Lecture 11: Primitive Roots

William Stein

Math 124 Harvard University **Fall 2001**

Key Idea: *There is an element of $(\mathbb{Z}/p\mathbb{Z})$ of order $p-1$.*

1 Polynomials over $\mathbb{Z}/p\mathbb{Z}$

Proposition 1.1. *Let $f \in (\mathbb{Z}/p\mathbb{Z})[x]$ be a nonzero polynomial over the ring $\mathbb{Z}/p\mathbb{Z}$. Then there are at most $\deg(f)$ elements $\alpha \in \mathbb{Z}/p\mathbb{Z}$ such that $f(\alpha) = 0$.*

Proof. We proceed by induction on $\deg(f)$. The cases $\deg(f) = 0, 1$ are clear. Write $f = a_n x^n + \cdots a_1 x + a_0$. If $f(\alpha) = 0$ then

$$\begin{aligned} f(x) &= f(x) - f(\alpha) \\ &= a_n(x^n - \alpha^n) + \cdots a_1(x - \alpha) + a_0(1-1) \\ &= (x-\alpha)(a_n(x^{n-1} + \cdots + \alpha^{n-1}) + \cdots a_1) \\ &= (x-\alpha)g(x), \end{aligned}$$

for some polynomial $g(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$. Next suppose that $f(\beta) = 0$ with $\beta \neq \alpha$. Then $(\beta - \alpha)g(\beta) = 0$, so, since $\beta - \alpha \neq 0$ (hence $\gcd(\beta - \alpha, p) = 1$, we have $g(\beta) = 0$. By our inductive hypothesis, g has at most $n-1$ roots, so there are at most $n-1$ possibilities for β. It follows that f has at most n roots. □

Proposition 1.2. *Let p be a prime number and let d be a divisor of $p-1$. Then $f(x) = x^d - 1 \in (\mathbb{Z}/p\mathbb{Z})[x]$ has exactly d solutions.*

Proof. Let e be such that $de = p - 1$. We have

$$\begin{aligned} x^{p-1} - 1 &= (x^d)^e - 1 \\ &= (x^d - 1)((x^d)^{e-1} + (x^d)^{e-2} + \cdots + 1) \\ &= (x^d - 1)g(x), \end{aligned}$$

where $\deg(g(x)) = p - 1 - d$. Recall that Fermat's little theorem implies that $x^{p-1} - 1$ has exactly $p-1$ roots in $\mathbb{Z}/p\mathbb{Z}$. By Proposition 1.1, $f(x)$ has *at most* $p - 1 - d$ roots and $x^d - 1$ has at most d roots, so $g(x)$ has exactly $p-1$ roots and $x^d - 1$ has exactly d roots, as claimed. □

WARNING: The analogue of this theorem is false for some $f \in (\mathbb{Z}/n\mathbb{Z})[x]$ with n composite. For example, if $n = n_1 \cdot n_2$ with $n_1, n_2 \neq 1$, then $f = nx$ has at least *two* distinct zeros, namely 0 and $n_2 \neq 0$.

2 The Structure of $(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, \ldots, p-1\}$

In this section, we prove that the group $(\mathbb{Z}/p\mathbb{Z})^*$ is cylic.

Definition 2.1. A *primitive root* modulo p is an element of $(\mathbb{Z}/p\mathbb{Z})^*$ of order $p-1$.

Question: For which primes p is there a primitive root? (Ans. Every prime.)

Lemma 2.2. *Suppose $a, b \in (\mathbb{Z}/n\mathbb{Z})^*$ have orders r and s, respectively, and that* $\gcd(r, s) = 1$. *Then ab has order rs.*

This is a general fact about commuting elements of a group.

Proof. Since $(ab)^{rs} = a^{rs}b^{rs} = 1$, the order of ab is a divisor $r_1 s_1$ of rs, where $r_1 \mid r$ and $s_1 \mid s$. Thus

$$a^{r_1 s_1} b^{r_1 s_1} = (ab)^{r_1 s_1} = 1.$$

Raise both sides to the power r_2, where $r_1 r_2 = r$. Then

$$a^{r_1 r_2 s_1} b^{r_1 r_2 s_1} = 1,$$

so, since $a^{r_1 r_2 s_1} = (a^{r_1 r_2})^{s_1} = 1$,

$$b^{r_1 r_2 s_1} = 1.$$

This implies that $s \mid r_1 r_2 s_1$, and, since $\gcd(s, r_1 r_2) = 1$, it follows that $s = s_1$. A similar argument shows that $r = r_1$, so the order of ab is rs. □

Theorem 2.3. *For every prime p there is a primitive root mod p. In other words, the group $(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group of order $p-1$.*

Proof. Write

$$p - 1 = q_1^{n_1} q_2^{n_2} \cdots q_r^{n_r}$$

as a product of distinct primes q_i.

By Proposition 1.2, the polynomial $x^{q_i^{n_i}} - 1$ has exactly $q_i^{n_i}$ roots, and the polynomial $x^{q_i^{n_i-1}} - 1$ has exactly $q_i^{n_i-1}$ roots. Thus there is an $a_i \in \mathbb{Z}/p\mathbb{Z}$ such that $a_i^{q_i^{n_i}} = 1$ but $a_i^{q_i^{n_i-1}} \neq 1$. This a_i has order $q_i^{n_i}$. For each $i = 1, \ldots, r$, choose such an a_i. By repeated application of Lemma 2.2, we see that

$$a = a_1 a_2 \cdots a_r$$

has order $q_1^{n_1} \cdots q_r^{n_r} = p - 1$, so a is a primitive root. □

Remark 2.4. There are $\varphi(p-1)$ primitive roots modulo p, since there are $q_i^{n_i} - q_i^{n_i-1}$ ways to choose a_i. To see this, we check that two distinct choices of sequence $a_1, \ldots, a_r$ define two different primitive roots. Suppose that

$$a_1 a_2 \cdots a_r = a_1' a_2' \cdots a_r',$$

with a_i, a_i' of order $q_i^{n_i}$, for $i = 1, \ldots, r$. Upon raising both sides of this equality to the power $s = q_2^{n_2} \cdots q_r^{n_r}$, we see that $a_1^s = a_1'^s$. Since $\gcd(s, q_1^{n_1}) = 1$, there exists t such that $st \equiv 1 \pmod{q_1^{n_1}}$. It follows that

$$a_1 = (a_1^s)^t = (a_1'^s)^t = a_1'.$$

Upon canceling a_1 from both sides, we see that $a_2 \cdots a_r = a_2' \cdots a_r'$; by repeating the above argument, we see that $a_i = a_i'$ for all i. Thus, different choices of the a_i must lead to different primitive roots; in other words, if the primitive roots are the same, then the a_i were the same.

For example, there are $\varphi(16) = 2^4 - 2^4 = 8$ primitive roots mod 17:

```
? for(n=1,16,if(znorder(Mod(n,17))==16,print1(n," ")))
3 5 6 7 10 11 12 14
```

Example 2.5. In this example, we illustrate the proof of Theorem 2.3 when $p = 13$. We have

$$p - 1 = 12 = 2^2 \cdot 3.$$

The polynomial $x^4 - 1$ has roots $\{1, 5, 8, 12\}$ and $x^2 - 1$ has roots $\{1, 12\}$, so we take $a_1 = 5$. The polynomial $x^3 - 1$ has roots $\{1, 3, 9\}$, so set $a_2 = 3$. Finally, $a = 5 \cdot 3 = 15 = 2$. Note that the successive powers of 2 are

$$2,\ 4,\ 8,\ 3,\ 6,\ 12,\ 11,\ 9,\ 5,\ 10,\ 7,\ 1,$$

so 2 really does have order 12.

Example 2.6. The result is false if, e.g., p is replaced by a big power of 2. The elements of $(\mathbb{Z}/8\mathbb{Z})^*$ all have order dividing 2, but $\varphi(8) = 4$.

Theorem 2.7. *Let p^n be a power of an odd prime. Then there is an element of $(\mathbb{Z}/p^n\mathbb{Z})^*$ of order $\varphi(p^n)$. Thus $(\mathbb{Z}/p^n\mathbb{Z})^*$ is cyclic.*

I will not prove Theorem 2.7 in class. I will probably put a problem on your next homework set that will guide you to a proof.

3 Artin's Conjecture

Conjecture 3.1 (Emil Artin). *If $a \in \mathbb{Z}$ is not -1 or a perfect square, then the number $N(x, a)$ of primes $p \leq x$ such that a is a primitive root modulo p is asymptotic to $C(a)\pi(x)$, where $C(a)$ is a constant that depends only on a. In particular, there are infinitely many primes p such that a is a primitive root modulo p.*

Nobody has proved this conjecture for even a single choice of a. There are partial results, e.g., that there are infinitely many p such that the order of a is divisible by the largest prime factor of $p - 1$. (See, e.g., Moree, Pieter, *A note on Artin's conjecture.*)