PROOF LAB III: CONTRADICTION

Problems. Prove each of the following using proof by contradiction.

I. ($\star$) For two integers a and b, assume that $4|(a^2+b^2)$. Then at least one of a or b is even.

Hint: Then negation of "at least one of a or b is even" is "a and b are both odd". So start with, "Suppose a and b are odd, so that $a = 2k+1$ and $b = 2\ell + 1$ for some $k, \ell \in \mathbb{Z}$."

II. ($\star$) Let $a, b, c \in \mathbb{Z}$. Assume that $\gcd(a, b) = 1$ and $ab = c^2$. Then both a and b are squares of integers.

Hint: Consider the prime factorizations of a, b, and c.

III. ($\star\ \star$) Let $\triangle ABC$ be a right triangle. Then at least one of the sides has either non-integer length or even-integer length.

[Hint: Start by drawing a picture, and writing a corresponding equation about the lengths of the triangle's sides. Then rewrite the statement "At least one of the sides has either non-integer length or even-integer length" as an if-then statement.]

Hint: Call the sides of the right triangle a, b, and c, with c being the length of the hypotenuse. Thus $a^2 + b^2 = c^2$. Now we can rewrite "At least one of the sides has either non-integer length or even-integer length" as "If $a, b, c \in \mathbb{Z}$ then at least one of a, b, or c is even." Therefore the negation is "There exists a solution $a, b, c \in \mathbb{Z}$ such that a, b, and c are all odd."

IV. ($\star\ \star$) The none of the roots of $f(x) = x^3 + x + 1$ are rational.

Hint: The negation of "none of the roots are rational" is "there exists a rational root." So start with "Let $x \in \mathbb{Q}$ satisfy $x^3 + x + 1 = 0$. Since $x \in \mathbb{Q}$, there exist $a, b \in \mathbb{Z}$ such that $x = a/b$."

V. ($\star\ \star$) Let $n > 1$ be a positive integer that is not prime (i.e. is *composite*). Then n has a prime divisor less than or equal to $\sqrt{n}$.

Hint: We have proven that every positive integer has a prime factorization, so start with "Since $n \in \mathbb{Z}_{>1}$, we can write $n = p_1 \cdots p_\ell$ for some (not necessarily distinct) primes $p_1, \ldots, p_\ell$. And since n is composite, $\ell \geq 2$." Then the negation of "n has a prime divisor less than or equal to $\sqrt{n}$" is "$p_i \geq \sqrt{n}$ for all i."

VI. Pick one:

($\star$) If x and y are positive real numbers, then $\sqrt{x+y} \neq \sqrt{x} + \sqrt{y}$.

($\star\star\star$) If x and y are non-zero real numbers, then $\sqrt{x+y} \neq \sqrt{x} + \sqrt{y}$.

Hint: Why is the second part worth *so* many more stars? Well, in the positive real numbers, $x \mapsto \sqrt{x}$ is a function; where we always map x to the positive real number whose square is x. But if x is a negative real number, then when we go to take a square root, we find that we're actually living in $\mathbb{C}$. And in $\mathbb{C}$, $x \mapsto \sqrt{x}$ isn't a function. Namely, $\sqrt{x}$ stands for any solution to the equation $y^2 = x$ (x is fixed; solve for y). So the added difficulty isn't in the problem solving or setting up the contradiction; it's in the care that you must take in *writing* the solution. The danger is in getting a 0 on the "fluency" and "validity" portions.

VII. ($\star\star\star$) Let $A \subseteq \mathbb{R}$. We say A is *dense* in $\mathbb{R}$ if for every open interval $(a,b) = \{x \in \mathbb{R} \mid a < x < b\}$ in $\mathbb{R}$, there is at least one element of A in (a,b), i.e. $(a,b) \cap A \neq \emptyset$.

Claim: The set of rational numbers $\mathbb{Q}$ and the set of irrational numbers $X = \mathbb{R} - \mathbb{Q}$ are both dense in $\mathbb{R}$.

[Note: This basically, is a two-part problem—(1) show $\mathbb{Q}$ is dense in $\mathbb{R}$, and (2) show $\mathbb{R} - \mathbb{Q}$ is dense in $\mathbb{R}$. You do not *have* to prove both by contradiction—you are just required to use proof by contradiction somewhere in your proof.]

Hint: Let (x,y) be an interval in $\mathbb{R}$. For (1), since $y > x$, we have $y - x > 0$. Let n be the smallest integer strictly greater than $1/(y-x)$ (in particular, $n \geq 1$). Then $0 < 1/n < y - x$. Can you prove that the intersection of $\{m/n \mid m \in \mathbb{Z}\}$ and (a,b) is non-empty?

For (2), show that $\mathbb{Q} + \sqrt{2} = \{x + \sqrt{2} \mid x \in \mathbb{Q}\}$ is a subset of $\mathbb{R} - \mathbb{Q}$ (every number of the form $m/n + \sqrt{2}$ with $m, n \in \mathbb{Z}$ is irrational); and then show $\mathbb{Q} + \sqrt{2}$ is dense in $\mathbb{R}$.