Math 25a Homework 1 Solutions

Ivan Corwin and Alison Miller

General Comments on the problems set:

- Take care in your write-ups. Do not spit up math on the paper and expect Alison and me to shape it into a proof.
- Organize your proofs and make it clear to us what you are doing and why you are doing it. If you need a lemma, state it as such and prove it.
- Be NEAT. If you want to learn tex, let us know and we'll teach you. Otherwise, write in a dark pencil or pen, don't cramp your words in, keep pages in order, only write on one side of the page, carefully staple pages together, write legibly.
- Try to be concise and clear. But also don't disrespect the problem by giving a solution to the point "This is trivial."
- Believe me, if you follow these points of advice you will do better on problem sets. This is for two reasons: (1) it is easier for us to grade and attracts less negative attention, and (2) if you give us chicken-scratch, we will not grade it and you will receive a grade of 0.

1 Sets and Maps

(1) Let $A, B \subset X$. Prove that $A \subset B$ if and only if $X \smallsetminus B \subset X \smallsetminus A$.

Solution. Denote $C = X \setminus Y = \{a{\in}X : a{\notin}Y\}$. Then, $X \setminus C = \{a{\in}X : a{\notin}C\} = \{a{\in}X : a{\in}Y\} = X \cap Y = Y$. □

(2) Prove the following statements (here A, B and C are three sets and $A \times B$ is defined to be the set of all pairs (a, b) with $a \in A$ and $b \in B$).

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

Solution. Consider $A \times (B \cup C) = \{(a, z) | a \in A, z \in B \cup C\}$. Since $z \in B \cup C$ the membership condition is $(a \in A, z \in B) \vee (a \in A, z \in C)$, thus any member of $A \times (B \cup C)$ is either a member of $A \times B = \{(a, z) | a \in A, z \in B\}$ or $A \times C = \{(a, z) | a \in A, z \in C\}$. Combining these gives that $A \times (B \cup C) = (A \times B) \cup (A \times C)$ as desired. □

(b) $A \smallsetminus (B \cup C) = (A \smallsetminus B) \cap (A \smallsetminus C)$

Solution. Note: Here is another style of proof

$$\begin{aligned} A \setminus (B \cap C) &= \{x \in A : x \notin (B \cap C)\} \\ &= \{x \in A : \text{not}(x \in B \text{ and } x \in C)\} \\ &= \{x \in A : x \notin B \text{ or } x \notin C\} \\ &= \{x \in A : x \notin B\} \cup \{x \in A : x \notin C\} \\ &= (A \setminus B) \cup (A \setminus C) \quad \square \end{aligned}$$

(3) Let $f : A \to B$ be a map, let W, X be two subsets of A and let Y, Z be two subsets of B. Determine whether the following are true or false.

(a) $f^{-1}(Y \cap Z) = f^{-1}(Y) \cap f^{-1}(Z)$

Solution. Say $x{\in}f^{-1}(Y) \cap f^{-1}(Z)$. Then, for some $y \in Y, z \in Z$, we have $f(x) = y$ and $f(x) = z$. But, as f is a function, we must then have $y = z$, and so $f(x) \in Y \cap Z$ (then $x \in f^{-1}(Y \cap Z)$.

Say $x \in f^{-1}(Y \cap Z)$. Then, $f(x) \in Y \cap Z$, so $f(x) \in Y$ and $f(x) \in Z$. From this, we see that $x \in f^{-1}(Y)$ and $x \in f^{-1}(Z)$, and so $x{\in}f^{-1}(Y) \cap f^{-1}(Z)$. □

(b) $f(W \cap X) = f(W) \cap f(X)$

Solution. A counterexample I enjoyed was to let $W = \mathbb{R}^+$ and $X = \mathbb{R}^-$ and consider $f(x) = x^2$. Then clearly $W \cap X = \emptyset$ while both their ranges coincide on $\mathbb{R}^+$. □

(c) If $Y \subset Z$ then $f^{-1}(Z \smallsetminus Y) = f^{-1}(Z) \smallsetminus f^{-1}(Y)$

Solution. Say $x{\in}f^{-1}(Z \setminus Y)$. Then, $f(x) \in Z \setminus Y$, so $f(x) \in Z$, hence $x \in f^{-1}(Z)$. Also, $f(x) \notin Y$, so $x \notin f^{-1}(Y)$, for $f(x) \notin Y$. So, $x \in f^{-1}(Z) \setminus f^{-1}(Y)$.

Say $x \in f^{-1}Z \setminus f^{-1}(Y)$. Then, $x \in f^{-1}Z$ (so $f(x) \in Z$) and $x \notin f^{-1}(Y)$ (so $f(x) \notin Y$). Thus, $f(x) \in Z \setminus Y$ and $x \in f^{-1}(Z \setminus Y)$. □

(4) Let $f : X \to Y$ be a map of sets. Prove that the following are equivalent:

(a) f is injective.

(b) $f^{-1}(t)$ contains at most one element for any $t \in Y$

(c) $f(A \cap B) = f(A) \cap f(B)$ for any $A, B \subset X$.

Solution. (a) ⇒ (b): For any fixed $t \in Y$, and any $a, b \in f^{-1}(t)$ we have $f(a) = f(b) = t$. So, if f is injective, then we must have $a = b$. Thus, for fixed t, $f^{-1}(t)$ can contain at most one distinct element.

(b) ⇒ (c): Say $y \in f(A \cap B)$. Then, $y = f(x)$ for $x \in A \cap B$, and so $f(x) \in f(A)$ and $f(x) \in f(B)$, so $y \in f(A) \cap f(B)$.

Say $y \in f(A) \cap f(B)$. Then, $y = f(a)$ for $a \in A$ and $y = f(b)$ for $b \in B$. But, by (b), y has a unique pre-image, so $a = b$. Then, $a = b \in A \cap B$, so $y \in f(A \cap B)$.

(c) ⇒ (a): We proceed by contradiction. Assume that (c) holds but that f is not injective, and that in particular it maps both x_1 and x_2 to y. Then, letting $A = \{x_1\}$ and $B = \{x_2\}$ we see that $f(A \cap B) = \emptyset$ while $f(A) \cap f(B) = \{y\}$. This yields a contradiction.

□

(5) Suppose that A and B are two sets, and denote by A^B the set of all maps $f : B \to A$. Construct a bijection between $A^{B\times C}$ and $(A^B)^C$.

Solution. We claim that the map $\phi : A^{B\times C} \to \left(A^B\right)^C$, given by $\left[(\phi f)(c)\right](b) = f(b,c)$, is such a bijection.

We note that it is clearly injective, for if $\phi f_1 = \phi f_2$ then for all $b{\in}B, c{\in}C$ we must have $f_1(b,c) = \left[(\phi f_1)(c)\right](b) = \left[(\phi f_2)(c)\right](b) = f_2(b,c)$. Furthermore, it is surjective, as we can give an inverse function defined by $(\phi^{-1}g)(b,c) = \left[g(b)\right](c)$.

□

(6) Prove that if X and Y are two sets such that there are injective maps $f : X \to Y$ and $g : Y \to X$, then there is a bijection from X to Y.

Claim 1. *Given $B \subset A$, and an injection $f' : A \to B$, then there is a bijection from A to B. (Note: Yes, there was a typo in the problem set's version of this claim. The injection was in the wrong direction (so that the inclusion map would've satisfied the condition!).*

Proof.

(a) Define a sequence $\{C_n\}$ of subsets of A by $C_0 = A \setminus B$ and $C_n = f(C_{n-1})$ for $n \geq 1$. The C_n are pairwise disjoint, for otherwise we could choose j, k such that $C_j \cap C_k \neq \emptyset$ and with $j + k$ minimal among such pairs. We note that C_0 is disjoint with C_n for $n > 0$, so $C_j = f(C_{j-1})$ and $C_k = f(C_{k-1})$. But, as f is an injection, this implies that $f(C_{j-1} \cup C_{k-1}) \neq \emptyset$, and so $C_{j-1} \cap C_{k-1} \neq \emptyset$. This violates our choice of j, k as minimizing $j+k$, yielding a contradiction, and showing the C_n pairwise disjoint.

(b) Let $C = \bigcup_{n=0}^{\infty} C_n$, and define $h : A \to B$ as:

$$h(x) = \begin{cases} f(x) & x \in C \\ x & x \notin C \end{cases}$$

Note that $A\setminus C = B\setminus f(C)$ (and that $C \subset A$, $f(C) \subset B$). So, if $x \in C$, then $h(x) = f(x) \in B$, while if $x \notin C$, then $h(x) = x \in B$, and $h(A) \subset B$. To see that h is bijective, we note that it maps C bijectively into $f(C)$ (by construction), and that it maps $A \setminus C$ bijective into $B \setminus f(C)$ (by inclusion). This yields our desired result. □

Problem 1 (Schroeder-Bernstein)**.** *Given two sets X, Y and injective maps $f : X \to Y$, $g : Y \to X$, there is a bijection from X to Y.*

Solution. We will show that our result is equivalent to the preceding claim. First, we note that the claim follows from our desired result, by letting $X = A$, $Y = B$, g the inclusion map, and $f = f'$. For the other direction, we note that g provides a bijection from Y to $g(Y) \subset X$. Then, apply the claim to $A = X$, $B = g(Y)$, and $f' = g \circ f$ (the composition of two injections is clearly injective). This gives a bijection of X to $g(Y)$. Then, as the composition of two bijections is bijective, we can construct a bijection from X to Y, as desired. □

2 Equivalence relations

(1) Given a set A and an equivalence relation $\sim$, recall from class that an *equivalence class* $[a]$ is defined as $[a] := \{b \in A : b \sim a\}$. Prove that if $[a], [b]$ are two equivalence classes, then either $[a] = [b]$ or $[a] \cap [b] = \emptyset$.

Solution. Say two equivalence classes have non-empty intersection. Without loss of generality, $x \in [a] \cap [b]$. But then, for any $a' \in [a]$ and $b' \in [b]$, $a' \sim x$ and $x \sim b'$, so $a' \sim b'$. So, a' and b' must be in the same equivalence class, that is we must have $[a] = [b]$.

□

(2) Let A be the set of all pairs of integers (a, b) such that $b \neq 0$. Define $(a, b) \sim (c, d)$ if and only $ad = bc$.

(a) Prove that this is an equivalence relation.

Solution.

Symmetric: $(a, b) \sim (c, d)$ implies $ad = bc$. For $(c, d) \sim (a, b)$ it must hold that $cb = da$, which by the commutative nature of integers holds.

Reflexive: $(a, b) \sim (a, b)$ since $ab = ba$.

Transitive: $(a, b) \sim (c, d)$ implies $ad = bc$ while $(c, d) \sim (e, f)$ implies $cf = de$. One approach is to notice that since $b, d, f \neq 0$ we may say that $a/b = c/d$ and $c/d = e/f$, and hence $a/b = e/f$ implying $(a, b) \sim (e, f)$. The problem with this is it assumes the concept of equality has been predefined for the rationals (such as a/b). If this approach is used to define the rational numbers, then there is circular reasoning. So, let us stay in the realm of the integers. Note that by combining $ad = bc$ and $cf = de$ we get $acdf = bcde$. We know that $d \neq 0$. So if $c \neq= 0$ we may cancel to find $af = be$ and hence $(a, b) \sim (e, f)$. However, if $c = 0$ observe that a must equal 0 (as $d \neq 0$) and so must $e = 0$. Therefore we still find that $af = be$ and hence $(a, b) \sim (e, f)$.

□

Definition: The quotient of A by the equivalence relation $\sim$ is the set of all equivalence classes: $A/\sim := \{[a] : a \in A\}$.

(b) In class, we saw that $A/\sim$ looks a lot like the rational numbers. We defined addition on $A/\sim$ to be $[(a, b)] + [(c, d)] = [(ad + bc, bd)]$. Check that this definition is well-defined. (That is, if $[(a, b)] = [(a', b')]$ and $[(c, d)] = [(c', d')]$, then $[(ad + bc, bd)] = [(a'd' + b'c', b'd')]$.)

Solution. We know $ab' = ba'$ and $cd' = dc'$. We must confirm that $adb'd' + bcb'd' = bda'd' + bdb'c'$ which making the appropriate substitutions becomes clear. □

(c) Define multiplication ($[(a, b)] \cdot [(c, d)] =?$) and check that it is well defined.

Solution. Multiplication is defined such that ? is replaced with $[(ac, bd)]$ and then well defined follows easily. □

(d) Prove the existence of additive inverses.

Solution. Defining the additive inverse of $[(a,b)]$ to be $[(-a,b)]$ is easily shown to work. Many people lost points by solving for an inverse which contained fractions inside the brackets. This is a big no-no since the entries must be integers (we can't use rational numbers to define rational numbers). □

(3) Let $f : S \to T$ be a map of sets. Define a relation on S by $s_1 \sim s_2$ if and only if $f(s_1) = f(s_2)$.
(a) Prove that this is an equivalence relation

Solution. We verify that $\sim$ is an equivalence relation:

(a) Symmetric: If $s_1 \sim s_2$, then $f(s_1) = f(s_2)$, so $f(s_2) = f(s_1)$ (as $=$ is definitely an equivalence relation), so $s_2 \sim s_1$.

(b) Reflexive: For any $s \in S$, $f(s) = f(s)$ and so $s \sim s$.

(c) Transitive: If $s_1 \sim s_2$ and $s_2 \sim s_3$, then $f(s_1) = f(s_2) = f(s_3)$, and so $s_1 \sim s_3$.

□

(b) Find an injective map $\tilde{f} : S/\sim \to T$.

Solution. Now, we define $\bar{f}$ as follows: Given $[s] \in S/\sim$, take any representative $s' \in [s]$, and set $\bar{f}([s]) = f(s')$. This gives a well defined map as for any two elements $s_1, s_2 \in [s]$, we have, by construction of $\sim$, that $f(s_1) = f(s_2)$. Moreoever, it is clearly injective for $\bar{f}(\bar{s}_1) = \bar{f}(\bar{s}_2)$ implies $f(s_1) = f(s_2)$, and thus $s_1 \sim s_2$, for all $s_1 \in \bar{s}_1, s_2 \in \bar{s}_2$, and so $\bar{s}_1 = \bar{s}_2$.

(3) Let $f : S \to T$ be a map of sets. Define a relation on S by $s_1 \sim s_2$ if and only if $f(s_1) = f(s_2)$.
(a) Prove that this is an equivalence relation
(b) Find an injective map $\tilde{f} : S/\sim \to T$.
Hint: first construct the map and prove that it is injective. □

3 Combinatorics

(1) Prove by induction that the following two statements are true for every positive integer n.
(a) $1^3 + 3^3 + 5^3 + \cdots + (2n-1)^3 = n^2(2n^2 - 1)$
(b) The number $2^{n+2} + 3^{2n+1}$ is a multiple of 7.

Solution. (a) We proceed by induction.

Base Case: $n = 1$. Then the sum on the left hand side is $1^3 = 1$, while the right hand formula amounts to $1^2(2 \cdot 1^2 - 1) = 1$, so the base case holds.

Inductive Step: We now assume that the formula holds for $n = k$, that is, $1^3 + 3^3 + 5^3 + \cdots + (2k-1)^3 = k^2(2k^2 - 1)$. We now need to show the formula for $n = k + 1$, that is, that

$1^3 + 3^3 + 5^3 + \cdots + (2n+1)^3 = (k+1)^2(2(k+1)^2 - 1)$. Using our inductive hypothesis to rewrite the sum,

$$\begin{aligned} 1^3 + 3^3 + 5^3 + \cdots + (2k-1)^3 + (2k+1)^3 &= k^2(2k^2 - 1) + (2k+1)^3 \\ &= 2k^4 + 8k^3 + 11k^2 + 6k + 1 \\ &= (k^2 + 2k + 1)(2k^2 + 4k + 1) \\ &= (k+1)^2(2(k+1)^2 - 1) \end{aligned}$$

so the formula holds for $n = k+1$. Hence by induction, the formula holds for all k. □

(b) Again, we proceed by induction. Let $A_n = 2^{n+2} + 3^{2n+1}$. We need to show that A_n is divisible by 7 for all n. *Base Case:* $n = 0$. For $n = 0$, $A_n = 4 + 3 = 7$, which is divisible by 7. (Note: the question did not actually ask us to prove the formula for $n = 0$, but $n = 0$ provides a simpler base case than $n = 1$.) *Inductive Step:* We assume that the statement is true for $n = k$, that is, $7 \mid A_k$, and we need to show that $7 \mid A_{k+1}$ as well. We rewrite A_{k+1} as

$$A_{k+1} = 2^{k+3} + 3^{2k+3} = 2(2^{k+2}) + 9(3^{2k+1}) = 2A_k + 7(3^{2k+1}).$$

The first term is a multiple of 7 by the induction hypothesis, and the second term is also a multiple of 7, so A_{k+1} is itself a multiple of 7. Hence we can apply mathematical induction to deduce that $7 \mid A_n$ for all n.

(2) Show that if A and B are non-empty finite sets, then $Card(A^B) = Card(A)^{Card(B)}$.

Solution. For convenience, denote $n = \text{Card}(A)$ and $m = \text{Card}(B)$. Then, note that $\text{Card}(A^B)$ is the number of functions with domain B and codomain A. For such a function, we can arbitrarily choose any of the n codomain elements as the image of any of the m domain elements, and so, because each choice multiplies the number of possibilities by n, there are n^m such functions. □

(Optional: Think about why this is true if one of A or B is empty.) If B is empty, then there is exactly one map in A^B (the map whose graph is the null set), and the RHS is always 1. If A is empty, then there can be no maps in A^B, unless B is also empty, and the RHS will always be 0 (unless B is also empty, in which case we can define $0^0 = 1$).

(3)(a) A string of left and right brackets is said to be balanced if each left bracket has (to its right) a matching right bracket. How many balanced strings of n left and n right brackets are there? (I'm only looking for answers for $n = 0, 1, 2, 3, 4$ and maybe 5.)

$n = 0$ 1: (null string)

$n = 1$ 1: []

$n = 2$ 2: [[]], [] []

$n = 3$ 5: [[[]]], [[] []] [[]] [], [] [[]], [] [] []

$n = 4$ 14: [[[[]]]], [[[] []]], [[[]] []], [[[]]] [], [[] [[]]], [[] [] []], [[] []] [], [[]] [[]], [[]] [] [], [] [[[]]], [] [[] []], [] [[]] [], [] [] [[]], [] [] [] []

$n = 5$ 42: check it yourself!

(b) For any positive integer n, evenly distribute $2n$ points on the circumference of a circle. In how many ways can these $2n$ points be paired off as n chords, where no two chords intersect? (I'm only looking for answers for $n = 1, 2, 3, 4$ and maybe 5.)

Again: $1, 1, 2, 5, 14, 42$. The pictures are unwieldy to make in TEX, but check it yourself using the lists from (a) and the bijection of (d).

(c) A railway track consists of a left track, a right track both of which merge into a central track. There are n railway wagons on the left track. The wagons are moved from the left track to the right track through the central track. It is assumed that the central track can accommodate all n of them and that they travel only from left to right (that is, they may not be moved from the central track back to the left track). How many different ways are there to move the n wagons from the left track to the right track? (I'm only looking for answers for $n = 0, 1, 2, 3, 4$ and maybe 5.)

The answer is the same as above: verify it yourself with the bijection.

(d) Hmmm, do the numbers from parts (a), (b) and (c) look familiar? Can you show that these problems are equivalent? (For example, given a bracketing, can you get a chord diagram and vice-versa?)

Bracketings ⇒ Railway Wagons Read through the bracketing left-to-right. Every time you encounter a left bracket, move a wagon from the left to the center. Every time you encounter a right bracket, move a wagon from the center to the right. This will always be possible because before every right bracket there must be at least one more left brackets than right brackets, so that whenever you need to move a wagon from center to right, there will be at least one wagon on the center track (at least one more train has arrived at the station than has left the station).

Railway Wagons ⇒ Bracketings This is just the inverse of the previous equivalence. Whenever you move a wagon from left to center, write down a left bracket. Whenever you move a wagon from center to right, write down a right bracket. This bracketing is balanced, because if we number the wagons $1, 2, 3, \dots n$, the bracket that corresponds to moving wagon number i from left to center is matched up with the bracket corresponding to moving wagon number i from center to right.

These two mappings are clearly inverses to each other, and give us an equivalence between the two problems, so either one is a bijection.

Railway Wagons ⇒ Chords As in the previous problem, label the railway wagons $1, 2, 3, \dots n$, in the order in which they are moved onto the center track: note that the setup of the track is such that one can only move a wagon off the center track if no wagons of larger number on the center track are blocking its exit. Additionally, it takes $2n$ moves to transport the wagons, which we can number as $1, 2, 3, \dots 2n$. Correspondingly, we can number the $2n$ points around the circle consecutively as $1, 2, 3, \dots, n$. For each $k = 1, 2, \dots, 2n$, number the kth point on the circle with the number of the wagon moved on step k. We can then connect the chords: we claim that two chords can never intersect. For the chords with endpoints numbered i intersected the chord with endpoints numbered j, $i < j$, the ith wagon would have had to leave the center track while the jth wagon was on the track, which is impossible. So all railway wagon schedules map to non-intersecting chords.

Chords ⇒ Railway Wagons Again, we run the previous mapping in the other direction. This is slightly more complicated, but the exact same idea: number the points on the circle as before, and label the chords from 1 to n in the order that their smaller-numbered endpoints appear: i.e., as we go around the circle starting at point 1 and going to point $2n$, the first chord we encounter is labeled 1, the second (not yet labeled) chord is labeled 2, the third labeled 3, and so on (where we skip over the chords we have already labeled). We can then read along the circle: for each point, if it lies on a chord numbered i, move wagon number i (either from left to center or from center to right, depending upon its position). Each wagon will get moved twice: we also claim that we will never get into a situation where we cannot move wagon i because it is blocked by wagon j, where

$j > i$. For if that happened, the smaller endpoint of chord j would lie between the two endpoints of chord i on the circle, but its larger endpoint would come after them both, causing an intersection. So as long as no chords intersect, no wagons will be blocked from moving.

In this way, we have an equivalence between sets of noncrossing chords and railway wagon schedules. Each of the two mappings is the inverse of each other, and the sets of chords that do not cross correspond exactly to the railway wagon schedules in which no wagon is blocked, so either mapping is a bijection between the two sets.

(4) We defined $\binom{n}{k}$ to be the number of subset s of $\{1, 2, 3, \ldots, n\}$ with k elements. By constructing bijections between appropriate sets, prove that:

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

Show also that

(a)

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-2}{k-1} + \cdots + \binom{k-1}{k-1}$$

(b)

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$$

Solution. We define $\binom{n}{k}$ as the number of k element subsets of a set S of n elements. Fix some one element x of the n element set. Then, all k element subsets of S will either be k element subsets of $S \setminus \{x\}$ or will be the union of a $k-1$ element subset of $S \setminus \{x\}$ with $\{x\}$ (depending on whether or not they contain x). There are $\binom{n-1}{k}$ k-element subsets of $S \setminus \{x\}$, and $\binom{n-1}{k-1}$ $k-1$-element subsets of $S \setminus \{x\}$.

We repeatedly invoke the previous result:

$$\begin{aligned}
\binom{n}{k} &= \binom{n-1}{k-1} + \binom{n-1}{k} \\
\binom{n-1}{k} &= \binom{n-2}{k-1} + \binom{n-2}{k} \\
\binom{n-2}{k} &= \binom{n-3}{k-1} + \binom{n-3}{k} \\
&\cdots \\
\binom{k}{k} &= \binom{k-1}{k-1} + \binom{k-1}{k} \\
\binom{k-1}{k} &= 0
\end{aligned}$$

Combining these equalities (from the bottom up, substituting in at each step), we get our desired result.

We observe that choosing an n-element subset of a $2n$-element set is equivalent to choosing a k-element subset of the first n-elements and then an $n-k$-element subset of the remaining n-elements. So:

$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}\binom{n}{k-n} = \sum_{k=0}^{n} \binom{n}{k}^2$$

□

Additional Note: For convenience, we set $\binom{n}{k} = 0$ for $k \notin \{0, 1, \dots, n\}$. Then, we can also show the following generalization of the first argument above and of (b):

Theorem 1 (Vandermonde Identity)**.**

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

Proof. Take $N = \{1, \dots, n\}$ and $M = \{n+1, \dots, n+m\}$. Then, the LHS can be regarded as the number of k element subsets of $N \cup M$. However, any k element subset, T, decomposes as $T \cap N$ and $T \cap M$, subsets of N, M with sizes i and $k - i$. Moreover, given a subset $T_N \subset N$ and $T_M \subset M$ with $\text{Card}(T_N) + \text{Card}(T_M) = k$, we have $T_N \cup T_M$ a k element subset of $N \cup M$. Thus, we have a bijection between the k element subsets of $N \cup M$ and the pairs of $i, k - i$ element subsets of N, M respectively (letting i range from 0 to k). This establishes our result. □

This result implies the first argument above, as:

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

In addition, it (along with $\binom{n}{k} = \binom{n}{n-k}$) implies (b) as:

$$\sum_{k=0}^{n} \binom{n}{k}^n = \sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k} = \binom{n+n}{n} = \binom{2n}{n}$$

4 Fields and other things

(1) Let F be a field. Prove that the axioms for multiplication imply the following statements:
(a) If $x \neq 0$ and $xy = x$ then $y = 1$.

Solution. Suppose $xy = x$. Then

$$y = 1y = (x\frac{1}{x})y = (\frac{1}{x}x)y = \frac{1}{x}(xy) = \frac{1}{x}x = x\frac{1}{x} = 1.$$

□

(b) If $x \neq 0$ and $xy = 1$ then y is uniquely determined. Suppose $xy = 1$. Then

$$y = 1y = (x\frac{1}{x})y = (\frac{1}{x}x)y = \frac{1}{x}(xy) = \frac{1}{x}1 = \frac{1}{x}.$$

The element $\frac{1}{x}$ does not depend upon the choice of y, so y must be uniquely determined.

(c) If $x \neq 0$ and $xy = xz$ then $y = z$.

$$y = 1y = (x\frac{1}{x})y = (\frac{1}{x}x)y = \frac{1}{x}(xy) = \frac{1}{x}xz = (\frac{1}{x}x)z = (x\frac{1}{x})z = 1z = z.$$

(*Note*: This solution is very similar to those of the preceding two parts. Can you deduce both (a) and (b) from (c)?) (d) If $x \neq 0$ then $1/(1/x) = x$. The subtle first step, which almost everyone in the class forgot, is to show that $\frac{1}{x} \neq 0$, so that the left hand side is defined. Assume for the sake of contradiction that $\frac{1}{x} = 0$. Then $1 = x\frac{1}{x} = x \cdot 0 = 0x = 0$. (The last fact was proved from the axioms in class, so we will not repeat it here.) This is a contradiction, so $\frac{1}{x}$ is nonzero, so $\frac{1}{1/x}$ exists, and we can start proving things with it:

$$\frac{1}{1/x} = 1\frac{1}{1/x} = (x\frac{1}{x})1\frac{1}{1/x} = x\left(\frac{1}{x}\frac{1}{1/x}\right) = x\left(\frac{1}{1/x}\frac{1}{x}\right) = x \cdot 1 = 1 \cdot x = x.$$

(2) Prove that $\mathbb{Z}/p\mathbb{Z}$ is a field if and only if p is a prime number.

Solution. There are two things to check here: first, that when p is prime $\mathbb{Z}/p\mathbb{Z}$ is a field, and second, that $Z/p\mathbb{Z}$ is not a field when p is not prime. The first part is substantially more involved, and contains a number of subtleties that tripped up a lot of you.

In order to show that $\mathbb{Z}/p\mathbb{Z}$ is a field, one must verify the field axioms for $\mathbb{Z}/p\mathbb{Z}$, but before that we must verify that addition and multiplication are well-defined operations on $\mathbb{Z}/p\mathbb{Z}$, something we talked about a bit in class. What this means is that we must check that if a_1, a_2 belong to the same equivalence class $[a] \in \mathbb{Z}/p\mathbb{Z}$, and similarly b_1, b_2 both belong to $[b]$, the equivalence classes $[a_1 + b_1]$ and $[a_2 + b_2]$ are the same. That it, it makes sense to add the two equivalence classes $[a]$ and $[b]$ and get a single equivalence class $[a + b]$. This is just unpacking the definitions: if a_1 and a_2 are congruent mod p, we can write $a_1 - a_2 = cp$, $c \in \mathbb{Z}$, and similarly $b_1 - b_2 = dp$. Then

$$(a_1 + b_1) - (a_2 + b_2) = (a_1 - b_1) + (a_2 - b_2) = (c + d)p,$$

which is a multiple of p, so they too are also congruent mod p. Hence addition is well-defined on $\mathbb{Z}/p\mathbb{Z}$. We can do the same thing for multiplication: if $[a_1] = [a_2]$ and $[b_1] = [b_2]$, as before write $a_1 - a_2 = cp$, $b_1 - b_2 = dp$. Then

$$a_1a_2 - b_1b_2 = (a_1a_2 - a_1b_2) + (a_1b_2 - b_1b_2) = a_1cp + b_2dp,$$

which is also a multiple of p, so a_1a_2 and b_1b_2 lie in the same equivalence class mod p.

Once we've shown this, proving most of the field axioms for $\mathbb{Z}/p\mathbb{Z}$ is a breeze, because (A1) - (A4), (M1 - M4), (D) are all true in $\mathbb{Z}$. Because the addition and multiplication operations in $\mathbb{Z}/p\mathbb{Z}$ are derived directly from addition and multiplication in $\mathbb{Z}$, those nine axioms transfer over immediately. So far, we have not used the fact that p is prime, so everything above applies for $\mathbb{Z}/p\mathbb{Z}$ when p is composite as well.

The axiom (M5) is the only one we should lose any sleep over: we need to show that when (and only when) p is prime, for any nonzero element $[a] \in \mathbb{Z}/p\mathbb{Z}$, we can find an element $\frac{1}{a}$ with $a \cdot \frac{1}{a} = 1$. There is more than one way to find such an inverse (or show that one exists) and all of them are tricky. I'll show two.

The first way to prove that there are inverses mod p uses the Euclidean Algorithm (for a reference on this topic, see `http://www.cut-the-knot.org/blue/Euclid.shtml`.) You might have seen this algorithm as a way of computing GCDs, but the algorithm also implies the general result that for two integers a, b with greatest common divisor d, we can find $m, n \in \mathbb{Z}$ with $am + bn = 1$. What does this have to do with $\mathbb{Z}/p\mathbb{Z}$? Well, suppose we want to find the inverse of a nonzero element $[a] \in \mathbb{Z}/p\mathbb{Z}$ where p is prime. Then we can apply the Euclidean algorthim to the pair of integers (a, p). Because $[a] \neq [0]$, p does not divide a, and p is prime, so $\gcd(a, b)$ must be 1. The Euclidean Algorithm then tells us that there are integers m, n with $am + bp = 1$. However, when we look at things mod p, the bp term goes away: $[am + bp] = [am] = [a][m] = 1$. Hence $[m]$ is an inverse of $[a]$ mod p.

The second way is rather different. Instead of finding a specific inverse for $[a]$ mod p, we assume that there is no such thing and derive a contradiction. Indeed, if a had no inverse mod p, we could consider the p equivalence classes $[0][a], [1][a], [2][a], \ldots, [p-1][a]$. By our assumption, none of these are equal to the equivalence class $[1]$. Additionally, there are only p different equivalence classes mod p, so there are only $p - 1$ possible values that each of these equivalence classes can take on. Therefore (by the Pigenhole Principle) some two of the equivalence clases must be equal. So then suppose that $[m][a] = [n][a]$, where $m \neq n$ and m and n both lie between 0 and $p - 1$. Then

$$0 = [m][a] - [m][a] = [m][a] - [n][a] = [(m - n)a].$$

This means that $(m - n)a$ is a multiple of p, so by unique prime factorization of integers, either p divides $(m - n)$ or p divides a. (By the way, the fact that integers factor uniquely into primes is proved using the Euclidean Algorithm. You just can't escape it!) We know that p doesn't divide a because the equivalence class $[a]$ is not $[0]$. On the other hand, m and n lie between 0 and $p - 1$, so their difference is somewhere between $-(p - 1)$ and $p - 1$: but also m and n are not equal, so p cannot divide $m - n$ either. We've run into a contradiction, so our assumption that $[a]$ had no inverse mod p must be false. $\Rightarrow\Leftarrow$

What goes wrong with the proof when p is not prime? The difficulty is easiest to see in the first case: $\gcd(a, b)$ no longer has to be 1. We'll now show that (M5) fails when p is not prime. If p is 1, we get the "field" with one element, which does not really count. Otherwise, p is composite, and we can write $p = ab$, for positive integers a, b less than p. Then both equivalence classes $[a]$ and $[b]$ are nonzero. We claim that $[a]$ does not have an inverse mod p. We use an argument by contradiction: suppose not. Then there is an element $\frac{1}{[a]} \in \mathbb{Z}/p\mathbb{Z}$ with $\frac{1}{[a]} \cdot [a] = 1$. We first note that by our choice of a and b, $[a][b] = 0$ in $\mathbb{Z}/p\mathbb{Z}$. Now,

$$0 = \frac{1}{[a]} \cdot 0 = \frac{1}{[a]}([a][b]) = (\frac{1}{[a]}[a][b]) = 1[b] = [b].$$

However, we assumed that $[b]$ is nonzero, so we have a contradiction, and $\mathbb{Z}/p\mathbb{Z}$ cannot be a field. $\Rightarrow\Leftarrow$

□

(3) If r is rational ($r \neq 0$) and x is irrational, prove that $r + x$ and rx are irrational.

Solution. Assume the contrary. Say $r + x = y \in \mathbb{Q}$. Then, $x = y + (-r)$ is also rational, as the rationals are closed under negation and addition. This yields a contradiction. Say $rx = y \in \mathbb{Q}$. Then, $x = \frac{y}{r}$ is also rational, as the rationals are closed under division by non-zero elements, again yielding a contradiction. □

(4) Let A be a nonempty set of real numbers which is bounded below. Let $-A$ be the set of all numbers $-x$, where $x \in A$. Prove that $\inf A = -\sup(-A)$.

Solution. This was a fairly straightforward problem if done with care, but there were two little tricky things that tripped up a number of you between them. Some of you started talking and proving things about $\sup(-A)$ without showing that this number even existed. That is, they didn't consider the possiblity that $-A$ was not bounded below (which of course can't happen, but you need to prove that). The other one was more serious. As a general rule, if you want to show that something is the least upper bound of a set, you need to show two things: 1) that it is actually an upper bound and 2) that it is greater than or equal to any upper bound for the set. Some people only proved one of those two statements, usually 1).

Let $b = \sup A$. We are going to show that $-b = \inf(-A)$. First, we show that $-b$ is a lower bound for A. Indeed, if $c \in -A$, $-c \in A$, but A is bounded above by b, so $-c \leq b$. We now want to take negatives of this, which requires a bit of axiom work: $-c + (-b) \leq b + (-b) = 0$, so

$$-b = 0 + (-b) = (c + (-c)) + (-b) = c + (-c + -b) \leq c + 0 = c.$$

Hence $-b \leq c$. This is true for any $c \in -A$, so $-b$ is a lower bound for $-A$.

Now we need to show that if d is also a lower bound for $-A$, $d \leq -b$. For one thing, if d is a lower bound for $-A$, $d \leq -a$ for any $a \in A$, so we can take negatives (as done above) to deduce that $-d \geq a$ for any $a \in A$. Hence $-d$ is an upper bound for A: because b is the least upper bound for A, $-d \geq b$: taking negatives again, $d \leq -b$, which is exactly what we wanted.

Putting the two preceding paragraphs together, we see that $-b = \inf(-A)$, so $\sup A = -($-$inf(-A))$.

□

(5)(a) Let $z_k = \cos(\frac{2\pi k}{n}) + i\sin(\frac{2\pi k}{n}) \in \mathbb{C}$. Show that the polynomial $x^n - 1$ factors as follows:

$$x^n - 1 = \prod_{k=0}^{n-1}(x - z_k).$$

(b) A regular n-gon is inscribed in a unit circle. Label the vertices of the n-gon $v_1, v_2, \ldots, v_n$. Pick a vertex, say v_1, and take all line segments from v_1 to the rest of the vertices. Find the product of the lengths of these $(n-1)$ segments.

Solution. (a) It is a consequence of De Moivre's Theorem (`http://mathworld.wolfram.com/deMoivresIdentity.html`) that $z_k^n = \cos(\frac{2\pi k}{n}) + i\sin(\frac{2\pi k}{n}) = \cos(2\pi n) + i\sin(2\pi n) = 1$. (Equivalently, $z_k = e^{\frac{2\pi ik}{n}}$, so $z_k^n = e^{2\pi ik} = 1$.) Hence each of the z_k are roots of the polynomial $x^n - 1$, so for each z_k, $x - z_k$ divides exactly into the polynomial $x^n - 1$. This polynomial is of degree n, and it has the n distinct roots $z_0, z_1, \ldots, z_{n-1}$ ($z_n = \cos(2\pi) + \sin(2\pi) =$

$1 = z_0$, and thereafter the sequence repeats itself), so those must be of its roots. That is, $x^n - 1$ factors as

$$x^n - 1 = \prod k = 0^{n-1}(x - z_k)$$

(b) *Answer: n.* We stare at this question in bewilderment for a little while, until we realize that, because this is part of the same question as (a), there must be some sneaky way of using (a) to solve this problem. Then we stare at this question in bewilderment a little while longer. But indeed there is a sneaky way of turning this problem into problem (a)!

In order to turn a geometry problem into a complex numbers problem, we work in the complex plane, where the point (x, y) in the coordinate plane corresponds the the complex number $x + iy$. We let our unit circle be the unit circle centered at the origin in the complex plane parametrized by $\{\cos\theta + i\sin\theta \mid \theta \in \mathbb{R}\}$. Our complex numbers z_k correspond to points $(\cos(\frac{2\pi ik}{n}), \sin(\frac{2\pi ik}{n})$ for $k = 0, 1, \ldots, n-1$ lying on this unit circle. These points are spaced apart equally to form a regular n-gon inscribed in the unit circle. Taking the hint, we use this as our inscribed n-gon, so that $v_i = z_{i-1}$ for each i with $1 \leq i \leq n$. Our special vertex v_1 corresponds to the complex number $z_0 = \cos 0 + i\sin 0 = 1$. The distance of each segment connecting v_1 and v_i is the same as the absolute value of the complex number $z_0 - z_{i-1}$ (which corresponds to the vector going from v_i to v_1. Because absolute value is multiplicative, we can write the product of our lengths as

$$\prod_{i=i}^{n-1} |z_0 - z_k| = \left|\prod_{i=1}^{n-1}(z_0 - z_k)\right|.$$

Now this is an algebra problem and we have to do a couple manipulations. We want to use the result of (a). However, currently setting $x = z_0$ in (a) gives us $0 = 0$, which tells us nothing, so we have to get rid of the $x - z_0$ factor. Dividing both sides of (a) by $x - z_0 = x - 1$, we get that

$$\prod_{k=1}^{n-1}(x - z_k) = \frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \ldots + x + 1.$$

(That last step is just the formula for the sum of a finite geometric series.) At this point we can now set $x = z_0 = 1$, and we get a sum which has n copies of 1:

$$\prod_{k=1}^{n-1}(z_0 - z_k) = 1^{n-1} + 1^{n-1} + \ldots + 1^2 + 1 + 1 = n.$$

Now we only have to take absolute values, and we are done:

$$\text{product of lengths } = \left|\prod_{i=1}^{n-1}(z_0 - z_k)\right| = |n| = n,$$

which is our answer.

□