Recall that $1/3 \pmod 7 = 5$. What about $2/3 \pmod 7$?

$$\frac{2}{3} = 2 \cdot \frac{1}{3} \equiv 2 \cdot 5 \equiv 3 \pmod 7.$$

More generally, once we know $1/q \pmod n$, it's easy to determine $a/q \pmod n$ for any $a \in \mathbb{Z}$.

Notation Note: We will usually denote $1/a \pmod n$ by $\overline{a}$. For example, $\overline{3} \equiv 5 \pmod 7$.

[Side story: the ancient Egyptians used a similar notation when describing fractions. In fact, they represented all fractions as sums of distinct fractions of the form $1/n$, e.g. $2/3 = 1/2 + 1/6$. This is called an 'Egyptian fraction decomposition'. Remarkably, any positive rational number has an Egyptian fraction decomposition, i.e. can be represented as a finite sum of *distinct* fractions of the form $1/n$. There's a famous open problem about Egyptian fractions:

Erdős-Straus Conjecture: Given any odd $n \geq 4$, the number $\frac{4}{n}$ admits an Egyptian fraction decomposition using at most 3 summands.]

An example of doing algebra within the world of modular arithmetic:

$$\begin{aligned} 3x + 2 \equiv 6 \pmod 7 &\implies 3x \equiv 4 \pmod 7 \\ &\implies x \equiv \overline{3} \cdot 4 \pmod 7 \\ &\implies x \equiv 5 \cdot 4 \pmod 7 \\ &\implies x \equiv 6 \pmod 7 \end{aligned}$$

This represents a larger phenomenon: we can do all the usual algebra we're used to, so long as we only divide by things relatively prime to the modulus.

We left off last time discussing $\varphi(n) := |\mathbb{Z}_n^\times|$.
Question: What is $\varphi(10000)$?

Max points out it is at most 5000, since all the evens are not relatively prime. But from there, further division runs into double counting issues. Ben expands this idea bringing in multiples of 5, but the same issue of counting exists.

Simpler question: what is $\varphi(49)$? Akhil: the only prime factors of 49 are 7, so take out all multiples of 7 from the range $1, 2, \ldots, 49$. These are $7, 14, 21, \ldots, 49$ (of which there are 7). The remaining numbers are relatively prime to 49, and there are $49 - 7 = 42$ of them. So $\varphi(49) = 42$.

Conjecture (Max): Given a prime p, $\varphi(p^2) = p(p-1) = p^2 - p$.
Proof: Same technique as for $\varphi(49)$.

Next question: what is $\varphi(p^k)$? Mia's Guess: $p^k - (k-1)p$. This was based on the example $\varphi(8)$. However $\varphi(27) = 18 \neq 27 - 2 \cdot 3$, so this doesn't work. Chris: $\varphi(p^k) = p^k - p^{k-1}$. This works for both 8 and 27. Why does this work? Again, need to remove all multiples of p, of which there are p^{k-1}, so we get $p^k - p^{k-1}$.

Note this checks out with what we already know.

$$\varphi(p^1) = p^1 - p^0 = p - 1 \checkmark$$
$$\varphi(p^2) = p^2 - p^1 = p^2 - p \checkmark$$

Great, we've figured out how $\varphi(\cdot)$ behaves on prime powers. What about at non-prime-powers? Let's make a little table:

$n = p^k$	$\varphi(n)$
2	1
3	2
$2^2 = 4$	2
5	4
7	6
$2^3 = 8$	4
$3^2 = 9$	6

$n \neq p^k$	$\varphi(n)$
$2 \cdot 3 = 6$	2
$2 \cdot 5 = 10$	4
$2^2 \cdot 3 = 12$	4
$2 \cdot 7 = 14$	6
$3 \cdot 5 = 15$	8
$2 \cdot 3^2 = 18$	6
$2^2 \cdot 5 = 20$	8

Conjecture (Oliver +secretly Max + Miranda + Kimberly): For $n = \prod_p p^{\nu_p(n)}$, $\varphi(n) = \prod_p \varphi(p^{\nu_p(n)})$.

This turns out to be true! In fact, we'll prove a slightly stronger result:

Theorem: $\varphi(mn) = \varphi(m)\varphi(n)$ whenever $(m, n) = 1$.

We say "φ is multiplicative". More generally, we say a function f is multiplicative iff $f(mn) = f(m)f(n)$ whenever m and n are coprime.

If $f(mn) = f(m)f(n)$ no matter what m and n are, we say f is "completely multiplicative". Note that φ is *not* completely multiplicative, because $\varphi(4) = 2 \neq \varphi(2) \cdot \varphi(2)$.

Oliver's question: does the converse hold? In other words, if $\varphi(mn) = \varphi(m)\varphi(n)$, must $(m, n) = 1$? Miranda thinks it might be true, since the formula for powers of primes is not multiplicative, and examining shared prime factors should yield different results for $\varphi(nm)$ and $\varphi(n)\varphi(m)$.

Max: Suppose p is the unique common prime factor between m and n. We can write $\varphi(m) = \varphi(p^k)\varphi(m/p^k)$ and $\varphi(n) = \varphi(p^\ell)\varphi(n/p^\ell)$, where p^k and p^ℓ are all the factors of p in

m and n respectively. Then

$$\varphi(m)\varphi(n) = (p-1)p^{k-1}(p-1)p^{\ell-1}\varphi(m/p^k)\varphi(n/p^\ell) = (p-1)^2p^{k+\ell-2}\varphi(mn/p^{k+\ell})$$

since $(\frac{m}{p^k}, \frac{n}{p^\ell}) = 1$. On the other hand,

$$\varphi(mn) = \varphi(p^{k+\ell})\varphi(mn/p^{k+\ell}) = (p-1)p^{k+\ell-1}\varphi(mn/p^{k+\ell})$$

Thus if $\varphi(mn) = \varphi(m)\varphi(n)$ we would deduce

$$p - 1 = p,$$

a contradiction. Thus we've proved:

Proposition (Max, Miranda, and Jeff): If m and n have precisely one prime factor in common, then $\varphi(mn) \neq \varphi(m)\varphi(n)$.

It would be interesting to generalize this result.

Returning to our question from the start of class, we see

$$\varphi(10,000) = \varphi(10^4) = \varphi(2^4 \cdot 5^4) = \varphi(2^4)\varphi(5^4) = 2^3(2-1)5^3(5-1) = 4000$$

Idea for proof of theorem:
We know $\varphi(mn) = |\mathbb{Z}_{nm}^\times|$, $\varphi(n) = |\mathbb{Z}_n^\times|$, and $\varphi(m) = |\mathbb{Z}_m^\times|$. So what does $\varphi(m)\varphi(n)$ count? Akhil proposes: $\varphi(n)\varphi(m) = |\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times| = |\{(a,b) : a \in \mathbb{Z}_n^\times, b \in \mathbb{Z}_m^\times\}|$.

Our strategy is going to be examining $\mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$ and $\mathbb{Z}_{mn}^\times$. We'd like to find a one-to-one correspondence between the elements of each set, showing that $\varphi(mn) = \varphi(m)\varphi(n)$. In other words, if we can find a bijection between $\mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$ and $\mathbb{Z}_{mn}^\times$, then $\varphi(mn) = \varphi(m)\varphi(n)$.