Week 5 List of Theorems

Here we stop repeating theorems from all previous weeks. Instead we try to contain the relevant weekly theorems in a single file. Notice that the techniques up to week 4 will be important throughout the course.

Fundamental Theorem of Arithmetic (UFT) [Some classes will do this in week 6]
Every integer greater than 1 can be uniquely expressed as a product of primes (apart from the order of the factors).

Infinitely Many Primes (INF P) (known as Euclid's Theorem outside of MATH 135)
The number of primes is infinite.

Finding a Prime Factor (FPF) [Some classes will do this in week 6]
An integer $n > 1$ is either prime or contains a prime factor less than or equal to $\sqrt{n}$.

GCD With Remainders (GCD WR)
Let $a, b, q, r \in \mathbb{Z}$. If $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.

GCD Characterization Theorem (GCD CT)
Let $a, b \in \mathbb{Z}$. If d is a positive common divisor of a and b, and $ax + by = d$ has an integer solution, then $d = \gcd(a, b)$.

Extended Euclidean Algorithm (EEA) (known as Bézout's Lemma outside of MATH 135)
Let $a, b \in \mathbb{Z}$. If $d = \gcd(a, b)$, then d can be computed and there exist $x, y \in \mathbb{Z}$ such that $ax + by = d$.

Primes and Divisibility (PAD) [Some classes will do this in week 6] (known as Euclid's Lemma outside of MATH 135)
If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.