Tuesday, October 8

Reminder: A primitive root modulo m is an integer with order $\phi(m)$.

Theorem: For every prime p, there exists a primitive root (and hence $\phi(\phi(p)) = \phi(p-1)$ primitive roots).

— Two proofs incoming!

Lemma: Let q^r be a prime power with $q^r \mid (p-1)$. Then there are $q^r - q^{r-1}$ residue classes of order $q^r \pmod p$.
(Hence there's at least 1)

- Strategy: since q is prime, we'll use $n = q^r \iff n \mid q^r$ and $n \nmid q^{r-1}$.

Proof: First, the order of $a \pmod p$ divides q^r if and only if $a^{q^r} \equiv 1 \pmod p$.

By a corollary from Thursday, this congruence has exactly q^r solutions.

- Similarly, the order of $a \pmod p$ divides q^{r-1} if and only if $a^{q^{r-1}} \equiv 1 \pmod p$; since still $q^{r-1} \mid (p-1)$, the same corollary gives q^{r-1} solutions of $a^{q^{r-1}} \equiv 1 \pmod p$.

— Difference: $q^r - q^{r-1}$ residue classes of order q^r. //

Proof #1 of Theorem:

- $p=2$ is trivial.

For $p \geq 3$, write $p-1 = q_1^{r_1} q_2^{r_2} \cdots q_k^{r_k}$ where the $q_j^{r_j}$ are powers of distinct primes. For each $1 \leq j \leq k$, let a_j be an element of order $q_j^{r_j}$ (mod p). Set $a = a_1 a_2 \cdots a_j$. The orders of the a_j are pairwise coprime, so by (☆) of Proposition from Thursday the order of the product equals the product of the orders: the order of a (mod p) is $q_1^{r_1} q_2^{r_2} \cdots q_k^{r_k} = p-1$; so a is a primitive root (mod p). //

__Lemma__. For $n \geq 1$, we have $\sum_{d \mid n} \phi(d) = n$.

(sum is over (positive) divisors d of n)

__Slick proof__: Reduce all n fractions $\left\{ \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n} \right\}$ to lowest terms. Every fraction $\left\{ \frac{n/d}{n}, \frac{2n/d}{n}, \ldots, \frac{d \cdot n/d}{d} \right\}$ reduces to $\left\{ \frac{1}{d}, \frac{2}{d}, \ldots, \frac{d}{d} \right\}$; exactly $\phi(d)$ of these are already in lowest terms (numerators coprime to d). Count the n fractions according to their lowest-terms denominator:

$$n = \sum_{d \mid n} \#\text{fractions w/ denominator } d$$

$$= \sum_{d \mid n} \phi(d).$$

Proof #2 of Theorem: We prove, by strong induction on k, that the number of elements of order k (mod p) is exactly
$$\begin{cases} 0, & \text{if } k \nmid (p-1), \\ \phi(k), & \text{if } k \mid (p-1). \end{cases}$$
(In particular, there are $\phi(p-1)$ elements of order $p-1$ — primitive roots.)

- Base $k=1$: trivial.
- Given $k \geq 2$: if $k \nmid \phi(p)$ then done.

Suppose $k \mid (p-1)$. By a Corollary from Thursday, we know $x^k - 1$ has k roots (mod p). Each such root has order dividing k. Thus

$$k = \sum_{d \mid k} \#\{\text{elements of order } d\}$$
$$= \#\{\text{elements of order } k\} + \underbrace{\sum_{\substack{d \mid k \\ d<k}} \phi(d)}.$$
by induction hypothesis

But also
$$k = \sum_{d \mid k} \phi(d)$$
$$= \phi(k) + \underbrace{\sum_{\substack{d \mid k \\ d<k}} \phi(d)}.$$

Hence
$$\#\{\text{elements of order } k\} = \phi(k). \quad //$$