Lecture notes on primitive roots

Siddhartha Sahi
Rutgers University

October 23, 2007

1 The fundamental theorem of algebra mod p

In number theory we consider polynomials with integer coefficients

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n$$

An integer a is said to be a root of f mod m, if $f(a)$ is divisible by m. We say that f has "k roots mod m" if there are k roots among the integers $0, 1, \ldots, m-1$. Any other root of f will be congruent to one of these, and any complete residue system mod m will contain exactly k roots.

If all coefficients of f are divisible by m, we say that $f \equiv 0 \bmod m$, in this case every a is a root of f mod m.

The fundamental theorem of algebra holds for roots modulo a prime p.

Theorem 1 *Let p be a prime and $f(x)$ a polynomial of degree n with integer coefficients. If $f \not\equiv 0 \bmod p$, then $f(x)$ has at most n roots* mod p.

Proof. We proceed by induction on n. For $n = 0$ the polynomial $f(x)$ is a constant a_0 where $p \nmid a_0$. Hence f has no roots mod p, and the result holds.

We now assume the result for polynomials of degree $\leq n-1$ and consider

$$f(x) \equiv a_0 + a_1 x + \ldots + a_n x^n.$$

Suppose f has $n+1$ roots mod p, we need to show that $f \equiv 0 \bmod p$.

Let $b_1, b_2, \ldots, b_{n+1}$ be roots of f and define

$$\begin{aligned} g(x) &= a_n (x - b_1)(x - b_2) \ldots (x - b_n) \\ h(x) &= f(x) - g(x). \end{aligned}$$

Note that $\deg_p(h) \leq n-1$, since the degree n terms cancel. Also $h(b_i) = f(b_i) - g(b_i) \equiv 0 \bmod p$, for all $i = 1, \ldots, n$. Hence by induction $h \equiv 0 \bmod p$.

Now $g(b_{n+1}) = f(b_{n+1}) - h(b_{n+1}) \equiv 0 \bmod p$, hence p divides

$$g(b_{n+1}) = a_n (b_{n+1} - b_1)(b_{n+1} - b_2) \ldots (b_{n+1} - b_n)$$

Now $p \nmid b_{n+1} - b_i$, since the b_i are incongruent mod p. Therefore p divides a_n, and hence $g \equiv 0 \bmod p$.

Hence $f = h + g \equiv 0 \bmod p$ as well. ■

2 Order mod m

Definition 2 *If m and a are positive integers, we define $o_m(a)$ (the order of a mod m) to be the smallest integer $h > 0$ such that $a^h \equiv 1 \bmod m$.*

[If there is no such h we say $o_m(a) = \infty$.]

Lemma 3 *If $a^n \equiv 1 \bmod m$ then $o_m(a)$ divides n.*

Proof. Let $h = o_m(a)$ and write $n = qh + r$ where $0 \le r < h$. Now

$$1 \equiv a^n = a^{qh+r} = a^{qh}a^r = \left(a^h\right)^q a^r \equiv (1)^q a^r = a^r \pmod{m}$$

Since $r < h = o_m(a)$, this forces $r = 0$. Hence $n = qh$ and h divides n. ■

Proposition 4 *If $\gcd(a,m) > 1$ then $o_m(a) = \infty$. If $\gcd(a,m) = 1$ then $o_m(a)$ divides $\phi(m)$.*

Proof. If $\gcd(a,m) = d > 1$ then $d|a^h$ for all $h > 0 \Rightarrow d \nmid a^h - 1$. Since d divides m, $m \nmid a^h - 1 \Rightarrow a^h \not\equiv 1 \bmod m$ for all $h > 0 \Rightarrow o_m(a) = \infty$.

If $\gcd(a,m) = 1$, then by Euler's theorem $a^{\phi(m)} \equiv 1 \pmod{m}$. So by the previous lemma $o_m(a)$ divides $\phi(m)$. ■

Lemma 5 *Suppose $\gcd(a,m) = 1$; let $\langle a \rangle = \left\{a^1, a^2, \ldots, a^h\right\}$ where $h = o_m(a)$.*

1. *The elements of $\langle a \rangle$ are coprime to m and pairwise incongruent $\bmod m$.*
2. *$\langle a \rangle$ contains at most $\phi(h)$ integers a^k such that $o_m\left(a^k\right) = h$.*

Proof. Since a is coprime to m, so is each a^k. If $a^k \equiv a^{k+r} \bmod m$ for some $h > r \ge 0$, then $a^r \equiv 1 \bmod m$, which forces $r = 0$.

If $d = \gcd(k,h) > 1$, then $\left(a^k\right)^{h/d} = \left(a^h\right)^{k/d} \equiv 1^{k/d} = 1 \bmod m$. Thus $o_m\left(a^k\right) < h$ except perhaps for the $\phi(h)$ integers k satisfying $\gcd(k,h) = 1$. ■

If $o_m(a) = \phi(m)$ then the lemma implies that $\langle a \rangle$ is a reduced residue system mod m. In this case we say that a is a *primitive root* mod m.

Notation 6 *For each h, we write $S_m(h) = \{a : 0 < a < m,\ o_m(a) = h\}$.*

3 Primitive roots mod p

Lemma 7 *If p is a prime then $|S_p(h)| \le \phi(h)$ for each h.*

Proof. If $|S_p(h)| = 0$ there is nothing to prove. Otherwise pick $a \in S_p(h)$ and write $\langle a \rangle = \left\{a^1, a^2, \ldots, a^h\right\}$ as before. The h elements of $\langle a \rangle$ are incongruent mod p, and all satisfy the congruence

$$x^h \equiv 1 \bmod p.$$

Since p is a prime, this congruence has at most h roots mod p. Therefore any other root must be congruent to an integer from $\langle a \rangle$. In particular the elements of $S_p(h)$ must be congruent to elements of $\langle a \rangle$ satisfying $o_m\left(a^k\right) = h$. By the previous lemma, there are $\le \phi(h)$ such elements. ■

Theorem 8 *If p is a prime then* $|S_p(h)| = \begin{cases} \phi(h) & \text{if } h|(p-1) \\ 0 & \text{otherwise} \end{cases}$.

Proof. If $h \nmid (p-1)$ then by the previous proposition $|S_p(h)| = 0$, thus

$$\{1, 2, \ldots, p-1\} = \bigcup_{h|(p-1)} S_p(h).$$

Computing the sizes of these sets and using the previous lemma gives

$$p - 1 = \sum_{h|(p-1)} |S_p(h)| \leq \sum_{h|(p-1)} \phi(h) = p - 1.$$

Therefore the equality $|S_p(h)| = \phi(h)$ must hold for every $h|(p-1)$. ■

Corollary 9 *If p is a prime then there exist primitive roots* mod p.

Proof. $|S_p(p-1)| = \phi(p-1) \neq 0$. ■