Math 299 **Lecture 32: Sections 11.4-11.5**
The Euclidean Algorithm

Theorem. (The Euclidean Algorithm) Let x and y be integers. Then there exist integers q_1, q_2, ..., q_k and a descending sequence of positive integers, r_1, ..., r_k, $r_{k+1} = 0$, such that:

$$x = q_1 y + r_1$$

$$y = q_2 r_1 + r_2$$

$$r_1 = q_3 r_2 + r_3$$

$$\vdots$$

$$r_{k-1} = q_k r_k + 0$$

Furthermore, $\gcd(x, y) = r_k$.

Use the Euclidean Algorithm to find $\gcd(51, 288)$. Find $x, y \in \mathbb{Z}$ such that $51x + 288y = \gcd(51, 288)$.

Proof of the Euclidean Algorithm

Why can we assume WLOG that x and y in the Euclidean Algorithm are positive and $x > y$?

Lemma. Let a and b be positive integers. If $b = aq + r$ for some integers q and r, then $\gcd(a, b) = \gcd(r, a)$.

How can we combine the above Lemma with the Division Algorithm to prove the Euclidean Algorithm?

Euclid's Lemma. Suppose n, a, and $b \in \mathbb{N}$. If $n \mid ab$ and $\gcd(n, a) = 1$, then $n \mid b$.
Proof:

Alternative version of Euclid's Lemma. If p is prime and p divides ab, then p divides a or p divides b.
Proof:

Definition. Two integers are called **coprime** or **relatively prime** if their greatest common divisor is 1.

Corollary. If $n \in \mathbb{N}$ is not a square number, then $\sqrt{n} \notin \mathbb{Q}$.
Proof: