More on Proofs

November 10, 2019

Question 1

a) Show that for any x $\in \mathbb{Z}, x^2 \equiv 0 \bmod 3$, or $x^2 \equiv 1 \bmod 3$. Furthermore, show that $x^2 \equiv 0 \bmod 3$ iff $x \equiv 0 \bmod 3$.
b) Suppose some number p $\in \mathbb{Z}$ has the property that whenever $p|ab$ for two numbers $a, b \in \mathbb{Z}$ then $p|a$ or $p|b$. Show this number p is prime. This is the converse to your homework question, showing that this is in fact an iff statement.
c) Show that if $x^2 + y^2$ is a perfect square, then x and y can't both be congruent to 1 (mod 4). (Hint, recall problem 1b from last week)

Question 2

a) Prove that $\{9^n : n \in \mathbb{Z}\} \subseteq \{3^n : n \in \mathbb{Z}\}$. Are the sets equal?
b) If A,B,C are sets, show that $(A \cap B) - C = (A - C) \cap (B - C)$

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- Supplemental Question
Modular arithmetic as an equivalence relation.
We say an operation $\sim$ is an "equivalence relation" on a set X if the following three conditions hold:

1) a $\sim a$ for any a in X. (called Reflexive)

2) if a $\sim b$ then $b \sim a$ (Called symmetric)
3) if a $\sim b, b \sim c$ then $a \sim c$ (called transitive)

For example, equality of numbers is an equivalence relation on the integers. If a set X has an equivalence relation then X is "partioned" (ie, broken up) into distinct (ie, disjoint) bits called equivalence classes, denoted $[x]$ or $\overline{x}$. In other words, for each y in X $y \in [x]$ for some x in X. We write this new set as $X/\sim$. Morally, we are creating a new set where we are squishing together all objects of the old set that "equaled" each other into a single object. Ok, here comes the actual question;
Show that for a fixed n $\in \mathbb{N}$ congruence (mod n) is an equivalence relation on the set $\mathbb{Z}$.
The equivalence classes under this equivalence relation are exactly the $\overline{x}'s$ I defined last challenge problem. Under our new notation, we have $\mathbb{Z}/$ (mod n) $=$ Z_n which explains the two notations I used last week. If you didn't attempt the challenge problem last week, go back to it now and see if it makes more sense.