Theory of Computation
Problem Set 2
Universidad Politecnica de San Luis Potosi

TPlease start solving these problems immediately, don’t procrastinate, and work in study groups. Please do not simply copy answers that you do not fully understand;

Advice: Please try to solve the easier problems first (where the meta-problem here is to figure out which are the easier ones). Don’t spend too long on any single problem without also attempting (in parallel) to solve other problems as well. This way, solutions to the easier problems (at least easier for you) will reveal themselves much sooner (think about this as a “hedging strategy” or “dovetailing strategy”).

Checkpoint Question: Multiples of Three (25 Points if Submitted)

A number is a *multiple of three* iff it can be written as $3k$ for some integer k. A number is *congruent to one modulo three* iff it can be written as $3k + 1$ for some integer k, and a number 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:

n is a multiple of three iff n^2 is a multiple of three.

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

If n is a multiple of three, then n^2 is a multiple of three.

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 5 at the start of class.

Problem One: Elementary Set Theory (4 points)

For the purposes of this problem, suppose that we are dealing with the following sets:

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

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

$C = \{ 1, 3 \}$

$D = \{ 2, 3, 4 \}$

$E = \{ x \mid x \in \mathbb{N} \text{ and } x \text{ is even} \}$

For each of the following, is the claim true or false? Explain why. You do not need to prove your assertions.

i. $A = B$.

ii. $C \mathbin{\Delta} D = C$

iii. $|D| > |A|$

iv. $E \cap D = C \cap D$

v. $C \in A$.

vi. $C \subseteq A$.

Problem Two: Two Is Irrational? (12 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 that $p^2 / q^2 = 4$, so $p^2 = 4q^2$. This means that p is a multiple of four, so $p = 4n$ for some natural number n.
>
> Since $4q^2 = p^2$ and $p = 4n$, this means that $4q^2 = (4n)^2 = 16n^2$, so $q^2 = 4n^2$. This means that q is a multiple of four as well. But since both p and q are multiples of four, this means 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! Specifically, this proof contains two invalid steps that let it claim that $\sqrt{4}$ is irrational. What are the two invalid steps? Why doesn't this error occur in the similar proofs that $\sqrt{2}$ and $\sqrt{3}$ are irrational?

Problem Three: Properties of Sets (20 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 are correct.

To prove that two sets are equal, remember that you need to 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. It is **not** sufficient to use Venn diagrams or any other informal reasoning here. You need to formally prove each result.

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

Problem Four: Ascending Sequences (12 points)

Suppose that you have an infinite sequence of real numbers x_0, x_1, …, x_n, … such that for any natural numbers i and j, if $i < j$, then $x_i < x_j$. Such a sequence is called an *ascending sequence*. For example, the series of natural numbers 0, 1, 2, 3, 4, … is such a sequence, as is the series 1, 2, 4, 8, 16, 32, … of powers of two.

Suppose that you have some number z that is sandwiched in-between two of the terms in the series; that is, there is some j such that $x_j < z < x_{j+1}$. Prove that z does not appear anywhere in the series by showing that there is no i such that $x_i = z$.

Problem Five: Pythagorean Triples (16 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 (28 points)

Many programming languages support a modulus operator (in many languages, using the `%` operator), which 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 $8 \equiv_3 11$.

Formally, we'll define $\equiv_k$ as follows. For any integer k, define the relation $\equiv_k$ 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, $x \equiv_k x$.

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:

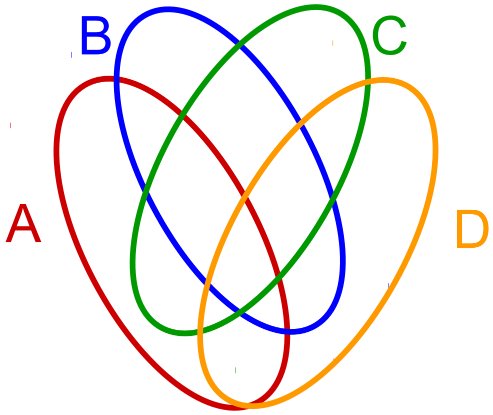
iv. Prove that for any integers w, x, y, z, and k, that if $x \equiv_k w$ and $y \equiv_k z$, then $x + y \equiv_k w + z$.

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

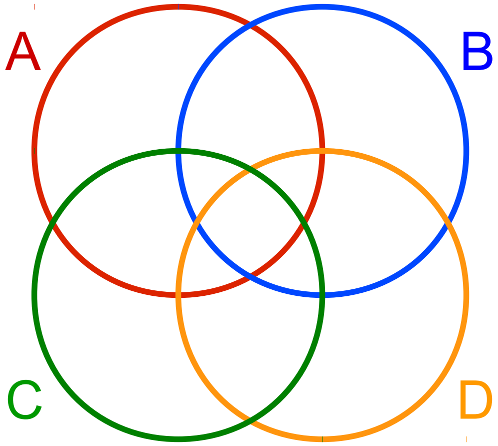
These last two results are important for how computers do arithmetic. Computers can't actually store arbitrarily large integers, because computers are inherently finite. Instead, when storing integers, computers typically represent them modulo some large power of two, such as 2^{32} or 2^{64}. For example, 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: Venn Diagrams (8 Points)

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



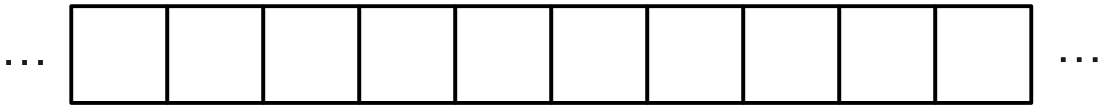
This picture is probably not what you would have initially expected. It might seem more reasonable to draw the Venn diagram this way:



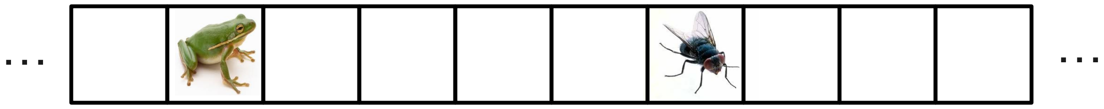
However, the way that these circles overlap is not sufficient to show all possible ways that four different sets can overlap. Come up with four sets *A*, *B*, *C*, and *D* such that there is no way to accurately represent the overlap of those four sets with the second Venn diagram, and briefly explain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

Problem Eight: The Quantum Frog (20 Points)

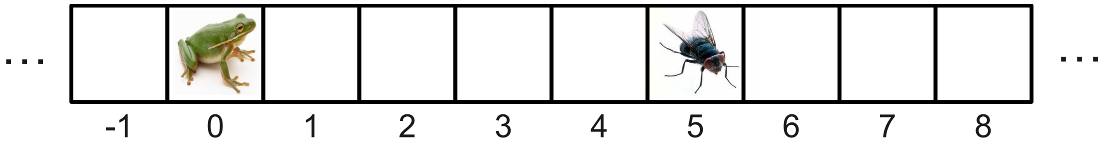
Imagine an infinitely long sequence of squares, such as below:



One of these squares contains a frog, and another square contains a fly:



For simplicity, let's number all of the (infinitely many) squares by assigning each an integer. We'll say that the frog starts in position 0, and will assign positive integers to the squares to the right of the frog and negative numbers to the squares to the left of the frog. For example:



Now this frog is a very special kind of frog called a *quantum frog*. The quantum frog can hop across the squares forward and backward, but can only make jumps of two different lengths: 3 and 7. For example, to get to square five to eat the fly, the frog might might jump forward seven squares to square 7, forward seven squares again to square 14, then back three squares three times to squares 11, 8, and (finally) 5.

i. Prove that, starting at position 0, the quantum frog can move to any other square using only jumps of length 3 and 7.

Suppose that this quantum frog is very concerned about catching the fly as early as possible (this is a hungry quantum frog!) and wants to minimize the number of jumps she has to make to get from her starting point to the fly. All jumps take the same amount of time (this is, after all, a quantum frog!), so all the frog cares about is the total number of jumps made. We'll say that a series of jumps from square 0 to square k is ***optimal*** iff there is no series of fewer jumps that, starting from square 0, also arrives at square k.

ii. Prove that in an optimal series of jumps from square 0 to square k, all jumps of the same distance must be made in the same direction. That is, all of the frog's jumps of distance 3 must be in the same direction and all of the frog's jumps of distance 7 must be in the same direction (though these two directions don't have to be the same).

iii. Prove that in an optimal series of jumps from square 0 to square k, the frog can never use jumps of size three more than six times.

Your results from (i), (ii), and (iii) can be used to devise a very efficient algorithm for finding the shortest number of hops required. Since you know that there can't be more than six jumps of size three and that all those jumps have to go in the same direction, you can just check, for each possible set of up to six jumps in each direction, how many remaining seven-hop jumps would be necessary. The minimum over all these options is the shortest sequence of jumps.