LECTURE 15: SUMMARY

In today's lecture, we proved the following result (which is half of David's conjecture from last lecture):

Theorem 1. *If* $(m, n) = 1$*, then* $\varphi(mn) = \varphi(m)\varphi(n)$.

Right off the bat, note that the hypothesis that m and n are relatively prime is necessary. For example, $\varphi(12) \neq \varphi(2)\varphi(6)$. We also practiced using this theorem to calculate $\varphi(n)$. As we saw, whenever we could factor n, the theorem made it easy to figure out $\varphi(n)$. Unfortunately, if n is not easy to factor, then it's less clear how to determine $\varphi(n)$. We will discuss this in more depth later, when talking about the RSA encryption algorithm.

Before writing down the proof of theorem, we discuss the strategy. By definition, we have

$$\varphi(mn) = |\mathbb{Z}_{mn}^\times|.$$

What about $\varphi(m)\varphi(n)$? A bit of thought showed that this, too, measures the size of a set:

$$\varphi(m)\varphi(n) = |\mathbb{Z}_m^\times \times \mathbb{Z}_n^\times|$$

where $A \times B := \{(a, b) : a \in A, b \in B\}$. Thus, if we can show that the two sets $\mathbb{Z}_{mn}^\times$ and $\mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$ have the same size, we win. How will we do this? We look for a bijection between the two sets, i.e. a way of pairing off elements of the two sets. Shichu suggested the following function:

$$\begin{aligned} \sigma : \mathbb{Z}_{mn}^\times &\longrightarrow \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times \\ a &\longmapsto (a \pmod{m}, a \pmod{n}) \end{aligned}$$

where $x \pmod{d}$ denotes the unique element of $\mathbb{Z}_d$ which is congruent to x modulo d. If we can show that this is a bijection – i.e. that for every $(x, y) \in \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$, there exists a unique $a \in \mathbb{Z}_{mn}^\times$ such that $\sigma(a) = (x, y)$ – then it would immediately follow that $\mathbb{Z}_{mn}^\times$ and $\mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$ have the same number of elements.

Before going into the proof of the theorem, we state a useful tool:

Lemma 2. *Suppose* $(a, N) = 1$*. Then the integer* $a \pmod{N}$ *is also relatively prime to* N*, i.e.* $a \pmod{N} \in \mathbb{Z}_N^\times$.

I leave the proof of this lemma as an exercise.

Proof. Consider the function σ defined above. We prove that it's a bijection in three steps:

(1) σ is **well-defined**, i.e. for all $x \in \mathbb{Z}_{mn}^\times$ there exists a unique $(a, b) \in \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$ such that $\sigma(x) = (a, b)$;

Date: March 5th, 2013.

(2) σ is **surjective**, i.e. for all $(a,b) \in \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$ there exists at least one $x \in \mathbb{Z}_{mn}^\times$ such that $\sigma(x) = (a,b)$; and
(3) σ is **injective**, i.e. for all $(a,b) \in \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$ there exists at most one $x \in \mathbb{Z}_{mn}^\times$ such that $\sigma(x) = (a,b)$.

First, why is σ well-defined? Well, certainly $\sigma(x) \in \mathbb{Z}_m \times \mathbb{Z}_n$; what's not immediate is that $\sigma(x) \in \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$. However, armed with the Lemma above this isn't so difficult. Since $x \in \mathbb{Z}_{mn}^\times$, we know that $(x, mn) = 1$. It follows that $(x, m) = 1$, whence (by the lemma) the integer $x \pmod{m} \in \mathbb{Z}_m^\times$. The same goes for $x \pmod{n}$, of course.

Next, why is σ surjective? Given $(a,b) \in \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$, can we find an $x \in \mathbb{Z}_{mn}^\times$ such that $\sigma(x) = (a,b)$? It's easy to see that this is equivalent to finding an $x \in \mathbb{Z}_{mn}^\times$ such that

$$x \equiv a \pmod{m} \qquad \text{and} \qquad x \equiv b \pmod{n}.$$

The trick is to write $x = (\cdots)m + (\cdots)n$, and find appropriate ways to fill in the blanks. The advantage of writing x this way is that when we reduce $x \pmod{m}$ we can focus on just the second term, while when we reduce $\pmod{n}$ we can focus on just the first term. A bit of thought showed that we should choose the first blank to be bm^{-1}, where m^{-1} denotes the inverse of m in $\mathbb{Z}_n^\times$, and the second blank to be an^{-1}, where n^{-1} denotes the inverse of n in $\mathbb{Z}_m^\times$.[1] In any event, let

$$x = (bm^{-1})m + (an^{-1})n.$$

It's easy to check that $x \pmod{m} = a$ and $x \pmod{n} = b$. The only remaining difficulty is that x is just some integer; it might not be an element of $\mathbb{Z}_{mn}^\times$! Fortunately, this can be fixed. I leave this as an exercise.

Finally, why is σ injective? Well, suppose $\sigma(x) = \sigma(y)$ for some $x, y \in \mathbb{Z}_{mn}^\times$. Then

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

It follows that $m \mid x - y$ and also $n \mid x - y$. By problem 1.9 from your homework, it follows that $mn \mid x - y$, i.e. that $x \equiv y \pmod{m}n$. Thus, $x = y$, so σ is injective. $\square$

Make sure that you go through and understand the theorem properly; there were some gaps in the sketch above. Among other questions, you should ask yourself: where did we use that $(m,n) = 1$?

[1] Actually, if we were being super careful, we should be referring to $n \pmod{m}$ and $m \pmod{n}$ in the previous sentence, rather than to n and m themselves.