August 27 *Let $A = \{1, \{1, 2\}, 3, \{2, 5\}\}$, and let $B = \{3, \{1, 2\}\}$. By explicitly listing out the elements, calculate $|A|$ and $|B|$. Explain why it is the case that B is a subset of A. What does the fact that $B \subseteq A$ tell you about the relationship between $|B|$ and $|A|$, and why?*

We observe that A has four elements: the number 1, the set $\{1, 2\}$, the number 3, and the set $\{2, 5\}$, and so $|A| = 4$. Likewise, B has two elements: the number 3, and the set $\{1, 2\}$, so $|B| = 2$. B must be a subset of A because each of the two elements of B are verifiably also elements of A. One obvious relationship between $|B|$ and $|A|$ which is apparently related to the fact that $B \subseteq A$ is the fact that $|B| \leq |A|$. Aside from the visual similarity of the symbols, this relationship is supported by the fact that the definition of $B \subseteq A$ is that every element of B is an element of A, so that when we count the elements in A, we must count every element of B and then perhaps more, which leads to the conclusion that $|B| \leq |A|$.

August 29 *Give a short explanation in words of what each of the following symbolic statements means, and why it must be true. Below, the letters A and B represent arbitrary sets — do not appeal to specific examples.*

- $A \in \mathcal{P}(A)$.

  In words, this symbolic statement would be "A is an element of the power set of A", which, expanded into definitions, would give "A is an element of the set whose elements are subsets of A". Clearly this is equivalent to the statement "A is a subset of A", which we know to be true, since every element of A is, in fact, an element of A.

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

  In words, this symbolic statement would be "The intersection of the difference between A and B with B is empty", which is to say, there is no object which is an element of both $A - B$ and B; the definition of difference means that this statement is equivalent to claiming that "There is no object which is simultaneously in A, not in B, and in B." Since the latter two conditions are contradictory, this is unsurprisingly true.

August 31 *Translate the following written statements to symbolic logic, and use a truth table to determine the circumstances under which each is true. Below, P, Q, and R represent named statements.*

- *"P is not true, or both P and Q are true."*

  "P is not true" is the negation of P, and would have symbolic representation $\neg P$; "both P and Q are true" is a conjunction of P and Q, and has symbolic representation $P \wedge Q$. The statement as a whole is a disjunction of these two statements, and would thus be $(\neg P) \vee (P \wedge Q)$.

  Below is the truth table for this statement's dependency on P and Q:

P	Q	$\neg P$	$P \wedge Q$	$(\neg P) \vee (P \wedge Q)$
T	T	F	T	T
T	F	F	F	F
F	T	T	F	T
F	F	T	F	T

- *"If either P or Q is true, then Q is not true."*

  "Either P or Q is true" is a disjunction of P and Q, written $P \vee Q$. "Q is not true" is a negation of Q, written $\neg Q$. The statement as a whole is an implication of the second above statement from the first, so it is symbolically $(P \vee Q) \to (\neg Q)$.

Below is the truth table for this statement's dependency on P and Q:

P	Q	$P \vee Q$	$\neg Q$	$(P \vee Q) \to (\neg Q)$
T	T	T	F	F
T	F	T	T	T
F	T	T	F	F
F	F	F	T	T

- *"It is not the case that if both P and Q are true, then either Q or R is true."*

  "Both P and Q are true" is the conjunction of P and Q, written $P \wedge Q$. "Either Q or R is true" is the disjunction of Q and R, written $Q \vee R$. The larger statment "If both P and Q are true, then either Q or R is true" is an implication involving these two statements, i.e. $(P \wedge Q) \to (Q \vee R)$, but the statement as a whole is in fact a *negation* of this implication, and thus $\neg[(P \wedge Q) \to (Q \vee R)]$.

  Below is the truth table for this statement's dependency on P, Q, and R:

P	Q	R	$P \wedge Q$	$Q \vee R$	$(P \wedge Q) \to (Q \vee R)$	$\neg[(P \wedge Q) \to (Q \vee R)]$
T	T	T	T	T	T	F
T	T	F	T	T	T	F
T	F	T	F	T	T	F
T	F	F	F	F	T	F
F	T	T	F	T	T	F
F	T	F	F	T	T	F
F	F	T	F	T	T	F
F	F	F	F	F	T	F

September 5 *For each of the following true implications, write out its converse and contrapositive in words (Indicate which is which when you write them). Determine whether the converse is true, and briey justify your determination.*

- *If A is a subset of B, then A is an element of the power set of B.*

  The converse of this statement is "If A is an element of the power set of B, then A is a subset of B." This statement is true, since every element of P(B) is definitionally a subset of B.

  The contrapositive of this statement is "If A is not an element of the power set of B, then A is not a subset of B."

- *If n is an even number larger than 2, then n is not prime.*

  The converse of this statement is "If n is not prime, then n is an even number larger than 2." This is not a generally true statement, as there are several non-prime n which are not even numbers larger than 2. Even if we mandate (which the statement above did not) that n should be a natural number, we still have such counterexamples as the case when n is 9: this satisfies the premise of being nonprime, but it does not satisfy the consequence of being an even number larger than 2.

  The contrapositive of this statement is "If n is prime, then n is not an even number larger than 2."

September 7 *The following statements are slightly modified versions of those in Lewis Carroll's 15th "Premisses for Sortises: Conclusions to be found" from Symbolic Logic. Translate each of*

them into symbolic logic with quantifiers, using the following names for things: let A be the set of ducks, $P(x)$ the proposition "x belongs to Mrs. Bond", $Q(x)$ the proposition "x is branded with a 'B"', $R(x)$ the proposition "x is gray", and $S(x)$ the proposition "x is wearing a lace collar".

- *All ducks branded with a 'B' belong to Mrs. Bond.*

  We could say the same thing as "For any duck x, if x is branded with a 'B', then x belongs to Mrs. Bond.", which, translated into symbols, is $\forall x \in A : Q(x) \to P(x)$.

- *Ducks never wear lace collars, unless they are branded with a 'B'.*

  We could say this as "There is no duck x such that x wears a lace collar and is not branded with a 'B'.", which, translated into symbols, is $\neg[\exists x \in A : S(x) \wedge \neg Q(x)]$. This could be considerably cleaned up by percolating the negation through the existential quantifier, making it universal to get $\forall x \in A : \neg[S(x) \wedge \neg Q(x)]$, which by DeMorgan's Law could also be written $\forall x \in A : [\neg S(x)] \vee Q(x)$, or even more concisely as $\forall x \in A : S(x) \to Q(x)$.

- *Mrs. Bond has no gray ducks.*

  We could say this as "There is no duck x such that x is gray and x belongs to Mrs. Bond.", which, translated into symbols, is $\neg[\exists x \in A : R(x) \wedge P(x)]$. This could be considerably cleaned up by percolating the negation through the existential quantifier, making it universal to get $\forall x \in A : \neg[R(x) \wedge P(x)]$, which by DeMorgan's Law could also be written $\forall x \in A : [\neg R(x)] \vee \neg P(x)$, or even more concisely as $\forall x \in A : R(x) \to \neg P(x)$.

Using the symbolic logic above, what can be said about a gray duck? Justify your assertion.

We might consider an x such that $R(x)$ is true. The third statement above asserts that it is universally true that $R(x) \to \neg P(x)$, so $P(x)$ must be false. By the contrapositive of the first assertion, $\neg P(x) \to \neg Q(x)$ universally, so $Q(x)$ must be false. Finally, the contrapositive of the second assertion is $\neg Q(x) \to \neg S(x)$, so $S(x)$ is false.

Thus, we may assert that a gray duck (one for which $R(x)$ is true) does not belong to Mrs. Bond ($P(x)$ is false), is not branded with a "B" ($Q(x)$ is false), and does not wear a lace collar ($S(x)$ is false).

September 10 *Perform the following steps in order to prove the statement: "The product of two odd numbers is an odd number."*

- *Rephrase this assertion as an implication, giving the unknown quantities names. Identify what part of your rewritten assertion is the premise and what part is the conclusion.*

  We may state the above assertion more explicitly in the following explicit form.

  Proposition 1. *If m and n are odd numbers, then mn is an odd number.*

  Note that in this proposition, the premise (which we may assume is true in the proof of the proposition) is that both m and n are odd numbers; the conclusion is that mn is an odd number.

- *Assume that the premise is true, and use known definitions to convert the premise to an arithmetical statement.*

  For structural-cohesion purposes, the elements associated with both this and the next part are collectively presented as a single proof.

- *Use arithmetic to explore the statement you have derived from your premise, and use a known definition to show that the conclusion follows.*

  Proof. Our premise permits us to assume that m and n are both odd; by the definition of an odd number, there is thus an integer k such that $m = 2k+1$ and an integer ℓ such that $n = 2\ell + 1$. Then, using familiar arithmetic, $mn = (2k+1)(2\ell+1) = 4k\ell + 2k + 2\ell + 1$. Regrouping this last form, it is clear that $mn = 2(2k+k+\ell)+1$. Since k and ℓ are integers, $2k\ell + k + \ell$ is an integer, from which it is then clear that mn is an odd number. □

September 12 *Prove that if a product of two integers is not even, then neither of the two factors are even. You will want to restate the above as an implication and use a contrapositive technique, but be very careful about how you negate things!*

Proposition 2. *For integers m and n, if mn is not even, then neither m nor n is even.*

Proof. We shall demonstrate this proposition by proving its contrapositive, namely, that if either $m$or n is even, then mn is even. Our new premise thus informs us, by the definition of an even number, that either $m = 2k$ for some integer k or $n = 2\ell$ for some integer ℓ. Thus, either $mn = (2k)n = 2(kn)$ or $mn = m(2\ell) = 2(m\ell)$, and in either case it meets the criterion to be an even number. □

September 17 *Prove that if n is an integer, then either $4 \mid n^2$ or $4 \mid (n^2 - 1)$.*

Proposition 3. *If n is an integer, then either $4 \mid n^2$ or $4 \mid (n^2 - 1)$.*

Proof. Since n is an integer, it is either even or odd; we divide into cases on this basis.

Case I: n is even. Then by the definition of an even number, $n = 2k$ for some integer k, so $n^2 = (2k)^2 = 4(k^2)$. Since k^2 is an integer, it follows from the definition of divisibility that $4 \mid n^2$.

Case II: n is odd. Then by the definition of an odd number, $n = 2k + 1$ for some integer k, so $n^2 = (2k+1)^2 = 4k^2 + 4k + 1$. Thus $n^2 - 1 = 4k^2 + 4k = 4(k^2 + k)$. Since $k^2 + k$ is an integer, it follows from the definition of divisibility that $4 \mid (n^2 - 1)$. □

September 19 *Prove that if n, k, a, and b are integers such that $k \mid n$ and $a \equiv b \pmod{n}$, then $a \equiv b \pmod{k}$.*

Proposition 4. *If n, k, a, and b are integers such that $k \mid n$ and $a \equiv b \pmod{n}$, then $a \equiv b \pmod{k}$.*

Proof. By our premises (translating the concept of modular congruence), $k \mid n$ and $n \mid a - b$. By transitivity of divisibility, it thus follows that $k \mid a - b$, so $a \equiv b \pmod{k}$. □

September 21 *Prove that $A \cup B = (A - B) \cup (B - A) \cup (A \cap B)$.*

Proposition 5. *For any sets A and B, $A \cup B = (A - B) \cup (B - A) \cup (A \cap B)$.*

Proof. We shall start by proving that $A \cup B \subseteq (A - B) \cup (B - A) \cup (A \cap B)$. Let us consider some $x \in A \cup B$, so $x \in A$ or $x \in B$. We can divide this possibility into three cases: x might be in exactly one of A or B, or it might be in both.

Case I: $x \in A$ **and** $x \in B$**.** Then it follows that $x \in A \cap B$, so it is true that x is in at least one of the three sets $A - B$, $B - A$, or $A \cap B$, since it is specifically in the third of these. Thus $x \in (A - B) \cup (B - A) \cup (A \cap B)$.

Case II: $x \in A$ **and** $x \notin B$**.** Then it follows that $x \in A - B$, so it is true that x is in at least one of the three sets $A - B$, $B - A$, or $A \cap B$, since it is specifically in the third of these. Thus $x \in (A - B) \cup (B - A) \cup (A \cap B)$.

Case III: $x \in B$ **and** $x \notin A$**.** Then it follows that $x \in B - A$, so proceeding as in the previous two cases we may see that $x \in (A - B) \cup (B - A) \cup (A \cap B)$.

Having proven that $A \cup B \subseteq (A - B) \cup (B - A) \cup (A \cap B)$, we shall proceed to show that $(A-B)\cup(B-A)\cup(A\cap B) \subseteq A\cup B$ to demonstrate equality. Let $y \in (A-B)\cup(B-A)\cup(A\cap B)$. Since y is an element of a union, it is an element of at least one of the three sets participating in the union, and we may consider casewise what can be determined when it is a member of each of them.

Case I: $x \in A - B$**.** Then it follows that $x \in A$ and $x \notin B$. Since $x \in A$, it is certainly true that either $x \in A$ or $x \in B$; thus $x \in A \cup B$.

Case II: $x \in A \cap B$**.** Then it follows that $x \in A$ and $x \in B$. Since $x \in A$, we may proceed as in case I.

Case III: $x \in B - A$**.** Then it follows that $x \notin A$ and $x \in B$. Since $x \in B$, it is certainly true that either $x \in A$ or $x \in B$; thus $x \in A \cup B$. □

September 24 *Prove that there is no smallest positive real number.*

Proposition 6. *There is no smallest positive real number.*

Proof. By way of contradiction, let us assume that there is a smallest positive real number, which we shall call x. Since $0 < \frac{1}{2} < 1$ and $0 < x$, we know via arithmetic that $0 < \frac{1}{2}x < x$; since $\frac{1}{2}x$ is a positive real number which is less than x, our counterfactual premise has been refuted. □

September 26 *Prove that for an irrational number α and a real number x, it is the case that either $\alpha + x$ or $\alpha - x$ is irrational.*

Proposition 7. *If α is an irrational number and x is a real number, then either $\alpha + x$ or $\alpha - x$ is irrational.*

Proof. We shall counterfactually assume that there are irrational α and real x such that $\alpha + x$ and $\alpha - x$ are both rational. Then $(\alpha+x)+(\alpha-x) = 2\alpha$ is rational, and thus so is $\frac{(\alpha+x)+(\alpha-x)}{2} = \alpha$, refuting our premise that α was irrational. □

Note that this proof, with slight changes in wording, could also be phrased as a proof by contrapositive.

September 28 *Disprove and suggest an improvement to this statement: if n is a natural number, then $3 \mid (2n^2 + 1)$.*

A disproof is as easy as finding a value of n for which it is not true, such as 3: $2 \cdot 3^2 + 1 = 19$, which is not divisible by 3. Some experimentation suggests that all the counterexamples are multiples of 3, so a good improvement might be the following proposition:

Proposition 8. *If n is a natural number such that $3 \nmid n$, then $3 \mid (2n^2 + 1)$.*

The following proof emphatically is not required in solution to this problem, but it demonstrates the truth of the statement:

Proof. Let us note that for any three consecutive numbers, one of them must be divisible by 3, so for any natural number n, one of $n-1$, n, or $n+1$ is divisible by 3. Since $3 \nmid n$, it must be the case that $3 \mid n-1$ or $3 \mid n+1$. Thus, no matter which of these is true, $3 \mid (n-1)(n+1)$, or in other words $3 \mid n^2 - 1$; since multiplication by an integer preserves divisibility, $3 \mid 2(n^2 - 1)$, and since $3 \mid 3$, it follows that $3 \mid 2(n^2 - 1) + 3$, or, in other words, $3 \mid 2n^2 + 1$. □

October 1 *Let A, B, and C be sets such that $A \subseteq B \subseteq C$, and let us consider the possible sets S such that $B \cap S = A$ and $B \cup S = C$. It is clear that there is at least one set satisfying this condition, namely, $S = A \cup (C - B)$. Prove that set is unique—i.e. there is no other set S such that $B \cap S = A$ and $B \cup S = C$.*

Proposition 9. *For sets A, B, and C with $A \subseteq B \subseteq C$, there is a unique set S such that $B \cap S = A$ and $B \cup S = C$.*

Proof. It is easy to show that there is at least one such set; if $S = A \cup (C - B)$, then

$$B \cap S = B \cap (A \cup C - B) = (B \cap A) \cup [B \cap (C - B)] = (B \cap A) \cup \emptyset = A$$

with the last equality justified by noting that $A \subseteq B$; likewise

$$B \cup S = B \cup (A \cup C - B) = [B \cup (C - B)] \cup A = C \cup A = C$$

with the last equality justified by noting that $A \subseteq C$.

Now, however, we must show uniqueness (which is all that you were asked to do; student solutions can omit the existence argument above). So we shall suppose that there are sets S and T such that both of them satisfy the given criteria: namely, that $B \cap S = A$, $B \cup S = C$, $B \cap T = A$, and $B \cup T = C$. We shall endeavor to show that S must equal T.

We begin by attempting to show that $S \subseteq T$. Let us consider an arbitrary element x of S. There are two dierent possibilities which we must address, but in both cases we may show that $x \in T$:

Case I: $x \in B$**.** Then, since $x \in S$ and $x \in B$, $x \in B \cap S$, but since $B \cap S = B \cap T$, it follows that $x \in B \cap T$, so $x \in T$.

Case II: $x \notin B$**.** Then, since $x \in S$, $x \in B \cup S$, but since $B \cup S = B \cup T$, it follows that $x \in B \cup T$. However, since x is *not* an element of B, the only way in which it could be an element of $B \cup T$ is if it is an element of T.

Since regardless of an element of S's membership in B, it is an element of T, we have shown that $S \subseteq T$. An identical argument with set names reversed demonstrates that $T \subseteq S$; thus $S = T$. □

October 3 *Prove that for any positive integer n, it is the case that*

$$1 \cdot 2^1 + 2 \cdot 2^2 + 3 \cdot 2^3 + \cdots + n \cdot 2^n = (2n-2)2^n + 2.$$

Proposition 10. *For any positive integer n, it is the case that* $1 \cdot 2^1 + 2 \cdot 2^2 + 3 \cdot 2^3 + \cdots + n \cdot 2^n = (2n-2)2^n + 2$.

Proof. We prove this statement by induction on n. The base case $n = 1$ is easily dispensed with: the one-term sum $1 \cdot 2^1 = 2$, which is indeed equal to $(2 \cdot 1 - 2)2^1 + 2$.

For our inductive step, we shall assume that for a specific value k, it is true that

$$1 \cdot 2^1 + 2 \cdot 2^2 + 3 \cdot 2^3 + \cdots + k \cdot 2^k = (2k-2)2^k + 2,$$

and we shall seek to prove therefrom that

$$1 \cdot 2^1 + 2 \cdot 2^2 + 3 \cdot 2^3 + \cdots + (k+1) \cdot 2^{k+1} = (2(k+1)-2)2^{k+1} + 2.$$

In order to do so, we shall simply use arithmetic, adding the final term $(k+1) \cdot 2^{k+1}$ to the equation provided by our inductive hypothesis:

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

□

October 15 *Let the sequence of values a_n be given by the recurrence relation $a_1 = 2$, $a_2 = 5$, and $a_n = 3a_{n-1} + 4a_{n-2}$ for $n \geq 3$. Using this recurrence, determine the values of a_3 and a_4 (showing your work). Then prove that a_n has the formula $\frac{7 \cdot 4^n - 12(-1)^n}{20}$.*

We calculate a_3 using the known values of a_1 and a_2:

$$a_3 = 3a_2 + 4a_1 = 3 \cdot 5 + 4 \cdot 2 = 23$$

and likewise calculate a_4 using the known value of a_2 and the just-calculated value of a_3:

$$a_4 = 3a_3 + 4a_2 = 3 \cdot 23 + 4 \cdot 5 = 89$$

Proposition 11. *For all positive integers n, $a_n = \frac{7 \cdot 4^n - 12(-1)^n}{20}$.*

Proof. We prove this by induction on n, beginning with the base cases $n = 1$ and $n = 2$:

$$\frac{7 \cdot 4^1 - 12(-1)^1}{20} = 2 = a_1,$$

$$\frac{7 \cdot 4^2 - 12(-1)^2}{20} = 5 = a_2.$$

We proceed to the inductive step, and take as our hypotheses the facts that for a specific $k \geq 3$:

$$a_{k-1} = \frac{7 \cdot 4^{k-1} - 12(-1)^{k-1}}{20}, \quad a_{k-2} = \frac{7 \cdot 4^{k-2} - 12(-1)^{k-2}}{20}$$

and we seek to prove that

$$a_k = \frac{7 \cdot 4^k - 12(-1)^k}{20}$$

To do so, we shall algebraically expand the result of the recurrence, and simplify until we get our desired result:

$$\begin{aligned} a_k &= 3a_{k-1} + 4a_{k-2} \\ &= 3 \cdot \frac{7 \cdot 4^{k-1} - 12(-1)^{k-1}}{20} + 4 \cdot \frac{7 \cdot 4^{k-2} - 12(-1)^{k-2}}{20} \\ &= \frac{21 \cdot 4^{k-1} - 36(-1)^{k-1} + 28 \cdot 4^{k-2} - 48(-1)^{k-2}}{20} \\ &= \frac{\frac{21}{4} \cdot 4^k + 36(-1)^k + \frac{28}{16} \cdot 4^k - 48(-1)^k}{20} \\ &= \frac{7 \cdot 4^k - 12(-1)^k}{20} \end{aligned}$$

□

October 17 *Let $F_1 = 1$, $F_2 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for all $n \geq 3$. Prove that for any positive integer n, F_n is even if and only if n is divisible by 3.*

Proposition 12. *For every positive integer n, F_n is even if and only if n is divisible by 3.*

Proof. We will prove this result by induction on n. For the base cases $n = 1$ and $n = 2$, this result is trivially true: $3 \nmid 1$, and F_1 is not even; likewise, $3 \nmid 2$, and F_2 is not even.

Now, let us fix a value of k, and assume that it is already known for all positive $n \leq k$ that F_n is even if and only if n is divisible by 3. We now want to show that the same parity criterion applies to F_{k+1}. There are two possibilities we should confront with regard to the possible value of $k + 1$, which we specify casewise:

Case I: $k+1$ is divisible by 3. Then neither k nor $k-1$ is divisible by 3, so by our inductive hypothesis, F_k and F_{k-1} will be both odd. Thus, $F_{k+1} = F_k + F_{k-1}$ is the sum of two odd numbers, and is thus even.

Case II: $k+1$ is not divisible by 3. Then, by exactly one of k and $k-1$ is divisible by 3. Thus by our inductive hypothesis, exactly one of F_k and F_{k-1} will be even (and the other will be odd). Thus, $F_{k+1} = F_k + F_{k-1}$ is the sum of an odd and even number, and is thus odd. □

October 19 *For each of the two following relations, determine if they are reflexive, symmetric, and/or transitive. Briefly give reasons for the properties you assert are true; give a counterexample for those which are false.*

- *The relation of "being a proper subset (written with $\subset$ or $\subsetneq$)" on the power set of the natural numbers (example usage: $1,3,4 \subsetneq 1,2,3,4,6$).*

  Since every set is (by definition) not a proper subset of itself, it follows that $\subsetneq$ is not a reflexive relation (it is in fact *antireflexive*). A specific counterexample would be, for instance, the fact that $\emptyset$ is not a proper subset of itself.

  Since $A \subsetneq B$ and $B \subsetneq A$ mean different things, the relation $\subsetneq$ is not symmetric (in fact, the stronger statement that when A is a proper subset of B, B is *not* a proper subset of A is the very polar opposite of symmetry, and is called *antisymmetry*. A specific counterexample would be that $\{1\} \subsetneq \{1,2\}$, but it is not the case that $\{1,2\} \subsetneq \{1\}$.

  It is well known that if $A \subsetneq B$ and $B \subsetneq C$, then $A \subsetneq C$, which is the transitive property; proving this is not difficult, but is outside the scope of a short argument.

- *The relation* R *on the rational numbers given by the criterion that xRy iff either $x = 2y$, $x = y$, or $x = y/2$ (example usage: the relation* 6R3 *is true, since $6 = 2 \cdot 3$, while* 2R7 *is not true, as* 7 *is not equal to* 4, 2, *or* 1*).*

  Since $x = x$, the pair (x, x) meets the second criterion for being included in the relation R; thus xRx for all rational x and R is thus reflexive.

  If xRy, then either $x = y$, $x = 2y$, or $x = \frac{y}{2}$. In these three cases, it would also be true that $y = x$, $y = \frac{x}{2}$, or $y = 2x$ respecively; in each case a criterion for satisfying yRx is met, so since xRy implies yRx, the relation is symmetric.

  This relation is not transitive, and a simple counterexample suffices: it is true that 1R2 and 2R4, but it is not true that 1R4.

October 22 *Let the relation* R *on the set* $1, 2, 3, ..., 100$ *be defined by making xRy iff $\lfloor \frac{x}{3} \rfloor = \lfloor \frac{y}{3} \rfloor$ (note that the "floor function" $\lfloor z \rfloor$ is the value of z rounded down to the next integer). Prove that* R *is an equivalence relation, and describe its equivalence classes.*

Proposition 13. *The relation* R *is an equivalence relation.*

Proof. It is always true that $\lfloor \frac{x}{3} \rfloor = \lfloor \frac{x}{3} \rfloor$ (by reflexivity of equality, actually), so xRx.

Given x and y such that xRy, it follows that $\lfloor \frac{x}{3} \rfloor = \lfloor \frac{y}{3} \rfloor$; symmetry of equality allows us to rewrite this as $\lfloor \frac{y}{3} \rfloor = \lfloor \frac{x}{3} \rfloor$, so yRx.

Finally, if x, y, and z are values such that xRy and yRz, the definition of the relation tells us that $\lfloor \frac{x}{3} \rfloor = \lfloor \frac{y}{3} \rfloor$ and $\lfloor \frac{y}{3} \rfloor = \lfloor \frac{z}{3} \rfloor$; by transitivity of equality we then know that $\lfloor \frac{x}{3} \rfloor = \lfloor \frac{z}{3} \rfloor$, and thus xRz.

Since all three properties of equivalence relations are satisfied, R is an equivalence relation. □

In determining equivalence classes, we can note that

$$\begin{aligned}\left\lfloor \frac{1}{3} \right\rfloor = \left\lfloor \frac{2}{3} \right\rfloor &= 0 \\ \left\lfloor \frac{3}{3} \right\rfloor = \left\lfloor \frac{4}{3} \right\rfloor = \left\lfloor \frac{5}{3} \right\rfloor &= 1 \\ \left\lfloor \frac{6}{3} \right\rfloor = \left\lfloor \frac{7}{3} \right\rfloor = \left\lfloor \frac{8}{3} \right\rfloor &= 2 \\ \left\lfloor \frac{9}{3} \right\rfloor = \left\lfloor \frac{10}{3} \right\rfloor = \left\lfloor \frac{11}{3} \right\rfloor &= 1 \\ &\vdots \\ \left\lfloor \frac{99}{3} \right\rfloor = \left\lfloor \frac{100}{3} \right\rfloor &= 33\end{aligned}$$

so $\{1, 2, 3, \ldots, 100\}$ is divided into 34 equivalence classes: $\{1, 2\}$, $\{3, 4, 5\}$, $\{6, 7, 8\}$, and so forth.

October 24 *Write multiplication tables for $\mathbb{Z}_6$ and $\mathbb{Z}_7$. Determine which elements of $\mathbb{Z}_6$ and $\mathbb{Z}_7$ it makes sense to consider "dividing by".*

Here is the multiplication table for $\mathbb{Z}_6$:

$\mathbb{Z}_6, \cdot$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

As we can see, the rows associated with [0], [2], [3], and [4] all make division problematic, since several products appear multiple times in those rows, and other products appear not at all. The rows associated with [1] and [5] do have every product appearing exactly once, indicating that divisibility is possible; note that these division rules are completely trivial and unsurprising: $\frac{[x]}{[1]} = [x]$, and $\frac{[x]}{[5]} = \frac{[x]}{[-1]} = [-x]$.

$\mathbb{Z}_7, \cdot$	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[0]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[0]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[0]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[0]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[0]	[6]	[5]	[4]	[3]	[2]	[1]

Here every row except for [0] has one representative from each congruence class appearing among its possible products; thus any congruence class except for [0] can be the denominator

of a division. While division by [1] and [6] are, as explained previously, identical to an identity operation and a negation, the other divisions are a bit less intuitive: $\frac{[x]}{[2]} = [4x]$, $\frac{[x]}{[3]} = [5x]$, $\frac{[x]}{[4]} = [2x]$, and $\frac{[x]}{[5]} = [3x]$.

October 26 *For each of the following three functions from $\mathbb{R}$ to $\mathbb{R}$, determine, with a brief justification, whether it is injective but not surjective, surjective but not injective, neither surjective nor injective, or both surjective and injective:*

- *The function f determined by the rule $f(x) = 2x^3$.*
  This function is injective, since it is increasing throughout, so if $x < y$, $2x^3 < 2y^3$, so unequal x and y never yield equal $f(x)$ and $f(y)$.
  This function is also surjective, since for every possible value y in the codomain, $f(\sqrt[3]{y}) = y$.
- *The function g determined by the rule $g(x) = x^2 - 3$.*
  This function is not injective, since $g(1) = g(-1) = -2$.
  This function is not surjective, since there is no element x of $\mathbb{R}$ such that $g(x) = -4$ (such a number would need to have a square of -1, which no real number has).
- *The function h determined by the rule $h(x) = e^x$.*
  This function is injective, since it is increasing throughout, so if $x < y$, $e^x < e^y$, so unequal x and y never yield equal $h(x)$ and $h(y)$.
  This function is not surjective, since e^x is always positive, so there is no x such that $h(x) = 0$.

The above three functions fit into three of the four categories given above. Find a function from $\mathbb{R}$ to $\mathbb{R}$ fitting into the fourth category (or assert that it is impossible), and justify your claim.

We know that what we want here is a surjective function which is not injective. There are several such, mostly rather contrived. One good example might be $q(x) = x^3 - x$; here $q(-1) = q(0) = q(1) = 0$, so it is manifestly not injective, but since it is a continuous function that increases and decreases without bound, it achieves every possible real value by the Intermediate Value Theorem. Other example functions include $\ln|x|$ and $x + |x - 1| - |x + 1|$.

October 29 *For a finite set A, we have known since early in the course that $\mathcal{P}(A)$ has $2^{|A|}$ elements. Note that the set of functions $\{0,1\}^A$ also has $2^{|A|}$ elements. Describe a straightforward correspondance between functions from A to $\{0,1\}$ and subsets of A. Does this correspondence still make sense if A is infinite?*

An easy correspondence is as such: for a function $f : A \to \{0,1\}$, we can define a set $S \subseteq A$ as such: $S = \{x \in A : f(x) = 1\}$ — which is to say, values where f evaluates to 1 are interpreted as "in the set", while values where f evaluates to 0 are interpreted as "out of the set". Conversely, we could build a function from a stated set: given $S \subseteq A$, we could build f by the definition $f(x) = \begin{cases} 1 \text{ if } x \in S \\ 0 \text{ if } x \notin S \end{cases}$.

To illustrate this correspondence, here is an example of how each of the eight functions in

$\{0,1\}^{\{a,b,c\}}$ could be mapped to the eight elements of $\mathcal{P}(\{a,b,c\})$:

$$\begin{aligned}
\{(a,0),(b,0),(c,0)\} &\mapsto \emptyset \\
\{(a,0),(b,0),(c,1)\} &\mapsto \{c\} \\
\{(a,0),(b,1),(c,0)\} &\mapsto \{b\} \\
\{(a,0),(b,1),(c,1)\} &\mapsto \{b,c\} \\
\{(a,1),(b,0),(c,0)\} &\mapsto \{a\} \\
\{(a,1),(b,0),(c,1)\} &\mapsto \{a,c\} \\
\{(a,1),(b,1),(c,0)\} &\mapsto \{a,b\} \\
\{(a,1),(b,1),(c,1)\} &\mapsto \{a,b,c\}
\end{aligned}$$

Note that this same correspondence—if not the enumerative result—would actually work just as well if A were infinite. For instance, if $A = \mathbb{R}$, we might associate such members of $\mathcal{P}(\mathbb{R})$ as $\mathbb{Z}$, $\mathbb{Q}$, and $[0,1]$ respectively with a function which evaluates to 1 at integers and 0 at nonintegers, a function which evaluates to 1 at rationals and 0 at irrationals, and a function which evaluates to 1 at numbers between 0 and 1 inclusive and 0 elsewhere.

October 31 *Given an injection $f : A \to B$ where A is nonempty, explain how a surjection $g : B \to A$ could be constructed. For $a \in A$, is it generally true that $g(f(a)) = a$? For $b \in B$, is it generally true that $f(g(b)) = b$?*

If $f : A \to B$ is an injection, then we know that each element of B is the image of *at most* one element of A under the function f. Thus, each element of B is either the image of a unique element of A, or of no element of A. We may define a function $g : B \to A$ as a sort of pseudo-inverse by choosing an arbitrary element a_0 of A and proceeding as such: if $f(a) = b$, then $g(b) = a$; if there is *no* a such that $f(a) = b$, then let $g(b) = a_0$.

By construction, for each $a \in A$, it is true that $g(f(a)) = a$; this will demonstrate surjectivity of g, since every element of A is the image of some element of B — specifically, a is the image under g of $f(a)$. However, it is *not* generally true that $f(g(b)) = b$, because if b is not the image of any element of a, then $f(g(b)) = f(a_0) \neq b$.

November 2 *We saw on the very first PotD that if A and B are finite with $A \subseteq B$, it is true that $|A| \leq |B|$. Prove that it's true for* all *sets — not just the finite ones!*

Let $f : A \to B$ be the trivial function given by $f(x) = x$ (since each $x \in A$ is an element of B, this works with the given codomain). Clearly f is an injection, since if $x \neq y$, then $f(x) = x \neq y = f(y)$. Thus, since there is an injection from A to B, $|A| \leq |B|$.

November 5 *Construct (and describe) a bijection f between the set of natural numbers $\mathbb{N}$ and the set of ordered pairs of natural numbers $\mathbb{N}^2$ (hint: you can use a geometric intuition; try to associate each lattice point in the first quadrant of the coordinate plane with a different integer). Illustrate that your construction works by specifically calculating, as an example, $f(15)$ and $f^{-1}((5,4))$ (i.e. find which natural number n gives $f(n) = (5,4)$.). What does your construction tell you about the comparative number of elements in $\mathbb{N}$ and $\mathbb{N}^2$?*

There are several ways to do this, but the easiest way to do it is by snaking along diagonals from the lower left corner out, e.g. associate $(1,1)$, on the lower left corner, with 1, then associate the points on the next diagonal out, $(1,2)$ and $(2,1)$ respectively with 2 and 3, and

then $(1,3)$, $(2,2)$, and $(3,1)$ respectively with 4, 5, and 6, and so forth. Using this scheme, $(5,1)$ would be associated with 15, so $f(15) = (5,1)$; likewise, $(5,4)$ would be associated with 33, so $f^{-1}((5,4)) = 33$. Different approaches are possible, but most of them involve some sourt of crawling outwards from the lower left corner of $\mathbb{N}^2$.

November 7 *Prove that for (not necessarily finite!) sets A, B, C, and D, if $|A| \leq |C|$ and $|B| \leq |D|$, then $|A \times B| \leq |C \times D|$.*

Since $|A| \leq |C|$ and $|B| \leq |D|$, there are injections $f : A \to C$ and $g : B \to D$. Let the function $H : A \times B \to C \times D$ be given by $h((a,b)) = (f(a), g(b))$. We shall show that h is injective (and thus that $|A \times B| \leq |C \times D|$): suppose there are some elements (a,b) and (a',b') of $A \times B$ such that $h((a,b)) = h((a',b'))$. Since $h((a,b)) = (f(a), g(b))$ and $h((a',b')) = (f(a'), g(b'))$; since these ordered pairs must be equal, their individual coordinates must be equal, so $f(a) = f(a')$ and $g(b) = g(b')$. By injectivity of f and g, it thus follows that $a = a'$ and $b = b'$, so $(a,b) = (a',b')$, demonstrating injectivity of h.

November 12 *A "phrase" is a finite sequence consisting of any of the 26 English letters and spaces. So, for instance, "i like pie" is a phrase, as is "this phrase has several consecutive spaces". Prove (most easily done by describing a procedure which lists every single phrase) that the number of phrases is countably infinite.*

Let us simply consider a space as a single letter. We can list all the possible phrases by wrting all 27 one-letter phrases in order: "a", "b", ..., "z", " ", then writing all 27^2 two-letter phrases in order: "aa", "ab", ..., "az", "a ", "ba", "bb", ..., " ", and so forth with each finite length in turn. This procedure would eventually list every single finite sequence.

November 14 *Let A be an uncountable set and B be a countable set. Prove that $A - B$ is uncountable.*

Suppose, contrariwise, that A is uncountable, B is countable, and $A - B$ is *not* uncountable — i.e., $A - B$ is countable. Then, since $A - B$ and B are both countable, their union, $(A - B) \cup B$ is countable. However, since $(A - B) \cup B = A$, it follows that A is countable, which contradicts the premise that A is uncountable.

November 26 *Let "1-3-4" Nim be a traditional Nim game in which there is a single pile of objects (stones or pennies or whatnot) and each player takes away 1, 3, or 4 objects on their turn. The player who removes the last object wins. Explore several small games of 1-3-4 Nim and determine which states one can win from; conjecture a general-winning-state criterion and prove it.*

As in every traditional nim, 0 is definitionally a losing state. 1 is a winning state since removal of a single object wins the game. 2 is a losing state since the only legal move is to remove one object, giving the opponent the winning state 1. 3 is a winning state since removal of three objects wins the game; likewise 4 is a winning state since removal of four objects wins the game. 5 and 6 are winning states since removal of three or four objects respectively furnishes the opponent with the losing state 2. 7 is a losing state since the three possible moves leave the opponent with states 6, 4, and 3, all of which are winning. Continuing in this fashion, a pattern should become apparent: states congruent to 0 or 2 modulo 7 are losing and all others are winning. We can prove this.

Proposition 14. *In "1-3-4" nim, a state is winning if and only if it is not congruent to 0 or 2 modulo 7.*

Proof. We prove this result by induction on the state n. The base cases up through $n = 4$ are amply demonstrated by the above investigation. Now we shall show that some specific k satisfies the given winning-state criterion, using the inductive hypothesis that all values smaller than k satisfy this winning criterion. We could divide into seven cases based on the seven congruence classes, but need not be quite so explicit; instead, we might divide into major cases based on whether k is congruent to 0, 2, or neither.

Case I: $k \equiv 0 \pmod 7$**.** From this state, the three possible moves furnish the opponent with one of the states $k-1$, $k-3$, or $k-4$. All three of these are less than k, and they are respectively congruent to 6, 4, and 3 modulo 7, so by our inductive hypothesis all three are winning states; since every move furnishes the opponent with a winning state, the state k is losing.

Case II: $k \equiv 2 \pmod 7$**.** From this state, the three possible moves furnish the opponent with one of the states $k-1$, $k-3$, or $k-4$. All three of these are less than k, and they are respectively congruent to 1, 6, and 5 modulo 7, so by our inductive hypothesis all three are winning states; since every move furnishes the opponent with a winning state, the state k is losing.

Case III: $k \not\equiv 0, 2 \pmod 7$**.** Since there are only 7 congruence classes, we know that k is congruent to 1, 3, 4, 5, or 6 modulo 7. In each of these cases there is a move such that the opponent is in a losing position: if $k \equiv 1 \pmod 7$, then $k - 1 \equiv 0 \pmod 7$; if $k \equiv 3 \pmod 7$, then $k - 1 \equiv 2 \pmod 7$; if $k \equiv 4 \pmod 7$, then $k - 4 \equiv 0 \pmod 7$; if $k \equiv 5 \pmod 7$, then $k-3 \equiv 2 \pmod 7$; and if $k \equiv 6 \pmod 7$, then $k-4 \equiv 2 \pmod 7$. By the inductive hypothesis, the given resulting states from these moves are losing for the opponent. □

November 28 *Here let $\oplus$ represent the Nimsum described in class. Prove that if $N = a_1 \oplus a_2 \oplus \cdots \oplus a_n$, then $(a_1 \oplus N) \oplus a_2 \oplus \cdots \oplus a_n = 0$. You may use the following universally true facts without proof: $a \oplus b = b \oplus a$, $(a \oplus b) \oplus c = a \oplus (b \oplus c)$, $a \oplus 0 = a$, and $a \oplus a = 0$.*