LECTURE 16: SUMMARY

Recall Euler's theorem: for all $a \in \mathbb{Z}_d^\times$, we have $a^{\varphi(n)} = 1$. One use of this is to calculate a^{-1}. For example, what is 3^{-1} in $\mathbb{Z}_8^\times$? We know $\varphi(8) = 4$, so $3^4 = 1$; dividing both sides by 3 (i.e. multiplying both sides by 3^{-1}) yields $3^{-1} = 3^3 = 3$. Actually, there's an easier way to find 3^{-1}: from the multiplication table for $\mathbb{Z}_8^\times$, we know that $3^2 = 1$, from which it immediately follows that $3^{-1} = 3$. More generally, if we want to determine a^{-1} in $\mathbb{Z}_d^\times$ using this method, it's desirable to know the smallest positive integer k such that $a^k = 1$ in $\mathbb{Z}_d^\times$. This quantity plays an important role in number theory (and other areas of math), so it has a special name:

Definition. *The* order of a in $\mathbb{Z}_d^\times$*, denoted* $\ell_n(a)$*, is defined to be the smallest positive integer such that* $a^{\ell_n(a)} = 1$ *in* $\mathbb{Z}_d^\times$.

After some playing around, we conjectured (and proved) the following result:

Proposition 1. *For every* $a \in \mathbb{Z}_n^\times$*, we have* $\ell_n(a) \mid \varphi(n)$.

Proof. Write $\varphi(n) = q\ell_n(a) + r$, where $q \in \mathbb{Z}$ and $r \in \mathbb{Z}_{\ell_n(a)}$. Then $a^{\varphi(n)} = 1 = a^{\ell_n(a)}$, whence

$$a^r = a^{\varphi(n) - q\ell_n(a)} = 1.$$

Since $a^k \neq 1$ for all integers $k \in [1, \ell_n(a) - 1]$ by the definition of the order of a, we conclude that $r = 0$; the claim follows. □

We next considered those $a \in \mathbb{Z}_n^\times$ whose order was as big as possible, i.e. $\ell_n(a) = \varphi(n)$. We figured out the following:

Proposition 2. *If* $a \in \mathbb{Z}_n^\times$ *and* $\ell_n(a) = \varphi(n)$*, then*

$$\{a^k : k \in \mathbb{Z}_{\varphi(n)}\} = \mathbb{Z}_n^\times.$$

Proving this is a good exercise. We will revisit this result next lecture.

Date: March 7th, 2013.