Week 6 List of Theorems

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 $p \mid b$.

GCD of One (GCD OO)
Let $a, b \in \mathbb{Z}$. Then $\gcd(a, b) = 1$ if and only if there exist integers x and y with $ax + by = 1$.

Division by GCD (DB GCD)
Let $a, b \in \mathbb{Z}$, not both 0. If $d = \gcd(a, b)$, then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Coprimeness and Divisibility (CAD)
Let $a, b, c \in \mathbb{Z}$. If $c \mid ab$ and a, c are coprime, then $c \mid b$.

Divisors from Prime Factorization (DFPF)
If x can be written as $p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ where $p_1, p_2, \ldots, p_n$ are distinct primes and each a_i is a natural number, then d is a positive divisor of x if and only if d can be written as $p_1^{d_1} p_2^{d_2} \cdots p_n^{d_n}$ where $0 \leq d_i \leq a_i$ for each i.

GCD from Prime Factorization (GCD PF)
If a can be written as $p_1^{a_1} \cdots p_k^{a_k}$ and b can be written as $p_1^{b_1} \cdots p_k^{b_k}$ where $p_1, p_2, \ldots, p_k$ are distinct primes and each a_i and b_i is a non-negative integer, then $\gcd(a, b) = p_1^{d_1} \cdots p_k^{d_k}$ where $d_i = \min\{a_i, b_i\}$ for each i.

The next two theorems might get pushed to week 7 depending on the class.

Linear Diophantine Equation Theorem Part 1 (LDET 1)
Let $a, b, c \in \mathbb{Z}$ and $d = \gcd(a, b)$. The linear Diophantine equation $ax + by = c$ has an integer solution if and only if $d \mid c$.

Linear Diophantine Equation Theorem Part 2 (LDET 2)
Let $a, b, c \in \mathbb{Z}$ and $d = \gcd(a, b) \neq 0$. If (x_0, y_0) is one particular integer solution to $ax + by = c$, then the complete set of integer solutions is

$$\left\{ \left(x_0 + \frac{b}{d} n, y_0 - \frac{a}{d} n \right) \;\middle|\; n \in \mathbb{Z} \right\}.$$