Last time we proved:

(1) $a\mathbb{Z} + b\mathbb{Z} \subseteq \gcd(a,b)\mathbb{Z}$

(2) Given $a, b \in \mathbb{Z}$ with $b > 0$, $\exists q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < b$.
This essentially means we subtract multiples of b until we can't anymore.

Addendum to (2):
Proposition: Given $a, b \in \mathbb{Z}$ with $b > 0$, the choices of q and r are unique.
Proof: (Max) We know that $a = qb + r$, suppose that $a = q'b + r'$. We want to show that $q = q'$ and $r = r'$.

Given this set up, then

$$\begin{aligned} qb + r &= q'b + r' \\ \text{whence} \qquad b(q - q') &= r' - r \end{aligned}$$

Then b divides $r' - r$. However $-b < r' - r < b$ since $0 \leq r, r' < b$. The only multiple of b in this range is 0, so $r' - r = 0$, and thus $r' = r$. So the choice of r is unique. Using this, $b(q - q') = 0$, so $q - q' = 0$ and thus $q = q'$. □

Returning to (1), we want to prove the following:
Claim: $\gcd(a,b)\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z}$.
Strategy: change our perspective! What role does $\gcd(a,b)$ play in $a\mathbb{Z} + b\mathbb{Z}$? Oliver's conjecture: $\gcd(a,b)$ is the minimal element in $a\mathbb{Z} + b\mathbb{Z}$.
Example: $4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$. So the $\gcd(a,b)$ isn't the smallest element but... Amelia notes that it generates all the others and Alex points out that it is the least positive number.
So (we conjecture) the $\gcd(a,b)$ is the minimal positive element in $a\mathbb{Z} + b\mathbb{Z}$.
Proposition: Given $a, b\mathbb{Z}$ (not both zero), let d denote the minimal positive element of $a\mathbb{Z}+b\mathbb{Z}$. Then $d\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z}$.
Proof: (Jeff) By definition, $d \in a\mathbb{Z}+b\mathbb{Z}$. Then, $d = ax+by$ for some $x, y \in \mathbb{Z}$. Take any multiple of d, then $dk = a(kx) + b(ky) \in a\mathbb{Z} + b\mathbb{Z}$ for any k. Then $d\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z}$. □
Lemma: Given $a, b \in \mathbb{Z}$ (not both zero), let d be the minimal positive element of $a\mathbb{Z} + b\mathbb{Z}$. Then $d = \gcd(a,b)$.
Proof: First, we prove that d is a *common divisor* of a and b, i.e. that $d \mid a$ and $d \mid b$. (Notation: $d \mid n$ means "d divides n".) Akhil points out that $d \in a\mathbb{Z} + b\mathbb{Z}$, so $d = ax + by$. However, we cannot choose what x and y are because d is a fixed number.
Oliver: Using (2) to compare a and d, this gives us $a = qd + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < d$. Jacob points out that there is no integer greater than zero less than d in the set. So if we

can show $r \in a\mathbb{Z} + b\mathbb{Z}$ we can win! Qiana notes that $r = a - qd$, and $d = ax + by$ for some $x, y \in \mathbb{Z}$. Then

$$r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy) \in a\mathbb{Z} + b\mathbb{Z}.$$

Since d is the minimal positive integer in $a\mathbb{Z} + b\mathbb{Z}$, $0 \le r < d$, and $r \in a\mathbb{Z} + b\mathbb{Z}$, we must have $r = 0$. Then $a = qd$ and thus $d \mid a$. The same approach shows that $d \mid b$.
Next, we need to prove that d is the *greatest* common divisor of a and b. Alex: assume there is another common divisor, c, i.e. $c \mid a$ and $c \mid b$. We need to show that $c \le d$. Since we think d is the gcd, it should be true that $c \mid d$ (Qiana). Ben reminds us that $d = ax + by$, so then dividing by c

$$\frac{d}{c} = \frac{ax + by}{c} = \frac{a}{c}x + \frac{b}{c}y \in \mathbb{Z}$$

so then $c \mid d$, which shows that $c \le d$. Thus $d = \gcd(a, b)$. □
Theorem: Given $a, b \in \mathbb{Z}$, $a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b)\mathbb{Z}$.
Corollary: (Bézout's Theorem) If a and b are coprime then $\exists x, y \in \mathbb{Z}$, such that $ax + by = 1$.

Fundamental Theorem of Arithmetic

Definition: A positive integer is composite if it can be expressed as the product of two smaller (positive) integers. For example: $60 = 12 \cdot 5 = 4 \cdot 3 \cdot 5 = 2 \cdot 2 \cdot 3 \cdot 5$.
Definition: A positive integer greater than 1 that is not composite is called prime.
Primes are the building blocks of the integers.
Note: 1 is neither prime nor composite.
Notice that we could have factored 60 differently, but would end up with the same primes.

Fundamental Theorem of Arithmetic: Any positive integer $n \ge 2$ can be expressed in the form $n = q_1 q_2 \cdots q_n$ where the q_i's are prime. This expression is unique, up to ordering of q_i's.

This isn't true in all number systems. For instance, let $\mathcal{E} := \{2, 4, 6, \ldots\}$. Now factor 60 in $\mathcal{E}$. Kimberly points out that $60 = 6 \cdot 10$, and that both 6 and 10 are prime in $\mathcal{E}$ (i.e. can't be broken down further). But also, $60 = 2 \cdot 30$, and 2 and 30 are also both prime in $\mathcal{E}$. Thus in $\mathcal{E}$, factorization into primes is not unique!

To prove the theorem, we shall need the following tool:
Lemma: If $p \mid ab$ where a and b are positive integers, then $p \mid a$ or $p \mid b$.
This is surprisingly difficult to prove. Ben suggests trying contradiction, so $p \nmid a$ and $p \nmid b$. Then Jacob says that p does not appear in the factorization of a and b, and thus does not appear in the prime factorization of ab. Qiana points out that this argument is circular, however, since it *assumes* the Fundamental Theorem of Arithmetic!