LECTURE 17: SUMMARY

We continued our discussion of order, but with some new notation which made things easier. First, given $a \in \mathbb{Z}_n^\times$, define

$$\langle a \rangle := \{a^k : k \in \mathbb{Z}\}$$

where a^k is computed in $\mathbb{Z}_n^\times$. This is called the set *generated* by a. The relation to the previous material is the following result:

Proposition 1. *The order of $a \in \mathbb{Z}_n^\times$ is the number of elements generated by a. In other words,*

$$|\langle a \rangle| = \ell_a(n).$$

Recall that $\ell_a(n) \mid \varphi(n)$. If $\ell_a(n) = \varphi(n)$ – or, equivalently, if $\langle a \rangle = \mathbb{Z}_n^\times$ – then a is said to be a *primitive root* of $\mathbb{Z}_n^\times$. For example, 2 is a primitive root of $\mathbb{Z}_{11}^\times$, since

$$\langle 2 \rangle = \{1, 2, 4, 8, 5, 10, 9, 7, 3, 6\} = \mathbb{Z}_{11}^\times.$$

By contrast, 3 is *not* a primitive root of $\mathbb{Z}_{11}^\times$:

$$\langle 3 \rangle = \{1, 3, 9, 5, 4\} \neq \mathbb{Z}_{11}^\times.$$

There are many reasons primitive roots are nice. One simple example is that they allow us to divide easily. For example, in $\mathbb{Z}_{11}^\times$, what is $5 \div 8$? From above, we see that $5/8 = 2$. Similarly, $9/5 = 2^2 = 4$.

Does $\mathbb{Z}_n^\times$ have a primitive root for every n? We quickly saw that the answer was no: $\mathbb{Z}_8^\times$ has no primitive root (every non-trivial element has order 2). Which $\mathbb{Z}_n^\times$s have a primitive root? An important theorem, which will take us a few classes to prove, is that $\mathbb{Z}_p^\times$ has a primitive root for every prime p. Are there other choices of n which give primitive roots? More generally, how many primitive roots does $\mathbb{Z}_n^\times$ have? How does one find them? After a bit of playing around, we conjectured the following:

Conjecture 2. *Given g a primitive root of $\mathbb{Z}_n^\times$. Then g^k is a primitive root of $\mathbb{Z}_n^\times$ iff $k \in \mathbb{Z}_{\varphi(n)}^\times$.*

We will return to this soon, during the course of our proof that $\mathbb{Z}_p^\times$ has a primitive root.

We next discussed (Emil) Artin's conjecture: if $a \in \mathbb{Z}$ does not equal -1 or a perfect square, then a is a primitive root of $\mathbb{Z}_p^\times$ for infinitely many primes p (in fact, for a positive proportion of primes p). I mentioned a result due to Heath-Brown, that Artin's conjecture is true for all but at most two prime values of a. For example, the conjecture holds for at least one of $a = 2, 3$, or 5. Despite this, Artin's conjecture is not known for any single choice of a!

We finished lecture by discussing the notion of a *field*. Recall that $\mathbb{Z}_n$ is closed under addition, but not under division, whereas $\mathbb{Z}_n^\times$ is closed under division, but not under addition. Very roughly, a *field* is a set with notions of addition and multiplication, which is closed both under addition *and*

Date: March 12th, 2013.

under division (except division by 0, of course). We know many examples of fields: $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ all spring to mind. All of these are infinite sets. Must any field be infinite? The answer is no: for any prime p, $\mathbb{Z}_p$ is a finite field. Fields are particularly nice universes to do math in, because one can solve equations in them. (By contrast, it's rather difficult to do this in sets which don't have division or addition.) As we shall see, this will be the key to proving that $\mathbb{Z}_p^\times$ has a primitive root.