Review of proofs from last time that $\sqrt{2} \notin \mathbb{Q}$:
<u>Theorem:</u> $\sqrt{2} \notin \mathbb{Q}$.
Main idea is to show that $S : \{n \geq 1 : n\sqrt{2} \in \mathbb{Z}\}$ is empty. Since S is a set of positive integers, if nonempty, it must have a least element. The contrapositive: if S has no least element, then S must be empty!
<u>Proof 1:</u> If $b \in S$, then $b/2 \in S$ so S has no least element. Thus $S = \varnothing$.
<u>Proof 2:</u> If $b \in S$, then $b(\sqrt{2}-1) \in S$ so S has no least element since $\sqrt{2}-1 < 1$. Thus $S = \varnothing$.
<u>Proof 3:</u> If $b \in S$, then $\exists b' \in S$ $b' < b$. S has no least element, thus $S = \varnothing$. (see Class 4 notes)

Now we give one more proof of this theorem.

<u>Proof 4:</u> Suppose $b \in S$. Then $\exists a \in \mathbb{Z}$ such that $\frac{a}{b} = \sqrt{2}$. We have

$$\frac{a}{b} = \sqrt{2} = \frac{\sqrt{2}-1}{\sqrt{2}-1}\sqrt{2} = \frac{2-\sqrt{2}}{\sqrt{2}-1} = \frac{2-\frac{a}{b}}{\frac{a}{b}-1} = \frac{2b-a}{a-b}$$

We would *like* to show that $0 < a-b < b$ so then $a-b < b$ and $a \in S$.

Miranda: We know $a/b = \sqrt{2}$ so then

$$1 < \sqrt{2} < b \implies 1 < \frac{a}{b} < 2 \implies b < a < 2b \implies 0 < a-b < b$$

Bézout representations

We next moved on to a topic related to the Euclidean algorithm (as well as to a problem for the homework you just submitted). Recall: that we know $\gcd(a,b) = ax + by$ for some $x, y \in \mathbb{Z}$. But how do we find x and y? Turns out we can run the Euclidean algorithm backwards.

$$\begin{aligned} 54 - 37 &= 17 \\ 37 - 2(17) &= 3 \\ 17 - 5(3) &= 2 \\ 3 - 2 &= 1 \end{aligned}$$

Konnor suggests substituting backwards. Akhil demonstrates:

$$\begin{aligned} 54 - 37 &= 17 \\ 37 - 2(17) = 37 - 2(54-37) &= 3 \\ 17 - 5(3) = (54-37) - 5\,(37 - 2(54-37)) &= 2 \\ 3 - 2 = 37 - 2(54-37) - ((54-37) - 5\,(37-2(54-37))) &= 1 \end{aligned}$$

So then expanding the last line,

$$37 - 2(54 - 37) - ((54 - 37) - 5(37 - 2(54 - 37))) = 19 \cdot 37 - 13 \cdot 54 = 1$$

Ben suggests a short cut, once we have one of the coefficients we can solve for the coefficient of the other. Max suggests simplifying as you go, to reduce possible arithmetic errors. Also, notice that you can go the other directions (i.e. up the lines instead of down). For example:

$$\begin{aligned} 1 &= 3 - 2 = 3 - (17 - 5(3)) = 6(3) - (17) = 6(37 - 2(17)) - 17 \\ &= 6(37) - 13(17) = 6(37) - 13(54 - 37) = -13(54) + 19(37) \end{aligned}$$

So we have $1 = -13 \cdot 54 + 19 \cdot 37$, which is what we had before!

Konnor: If $3x + 5y = 1$, then $\gcd(x, y) = 1$. But what if $3x + 5y = 8$? Then 8 is not necessarily the gcd, but it *is* a multiple of the gcd. So if $3x + 5y = 1$, the 1 is a multiple of the gcd, so gcd is 1. Miranda remarks then that if $ax + by = p$ for a prime p, then $\gcd(a, b)$ must either be 1 or p.

Distribution of Primes

List of primes: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, \ldots$.
Theorem: There are infinitely many primes.
Proof: ($\geq 2,000$ years old, written down by Euclid in the *Elements*)
It suffices to prove the following assertion:
Claim: Given any finite collection of primes, there exists a prime p not in the collection.
Proof of claim: Given a finite list of primes, $q_1, q_2, \ldots, q_n$. Consider the integer $q_1 q_2 \cdots q_n + 1$. The FTA implies that this integer is a product of primes; in particular, there exists some prime p such that

$$p \mid q_1 q_1 \cdots q_n + 1.$$

Konnor pointed out that p must be different than any of the primes in our list. To see this, suppose $p = q_i$ for some i. Then we'd have $p \mid q_1 q_2 \cdots q_n$, whence

$$p \mid (q_1 q_1 \cdots q_n + 1) - q_1 q_2 \cdots q_n = 1$$

but $p \nmid 1$ because p is a prime. Thus $p \neq q_i$ for any i, and is a new prime not on our list. $\square$

We can use Euclid's approach to generate primes. Starting with $\{2\}$, we can get 3, so we have $\{2, 3\}$. Then $2 \cdot 3 + 1 = 7$, so we have $\{2, 3, 7\}$. Using these we get $\{2, 3, 7, 43\}$, etc.

Open question. Does this process generate all the primes? Or does there exist some prime that will never get generated?

OK, so there are infinitely many primes. How quickly do they grow? There are many ways to make this question precise. A natural approach is to ask how large the nth prime is? Write the sequence of primes in increasing order:

$$2 = p_1 < p_2 < p_3 < \cdots$$

(so that, for example, $p_2 = 3$ and $p_3 = 5$).

Proposition: $p_n \leq 2^{2^{n-1}}$ for all $n \geq 1$.
Proof: By (strong) induction. First we check the base case $n = 1$: $p_1 = 2 = 2^{2^{1-1}}$. ✓

Now suppose that $p_k \leq 2^{2^{k-1}}$ for every $1 \leq k < n$. We want to show that the claim holds for n. By the FTA there exists some prime $p \mid p_1 p_2 p_3 \cdots p_{n-1} + 1$. From Euclid's proof we know that $p \neq p_i$ for any of $i \leq n-1$, which means that $p \geq p_n$. Thus

$$p_n \leq p \leq p_1 p_2 \cdots p_{n-1} + 1 \leq 2^{2^0} 2^{2^1} \cdots 2^{2^{n-2}} + 1 = 2^{2^0 + 2^1 + \cdots 2^{n-2}} + 1 = 2^{2^{n-1}-1} + 1 \leq 2^{2^{n-1}}.$$

By induction, $p_n \leq 2^{2^{n-1}}$ for every $n \geq 1$.