Proofs by Contrapositive/Contradiction

August 31, 2021

Question 1

a) Suppose $a, b, c \in \mathbb{Z}$. Show that if a does not divide bc then a does not divide b.
b) We call n a perfect square if $n = k^2$ for some integer k. Show that if $n \equiv 2 \bmod 4$ or $n \equiv 3 \bmod 4$ then n is not a perfect square.

Question 2

a) If A and B are sets, show that $A \cap (B - A) = \phi$
b) Show there are no integer solutions to the equation $x^2 - y^2 = 1$.

Question 3
a) Prove that if n is an integer, then $2n^2 + 3n + 2$ is not divisible by 5.
b) Suppose that a,b are integers. Show that $a \equiv b \bmod 10$ iff $a \equiv b \bmod 2$ and $a \equiv b \bmod 5$.

Question 4- Challenge Question
Modular arithmetic with a view towards group theory.
For a given n, we can consider the congruence classes mod n, and we denote it Z/nZ or Z_n. Namely $Z_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ where each $\overline{i}$ is a "representative" of each congruence class.
For example $Z_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ where $\overline{0} = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$, $\overline{1} = \{\ldots, -9, -4, 0, 1, 6, \ldots\}$ and so on.
We can add elements in Z_n by declaring an addition $\overline{i} + \overline{j} = \overline{i+j}$. (For example $\overline{2} + \overline{3} = \overline{0}$ in Z_5.)
Show that for each $n \in \mathbb{Z}$ the following is true for Z_n

a) There exists a congruence class $\overline{x}$ such that $\overline{i} + \overline{x} = \overline{i}$ for any congruence class $\overline{i}$. We call such a class x the identity and denote it $\overline{e}$

b) For each congruence class $\overline{i}$, there exists a congruence class $\overline{j}$ such that $\overline{i} + \overline{j} = \overline{e}$. This shows that each element has an inverse.

These conditions (and checking that addition is associate) verify that Z_n is what is called "a group". The study of things that can be made into groups will occupy much of your further mathematical courses, as it turns out groups pop up just about everywhere (it is also what I study).
One can also define a multiplication on Z_n (think about how to do this) and this multiplication turns Z_n into something called a ring. Much of the proofs we have done involving modular arithmetic thus far are really statements about groups and rings in general, and can be greatly generalized.