

Section 3.7: Two Classical Theorems

1. Ancient Greeks thought that for any line segments A and B , $\exists a, b \in \mathbb{Z}$ s.t. $\frac{\text{length } A}{\text{length } B} = \frac{a}{b}$.
2. This would imply that $\sqrt{2}$ is rational, since it's the ratio of the lengths of the hypotenuse and side of a square with side length 1.
3. Theorem 3.7.1: $\sqrt{2}$ is irrational. (Proof known to Aristotle and to Euclid in *Elements of Geometry*)
pf.
 - Suppose $\exists m, n \in \mathbb{Z}$ s.t. $\sqrt{2} = \frac{m}{n}$, where m and n have no common factors.
 - Hence $2 = \frac{m^2}{n^2}$ or $m^2 = 2n^2$, which implies that m^2 is even.
 - Proposition 3.6.4 hence implies that m^2 is even $\Rightarrow m = 2k$ for some $k \in \mathbb{Z}$.
 - Hence, $m^2 = (2k)^2 = 4k^2 = 2n^2 \Rightarrow n^2 = 2k^2$.
 - It follows that n^2 and consequently n must be even.
 - But m is also even, so m and n have 2 as a common factor. **C!**
4. Example #1: Prove that $3 - 5\sqrt{2}$ is irrational (by Contradiction).
5. Euclid's *Elements* Book 9 (of 10) also established that there are infinitely many primes. (Books 1-6 are Geometry, and Books 7-10 are Number Theory.)
6. Proposition 3.7.3: For any $a \in \mathbb{Z}$ and any prime p , if $p \mid a$ then $p \nmid (a + 1)$.
pf.
 - Suppose not $\Rightarrow \exists a \in \mathbb{Z}$ and prime p s.t. $p \mid a$ and $p \mid (a + 1)$.
 - Hence, $\exists k, \ell \in \mathbb{Z}$ s.t. $a = pk$ and $a + 1 = p\ell$.
 - Thus, $1 = (a + 1) - a = p(k - \ell) \Rightarrow p \mid 1 \Rightarrow p = \pm 1$. **C!**
7. Theorem 3.7.4: There are infinitely many prime numbers.
pf.
 - Suppose the set of primes is finite \Rightarrow can be listed: $p_1 = 2, p_2 = 3, p_3 = 5, \dots, p_n$.
 - Consider $N = p_1 p_2 p_3 \cdots p_n + 1$.
 - $N > 1$, Theorem 3.3.2 $\Rightarrow N$ is divisible by a prime p (must be p_1, p_2, \dots , or p_n).
 - Hence $p \mid (p_1 p_2 \cdots p_n)$.
 - Proposition 3.7.3 $\Rightarrow p \nmid (p_1 p_2 \cdots p_n + 1) \Rightarrow p \nmid N$. **C!**
8. Using Direct or Indirect Proof:
Many theorems can be proved both ways. If not obvious, first try to prove directly. Then look for a counterexample. Then, prove by contradiction/contrapositive.

9. Open Questions in Number Theory:

- Are there infinitely many Mersenne primes: $2^p - 1$?
- Are there infinitely many Fermat primes: $2^{2^n} + 1$?
- Are there infinitely many primes of the form $n^2 + 1$, where $n \in \mathbb{Z}^+$?
- Is there always a prime between n^2 and $(n + 1)^2$?
- In 1844, Catalan conjectured that the only solution to $x^n - y^m = 1$ where $x, y, n, m \in \mathbb{Z}, > 1$ is $3^2 - 2^3 = 1$.
- Beal's Conjecture (\$100,000 prize): No solutions exist to $x^m + y^n = z^k$, where no two of x, y , or z have common factors other than ± 1 .