Math 406 Section 3.1: Prime Numbers - Basic Facts

1. **Introduction:** When studying the integers the place to start is with the prime numbers. The reason for this is that the prime numbers form a set of building blocks for all integers and so proving things about all integers often comes down to proving things about primes. First we'll define primes and make some statements about them.

2. **Definition:** An integer greater than 1 is *prime* if its only divisors are 1 and itself. If an integer greater than 1 is not prime then it is *composite*. In other words $n > 1$ is composite if $n = ab$ for $a, b \in \mathbb{Z}$ with $a, b > 1$. Note that integers less than or equal to 1 do not technically fall into either category.

3. **Theorem:** Every integer greater than 1 has a prime divisor.

   Proof: We proceed by well-ordering. Suppose the statement is false. Define the set

   $$S = \{n \in \mathbb{Z} \,|\, n > 1 \text{ and } n \text{ has no prime divisors}\}$$

   By assumption S is nonempty and therefore has a least element m. Since m has no prime divisors but $m \mid m$ we know that m itself is not prime and hence $m = ab$ with $a, b > 1$. Since $1 < a < m$ we know that $a \notin S$ and hence a has a prime divisor so $p \mid a$. But since $a \mid m$ we have $p \mid m$, a contradiction. $\mathcal{QED}$

4. **Theorem:** There are infinitely many primes.

   Proof: By way of contradiction suppose this is false and that there are only finitely many primes. List them as $p_1, p_2, ..., p_n$.

   Construct the integer:

   $$P = 1 + p_1 p_2 ... p_n$$

   We know that P has a prime divisor and it must be one of the p_i because that's all there are. But if $p_i \mid P$ and $p_i \mid (p_1 ... p_n)$ then $p_i \mid 1$, a contradiction. $\mathcal{QED}$

5. **Theorem:** If $n \in \mathbb{Z}$ is composite then n has a prime factor less than or equal to $\sqrt{n}$.

   Proof: Since n is composite we know $n = ab$ with one of a, b less than or equal to $\sqrt{n}$. Suppose $1 < a \leq \sqrt{n}$. Since a has a prime factor $p \leq a$ we have $p \mid a$ and $a \mid n$ so $p \mid n$ and we have $p \leq a \leq \sqrt{n}$. $\mathcal{QED}$

   Note: Keep this in mind when checking primality. If we want to check if 653 is prime we only need to check prime divisors up to and including $\sqrt{653} \approx 25.5539$, meaning we only need to check $2, 3, 5, 7, 11, 13, 17, 19, 23$ and some of these are really obvious.

6. **Theorem (Dirichlet's Theorem on Primes in Arithmetic Progressions):** Suppose $a, b \in \mathbb{Z}^+$ with $\gcd(a, b) = 1$. Then the sequence:

   $$a + b, a + 2b, a + 3b, ...$$

   contains infinitely many primes.

   Proof: LOL hard nope. $\mathcal{QED}$

7. **Fact:** As of January 2020 the largest known prime is $2^{82589933} - 1$, discovered in 2018. This number has 24862048 digits.