# Problem Set for Unit 1

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.

$$\begin{aligned}\mathbb{Z} &= \text{the set of all integers},\\ \mathbb{N} &= \text{the set of all non-negative integers},\\ \mathbb{N}^+ &= \text{the set of all positive integers},\\ \mathbb{R} &= \text{the set of all real numbers}.\end{aligned}$$

***PS1-1***

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

***a.*** $\{x : x \text{ is a multiple of 7 and } 0 < x < 50\}$.

***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.*** $(A - C) \cap (C - B) = \varnothing$.

***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 $\mathscr{P}(\mathbb{Z})$.

***c.*** The relation "is no larger than", on $\mathscr{P}(\mathbb{Z})$. 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 $\mathscr{P}(\mathbb{Z})$. [4 points]

***b.*** $\{(m, n) \in \mathbb{N} \times \mathbb{N} :$ the sum of the digits of $m$ 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 $S =$ {"RED", "BLUE", "GREEN", "YELLOW", "ORANGE", "BLACK"} and $T = \{1, 2, 3, 4, 5, 6\}$. Consider the function len: $S \to T$ given by len($s$) = 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 $g : T \to S$. If not, why not?

***PS1-10*** Let $f : A \to B$ 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 $g : A \to B$ and $f : B \to C$ 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 $f, g : \mathbb{R} \to \mathbb{R}$ 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 $f, \mathrm{id} : \mathbb{R} \to \mathbb{R}$ are given by the formulas $f(x) = x^3 + 7$ and $\mathrm{id}(x) = x$. You may recall that "id" is called the *identity function* on $\mathbb{R}$.

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

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

# Problem Set for Unit 2

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 $f : A \to B$ 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 $f : A \to B$ 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*:

$$f(S) \;=\; \{f(x) : x \in S\},$$
$$f^{-1}(T) \;=\; \{x \in A : f(x) \in T\}.$$

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 $f : B \to C$ and $g : A \to B$ 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 $g : \mathscr{P}(S) \to \mathscr{P}(S)$ 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

$$\mathscr{P}^{\text{odd}}(S) = \{A \subseteq S : |A| \text{ is an odd number}\},$$
$$\mathscr{P}^{\text{even}}(S) = \mathscr{P}(S) - \mathscr{P}^{\text{odd}}(S).$$

Make sure you understand what these notations mean by taking the *particular* 3-element set $T = \{1,2,3\}$ and writing out $\mathscr{P}^{\text{odd}}(T)$ and $\mathscr{P}^{\text{even}}(T)$ in roster notation. No need to turn this part in.

Now, let $S$ be an *arbitrary* nonempty finite set. Construct a bijection $h : \mathscr{P}^{\text{odd}}(S) \to \mathscr{P}^{\text{even}}(S)$ 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.

- ***a.*** If there exists a surjection $f : A \to B$, then $|A| \geq |B|$.
- ***b.*** If there exists an injection $g : A \to B$, then $|A| \leq |B|$.
- ***c.*** If there exists a surjection $f : A \to B$ as well as an injection $g : A \to B$, 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:

$$0,\ 1,\ -1,\ 2,\ -2,\ 3,\ -3,\ \ldots. \tag{1}$$

Let's define the same bijection explicitly using algebraic formulas. First, define the function $f : \mathbb{N} \to \mathbb{Z}$ 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 $f(0), f(1), f(2), \ldots$ 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 $g : \mathbb{Z} \to \mathbb{N}$ 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 $f : A \to \mathbb{N}$. Prove that $A$ is countable.

***PS2-9***

Prove that $\mathbb{N} \times \mathbb{N}$ is countable by constructing an injection $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ 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 $\mathbb{N}^*$:

$$(5, 93, 12, 0, 51); \qquad (42, 42, 42); \qquad (65); \qquad (1, 2, 3, \ldots, 2019)$$

Give a detailed proof that $\mathbb{N}^*$ is countable.

# Problem Set for Unit 4

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 $\mathbb{Z}_d = \{0, 1, 2, \ldots, d-1\}$, 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

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

Using the definition of congruence, prove that

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

***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.

# Problem Set for Unit 3

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 $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ 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

$$2^a 3^b = 2^c 3^d . \tag{1}$$

- ***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 $f : A \to \mathbb{N}$. [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 $f : (0, 1) \times (0, 1) \to (0, 1)$.

***PS3-10*** ***HW***

Construct a bijection $g : (0, 1] \to (0, 1)$. [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 $h : (0, 1) \times (0, 1) \to (0, 1)$.

# Problem Set for Unit 5

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.

- ***a.*** In a similar way, compute the gcd of 13631 and 8213, showing your work at each step.
- ***b.*** Let the gcd be $g$. Then, according to the GCD Linear Combination Theorem (LCT), there exists a pair of integers $(k, \ell)$, such that $13631k + 8213\ell = g$. Find one such pair.
- ***c.*** 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 $\ell$ 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 $a, b, c, n \in \mathbb{N}^+$,

- ***a.*** $\gcd(a, b) \neq 1 \wedge \gcd(b, c) \neq 1 \implies \gcd(a, c) \neq 1$.
- ***b.*** $\gcd(a^n, b^n) = \gcd(a, b)^n$.
- ***c.*** $\gcd(ab, ac) = a \cdot \gcd(b, c)$.
- ***d.*** $\gcd(1 + a, 1 + b) = 1 + \gcd(a, b)$.
- ***e.*** if an IntLC of $a$ and $b$ equals 1, then so does some IntLC of $a$ and $b^2$.
- ***f.*** 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 $(a, b) \in \mathbb{Z} \times \mathbb{Z} - \{(0, 0)\}$.

- ***a.*** Find a pair of integers $(a, b)$ for which the answer returned by egcd$(a, b)$ is incorrect, according to the definition of gcd given in class and the lecture notes.
- ***b.*** 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 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 $a + b$.

- ***a.*** 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 $< s$.
- ***b.*** 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).

***a.*** Prove that $\exists\, x, y \in \mathbb{N}^+$ such that $\text{lcm}(a, b) = ax = by$ and $\gcd(x, y) = 1$.

***b.*** Using LCT, express $a/y$ as an integer linear combination of $a$ and $b$.

***c.*** Using the above, show that $\gcd(a, b) \mid a/y$.

***d.*** On the other hand, show that $a/y$ is a divisor of both $a$ and $b$.

***e.*** Conclude that $\gcd(a, b) = a/y$.

***f.*** 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

***a.*** $b$ has an inverse modulo $p$;

***b.*** the function $f_b : \mathbb{Z}_p \to \mathbb{Z}_p$ 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."

***a.*** 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 $u, v \in \mathbb{N}^+$.

***b.*** 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.

***c.*** Give a detailed proof that $\sqrt{p}$ is irrational for every prime $p$.

***d.*** 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, $a^2 \equiv 1 \pmod{m}$.

***a.*** Prove that if $p \geq 3$ is a prime, there are exactly two self-inverses modulo $p$.

***b.*** Find all numbers is $\mathbb{Z}_{15}$ 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.

# Problem Set for Unit 6

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

***a.*** its inverse modulo 30;

***b.*** 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 $a \in \mathbb{Z}_m^*$.

***a.*** 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***.

***b.*** Using the above result and the Inverse Existence Theorem, prove that $a^{\phi(m)} \equiv 1 \pmod{m}$.

***c.*** 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 $m$:

$$P_{m,a} := (a^0 \bmod m,\ a^1 \bmod m,\ a^2 \bmod m,\ a^3 \bmod m,\ \ldots).$$

For instance, $P_{7,3} = (1, 3, 2, 6, 4, 5, 1, 3, 2, 6, 4, 5, 1, 3, \ldots)$. 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: $P_{11,5} = (1, 5, 3, 4, 9, 1, 5, 3, 4, 9, 1, 5, \ldots)$. 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 pairs[1] 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 $\gcd(a, b)$, then make use of LCT.

***b.*** Using the above result repeatedly, prove that if $p_1, p_2, \ldots, p_k$ 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.

[1] This means that every element of $S$ occurs in exactly one of the pairs.

# Problem Set for Unit 7

Prof. Amit Chakrabarti
Computer Science Dept
Dartmouth College

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 $\mathscr{A}$ to quickly compute $\phi(N)$, given $N$. We believe that factoring is hard, but why should computing $\phi$ be hard?

Prove that if computing $\phi$ were easy—i.e., algorithm $\mathscr{A}$ exists—then $\mathscr{A}$ 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. Tricksy 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. Tricksy'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 $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ 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

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

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 tells 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 $\mathscr{B}$ 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 $\mathscr{B}$ exists, then $\mathscr{B}$ 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

$$b_0 = a^s \bmod m,\ b_1 = a^{2s} \bmod m,\ b_2 = a^{2^2 s} \bmod m,\ \ldots,\ b_r = a^{2^r s} \bmod m\,.$$

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 $\forall\, j \in \{0, 1, \ldots, r\} :\ b_j \neq m-1$.

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 $\mathscr{B}$ can be used to factor $m$ quickly.

# Problem Set for Unit 8

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).

***a.*** An office building contains 27 floors and has 37 offices on each floor. How many offices are in the building?

***b.*** 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?

***c.*** 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.*** 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...

(a) ...you *must* answer every question?

(b) ...you can leave answers blank? [2+2 points]

***b.*** 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.

***a.*** 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]

***b.*** 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.

***a.*** How many permutations does the four-term sequence $(1, 3, 8, 9)$ have?

***b.*** 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?

***a.*** 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.

***b.*** 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 $|B| = n$.

***a.*** How many relations are there from $A$ to $B$?

***b.*** How many functions are there from $A$ to $B$?

***c.*** How many injective functions are there from $A$ to $B$?

***d.*** 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.

***a.*** How many ways are there to choose 10 players to take the field?

***b.*** How many ways are there to assign the 10 positions by selecting from the players who showed up?

***c.*** 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...

***a.*** ...exactly four 1s?

***b.*** ...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.

# Problem Set for Unit 9

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 $\forall\, n \in \mathbb{N}$: $\displaystyle\sum_{i=1}^{n}(2i-1) = n^2$.

***PS9-2***

Using mathematical induction, prove that $\forall\, n \in \mathbb{N}$: $\displaystyle\sum_{j=1}^{n} j \cdot j! = (n+1)! - 1$.

***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 $n > 1$: $\displaystyle\sum_{i=1}^{n} \frac{1}{i^2} < 2 - \frac{1}{n}$. [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 $A_1, A_2, \ldots, A_n$ is countable, then so is $A_1 \times A_2 \times \cdots \times A_n$. [5 points]

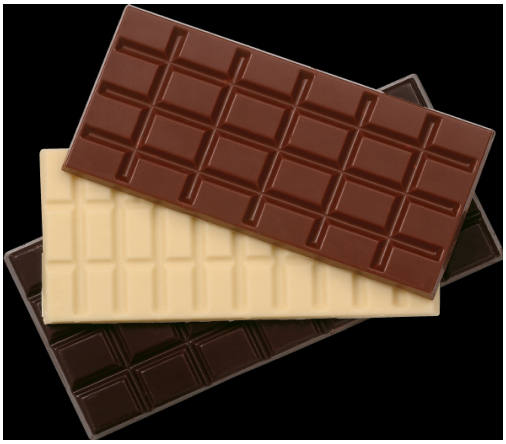
***PS9-9***

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 $\{p_1, p_2, \ldots, p_m\}$ 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!

***a.*** 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?

***b.*** 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.

***a.*** 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.

***b.*** 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.

***c.*** 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 $n, k \in \mathbb{N}^+$.

***a.*** Let $S_{n,k}$ be the possible nonnegative integer solutions to the inequality $x_1 + x_2 + \cdots + x_k \leq n$. That is,

$$S_{n,k} = \{(x_1, x_2, \ldots, x_k) \in \mathbb{N}^k : x_1 + x_2 + \cdots + x_k \leq n\}.$$

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.

***b.*** Let $L_{n,k}$ be the length-$k$ non-decreasing sequences of nonnegative integers $\leq n$. That is,

$$L_{n,k} = \{(y_1, y_2, \ldots, y_k) \in \mathbb{N}^k : y_1 \leq y_2 \leq \cdots \leq y_k \leq n\}.$$

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.

***c.*** 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 ***PS10-7 c*** and ***PS10-7 a*** 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 $A \subseteq \{1, 2, \ldots, n\}$ 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.

$$\forall\, a, p \in \mathbb{N} \text{ with } p \text{ prime}, \quad p \mid a^p - a .$$

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).

***a.*** What is the probability that '0' does not appear among $k$ digits chosen independently and uniformly at random?

***b.*** 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?

***c.*** 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?

***d.*** Suppose that you *randomly* permute the symbols $1, 2, \ldots, n$ (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?

***e.*** 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.)

***f.*** You hold the following hand of five cards from a standard 52-card deck: $\{\spadesuit 2, \spadesuit 3, \spadesuit 9, \heartsuit \text{K}, \diamondsuit 5\}$. 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).

***a.*** 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?

***b.*** 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?

***c.*** 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.

***a.*** What is the probability that a total of 3 games are played?

***b.*** What is the probability that the winner of the series loses the first game?

***c.*** 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 $E_1, E_2, \ldots, E_n$ are pairwise disjoint events, then

$$\Pr[E_1 \cup E_2 \cup \cdots \cup E_n] = \Pr[E_1] + \Pr[E_2] + \cdots + \Pr[E_n],$$

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: $\Pr[\overline{A}] = 1 - \Pr[A]$.
- ***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 $\{1, 2, \ldots, d\}$ are equally likely to be birthdays. Specifically, there are non-negative real numbers $p_1, p_2, \ldots, p_d$ with $p_1 + p_2 + \cdots + p_d = 1$ 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.

- ***a.*** Your friend calls out that one of the dice came up six. Given this information, what is the probability that you won?
- ***b.*** 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.

- ***a.*** If at least one of them succeeds, what is the probability that Kim learns to levitate?
- ***b.*** 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 $A_1, A_2, \ldots, A_n$ are events in a probability space $(\mathscr{S}, \Pr)$, then

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

- ***a.*** 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.
- ***b.*** 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.

- ***a.*** If you have one ace, what is the probability that you have a second ace?
- ***b.*** 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 $0 < \Pr[E] < 1$ and $0 < \Pr[F] < 1$.

***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 $\mathrm{Ex}[Y]$ 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 $S := \{1, 2, \ldots, 50\}$. 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 $W_1, \ldots, W_{24}$.

***a.*** How many sixes do we expect to see? In other words, compute $\mathrm{Ex}\big[|\{j : W_j = 6\}|\big]$.

***b.*** Even though each die is fair, they have been connected together by very thin weightless threads and this causes $W_1, \ldots, W_{24}$ 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 $Y_1, \ldots, Y_{75}$.

***b.*** Compute $\mathrm{Ex}[Y_i]$, 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 $\mathrm{Ex}[X^2 \mid X \text{ is a perfect square}]$.
2. Show that $\mathrm{Ex}[WX] \neq \mathrm{Ex}[W]\,\mathrm{Ex}[X]$.

***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.

***a.*** Let $I_A$ be an indicator random variable for an event $A$. Prove that $\text{Ex}[I_A] = \Pr[A]$.

***b.*** Prove the **law of total expectation**, which states that if $X$ is a random variable on a probability space $(\mathcal{S}, \Pr)$ and $A_1, \ldots, A_n \subseteq \mathcal{S}$ are pairwise disjoint events such that $A_1 \cup \cdots \cup A_n = \mathcal{S}$, then

$$\text{Ex}[X] = \sum_{j=1}^{n} \text{Ex}[X \mid A_j] \Pr[A_j].$$

***c.*** 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 $\{1, 2, \ldots, n\}$, where $n \geq 1$ is an integer. What is $\text{Ex}[|X - Y|]$ ?

***PS13-12***

A computer user, working on a $1000 \times 1000$ 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.

- Bern($p$) denotes the Bernoulli distribution with parameter $p$.
- Bin($n, p$) denotes the binomial distribution with parameters $n$ and $p$.
- Geom($p$) denotes the geometric distribution with parameter $p$.
- Pois($\lambda$) denotes the Poisson distribution with parameter $\lambda$.
- 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 $\text{pdf}_M$ and $\text{CDF}_M$.

***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 $2 \times 40$ dollars after his win on the third bet, for a net profit of \$10.

***a.*** What is the expected number of bets the gambler makes before he wins?

***b.*** What is his probability of winning?

***c.*** What is his expected final profit (amount won minus amount lost)?

***d.*** 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:

$$\text{pdf}_J(k-1) < \text{pdf}_J(k) \qquad \text{for } k < np + p\,,$$
$$\text{pdf}_J(k-1) > \text{pdf}_J(k) \qquad \text{for } k > np + p\,.$$

Prove the above inequalities, using the formula for the PDF of a binomial distribution. Explain in words what this says about the "graph" of $\text{pdf}_J$.

***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, $C \sim \text{Geom}(p)$.

***a.*** Let $A$ be the event that the first trial succeeds. Conditioning on $A$ and $\overline{A}$, 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 $\text{Var}[C] = \dfrac{1-p}{p^2}$ .

***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.

***a.*** If $\text{Ex}[R] = 2$, how large can $\text{Var}[R]$ be?

***b.*** How large can $\text{Ex}[1/R]$ be? (Do not assume that $\text{Ex}[R] = 2$. That's only for the previous part.)

***c.*** 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...

***a.*** ...he tries the keys at random (possibly repeating a key tried earlier).

***b.*** ...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 $Y$, $\text{Ex}[XY] = \text{Ex}[X]\,\text{Ex}[Y]$.

***a.*** Using these two theorems and algebraic manipulation, prove that if $X$ and $Y$ are independent random variables, then

$$\text{Var}[X+Y] = \text{Var}[X] + \text{Var}[Y]. \tag{1}$$

***b.*** 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 $X$, $Y$.

***c.*** Extend Eq. (1) to show that if the random variables $X_1, \ldots, X_n$ are pairwise independent, then

$$\text{Var}[X_1 + \cdots + X_n] = \text{Var}[X_1] + \cdots + \text{Var}[X_n].$$

We saw in class that the sum of mutually independent Bernoulli random variables, all having the same parameter, is a binomial random variable: if $X_1 \sim \text{Bern}(p)$, $\ldots$, $X_n \sim \text{Bern}(p)$ and the $X_i$s are mutually independent, then $X_1 + \cdots + X_n \sim \text{Bin}(n, p)$. 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 $\text{pdf}_{X+Y}$ 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 **