Recall the definition of the Euler totient function: $\varphi(n) = |\mathbb{Z}_n^\times|$. Last time, we proved that $\varphi(p^k) = (p-1)p^{k-1}$ and stated the following:
Theorem: φ is multiplicative, i.e. $\varphi(mn) = \varphi(m)\varphi(n)$ whenever $(m,n) = 1$.
Proof idea: $\varphi(mn) = |\mathbb{Z}_{mn}^\times|$ and $\varphi(m)\varphi(n) = |\mathbb{Z}_m^\times \times \mathbb{Z}_n^\times|$. Thus if we can find a bijective map $f : \mathbb{Z}_{mn}^\times \to \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$, this will prove that φ is multiplicative.

> Recall: a map $f : X \to Y$ is *bijective* if and only if for every $y \in Y$, there is a unique $x \in X$ such that $f(x) = y$. Most commonly this is proved in two steps: first one proves that f is injective, and then that it's surjective. For f to be *injective* means that for all $y \in Y$, there is at most one $x \in X$ such that $f(x) = y$. For f to be *surjective* means that for every $y \in Y$ there exists at least one $x \in X$ such that $f(x) = y$. Thus if f is simultaneously injective and surjective we see that f must be bijective.

Our goal for proving the theorem is to come up with a bijection mapping $\mathbb{Z}_{mn}^\times \to \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$. The first problem is to come up with any map. Here are a few we came up with:

Map	Issues
$x \mapsto (1,1)$	neither injective nor surjective
$x \mapsto (\frac{x}{n}, \frac{x}{m})$	an interesting candidate, so long as division by m and n is ok
$xy \leftarrow (x,y)$	xy might not be in $\mathbb{Z}_{mn}^\times$
$x = \prod p_i^{e_i} \mapsto (\prod_{(p,m)=1} p_i^{e_i}, \prod_{(p,n)=1} p_i^{e_i})$	factorization into primes isn't unique in $\mathbb{Z}_{mn}^\times$!
$x \mapsto (x \pmod m, x \pmod n)$	another interesting candidate

We'll explore the last of these. For ease of reference, and to honor the originator of the idea (Ben), let's give this function a name:

$$\begin{aligned} \beta : \mathbb{Z}_{mn}^\times &\to \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times \\ x &\to \big(x \pmod m, x \pmod n\big) \end{aligned}$$

For example: $m = 3$ and $n = 5$. Then $\beta(7) = (1,2)$.

Is β well-defined? We must check
(i) that any $x \in \mathbb{Z}_{mn}^\times$ gets mapped to $\mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$, and
(ii) that whenever $x \equiv y \pmod{mn}$ we have $f(x) = f(y)$.
First we check (i):

$$x \in \mathbb{Z}_{mn}^\times \implies (x, mn) = 1 \implies (x, m) = 1.$$

By problem **3.5**, we deduce that $x \pmod m \in \mathbb{Z}_m^\times$; similarly, $x \pmod n \in \mathbb{Z}_n^\times$. Thus, we conclude that $\beta(x) \in \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$ as claimed.

Next, we verify (ii).

$$x \equiv y \pmod{mn} \implies x = y + kmn \implies \Big(x \equiv y \pmod m \quad \text{and} \quad x \equiv y \pmod n\Big).$$

Thus, $\beta(x) = \beta(y)$ whenever $x \equiv y \pmod{mn}$.

Thus we've shown that β is well-defined (i.e. doesn't misbehave). Now let's show what we really want: that it's a bijection.

<u>Claim:</u> β is a injective.
<u>Proof:</u> Suppose $\beta(x) = \beta(y)$. Then $x \equiv y \pmod m$ and $x \equiv y \pmod n$, or in other words, $m \mid x - y$ and $n \mid x - y$. But $(m, n) = 1$, whence $mn \mid x - y$. This implies $x \equiv y \pmod{mn}$, which in turn yields $x = y$ (since $x, y \in \mathbb{Z}_{mn}^\times$).

To recap, we just proved that distinct inputs produce distinct outputs, which is the same as saying β is injective. We're halfway there!

<u>Claim:</u> β is surjective.
<u>Proof:</u> Given $(a, b) \in \mathbb{Z}_n^\times \times \mathbb{Z}_m^\times$ we want to show that there exists $x \in \mathbb{Z}_{mn}^\times$ such that $\beta(x) = (a, b)$. We will do this in three steps.

<u>Step 1:</u> *Given $(a, b) \in \mathbb{Z}_n^\times \times \mathbb{Z}_m^\times$, we construct an $x \in \mathbb{Z}$ such that $x \pmod m = a$ and $x \pmod n = b$.*

Inspired by an idea of Miranda, we consider integers of the form

$$x = (\cdots)m + (\cdots)n.$$

How can we insert integers in place of the ellipses to force $x \pmod m = a$? Well, the first term disappears, and if we want the second term to produce a we simply put $x = (\cdots)m + (a\overline{n})n$; here $\overline{n} := \frac{1}{n} \pmod m$. We make a similar choice for the coefficient of m to get

$$x = (b\overline{m})m + (a\overline{n})n.$$

We've done it!

<u>Step 2:</u> *We prove that $(x, mn) = 1$.*

Suppose $p \mid (x, mn)$. Then $p \mid mn$, whence it must divide one of m or n; WLOG say $p \mid m$. But then from our definition of x we deduce $p \mid a\overline{n}n$, which contradicts the fact that all three of the numbers $a, \overline{n}, n \in \mathbb{Z}_m^\times$.

Step 3: *Win.*

By problem **3.5**, $x \pmod{mn} \in \mathbb{Z}_{mn}^{\times}$. Moreover,

$$x \pmod{mn} \equiv x \pmod{m} \qquad \text{and} \qquad x \pmod{mn} \equiv x \pmod{n}$$

whence $\beta\big(x \pmod{mn}\big) = (a, b)$ as desired.

Combining these three steps yields that β is surjective. Thus, we've proved that β is bijective. But this means that $\mathbb{Z}_{mn}^{\times}$ and $\mathbb{Z}_{m}^{\times} \times \mathbb{Z}_{n}^{\times}$ have the same number of elements, whence

$$\varphi(mn) = \varphi(m)\varphi(n)$$

whenever $(m, n) = 1$ as claimed. □

To see this approach in action, let's consider an example. Take $m = 3$ and $n = 5$. Then $\overline{m} = 2$ and $\overline{n} = 2$, whence $x = 6b + 10a$ has the desired property that

$$x \equiv a \pmod{3} \qquad \text{and} \qquad x \equiv b \pmod{5}.$$

Thus the number $6b + 10a \pmod{15}$ lives in $\mathbb{Z}_{15}^{\times}$ and gets mapped to (a, b) by β.