Definition (Rosen p. 257): An integer p greater than 1 is called **prime** means the only positive factors of p are 1 and p. A formal definition of the predicate Pr over the domain $\mathbb{Z}$ which evaluates to T exactly when the input is prime is: $(x > 1) \wedge \forall a(\ (\ a > 0 \wedge F(a, x)\ ) \rightarrow (a = 1 \vee a = x)\ )$

New! Proof by Contradiction (Rosen 1.7 p86)
To prove that a statement p is true, pick another statement r and once we show that $\neg p \rightarrow (r \wedge \neg r)$ then we can conclude that p is true.

Extra examples: Prove or disprove that $\mathbb{N}$, $\mathbb{Q}$ each have a least and a greatest element.

Prove or **disprove** the following claims:

Claim: There is a greatest integer. *Approach 1*: *Approach 2*:	Claim: There is a least integer.
Claim: There is a greatest prime number.	Claim: There is a least prime number.

The **set of rational numbers**, $\mathbb{Q}$ is defined as

$$\left\{ \frac{p}{q} \mid p \in \mathbb{Z} \text{ and } q \in \mathbb{Z} \text{ and } q \neq 0 \right\} \quad \text{or, equivalently,} \quad \{x \in \mathbb{R} \mid \exists p \in \mathbb{Z} \exists q \in \mathbb{Z}^+ (p = x \cdot q)\}$$

Extra practice: Use the definition of set equality to prove that the definitions above give the same set.

Goal: The square root of 2 is not a rational number. In other words: $\neg \exists x \in \mathbb{Q}(x^2 - 2 = 0)$

Attempted proof: The definition of the set of rational numbers is the collection of fractions p/q where p is an integer and q is a nonzero integer. Looking for a **witness** p and q, we can write the square root of 2 as the fraction $\sqrt{2}/1$, where 1 is a nonzero integer. Since the numerator is not in the domain, this witness is not allowed, and we have shown that the square root of 2 is not a fraction of integers (with nonzero denominator). Thus, the square root of 2 is not rational.

The problem in the above attempted proof is that _____

Proof:

Lemma 1: For every two integers p and q, not both zero, $gcd\left(\frac{p}{gcd(p,q)}, \frac{q}{gcd(p,q)}\right) = 1$.

Lemma 2: For every two integers a and b, not both zero, with $gcd(a, b) = 1$, it is not the case that both a is even and b is even.

Lemma 3: For every integer x, x is even if and only if x^2 is even.

Greatest common divisor (Rosen 4.3 p265) Let a and b be integers, not both zero. The largest integer d such that d is a factor of a and d is a factor of b is called the greatest common divisor of a and b and is denoted by $gcd(a, b)$.