LECTURES 18–20: SUMMARY

In these lectures, we proved the following fundamental theorem:

Theorem 1. *$\mathbb{Z}_p^\times$ has a primitive root for every prime p.*

Recall that given $a \in \mathbb{Z}_p^\times$, the set *generated* by a is defined $\langle a \rangle := \{a^k : k \in \mathbb{Z}\} \subseteq \mathbb{Z}_p^\times$. The *order* of a in $\mathbb{Z}_p^\times$, denoted $\ell_a(n)$, is defined to be the number of distinct elements of $\mathbb{Z}_p^\times$ generated by a. In symbols: $\ell_a(n) := |\langle a \rangle|$. Finally, we say $g \in \mathbb{Z}_p^\times$ is a *primitive root* of $\mathbb{Z}_p^\times$ if and only if $\langle g \rangle = \mathbb{Z}_p^\times$.

Thus, Theorem 1 asserts that for every prime p, there exists some element $g_p \in \mathbb{Z}_p^\times$ such that $\mathbb{Z}_p^\times = \langle g_p \rangle$. In fact, we will prove something stronger: we shall show that $\mathbb{Z}_p^\times$ has precisely $\varphi(p-1)$ primitive roots. Rather than presenting the proof linearly, I'll present it in stages. First, the bird's eye view:

Proof. Let

$$\psi(n) := \Big|\Big\{a \in \mathbb{Z}_p^\times : \ell_a(p) = n\Big\}\Big|.$$

Note that $\psi(n)$ does *not* say anything about which elements have order n; it merely counts them. Thus in $\mathbb{Z}_7^\times$, we have $\psi(2) = 1$ and $\psi(3) = 2$.

Here are the steps of the proof. We will justify the steps subsequently.

<u>STEP 1:</u> $\psi(n) \leq \varphi(n)$ for all $n \in \mathbb{N}$.

<u>STEP 2:</u> $\displaystyle\sum_{d|p-1} \psi(d) = p - 1.$

<u>STEP 3:</u> $\displaystyle\sum_{d|p-1} \varphi(d) = p - 1.$

<u>STEP 4:</u> WIN.

More precisely, combining steps 2 and 3 gives

$$\sum_{d|p-1} \Big(\varphi(d) - \psi(d)\Big) = 0.$$

Step 1 implies that each term in this sum is non-negative. The only way a sum of non-negative terms can equal 0 is for every term to be 0. We have thus shown that for all $d \mid p-1$,

$$\psi(d) = \varphi(d).$$

Taking $d = p - 1$ concludes the proof. ∎

Date: March 14th, 19th, and 21st, 2013.

Of course, this isn't really a proof until we prove the missing steps.

Proof of Step 1. First, note that $\varphi(n) \geq 1$ for all $n \in \mathbb{N}$ (why?). Thus, if $\psi(n) < 1$, we're done.

Suppose that $\psi(n) \geq 1$. By definition, this means that there exists some $a \in \mathbb{Z}_p^\times$ such that $|\langle a \rangle| = n$. The proof now proceeds in three steps:

STEP I: Every element of order n is a solution to $x^n = 1$.

STEP II: The set of all solutions of $x^n = 1$ in $\mathbb{Z}_p^\times$ is $\{1, a, a^2, \ldots, a^{n-1}\}$.

STEP III: a^k has order n in $\mathbb{Z}_p^\times$ if and only if $(k, n) = 1$.

Combining these three steps immediately implies that the set of all elements of $\mathbb{Z}_p^\times$ of order n is precisely the set $\{a^k : k \leq n, (k, n) = 1\}$, whence $\psi(n) = \varphi(n)$. Thus, once we prove the three steps above, our proof of Step 1 will be complete.

Proof of STEP I

This is an easy exercise. □

Proof of STEP II

First, we verify that each element of the set $\{1, a, a^2, \ldots, a^{n-1}\}$ is a solution to $x^n = 1$:

$$(a^k)^n = (a^n)^k = 1^k = 1.$$

Thus, we have found n distinct solutions to the equation $x^n = 1$. It turns out (see Lemma 2 below) that $x^n = 1$ cannot have more than n distinct solutions in $\mathbb{Z}_p^\times$; STEP II immediately follows. □

Proof of STEP III

Suppose $(k, n) = 1$. I claim that

$$\langle a^k \rangle = \langle a \rangle.$$

Clearly, $\langle a^k \rangle \subseteq \langle a \rangle$. (Why?) To prove the other inclusion, note that there exist integers $x, y \in \mathbb{Z}$ such that $kx + ny = 1$. Then for any $\ell \in \mathbb{Z}$,

$$a^\ell = a^{kx\ell + ny\ell} = (a^k)^{x\ell} = (a^k)^{x\ell} \in \langle a^k \rangle.$$

Thus, $\langle a^k \rangle = \langle a \rangle$, so $|\langle a^k \rangle| = |\langle a \rangle| = n$ as claimed.

Now suppose instead that $(k, n) = d > 1$. Then

$$(a^k)^{n/d} = (a^n)^{k/d} = 1.$$

Thus $|\langle a^k \rangle| \leq n/d < n$. □

This concludes the proof of Step 1 (aside from Lemma 2, which will be proved below). QED

Here's a question to check whether you understood the proof. In Theorem 1, we're trying to prove that $\psi(n) = \varphi(n)$. In the proof of Step 1 above, we also proved that $\psi(n) = \varphi(n)$. So why do we need Steps 2, 3, and 4 in the proof of Theorem 1?

The proof of Step 1 is still incomplete, because we crucially relied on a result (Lemma 2) which we haven't yet proved. We will return to this soon, after proving Step 2.

Proof of Step 2. I'll give two proofs: one in words, one in symbols.

In words: Every element of $\mathbb{Z}_p^\times$ has *some* order; moreover, this order must divide $\varphi(p) = p - 1$. (Why?) Thus, $\displaystyle\sum_{d|p-1} \psi(d)$ is exactly the total number of elements of $\mathbb{Z}_p^\times$, namely, $p - 1$.

Now in symbols:

$$\sum_{d|p-1} \psi(d) = \sum_{d|p-1} \sum_{\substack{a \in \mathbb{Z}_p^\times \text{ s.t.} \\ |\langle a \rangle| = d}} 1 = \sum_{a \in \mathbb{Z}_p^\times} \sum_{\substack{d|p-1 \text{ s.t.} \\ |\langle a \rangle| = d}} 1 = \sum_{a \in \mathbb{Z}_p^\times} 1 = p - 1.$$

Either way, we conclude the proof. QED

Proof of Step 3. This is problem 3.7 from your problem set. QED

We have thus completely proved Theorem 1, except for the following (which we used in STEP I during the proof of Step 1):

Lemma 2. *Given any monic polynomial $f \in \mathbb{Z}[x]$ of degree $n \geq 1$. Then the equation $f(x) = 0$ has at most n distinct solutions in $\mathbb{Z}_p$.*

Recall that $\mathbb{Z}[x]$ is the collection of all polynomials whose coefficients are all integers. Given a polynomial $f(x) = c_k x^k + c_{k-1}x^{k-1} + \cdots + c_1 x + c_0$ with $c_k \neq 0$, we say the *degree* of f is k, and that f is *monic* iff $c_k = 1$.

Proof of Lemma 2. We proceed by induction on n. If $n = 1$, the theorem is clearly true (why?). Now suppose $f \in \mathbb{Z}[x]$ is monic of degree $n > 1$, and that the theorem is true for all polynomials in $\mathbb{Z}[x]$ of degree $n - 1$. If f has no roots in $\mathbb{Z}_p$, we're done, so we suppose that there exists $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ in $\mathbb{Z}_p$. We can write

$$f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$$

whence

$$\begin{aligned} f(x) - f(\alpha) &= (x^n - \alpha^n) + c_{n-1}(x^{n-1} - \alpha^{n-1}) + \cdots + c_1(x - \alpha) \\ &= (x - \alpha) \cdot g(x) \end{aligned}$$

for some monic $g \in \mathbb{Z}[x]$ of degree $n - 1$. Now, α may or may not be a root of g. I claim that, with the possible exception of α, the polynomials f and g have precisely the same roots in $\mathbb{Z}_p$. To see this, take any $\beta \not\equiv \alpha \pmod{p}$ such that $f(\beta) \equiv 0 \pmod{p}$. Then

$$(\beta - \alpha)g(\beta) = f(\beta) - f(\alpha) \equiv 0 \pmod{p},$$

and since $\beta - \alpha \not\equiv 0 \pmod{p}$, we deduce that $g(\beta) \equiv 0 \pmod{p}$ as claimed. This means that f has at most one more root in $\mathbb{Z}_p$ than g does. But by induction, g has at most $n - 1$ distinct roots. □