Problem Set 1

This first problem set is designed to help you gain a familiarity with set theory and basic proof techniques. By the time you're done, you should have a much stronger sense of how to rigorously establish mathematical results.

Start this problem set early. It contains eleven problems (one checkpoint question, eight graded problems, one survey question, and one optional extra credit problem), several of which require a fair amount of thought. I would suggest reading through this problem set as soon as you get it to get a sense of what it covers.

Please read Handout #02 (Problem Set Policies) and Handout #03 (CS103 and the Stanford Honor Code) before starting this problem set. These handouts contains our collaboration policy, submission instructions, and general advice on how to approach these problems.

As always, please feel free to drop by office hours or send us emails if you have any questions. We'd be happy to help out.

This problem set has 150 possible points. It is weighted at 6% of your total grade. The earlier questions serve as a warm-up for the later problems, so the difficulty of the problems increases over the course of this problem set.

Good luck, and have fun!

Checkpoint Questions Due Monday, September 30 at 2:15 PM
Remaining Questions Due Friday, October 4 at 2:15 PM

Write your solutions to the following checkpoint problems and submit them by Monday, September 30 at the start of class. These problems will be graded on a 0/12/25 scale, where

- Solutions that reasonably attempt to solve all of the problems, even if the attempts are incorrect, will receive 25 points.
- Solutions that reasonably attempt some but not all of the problems will receive 12 points.
- Solutions that do not reasonably attempt any of the problems will receive 0 points.

Essentially, if you've made a good, honest effort to solve all of the problems, you should receive 25 points even if your solutions contain errors.

Please make the best effort you can when solving these problems. We want the feedback we give you on your solutions to be as useful as possible, so the more time and effort you put into them, the better we'll be able to comment on your proof style and technique.

We will try to get these problems returned to you with feedback on your proof style this Wednesday, October 2. Submission instructions are included in the "Problem Set Policies" handout.

Checkpoint Problem: Multiples of Three (25 Points)

An integer is a *multiple of three* iff it can be written as $3k$ for some integer k. An integer is *congruent to one modulo three* iff it can be written as $3k + 1$ for some integer k, and an integer is *congruent to two modulo three* iff it can be written as $3k + 2$ for some integer k. For each integer n, exactly one of the following is true (you don't need to prove this):

- n is a multiple of three.
- n is congruent to one modulo three.
- n is congruent to two modulo three.

Suppose that we want to prove this result:

For every integer n, n is a multiple of three iff n^2 is a multiple of three.

To do this, we will prove the following two statements:

For any integer n, if n a multiple of three, then n^2 is a multiple of three.

For any integer n, if n^2 is a multiple of three , then n is a multiple of three.

i. Prove the first of these statements with a direct proof.

ii. Prove the second of these statements using the contrapositive. Make sure that you state the contrapositive of the statement explicitly before you attempt to prove it.

iii. Prove, by contradiction, that $\sqrt{3}$ is irrational. Make sure that you explicitly state what assumption you are making before you derive a contradiction from it. Recall from lecture that a rational number is one that can be written as p / q for integers p and q where $q \neq 0$ and p and q have no common divisor other than ± 1.

The remainder of these problems should be completed and returned by Friday, October 4 at the start of class.

Problem One: Set Theory Warmup (4 points)

This question is designed to help you get used to the notation and mathematical conventions surrounding sets. We strongly suggest working through this problem and checking your answers before starting Problem Two.

Consider the following sets:

$W = \{ 1, 2, 3, 4 \}$

$X = \{ 2, 2, 2, 1, 4, 3 \}$

$Y = \{ 1, \{2\}, \{\{3, 4\}\} \}$

$Z = \{ 1, 3 \}$

Answer each of the following questions and briefly justify your answers. No formal proofs are necessary.

i. Which pairs of the above sets, if any, are equal to one another?

ii. Is $Z \in W$? Is $Z \subseteq W$?

iii. Is $Z \in \wp(W)$? Is $Z \subseteq \wp(W)$?

iv. What is $W \cap Y$? How about $W \cup Y$? How about $W \Delta Y$?

v. What is $|X|$?

Problem Two: Properties of Sets (28 points)

Below are four claims about sets. For each statement, if it is always true, prove it. If it is always false, prove that it is always false. If it is sometimes true and sometimes false, provide an example for which it is true and an example for which it is false and briefly explain why your examples have these properties.

When writing your proofs for this problem, you should try as much as possible to work directly with the definitions of sets and set operations and not use results that we have not yet proven. For example, to show that one set is a subset of another, prove that all elements of the first set belong to the second set. Similarly, to prove that two sets are equal, you should show that any element of the first set must also be an element of the second set and vice versa (recall that this is equivalent to showing that the two sets are subsets of one another.) Handout #04 (Set Theory Definitions) contains formal definitions of the terms we've used so far.

The point of this question is to help you learn how to manipulate definitions in proofs, so please try to justify each step in your proofs.

i. If $A \in B$ and $B \in C$, then $A \in C$.

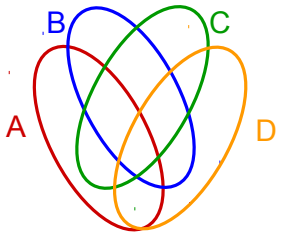
ii. If $\wp(A) = \wp(B)$, then $A = B$.

iii. $(A - B) \cup B = A$.

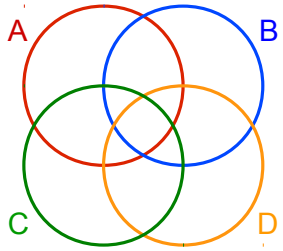
iv. $A \cap (B - A) \neq \varnothing$

Problem Three: Venn Diagrams (4 Points)

In our first lecture, we saw the following picture, which represents a Venn diagram for four sets:



This picture is probably not what you would have initially expected. It might seem more reasonable to draw the Venn diagram this way:



However, the way that these circles overlap is not sufficient to show all possible ways that four different sets can overlap. Give concrete examples of four sets A, B, C, and D such that there is no way to accurately represent the overlap of those four sets with the second Venn diagram, and briefly explain why your sets have this property.

Problem Four: Two Is Irrational? (8 points)

In lecture, we proved that $\sqrt{2}$ is irrational, and in the checkpoint problem you proved that $\sqrt{3}$ is irrational. Below is a purported proof that $\sqrt{4}$ is irrational:

> ***Theorem*:** $\sqrt{4}$ is irrational.
>
> ***Proof:*** By contradiction; assume that $\sqrt{4}$ is rational. Then there must exist integers p and q such that $q \neq 0$, $p / q = \sqrt{4}$, and p and q have no common factors other than 1 and -1.
>
> Since $p / q = \sqrt{4}$, we have $p^2 / q^2 = 4$, so $p^2 = 4q^2$. Since q^2 is an integer, we see p^2 is a multiple of four, and therefore p is a multiple of four. Thus $p = 4n$ for some integer n.
>
> Since $4q^2 = p^2$ and $p = 4n$, we have $4q^2 = (4n)^2 = 16n^2$, so $q^2 = 4n^2$. Since n^2 is an integer, we see q^2 is a multiple of four, so q is a multiple of four as well. But since both p and q are multiples of four, we get that p and q share a common divisor other than 1 and -1, contradicting our initial assumption. We have reached a contradiction, so our assumption must have been incorrect. Thus $\sqrt{4}$ is irrational. ■

This proof has to be wrong, because $\sqrt{4} = 2 = {}^2/_1$, which is indeed rational!

What error does this proof make that lets it conclude $\sqrt{4}$ is irrational? Why doesn't this error occur in the similar proofs that $\sqrt{2}$ and $\sqrt{3}$ are irrational?

Problem Five: Pythagorean Triples (12 points)

A *Pythagorean triple* is a triple (a, b, c) of positive natural numbers such that $a^2 + b^2 = c^2$. For example, (3, 4, 5) is a Pythagorean triple, since $3^2 + 4^2 = 9 + 16 = 25 = 5^2$. Similarly, (5, 12, 13) is a Pythagorean triple, as is (8, 15, 17).

Prove that if (a, b, c) is a Pythagorean triple, then $(a + 1, b + 1, c + 1)$ is ***not*** a Pythagorean triple.

Problem Six: Modular Arithmetic (24 points)

Many programming languages support a modulus operator (in some languages, using the `%` operator) that gives the remainder when one number is divided by another. For example, `5 % 3` = 2, since three divides five with remainder two. Similarly, `17 % 6` = 5.

Many different numbers yield the same remainder when divided by some number. For example, the numbers 2, 5, 8, 11, 14, and 17, all leave a remainder of two when divided by three, while the numbers 1, 12, 23, 34, and 45 all leave a remainder of one when divided by eleven. To formalize this relationship between numbers, we'll introduce a relation $\equiv_k$ that, intuitively, indicates that two numbers leave the same remainder when divided by k. For example, we'd say that $1 \equiv_{11} 12$ and that $8 \equiv_3 11$.

To be more rigorous, we'll give a formal definition of $\equiv_k$. For any integer k, we'll define $a \equiv_k b$ as follows:

$$a \equiv_k b \text{ iff there exists an integer } q \text{ such that } a - b = kq$$

For example, $7 \equiv_3 4$, because $7 - 4 = 3 = 3 \cdot 1$, and $13 \equiv_4 5$ because $13 - 5 = 8 = 4 \cdot 2$. If $x \equiv_k y$, we say that *x is congruent to y modulo k*, hence the terminology in the checkpoint problem. In this problem, you will prove several properties of modular congruence.

i. Prove that for any integer x and any integer k that $x \equiv_k x$.

ii. Prove that for any integers x and y and any integer k that if $x \equiv_k y$, then $y \equiv_k x$.

iii. Prove that for any integers x, y, and z and any integer k that if $x \equiv_k y$ and $y \equiv_k z$, then $x \equiv_k z$.

The three properties you have just proven show that modular congruence is an *equivalence relation*. Equivalence relations are important throughout mathematics, and we'll see more examples of them later in the quarter.

Modular congruence plays well with arithmetic:

iv. Prove that for any integers w, x, y, z, and k that if $x \equiv_k w$ and $y \equiv_k z$, then $x + y \equiv_k w + z$.

v. Prove that for any integers w, x, y, z, and k that if $x \equiv_k w$ and $y \equiv_k z$, then $xy \equiv_k wz$.

These last two results are important for how computers do arithmetic. Computers can't actually store arbitrarily large integers, because computers are inherently finite. Instead, when storing integers, computers typically represent them modulo some large power of two, such as 2^{32} or 2^{64}. For example, in C or C++, the **`unsigned int`** type often represents an integer modulo 2^{32}, and the **`unsigned long`** type often represents an integer modulo 2^{64}. The result that you have just proven shows that if the computer adds or multiplies numbers, the result will at least be correct modulo the large power of two, even if the actual result is too large to hold in memory.

Problem Seven: Subverting XOR Encryption (16 Points)

In lecture, we saw how to use the XOR operator (denoted $\oplus$) to encrypt a message. Let's suppose two parties (we'll call them Alice and Bob) want to communicate a secret message consisting of n bits. In advance, they agree on a secret key K (a random string of n bits). If Alice then wants to send Bob a secret n-bit message M, she and Bob can do the following:

- Alice computes $M \oplus K$ and sends it to Bob.
- Bob receives $M \oplus K$ and computes $(M \oplus K) \oplus K = M$ to recover the original message M.

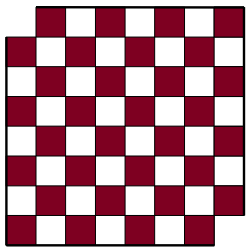
As long as the key K is chosen uniformly at random and known only to Alice and Bob, the message can't be recovered by an eavesdropper, even if the eavesdropper can see the value of $M \oplus K$. However, that doesn't mean this system is perfectly secure. Suppose Alice wants to send a message to Bob using XOR encryption. Alice and Bob have already chosen their secret key K, which you don't know. However, you do know the message Alice will send will be one of the two messages M_1 and M_2. Your goal is to trick Bob into receiving the wrong message from Alice.

When Alice encrypts the message and sends it to Bob, you intercept it before it reaches Bob. You can then tamper with the message however you'd like before sending it on to Bob. If Alice really sent message M_1, then you want Bob to receive message M_2, and if Alice really sent message M_2, you want Bob to receive message M_1.

Suppose you know $M \oplus K$ (the encrypted version of the message M that Alice sent to Bob), M_1, and M_2, but not K. Describe a procedure you can use to produce $M' \oplus K$ from these values, where M' is the message Alice didn't send (for example, if $M = M_1$, then $M' = M_2$). That way, when Bob decrypts the message, he'll get back M' instead of M. Prove that your procedure works correctly.

Problem Eight: Tiling a Chessboard (24 Points)

Suppose that you have a standard 8 × 8 chessboard with two opposite corners removed:



In the course notes (page 62), there's a proof that it's impossible to tile this chessboard using 2 × 1 dominoes. This question considers what happens if you try to tile the chessboard using *right triominoes*, L-shaped tiles that look like this:

i. Prove that it is impossible to tile an 8 × 8 chessboard missing two opposite corners with right triominoes.

ii. For $n \geq 3$, is it *ever* possible to tile an $n \times n$ chessboard missing two opposite corners with right triominoes? If so, find a number $n \geq 3$ such that it's possible and show how to tile that chessboard with right triominoes. If not, prove that for every $n \geq 3$, it's impossible to tile an $n \times n$ chessboard missing two opposite corners with right triominoes.

Problem Nine: Course Feedback (5 Points)

We want this course to be as good as it can be, and we'd appreciate your feedback on how we're doing. For a free five points, please answer the following questions. We'll give full credit for any answers to these five questions.

i. How hard did you find this problem set? How long did it take you to finish? Does that seem unreasonably difficult or time-consuming for a five-unit class?

ii. Did you attend any of the recitation sections or look over the discussion problems? If so, did you find them useful?

iii. Did you read the online course notes? If so, did you find them useful?

iv. How is the pace of this course so far? Too slow? Too fast? Just right?

v. Is there anything in particular we could do better? Is there anything in particular that you think we're doing well?

Extra Credit Problem: Symmetric Latin Squares (5 Points Extra Credit)

A *Latin square* is an $n \times n$ grid filled with the numbers 1, 2, 3, …, n such that every number appears in every row and every column exactly once. For example, the following are Latin squares:

1	2	3
3	1	2
2	3	1

4	2	1	3
1	3	2	4
3	1	4	2
2	4	3	1

1	3	5	2	4
2	4	1	3	5
3	5	2	4	1
4	1	3	5	2
5	2	4	1	3

A *symmetric Latin square* is a Latin square that is symmetric across the main diagonal. That is, the elements at positions (i, j) and (j, i) are always the same. For example:

1	2	3
2	3	1
3	1	2

4	2	3	1
2	3	1	4
3	1	4	2
1	4	2	3

1	2	3	4	5
2	4	5	3	1
3	5	2	1	4
4	3	1	5	2
5	1	4	2	3

Prove that in any $n \times n$ symmetric Latin square where n is odd, every number 1, 2, 3, …, n must appear exactly once on the diagonal from the upper-left corner to the lower-right corner.