_k$. Since $P(k)$ is true (this is the induction hypothesis), B is a countable set. Now $C = B \times A_{k+1}$ and we have proved earlier that the Cartesian product of two countable sets is countable. Therefore, C is countable, establishing $P(k+1)$.

Thus, by the principle of mathematical induction, the proof is complete.

Solution for PS9-9. Let $P(n)$ be the statement “ n can be written as a sum of one or more distinct powers of 2.” We shall prove it for all $n \in \mathbb{N}^+$ by induction on n .

Base case. $P(1)$ states “1 can be written as a sum of one or more distinct powers of 2.”

This is true: we simply write $1 = 2^0$.

Induction step. Assume that $P(m)$ is true for all m with $1 \leq m < k$. We shall now prove $P(k)$.

Let 2^r (where $r \in \mathbb{N}$) be the largest power of 2 that is $\leq k$. In other words, $2^r \leq k < 2^{r+1}$. Two cases arise.

Case 1. We have $k = 2^r$. In this case, k can be written as the “sum” of a single power of 2, namely 2^r . Therefore, $P(k)$ holds.

Case 2. We have $k > 2^r$. In this case, let $\ell = k - 2^r \in \mathbb{N}^+$. By the induction hypothesis, $P(\ell)$ is true, so we can write $\ell = 2^{a_1} + 2^{a_2} + \dots + 2^{a_s}$, where $a_1 < a_2 < \dots < a_s$. Therefore,

$$k = \ell + 2^r = 2^{a_1} + 2^{a_2} + \dots + 2^{a_s} + 2^r.$$

We’re almost there, but we have to show that 2^r is distinct from all the other powers of 2 appearing above. But $k < 2^{r+1}$, so $2^{a_s} \leq \ell = k - 2^r < 2^r$. It follows that $a_s < r$, which proves the distinctness. Therefore, $P(k)$ holds.

We have now proved that $P(1) \wedge P(2) \wedge \dots \wedge P(k-1) \implies P(k)$.

Thus, by the (strong version of the) principle of mathematical induction, the proof is complete.

Alternate Solution for PS9-9. We can do the induction step differently. Let’s jump right in to that part of the proof. We’re trying to prove $P(k)$.

Case 1. k is even. By the induction hypothesis, $P(k/2)$ is true, so we can write $k/2 = 2^{a_1} + 2^{a_2} + \dots + 2^{a_s}$, where $a_1 < a_2 < \dots < a_s$. Therefore,

$$k = 2^{1+a_1} + 2^{1+a_2} + \dots + 2^{1+a_s}$$

and these powers of 2 are in ascending order, so they are distinct. Therefore, $P(k)$ holds.

Case 2. k is odd. By the induction hypothesis, $P((k-1)/2)$ is true. This means that we can write $(k-1)/2 = 2^{a_1} + 2^{a_2} + \dots + 2^{a_s}$, where $a_1 < a_2 < \dots < a_s$. Therefore,

$$k = 1 + 2\left(\frac{k-1}{2}\right) = 2^0 + 2^{1+a_1} + 2^{1+a_2} + \dots + 2^{1+a_s}.$$

Again, these powers of 2 are in ascending order, so they are distinct. Therefore, $P(k)$ holds.

The rest of the proof is the same as before.

Solution for PS9-10. For all integers $r \in \mathbb{N}^+$, let $Q(r)$ be the statement that for all rectangular bars of chocolate with r tiles, the number of snap operations used to break the bar into individual tiles must be exactly $r - 1$. The proof is by strong induction on $Q(r)$.

Base Case $Q(1) = 0$, because a bar with one tile is already broken into individual tiles, and because the bar can not longer be broken into two distinct parts.

Induction Step For any $t \geq 2$, assume that for all $1 \leq k < t$, $Q(k)$ is true. To prove that $Q(t)$ follows, consider any rectangular bar with t tiles. Any snap operation divides the rectangle into two rectangular fragments with a and b tiles, respectively, so that $a + b = t$. The number of snaps used to reduce the bar into individual tiles is one plus the number of snaps required to resolve each of the two fragments:

$$Q(t) = 1 + Q(a) + Q(b) = 1 + (a - 1) + (b - 1) = a + b - 1 = t - 1.$$

This is always the same value, no matter how the bar is partitioned into two parts.

By strong induction, $Q(t) = t - 1$ for all rectangular chocolate bars. As an $m \times n$ bar has mn tiles, it uses exactly $mn - 1$ snaps to break up into individual tiles.

(The proof only uses the fact that each snap partitions the bar—a collection of tiles—into two (disjoint) smaller collections. The shape of the bar and manner of snapping do not matter.)

Solution for PS9-11. Let $P(m)$ denote the statement “if a tournament has a cycle of length m , then it has a cycle of length 3”. We shall prove that for all $m \geq 3$ ($P(m)$), by induction on m .

Base case ($m = 3$). $P(3)$ is a statement of the form “if X , then X ”, so it is trivially true.

Assume $P(k)$ is true for some $k \geq 3$. We’re going to prove $P(k + 1)$.

First note that $P(k + 1)$ is implicitly a “for all” statement. So, to prove it, we consider an arbitrary tournament that has a cycle of length $k + 1$, consisting of the players $\{p_1, p_2, p_3, \dots, p_k, p_{k+1}\}$, where p_1 beats p_2 , who beats p_3, \dots , who beats p_{k+1} , who beats p_1 . Now consider first 3 players in the cycle: $\{p_1, p_2, p_3\}$. Two cases arise.

Case 1: p_3 beats p_1 . Then we have a cycle of length 3, consisting of the players $\{p_1, p_2, p_3\}$, where p_1 beats p_2 , who beats p_3 , who beats p_1 .

Case 2: p_1 beats p_3 . Then our tournament has a cycle of length k , consisting of the players $\{p_1, p_3, p_4, \dots, p_k, p_{k+1}\}$, where p_1 beats p_3 , who beats p_4, \dots , who beats p_{k+1} , who beats p_1 . By the induction hypothesis, the existence of this cycle implies that the tournament has a cycle of length 3.

In both cases we concluded that our tournament has a cycle of length 3. Therefore $P(k + 1)$ is true. This shows that $P(k) \implies P(k + 1)$.

Thus, by mathematical induction, it follows that $\forall m \geq 3 (P(m))$. □

- a. If we pick just one kind of candy (two pieces of it), there are 6 choices.
If we pick two distinct kinds of candy, there are $\binom{6}{2}$ choices.
Together, there are $6 + \binom{6}{2} = 21$ choices.
- b. We break this down into three disjoint cases and add up the results.
- All three pieces of candy are of the same kind: $\binom{6}{1}$ choices.
 - We pick exactly two kinds of candy: this gives us $\binom{6}{2}$ to choose the two kinds, following which we have to choose which of the two kinds we're going to pick two pieces of. By the generalized product principle, there are $\binom{6}{2} \cdot 2$ choices overall.
 - We pick three distinct kinds of candy: $\binom{6}{3}$ choices.

- a. With books \square and separator \blacklozenge , one configuration is $\square\square\blacklozenge\square\square\square\square\square\blacklozenge\square\square\square\square\square\blacklozenge\square\square\blacklozenge$. If the candy types are ordered and denoted A,B,C,D,E,F , then number of each type can be determined by counting the number of books between a given pair of separators. The configuration can be written as $AA\blacklozengeBBBBB\blacklozengeDDDDDD\blacklozengeEE\blacklozenge$, so that 2 pieces of A , 5 pieces of type B , 6 pieces of D , and 2 of E are chosen.
- A second layout is $\square\blacklozenge\square\square\blacklozenge\square\square\square\square\blacklozenge\square\square\square\square\square\blacklozenge\square\square$, producing 1, 2, 3, 4, 3, 2 counts of types A, B, C, D, E, F , respectively.
- b. $\binom{20}{5}$, the number of ways to place 5 separators in a list of 20 items (books + separators).
- c. Applying the book/separator model, there are t books, and $n - 1$ separators. The final count is $\binom{t+n-1}{n-1}$.

- a. Use $f(x_1, x_2, \dots, x_k) = \underbrace{000 \cdots 0}_x 1 \underbrace{000 \cdots 0}_x 1 \cdots \cdots \underbrace{000 \cdots 0}_x 1 \underbrace{000 \cdots 0}_{n-(x_1 + \cdots + x_k)}$.
- b. Use $g(y_1, y_2, \dots, y_k) = (y_1, y_2 - y_1, y_3 - y_2, \dots, y_k - y_{k-1})$.
- c. $|S_{n,k}| = |L_{n,k}| = \binom{n+k}{k}$.

- a.
- $$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n \cdot (n-1)!}{k \cdot (k-1)!(n-k)!} = \frac{n}{k} \frac{(n-1)!}{(k-1)!((n-1)-(k-1))!} = \frac{n}{k} \binom{n-1}{k-1}$$
- b.
- $$\binom{n}{m} \binom{m}{k} \cdot 1 = \frac{n!}{m!(n-m)!} \cdot \frac{m!}{k!(m-k)!} \cdot \frac{(n-k)!}{(n-k)!} = \frac{n!}{k!(n-k)!} \cdot \frac{(n-k)!}{(m-k)!(n-k-(m-k))!} = \binom{n}{k} \binom{n-k}{m-k}$$

- a.** Let $x = 1, y = 1$. By the binomial theorem,

$$\begin{aligned} 2^n &= (1+1)^n = (x+y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k \\ &= \sum_{k=0}^n \binom{n}{k} 1^{n-k} 1^k = \sum_{k=0}^n \binom{n}{k}. \end{aligned}$$

- b. Let $x = -1$, $y = 1$. Applying the binomial theorem,

$$\begin{aligned} 0 &= (1 - 1)^n = (x + y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k \\ &= \sum_{k=0}^n \binom{n}{k} 1^{n-k} (-1)^k = \sum_{k=0}^n (-1)^k \binom{n}{k}. \end{aligned}$$

Solution for PS10-6.

- a. By the binomial theorem,

$$3^n = (1 + 2)^n = \sum_{k=0}^n \binom{n}{k} 2^k 1^{n-k} = \sum_{k=0}^n \binom{n}{k} 2^k.$$

- b. Starting with the binomial theorem on $(1 + 1)^{n-1}$,

$$\begin{aligned} (1 + 1)^{n-1} &= \sum_{k=0}^{n-1} \binom{n-1}{k} \\ n2^{n-1} &= \sum_{k=0}^{n-1} n \binom{n-1}{k} && \text{multiplying by } n \\ n2^{n-1} &= \sum_{k=0}^{n-1} (k+1) \frac{n}{k+1} \binom{n-1}{k} \\ n2^{n-1} &= \sum_{k=0}^{n-1} (k+1) \binom{n}{k+1} && \text{by PS10-4 a} \\ n2^{n-1} &= \sum_{k=1}^n k \binom{n}{k} && \text{reindexing} \\ n2^{n-1} &= \sum_{k=0}^n k \binom{n}{k} && \text{adding a term at } k = 0 \text{ whose value is } 0 \end{aligned}$$

We have derived the statement to be proven.

Solution for PS10-7.

- a. Both sides of the equation equal the number of subsets of an arbitrary n -element set S . The total number of subsets is well known to be 2^n . The sum on the left hand side, counts, for each $0 \leq k \leq n$, the number of subsets of S containing k elements, and sums the result. Since all subsets of S are counted exactly once on the left hand side, the left hand side counts all subsets of S , and equals the right hand side. \square
- b. The equation is equivalent to the claim that the number of odd subsets of a given n -element set equals the number of even subsets. This is true by the previous homework problem **PS2-5**^{HW}. \square
- c. There is a well-known committee-chairperson fable. Both expressions indicate the number of ways to pick a k person committee from n candidates, with a single designated chairperson. Using Generalized Product Principle, $k \binom{n}{k}$ is the number of ways ($\binom{n}{k}$) to pick a committee, multiplied by the number of ways to then pick a chairperson from that committee (k). $n \binom{n-1}{k-1}$ is the number of ways to pick a chairperson (n) times the number of ways to pick everyone else in the committee ($\binom{n-1}{k-1}$). \square
- d. A generalization of the committee-chairperson story. Given a set A of n elements, both sides express the number of ways to pick an m -element subset B of A , and a k -element subset C of B . The $\binom{n}{m} \binom{m}{k}$ is the number of ways to pick the subset B as a subset of A first, and then pick C as a subset of B ; the $\binom{n}{k} \binom{n-k}{m-k}$ is the number of ways to pick C as a subset of A , and then pick $B - C$ as a subset of $A - C$. \square

- e. For a given set S with n elements, 3^n is the number of functions from S to $0, 1, 2$. For each such function f , we can define a function $g : R(f) \rightarrow 0, 1$ on the set $R(f) = \{x \in S : f(x) \in \{1, 2\}\}$ by $g(x) = f(x)$. Counting the number of functions g , we find that for each size k of the domain for g , there are $\binom{n}{k}$ possible k -element domains that are subsets of S , and 2^k possible functions.

Viewed in terms of the hint, there are two methods to find the number of possible sets A, B for which $B \subseteq A \subseteq \{1, 2, \dots, n\}$. First, for each $i \in \{1, 2, \dots, n\}$, there are three possible states relative to A and B : either $i \notin A$, $i \in B$, or $i \in A - B$. From this one can derive a total count of 3^n . An argument, partitioning by the size of A , as in the previous paragraph will also give $\sum_{k=0}^n \binom{n}{k} 2^k = 3^n$.

- f. Both sides indicate the number of ways to pick a committee (with at least one person) from a set of n candidates. One could first pick a chairperson (n choices), and then pick the rest of the committee (2^{n-1} choices). Alternatively, one could, for each size of a committee, first pick a committee ($\binom{n}{k}$ choices), and then pick a chairperson (k choices); adding the product over all possible committee sizes gives $\sum_{k=0}^n k \binom{n}{k}$.

Solution for PS10-8.

- a. For each k , we prove the identity by induction over n . Let $P_k(n)$ be the proposition that the equation

$$\sum_{m=k}^n \binom{m}{k} = \binom{n+1}{k+1}.$$

is true. We will show by induction that $P_k(n)$ is true for all $n \geq k$.

Base case. This is $P_k(k)$, which is true since

$$\sum_{m=k}^k \binom{m}{k} = \binom{k}{k} = 1 = \binom{k+1}{k+1}$$

Induction step. We seek to prove $P_k(n)$, for $n > k$, assuming that $P_k(n-1)$ is true. Since by $P_k(n-1)$,

$$\sum_{m=k}^{n-1} \binom{m}{k} = \binom{n}{k+1},$$

adding $\binom{n}{k}$ to both sides produces

$$\begin{aligned} \sum_{m=k}^{n-1} \binom{m}{k} + \binom{n}{k} &= \binom{n}{k+1} + \binom{n}{k} \\ \sum_{m=k}^n \binom{m}{k} &= \binom{n}{k+1} + \binom{n}{k} \\ \sum_{m=k}^n \binom{m}{k} &= \binom{n+1}{k+1}, \end{aligned}$$

where the last line follows by Pascal's identity. □

- b. Let $V = \{1, 2, \dots, n+1\}$. Then the number of ways to pick a $k+1$ element set $J \subset V$ is $\binom{n+1}{k+1}$. One can also pick a such a subset J by first picking the *smallest* element i_{\min} of J , and then the remainder of J , ($J - \{i_{\min}\}$, a set of k elements), for which there are $\binom{n+1-i_{\min}}{k}$ choices. As the possible values of i_{\min} range from 1 to $n+1-k$, combining the number of sets produced for each value of i_{\min} gives the sum $\sum_{m=1}^{n+1-k} \binom{n+1-m}{k} = \sum_{m=k}^n \binom{m}{k}$. □

Solution for PS10-9. If p is a prime, $0 < k < p$,

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}.$$

Since $p! = p \cdot (p-1) \cdots 2 \cdot 1$, $p \mid p!$. On the other hand, since $k < p$, $p \nmid i$, for all $1 \leq i \leq k$, so by iterated applications of the contrapositive of Euclid's lemma, $p \nmid k!$. Similarly, as $p - k < p$, $p \nmid (p - k)!$.

Let $a = n!$, $b = k!(p - k)!$. Since we know $\frac{a}{b} \in \mathbb{Z}$, there is some constant $c \in \mathbb{Z}$ for which $a = bc$. Since $p \mid a$, and $p \nmid b$, by Euclid's lemma, $p \mid c$. Defining $d = \frac{c}{p} \in \mathbb{Z}$, we find $\frac{a}{b} = \frac{p d b}{b} = p d$. Since p is a factor of the integer product $p d$, it is a factor of $\frac{a}{b} = \binom{p}{k}$.

Solution for PS11-1.

- a. For this problem, let $D = \{0, 1, 2, \dots, 9\}$ and $P = \{1, 2, \dots, 9\}$.
- *Sample space:* $S = \{(d_1, d_2, \dots, d_k) : \text{each } d_i \text{ is a digit}\} = D^k$.
 - *Events of interest:* $E = \{(d_1, d_2, \dots, d_k) \in S : \text{each } d_i \neq 0\} = P^k$.
 - *Outcome probabilities:* Each outcome in S is given to be equally likely (see the words “independently and uniformly at random” in the problem statement), so the probability of each outcome is $1/|S|$.
 - *Event Probabilities:* Because of the uniformity, $\Pr[E] = |E|/|S| = |P^k|/|D^k| = (9/10)^k$.

b. Zephyr, please fill in details.

$$\text{Final answer} = \binom{90}{10} / \binom{100}{10}.$$

- c.
- *Sample space:* $S = \{(a, b) : a \neq b \text{ and } 1 \leq a, b \leq 5\}$.
 - *Events of interest:* $E = \{(2, 1), (3, 1), (4, 1), (5, 1), (1, 3), (2, 3), (4, 3), (5, 3), (1, 5), (2, 5), (3, 5), (4, 5)\}$.
 - *Outcome probabilities:* Uniform, by the given info.
 - *Event Probabilities:* $\Pr[E] = |E|/|S| = 12/(5 \times 4) = 3/5$.

d. Zephyr, please fill in details.

$$\text{Final answer} = 1/n.$$

- e.
- *Sample space:* $S = \{H, T\}^n = \{\text{length } n \text{ sequences of letters H or T}\}$.
 - *Events of interest:*

$$\begin{aligned} E &= \{HHH \cdots H, THH \cdots H, TTH \cdots H, \dots, TT \cdots TH, TTT \cdots T\} \\ &= \{T^i H^{n-i} : 0 \leq i \leq n\}. \end{aligned}$$

- *Outcome probabilities:* Uniform, as each character in a string of heads or tails has equal probability to be H or T. The probability of any specific string is the probability that n independent coin flips produce the string, namely $(1/2)^n$, and is the same for all strings.
 - *Event Probabilities:* $\Pr[E] = |E|/|S| = (n+1)/2^n$.
- f. Let D be the set of all cards in the deck, so that $|D| = 52$, S be the set of 13 spades, and H be the initial hand of five cards.
- *Sample space:* $\Omega = \{\{a, b\} \subset D - H\}$, the set of groups of two cards drawn from the set of cards not currently in the hand. As the cards are drawn from “the rest of the deck”, the two discarded cards are not eligible to be selected.
 - *Events of interest:* $E = \{\{a, b\} \subset S - H\}$, the set of spades that are not currently in hand.
 - *Outcome probabilities:* As the cards are selected uniformly at random, the probabilities corresponding to each set of two cards are also uniform.
 - *Event Probabilities:* $\Pr[E] = |E|/|S| = \binom{|S-H|}{2} / \binom{|D-H|}{2} = \binom{10}{2} / \binom{47}{2}$.

Solution for PS11-2.

- a. Let D be the standard set of 52 cards.
- *Sample space:* $S = \{H \subseteq D : |H| = 5\}$.
 - *Events of interest:* $E = \{H \in S : H \text{ is a full house}\}$.
 - *Outcome probabilities:* Uniform, according to the given information.
 - *Event Probabilities:* Because of the uniformity, $\Pr[E] = |E|/|S|$. Clearly, $|S| = \binom{52}{5}$. To count $|E|$, break down the processing of choosing five cards to create a full house as follows:
 - Step 1. Choose the rank of the triplet; there are 13 choices.
 - Step 2. Choose the rank of the doublet; there are 12 choices, given the previous choice.
 - Step 3. Choose the suits of the three cards in the triplet; there are $\binom{4}{3} = 4$ choices.
 - Step 4. Choose the suits of the two cards in the doublet; there are $\binom{4}{2} = 6$ choices.

By the generalized product principle, $|E| = 13 \times 12 \times 4 \times 6$.

Therefore, $\Pr[E] = 3744 / \binom{52}{5} \approx 0.0014405762304921968 \approx 0.14\%$.

b. Let B be the standard bag of 100 Scrabble tiles and let $C \subseteq B$ be the set of non-blank tiles: $|C| = 98$.

- *Sample space:* $S = \{R \subseteq B : |R| = 7\}$.
- *Events of interest:* $E = \{R \in S : R \not\subseteq C\}$ is the event that our rack doesn't consist only of non-blanks, i.e., that our rack contains a blank. We'll work instead with the complement $\bar{E} = \{R \subseteq C : |R| = 7\}$.
- *Outcome probabilities:* Uniform, according to the given information.
- *Event Probabilities:* Because of the uniformity,

$$\Pr[E] = \frac{|E|}{|S|} = 1 - \frac{|\bar{E}|}{|S|} = 1 - \frac{\binom{98}{7}}{\binom{100}{7}} = 1 - \frac{93 \times 92}{100 \times 99} \approx 0.1357575758 \approx 13.58\%.$$

c. The answer is the same as before.

The easiest way to see this by using a different sample space that makes a certain symmetry clear. First, let's give each of the 100 Scrabble tiles a unique index and assume that tiles #99 and #100 are the two blanks. Now let's model the experiment as choosing 14 tiles from the bag: the first seven for your opponent and the next seven for you.

- *Sample space:* $S = \{(x_1, \dots, x_{14}) : \text{each } x_i \in \{1, \dots, 100\} \text{ and } x_i \neq x_j \text{ for } i \neq j\}$.
- *Events of interest:* $F = \{(x_1, \dots, x_{14}) \in S : x_i \geq 99 \text{ for some } i \in \{8, \dots, 14\}\}$. Let's also consider another event $G = \{(x_1, \dots, x_{14}) \in S : x_i \geq 99 \text{ for some } i \in \{1, \dots, 7\}\}$; we'll soon see why.
- *Outcome probabilities:* Uniform, according to the given information.
- *Event Probabilities:* We want to compute $\Pr[F]$. In **PS11-2 b**, we computed $\Pr[G]$ (using a different sample space to model the experiment). But now consider the function $f : F \rightarrow G$ given by

$$f(x_1, \dots, x_7, x_8, \dots, x_{14}) = f(x_8, \dots, x_{14}, x_1, \dots, x_7).$$

It is a bijection from F to G (notice that $f^{-1} = f$), proving that $|F| = |G|$. Therefore,

$$\Pr[F] = |F|/|S| = |G|/|S| = \Pr[G] \approx 13.58\%.$$

Solution for PS11-3.

Step 1: Define the sample space.

Let W denote a Boston Red Sox win in a particular game, and L denote a Boston Red Sox loss. Then, $S = \{WW, WLW, LL, LWL, LWW, WLL\}$.

Step 2: Define events of interest.

Part (a): Let A be the event that a total of 3 games are played.

So, $A = \{WLW, LWL, LWW, WLL\}$.

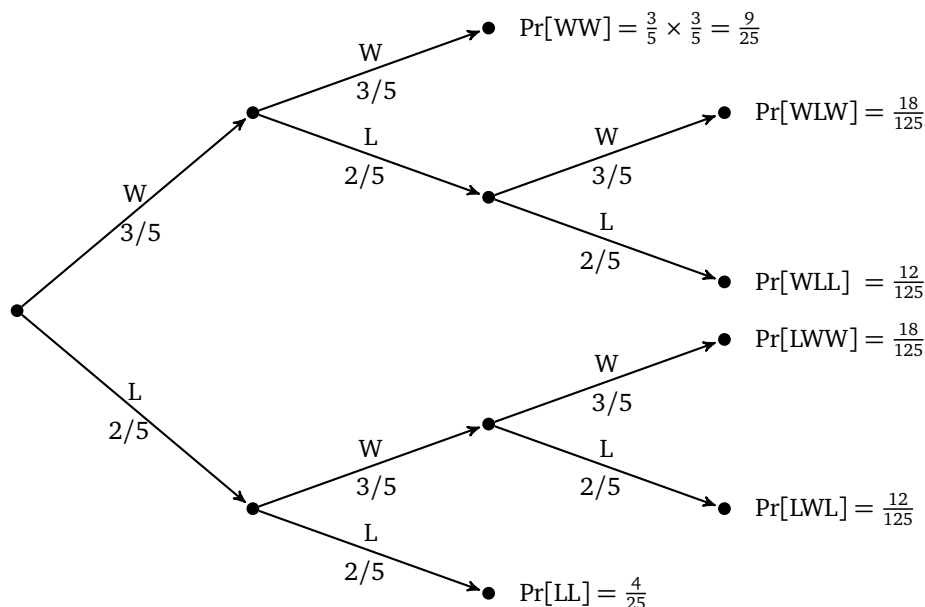
Part (b): Let B be the event that the winner of the series loses the first game.

So, $B = \{LWW, WLL\}$.

Part (c): Let C be the event that the *correct* team (which is obviously Red Sox) wins the series.

So, $C = \{WW, WLW, LWW\}$.

Step 3: Figure out outcome probabilities.



Sample space is set of leaves of the tree in the figure.

Step 4: Compute event probabilities.

$$\Pr[A] = \Pr[\{WLW, LWL, LWW, WLL\}] = \frac{18}{125} + \frac{12}{125} + \frac{18}{125} + \frac{12}{125} = \frac{12}{25},$$

$$\Pr[B] = \Pr[\{LWW, WLL\}] = \frac{18}{125} + \frac{12}{125} = \frac{6}{25},$$

$$\Pr[C] = \Pr[\{WW, WLW, LWW\}] = \frac{9}{25} + \frac{18}{125} + \frac{18}{125} = \frac{45 + 18 + 18}{125} = \frac{81}{125}.$$

Solution for PS11-4. Part (i). Rolling total is 8.

- (a) When two dice are rolled, the sample space $S = \{(x, y) : 1 \leq x \leq 6; 1 \leq y \leq 6\}$

Our event of interest $A = \{(x, y) : x + y = 8; 1 \leq x \leq 6; 1 \leq y \leq 6\} = \{(2, 6), (3, 5), (4, 4), (5, 3), (6, 2)\}$.

Each outcome is equally likely. Hence, $\Pr[A] = |A|/|S| = 5/36$

- (b) When three dice are rolled, the sample space $S = \{(x, y, z) : 1 \leq x \leq 6; 1 \leq y \leq 6; 1 \leq z \leq 6\}$

Our event of interest $B = \{(x, y, z) : x + y + z = 8; 1 \leq x \leq 6; 1 \leq y \leq 6; 1 \leq z \leq 6\}$

Each outcome is equally likely. Hence, $\Pr[B] = |B|/|S| = |B|/216$.

So we need to find $|B|$. We shall check the possible unordered outcomes and then find the number of ways each of them can be permuted to get the number of ordered outcomes (x, y, z) .

$(1, 1, 6) \rightarrow 3!/2! = 3$ ways.

$(1, 2, 5) \rightarrow 3! = 6$ ways.

$(1, 3, 4) \rightarrow 3! = 6$ ways.

$(2, 2, 4) \rightarrow 3!/2! = 3$ ways.

$(2, 3, 3) \rightarrow 3!/2! = 3$ ways.

Hence, $|B| = 3 + 6 + 6 + 3 + 3 = 21$. Hence $\Pr[B] = 21/216 = 7/72$.

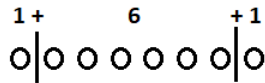
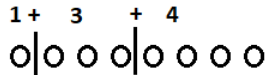
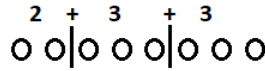
Alternate Solution 1: Let $x = 1 + x_1$ and $y = 1 + x_2$. Then, $x_1, x_2 \geq 0$ and $x + y + z = 8 \Rightarrow x_1 + x_2 + z = 6$.

Since $z \geq 1$, we get $x_1 + x_2 \leq 5$. Note that this ensures $0 \leq x_1, x_2 \leq 5$ and hence, $x, y, z \leq 6$.

Thus, to count $|B|$, it is enough to find the number of possible non-negative integer solutions to the inequality $x_1 + x_2 \leq 5$.

This is exactly $|S_{5,2}|$ as defined in **PS6-4**. So, by Part **c** of **PS6-4**, $|S_{5,2}| = \binom{5+2}{2} = 21$.

Alternate Solution 2: Finding the value of $|B|$ is same as finding the number of possible positive integer solutions to the equation $x + y + z = 8$. (Note that x, y, z being positive and summing up to 8 ensures that $x, y, z \leq 6$.) This is same as the number of ways of partitioning 8 identical objects into 3 groups. So this is same as arranging the 8 objects in a row and finding the number of ways of placing partition markers in any 2 gaps between the elements (so that it is partitioned into $2 + 1 = 3$ groups). There are 7 gaps between the 8 elements and we choose any 2 gaps to place the markers. So this can be done in $\binom{7}{2} = 21$ ways.



Therefore, $Pr[A] = 5/36 = 10/72 > 7/72 = Pr[B]$.

Hence it is more likely to get a total of 8 when two dice are rolled than when three dice are rolled.

Part (ii). Rolling total is 9.

This is similar to **Part(i)** and we get that when two dice are rolled, the probability is $1/9$ and when three dice are rolled, it is $25/216$. So it is more likely to get a rolling total of 9 when three dice are rolled than when two dice are rolled.

Note: For **Part(ii)**, if you use one of the alternate methods mentioned in **Part(i)**, the equations will no longer ensure that $x, y, z \leq 6$. However, it will ensure that $x, y, z \leq 7$. So you have to eliminate the 3 cases $(1, 1, 7), (1, 7, 1), (7, 1, 1)$ in the end to get the correct number.

Solution for PS11-5.

Step 1: Define the sample space.

Let's think from the perspective of the first player. In each *round* (two tosses), let W denote the first player wins; let L denote the first player loses; let T denote neither player wins (tie). Then

$$S = \{W, L, TW, TL, TTW, TTL, \dots\}$$

Step 2: Define events of interest.

At the end of the game, let E_W denote the first player wins, E_L denote the first player loses, E_T denote neither player wins. Note that the game will not stop until the winner is determined. Then

$$E_W = \{W, TW, TTW, \dots\}$$

$$E_L = \{L, TL, TTL, \dots\}$$

$$E_T = \phi$$

Step 3: Figure out outcome probabilities.

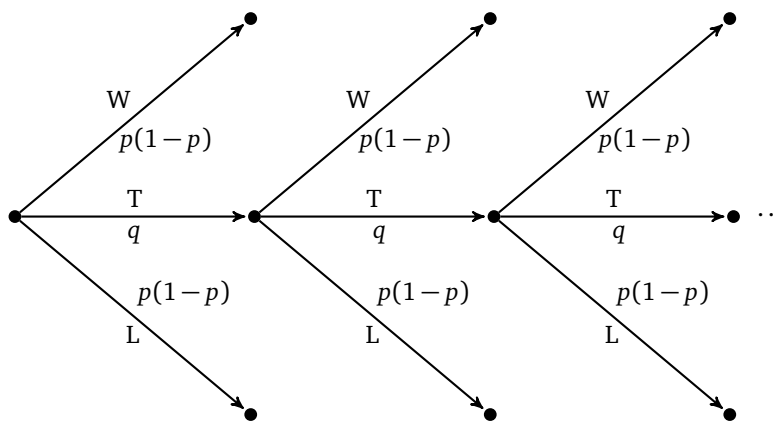
In each round,

$$Pr[W] = p(1-p)$$

$$Pr[L] = p(1-p)$$

$$\Pr[T] = p^2 + (1-p)^2 = q \text{ (Say)}$$

$$\Pr[W] = p(1-p) \quad \Pr[TW] = qp(1-p) \quad \Pr[TTW] = q^2p(1-p)$$



$$\Pr[L] = p(1-p) \quad \Pr[TL] = qp(1-p) \quad \Pr[TTL] = q^2p(1-p)$$

Step 4: Compute event probabilities.

$$\Pr[E_W] = \Pr[\{W, TW, TTW, \dots\}] = \sum_{i=0}^{\infty} q^i p(1-p)$$

$$\Pr[E_L] = \Pr[\{L, TL, TTL, \dots\}] = \sum_{i=0}^{\infty} q^i p(1-p)$$

$$\Pr[E_T] = \Pr[\phi] = 0$$

We can obtain the probabilities by summing the infinite series. But let's use some neat trick here. Let $s = \Pr[E_W]$. We can observe that $\Pr[E_W] = \Pr[E_L]$, so, $s = \Pr[E_L]$. And because $E_W \cap E_L = \emptyset$, we can apply *Disjoint Sum Rule* here. So, $\Pr[E_W \cup E_L] = \Pr[E_W] + \Pr[E_L] = 2s$. Besides, we know that $E_W \cup E_L = S$ is a certain event. So,

$$\Pr[E_W \cup E_L] = \Pr[E_W] + \Pr[E_L] = 2s = 1$$

So,

$$s = \frac{1}{2}$$

Alternate Solution: We can see that the tree is repeating itself. In the beginning of every new round, the probability that the first player wins is always s , regardless of previous results. So, we can obtain an equation as follows:

$$s = \underbrace{p(1-p)}_{\text{wins in the first round}} + \underbrace{qs}_{\text{wins in the other rounds}}$$

$$s = p(1-p) + (p^2 + (1-p)^2)s$$

$$2p(p-1)s = p(p-1)$$

Because $0 < p < 1$

$$s = \frac{1}{2}$$

Solution for PS11-6. Let's first clarify what a strategy is. A strategy is a *plan* for a game, which tells you what to do ("take" or "skip") under *all* circumstances in the course of a game until you reach the end of the game. Under a strategy, there is a probability to win the game. So we can define a function $q(n, k, S)$ as the probability of winning when we have n cards with k black ones and we use strategy S . If we let S_0 denote the strategy "take the top card", then

$$q(n, k, S_0) = \frac{k}{n}$$

Then let's define our predicate. Let $P(n)$ denote the statement "for any k such that $0 \leq k \leq n$ and any strategy S , $q(n, k, S) \leq q(n, k, S_0) = k/n$." We shall prove that for all $n \geq 1$ ($P(n)$), by induction on n .

Base case: ($n = 1$). As we have only one card, there is only one strategy, which is "take the top card". So, for $k = 0, 1$ and any strategy S , $q(n, k, S) \leq q(n, k, S_0) = k/n$, i.e., $p(1)$ holds.

Induction step: ($n \geq 1$).

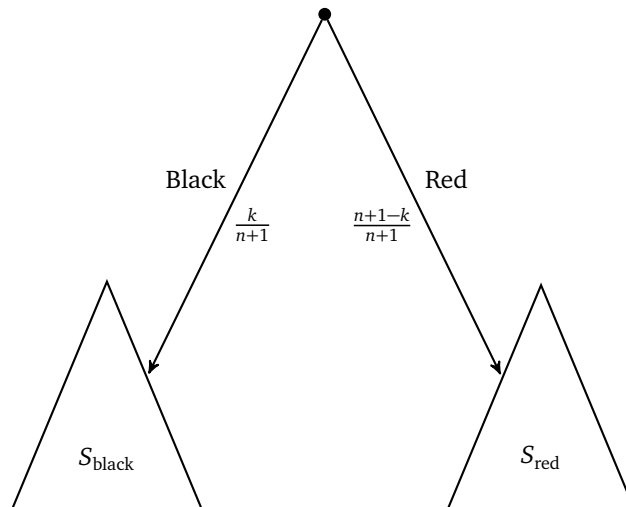
Assume $P(n)$. Consider $P(n + 1)$.

if $k = 0$, whatever your strategy S is, $q(n + 1, k, S) = 0$, because there are no black cards, which means we will never win the game. So, $q(n + 1, k, S) \leq q(n + 1, k, S_0) = k/(n + 1)$.

if $k = n + 1$, whatever your strategy S is, $q(n + 1, k, S) = 1$, because there are all black cards, which means we will always win the game. So, $q(n + 1, k, S) \leq q(n + 1, k, S_0) = k/(n + 1)$.

if $1 \leq k \leq n$, consider any other strategy but S_0 . We shall skip the first card, otherwise it is S_0 . After the first card is revealed: if it turns out to be black (in a probability of $k/(n + 1)$), we know that $k - 1$ black cards remain in the rest n cards, and let S_{black} denote the following sub-strategy; if it turns out to be red (in a probability of $(n + 1 - k)/(n + 1)$), we know that k black cards remain in the rest n cards, and let S_{red} denote the following sub-strategy. So,

$$\begin{aligned} q(n + 1, k, S) &= \frac{k}{n + 1} \cdot q(n, k - 1, S_{\text{black}}) + \frac{n + 1 - k}{n + 1} \cdot q(n, k, S_{\text{red}}) \\ &\leq \frac{k}{n + 1} \cdot \frac{k - 1}{n} + \frac{n + 1 - k}{n + 1} \cdot \frac{k}{n} && \text{(by assumption } p(n)) \\ &= \frac{k^2 - k + nk + k - k^2}{n(n + 1)} \\ &= \frac{k}{n + 1} \\ &= q(n + 1, k, S_0) \end{aligned}$$



So we proved that

$$q(n+1, k, S) \leq q(n+1, k, S_0)$$

This is exactly $P(n+1)$. So we have shown that $P(n) \implies P(n+1)$. This completes the proof by induction.

Solution for PS11-7.

- a. $\Pr[A] = \Pr[(A-B) \cup (A \cap B)] = \Pr[A-B] + \Pr[A \cap B]$
- b. $1 = \Pr[S] = \Pr[A] + \Pr[\bar{A}]$, where S is the sample space.
- c. $\Pr[A \cup B] = \Pr[(A-B) \cup B] = \Pr[A-B] + \Pr[B]$; now use Part a.
- d. Use Part c and the fact that $\Pr[A \cap B] \geq 0$.
- e. $\Pr[B] = \Pr[A \cup (B-A)] = \Pr[A] + \Pr[B-A] \geq \Pr[A]$.

Solution for PS12-1. There is a tempting intuitive approach to the first question: “Given the value of one die, the other die still equally likely to be any of the six possible values, so the probability of hitting the exact value required to win is $1/6$.” This is incorrect!

Instead, let us do our usual four steps. Let $D = \{1, 2, 3, 4, 5, 6\}$ be the possible values shown by one die.

- *Sample space:* $S = D \times D$.
- *Events of interest:*

$W = \{(x, y) \in S : x + y = 7\}$ is the event that you won;

$E_6 = \{(x, y) \in S : x = 6 \vee y = 6\}$ is the event that one of the dice came up six;

$E_5 = \{(x, y) \in S : x = 5 \vee y = 5\}$ is the event that one of the dice came up five.

- *Outcome probabilities:* Uniform on S , since the dice are fair.
- *Event Probabilities:* The two parts of the problem are asking for $\Pr[W \mid E_6]$ and $\Pr[E_5 \mid W]$, respectively.

a. Using the definition of conditional probability,

$$\Pr[W \mid E_6] = \frac{\Pr[W \cap E_6]}{\Pr[E_6]} = \frac{|W \cap E_6|/|S|}{|E_6|/|S|} = \frac{|\{(1, 6), (6, 1)\}|}{|\{(1, 6), \dots, (5, 6), (6, 6), (6, 5), \dots, (6, 1)\}|} = \frac{2}{11}.$$

b. Similarly,

$$\Pr[E_5 \mid W] = \frac{\Pr[E_5 \cap W]}{\Pr[W]} = \frac{|E_5 \cap W|/|S|}{|W|/|S|} = \frac{|\{(2, 5), (5, 2)\}|}{|\{(1, 6), (2, 5), (3, 4), (4, 3), (5, 2), (6, 1)\}|} = \frac{1}{3}.$$

Solution for PS12-2.

- 4/9.
- 5/23.

Solution for PS12-5.

a.

$$\begin{aligned} & \Pr[A_1] \cdot \Pr[A_2 \mid A_1] \cdot \Pr[A_3 \mid A_1 \cap A_2] \cdots \Pr[A_n \mid A_1 \cap A_2 \cap \cdots \cap A_{n-1}] \\ &= \Pr[A_1] \cdot \frac{\Pr[A_1 \cap A_2]}{\Pr[A_1]} \cdot \frac{\Pr[A_1 \cap A_2 \cap A_3]}{\Pr[A_1 \cap A_2]} \cdot \frac{\Pr[A_1 \cap A_2 \cap A_3 \cap A_4]}{\Pr[A_1 \cap A_2 \cap A_3]} \cdots \frac{\Pr[A_1 \cap A_2 \cap \cdots \cap A_n]}{\Pr[A_1 \cap A_2 \cap \cdots \cap A_{n-1}]} \\ &= \Pr[A_1 \cap A_2 \cap \cdots \cap A_n] \end{aligned}$$

b. For $i = 1, 2, \dots, n$, let A_i be the event that the i th passenger (to board the flight) sits on his assigned seat.

$$\begin{aligned} \Pr[A_1 \cap A_2 \cap \cdots \cap A_k] &= \Pr[A_1] \cdot \Pr[A_2 \mid A_1] \cdot \Pr[A_3 \mid A_1 \cap A_2] \cdots \Pr[A_k \mid A_1 \cap A_2 \cap \cdots \cap A_{k-1}] \\ &= \frac{1}{n} \cdot \frac{1}{n-1} \cdots \frac{1}{n-k+1} \\ &= \frac{(n-k)!}{n!} \end{aligned}$$

Solution for PS12-7. We'll denote the outcomes using two-letter strings: the first letter will be one of B (for Brown), D (for Dartmouth), or L (for Little Hoop); the second letter will be one of H (for happy) or U (for unhappy). Draw a tree diagram showing these outcomes: the root will have three children and each of those children will have two leaf children.

- *Sample space:* $S = \{BH, BU, DH, DU, LH, LU\}$.
- *Events of interest:*

$$\begin{aligned}\text{Happy} &= \{BH, DH, LH\}; \\ \text{Brown} &= \{BH, BU\}; \\ \text{Dartmouth} &= \{DH, DU\}.\end{aligned}$$

- *Outcome probabilities:* Label the tree diagram using the given numbers, then compute:

$$\begin{aligned}\Pr[BH] &= \frac{4}{12} \cdot \frac{4}{12} = \frac{16}{144}; & \Pr[BU] &= \frac{4}{12} \cdot \frac{8}{12} = \frac{32}{144}; \\ \Pr[DH] &= \frac{5}{12} \cdot \frac{7}{12} = \frac{35}{144}; & \Pr[DU] &= \frac{5}{12} \cdot \frac{5}{12} = \frac{25}{144}; \\ \Pr[LH] &= \frac{3}{12} \cdot \frac{11}{12} = \frac{33}{144}; & \Pr[LU] &= \frac{3}{12} \cdot \frac{1}{12} = \frac{3}{144}.\end{aligned}$$

- *Event Probabilities:* Computed below.
- $\Pr[\text{Happy}] = \Pr[BH, DH, LH] = 84/144 = 7/12$.
 - $\Pr[\text{Brown} \mid \text{Happy}] = \frac{\Pr[BH]}{\Pr[\text{Happy}]} = \frac{16/144}{7/12} = \frac{4}{21}$.
 - Observe that $\Pr[\text{Brown} \mid \text{Happy}] \neq \Pr[\text{Brown}]$.
 - Observe that $\Pr[\text{Happy} \mid \text{Dartmouth}] = \Pr[\text{Happy}]$.

Solution for PS12-8. Uniform probability space on $\{1, 2, 3, 4, 5, 6\}$; take $A = \{2, 4, 5, 6\}$, $B = \{2, 4, 5\}$, $C = \{1, 2, 3\}$.

Solution for PS12-10.

- Just as in the original Monty Hall game, $\Pr[GP] = 1/3$, because the prize is equally likely to be behind any particular door.
- If the contestant does not pick the prize door, then the prize is behind one of the two remaining doors, both equally likely. When Carol picks a random door from among these two, she reveals the prize with probability $1/2$. Therefore, $\Pr[OP \mid \overline{GP}] = 1/2$.
- We use the law of total probability:

$$\Pr[OP] = \Pr[OP \mid GP] \cdot \Pr[GP] + \Pr[OP \mid \overline{GP}] \cdot \Pr[\overline{GP}] = 0 \times \frac{1}{3} + \frac{1}{2} \times \frac{2}{3} = \frac{1}{3}.$$

- In each round of the game, the probability that Carol will open the prize door (causing it to continue for at least one more round) is precisely $\Pr[OP]$, which we just calculated to be $1/3$. Since the rounds are independent,

$$\begin{aligned}\Pr[\text{game continues at least to round } n+1] &= \prod_{i=1}^n \Pr[\text{Carol opens prize door in } i\text{th round}] \\ &= \prod_{i=1}^n \Pr[OP] = \frac{1}{3^n}.\end{aligned}$$

Thus, the probability that the game will continue forever is $\lim_{n \rightarrow \infty} 1/3^n = 0$.

- These probabilities are as follows.
 - When GP occurs, the contestant has chosen the prize door and the strategy of sticking with the choice is going to win. So $\Pr[W \mid GP] = 1$.

- ii) When $\overline{GP} \cap OP$ occurs, the game gets restarted, which means we're back to square one. The probability of winning is again $\Pr[W]$. Thus, $\Pr[W \mid \overline{GP} \cap OP] = \Pr[W] = w$.
- iii) When $\overline{GP} \cap \overline{OP}$ occurs, the initial guess was wrong, the game ends in the first round, and by sticking with his initial choice, the contestant is guaranteed to lose. So, $\Pr[W \mid \overline{GP} \cap \overline{OP}] = 0$.

f. Using the law of total probability, we have

$$\begin{aligned} w &= \Pr[W] \\ &= \Pr[GP] \cdot \Pr[W \mid GP] + \Pr[\overline{GP} \cap OP] \cdot \Pr[W \mid \overline{GP} \cap OP] + \Pr[\overline{GP} \cap \overline{OP}] \cdot \Pr[W \mid \overline{GP} \cap \overline{OP}] \\ &= \frac{1}{3} \cdot 1 + \Pr[OP \mid \overline{GP}] \cdot \Pr[\overline{GP}] \cdot w + \Pr[\overline{GP} \cap \overline{OP}] \cdot 0 \\ &= \frac{1}{3} + \frac{1}{2} \left(1 - \frac{1}{3}\right) w + 0 \\ &= \frac{1+w}{3}. \end{aligned}$$

Solving this equation gives us the answer: $w = 1/2$.

- g.** In the modified game, there are three possibilities for each outcome of the overall random experiment.
- i) The contestant would win by using a “stick” strategy.
 - ii) The contestant would win by using a “switch” strategy.
 - iii) The game simply continues forever.

Because of the third possibility, we can't *immediately* conclude that $\Pr[\text{win using “switch” strategy}] = 1 - \Pr[W]$. Instead, we conclude that this probability equals $1 - \Pr[W] - \Pr[\text{game continues forever}]$.

However, we have computed $\Pr[\text{game continues forever}] = 0$, so in fact the desired probability is still equal to $1 - \Pr[W]$, i.e., the conclusion is still sound.

Solution for PS13-1. In each case, the sample space is \mathbb{Z}_n and the probability function is $\Pr[j] = 1/n$ for all $j \in \mathbb{Z}_n$.

- $\text{Ex}[Y] = \sum_{j=0}^{n-1} Y(j) \Pr[j] = (1/n) \sum_{j=0}^{n-1} \gcd(j, n) = (1/7) \left(7 + \sum_{j=1}^6 1 \right) = 13/7$.
- In this case, $\gcd(j, 9)$ equals 9 for one value of j (namely, $j = 0$), equals 3 for two values of j (namely, $j = 3$ and $j = 6$), and equals 1 for the remaining six values of j . Therefore, $\text{Ex}[Y] = (1/9)(9 \times 1 + 3 \times 2 + 1 \times 6) = 21/9 = 7/3$.
- By similar reasoning, $\text{Ex}[Y] = (1/15)(15 \times 1 + 3 \times 4 + 5 \times 2 + 1 \times 8) = 45/15 = 3$.
- Please solve this yourself. The final answer is $3 - 2/p$.
- Please solve this yourself. The final answer is $(2 - 1/p)(2 - 1/q)$.

Solution for PS13-3. Let the random variable X denote the amount (in dollars) that you win. Then $\text{range}(X) = \{0, 10^7\}$ and $\Pr[X = 10^7] = 1/\binom{50}{6}$. Therefore,

$$\text{Ex}[X] = 0 \cdot \Pr[X = 0] + 10^7 \cdot \Pr[X = 10^7] = \frac{10^7}{\binom{50}{6}} \approx 0.63.$$

Since this is below the ticket's price of \$1, the ticket is not worth its price.

Solution (Sketch) for PS13-4.

- Let X_j be the indicator r.v. for the event " $W_j = 6$." Then $\text{Ex}[X_j] = \Pr[X_j = 1] = \Pr[W_j = 6] = 1/6$.
The number of sixes seen is $Y := \sum_{j=1}^{24} X_j$, so by linearity of expectation,

$$\text{Ex}[Y] = \text{Ex}\left[\sum_{j=1}^{24} X_j\right] = \sum_{j=1}^{24} \text{Ex}[X_j] = 4.$$

- This doesn't affect our answer. Linearity of expectation always holds and has nothing to do with correlation (or independence).

Solution for PS13-6.

- Let's use the sample space $\{1, 2, 3, 4, 5, 6\}$ for the experiment of rolling the red die. Upon conditioning on the event " X is a perfect square," the probability function is as follows:

$$\Pr[1] = \frac{1}{2}, \quad \Pr[4] = \frac{1}{2}, \quad \Pr[2] = \Pr[3] = \Pr[5] = \Pr[6] = 0.$$

Therefore, $\text{Ex}[X^2 \mid X \text{ is a perfect square}] = 1^2 \times \frac{1}{2} + 4^2 \times \frac{1}{2} = 17/2$.

- We compute

$$\begin{aligned} \text{Ex}[WX] &= \text{Ex}[X^2 + XY] = \text{Ex}[X^2] + \text{Ex}[X] \text{Ex}[Y], \\ \text{Ex}[W] \text{Ex}[X] &= \text{Ex}[X + Y] \text{Ex}[X] = \text{Ex}[X]^2 + \text{Ex}[X] \text{Ex}[Y]. \end{aligned}$$

The two are unequal because $\text{Ex}[X^2] \neq \text{Ex}[X]^2$, by direct computation.

Solution (Sketch) for PS13-7. Number the pairs of students as pair 1, pair 2, ..., pair $\binom{n}{2}$ in some manner.

Let Y be the number of bonds. Let X_i be the indicator r.v. for the event "pair i forms a bond."

Then $\text{Ex}[X_i] = \Pr[X_i = 1] = 1/d$, so

$$\text{Ex}[Y] = \text{Ex}\left[\sum_{i=1}^{\binom{n}{2}} X_i\right] = \sum_{i=1}^{\binom{n}{2}} \text{Ex}[X_i] = \frac{1}{d} \binom{n}{2}.$$

Solution (Sketch) for PS13-9. Let Y be the number of bins that remain empty. Let X_i be the indicator r.v. for the event “bin i remains empty.”

Then $\text{Ex}[X_i] = \Pr[X_i = 1] = (1 - 1/n)^n$, so $\text{Ex}[Y] = \text{Ex}\left[\sum_{i=1}^n X_i\right] = \sum_{i=1}^n \text{Ex}[X_i] = n(1 - 1/n)^n$.

If you’ve taken calculus, you know that $\lim_{n \rightarrow \infty} (1 - 1/n)^n = 1/e$, so $\text{Ex}[Y] \approx n/e$ for large n .

Solution (Sketch) for PS13-11. Please do this computation. The final answer is $\frac{n^2 - 1}{3n}$.

Solution (Sketch) for PS13-12. The square of the previous expression, with $n = 1000$.

1. **(Roster and Set-Builder Notations)** Here are some sets described in set-builder notation. Describe each of them in roster notation. Note: \mathbb{Z} denotes the set of all integers.
 - 1.1. $\{k \in \mathbb{Z} : 10 \leq k \leq 99 \text{ and the sum of the digits of } k \text{ is } 9\}$
 - 1.2. $\left\{x \in \mathbb{Z} : 0 \leq x \leq 10 \text{ and } \frac{x}{2} \notin \mathbb{Z}\right\}$
 - 1.3. $\{S : S \subseteq \{a, b, c\}\}$
 - 1.4. $\{S : S \subseteq \{a, b, c, d\} \text{ and } |S| \text{ is even}\}$
2. **(Basic Operations on Sets)** Let $A = \{1, 2, 3, 4, 5, 6\}$, $B = \{2, 4, 6, 8, 10\}$ and $C = \{0, 1, 5, 6, 9\}$. In the following subproblems, you must show your steps for those cases where the statement asks you to “verify” an equation. For the rest, you do not need to show any steps.
 - 2.1. What is $A \cup B$? What is $(A \cup B) \cup C$?
 - 2.2. What is $B \cup C$? What is $A \cup (B \cup C)$?
 - 2.3. What is $A \cap B \cap C$?
 - 2.4. Verify by direct computation that $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.
 - 2.5. What is $A - B$? What is $B - C$?
 - 2.6. What is $(A - B) - C$? What is $A - (B - C)$?
 - 2.7. Verify by direct computation that $(A - B) - C = A - (B \cup C)$.
 - 2.8. Verify by direct computation that $A - (B - C) = (A - B) \cup (A \cap B \cap C)$.
3. **(Further Set Operations and Thinking)** For each of the following equations involving arbitrary sets A , B , C , and D , state whether or not it always holds. Further ...
 - If you say *no*, justify your answer by giving a specific counterexample.
 - If you say *yes*, justify your answer by writing out your reasoning in English sentences peppered with some math. Explain this reasoning to your group’s Discrete Math Ninja. (This kind of justification is called a *mathematical proof*. This entire course is about learning to write *good* mathematical proofs.)
 - 3.1. $(A \cup B) \times (C \cup D) = (A \times C) \cup (B \times D)$.
 - 3.2. $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
 - 3.3. $(A - C) \cap (C - B) = \emptyset$.

1. **(Proving Set Equality)** Let A , B , and C be arbitrary sets. Prove each of the following statements.

I want each group to write down at least one of these proofs in full English sentences. Ninjas, please ensure that your group does this (and give them plenty of help if needed).

1.1. $A \times (B - C) = A \times B - A \times C$.

◁ Operator precedence: “ \times ” has higher precedence than “ $-$ ”.

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

◁ We need parentheses because “ \cup ” and “ \cap ” have equal precedence.

2. **(Symmetric and transitive relations)** A relation R with the property that

$$\text{whenever } (a, b) \in R, \text{ we also have } (b, a) \in R$$

is called a *symmetric relation*. A relation S with the property that

$$\text{whenever } (a, b) \in R \text{ and } (b, c) \in R, \text{ we also have } (a, c) \in R$$

is called a *transitive relation*. For each of the following relations, state whether or not it is (a) symmetric; (b) transitive. Whenever your answer is “no”, explain why. This means that if, for instance, you say that a relation R is not symmetric, you must exhibit a pair (a, b) such that $(a, b) \in R$ but $(b, a) \notin R$.

2.1. The relation “divides”, on \mathbb{N} (“ m divides n ” means “ n/m is an integer”).

2.2. The relation “is disjoint from”, on $\mathcal{P}(\mathbb{Z})$.

2.3. The relation “is no larger than”, on $\mathcal{P}(\mathbb{Z})$. We say that A is no larger than B when one of the following holds:

- A and B are both finite sets, and $|A| \leq |B|$.
- A is a finite set and B is an infinite set.
- A and B are both infinite sets.

3. **(Understanding functions)** Let $S = \{\text{“RED”}, \text{“BLUE”}, \text{“GREEN”}, \text{“YELLOW”}, \text{“ORANGE”}, \text{“BLACK”}\}$ and $T = \{1, 2, 3, 4, 5, 6\}$. Consider the function $\text{len}: S \rightarrow T$ given by $\text{len}(s) = \text{the length of the string } s$ (as in the Python programming language).

3.1. Describe the “len” function pictorially, using arrows, as done in class.

3.2. Reverse the directions of all the arrows in your picture. Does this new picture represent another function $g: T \rightarrow S$? If not, why not?

1. Let $f : B \rightarrow C$ and $g : A \rightarrow B$ be two bijections, where A , B , and C are arbitrary nonempty sets.

1.1. Prove that $f \circ g$ is a bijection.

1.2. Recall that every bijection has an inverse function. Prove that $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

2. Define the function $f : \mathbb{N} \rightarrow \mathbb{Z}$ by

$$f(m) = \begin{cases} (m+1)/2, & \text{if } m \text{ is odd,} \\ -m/2, & \text{if } m \text{ is even.} \end{cases}$$

First, convince yourself that the infinite lists $(f(0), f(1), f(2), \dots)$ and $(0, 1, -1, 2, -2, 3, -3, \dots)$ are identical.

Now, prove that f is a bijection. Instead of using the definition of bijection, give an algebraic formula for a function $g : \mathbb{Z} \rightarrow \mathbb{N}$ such that $f \circ g = \text{id}_{\mathbb{Z}}$ and $g \circ f = \text{id}_{\mathbb{N}}$. Why does this prove that f is a bijection?

3. Prove that $\mathbb{N} \times \mathbb{N}$ is countable.

Method 1: You can directly use the definition of a countably infinite set, i.e., give a bijection $h : \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$

Method 2: Alternatively, you can construct an injection $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ and invoke the following result.
“If there exists an injection $f : A \rightarrow \mathbb{N}$, then A is countable.”

1. Consider the function $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ given by $f(a, b) = 2^a 3^b$. Prove that f is injective using just simple algebra and observations about odd and even numbers, without using the powerful Unique Factorization Theorem (UFT). You'll need the following facts:

- The product of an even integer and an arbitrary integer is even.
- The product of two odd integers is odd.

Suppose that we have arbitrary $a, b, c, d \in \mathbb{N}$ such that

$$2^a 3^b = 2^c 3^d. \quad (1)$$

- 1.1. Consider the case when $b = d$. Prove that $(a, c) = (b, d)$.
- 1.2. Now consider the case when $b \neq d$. Say $b < d$. Rewrite Eq. (1) in the form $2^p = 3^q$ with $q \in \mathbb{N}$.
- 1.3. Based on the facts noted above, conclude that 3^q is odd.
- 1.4. Based on the facts noted above and the previous part, conclude that $p = 0$.
- 1.5. Based on all of the above, conclude that $(a, c) = (b, d)$.
- 1.6. Wrap up the proof that f is injective.

2. Problem Set 3 asks you to prove the following fact:

- If A and B are countable sets, then $A \times B$ is countable.

Using the above fact, prove that $\mathbb{N} \times \mathbb{N} \times \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ is countable.

3. Given a character set S (sometimes called an *alphabet*), we can consider *strings* formed from the characters in S . Formally:

- An *alphabet* is a nonempty finite set.
- Having chosen an alphabet S , each of its elements is called a character.
- A string is a finite-length sequence of zero or more characters.
- The set of all such strings (over the alphabet S) is denoted S^* .

- 3.1. Prove that S^* is countable.

Hint: Come up with a systematic scheme for listing all the strings in S^* .

- 3.2. Argue that the set of all conceivable Python programs is countable.

1. Let $d \in \mathbb{N}^+$ and $a, b, x, y \in \mathbb{Z}$ be such that

$$a \equiv b \pmod{d},$$

$$x \equiv y \pmod{d}.$$

Using the definition of congruence, prove that

$$a + x \equiv b + y \pmod{d},$$

$$ax \equiv by \pmod{d}.$$

2. Compute $2^{2019} \bmod 17$. Do not use a calculator. In fact, think of a way to compute this entirely in your head.

3. Prove that a perfect square cannot end in the digit 7 when written out in decimal representation.

Hint: For what value of d would arithmetic modulo d help you reason about the last digit of an integer?

4. Prove that the product of any three consecutive integers must be divisible by 6.

Write a careful proof using only the facts established in the course up to this point. Don't jump to conclusions.

Have a copy of the lecture notes on modular arithmetic available as you work on these problems.

1. Using Euclid's GCD algorithm, compute the gcd of 276 and 437, showing your work at each step.

2. An “integer linear combination (IntLC) of a and b ” is defined to be an expression of the form $ka + \ell b$, where k and ℓ are integers. For each of the following statements, indicate “true” or “false.” If true, provide a concise proof. If false, provide a specific counterexample.

For all $a, b, c, n \in \mathbb{N}^+$,

2.1. $\gcd(a, b) \neq 1 \wedge \gcd(b, c) \neq 1 \implies \gcd(a, c) \neq 1$.

2.2. $\gcd(ab, ac) = a \cdot \gcd(b, c)$.

2.3. $\gcd(1 + a, 1 + b) = 1 + \gcd(a, b)$.

2.4. if an IntLC of a and b equals 1, then so does some IntLC of a and b^2 .

3. Using the Inverse Existence Theorem (see the lecture notes), prove the following. If p is a prime, $b \in \mathbb{Z}_p$, and $b \neq 0$, then

3.1. b has an inverse modulo p ;

3.2. the function $f_b: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ given by $f_b(x) = bx \bmod p$ is a bijection.

1. Consider arithmetic modulo 30, in the domain \mathbb{Z}_{30} . For each of the following numbers, find

- 1.1. its inverse modulo 30;
- 1.2. the smallest positive power of the number that is congruent to 1 modulo 30.

1, 10, 13, 19, 27, 29.

Some of your answers might be “does not exist.” You may use a calculator and/or the Python ‘egcd’ function from class.

Recall some notation from the lecture notes:

$$\mathbb{Z}_m^* := \{a \in \mathbb{Z} : 0 \leq a < m \text{ and } \gcd(a, m) = 1\}; \quad \phi(m) = |\mathbb{Z}_m^*|.$$

Let’s introduce an important piece of mathematical vocabulary. Consider a set S and an operation “op” on elements on S . We say that S is closed under “op” if the result of applying “op” to elements of S always produces an element of S . The concept is best understood through concrete examples.

- The set \mathbb{N} is closed under the *addition* operation, because if $x, y \in \mathbb{N}$, then $x + y \in \mathbb{N}$.
- Similarly, \mathbb{N} is closed under *multiplication*.
- However, \mathbb{N} is not closed under *subtraction*, because there do exist $x, y \in \mathbb{N}$ such that $x - y \notin \mathbb{N}$.
- On the other hand, the larger set \mathbb{Z} is indeed closed under subtraction.

2. Prove that \mathbb{Z}_m^* is closed under multiplication modulo m , for all $m \in \mathbb{N}^+$.

3. Let p and q be two distinct primes. Prove that $\phi(pq) = (p-1)(q-1)$.

4. Suppose that p and q are distinct primes and $n \in \mathbb{Z}$ is such that $p \mid n$ and $q \mid n$. Prove that $pq \mid n$.

Hint: Use the GCD Linear Combination Theorem and write $n = n(kp + \ell q)$.

1. Dr. Speedy proposes a cryptosystem that would work faster than RSA by working modulo a large *prime*.
 - Bob chooses a public key of the form (P, e) , where P is a very large (say 300-digit) prime.
 - When Alice wants to send a message $M \in \mathbb{Z}_P$ to Bob, she will send $C := M^e \pmod{P}$.
 - Bob has a secret key d such that $ed \equiv 1 \pmod{P-1}$; using it, he decrypts $M' := C^d \pmod{P}$.
 - 1.1. Show that Dr. Speedy's cryptosystem is sane, in the sense that $M' = M$ always.
 - 1.2. Why aren't we all using Dr. Speedy's cryptosystem instead of RSA, which is more complicated?

2. The security of RSA would be compromised if you could find an algorithm \mathcal{A} to quickly compute $\phi(N)$, given N . We believe that factoring is hard, but why should computing ϕ be hard?
Prove that if computing ϕ were easy—i.e., algorithm \mathcal{A} exists—then \mathcal{A} can be used to quickly factor the RSA modulus N . You'll need to use the fact that N is the product of *exactly two* primes.

3. In class (see the slides), we used a clever method to compute $a^{42} \bmod n$, based on the decomposition $42 = 32 + 8 + 2$.
 - 3.1. Find a connection between the above decomposition and the binary representation of 42.
 - 3.2. Explain how you would compute $a^{83} \bmod n$ along similar lines.

These exercises are about basic counting. Some of them will continue the development of ideas and methods we touched upon in the lecture. Do good work on them, understand them well, and seek help from your Ninja as needed.

Here are some important counting principles for *finite* sets.

- *Sum Principle*. If A and B are disjoint (i.e., $A \cap B = \emptyset$), then $|A \cup B| = |A| + |B|$.
- *Extended Sum Principle*. If A_1, \dots, A_k are pairwise disjoint, then $|A_1 \cup \dots \cup A_k| = |A_1| + \dots + |A_k|$.
- *Generalized Sum Principle*. For all sets A and B , $|A \cup B| = |A| + |B| - |A \cap B|$.
- *Product Principle*. For all sets A and B , $|A \times B| = |A| \cdot |B|$.
- *Extended Product Principle*. For all sets A_1, A_2, \dots, A_k , $|A_1 \times A_2 \times \dots \times A_k| = |A_1| \cdot |A_2| \cdot \dots \cdot |A_k|$.
- *Generalized Product Principle*. If we have to make a sequence of k choices and
 - there are n_1 ways to make the first choice,
 - for each first choice, there are n_2 ways to make the second choice,
 - for each of the first two choices, there are n_3 ways to make the third choice,
 - ...
 - for each of the first $k - 1$ choices, there are n_k ways to make the k th choice,then the overall number of ways to make the entire sequence of choices is $n_1 n_2 \dots n_k$.
- *Bijection Principle*. If there exists a bijection $f : A \rightarrow B$, then $|A| = |B|$.
- *Division Principle*. If there exists an r -to-1 correspondence $f : A \rightarrow B$, then $|B| = |A|/r$.

-
1. Solve each of the following counting problems. In each case, name the counting principle(s) you used.
 - 1.1. An office building contains 27 floors and has 37 offices on each floor. How many offices are in the building?
 - 1.2. Alice picks a card out of a standard 52-card deck. Then Bob picks a card from the ones that remain. Overall, how many different outcomes can there be?
 - 1.3. How many of the integers between 1 and 1000 (inclusive) are multiples of either 3 or 5?
 2. Solve each of the following counting problems. In each case, name the counting principle(s) you used. You may need to further extend one of the given counting principles. Get help from your Ninja as needed.
 - 2.1. Each user on a certain computer system has a password, which is six to eight characters long, where each character is a letter (either uppercase or lowercase) or a digit. Each password must contain at least one digit. How many possible passwords are there?
 - 2.2. The password rules in the above system have been modified. Now each password must contain at least one uppercase letter, at least one lowercase letter, and at least one digit. How many possible passwords are there now?

3. This part is warm-up. A *permutation* of a sequence is another sequence obtained by rearranging its terms. For instance, the three-term sequence (apple, pear, mango) has six permutations, shown below.

(apple, mango, pear)	(apple, pear, mango)	(mango, apple, pear)
(mango, pear, apple)	(pear, apple, mango)	(pear, mango, apple)

Notice that a sequence is considered to be a permutation of itself.

- 3.1. How many permutations does the four-term sequence (1, 3, 8, 9) have?
3.2. Generalize! How many permutations does an n -term sequence have, assuming the terms are all distinct?

Now for the real problem. Suppose $|S| = n$. We're going to work out the number of k -element subsets of S . Define

$$\mathcal{T} = \{(a_1, a_2, \dots, a_k) \in S^k : a_i \neq a_j \text{ whenever } i \neq j\};$$
$$\mathcal{U} = \{A \subseteq S : |A| = k\}.$$

Study these definitions carefully!

- 3.3. To solidify your understanding, redefine \mathcal{T} in words like this: " \mathcal{T} is the set of all k -tuples such that..."
3.4. Determine $|\mathcal{T}|$ using the extended product principle.
3.5. Define the function MAKESET: $\mathcal{T} \rightarrow \mathcal{U}$ by

$$\text{MAKESET}(a_1, a_2, \dots, a_k) = \{a_1, a_2, \dots, a_k\}.$$

For what value of r is MAKESET an r -to-1 correspondence?

- 3.6. Apply the division principle to determine $|\mathcal{U}|$.

4. Suppose that 13 people on a softball team show up for a game.
- 4.1. How many ways are there to choose 10 players to take the field?
4.2. How many ways are there to assign the 10 positions by selecting from the players who showed up?
4.3. Of the 13 who showed up, 11 are students and the other 2 are professors. How many ways are there to choose 10 players to take the field if at least one of these players must be a professor?

For today's exercises, please write out a detailed proof for the first problem, following the proof-by-induction template I've shown you. For the next two problems, if you don't have enough time, skip the template and just show your pod's Ninja the "meat" of your proof.

1. Using mathematical induction, prove that $\forall n \in \mathbb{N}: \sum_{i=1}^n (2i - 1) = n^2$.

2. Using mathematical induction, prove that the following identity holds for all $n \in \mathbb{N}$ and all $x \in \mathbb{R} - \{1\}$:

$$1 + x + x^2 + \cdots + x^n = \frac{x^{n+1} - 1}{x - 1},$$

Careful: the identity has two variables; your first step should be to write an appropriate one-variable predicate.

3. Using mathematical induction, prove that every positive integer n can be written as a sum of one or more *distinct* powers of 2. For example, $42 = 2^5 + 2^3 + 2^1$ and $77 = 2^6 + 2^3 + 2^2 + 2^0$.

Hint: You might want to consider using strong induction.

4. [Optional problem, if you've finished the first three.]

Recall that the basic sum principle applies to *exactly two* disjoint sets whereas the extended sum principle applies to $n \geq 2$ pairwise disjoint sets.

Use mathematical induction to prove that the extended sum principle follows from the basic sum principle.

1. We'll now study the fourth (and most complicated) case of the four-fold formulas. For starters, let's consider special cases. You are in a candy store. There are six (6) kinds of candy on offer and the store has plenty of pieces of each kind in stock. You love all six kinds on offer. You just want to take home as much candy as your parent will allow!

1.1. You have been allowed to pick two (2) pieces of candy to take home. The two pieces may be of the same kind or of different kinds. In how many different ways can you make your picks?

1.2. Suppose, instead, that you have been allowed to pick three (3) pieces. How does the answer change? The new answer is $\binom{6}{1} + 2\binom{6}{2} + \binom{6}{3}$. How did I get this?

2. It's your lucky day: you have been allowed to pick 15 pieces of candy from the above candy store! In how many ways can you make your choice now?

It's going to be tedious to generalize the expressions you wrote in the previous problem, so you try another idea. Visualize a row of 15 books laid out on a bookshelf, to represent the 15 pieces of candy you'll pick. Now you want to assign a kind of candy to each book: remember that there are 6 kinds of candy in the store. To do so, visualize 5 separators placed on the same bookshelf, dividing up the row of books into 6 sections. The number of books in the j th section will correspond to the number of pieces of the j th kind of candy you'll pick.

2.1. Draw a picture showing two different bookshelf layouts with the 15 books and 5 separators. For each of the layouts, write down the candy choices they indicate.

2.2. In how many ways can you lay out 15 books and 5 separators on a bookshelf? The books are to be treated as indistinguishable from one another and so are the separators.

2.3. Generalize! Suppose the candy store had n kinds of candy on offer and you are allowed to take home t pieces (repetitions allowed, as usual). How many books and how many separators should you use to represent your possible picks? Based on this, what is the number of ways to pick t pieces of candy from a store than offers n kinds of candy?

3. Give combinatorial proofs of the following identities.

3.1. For all $n \in \mathbb{N}^+$: $\sum_{k=0}^n (-1)^k \binom{n}{k} = 0$.

3.2. For all $k, n \in \mathbb{N}^+$ with $k \leq n$: $k \binom{n}{k} = n \binom{n-1}{k-1}$.

Hint: Consider choosing a k -person committee and then a chairperson of that committee.

1. Work out each of the following probabilities *systematically*, using the Four-Step Method. No need to get final numerical answers unless you have a calculator handy.
 - 1.1. First one digit is chosen uniformly at random from $\{1, 2, 3, 4, 5\}$ and is removed from the set; then a second digit is chosen uniformly at random from the remaining digits. What's the probability that an odd digit is picked the second time?
 - 1.2. You are dealt a poker hand of 5 cards drawn at random from a well-shuffled standard deck of 52 cards. The hand is called a *full house* if it has three cards of one rank and two of another rank (e.g., three kings and two 7s). What is the probability that your hand is a full house?
 - 1.3. A fair coin is flipped n times. What's the probability that all the heads occur at the end of the sequence? If no heads occur, then the statement "all the heads are at the end of the sequence" is vacuously true.

2. Work out each of the following probabilities. It's okay to shortcut, but if you get confused, do use the Four-Step Method. No need to get final numerical answers unless you have a calculator handy.
 - 2.1. A standard bag of Scrabble tiles has 100 tiles, exactly two (2) of which are *blank tiles*. Blanks are valuable assets in the game, since they can be turned into whatever letter you want.
You have just begun a game of Scrabble, drawing your first rack of seven (7) tiles from a full bag. What is the probability that your rack contains a blank?
 - 2.2. How does the answer to the above question change if your opponent is to make the first move, so your opponent picks seven random tiles first and *then* you get to pick seven from the 93 remaining tiles?

3. A card C is drawn uniformly at random from a standard 52-card deck. This is naturally modeled using the sample space $\mathcal{S} = \{\clubsuit 2, \diamondsuit 2, \heartsuit 2, \spadesuit 2, \clubsuit 3, \diamondsuit 3, \heartsuit 3, \spadesuit 3, \dots, \spadesuit A\}$ and the function Pr that sets $\text{Pr}[x] = 1/52$ for each $x \in \mathcal{S}$.
 - 3.1. Suppose you are *told* that C is a black card. Without changing the sample space \mathcal{S} , how should you modify the probability function to model this new reality?
 - 3.2. Suppose, instead, that you are told that C has a prime number on it (you are not told anything about the color). Again, sticking with the same sample space \mathcal{S} , what probability function should you use to model this new reality?
 - 3.3. Continue to assume that you are told that C has a prime number on it. Under this *condition*, based on your modified probability function, work out the probability of each of the following events.
 - i. The event that C is a red card.
 - ii. The event that C has the number 2 on it.
 - iii. The event that C has the number 6 on it.
 - iv. The event that C either has a 5 or a 6 on it.

1. Two fair dice are rolled in another room, out of your sight. If the sum of the two dice values is seven, you *win*. Your friend is in the other room and can observe the dice.
 - 1.1. Your friend calls out that one of the dice came up six. Given this information, what is the probability that you won?
 - 1.2. Suppose, instead, that your friend tells you that you won. In this case, what is the probability that one of the dice came up five?

2. Sally Smart just graduated from high school. She was accepted to three reputable colleges.

- With probability $4/12$, she attends Brown.
- With probability $5/12$, she attends Dartmouth.
- With probability $3/12$, she attends Little Hoop Community College.

Sally is either happy or unhappy in college.

- If she attends Brown, she is happy with probability $4/12$.
- If she attends Dartmouth, she is happy with probability $7/12$.
- If she attends Little Hoop, she is happy with probability $11/12$.

- 2.1. What is the probability that Sally is happy in college?
- 2.2. What is the probability that Sally attends Brown, given that she is happy in college?
- 2.3. Show that the events “Sally attends Brown” and “Sally is happy” **are not** independent.
- 2.4. Show that the events “Sally attends Dartmouth” and “Sally is happy” **are** independent.

3. The Chain Rule for probability says that if A_1, A_2, \dots, A_n are events in a probability space (\mathcal{S}, \Pr) , then

$$\begin{aligned}\Pr[A_1 \cap A_2 \cap \dots \cap A_n] &= \Pr[A_1] \cdot \Pr[A_2 \mid A_1] \cdot \Pr[A_3 \mid A_1 \cap A_2] \cdot \dots \cdot \Pr[A_n \mid A_1 \cap A_2 \cap \dots \cap A_{n-1}] \\ &= \Pr[A_1] \cdot \Pr[A_2 \mid A_1] \cdot \Pr[A_3 \mid A_1, A_2] \cdot \dots \cdot \Pr[A_n \mid A_1, A_2, \dots, A_{n-1}] \\ &= \prod_{j=1}^n \Pr[A_j \mid A_1, A_2, \dots, A_{j-1}].\end{aligned}$$

- 3.1. Prove this rule, i.e., prove the first equation. (The other two lines are just rewritings.)
Hint: Don't use induction. Start with the right-hand side.
- 3.2. Use this rule to answer the following question. Suppose n passengers board a flight that has n seats and they each take a seat at random, ignoring their assigned seating. The passengers board one by one. What is the probability that passengers 1 through k (inclusive) all end up in their assigned seats?

Bonus question: What do #2.3 and #2.4 teach you about independence of events?

1. Let $n \geq 2$ be an integer. We choose a random integer $X \in \mathbb{Z}_n$ uniformly. Let $Y = \gcd(X, n)$. Determine $\text{Ex}[Y]$ in each of the following cases.
 - 1.1. $n = 7$.
 - 1.2. $n = 9$.
 - 1.3. $n = p^2$, where p is a prime.

2. We roll two fair dice, a *red* die and a *blue* die, and they show numbers X and Y , respectively (these are therefore random variables). Let $W = X + Y$.
 - 2.1. Compute $\text{Ex}[X^2 \mid X \text{ is a perfect square}]$.
 - 2.2. Show that $\text{Ex}[WX] \neq \text{Ex}[W] \text{Ex}[X]$.

3. We roll 24 fair dice, and they show numbers X_1, \dots, X_{24} .
 - 3.1. How many sixes do we expect to see? In other words, compute $\text{Ex}[|\{j : X_j = 6\}|]$.
 - 3.2. Even though each die is fair, they have been connected together by very thin weightless threads and this causes X_1, \dots, X_{24} to be correlated in some unknown way. (For example, it may be that whenever X_1 is even, X_2 is more likely to be even than odd; or that whenever X_8 is a prime number, X_{20} is sure to be prime; or both of the above.) How does this affect your answer above?

4. The below problems have special significance in Computer Science. They model the process of inserting keys into a hash table.
 - 4.1. Two people that have the same birthday are said to form a *calendrical bond*. Assuming that the n students in a class have birthdays distributed uniformly among the d days in a year, and birthdays are mutually independent, what is the expected number of calendrical bonds among students in the class? Derive a formula in terms of n and d , then apply it to our CS30 class, using $n = 57$ and $d = 365$.

Hint: The random variable of interest here is a sum of $\binom{n}{2}$ indicator RVs.
 - 4.2. There are n bins, initially all empty. Then n balls are thrown randomly (uniformly) and independently into the bins: “uniformly” means that each ball is equally likely to go into each of the bins. What is the expected number of bins that remain empty after this process?

Hint: Again use a sum of appropriate indicator RVs.

Here are some problems about **sets, relations, and functions**. Use these as practice problems to strengthen your understanding as you do the reading corresponding to this unit. The topics you will want to read up on are listed at the end of the slides for this unit. Problems marked “HW” are to be submitted as your weekly written homework for HW1, which covers this unit.

Unmarked problems are for your own practice only and will not be graded.

As a reminder, here are our notations for some important sets.

- \mathbb{Z} = the set of all integers,
- \mathbb{N} = the set of all non-negative integers,
- \mathbb{N}^+ = the set of all positive integers,
- \mathbb{R} = the set of all real numbers.

PS1-1

Here are some sets described in set-builder notation. Describe each of them in roster notation.

- a. $\{x : x \text{ is a multiple of } 7 \text{ and } 0 < x < 50\}$.
- b. $\{x + y : x \in \mathbb{N}, y \in \mathbb{N}, \text{ and } xy = 12\}$.
- c. $\{S : S \subseteq \{1, 2, 3, 4\} \text{ and } |S| \text{ is odd}\}$.

PS1-2^{HW}

Here are some sets described in set-builder notation. Describe each of them in roster notation. You can write each answer on a single line and you do not need to show any steps.

- a. $\{x^3 : x \in \mathbb{Z} \text{ and } x^2 < 20\}$ [2 points]
- b. $\{x \in \mathbb{R} : x = x^2\}$. [2 points]
- c. $\{S : \{1, 2\} \subseteq S \subseteq \{1, 2, 3, 4\}\}$ [2 points]
- d. $\{S \subseteq \{1, 2, 3, 4\} : S \text{ is disjoint from } \{2, 3\}\}$ [2 points]

PS1-3

Let $A = \{1, 2, 3, 4, 5, 6\}$, $B = \{2, 4, 6, 8, 10\}$, and $C = \{0, 1, 5, 6, 9\}$. In the following subproblems, show your steps for those cases where the statement asks you to “verify” an equation. For the rest, you do not need to show any steps.

- a. What is $A \cup B$? What is $(A \cup B) \cup C$?
- b. What is $B \cup C$? What is $A \cup (B \cup C)$?
- c. What is $A \cap B \cap C$?
- d. Verify by direct computation that $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.
- e. What is $A - B$? What is $B - C$?
- f. What is $(A - B) - C$? What is $A - (B - C)$?
- g. Verify by direct computation that $(A - B) - C = A - (B \cup C)$.
- h. Verify by direct computation that $A - (B - C) = (A - B) \cup (A \cap B \cap C)$.
- i. What is $(A \cap B) \times (B - C)$?
- j. Verify by direct computation that $A \cup B \cup C = (A - B) \cup (B - C) \cup (C - A) \cup (A \cap B \cap C)$.

PS1-4

Let A , B , and C be arbitrary sets. Prove each of the following statements. Review the slides and be sure you understand how to prove that two sets are equal.

- a. $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
- b. $(A - C) \cap (C - B) = \emptyset$.
- c. $A \cup B \cup C = (A - B) \cup (B - C) \cup (C - A) \cup (A \cap B \cap C)$. ◁ It may help to draw a Venn diagram.

PS1-5^{HW}

Let A , B , and C be arbitrary sets, within some universal set. Prove each of the following statements as indicated.

- a. Using Venn diagrams to justify your steps, prove that $\overline{A \cup B} = \overline{A} \cap \overline{B}$. It's not enough to *just* draw diagrams: you must write down your steps of reasoning in full English sentences. [4 points]
- b. Similarly, prove that $(A - B) - C = (A - C) - (B - C)$. [4 points]
- c. Without diagrams, working algebraically, prove that $(A \cap B) \cup (A \cap \overline{B}) = A$. Don't *just* write some algebraic steps; your proof must use complete and grammatical English sentences. [4 points]

PS1-6^{HW}

Let $S = \{1, 3, 5, 7, 9\}$ and $T = \{0, 2, 4, 6, 8\}$. Let's say that an element $x \in S$ "completes" an element $y \in T$ if $x + y$ is divisible by 3. Describe the relation "completes" from S to T as a subset of $S \times T$ (i.e., write out all the pairs in this relation). Then describe the same relation pictorially, using arrows, as done in class. [4 points]

PS1-7

A relation R with the property that

$$\text{whenever } (a, b) \in R, \text{ we also have } (b, a) \in R$$

is called a *symmetric relation*. A relation S with the property that

$$\text{whenever } (a, b) \in R \text{ and } (b, c) \in R, \text{ we also have } (a, c) \in R$$

is called a *transitive relation*. For each of the following relations, state whether or not it is (a) symmetric; (b) transitive. Whenever your answer is "no", explain why. This means that if, for instance, you say that a relation R is not symmetric, you must exhibit a pair (a, b) such that $(a, b) \in R$ but $(b, a) \notin R$.

- a. The relation "divides", on \mathbb{N} ("m divides n" means " n/m is an integer").
- b. The relation "is disjoint from", on $\mathcal{P}(\mathbb{Z})$.
- c. The relation "is no larger than", on $\mathcal{P}(\mathbb{Z})$. We say that A is no larger than B when one of the following holds:
 - A and B are both finite sets, and $|A| \leq |B|$.
 - A is a finite set and B is an infinite set.
 - A and B are both infinite sets.

PS1-8^{HW}

Same instructions as the previous problem, **PS1-7**.

- a. The relation "is a subset of", on $\mathcal{P}(\mathbb{Z})$. [4 points]
- b. $\{(m, n) \in \mathbb{N} \times \mathbb{N} : \text{the sum of the digits of } m \text{ equals the sum of the digits of } n\}$. [4 points]
- c. The relation "overlapped" on the set of all US presidents. Two persons are said to "overlap" if there exists an instant in time when they were both alive. [4 points]

PS1-9 Let $S = \{\text{"RED"}, \text{"BLUE"}, \text{"GREEN"}, \text{"YELLOW"}, \text{"ORANGE"}, \text{"BLACK"}\}$ and $T = \{1, 2, 3, 4, 5, 6\}$. Consider the function $\text{len}: S \rightarrow T$ given by $\text{len}(s) = \text{the length of the string } s$ (as in the Python programming language).

- a. Describe the "len" function pictorially, using arrows, as done in class.
- b. Reverse the directions of all the arrows in your picture. Does this new picture represent a function $g: T \rightarrow S$. If not, why not?

PS1-10 Let $f : A \rightarrow B$ be a function. Then the basic notation $f(x)$ applies to elements $x \in A$, but let's now extend the notation to subsets $S \subseteq A$, by *defining* $f(S) = \{f(x) : x \in S\}$.

The set $f(S) \subseteq B$ is called the *image* of S under f . Prove the following fact about images.

$$\text{If } S_1, S_2 \subseteq A, \text{ then } f(S_1 \cup S_2) = f(S_1) \cup f(S_2).$$

Write out the steps of your reasoning. Notice that you are being asked to prove equality between two sets (you know what to do, right?).

PS1-11

Suppose that $g : A \rightarrow B$ and $f : B \rightarrow C$ are two functions. Then we define the *composition* $f \circ g$ to be the function from A to C given by

$$(f \circ g)(x) = f(g(x)), \text{ for all } x \in A.$$

The functions $f, g : \mathbb{R} \rightarrow \mathbb{R}$ are given by the formulas $f(x) = x^2 + 1$ and $g(x) = x + 2$. Find $f \circ g$ and $g \circ f$.

PS1-12^{HW}

The functions $f, \text{id} : \mathbb{R} \rightarrow \mathbb{R}$ are given by the formulas $f(x) = x^3 + 7$ and $\text{id}(x) = x$. You may recall that “id” is called the *identity function* on \mathbb{R} .

- a. Find a function $g : \mathbb{R} \rightarrow \mathbb{R}$ such that $f \circ g = \text{id}$. [2 points]
- b. For the function g you found above, find $g \circ f$. [2 points]

Here are some problems about **functions**. Use these as practice problems to strengthen your understanding as you do the reading corresponding to this unit. The topics you will want to read up on are listed at the end of the slides for this unit. Problems marked “HW” are to be submitted as part of your weekly written homework for HW2, which covers this unit and the next unit.

Problems marked “EC” are for extra credit. They are meant to provide a higher level for challenge for students who are *already comfortable* with the rest of the problem set. No one should feel pressured to submit solutions to these, as they won’t count towards your grade in the course. However, if *after finishing the official homework* you are able to write up a *nice* solution to an extra credit problem, please submit it for my reading pleasure and to fuel interesting conversations outside of class.

Unmarked problems are for your own practice only and will not be graded.

PS2-1 ^{HW}

Suppose $f : A \rightarrow B$ is a function. Define the *relation* f^{-1} from B to A as follows:

$$f^{-1} = \{(y, x) \in B \times A : f(x) = y\}.$$

Prove the following statements.

- a. If f is a bijection, then f^{-1} is a function. [4 points]
- b. If f^{-1} is a function, then f is a bijection. [4 points]

We can combine the above two statements into one like this: f^{-1} is a function iff f is a bijection.

Or in symbols: f^{-1} is a function $\iff f$ is a bijection

The word “iff” and the symbol “ \iff ” are pronounced “if and only if.”

PS2-2

Let $f : A \rightarrow B$ be a function. Given subsets $S \subseteq A$ and $T \subseteq B$, we can extend the f and f^{-1} notations by making the following *definitions*:

$$\begin{aligned} f(S) &= \{f(x) : x \in S\}, \\ f^{-1}(T) &= \{x \in A : f(x) \in T\}. \end{aligned}$$

The set $f(S) \subseteq B$ is called the *image* of S under f . The set $f^{-1}(T) \subseteq A$ is called the *preimage* of T under f .

Prove the following facts about images and preimages.

- a. If $S_1, S_2 \subseteq A$, then $f(S_1 \cup S_2) = f(S_1) \cup f(S_2)$.
- b. If $T_1, T_2 \subseteq B$, then $f^{-1}(T_1 \cup T_2) = f^{-1}(T_1) \cup f^{-1}(T_2)$.

PS2-3

Let $f : B \rightarrow C$ and $g : A \rightarrow B$ be two bijections, where A , B , and C are arbitrary nonempty sets.

- a. Prove that $f \circ g$ is a bijection.
- b. According to **PS2-1**, $f \circ g$ must have an inverse function. Prove that $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

PS2-4

Let S be a nonempty finite set. Consider the function $g : \mathcal{P}(S) \rightarrow \mathcal{P}(S)$ defined by $g(A) = S - A$ for all $A \subseteq S$. Give a careful proof that g is a bijection.

Use the definition of “bijection” and recall how you should prove that two sets are equal.

PS2-5^{HW}

Let us denote

$$\mathcal{P}^{\text{odd}}(S) = \{A \subseteq S : |A| \text{ is an odd number}\},$$
$$\mathcal{P}^{\text{even}}(S) = \mathcal{P}(S) - \mathcal{P}^{\text{odd}}(S).$$

Make sure you understand what these notations mean by taking the *particular* 3-element set $T = \{1, 2, 3\}$ and writing out $\mathcal{P}^{\text{odd}}(T)$ and $\mathcal{P}^{\text{even}}(T)$ in roster notation. No need to turn this part in.

Now, let S be an *arbitrary* nonempty finite set. Construct a bijection $h: \mathcal{P}^{\text{odd}}(S) \rightarrow \mathcal{P}^{\text{even}}(S)$ and prove that your constructed function h is indeed a bijection. [7 points]

The above problem requires more thought than usual. It requires you to come up with a clever idea.

PS2-6

Let A and B be arbitrary finite sets. Explain to a friend why each of the following statements is true. Listen to your own explanation and based on that, give written proofs for each statement.

- If there exists a surjection $f: A \rightarrow B$, then $|A| \geq |B|$.
- If there exists an injection $g: A \rightarrow B$, then $|A| \leq |B|$.
- If there exists a surjection $f: A \rightarrow B$ as well as an injection $g: A \rightarrow B$, then each of the functions f and g is, in fact, a bijection.

PS2-7

In class, we wrote down a bijection from \mathbb{N} to \mathbb{Z} by listing the integers in the following order:

$$0, 1, -1, 2, -2, 3, -3, \dots \quad (1)$$

Let's define the same bijection explicitly using algebraic formulas. First, define the function $f: \mathbb{N} \rightarrow \mathbb{Z}$ by

$$f(m) = \begin{cases} (m+1)/2, & \text{if } m \text{ is odd,} \\ -m/2, & \text{if } m \text{ is even.} \end{cases}$$

Do a few computations to convince yourself that the list $f(0), f(1), f(2), \dots$ is identical to the list in (1) above.

Now, prove that f is a bijection. Instead of using the definition of bijection, give an algebraic formula for a function $g: \mathbb{Z} \rightarrow \mathbb{N}$ such that $f \circ g = \text{id}_{\mathbb{Z}}$ and $g \circ f = \text{id}_{\mathbb{N}}$. Why does this prove that f is a bijection?

PS2-8

Let A be a set such that there exists an injection $f: A \rightarrow \mathbb{N}$. Prove that A is countable.

PS2-9

Prove that $\mathbb{N} \times \mathbb{N}$ is countable by constructing an injection $f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ and invoking the result of **PS2-8**.

PS2-10^{EC}

Let \mathbb{N}^* denote the set of all finite-length lists (i.e., sequences) of non-negative integers. For example, here are four elements of \mathbb{N}^* :

$$(5, 93, 12, 0, 51); \quad (42, 42, 42); \quad (65); \quad (1, 2, 3, \dots, 2019)$$

Give a detailed proof that \mathbb{N}^* is countable.

Here are some problems about **divisors and modular arithmetic**.

By now you are familiar with what needs to be submitted towards graded homework and when.

The symbols \mathbb{N} , \mathbb{N}^+ , \mathbb{Z} , \mathbb{Q} , and \mathbb{R} have their usual meanings. Additionally, for each $d \in \mathbb{N}^+$, we define $\mathbb{Z}_d = \{0, 1, 2, \dots, d-1\}$, the set of possible remainders when an integer is divided by d .

PS4-1

List all positive divisors of each of the following integers:

12, 15, 29, 64, 72, 73, 75.

Which of the above integers are primes?

PS4-2^{HW}

Count the number of positive divisors of each integer in the above list. You'll notice that the counts are all even numbers, with one exception. Work out exactly which integers from 1 to 100 (inclusive) have an odd number of positive divisors. Prove your answer.

Hint: I'm not expecting a super-long proof that lists out all 100 cases. I want you to discover a pattern and use that to cut down your work a lot.

PS4-3^{HW}

Write out a multiplication table for \mathbb{Z}_{11} using multiplication modulo 11 and another multiplication table for \mathbb{Z}_{12} using multiplication modulo 12. What do you observe about the occurrences of zeroes in these tables?

PS4-4

Let $d \in \mathbb{N}^+$ and $a, b, x, y \in \mathbb{Z}$ be such that

$$\begin{aligned}a &\equiv b \pmod{d}, \\x &\equiv y \pmod{d}.\end{aligned}$$

Using the definition of congruence, prove that

$$\begin{aligned}a + x &\equiv b + y \pmod{d}, \\ax &\equiv by \pmod{d}.\end{aligned}$$

PS4-5

Prove that $\forall a, b \in \mathbb{Z} \forall n \in \mathbb{N}^+$, if $a \neq b$, then $a^n - b^n$ is divisible by $a - b$.

Hint: Think of arithmetic modulo $a - b$, assuming $a > b$.

PS4-6^{HW}

Prove that $\forall a, b, n \in \mathbb{N}^+$, if n is odd, then $a^n + b^n$ is divisible by $a + b$.

Hint: First figure out the square, cube, fourth power, etc. of -1 .

PS4-7

Compute $2^{2019} \bmod 17$. Do not use a calculator. In fact, think of a way to compute this entirely in your head.

PS4-8

Prove that a perfect square cannot end in the digit 7 when written out in decimal representation.

Hint: For what value of d would arithmetic modulo d help you reason about the last digit of an integer?

PS4-9^{HW}

If you're given a somewhat large number such as 803411927792 and asked whether or not it's a multiple of 3, there's a nifty trick you can use. Simply add up all the digits and test whether the sum is divisible by 3. In the above example, $8 + 0 + 3 + 4 + 1 + 1 + 9 + 2 + 7 + 7 + 9 + 2 = 53$, which isn't divisible by 3, so we can answer "No."

Explain why this test works, by proving the following theorem. If the decimal representation of $n \in \mathbb{N}^+$ is $a_k a_{k-1} \cdots a_2 a_1 a_0$, where the a_i s are the digits, then

$$n \equiv a_k + \cdots + a_1 + a_0 \pmod{3}.$$

PS4-10

Prove that the product of any three consecutive integers must be divisible by 6.

Write a careful proof using only the facts established in the course up to this point. Don't jump to conclusions.

Here are some problems about **countability and uncountability**. Use these as practice problems to strengthen your understanding as you do the reading corresponding to this unit. Problems marked “HW” are to be submitted as part of your weekly written homework for HW2, which covers this unit and the previous one.

The symbols \mathbb{N} , \mathbb{Z} , \mathbb{Q} , and \mathbb{R} have their usual meanings.

PS3-1 ^{HW}

Prove the following basic facts about odd and even integers. Remember that integers can be negative or zero, and that zero is even.

- a. The sum of two even integers is even. [2 points]
- b. The sum of two odd integers is even. [2 points]
- c. The sum of an odd integer and an even integer is odd. [2 points]
- d. The product of an even integer and an arbitrary integer is even. [2 points]
- e. The product of two odd integers is odd. [3 points]

PS3-2

Consider the function $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ given by $f(a, b) = 2^a 3^b$. In class, we proved that f is injective by using the powerful *unique factorization theorem* (UFT), a.k.a., the *fundamental theorem of arithmetic*. Give a different proof that uses just simple algebra and observations about odd and even numbers, without using UFT.

Suppose that we have arbitrary $a, b, c, d \in \mathbb{N}$ such that

$$2^a 3^b = 2^c 3^d. \quad (1)$$

- a. Consider the case when $b = d$. Prove that $(a, b) = (c, d)$.
- b. Now consider the case when $b \neq d$. Say $b < d$. Rewrite Eq. (1) in the form $2^p = 3^q$ with $q \in \mathbb{N}$.
- c. Based on **PS3-1**, conclude that 3^q is odd.
- d. Based on **PS3-1** and the previous part, conclude that $p = 0$.
- e. Based on all of the above, conclude that $(a, b) = (c, d)$.
- f. Wrap up the proof that f is injective.

PS3-3

Prove that if A is a countable set and $B \subseteq A$, then B is countable.

PS3-4

Let A and B be two countable sets.

- a. Prove that $A \cup B$ is countable.
- b. Prove that $A \times B$ is countable.

PS3-5

Prove that $\mathbb{N} \times \mathbb{N} \times \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ is countable.

PS3-6 ^{HW}

Let A be an infinite set. Prove that there exists a surjection $f : A \rightarrow \mathbb{N}$. [7 points]

Warning: A proof that tries to “list all the elements of A ” is flawed, because A might not be countable.

PS3-7

Given a character set S (sometimes called an *alphabet*), we can consider *strings* formed from the characters in S . Formally:

- An *alphabet* is a nonempty finite set.
- Having chosen an alphabet S , each of its elements is called a character.
- A string is a finite-length sequence of zero or more characters.
- The set of all such strings (over the alphabet S) is denoted S^* .

Prove that S^* is countable.

Hint: Come up with a systematic scheme for listing all the strings in S^* .

PS3-8

Argue that the set of all conceivable Python programs is countable.

PS3-9

The open interval $(0, 1)$ can be visualized as a line segment within the number line and the Cartesian product $(0, 1) \times (0, 1)$ can be visualized as a unit square in the 2-D plane. You might expect that the latter set, being two-dimensional, has way more elements than the former, but you would be wrong!

Construct an injection $f : (0, 1) \times (0, 1) \rightarrow (0, 1)$.

PS3-10^{HW}

Construct a bijection $g : (0, 1] \rightarrow (0, 1)$.

[7 points]

The notation $(0, 1]$ denotes the half-open interval $\{x \in \mathbb{R} : 0 < x \leq 1\}$.

Hint: You can come up with a construction where $g(x) = x$ “most of the time” though obviously you can’t do this for $x = 1$. So make $g(1) = \frac{1}{2}$. But now what should you do with $g(\frac{1}{2})$?

PS3-11^{EC}

Is the injection you constructed in **PS3-9** in fact a bijection? If so, prove it. If not, explain clearly why not and then construct a bijection $h : (0, 1) \times (0, 1) \rightarrow (0, 1)$.

Here are some problems about **GCDs and inverses**. Before working on this problem set, you will need to have read the corresponding lecture notes posted on the course website. Some of these problems ask you to write out proofs for things mentioned without proof in the lecture notes. In such cases, you can't just cite the lecture notes to say that the result has been proved in class (since it hasn't).

By now you are familiar with what needs to be submitted towards graded homework and when.

The symbols \mathbb{N} , \mathbb{N}^+ , \mathbb{Z} , \mathbb{Z}_d , \mathbb{Q} , and \mathbb{R} have their usual meanings.

PS5-1^{HW}

The lecture notes contain an example gcd computation, using the numbers 1147 and 899.

- In a similar way, compute the gcd of 13631 and 8213, showing your work at each step.
- Let the gcd be g . Then, according to the GCD Linear Combination Theorem (LCT), there exists a pair of integers (k, ℓ) , such that $13631k + 8213\ell = g$. Find one such pair.
- Find another such pair.

PS5-2

An “integer linear combination (IntLC) of a and b ” is defined to be an expression of the form $ka + \ell b$, where k and ℓ are integers.

For each of the following statements, indicate “true” or “false.” If true, provide a concise proof. If false, provide a specific counterexample.

For all $a, b, c, n \in \mathbb{N}^+$,

- $\gcd(a, b) \neq 1 \wedge \gcd(b, c) \neq 1 \implies \gcd(a, c) \neq 1$.
- $\gcd(a^n, b^n) = \gcd(a, b)^n$.
- $\gcd(ab, ac) = a \cdot \gcd(b, c)$.
- $\gcd(1 + a, 1 + b) = 1 + \gcd(a, b)$.
- if an IntLC of a and b equals 1, then so does some IntLC of a and b^2 .
- if no IntLC of a and b equals 2, then neither does any IntLC of a^2 and b^2 .

PS5-3^{HW}

The Python code for the function “egcd” given in the lecture notes does not correctly handle *all* possible inputs $(a, b) \in \mathbb{Z} \times \mathbb{Z} - \{(0, 0)\}$.

- Find a pair of integers (a, b) for which the answer returned by $\text{egcd}(a, b)$ is incorrect, according to the definition of gcd given in class and the lecture notes.
- Fix the code for egcd to handle all cases correctly. You should add a small bit of logic to the existing code; don't write a completely new egcd function.

PS5-4

The proof of LCT given in the lecture notes has a subtle flaw: it assumes that the recursion will terminate. Thankfully, we can *prove* that it will indeed terminate.

Consider a function call $\text{egcd}(a, b)$. We'll say that it is a “good” call if $0 \neq a \geq b \geq 0$ and that the “size” of the call is $a + b$.

- Prove that if we make a good call to egcd whose size is s and this results in an immediate recursive call to egcd , then this new call is also good and it has size $< s$.
- Using the above result, prove that every good call to egcd eventually terminates (i.e., recursive calls don't keep happening forever).

You'll find that your proof depends on the following crucial property of \mathbb{N} : every nonempty subset of \mathbb{N} has a minimal element. This is called the *Well-Ordering Principle*.

PS5-5

Study the Fundamental Theorem of Arithmetic (a.k.a. Unique Factorization Theorem) and its proof, as presented in the [LLM] textbook. It's Lemma 9.4.3 in the June 2018 edition of the book (linked from the course website).

PS5-6^{HW}

For $a, b \in \mathbb{N}^+$, the *least common multiple* $\text{lcm}(a, b)$ is defined to be the minimum positive integer that is a multiple of both a and b , i.e.,

$$\text{lcm}(a, b) = \min\{m \in \mathbb{N}^+ : a \mid m \text{ and } b \mid m\}.$$

The result is well-defined because there is always at least one common multiple—namely, ab —and we're taking the minimum of a subset of \mathbb{N} (recall the Well-Ordering Principle).

- Prove that $\exists x, y \in \mathbb{N}^+$ such that $\text{lcm}(a, b) = ax = by$ and $\gcd(x, y) = 1$.
- Using LCT, express a/y as an integer linear combination of a and b .
- Using the above, show that $\gcd(a, b) \mid a/y$.
- On the other hand, show that a/y is a divisor of both a and b .
- Conclude that $\gcd(a, b) = a/y$.
- Based on all of the above, prove the following very pretty theorem:

$$\gcd(a, b) \cdot \text{lcm}(a, b) = ab.$$

PS5-7

Using the Inverse Existence Theorem (see the lecture notes), prove the following. If p is a prime, $b \in \mathbb{Z}_p$, and $b \neq 0$, then

- b has an inverse modulo p ;
- the function $f_b: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ given by $f_b(x) = bx \bmod p$ is a bijection.

PS5-8

Establish the fact that " n^2 is even $\Rightarrow n$ is even."

- Using the above fact, give a detailed proof that $\sqrt{2}$ is irrational. Do a proof by contradiction, starting with the assumption that $\sqrt{2} = u/v$, in lowest terms, for some $u, v \in \mathbb{N}^+$.
- A generalization of the above fact is that if p is a prime, then n^2 is divisible by p only if n is. Prove this generalization using Euclid's Lemma.
- Give a detailed proof that \sqrt{p} is irrational for every prime p .
- Generalize further to show that $p^{1/n}$ is irrational for every prime p and every integer $n \geq 2$.

PS5-9^{HW}

Let $m \in \mathbb{N}^+$ and $a \in \mathbb{Z}_m$. We say that a is a self-inverse modulo m if $a = a^{-1}$. Equivalently, $a^2 \equiv 1 \pmod{m}$.

- Prove that if $p \geq 3$ is a prime, there are exactly two self-inverses modulo p .
- Find all numbers in \mathbb{Z}_{15} that are self-inverses modulo 15.

Hint: Use Euclid's Lemma.

PS5-10^{EC}

Generalize your work in **PS5-8** to show that for all $a, n \in \mathbb{N}^+$, $a^{1/n}$ is either an integer or an irrational number.

Here are some problems about **modular exponentiation** and modular arithmetic in general, now that we've developed the subject quite a bit. Before working on this problem set, you will need to have read the corresponding lecture notes posted on the course website. Some of these problems ask you to write out proofs for things mentioned without proof in the lecture notes. In such cases, you can't just cite the lecture notes to say that the result has been proved in class (since it hasn't).

By now you are familiar with what needs to be submitted towards graded homework and when.

The symbols \mathbb{N} , \mathbb{N}^+ , \mathbb{Z} , \mathbb{Z}_m , \mathbb{Q} , and \mathbb{R} have their usual meanings. The lecture notes define \mathbb{Z}_m^* and $\phi(m)$.

PS6-1

Consider arithmetic modulo 30, in the domain \mathbb{Z}_{30} . For each of the following numbers, find

- its inverse modulo 30;
- the smallest positive power of the number that is congruent to 1 modulo 30.

Some of your answers might be "does not exist."

1, 10, 13, 19, 27, 29.

PS6-2^{HW}

Let $p, n, a \in \mathbb{Z}$ be such that p is a prime and $p \nmid a$. Prove that $a^n \equiv a^{n \bmod (p-1)} \pmod{p}$. [4 points]

Let's introduce an important piece of mathematical vocabulary. Consider a set S and an operation "op" on elements on S . We say that S is closed under "op" if the result of applying "op" to elements of S always produces an element of S . The concept is best understood through concrete examples.

- The set \mathbb{N} is closed under the *addition* operation, because if $x, y \in \mathbb{N}$, then $x + y \in \mathbb{N}$.
- Similarly, \mathbb{N} is closed under *multiplication*.
- However, \mathbb{N} is not closed under *subtraction*, because there do exist $x, y \in \mathbb{N}$ such that $x - y \notin \mathbb{N}$.
- On the other hand, the larger set \mathbb{Z} is indeed closed under subtraction.

PS6-3

Prove that \mathbb{Z}_m^* is closed under multiplication modulo m , for all $m \in \mathbb{N}^+$.

PS6-4

Let's generalize Fermat's Little Theorem using a proof along the lines of that given in the lecture notes. Take an arbitrary integer $m \geq 2$ and $a \in \mathbb{Z}_m^*$.

- Prove that $f_a(x) = ax \bmod m$ is a bijection from \mathbb{Z}_m^* to \mathbb{Z}_m^* . A fully rigorous proof will need to use **PS6-3**.
- Using the above result and the Inverse Existence Theorem, prove that $a^{\phi(m)} \equiv 1 \pmod{m}$.
- What does the previous congruence say when m is a prime?

PS6-5^{HW}

Let $m \in \mathbb{Z}$ with $m \geq 2$ and $a \in \mathbb{Z}_m^*$. Consider the infinite sequence $P_{m,a}$ of nonnegative powers of a modulo m :

$$P_{m,a} := (a^0 \bmod m, a^1 \bmod m, a^2 \bmod m, a^3 \bmod m, \dots).$$

For instance, $P_{7,3} = (1, 3, 2, 6, 4, 5, 1, 3, 2, 6, 4, 5, 1, 3, \dots)$. Notice that this sequence is *periodic*, i.e., it consists of a finite-length block repeated infinitely often. In this case, the block is $(1, 3, 2, 6, 4, 5)$. Since this block is six elements long and it's the shortest such block, we say the sequence has period 6.

Another example: $P_{11,5} = (1, 5, 3, 4, 9, 1, 5, 3, 4, 9, 1, 5, \dots)$. Again this is a periodic sequence. The shortest block whose repetition generates $P_{11,5}$ is $(1, 5, 3, 4, 9)$, so the period is 5.

- a. The sequence $P_{m,a}$ always starts with the number 1. Prove that 1 will reappear in the sequence.
- b. Prove that $P_{m,a}$ is always a periodic sequence.
Hint: Sometimes the period is 1.
- c. Prove that the period of $P_{m,a}$ is at most m .
- d. Is every integer in the interval $[1, m]$ equal to the period of some sequence $P_{m,a}$, or are some integers in $[1, m]$ forbidden from being periods? Why? [3+3+3+1 points]
Hint: Play around with some examples for a small value of m , such as $m = 6$.

PS6-6

Let p and q be two distinct primes. Prove that $\phi(pq) = (p-1)(q-1)$.

PS6-7^{HW}

Let p be a prime.

- a. Suppose $p \geq 5$. Prove that the numbers in the set $S := \{a \in \mathbb{N} : 2 \leq a \leq p-2\}$ can be partitioned into pairs¹ such that the two numbers in each pair are inverses of one another, modulo p .
Hint: You'll want to review your work in **PS5-9^{HW}** and use some of its results here.
- b. Using the above, work out the value of $(p-1)! \bmod p$.
- c. Hence, prove that for *all* primes p , we have $p \mid (p-1)! + 1$. This is called Wilson's Theorem. [4+2+1 points]

PS6-8

Prove that for all composite numbers m , we have $m \nmid (m-1)! + 1$.

Hint: Try dividing $(m-1)!$ by m for some small example cases.

PS6-9

Let $a, b, n \in \mathbb{N}^+$.

- a. Prove that if $a \mid n$ and $b \mid n$, then $\text{lcm}(a, b) \mid n$.
Review your work in **PS5-6^{HW}** and rewrite things in terms of $\text{gcd}(a, b)$, then make use of LCT.
- b. Using the above result repeatedly, prove that if p_1, p_2, \dots, p_k are distinct primes and each $p_i \mid n$, then the product $p_1 p_2 \cdots p_k \mid n$.

PS6-10^{HW}

Prove that $\forall n \in \mathbb{Z}: 2730 \mid n^{13} - n$.

[7 points]

Hint: Use the result of **PS6-9**. In your submission it's okay to use that result without writing up its proof.

¹This means that every element of S occurs in exactly one of the pairs.

Here are some problems about the **RSA cryptosystem** and related topics. Have the modular arithmetic lecture notes handy as you work on this set.

By now you are familiar with what needs to be submitted towards graded homework and when.

The symbols \mathbb{N} , \mathbb{N}^+ , \mathbb{Z} , \mathbb{Z}_m , \mathbb{Z}_m^* , \mathbb{Q} , \mathbb{R} , and $\phi(m)$ have their usual meanings.

PS7-1

Dr. Speedy proposes a cryptosystem that would work faster than RSA by working modulo a large *prime*.

- Bob chooses a public key of the form (P, e) , where P is a very large (say 300-digit) prime.
- When Alice wants to send a message $M \in \mathbb{Z}_P$ to Bob, she will send $C := M^e \pmod{P}$.
- Bob has a secret key d such that $ed \equiv 1 \pmod{P-1}$; using it, he decrypts $M' := C^d \pmod{P}$.

a. Show that Dr. Speedy's cryptosystem is sane, in the sense that $M' = M$ always.

b. Why aren't we all using Dr. Speedy's cryptosystem instead of RSA, which is more complicated?

PS7-2

The security of RSA would be compromised if you could find an algorithm \mathcal{A} to quickly compute $\phi(N)$, given N . We believe that factoring is hard, but why should computing ϕ be hard?

Prove that if computing ϕ were easy—i.e., algorithm \mathcal{A} exists—then \mathcal{A} can be used to quickly factor the RSA modulus N . You'll need to use the fact that N is the product of *exactly two* primes.

PS7-3^{HW}

Dr. Tricky proposes a cryptosystem that works just like RSA, except that the modulus N is chosen as the product of *ten* distinct primes, not two. "Using ten primes makes it five times as secure as RSA," they say.

What's wrong with Dr. Tricky's idea?

[5 points]

PS7-4^{HW}

As you have seen, the basic operation of RSA encryption and decryption is *modular exponentiation*. In this problem, you will develop a fast algorithm for carrying out this operation. Suppose that we want to compute $a^k \bmod n$, where $a \in \mathbb{Z}_n$, and n and k are very large integers (say 1024 bits each, which is about 308 digits).

Let's say you have a function `modmult(a, b, n)` that returns $ab \bmod n$ (code shown below). Your goal is to write a function `modpow(a, k, n)` that returns $a^k \bmod n$. Here's a bad way to do it.

```
def modmult(a, b, n):  
    """multiply a and b modulo n, assuming n > 0"""  
    return (a * b) % n  
  
def modpow_bad(a, k, n):  
    """compute a**k modulo n, assuming k >= 0, n > 0"""  
    result = 1  
    for i in range(k):  
        result = modmult(result, a, n)  
    return result
```

a. What's bad about the `modpow_bad` function above?

b. In class (see the posted slides), we used a clever method to compute $a^{42} \bmod n$, based on the decomposition $42 = 32 + 8 + 2$. Explain how you would compute $a^{83} \bmod n$ along similar lines. Don't write code. Instead, write something analogous to what you see on the posted slides for $a^{42} \bmod n$.

c. Give a very short proof that $\forall x \in \mathbb{R} \forall n \in \mathbb{N}$,

$$x^n = \begin{cases} (x^2)^{\lfloor n/2 \rfloor}, & \text{if } n \text{ is even,} \\ x \cdot (x^2)^{\lfloor n/2 \rfloor}, & \text{if } n \text{ is odd.} \end{cases}$$

- d. The above equation captures the general idea behind the tricks for quickly computing $a^{42} \bmod n$ and $a^{83} \bmod n$. Based on the equation, write a much more efficient Python function `modpow(a, k, n)`.
Warning: It should go without saying that the Honor Code forbids you from looking at modular exponentiation code online if you intend to submit this problem for credit.
- e. Use your code to evaluate $5921400673^{6626043712} \bmod 9999988887$. [1+1+2+4+1 points]

PS7-5

In one of the cases of our in-class proof of the Decryption Theorem for the RSA cryptosystem (see the posted slides), we argued that a certain congruence was true modulo p and also true modulo q and said that *therefore* it was true modulo pq . This is a baby step towards a beautiful theorem that you'll now prove.

Suppose that $m, n \in \mathbb{Z}$ are such that $m \geq 2$, $n \geq 2$, and $\gcd(m, n) = 1$.

- a. Generalize the argument to show that if $x \equiv y \pmod{m}$ and $x \equiv y \pmod{n}$, then $x \equiv y \pmod{mn}$.
- b. Prove that the function $f: \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ given by $f(x) = (x \bmod m, x \bmod n)$ is injective.
- c. Conclude that f is therefore surjective.
Give a precise reason! Naturally, you need something in addition to the just-derived fact that f is injective.
- d. Conclude that given any two values $a, b \in \mathbb{Z}$, the system of congruences

$$\begin{aligned}x &\equiv a \pmod{m} \\x &\equiv b \pmod{n}\end{aligned}$$

in the unknown x has one and only one solution modulo mn . This is called the Chinese Remainder Theorem. Read the Rosen textbook for the story behind this name; it dates back to ancient China.

PS7-6^{HW}

Suppose that $m, n \in \mathbb{Z}$ are such that $m \geq 2$, $n \geq 2$, and $\gcd(m, n) = 1$.

- a. Prove that the function f defined in PS7-5 is also a bijection from \mathbb{Z}_{mn}^* to $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$.
You may use the results of PS7-5 without proof, provided you swear that you have solved PS7-5 first!
- b. Conclude that $\phi(mn) = \phi(m)\phi(n)$. [7+1 points]

PS7-7

Consider arithmetic modulo m , where $m \geq 3$. We say that $a \in \mathbb{Z}_m$ is a *square root of unity* modulo m if $a^2 \equiv 1 \pmod{m}$. For any $m \geq 3$, there are always two such square roots, namely, 1 and $m-1$: these are called “trivial” square roots. If $a \not\equiv \pm 1 \pmod{m}$, we say that a is a *nontrivial* square root of unity.

- a. Prove that if there exists a nontrivial square root of unity modulo m , then m is composite.
Hint: Take a look at PS5-9^{HW}.
- b. Now suppose that b is a nontrivial square root of unity modulo m . The existence of b implies that m is composite, but this by itself doesn't tell us how to *find* a nontrivial divisor of m . (A nontrivial divisor is a positive divisor besides 1 and m .) That's where the following result comes in.
Prove that either $\gcd(m, b-1)$ or $\gcd(m, b+1)$ is a nontrivial divisor of m .

PS7-8^{EC}

The security of RSA would be compromised if you could find an algorithm \mathcal{B} to quickly compute the (secret) decryption key d , given the (public) encryption key (N, e) . Again, we believe that factoring is hard, but why should this computation be hard? In this problem, you'll prove if algorithm \mathcal{B} exists, then \mathcal{B} can be used to quickly factor N . Unfortunately, the proof will rest on an advanced theorem that is beyond the scope of this course (talk to me if you want to learn more).

Suppose that $m \in \mathbb{N}^+$ is divisible by at least two different odd primes.

- a. Prove that there exists a nontrivial square root of unity modulo m .

Hint: Use the Chinese Remainder Theorem.

- b. Suppose $t \in \mathbb{N}^+$ is divisible by $\phi(m)$ and $t = 2^r s$, where $r \in \mathbb{N}$ and s is odd. For each $a \in \mathbb{Z}_m$, consider the sequence

$$b_0 = a^s \bmod m, b_1 = a^{2s} \bmod m, b_2 = a^{2^2 s} \bmod m, \dots, b_r = a^{2^r s} \bmod m.$$

We'll say that a is *useful* if at least one of the following conditions holds:

- $b_r \neq 1$;
- $b_0 \neq 1$ and $\forall j \in \{0, 1, \dots, r\} : b_j \neq m - 1$.

Prove that if a is useful, then from the sequence of b_i values one can find a nontrivial divisor of m .

Hint: This has something to do with nontrivial square roots of unity.

- c. Here is the advanced theorem you need now: "At least half of the elements of \mathbb{Z}_m are useful."

Based on this theorem and your results above, show that if m is an RSA modulus (i.e., a product of two distinct odd primes), then algorithm \mathcal{B} can be used to factor m quickly.

Here are some problems on **basic counting principles**. Do read the posted slides and relevant sections from the [LLM] book before you begin.

Reminder: You are expected to solve all the problems on every problem set, even though you only have to turn in a few for credit. This is especially important in the run up to the first midterm. A student who is thoroughly practiced will do well in the exam. The course staff is allowed to discuss the non-HW problems very thoroughly in the office hours, up to explaining solutions in full.

In all cases, you must demonstrate *how* you arrived at your final answers—i.e., you must show your steps—unless the problem statement makes an exception. Without such explanation, even a correct answer is worth nothing. You must also justify any steps that are not trivial. Please think carefully about how you are going to organize your answers *before* you begin writing.

PS8-1

Solve each of the following counting problems. In each case, explain how you obtained your answer (i.e., refer to the posted slides and name the counting principle(s) you used).

- An office building contains 27 floors and has 37 offices on each floor. How many offices are in the building?
- Alice picks a card out of a standard 52-card deck. Then Bob picks a card from the ones that remain. Overall, how many different outcomes can there be?
- How many of the integers between 1 and 1000 (inclusive) are multiples of either 3 or 5?

PS8-2^{HW}

Same instructions as above.

- A multiple-choice test contains 10 questions. There are 4 possible answers for each question. In how many ways can you answer the questions on the test if...
 - ...you *must* answer every question?
 - ...you can leave answers blank? [2+2 points]
- How many of the billion numbers in the range from 1 to 10^9 contain the digit 1? [4 points]

PS8-3^{HW}

Using only algebra and elementary arithmetic—i.e., without writing a computer program—determine the sum of all the integers between 1 and 1000 (inclusive) that are multiples of either 3 or 5. You must show all your steps of algebra clearly. You're allowed to use a calculator at the final step, where you'll need to multiply and add/subtract a handful of numbers. [5 points]

PS8-4

Each user on a certain computer system has a password, which is six to eight characters long, where each character is a letter (either uppercase or lowercase) or a digit. Each password must contain at least one digit. How many possible passwords are there?

PS8-5

The password rules in the above computer system have been modified and now each password must contain at least one uppercase letter, at least one lowercase letter, and at least one digit. How many possible passwords are there now?

PS8-6^{HW}

Use the generalized product principle to solve the following counting problems.

- Let $D = \{n \in \mathbb{Z} : 0 \leq n \leq 9\}$. Determine $|T|$, where $T = \{(x, y, z) \in D^3 : x + y + z \text{ is even}\}$. [4 points]
- Let $n \geq 2$. How many n -digit natural numbers have the property that the sum of their digits is even? Note that the leftmost digit (i.e., most significant digit) cannot be zero. [4 points]

PS8-7

A *permutation* of a sequence is another sequence obtained by rearranging its terms. For instance, the three-term sequence (apple, pear, mango) has six permutations, shown below.

(apple, mango, pear) (apple, pear, mango) (mango, apple, pear)
(mango, pear, apple) (pear, apple, mango) (pear, mango, apple)

Notice that a sequence is considered to be a permutation of itself.

- How many permutations does the four-term sequence (1, 3, 8, 9) have?
- How many permutations does an n -term sequence have, assuming the terms are all distinct?

PS8-8^{HW}

We have seen that an n -term sequence *with distinct terms* has exactly $n!$ permutations. But what if the terms are not distinct?

- How many permutations does the four-term sequence (1, 1, 4, 9) have? Don't just write down a formula and calculate; explain why your formula is correct. [4 points]
Hint: For starters, pretend that one of two 1s is "red" and the other is "black" so that you can tell them apart. Now apply the division principle.
- How many anagrams does the word "CONDESCENDENCE" have? This is the same as asking how many permutations the sequence (C, O, N, D, E, S, C, E, N, D, E, N, C, E) has. [6 points]
Hint: Generalize your reasoning in the previous problem. You may refer to results derived in either of the recommended textbooks. If you do so, point out precisely which results you are using.

PS8-9

Let A and B be finite sets with $|A| = m$ and $|B| = n$.

- How many relations are there from A to B ?
- How many functions are there from A to B ?
- How many injective functions are there from A to B ?
- How many bijections are there from A to B ?

PS8-10^{HW}

A *palindrome* is a string that is identical to its reversal (in other words, it reads the same backwards as forwards). How many n -bit strings are palindromes?

Express your answer succinctly (i.e., avoid multiple cases) by cleverly using the "ceiling" function, $\lceil x \rceil$, defined as the smallest integer $\geq x$. [4 points]

PS8-11

Suppose that 13 people on a softball team show up for a game.

- How many ways are there to choose 10 players to take the field?
- How many ways are there to assign the 10 positions by selecting from the players who showed up?
- Of the 13 who showed up, 11 are students and the other 2 are professors. How many ways are there to choose 10 players to take the field if at least one of these players must be a professor?

PS8-12

How many bit strings of length 10 contain...

- ...exactly four 1s?
- ...at most four 1s?

- c. ...at least four 1s?
- d. ...an equal number of 0s and 1s?

PS8-13

Solve all parts of Problem 15.12 (about seating 8 students around a circular table) from the [LLM] book. Make sure you are able to explain every step of your calculations.

Here are some problems on **mathematical induction**. You may use either “ordinary” induction or “strong” induction, as described on the posted slides. To receive full credit, please do follow the template for proofs by induction as seen on the slides. In particular, we’ll be looking for a clear definition of a *one-variable predicate* and a clear statement of what variable you are doing induction on.

If you need a review of sum and product notation (i.e., \sum and \prod), bring this up in office hours with any of the course staff and we can help you.

PS9-1

Using mathematical induction, prove that $\forall n \in \mathbb{N}$: $\sum_{i=1}^n (2i-1) = n^2$.

PS9-2

Using mathematical induction, prove that $\forall n \in \mathbb{N}$: $\sum_{j=1}^n j \cdot j! = (n+1)! - 1$.

PS9-3

Using mathematical induction, prove that the following identity holds for all $n \in \mathbb{N}$ and all $x \in \mathbb{R} - \{1\}$:

$$1 + x + x^2 + \cdots + x^n = \frac{x^{n+1} - 1}{x - 1},$$

Careful: the identity has two variables; your first step should be to write an appropriate one-variable predicate.

PS9-4

Using mathematical induction, prove that $\forall n \in \mathbb{N} : 3 \mid n^3 + 2n$. Pretend that you don’t know modular arithmetic.

PS9-5^{HW}

Using mathematical induction, prove that $\forall n \in \mathbb{N} : 5 \mid 8^n - 3^n$. Pretend that you don’t know modular arithmetic and don’t use any number-theoretic results from previous problem sets. [5 points]

PS9-6^{HW}

Prove each of the following statements by mathematical induction.

- a. For all integers $n \geq 10$, we have $2^n \geq n^3$. [5 points]

Hint: Consider the following calculation, used in the *inductive step* of a proof that $2^n \geq n^2$ for all $n \geq 4$:

$$\begin{aligned} 2^{n+1} &= 2 \cdot 2^n \\ &\geq 2n^2 && \text{(by the induction hypothesis)} \\ &\geq n^2 + 4n && \text{(since } n \geq 4\text{)} \\ &\geq n^2 + 2n + 1 && \text{(using } n \geq 4 \text{ again)} \\ &= (n+1)^2. \end{aligned}$$

- b. For all integers $n > 1$: $\sum_{i=1}^n \frac{1}{i^2} < 2 - \frac{1}{n}$. [5 points]

Hint: First prove the following inequality for all $n > 1$ by direct algebraic manipulation (no induction!):

$$\frac{1}{n} - \frac{1}{(n+1)^2} > \frac{1}{n+1}.$$

Then use this inequality at the appropriate point in the inductive step of your main proof.

PS9-7

Recall that the basic sum principle applies to *exactly two* disjoint sets whereas the extended sum principle applies to $n \geq 2$ pairwise disjoint sets.

Use mathematical induction to prove that the extended sum principle follows from the basic sum principle.

PS9-8^{HW}

Using mathematical induction, prove that if each of the sets A_1, A_2, \dots, A_n is countable, then so is $A_1 \times A_2 \times \dots \times A_n$.
[5 points]

PS9-9

Using mathematical induction, prove that every positive integer n can be written as a sum of one or more *distinct* powers of 2. For example, $42 = 2^5 + 2^3 + 2^1$ and $77 = 2^6 + 2^3 + 2^2 + 2^0$.

Hint: You might want to consider using strong induction.

PS9-10

You have a bar of chocolate with ridges dividing it into small pieces arranged in an $m \times n$ rectangular grid in the usual fashion (examples below). You'd like to break it down into its individual small pieces using as few "snap" operations as possible: a single snap occurs along a ridge line and breaks a larger rectangle down into two smaller rectangles.



Prove that no matter how you sequence your snaps, you'll always need exactly $mn - 1$ snaps. Use mathematical induction.

PS9-11^{HW}

Suppose a finite number of players play a round-robin tournament, with everyone playing everyone else exactly once. Each match has a winner and a loser (no ties). We say that the tournament has a *cycle of length m* if there exist m players $\{p_1, p_2, \dots, p_m\}$ such that p_1 beats p_2 , who beats p_3 , ..., who beats p_m , who beats p_1 . Clearly this is possible only for $m \geq 3$.

Using mathematical induction, prove that if such a tournament has a cycle of length m , for some $m \geq 3$, then it has a cycle of length 3.
[5 points]

Here are some problems on **binomial coefficients** and **combinatorial proofs**.

PS10-1

We'll now study the fourth (and most complicated) case of the four-fold formulas. For starters, let's consider special cases.

You are in a candy store. There are six (6) kinds of candy on offer and the store has plenty of pieces of each kind in stock. You love all six kinds on offer. You just want to take home as much candy as your parent will allow!

- You have been allowed to pick two (2) pieces of candy to take home. The two pieces may be of the same kind or of different kinds. In how many different ways can you make your picks?
- Suppose, instead, that you have been allowed to pick three (3) pieces. How does the answer change? The new answer is $\binom{6}{1} + 2\binom{6}{2} + \binom{6}{3}$. How did I get this?

PS10-2

It's your lucky day: you have been allowed to pick 15 pieces of candy from the above candy store! In how many ways can you make your choice now?

It's going to be tedious to generalize the expressions you wrote in the previous problem, so you try another idea. Visualize a row of 15 books laid out on a bookshelf, to represent the 15 pieces of candy you'll pick. Now you want to assign a kind of candy to each book: remember that there are 6 kinds of candy in the store. To do so, visualize 5 separators placed on the same bookshelf, dividing up the row of books into 6 sections. The number of books in the j th section will correspond to the number of pieces of the j th kind of candy you'll pick.

- Draw a picture showing two different bookshelf layouts with the 15 books and 5 separators. For each of the layouts, write down the candy choices they indicate.
- In how many ways can you lay out 15 books and 5 separators on a bookshelf? The books are to be treated as indistinguishable from one another and so are the separators.
- Generalize! Suppose the candy store had n kinds of candy on offer and you are allowed to take home t pieces (repetitions allowed, as usual). How many books and how many separators should you use to represent your possible picks? Based on this, what is the number of ways to pick t pieces of candy from a store than offers n kinds of candy?

PS10-3^{HW}

Let $n, k \in \mathbb{N}^+$.

- Let $S_{n,k}$ be the possible nonnegative integer solutions to the inequality $x_1 + x_2 + \cdots + x_k \leq n$. That is,

$$S_{n,k} = \{(x_1, x_2, \dots, x_k) \in \mathbb{N}^k : x_1 + x_2 + \cdots + x_k \leq n\}.$$

Construct a bijection from $S_{n,k}$ to the set of bit strings that have exactly n zeroes and exactly k ones. You should define a function precisely, and prove that your function is indeed a bijection.

- Let $L_{n,k}$ be the length- k non-decreasing sequences of nonnegative integers $\leq n$. That is,

$$L_{n,k} = \{(y_1, y_2, \dots, y_k) \in \mathbb{N}^k : y_1 \leq y_2 \leq \cdots \leq y_k \leq n\}.$$

Construct a bijection from $L_{n,k}$ to $S_{n,k}$. As usual, you should define a function precisely, and prove that your function is indeed a bijection.

- Based on your work above, determine the cardinalities $|S_{n,k}|$ and $|L_{n,k}|$. [5+5+2 points]

Do you see the connection between your answers above and the fourth of the four-fold formulas you developed in **PS10-2 c**?

PS10-4

By using the factorials formula for binomial coefficients, give algebraic proofs of the following identities.

- a. For all $k, n \in \mathbb{N}$ with $k \leq n$: $\binom{n}{k} = \frac{n}{k} \cdot \binom{n-1}{k-1}$.
- b. For all $k, m, n \in \mathbb{N}$ with $k \leq m \leq n$: $\binom{n}{m} \binom{m}{k} = \binom{n}{k} \binom{n-k}{m-k}$.

PS10-5

Write down the binomial theorem, i.e., expand $(x + y)^n$. Now, by plugging in appropriate values for x and y in the binomial theorem, give algebraic proofs of each of the following identities.

- a. For all $n \in \mathbb{N}$: $\sum_{k=0}^n \binom{n}{k} = 2^n$.
- b. For all $n \in \mathbb{N}^+$: $\sum_{k=0}^n (-1)^k \binom{n}{k} = 0$.

PS10-6^{HW}

Give algebraic proofs of the following identities.

- a. For all $n \in \mathbb{N}$: $\sum_{k=0}^n \binom{n}{k} 2^k = 3^n$.
- b. For all $n \in \mathbb{N}$: $\sum_{k=0}^n k \binom{n}{k} = n 2^{n-1}$.

You can solve the latter problem by using **PS10-7c** and **PS10-7a** appropriately. Alternatively, if you know basic calculus, you can do it by expanding $(1 + x)^n$ and taking a derivative. [3+5 points]

PS10-7

Give combinatorial proofs for the following identities, which you've already proved algebraically.

- a. For all $n \in \mathbb{N}$: $\sum_{k=0}^n \binom{n}{k} = 2^n$.
- b. For all $n \in \mathbb{N}^+$: $\sum_{k=0}^n (-1)^k \binom{n}{k} = 0$.
- c. For all $k, n \in \mathbb{N}$ with $k \leq n$: $k \binom{n}{k} = n \binom{n-1}{k-1}$.
- d. For all $k, m, n \in \mathbb{N}$ with $k \leq m \leq n$: $\binom{n}{m} \binom{m}{k} = \binom{n}{k} \binom{n-k}{m-k}$.
- e. For all $n \in \mathbb{N}$: $\sum_{k=0}^n \binom{n}{k} 2^k = 3^n$.

Hint: Consider choosing a set $A \subseteq \{1, 2, \dots, n\}$ and then a subset $B \subseteq A$.

- f. For all $n \in \mathbb{N}$: $\sum_{k=0}^n k \binom{n}{k} = n 2^{n-1}$.

Hint: Consider choosing a committee and then a chairperson of that committee.

PS10-8^{HW}

Consider the following identity, which holds for all $k, n \in \mathbb{N}$ with $k \leq n$:

$$\sum_{m=k}^n \binom{m}{k} = \binom{n+1}{k+1}.$$

- a. Prove the above identity by induction, making use of Pascal's identity in the inductive step.
- b. Give a combinatorial proof of the same identity. You will have to be creative! [5+5 points]

PS10-9

Prove that if p is a prime and $0 < k < p$, then p divides $\binom{p}{k}$.

PS10-10^{EC}

Give a combinatorial proof of the following identity, where n is a positive integer.

$$\sum_{j=1}^n j \cdot j! = (n+1)! - 1.$$

PS10-11^{EC}

Using mathematical induction and the binomial theorem, give an alternate proof of the following version of Fermat's little theorem.

$$\forall a, p \in \mathbb{N} \text{ with } p \text{ prime, } p \mid a^p - a.$$

Do not use anything about multiplicative inverses modulo p .

Here are some problems on **basic probability**. Before working on these problems, it is **absolutely required** that you read Chapter 17 from the [LLM] book. Several of these problems are from the [LLM] book, but may be slightly modified, so read the wording carefully.

The symbols \mathbb{N} , \mathbb{N}^+ , \mathbb{Z} , \mathbb{Q} , and \mathbb{R} have their usual meanings.

PS11-1

Solve the following problems, each of which asks you to compute a probability. Be systematic and use the Four-Step Method (resist the urge to jump right into the calculations).

- What is the probability that '0' does not appear among k digits chosen independently and uniformly at random?
- A box contains 90 good and 10 defective screws. What is the probability that if we pick 10 screws from the box, none will be defective?
- First one digit is chosen uniformly at random from $\{1, 2, 3, 4, 5\}$ and is removed from the set; then a second digit is chosen uniformly at random from the remaining digits. What is the probability that an odd digit is picked the second time?
- Suppose that you *randomly* permute the symbols $1, 2, \dots, n$ (that is, you select a permutation uniformly at random). What is the probability that the symbol k ends up in the i th position after the permutation?
- A fair coin is flipped n times. What is the probability that all the heads occur at the end of the sequence? (If no heads occur, then "all the heads are at the end of the sequence" is vacuously true.)
- You hold the following hand of five cards from a standard 52-card deck: $\{\spadesuit 2, \spadesuit 3, \spadesuit 9, \heartsuit K, \diamondsuit 5\}$. If you discard the two non-spade cards from this hand and replace them with two uniformly random cards from the rest of the deck, what is the probability that your hand now consists of all spades?

PS11-2

Solve the following problems, each of which asks you to compute a probability. Be systematic and use the Four-Step Method (resist the urge to jump right into the calculations).

- You are dealt a poker hand of 5 cards drawn at random from a well-shuffled standard deck of 52 cards. The hand is called a *full house* if it has three cards of one rank and two of another rank (e.g., three kings and two 7s). What is the probability that your hand is a full house?
- A standard bag of Scrabble tiles has 100 tiles, exactly two (2) of which are *blank tiles*. Blanks are valuable assets in the game, since they can be turned into whatever letter you want.
You have just begun a game of Scrabble, drawing your first rack of seven (7) tiles from a full bag. What is the probability that your rack contains a blank?
- How does the answer to the above question change if your opponent is to make the first move, so your opponent picks seven random tiles first and *then* you get to pick seven from the 93 remaining tiles?

PS11-3^{HW}

The New York Yankees and the Boston Red Sox are playing a two-out-of-three series. In other words, they play until one team has won two games. Then that team is declared the overall winner and the series ends. Assume that the Red Sox win each game with probability $3/5$, regardless of the outcomes of previous games.

Answer the questions below using the Four-Step Method. You can use the same tree diagram for all three problems.

- What is the probability that a total of 3 games are played?
- What is the probability that the winner of the series loses the first game?
- What is the probability that the *correct* team wins the series? [6 points]

PS11-4

Which is more likely: rolling a total of 8 when two dice are rolled or rolling a total of 8 when three dice are rolled? Answer the same question with 8 changed to 9. Assume that all dice involved are standard, six-sided, fair dice.

PS11-5 ^{HW}

To determine which of two people gets a prize, a coin is flipped twice. If the flips are H (Head) followed by T (Tail), the first player wins. If the flips are T followed by H, the second player wins. However, if both flips land the same way, the flips don't count and the whole process starts over.

Assume that each flip results in H with probability p , regardless of what happened on other flips. Use the Four-Step Method to find a simple formula for the probability that the first player wins. What is the probability that neither player wins? [7 points]

Hint: The tree diagram and sample space are infinite, so you're not going to finish drawing the tree. Try drawing only enough to see a pattern. Summing all the winning outcome probabilities directly is cumbersome. However, a neat trick solves this problem—and many others. Let s be the sum of all winning outcome probabilities in the whole tree. Notice that you can write the sum of all the winning probabilities in certain subtrees as a function of s . Use this observation to write an equation in s and then solve it.

PS11-6 ^{HW}

We play a game with a deck of 52 regular playing cards, of which 26 are red and 26 are black. I randomly shuffle the cards and place the deck face down on a table. You have the option of “taking” or “skipping” the top card. If you skip the top card, then that card is revealed and we continue playing with the remaining deck. If you take the top card, then the game ends. If we get to a point where there is only one card left in the deck, you must take it.

You win if the card you took was revealed to be black, and you lose if it was red.

Prove that you have no better strategy than to take the top card—which means your probability of winning is exactly $1/2$. [8 points]

Hint: Prove by induction the more general claim that for a randomly shuffled deck of n cards that are red or black—not necessarily with the same number of red cards and black cards—there is no better strategy than taking the top card. To precisely state this more general claim, first work out your probability of winning if you simply take the top card.

PS11-7

The Disjoint Sum Rule for probabilities says that if A and B are two disjoint events then $\Pr[A \cup B] = \Pr[A] + \Pr[B]$. As you know, this is a consequence of the Sum Principle from basic counting. There is also the extended version of the Disjoint Sum Rule, which applies to multiple events. This states that if E_1, E_2, \dots, E_n are pairwise disjoint events, then

$$\Pr[E_1 \cup E_2 \cup \dots \cup E_n] = \Pr[E_1] + \Pr[E_2] + \dots + \Pr[E_n],$$

or in shorthand,

$$\Pr\left[\bigcup_{i=1}^n E_i\right] = \sum_{i=1}^n \Pr[E_i].$$

Starting with the Disjoint Sum Rule, derive (i.e., prove) each of the following other useful rules for reasoning about probability.

- a. Difference Rule: $\Pr[A - B] = \Pr[A] - \Pr[A \cap B]$.
- b. Complement Rule: $\Pr[\bar{A}] = 1 - \Pr[A]$.
- c. Inclusion-Exclusion: $\Pr[A \cup B] = \Pr[A] + \Pr[B] - \Pr[A \cap B]$.
- d. Union Bound for Two Events: $\Pr[A \cup B] \leq \Pr[A] + \Pr[B]$.
- e. Monotonicity: If $A \subseteq B$, then $\Pr[A] \leq \Pr[B]$.

State your reasoning for each step of each proof. Some of the proofs will be simple calculations with just a couple of steps. Venn diagrams could be useful.

PS11-8^{EC}

In the birthday problem discussed in class, there are n students with birthdays distributed *uniformly* across the d days in a year. We showed that the probability of some two students sharing a birthday is “paradoxically” high. Suppose we remove the uniformity assumption, so that not all days in $\{1, 2, \dots, d\}$ are equally likely to be birthdays. Specifically, there are non-negative real numbers p_1, p_2, \dots, p_d with $p_1 + p_2 + \dots + p_d = 1$ such that a student’s birthday equals i with probability p_i . The birthdays of different students are still independent of one another.

Prove that in this more general situation, the probability of some two students sharing a birthday is at least as high as in the uniform case.

Here are some problems on **conditional probability**. Several of these problems are from the [LLM] book, but may be slightly modified, so read the wording carefully.

PS12-1

Two fair dice are rolled in another room, out of your sight. If the sum of the two dice values is seven, you *win*. Your friend is in the other room and can observe the dice.

- Your friend calls out that one of the dice came up six. Given this information, what is the probability that you won?
- Suppose, instead, that your friend tells you that you won. In this case, what is the probability that one of the dice came up five?

PS12-2

Outside of their humdrum duties as Discrete Mathematics Ninjas, Kim is trying to learn to levitate using only intense concentration and Liz is trying to become the world champion flaming torch juggler. Suppose that Kim's probability of success is $1/6$, Liz's probability of success is $1/4$, and these two events are independent.

- If at least one of them succeeds, what is the probability that Kim learns to levitate?
- If at most one of them succeeds, what is the probability that Liz becomes the world flaming torch juggling champion?

PS12-3^{HW}

When a test for steroids is given to soccer players, 98% of the players taking steroids test positive and 12% of the players not taking steroids test (falsely) positive. Suppose that exactly 5% of soccer players take steroids. What is the probability that a soccer player who tests positive takes steroids? Be systematic: use the four-step method.

PS12-4^{HW}

Solve Problem 18.2 ("Dirty Harry") from [LLM]. Be systematic: use the four-step method.

PS12-5

The Chain Rule for probability says that if A_1, A_2, \dots, A_n are events in a probability space (\mathcal{S}, \Pr) , then

$$\begin{aligned}\Pr[A_1 \cap A_2 \cap \dots \cap A_n] &= \Pr[A_1] \cdot \Pr[A_2 | A_1] \cdot \Pr[A_3 | A_1 \cap A_2] \cdot \dots \cdot \Pr[A_n | A_1 \cap A_2 \cap \dots \cap A_{n-1}] \\ &= \Pr[A_1] \cdot \Pr[A_2 | A_1] \cdot \Pr[A_3 | A_1, A_2] \cdot \dots \cdot \Pr[A_n | A_1, A_2, \dots, A_{n-1}] \\ &= \prod_{j=1}^n \Pr[A_j | A_1, A_2, \dots, A_{j-1}].\end{aligned}$$

- Prove this rule, i.e., prove the first equation. (The other two lines are just rewritings.)
Hint: You could use induction, but don't. Also, start with the right-hand side.
- Use this rule to answer the following question. Suppose n passengers board a flight that has n seats and they each take a seat at random, ignoring their assigned seating. The passengers board one by one. What is the probability that passengers 1 through k (inclusive) all end up in their assigned seats?

PS12-6^{HW}

A 52-card deck is thoroughly shuffled and you are dealt a hand of 13 cards.

- If you have one ace, what is the probability that you have a second ace?
- If you have the ace of spades, what is the probability that you have a second ace? Remarkably, the answer is different from the previous one!

You may leave your answers in terms of binomial coefficients and/or factorials, but you must do enough work to convince your grader that the answers in Part (a) and Part (b) are different. [3+3 points]

PS12-7

Sally Smart just graduated from high school. She was accepted to three reputable colleges.

- With probability $4/12$, she attends Brown.
- With probability $5/12$, she attends Dartmouth.
- With probability $3/12$, she attends Little Hoop Community College.

Sally is either happy or unhappy in college.

- If she attends Brown, she is happy with probability $4/12$.
 - If she attends Dartmouth, she is happy with probability $7/12$.
 - If she attends Little Hoop, she is happy with probability $11/12$.
- a. What is the probability that Sally is happy in college?
 - b. What is the probability that Sally attends Brown, given that she is happy in college?
 - c. Show that the events “Sally attends Brown” and “Sally is happy” **are not** independent.
 - d. Show that the events “Sally attends Dartmouth” and “Sally is happy” **are** independent.

PS12-8

Study Section 18.8 (Mutual Independence) of [LLM]. Then solve Problem 18.34, about non-independent events that nevertheless satisfy a “product rule”.

PS12-9^{HW}

Let E and F be two independent events in some probability space (\mathcal{S}, Pr) . Assume that $0 < \text{Pr}[E] < 1$ and $0 < \text{Pr}[F] < 1$.

- a. Prove or disprove that \overline{E} and \overline{F} *must* be independent.
- b. Prove or disprove that \overline{E} and F *must* be independent.

PS12-10

Solve Problem 18.17 (variation of Monty Hall’s game) from [LLM]. You will of course need to have done your earlier homework of reading Chapter 17, where Monty Hall’s game is discussed. You will also need to review how to sum an *infinite* geometric series, which is discussed in Section 14.1.4 of [LLM].

Here are some problems on **random variables and expectation**.

PS13-1

Let $n \geq 2$ be an integer. We choose a random integer $X \in \mathbb{Z}_n$ uniformly. Let $Y = \gcd(X, n)$. Determine $\text{Ex}[Y]$ in each of the following cases.

- a. $n = 7$.
- b. $n = 9$.
- c. $n = 15$.
- d. $n = p^2$, where p is a prime.
- e. $n = pq$, where p and q are distinct primes.

PS13-2^{HW}

We flip a fair coin repeatedly until either it comes up heads twice or we have flipped it six times. What is the expected number of times we flip the coin?

PS13-3

A lottery ticket costs \$1. It contains six distinct integers, each from the set $S := \{1, 2, \dots, 50\}$. The ticket wins and pays off \$10 million iff, on the day of the drawing, the six winning numbers chosen from S all appear on the ticket (the drawing is without replacement, so the same integer cannot be drawn more than once).

Perform an expected value analysis and answer this: is the lottery ticket worth its price?

PS13-4

We simultaneously roll 24 fair dice, and they show numbers W_1, \dots, W_{24} .

- a. How many sixes do we expect to see? In other words, compute $\text{Ex}[|\{j : W_j = 6\}|]$.
- b. Even though each die is fair, they have been connected together by very thin weightless threads and this causes W_1, \dots, W_{24} to be correlated in some unknown way. (For example, it may be that whenever W_1 is even, W_2 is more likely to be even than odd; or that whenever W_8 is a prime number, W_{20} is sure to be prime; or both of the above.) How does this affect your answer above?

PS13-5^{HW}

The final exam of a discrete mathematics course consists of 50 true/false questions, each worth two points, followed by 25 multiple-choice questions, each worth four points. Zoe answers each true/false question correctly with 90% probability and each multiple-choice question correctly with 80% probability.

Let the random variable X denote Zoe's score on the exam. Let Y_i be an indicator random variable for the event "Zoe gets question i correct," for $1 \leq i \leq 75$.

- a. Express X in terms of Y_1, \dots, Y_{75} .
- b. Compute $\text{Ex}[Y_i]$, for each i .
- c. Use linearity of expectation to compute Zoe's expected score on the exam.

PS13-6

We roll two fair dice, a *red* die and a *blue* die, and they show numbers X and Y , respectively (these are therefore random variables). Let $W = X + Y$.

- 1. Compute $\text{Ex}[X^2 \mid X \text{ is a perfect square}]$.
- 2. Show that $\text{Ex}[WX] \neq \text{Ex}[W] \text{Ex}[X]$.

PS13-7

Two people that have the same birthday are said to form a *calendrical bond*. Assuming that the n students in a class have birthdays distributed uniformly among the d days in a year, and birthdays are mutually independent, what is the expected number of calendrical bonds among students in the class? Derive a formula in terms of n and d , then apply it to our CS30 class, using $n = 40$ and $d = 365$.

Hint: The random variable of interest here is a sum of $\binom{n}{2}$ indicator RVs.

PS13-8^{HW}

The following fragment of C code finds the maximum value in an array `arr` consisting of n integers:

```

1  max = arr[0];
2  for(i = 1; i < n; i++)
3      if(arr[i] > max)
4          max = arr[i];

```

In words, we pick the zeroth element of the array and store it in `max`, then for each successive element of the array, if it exceeds `max` then we update `max` with that element.

Determine the expected number of times that `max` is updated—i.e., Line 4 is executed—assuming that the elements of `arr` are all distinct and arranged in a uniformly random order. (Careful: I did not say that the *elements* are random, it's their *order* which is random.)

PS13-9

(This problem has special significance in Computer Science, for it is meant to model the process of inserting keys into a hash table.) There are n bins, initially all empty. Then n balls are thrown randomly (uniformly) and independently into the bins: “uniformly” means that each ball is equally likely to go into each of the bins. What is the expected number of bins that remain empty after this process?

PS13-10^{HW}

Prove these useful facts about expectation. Each proof can be written in a few lines of algebra.

- Let I_A be an indicator random variable for an event A . Prove that $\text{Ex}[I_A] = \Pr[A]$.
- Prove the **law of total expectation**, which states that if X is a random variable on a probability space (\mathcal{S}, \Pr) and $A_1, \dots, A_n \subseteq \mathcal{S}$ are pairwise disjoint events such that $A_1 \cup \dots \cup A_n = \mathcal{S}$, then

$$\text{Ex}[X] = \sum_{j=1}^n \text{Ex}[X | A_j] \Pr[A_j].$$

- Let X be a nonnegative integer valued random variable on a probability space (\mathcal{S}, \Pr) where \mathcal{S} is a finite set. For each integer $k \geq 0$, let A_k be the event “ $X \geq k$.” Prove that

$$\text{Ex}[X] = \sum_{k=1}^{\infty} \Pr[A_k].$$

PS13-11

Two independent random variables, X and Y , are each drawn uniformly from $\{1, 2, \dots, n\}$, where $n \geq 1$ is an integer. What is $\text{Ex}[|X - Y|]$?

PS13-12

A computer user, working on a 1000×1000 image (measured in pixels), makes a rectangular selection of a portion of the image by clicking on a pixel P and another pixel Q . The selected rectangle is the one that has P and Q as opposite corners. If P and Q are chosen at random, independently and uniformly, then what is the expected area of the selected rectangle?

Hint: What do you know about the expectation of the product of two independent random variables?

PS13-13^{EC}

Upon moving into her new house with one front door and one back door, Professor Random places three pairs of walking shoes at each door; all six pairs are distinct. From then on, she starts the following morning routine. Each morning she picks a door at random (uniformly), puts on a pair of shoes at that door, takes a walk outside and returns to a door chosen at random (uniformly), leaving the shoes at *that* door. What is the expected number of walks that Professor Random takes until one morning she finds that her chosen exit door has no walking shoes available?

Here are some problems on **distributions and variance**. Use these as practice problems to strengthen your understanding as you do the reading corresponding to this unit. The topics you will want to read up on are listed at the end of the slides for this unit. You do not need to submit solutions to these problems. You are free to discuss these problems on Piazza.

We will use the following notation for the important probability distributions discussed in class.

- $\text{Bern}(p)$ denotes the Bernoulli distribution with parameter p .
- $\text{Bin}(n, p)$ denotes the binomial distribution with parameters n and p .
- $\text{Geom}(p)$ denotes the geometric distribution with parameter p .
- $\text{Pois}(\lambda)$ denotes the Poisson distribution with parameter λ .
- $\text{Unif}(A)$ denotes the uniform distribution over the set A .

We write $X \sim \text{Bern}(p)$ to denote that X is a random variable that has the Bernoulli distribution with parameter p , and so on.

PS14-1

Suppose R, S , and T are mutually independent random variables on the same probability space with uniform distribution on the range $\{1, 2, 3\}$. Let $M = \max\{R, S, T\}$. Compute the functions pdf_M and CDF_M .

PS14-2

A gambler bets \$10 on “red” at a roulette table (the odds of red are 18/38, slightly less than even) to win \$10. If he wins, he gets back twice the amount of his bet, and he quits. Otherwise, he doubles his previous bet and continues. For example, if he loses his first two bets but wins his third bet, the total spent on his three bets is $10 + 20 + 40$ dollars, but he gets back 2×40 dollars after his win on the third bet, for a net profit of \$10.

- What is the expected number of bets the gambler makes before he wins?
- What is his probability of winning?
- What is his expected final profit (amount won minus amount lost)?
- You can beat a biased game by bet doubling, but bet doubling is not feasible because it requires an infinite bankroll. Verify this by proving that the expected size of the gambler’s last bet is infinite.

PS14-3^{HW}

Take a biased coin with heads probability p and flip it n times. Let the random variable J denote the number of heads obtained. Recall that, by definition, $J \sim \text{Bin}(n, p)$. Following our analysis from class (or Section 19.5.3 from [LLM]), we have $\text{Ex}[J] = np$.

Intuitively, the PDF of J should peak roughly at this expected value np . Here is what you can prove formally:

$$\begin{aligned} \text{pdf}_J(k-1) &< \text{pdf}_J(k) && \text{for } k < np + p, \\ \text{pdf}_J(k-1) &> \text{pdf}_J(k) && \text{for } k > np + p. \end{aligned}$$

Prove the above inequalities, using the formula for the PDF of a binomial distribution. Explain in words what this says about the “graph” of pdf_J .

PS14-4

Let C be the number of trials to first success, where a single trial success with probability p and the trials are mutually independent. Assume that $0 < p \leq 1$.

By definition, $C \sim \text{Geom}(p)$.

- Let A be the event that the first trial succeeds. Conditioning on A and \bar{A} , using the law of total expectation, write an equation for $\text{Ex}[C^2]$.

- b. Solve the equation, then use the solution to work out $\text{Var}[C]$. You should obtain $\text{Var}[C] = \frac{1-p}{p^2}$.

PS14-5

Solve [LLM] Problem 19.12 (about flipping a coin until certain patterns appear).

PS14-6^{HW}

Let R be a positive integer valued random variable.

- If $\text{Ex}[R] = 2$, how large can $\text{Var}[R]$ be?
- How large can $\text{Ex}[1/R]$ be? (Do not assume that $\text{Ex}[R] = 2$. That's only for the previous part.)
- If $R \leq 2$, that is, the only possible values of R are 1 and 2, then how large can $\text{Var}[R]$ be?

PS14-7^{HW}

Dr. Markov has a set of n keys, only one of which will fit the lock on the door to his apartment. He tries the keys until he finds the right one. Give the expectation and variance of the number of keys he has to try, when...

- ...he tries the keys at random (possibly repeating a key tried earlier).
- ...he chooses keys randomly among the ones that he has not yet tried.

PS14-8

Recall the theorem $\text{Var}[X] = \text{Ex}[X^2] - \text{Ex}[X]^2$, and the theorem that for independent RVs X and Y , $\text{Ex}[XY] = \text{Ex}[X]\text{Ex}[Y]$.

- Using these two theorems and algebraic manipulation, prove that if X and Y are independent random variables, then

$$\text{Var}[X + Y] = \text{Var}[X] + \text{Var}[Y]. \quad (1)$$

- If $c \in \mathbb{R}$ is a constant and X is a random variable, prove that $\text{Var}[cX] = c^2 \text{Var}[X]$. Explain why this shows that Eq. (1) does not hold for an *arbitrary* pair of RVs X, Y .
- Extend Eq. (1) to show that if the random variables X_1, \dots, X_n are pairwise independent, then

$$\text{Var}[X_1 + \dots + X_n] = \text{Var}[X_1] + \dots + \text{Var}[X_n].$$

We saw in class that the sum of mutually independent Bernoulli random variables, all having the same parameter, is a binomial random variable: if $X_1 \sim \text{Bern}(p)$, ..., $X_n \sim \text{Bern}(p)$ and the X_i s are mutually independent, then $X_1 + \dots + X_n \sim \text{Bin}(n, p)$. The next few problems explore what happens when independent random variables from other important distributions are added.

PS14-9^{HW}

Consider adding two uniform distributions. Suppose that $X \sim \text{Unif}(A)$ and $Y \sim \text{Unif}(A)$ for some set $A \subseteq \mathbb{R}$ and that X and Y are independent. Is $X + Y \sim \text{Unif}(B)$ for some $B \subseteq \mathbb{R}$?

PS14-10

Show that if $X \sim \text{Geom}(p)$ and $Y \sim \text{Geom}(q)$, with X and Y independent, then $X + Y$ need not have a geometric distribution. For the special case $p = q = 1/2$, work out what pdf_{X+Y} is.

PS14-11^{EC}

Let X and Y be independent nonnegative-integer-valued random variables. Let $f = \text{pdf}_X$, $g = \text{pdf}_Y$, and $h = \text{pdf}_{X+Y}$. Then prove that, for all integers $r \geq 0$,

$$h(r) = \sum_{t=0}^r f(t)g(r-t).$$

We say that h is the *convolution* of f and g .

Hint: Use the law of total probability. Study the event “ $X + Y = r$ ” conditioned on the various values that X can take.

PS14-12^{EC}

Suppose that $X \sim \text{Pois}(\lambda)$ and $Y \sim \text{Pois}(\mu)$ are independent random variables, for some real numbers $\lambda, \mu \geq 0$. Prove that $X + Y \sim \text{Pois}(\lambda + \mu)$. Does this result make intuitive sense to you, considering what a Poisson distribution is attempting to model?

Hint: Use the above convolution formula and the binomial theorem.

**** I will add a couple of problems to this set ****