21-127 Final Exam Practice Problems Solutions

Mary Radcliffe

1 Logic and Proof Techniques

1. Let p, q be logical propositions. Prove that $(\neg(p \wedge q)) \wedge (p \vee q)$ is logically equivalent to $(p \wedge \neg q) \vee (q \wedge \neg p)$.

   Solution:

$$\begin{aligned}
(\neg(p \wedge q)) \wedge (p \vee q) &\equiv (\neg p \vee \neg q) \wedge (p \vee q) \qquad \text{(by De Morgan's Laws)}\\
&\equiv [(\neg p \vee \neg q) \wedge p] \vee [(\neg p \vee \neg q) \wedge q] \qquad \text{(by distributivity)}\\
&\equiv (\neg p \wedge p) \vee (\neg q \wedge p) \vee (\neg p \wedge q) \vee (\neg q \wedge q) \qquad \text{(by distributivity)}\\
&\equiv (\neg q \wedge p) \vee (\neg p \wedge q) \qquad \text{(since } \neg p \wedge p \text{ and } \neg q \wedge q \text{ are false)}
\end{aligned}$$

2. Prove that $\sqrt{p}$ is irrational for any prime $p > 0$.

   Solution: Suppose, to the contrary, that $\sqrt{p}$ is rational. Write $\sqrt{p} = \frac{a}{b}$ for $a, b \in \mathbb{Z}$ where a and b share no factors. Then $p = \frac{a^2}{b^2}$, and hence $pb^2 = a^2$. Since p is prime and $p|a^2$, we must have $p|a$, and hence there exists $k \in \mathbb{Z}$ with $a = pk$. Thus, $pb^2 = p^2k^2$, and hence $b^2 = pk^2$. As above, $p|b$, and hence a and b share the factor p. This is a contradiction, since it was assumed that a and b share no factors. Therefore, $\sqrt{p}$ is irrational.

3. Find the smallest $n > 0$ such that $n!$ is divisible by 990.

   Solution: Note, $990 = 2 * 5 * 9 * 11$. We claim that the smallest $n > 0$ having $n!$ divisible by 990 is $n = 11$. Note, indeed, that $11!$ is divisible by 990, as $11! = 1*2*3*4*5*6*7*8*9*10*11 = (2*5*9*11)*3*4*6*7*8*10$, and is thus divisible by 990. Moreover, if $n < 11$, then $n!$ is not divisible by 11, since 11 is prime. Therefore, if $n < 11$, then $n!$ is not divisible by 990.

4. Let p and q be logical propositions.

   (a) Prove that $p \Rightarrow q$ is logically equivalent to $\neg q \Rightarrow \neg p$.

   (b) Explain in words why the above statement makes sense.

   Solution:

   (a) Consider:

$$\begin{aligned}
p \Rightarrow q &\equiv \neg p \vee q\\
&\equiv \neg(\neg q) \vee \neg p\\
&\equiv \neg q \Rightarrow \neg p.
\end{aligned}$$

(b) The statement $p \Rightarrow q$ means that if p is true, we must also have q to be true. That means if we know q is not true, we can't have p to be true either, since p being true would force q to be true. Thus, if $p \Rightarrow q$ is true, it must also be that $\neg q \Rightarrow \neg p$ is true.

5. Let p, q, r be logical propositions. Prove that

$$[p \Rightarrow (q \Rightarrow r)] \Rightarrow [(p \Rightarrow q) \Rightarrow (p \Rightarrow r)]$$

is tautologically true (that is, it is true regardless of the truth values of p, q, r).

Solution: Consider:

$$\begin{aligned}
[p \Rightarrow (q \Rightarrow r)] \Rightarrow [(p \Rightarrow q) \Rightarrow (p \Rightarrow r)] &\equiv [p \Rightarrow (\neg q \vee r)] \Rightarrow [(\neg p \vee q) \Rightarrow (\neg p \vee r)] \\
&\equiv \neg p \vee (\neg q \vee r) \Rightarrow \neg(\neg p \vee q) \vee (\neg p \vee r) \\
&\equiv \neg(\neg p \vee (\neg q \vee r)) \vee (p \wedge \neg q) \vee (\neg p \vee r) \\
&\equiv [p \wedge (q \wedge \neg r)] \vee (p \wedge \neg q) \vee (\neg p \vee r).
\end{aligned}$$

Note, if the first term is true, then we have p is true, q is true, and r is false. If it is not, then we have three cases:

Case 1: r is true. Then $\neg p \vee r$ is true, and the statement is true.

Case 2: p is false. Then $\neg p \vee r$ is true, and the statement is true.

Case 3: q is false. If p is also false, then see Case 2. If p is true, then $p \wedge \neg q$ is true, and the statement is true.

Hence, in any case, the statement is true. Therefore, it is a tautology.

2 Induction

1. Use induction to prove that $\sum_{i=1}^{k}(2i-1) = k^2$.

Solution: We work by induction on k.
For the base case, consider $k = 1$. Then we have $\sum_{i=1}^{k}(2i-1) = 2 * 1 - 1 = 1 = 1^2$, and the result holds.
Now, suppose that for some $k \in \mathbb{N}$, we have $\sum_{i=1}^{k}(2i-1) = k^2$. Then

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

Therefore, the result holds by induction.

2. Let $n \in \mathbb{N}$ be written, in base 10, as $111 \cdots 11$, where there are 3^k 1s in the base expansion. Prove that n is divisible by 3^k.

   Solution: We work by induction on k. If $k = 1$, then we have $n = 111 = 3 * 37$, so n is divisible by 3^k.

   Now, suppose that for some $k \in \mathbb{N}$, if $n = 111 \cdots 11$ with 3^k 1s in the expansion, then n is divisible by 3^k. Write $n = 3^k t$ for $t \in \mathbb{Z}$.

   Consider $m = 111 \cdots 111$, having 3^{k+1} 1's in its expansion. Note that this is precisely 3 times as many 1s as in the expansion for n, and so we can think of the base expansion for m as the concatenation of 3 copies of that of m. In particular, we can write $m = n + 10^{3^k} n + 10^{3^k+3^k} n$, where in the second term the coefficient 10^{3^k} moves the copy of n over 3^k positions, and in the third term the coefficient $10^{3^k+3^k}$ moves the copy of n over 3^k positions, twice. Thus, we can write $m = n(1 + 10^{3^k} + 10^{3^k+3^k})$. Note that $1 + 10^{3^k} + 10^{3^k+3^k}$ has a base expansion containing exactly 3 1s, and hence it is divisible by 3, as the sum of the base 10 digits is 3. Therefore, there is some $s \in \mathbb{Z}$ with $1 + 10^{3^k} + 10^{3^k+3^k} = 3s$. Thus, $m = n(1 + 10^{3^k} + 10^{3^k+3^k}) = 3^k t 3s = 3^{k+1} st$, and thus m is divisible by 3^{k+1}.

   Hence, the result holds by induction on k.

3. Suppose you draw n straight lines in the plane, where no two lines are parallel and no three lines meet at a point. How many regions have you divided the plane into? Prove that your answer is correct.

   Solution: This process divides the plane into $\frac{n(n+1)}{2}+1$ regions. We prove this by induction on n.

   First, suppose that $n = 0$. Then there are no lines, and one region. Moreover, $\frac{n(n+1)}{2}+1 = 0+1 = 1$, so the formula is true.

   Now, suppose that for some $n \in \mathbb{N}$, it is known that drawing n such lines in the plane divides the plane into $\frac{n(n+1)}{2}+1$ regions.

   Suppose we draw $n+1$ such lines. Note that first, we draw n lines, so that we have $\frac{n(n+1)}{2}+1$ regions before the $(n+1)^{\text{st}}$ line is drawn. Now, this new line must cross each of the existing n lines. Each time it does so, it enters a region and divides it in half. Hence, it starts in one region (dividing it in two), and enters and cuts n additional regions, one each time it crosses an existing line. Thus, the $(n+1)^{\text{st}}$ line adds $n+1$ additional regions. We therefore have that with $n+1$ lines, we obtain

   $$\frac{n(n+1)}{2}+1+n+1 = (n+1)\left(\frac{n}{2}+1\right)+1 = \frac{(n+1)(n+2)}{2}+1$$

   regions in the plane.

   Therefore, the result holds by induction.

4. Define a sequence by $a_0 = 0$, $a_1 = 1$, and $a_n = 3a_{n-1} - 2a_{n-2}$ for $n \geq 2$. Derive and prove a nonrecursive formula for a_n.

Solution: Let us consider some terms.

$$\begin{aligned}
a_0 &= 0\\
a_1 &= 1\\
a_2 &= 3a_1 - 2a_0 = 3 * 1 - 0 = 3\\
a_3 &= 3a_2 - 2a_1 = 3 * 3 - 2 * 1 = 7\\
a_4 &= 3a_3 - 2a_1 = 3 * 7 - 2 * 3 = 21 - 6 = 15
\end{aligned}$$

We conjecture that $a_n = 2^n - 1$. Let's prove this with induction. Note that for $n = 0$ and $n = 1$, we have $a_n = 2^n - 1$ is true.

Suppose for some $n \in \mathbb{N}$ that $a_k = 2^k - 1$ for every $k \leq n$.

Consider

$$\begin{aligned}
a_{n+1} &= 3a_n - 2a_{n-1}\\
&= 3(2^n - 1) - 2(2^{n-1} - 1) && \text{(by the inductive hypothesis)}\\
&= 3 * 2^n - 3 - 2^n + 2\\
&= 2^n(3 - 1) - 1\\
&= 2^{n+1} - 1.
\end{aligned}$$

Therefore, the result holds for all $n \in \mathbb{N}$ by induction.

5. Prove that for $x_1, x_2, \ldots, x_n \in \mathbb{R}$, with $x_i \geq 0$ for all i,

$$\frac{x_1 + x_2 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 x_2 \ldots x_n}.$$

Solution: Let's work by induction on n. For $n = 1$, we have $\frac{x_1+x_2+\cdots+x_n}{n} = x_1$ and $\sqrt[n]{x_1 x_2 \ldots x_n} = \sqrt[1]{x_1} = x_1$, and hence the result is true, since we obtain equality.

Suppose that for some $n \in \mathbb{N}$, we have $\frac{x_1+x_2+\cdots+x_n}{n} \geq \sqrt[n]{x_1 x_2 \ldots x_n}$ for any nonnegative $x_i \in \mathbb{R}$.

Let $x_1, x_2, \ldots, x_{n+1}$ be nonnegative real numbers. Put

$$m = \frac{x_1 + x_2 + \cdots + x_{n+1}}{n + 1}.$$

First note that if $x_i = m$ for all i, then the result is immediate, since both the right and left hand sides equal m. If not all $x_i = m$, then since m is the average of the x_i, there exists some i with $x_i > m$ and there exists some j with $x_j < m$. Wolog, suppose that these are x_n and x_{n+1}, respectively.
Set $y_1 = x_1, y_2 = x_2, \ldots, y_{n-1} = x_{n-1}, y_n = x_n + x_{n+1} - m$. Then by the inductive hypothesis, we have that

$$\frac{y_1 + y_2 + \cdots + y_n}{n} \geq \sqrt[n]{y_1 y_2 \ldots y_n}.$$

We first note that

$$\begin{aligned}\frac{y_1+y_2+\cdots+y_n}{n} &= \frac{x_1+x_2+\cdots+x_{n-1}+x_n+x_{n+1}-m}{n}\\ &= \frac{(n+1)m-m}{n}\\ &= m.\end{aligned}$$

We next note that

$$\begin{aligned}x_1x_2\ldots x_{n-1}(x_n+x_{n+1}-m) &= y_1y_2\ldots y_n\\ &\leq \left(\frac{y_1+y_2+\cdots+y_n}{n}\right)^n \qquad \text{(by the inductive hypothesis)}\\ &= m^n.\end{aligned}$$

Therefore, we have

$$\begin{aligned}\left(\frac{x_1+x_2+\cdots+x_n+x_{n+1}}{n+1}\right)^{n+1} &= m^{n+1}\\ &= m^n m\\ &\geq x_1x_2\ldots x_{n-1}(x_n+x_{n+1}-m)m.\end{aligned}$$

Finally, consider $(x_n+x_{n+1}-m)m-x_nx_{n+1}=(x_n-m)(m-x_{n+1})$. Note that by our wolog above, we have $x_n-m>0$ and $m-x_{n+1}>0$, so this is positive. Therefore, $(x_n+x_{n+1}-m)m-x_nx_{n+1}>0 \Rightarrow (x_n+x_{n+1}-m)m>x_nx_{n+1}$. Making this substitution, then, we have

$$\left(\frac{x_1+x_2+\cdots+x_n+x_{n+1}}{n+1}\right)^{n+1} > x_1x_2\ldots x_{n-1}x_nx_{n+1}.$$

Raising both sides to the $\frac{1}{n+1}$ power yields the result.

6. Let $k\in\mathbb{N}$, with $k\neq 0$. Prove that $k(k+1)(k+2)$ is divisible by 3.

Solution: If $k=1$, then $k(k+1)(k+2)=1(2)(3)=6$ which is divisible by 3.
Suppose that for some $k\in\mathbb{N}$, we have $k(k+1)(k+2)$ is divisible by 3. Write $k(k+1)(k+2)=3t$ for some $t\in\mathbb{Z}$.
Consider

$$\begin{aligned}(k+1)(k+2)(k+3) &= (k+1)(k+2)k+(k+1)(k+2)3\\ &= 3t+3(k+1)(k+2) \qquad \text{(by the inductive hypothesis)}\\ &= 3(t+(k+1)(k+2)).\end{aligned}$$

Therefore, $(k+1)(k+2)(k+3)$ is also divisible by 3.

Thus, by induction, the result holds for all $k\in\mathbb{N}$.

3 Set Theory and functions

1. Let $U_1, U_2, \ldots, U_k$ be a finite partition of a set X, and let $A \subseteq X$. Prove that $A = \bigcup_{i=1}^{k}(A \cap U_i)$.

   Solution: We work by induction on k. If $k = 1$, then $U_1 = X$ and $A = A \cap X = A \cap U_1$ is true.

   Suppose, now, that if $U_1, U_2, \ldots, U_k$ is a finite partition of X and $A \subseteq X$, then $A = \bigcup_{i=1}^{k}(A \cap U_i)$.
   Let $V_1, V_2, \ldots, V_{k+1}$ be a finite partition of X, and set $A \subseteq X$. Set $U_1 = V_1, U_2 = V_2, \ldots, U_{k-1} = V_{k-1}$, and $U_k = V_k \cup V_{k+1}$. Then $U_1, U_2, \ldots, U_k$ is also a finite partition of X, and by the inductive hypothesis we have

   $$A = \bigcup_{i=1}^{k}(A \cap U_i).$$

   Therefore,

   $$\begin{aligned} A &= \bigcup_{i=1}^{k}(A \cap U_i) \\ &= \left[\bigcup_{i=1}^{k-1}(A \cap U_i)\right] \cup (A \cap U_k) \\ &= \left[\bigcup_{i=1}^{k-1}(A \cap U_i)\right] \cup (A \cap (V_k \cup V_{k-1})) \\ &= \left[\bigcup_{i=1}^{k-1}(A \cap U_i)\right] \cup (A \cap V_k) \cup (A \cap V_{k-1})) \qquad \text{(by distributivity)} \\ &= \bigcup_{i=1}^{k+1}(A \cap V_i) \end{aligned}$$

   Therefore, the result holds for all k by induction.

2. Let X and Y be sets. Prove that $X \subseteq Y$ if and only if $X = Y \backslash (Y \backslash X)$.

   Solution:
   ($\Rightarrow$) Suppose that $X \subseteq Y$. Then $x \in X$ implies $x \in Y$ and $x \notin Y \backslash X$, and hence $x \in Y \backslash (Y \backslash X)$. Likewise, if $x \in Y \backslash (Y \backslash X)$, then $x \in Y$ and $x \notin Y \backslash X$, so $x \in X$. Therefore, $X = Y \backslash (Y \backslash X)$.
   ($\Leftarrow$) Suppose that $X = Y \backslash (Y \backslash X)$. Then $x \in X \Rightarrow x \in Y \backslash (Y \backslash X)$, so in particular, $x \in Y$. Therefore, $X \subseteq Y$.

3. Define a function $f : \mathbb{R} \to \mathbb{R}$ by the following: for every $a \in \mathbb{R}$, let $f(a) = x$, where $x^2 + 2ax + a^2 = 0$. Prove that this function is well-defined.

   Solution: In order to prove that this function is well-defined, we must show that for each $a \in \mathbb{R}$, there is a unique choice of $x \in \mathbb{R}$ satisfying $x^2 + 2ax + a^2 = 0$. Note, however, that

$x^2 + 2ax + a^2 = (x+a)^2$, and hence $x^2 + 2ax + a^2 = 0$ if and only if $x = -a$. Therefore, for all $a \in \mathbb{R}$, $\exists! x \in \mathbb{R}$ such that $f(a) = x$, and therefore f is well-defined.

4. Let X and Y be sets, and let $f : X \to Y$ be a function.

   (a) For $A, B \subseteq X$, prove that $f(A \cup B) = f(A) \cup f(B)$.

   (b) For $A, B \subseteq X$, prove that $f(A \cap B) \subseteq f(A) \cap f(B)$, but that sometimes these sets may not be equal.

   Solution:

   (a) Let $A, B \subseteq X$. Suppose $y \in f(A \cup B)$. Then there exists $x \in A \cup B$ with $f(x) = y$. If $x \in A$, then $y = f(x) \in f(A) \Rightarrow y \in f(A) \cup f(B)$. Likewise, if $x \in B$, then $y \in f(A) \cup f(B)$. Therefore, $f(A \cup B) \subseteq f(A) \cup f(B)$.

   On the other hand, suppose that $y \in f(A) \cup f(B)$. Then y is in at least one of $f(A)$ or $f(B)$; suppose wolog that $y \in f(A)$. Then $\exists x \in A$ with $f(x) = y$. Since $x \in A$, we also have $x \in A \cup B$, and hence $y = f(x) \in f(A \cup B)$. Therefore, $f(A) \cup f(B) \subseteq f(A \cup B)$.

   Combining these two containments, we obtain $f(A \cup B) = f(A) \cup f(B)$.

   (b) Let $A, B \subseteq X$. Suppose $y \in f(A \cap B)$. Then there exists $x \in A \cap B$ having $f(x) = y$. Since $x \in A \cap B$, we have $x \in A$ and $x \in B$. Thus, $y = f(x) \in f(A)$ and $y = f(x) \in f(B)$, so $y \in f(A) \cap f(B)$.

   However, these sets may not be equal. Consider, for example $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = n^2$. Put $A = \{1\}$ and $B = \{-1\}$. Then $f(A) = \{1\} = f(B)$, so $f(A) \cap f(B) = \{1\}$. However, $A \cap B = \emptyset$, and thus $f(A \cap B) = \emptyset$. Therefore, $f(A \cap B) \neq f(A) \cap f(B)$.

5. Let $f : X \to Y$ be a function. Prove that f is injective if and only if $f(A \backslash B) = f(A) \backslash f(B)$ for every $A, B \subseteq X$.

   Solution: First, suppose that f is injective, and let $A, B \subseteq X$. Then

$$\begin{aligned} y \in f(A\backslash B) &\Leftrightarrow \exists x \in A\backslash B \text{ with } f(x) = y \\ &\Leftrightarrow y = f(x) \in f(A) \text{ and } y = f(x) \notin f(B) \qquad (**) \\ &\Leftrightarrow y \in f(A)\backslash f(B). \end{aligned}$$

   where line $(**)$ follows since by injectivity no other x-value can output y under f.

   Therefore, the forward direction is true.

   For the converse, suppose that f is not injective. Then there exist $x_1, x_2 \in X$ with $x_1 \neq x_2$ and $f(x_1) = f(x_2) = y$. Put $A = \{x_1, x_2\}$ and $B = \{x_2\}$. Then $f(A) = f(B) = \{y\}$, and $f(A\backslash B) = f(\{x_1\}) = \{y\}$ also. But then $f(A\backslash B) \neq f(A)\backslash f(B)$, and hence we do not have $f(A\backslash B) = f(A)\backslash f(B)$ for every $A, B \subseteq X$. By contrapositive, then, if $f(A\backslash B) = f(A)\backslash f(B)$ for every $A, B \subseteq X$, then f is injective.

6. Let $f : X \to X$ be a function, where X is a finite set. Prove that f is injective if and only if f is surjective. Explain why this is not true in the case that X is infinite.

   Solution: Suppose that f is injective. Then $|X| = |f(X)|$. Moreover, $f(X) \subseteq X$, and since X is finite we therefore have $f(X) = X$. Thus, $\forall y \in X$, we have that $y \in f(X)$, so $\exists x \in X$ with $f(x) = y$. Thus, f is surjective.

   For the converse, suppose that f is surjective. Then we have $f(X) = X$, so $|f(X)| = |X|$. Since X is finite, this implies that f is injective by the Pigeonhole Principle.

   In the case that X is infinite, this result is no longer true because $f(X) \subseteq X$ and $|f(X)| = |X|$ does not require that $f(X) = X$, as it does in the finite case. Consider, for example, $f : \mathbb{N} \to \mathbb{N}$ by $f(x) = x^2$. Then $|X| = |f(X)|$, but $f(X) \neq X$.

7. We know that function composition is associative. Is it also commutative? Why/why not?

   Solution: No. Indeed, we may not even be allowed to change the order of composition, since if $f : X \to Y$ and $g : Y \to Z$, we can compose $g \circ f$ but not $f \circ g$.

4 Counting: finite

1. (a) How many ways are there to rearrange the letters in the word "VECTOR"?

   (b) How many ways are there to rearrange the letters in the word "TRUST," in such a way that the two Ts are not next to each other?

   (c) How many ways are there to rearrange the letters in the word "MATHEMATICS" so that no two consecutive letters are the same?

   Solution:

   (a) 6!

   (b) First, we consider the number of ways to rearrange the letters in general. We can first choose the positions of the two Ts, in $\binom{5}{2}$ ways. We then order the remaining elements in 3! ways into the remaining spots. This yields a total of $\binom{5}{2}3! = \frac{5!3!}{2!3!} = 60$ possible rearrangements.

   Now, we consider rearrangements in which the two Ts are next to each other. If this is the case, we can treat the Ts as a block, and consider permutations of the set $\{\mathrm{TT}, \mathrm{R}, \mathrm{U}, \mathrm{S}\}$, of which there are $4! = 24$ permutations.

   Together, this yields $60 - 24 = 36$ rearrangements for which the two Ts are not next to each other.

   (c) Let us consider the number of duplicates: there are two Ms, two As, and two Ts. There are 5 letters (H, E, I, C, S) that are not duplicates.

   First, we note that the total number of rearrangements of the letters is $\frac{11!}{2*2*2}$, since there are 11! permutations of the

11 letters, but switching each of the Ms, As, or Ts results in the same permutation, so each is counted twice. (This could also be counted as $\binom{11}{2}\binom{9}{2}\binom{7}{2}5!$)

Let S_M denote those permutations for which the Ms are consecutive, S_A those for which the As are consecutive, and S_T those for which the Ts are consecutive. Then by using the counting procedures above, we have

$$\begin{aligned} |S_M \cup S_A \cup S_T| &= |S_M| + |S_A| + |S_T| - |S_M \cap S_A| - |S_M \cap S_T| \\ &\quad -|S_A \cap S_T| + |S_M \cap S_A \cap S_T| \\ &= \frac{10!}{2*2} + \frac{10!}{2*2} + \frac{10!}{2*2} - \frac{9!}{2} - \frac{9!}{2} - \frac{9!}{2} + 8! \end{aligned}$$

Taken all together, we have that the number of permutations for which no consecutive letters are the same is

$$\frac{11!}{8} - \frac{3*10!}{4} + \frac{3*9!}{2} - 8!$$

2. Let $n \in \mathbb{N}$, with $n \geq 1$. How many surjective functions are there from $[n+1]$ to $[n]$?

Solution: If we have a surjective function $f : [n+1] \to [n]$, it must be the case that there exists exactly one $k \in [n]$ such that $|f^{-1}(k)| = 2$. Let $\mathcal{S} = \{f : [n+1] \to [n] \mid f \text{ is surjective}\}$, and let $A_k \subseteq \mathcal{S}$ be the set of surjective functions having $|f^{-1}(k)| = 2$. Then $A_1, A_2, \ldots, A_n$ is a pairwise disjoint partition of $\mathcal{S}$, so $|\mathcal{S}| = |A_1| + |A_2| + \cdots + |A_n|$.

Let us consider $|A_k|$. First, there are exactly two elements $i, j \in [n+1]$ having $f(i) = f(j) = k$. These can be selected in $\binom{n+1}{2}$ ways. The remaining $n-1$ elements of $[n+1]$ are mapped in a one-to-one fashion to the remaining $n-1$ elements of $[n]$; this can be done in $(n-1)!$ ways. Hence, there are $\binom{n+1}{2}(n-1)! = \frac{(n+1)!(n-1)!}{2!(n-1)!} = \frac{(n+1)!}{2}$ such mappings, and $|A_k| = \frac{(n+1)!}{2}$.

Therefore, $|\mathcal{S}| = n\frac{(n+1)!}{2}$.

3. Prove that for all $n, m, k \in \mathbb{N}$, we have

$$\sum_{\ell=0}^{k} \binom{n}{\ell}\binom{m}{k-\ell} = \binom{n+m}{k}$$

Solution: Suppose there is a group of n men and m women, and we must choose k of them to sit on a committee. Clearly, this can be done in $\binom{n+m}{k}$ ways.

On the other hand, we could also choose the men first and women second. There is some number of men between 0 and k; denote this by ℓ. Then we wish to assign ℓ men and $k-\ell$ women to the committee, so that we have a total of k members. This can be done in $\binom{n}{\ell}\binom{m}{k-\ell}$ ways. Letting ℓ range from 0 to k forms a finite partition of all committee assignments, and hence we have that the number of ways to select the committee is

$$\sum_{\ell=0}^{k} \binom{n}{\ell}\binom{m}{k-\ell}.$$

Since both the right and left hand sides of the equation count the same thing (the number of ways to assign the committee), they are equal.

4. Use counting in two ways to prove that for all $n, k \in \mathbb{N}$ with $n \geq k > 0$, we have
$$\sum_{j=n-k}^{n} \binom{n}{j} = \sum_{j=n-k}^{n} \binom{j-1}{n-k-1} 2^{n-j}.$$

   Solution: Let us count the number of subsets of $[n]$ of size at least $n-k$. Note that such subsets can have any size from $n-k$ to n, and hence the number of such subsets is $\sum_{j=n-k}^{n} \binom{n}{j}$.

   Let us count in a different way. Since each subset has size at least $n-k$, let j denote the $(n-k)^{\text{th}}$ element of the subset; note that j can take any value between $n-k$ and n. Then there are $n-k-1$ elements of the subset less than j, which can be chosen in $\binom{j-1}{n-k-1}$ ways. The $n-j$ elements larger than j can either be in the subset or not; choosing whether to include such elements can be done in 2^{n-j} ways. Hence, for any particular j, there are $\binom{j-1}{n-k-1} 2^{n-j}$ subsets of size at least $n-k$ for which j is the $(n-k)^{\text{th}}$ element of the set. As every set has a unique $(n-k)^{\text{th}}$ element, this is a finite partition of the sets in question, and hence the number of such sets is
$$\sum_{j=n-k}^{n} \binom{j-1}{n-k-1} 2^{n-j}.$$

   Therefore, by counting in two ways, we obtain
$$\sum_{j=n-k}^{n} \binom{n}{j} = \sum_{j=n-k}^{n} \binom{j-1}{n-k-1} 2^{n-j}.$$

5. Use Inclusion-Exclusion to determine the number of subsets of [20] that contain a multiple of 5.

   Solution: Let A_d denote the set of subsets of [20] that contain d; we wish to count $|A_5 \cup A_{10} \cup A_{15} \cup A_{20}|$. Using inclusion-exclusion, we have
$$\begin{aligned}
|A_5 \cup A_{10} \cup A_{15} \cup A_{20}| &= |A_5| + |A_{10}| + |A_{15}| + |A_20| - |A_5 \cap A_{10}| \\
&\quad -|A_5 \cap A_{15}| - |A_5 \cap A_{20}| - |A_{10} \cap A_{15}| \\
&\quad -|A_{10} \cap A_{20}| - |A_{15} \cap A_{20}| + |A_5 \cap A_{10} \cap A_{15}| \\
&\quad +|A_5 \cap A_{10} \cap A_{20}| + |A_5 \cap A_{15} \cap A_{20}| \\
&\quad +|A_{10} \cap A_{15} \cap A_{20}| - |A_5 \cap A_{10} \cap A_{15} \cap A_{20}| \\
&= 4 * 2^{19} - 6 * 2^{18} + 4 * 2^{17} - 2^{16}
\end{aligned}$$

6. Suppose we have a box containing a set of standard chess pieces. You select three pieces from the box. In how many ways can you select the pieces so that

   (a) all three are the same color.

   (b) all three are the same color and all three are pawns.

   (c) all three are rooks.

   Solution:

   (a) Given a choice of color, there are $\binom{16}{3}$ ways to select 3 pieces of the same color. Hence, there are $2 * \binom{16}{3}$ ways to select 3 pieces of the same color.

   (b) Given a choice of color, there are $\binom{8}{3}$ ways to select 3 pawns of that color. Hence, there are $2 * \binom{8}{3}$ ways to select three pawns of the same color.

   (c) There are 4 rooks in the box, so there are $\binom{4}{3}$ ways to select 3 rooks.

7. From a standard deck of cards, you deal out a five-card poker hand. How many different hand have at least three cards of the same type (i.e., a 3-of-a-kind or 4-of-a-kind).

   Solution: First, we have 13 different types of cards that could have a 3-of-a-kind or a 4-of-a-kind. From these, there are 4 ways to choose 3 of these cards. Once these 3 are chosen, there are 49 remaining cards in the deck, two of which must be added to the hand (this will sometimes produce a 4-of-a-kind). Hence there are $13 * 4 * \binom{49}{2}$ such hands.

5 Counting: infinite

1. Suppose that A, B, C are countably infinite disjoint sets. Prove that $A \cup B \cup C$ is countably infinite directly, by finding a bijection between $A \cup B \cup C$ and $\mathbb{N}$.

   Solution: Let $f : \mathbb{N} \to A$, $g : \mathbb{N} \to B$, and $h : \mathbb{N} \to C$ be bijections. Define a function $F : \mathbb{N} \to A \cup B \cup C$ by

$$F(k) = \begin{cases} f(\frac{k+2}{3}) & k \equiv 1 \pmod 3 \\ g(\frac{k+1}{3}) & k \equiv 2 \pmod 3 \\ h(\frac{k}{3}) & k \equiv 0 \pmod 3 \end{cases}$$

   Note then that $F(1) = f(1), F(4) = f(2), F(7) = f(3)$, etc, so that $F([1]_3) = A$, where $[1]_3$ denotes the equivalence class of 1 modulo 3. Likewise, $F([2]_3) = B$ and $F([3]_3) = C$. Thus, F is surjective. Moreover, F is injective, since each of f, g, h are injective.

   Therefore F is a bijection, so $|A \cup B \cup C|$ is countably infinite.

2. Let $\mathcal{F} = \{f : X \to \{0,1\}\}$, where X is any set. Carefully go through the Cantor diagonalization argument to show that $|\mathcal{F}| > |X|$.

   Solution: Suppose, to the contrary, that $|\mathcal{F}| \leq |X|$. For each $x \in X$, note that we can define a function f_x by $f_x(x) = 1$ and $f_x(y) = 0$ for $y \neq x$. Hence, we can produce an injection $G : X \to \mathcal{F}$ by $G(x) = f_x$, so $|X| \leq |\mathcal{F}|$. Therefore, we must have that $|X| = |\mathcal{F}|$.

   Therefore, there exists a bijection $H : X \to \mathcal{F}$. For simplicity of notation, put $H(x) = H_x : X \to \{0,1\}$. Define a function $f : X \to \{0,1\}$ by

$$f(x) = \begin{cases} 0 & \text{if } H_x(x) = 1 \\ 1 & \text{if } H_x(x) = 0 \end{cases}$$

   Since f is a function from $X \to \{0,1\}$ we have that $f \in \mathcal{F}$. Since H is a bijection, there exists $x \in X$ such that $f \equiv H_x$. But $f(x) \neq H_x(x)$, and hence $f \not\equiv H_x$. This is a contradiction, and hence we cannot have that $|\mathcal{F}| \leq |X|$.

   Therefore, we must have $|\mathcal{F}| > |X|$.

3. Let X, Y be nonempty sets of positive real numbers. Define

$$XY = \{xy \mid x \in X, y \in Y\}.$$

   Prove that XY is infinite if and only if at least one of X or Y is infinite.

   Solution:
   ($\Rightarrow$) Suppose, for the sake of contrapositive, that neither X nor Y is infinite, so that both are finite. Define a function $F : X \times Y \to XY$ by $F((x,y)) = xy$. By definition of XY, we have that F is surjective, and therefore $|XY| \leq |X \times Y| = |X||Y|$, which is finite (by theorem from class). Hence, XY is finite.
   Therefore, if XY is infinite, we must have at least one of X or Y is infinite.

   ($\Leftarrow$) Suppose at least one of X or Y is infinite, wolog say that X is infinite. Let $y_0 \in Y$ be any element of Y. Then consider $\{xy_0 \mid x \in X\} \subseteq XY$. For $x \neq x'$, we also have $xy_0 \neq x'y_0$, and hence $h : X \to \{xy_0 \mid x \in X\}$ defined by $h(x) = xy_0$ is a bijection. Therefore, $|\{xy_0 \mid x \in X\}| = |X|$, and thus XY contains an infinite subset. Therefore XY is infinite.

4. Let $\mathcal{A}$ be a collection of sets. We say that $\mathcal{A}$ has the *finite intersection property* if the intersection of any finite number of sets in $\mathcal{A}$ is nonempty.

   Give an example of an infinite collection of sets $\mathcal{A}$ that have the finite intersection property, but $\bigcap_{A \in \mathcal{A}} A$ is empty.

   Solution: There are MANY answers here.
   Define $\mathcal{A} = \{A_1, A_2, A_3, \ldots\}$, where $A_k = \{k, k+1, k_2, \ldots\}$. Then for $k_1, k_2, \ldots, k_n$, we have $A_{k_1} \cap A_{k_2} \cap \cdots \cap A_{k_n} = A_{\max\{k_1, k_2, \ldots, k_n\}}$, so any finite intersection of the A_k is nonempty.

On the other hand, $\bigcap_{A\in\mathcal{A}} A = \bigcap_{k=1}^{\infty} A_k$ is empty. Indeed, suppose that $N \in \bigcap_{k=1}^{\infty} A_k$. This would imply that $N \in A_k$ for all $k \in \mathbb{N}$. But $N \notin A_{N+1}$, which is a contradiction. Hence, $\bigcap_{k=1}^{\infty} A_k$ is empty.

6 Divisibility and Number Theory

1. Use the Euclidean Algorithm to prove that for all $n \in \mathbb{N}$, the fraction $\frac{12n+1}{30n+2}$ is in lowest terms.

   Solution: Let us consider $\gcd(12n+1, 30n+2)$. Since $n \in \mathbb{N}$, we have $30n+2 > 12n+1$. Following the Euclidean Algorithm:

   $$30n + 2 \quad = \quad 2 * (12n + 1) + 6n,$$

   so $\gcd(30n + 2, 12n + 1) = \gcd(12n + 1, 6n)$. But $12n + 1 \equiv 1 \pmod 6$, and $6n \equiv 0 \pmod 6$, so $12n + 1 \perp 6n$. Therefore, $\gcd(30n + 2, 12n + 1) = 1$, so $30n + 2$ and $12n + 1$ share no common factors, and thus the fraction is in lowest terms.

2. Suppose that $a, b, c, d \in \mathbb{N}$ with $ab-cd$ divides each of a, b, c, and d. Prove that $ab - cd = \pm 1$.

   Solution: First, if $ab - cd = 0$, note that this is impossible, since $a \in \mathbb{N}$, so $a > 0$ and 0 is therefore not a factor of a. Hence, we can assume that $ab - cd \neq 0$.

   Then we have integers k, j, n, m such that $a = k(ab - cd), b = j(ab - cd), c = n(ab - cd), d = m(ab - cd)$. Therefore, by substitution, we have

   $$\begin{aligned} ab - cd &= k(ab - cd)j(ab - cd) - n(ab - cd)m(ab - cd) \\ &= (ab - cd)^2(kj - nm). \end{aligned}$$

   Since $ab - cd \neq 0$, we can divide by $ab - cd$ to obtain $1 = (ab - cd)(kj - nm)$. Moreover, both $ab - cd$ and $kj - nm$ are integers, and hence as we have the product of integers equalling 1, we must have that $ab - cd = kj - nm = \pm 1$.

3. Find the set of all integer solutions to the equation $3x + 4y = 5$.

   Solution: First, notice that we have one solution $x = -1, y = 2$. Moreover, we have $\gcd(3, 4) = 1$, so we have that other solutions can be constructed as $(-1 + 4k, 2 - 3k)$ for $k \in \mathbb{Z}$. Hence, we have the set of all such solutions is

   $$\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x = -1 + 4k, y = 2 - 3k \text{ for some } k \in \mathbb{Z}\}.$$

7 Modular arithmetic

1. Suppose that $a \equiv b \pmod{n}$, and $c \equiv d \pmod{n}$. Prove that $ac \equiv bd \pmod{n}$.

   Solution: Let $k, j \in \mathbb{N}$ be such that $a = b + kn$ and $c = d + jn$. Then

   $$\begin{aligned} ac &= (b + kn)(d + jn) \\ &= bd + n(kd + bj + kjn), \end{aligned}$$

   and thus $ac \equiv bd \pmod{n}$.

2. Calculate the remainder of 3^{1000} when divided by 7.

   Solution: Note that $\varphi(7) = 6$, so $3^6 \equiv 1 \pmod{7}$. Therefore,

   $$3^{1000} \equiv 3^{6*166+4} \equiv (3^6)^{166} 3^4 \equiv 3^4 \equiv 9^2 \equiv 2^2 \equiv 4 \pmod{7}$$

3. Suppose that $a, b, c \in \mathbb{Z}_n$, and $a + b \equiv a + c \pmod{n}$. Is it true that $b \equiv c \pmod{n}$? If so, prove it. If not, explain why not.

   Solution: Yes, this is true. Since $a + b \equiv a + c \pmod{n}$, we have $a + b - a \equiv a + c - a \pmod{n}$, so $b \equiv c \pmod{n}$.

4. Find the set of all solutions to the congruences

   $$\begin{gathered} x \equiv 7 \pmod{1}1 \\ x \equiv 3 \pmod{5} \\ x \equiv 1 \pmod{6} \end{gathered}$$

   Solution: By the Chinese Remainder Theorem, we know that solutions must exist, since 11, 5, and 6 are coprime.
   Put $m_1 = 5 * 6 = 30 \equiv 8 \pmod{1}1$, $m_2 = 11 * 6 = 66 \equiv 1 \pmod{5}$, and $m_3 = 11 * 5 = 55 \equiv 1 \pmod{6}$. Note then that m_1 has inverse $y_1 = 7$ modulo 11, since $8*7 = 56 \equiv 1 \ (\bmod\ 1)1$. Moreover, m_2 and m_3 both have inverse $y_2 = y_3 = 1$. Therefore, by the CRT, we have that solutions x satisfy

   $$x \equiv 7 * 7 * 30 + 3 * 1 * 66 + 1 * 1 * 55 \equiv 1723 \pmod{330}.$$

   Therefore, the set of all solutions is

   $$\{1723 + 330k \mid k \in \mathbb{Z}\}.$$

5. Suppose $n > 1$ is an integer such that $4((n-1)! + 1) \equiv 0 \pmod{n}$. Prove that $n = 4$ or n is prime.

   Solution: First, suppose that n is composite, so $n = ab$ for some $a, b \neq 1$ in $\mathbb{N}$. We claim that $(n-1)! + 1$ shares no factors with n. Indeed, suppose that $d|n$. If $d < n$, then $d|(n-1)!$, and therefore d cannot divide $(n-1)! + 1$. Therefore, a does not divide $(n-1)! + 1$ and neither does b. As a result, n does not divide $(n-1)! + 1$ either, and hence $(n-1)! + 1$ is coprime to n. Let y be the inverse of $(n-1)! + 1$ modulo n. Then we have

   $$\begin{aligned} 4((n-1)! + 1) \equiv 0 \pmod{n} &\Rightarrow 4((n-1)! + 1)y \equiv 0y \pmod{n} \\ &\Rightarrow 4 \equiv 0 \pmod{n}. \end{aligned}$$

Since n is assumed to be composite, and $4 \equiv 0 \pmod{n}$, we must have that $n = 4$.

Therefore, if n is composite and $4((n-1)!+1) \equiv 0 \pmod{n}$, we have $n = 4$. Thus,

$$4((n-1)!+1) \equiv 0 \pmod{n} \Rightarrow n \text{ is prime or } n = 4.$$

6. Let $S \subseteq [2n]$ with $|S| \geq n+1$. Prove that there exist $a, b \in S$, $a \neq b$, with $a|b$.

Solution: Upon further reflection, this problem is probably in the wrong section in this review. Sorry about that.

For each number $x \in [2n]$, there is a unique choice of a, b such that b is odd and $x = 2^a b$, by the Fundamental Theorem of Arithmetic. Let $O = \{x \in [2n] \mid x \text{ is odd}\}$.

Define a function $f : S \to O$ by $f(x) = b$, where $x = 2^a b$ as described above. By the observation above, f is well-defined. Moreover, $|O| = n$ and $|S| \geq n+1$, and hence there exists $x_1, x_2 \in S$ having $f(x_1) = f(x_2)$. Therefore, $x_1 = 2^{a_1} b$ and $x_2 = 2^{a_2} b$ for some $a_1 \neq a_2 \in \mathbb{N}$. Wolog, suppose that $a_2 > a_1$. Then $x_1 | x_2$.

8 Posets

1. Define a relation $\preceq$ on $\mathbb{N}$ by $x \preceq y$ if and only if $x \leq y$ and x and y have the same parity. Is $\mathbb{N}$ a poset under $\preceq$? If so, prove it. If not, explain why not.

Solution: Yes, this is a poset.

Reflexivity: Note that $\forall x \in \mathbb{N}$, $x \leq x$ and x has the same parity as itself, so $x \preceq x$.

Transitivity: Suppose that $x \preceq y$ and $y \preceq z$. Then $x \leq y$ and $y \leq z$, so $x \leq z$. Moreover, x and y have the same parity, and y and z have the same parity, so x and z also have the same parity. Thus, $x \preceq z$.

Antisymmetry: Suppose that $x \preceq y$ and $y \preceq x$. Then in particular, $x \leq y$ and $y \leq x$, so $x = y$.

2. Define a relation $\preceq$ on $\mathbb{N}$ by $x \preceq y$ if and only if $x \leq y$ and $x \perp y$. Is $\mathbb{N}$ a poset under $\preceq$? If so, prove it. If not, explain why not.

Solution: No, this is not a poset. It is not transitive. Consider $x = 2$, $y = 3$, and $z = 4$. Then $x \perp y$, so $x \preceq y$, and $y \perp z$, so $y \preceq z$, but x shares a factor with z, so $x \not\preceq z$.