Math 3110: Existence of Primitive Roots

April 11, 2019

Thank you to Khaled Allen for scribing some of this.

Overview. We wish to show there are primitive roots, i.e. elements of order $\phi(p)$ modulo p. To do this, we more generally count the elements of order λ modulo p. If we have one element of order λ, we are able to find $\phi(\lambda)$ total elements amongst its powers. We are also able to rule out the existence of more elements of order λ because that would mean more roots of the polynomial $T^\lambda - 1$, and we can bound the number of roots of any polynomial. Therefore there are either 0 or $\phi(\lambda)$ elements of order λ. Finally, we use a clever counting argument on fractions to show that if we don't have a full $\phi(\lambda)$ in every case, we simply wouldn't have enough invertible elements modulo p at all. Hence the number of elements of order λ is exactly $\phi(\lambda)$. In particular, there are some elements of every order, including full order, i.e. primitive roots.

Proposition 1. *Let p be a prime. Let T be a variable. Let $f(T)$ be a polynomial of degree $d \geq 1$ with integer coefficients. Then $f(T)$ has at most d roots modulo p.*

Note: In other words, there are at most d distinct residues x modulo p such that $f(x) \equiv 0 \pmod{p}$.

Proof. Let us set notation and write

$$f(T) = c_d T^d + c_{d-1} T^{d-1} + \cdots + c_1 T + c_0.$$

Let a be a root of f, i.e. $f(a) \equiv 0 \pmod{p}$. First we will show that $f(T)$ has a linear factor $T - a$. We have

$$\begin{aligned} f(T) &\equiv f(T) - f(a) \pmod{p} \\ &\equiv c_d(T^d - a^d) + c_{d-1}(T^{d-1} - a^{d-1}) + \cdots + c_1(T - a) \pmod{p} \\ &\equiv (T - a)\left(c_d\left(\frac{T^d - a^d}{T - a}\right) + c_{d-1}\left(\frac{T^{d-1} - a^{d-1}}{T - a}\right) + \cdots + c_1\left(\frac{T - a}{T - a}\right)\right) \pmod{p} \end{aligned}$$

There is a useful identity that $x - y$ always divides $x^n - y^n$ (as polynomials with integer coefficents) for positive integers n:

$$\frac{x^n - y^n}{x - y} = x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}.$$

In particular, we have shown that

$$f(T) \equiv (T - a)g(T) \pmod{p}$$

where $g(T)$ is a polynomial of degree at most $d - 1$.

Now we can consider any root b of f. Then, plugging in b, we have

$$0 \equiv f(b) \equiv (b - a)g(b) \pmod{p}.$$

But *since p is prime*, a product is zero modulo p if and only if one of the factors is zero modulo p. Hence,

$$\text{either} \quad b \equiv a \pmod{p} \quad \text{or} \quad g(b) \equiv 0 \pmod{p}.$$

Now we use induction on the degree of the polynomial. The base case is that of a linear polynomial, i.e. degree one, which has exactly one root. Since $g(T)$ is of lower degree, in fact of degree at most $d - 1$, we can assume (as the inductive hypothesis) that it has at most $d - 1$ roots. Hence $f(T)$ has at most d roots (the roots of $g(T)$ or the value a).

Proposition 2. *Let p be prime. Suppose there exists an element a of order $\lambda \mod p$. Then the number of elements of order λ is $\phi(\lambda)$.*

Proof. Let p be a prime. Suppose we have an element a of order λ. In particular, $a^\lambda \equiv 1 \mod p$, i.e. a is a root of the polynomial $T^\lambda - 1$ modulo p.

Then any power $a^0, a^1, \ldots, a^{\lambda-1}$ of a will also be a root of $T^\lambda - 1 \equiv 0 \mod p$, since if we set $T = a^n$, then

$$\begin{aligned} T^\lambda - 1 &\equiv (a^n)^\lambda - 1 \pmod p \\ &\equiv (a^\lambda)^n - 1 \pmod p \\ &\equiv 1 - 1 \pmod p \\ &\equiv 0 \pmod p. \end{aligned}$$

Then $a^0, a^1, \ldots, a^{\lambda-1}$ give us λ distinct roots of $T^\lambda - 1 \mod p$ and so by the previous Proposition, there are no more roots.

But any element of order λ is a root of $T^\lambda - 1$ and hence a power of a. Therefore we have reduced our search for elements of order λ to searching in the list of powers of a.

However, some of these powers of a may be of lower order (for example, $a^0 = 1$). So we will compute the order of a^e for any $1 < e \leq \lambda - 1$. In fact, we will show its order is $\frac{\lambda}{\gcd(e,\lambda)}$.

First, its order is at most this, because

$$(a^e)^{\frac{\lambda}{\gcd(e,\lambda)}} \equiv a^{\mathrm{lcm}(e,\lambda)} \equiv a^{\text{a multiple of } \lambda} \equiv 1 \mod p.$$

But note that the exponent $\mathrm{lcm}(e, \lambda)$ is the *smallest* multiple of e such that $a^x \equiv 1 \mod p$ (because $a^x \equiv 1$ only for multiples of λ). Therefore the order of a^e is $\frac{\lambda}{\gcd(e,\lambda)}$.

Therefore a^e is of order λ if and only if $\gcd(e, \lambda) = 1$. So the number of a^e of order λ is exactly $\phi(\lambda)$. □

The next proposition is called the Totient Sum Formula.

Proposition 3. *Let $n > 1$ be an integer. Then*

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

Proof. We prove this by showing that there are two ways to count the fractions of denominator n in the interval $(0, 1]$ (not necessarily in reduced form).

The first is to allow the numerators to range from 1 to n, hence there are n such fractions.

The second is to remark that this is the same as the set of reduced fractions with denominator dividing n. This is because any fraction with denominator n which is not reduced, reduces to one of these fractions, and any reduced fraction with denominator dividing n can be multiplied top and bottom to have denominator n.

So let us count the reduced fractions of denominator $d \mid n$. There are $\phi(d)$ allowable numerators, hence $\phi(d)$ such fractions. Summing up over d, we have

$$\sum_{d|n} \phi(d)$$

total fractions in our set. □

Theorem 1. *There are $\phi(p-1)$ primitive roots modulo p.*

Proof. Primitive roots are to be found amongst the invertible elements modulo p. There are $p-1$ total invertible elements, each of order $\lambda \mid p-1$, for some λ. We know that the number of elements of order λ is either 0 or $\phi(\lambda)$. Hence,

$$p-1 = \sum_{\lambda|p-1} (\text{number of elements of order } \lambda) = \sum_{\lambda|p-1} (0 \text{ or } \phi(\lambda))\,.$$

But we also know, from the Totient Sum Formula, that

$$p-1 = \sum_{\lambda|p-1} \phi(\lambda).$$

Hence none of the summands in the first displayed equation can actually be 0. That is, for each λ, the number of elements of order λ is exactly $\phi(\lambda)$. In particular, our theorem is this fact with $\lambda = p-1$. $\square$