Students, insert your header here (including name, date, section number, etc.).

The goal of this project is to prove the following proposition:

Proposition 1 (Main proposition)**.** *If p is prime, then $\sqrt{p}$ is irrational.*

We will prove this result by first establishing two lemmas. These results are useful in their own right in the study of number theory.

Lemma 1. *Suppose $a, b \in \mathbb{Z}$. Then there exists a linear combination of a and b equal to $\gcd(a, b)$. In other words, there exist integers c_1 and c_2 such that*

$$c_1 a + c_2 b = \gcd(a, b).$$

Example 1. *Say $a = 5$ and $b = 12$. Then $\gcd(a, b) = \gcd(5, 12) = 1$. Lemma 1 guarantees the existence of c_1 and c_2 so that $c_1 \cdot 5 + c_2 \cdot 12 = 1$. As expected, the Lemma holds, since if we let $c_1 = 5$ and $c_2 = -2$, then*

$$c_1 a + c_2 b = 5 \cdot 5 - 2 \cdot 12 = 1.$$

Example 2. *Say $a = 6$ and $b = 10$. Students, complete Example 2, following the format of Example 1.*

Proof of Lemma 1. Students: On the last page of this document are the steps for this proof, but in scrambled order. Print out the .pdf file for this document, cut up the steps and rearrange them to produce a valid proof of Lemma 1. Then insert the unscrambled latex code here (with spaces removed) to create a complete proof of Lemma 1.

■

Lemma 2 (Lemma 2)**.** *Suppose a and b are integers and p is prime. If $p|ab$ then $p|a$ or $p|b$.*

Proof of Lemma 2. Students, insert your proof of Lemma 2 here. ■

Corollary 1. *Suppose $a \in \mathbb{Z}$ and p is prime. If $p|a^2$ then $p|a$.*

Proof of Corollary. Students, insert your short proof of the above Corollary here ■

Proof of main proposition. Students, insert your proof of the main proposition here ■

We know $d = c_1a + c_2b$, so substituting gives $d = c_1nf + c_2mf = f(c_1n + c_2m)$

Define the set $S = \{k_1a + k_2b : k_1, k_2 \in \mathbb{Z}, k_1a + k_2b > 0\}$. In other words, S is the set of all linear combinations of a and b that are positive.

So d is the greatest common divisor of a and b.

By way of contradiction assume f is common divisor of a and b, and $f > d$.

But d is the smallest positive linear combination of a and b. We also know that $0 \leq r < d$. So this means $r = 0$.

This shows r is a linear combination of a and b.

By the definition of divisor, There are integers n and m such that $nf = a$ and $mf = b$.

Since $d \in S$, There exist integers c_1 and c_2 such that $d = c_1a + c_2b$.

We conclude that $\gcd(a, b) = d = c_1a + c_2b$, as was to be shown.

Now we will first prove that $d|a$.

Solving, substituting and rearranging gives the following:

$$\begin{aligned} r &= a - dq \\ &= \textit{Students fill in this line} \\ &= (1 - qc_1)a - c_2qb \end{aligned}$$

Thus $f|d$. But this means $f \leq d$, a contradiction.

Suppose that $a, b \in \mathbb{Z}$.

Let d be the smallest element of S.

In an identical manner, we can show $d|b$. So d is a common divisor of a and b.

Substituting gives $a = dq + 0$, and thus $d|a$.

We will now prove that d is the *greatest* common divisor of a and b.

By the division algorithm, there exist integers q and r such that $a = dq + r$, where $0 \leq r < d$.
