Math 311 - Introduction to Proof and Abstract Mathematics
Group Assignment # 8 **Name:**_____
Due: Tuesday, September 25th

Without Loss of Generality: The phrase "without loss of generality" is a phrase (and principle) that we often use when writing proofs in order to eliminate unnecessary cases and to simplify our arguments. Although it is quite useful, it should be used with caution, since when using it, we are claiming that the "simplifying assumption" we are making does not impact the "generality" of our proof. That is, the cases we eliminate should be able to be proven by nearly identical arguments that only involve renaming or reordering the elements involved. This type of simplification is common enough that some even abbreviate it by writing WLOG.

Example: On Group Assignment #6 problem #1b we built an argument starting from the fact that x and y were distinct positive integers. In order to simplify our notation (and proof), we could make the following simplifying assumption: Without loss of generality, suppose that $x > y$. The idea here is that we know x and y are different, so one of them must be bigger. It does not really matter which one is bigger (it is only a matter of labeling), so we simply declare that x names the bigger of the two). This allows us to write $x - y > 0$ rather than having to consider two separate cases: $x - y > 0$ and $y - x > 0$.

Theorem 2.3.1 $\sqrt{2}$ is irrational.

Proof: Suppose, in order to obtain a contradiction, that $\sqrt{2}$ is rational. Then, by definition, we may write $\sqrt{2} = \frac{p}{q}$ with $p, q \in \mathbb{Z}$. WLOG, assume that the fraction $\frac{p}{q}$ has been written so that p and q have no common factors other than 1.

Since $\sqrt{2} = \frac{p}{q}$, then, squaring both sides, we have $2 = \frac{p^2}{q^2}$. Multiplying both sides by q^2 gives $2q^2 = p^2$. Notice that this means p^2 is even, and hence p must be even. Since p is even, $p = 2k$ for some integer k. then $p^2 = 4k^2$, so we have $2q^2 = p^2 = 4k^2$, or, dividing both sides by 2, $q^2 = 2k^2$. From this, we see that q^2 is even, and hence q is also even.

Notice that since p and q are both even, they have a common factor of 2. This contradicts the fact that p and q, as chosen, have no common factors. Since we have reached a contradiction, our initial assumption that $\sqrt{2}$ is rational must be false. Hence $\sqrt{2}$ is irrational. $\square$.

1. Prove that for all integers n, if $3|n^2$, then $3|n$ [Hint: use proof by contraposition].

2. Use the previous problem and ideas from the proof of Theorem 2.3.1 to prove that $\sqrt{3}$ is irrational.

Recall: Definition 2.3.2 A positive integer p is **prime** if $p > 1$ and $(\forall m, n, \in \mathbb{Z}^+)[p = mn \Rightarrow (m = 1 \vee n = 1)]$

Theorem 3.3 (Fundamental Theorem of Arithmetic Every positive integer greater than 1 can be written as a product of primes. Furthermore, this product of primes is unique, up to the order in which the factors appear.

Note: We will postpone the proof of this result until later in the course. to prove it, we will need to use a proof technique called Strong Induction.

Theorem 2.3.4 (Euclid) There are an infinite number of prime numbers.

3. The goal of this next series of exercises is to develop a proof of Theorem 2.3.4. I will get you started, outline the proof, and provide some of the details. The rest will be completed by you.

   Proof: Suppose, in order to obtain a contradiction, that there is only a finite number of prime numbers. Since there are only finitely many primes, we can list them all in strictly increasing order. Therefore, we can suppose that $p_1, p_2, p_3, \cdots, p_k$ for some $k \in \mathbb{N}$ is a complete listing of all prime numbers with $1 < p_1 < p_2 < \cdots < p_k$.

   Suppose that $n = p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_k + 1$ (the product of all k primes plus 1)

   (a) Explain why we must have $n > p_k > 1$.

   (b) Explain why the previous fact implies that n is not prime.

   Since n is not prime, by the Fundamental Theorem of Arithmetic (Theorem 2.3.3), some prime number must divide n (n is a product of primes and is not prime). Therefore, we must have $n = p_j \cdot m$ for some specific j with $1 \leq j \leq k$ and some $m \in \mathbb{N}$. Therefore, we have $n = p_j \cdot m = p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_k + 1$.

   (c) Show that p_j cannot evenly divide $p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_k + 1$

   On one hand, since $n = p_j \cdot m$ for $m \in \mathbb{N}$, we have $p_j | n$. On the other hand, p_j does not divide $n = p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_k + 1$. This is a contradiction, so our initial assumption that there are only a finite number of primes is false. Hence there must be an infinite number of primes. $\square$.

Note: If you have time remaining, you may work on the assigned homework problems from your textbook in your group.