Lecture 14: The primitive element theorem

In this lecture, it will be convenient to recall that $\mathbb{Z}_n$ is actually a ring, and that it is a field if and only if n is a prime. It follows that $\mathbb{Z}_p$ are examples of *finite fields.* There are in fact other examples of finite fields and they play an important role in the theory of error-correcting codes although we shall not deal with the general case in this course. Such fields are also called *Galois fields* named after the French mathematician Galois. The Galois field of order n is often denoted by $GF(n)$.

Let $\mathbb{F}$ be a finite field and denote by $\mathbb{F}^*$ the set of non-zero elements of $\mathbb{F}$. Under multiplication this set forms a finite abelian group called the *multiplicative group* of the field.

We now recall a fact about polynomials.

Lemma 0.1. *Let $p(x)$ be a non-zero polynomial of degree n whose coefficients are taken from the field $\mathbb{F}$. Then $p(x)$ has* at most *n roots in $\mathbb{F}$.*

Proof. This result relies on the remainder theorem for polynomials. If $b(x)$ is a polynomial of degree n and $a(x)$ is a polynomial of degree $m \leq n$ then either $a(x)$ exactly divides $b(x)$ or we may write $b(x) = q(x)a(x) + r(x)$ where $r(x)$ is polynomial of degree strictly less than that of $a(x)$. We can deduce from this result the following: r is a root of a polynomial $p(x)$ if and only if $p(x) = (x-r)p_1(x)$ where the degree of $p_1(x)$ is one less than that of $p(x)$. If we repeatedly apply this result, we deduce that a polynomial of degree n has at most n roots. □

Theorem 0.2 (Primitive element)**.** *The multiplicative group of a finite field is cyclic.*

Proof. We denote the multiplicative group of our field $\mathbb{F}$ by G. Let the order of the multiplicative group of our field be n. By Lagrange's theorem, the order of each element of G divides n.

For each $d \mid n$, define the subset X_d of G which consists of all elements whose order is exactly d. Thus $X_1 = \{1\}$ since the identity is the only element with order 1. The union of the sets X_d is G and they are pairwise disjoint although some of them might be empty. It follows that

$$n = \sum_{d|n} |X_d| \,.$$

We shall prove the following: if there is an element of order d then there are exactly $\phi(d)$ elements of order d. This means in terms of our notation above that if $X_d \neq \emptyset$ then $|X_d| = \phi(d)$. We show first how this may be used to deduce the theorem. We have proved that

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

This means that in fact *none* of the sets X_d can be empty. In particlar, there must be $\phi(d)$ elements of order d: these elements will all be generators of the multiplicative group and so the group is cyclic. This is a nice example of how by merely counting we can prove that something exists.

We now prove the claim. Let a be an element of order d dividing n. We shall prove that there are exactly $\phi(d)$ elements of order d. Specifically, we shall prove that the elements

$$a^j \text{ where } 1 \leq j \leq d-1, \gcd(j, d) = 1$$

are precisely all the elements of order d.

From our work on the subgroup generated by an element in a group, we know that the elements $a, a^2, \ldots, a^{d-1}, a^d = 1$ are distinct. By Langrange's theorem applied to the subgroup generated by a, we know that they all have orders that divide d. Now the polynomial $x^d - 1$ with coefficients from $\mathbb{F}$ has at most d roots in $\mathbb{F}$ from the Remainder Theorem for polynomials, and any element b such that $b^d = 1$ will be a root. It follows that all the elements of order d must be amongst the powers of a.

However, not all powers of a have *order* d. Consider a^i where $\gcd(d, i) = d' > 1$. Then the order of a^i is strictly less than d which we now prove. We have that $d = d'j$ and $i = d'k$ for some j and k. Now $(a^i)^j = a^{ij}$ and ij is divisible by d and so $a^{ij} = 1$. Thus the order of a^i is at most j and j is a proper factor of d and therefore strictly smaller than d. We have therefore shown that a^i has order strictly less than d.

Suppose now that a^i is such that $\gcd(d, i) = 1$. We prove that a^i has order d. Suppose it has order d' smaller than d. Then $a^{id'} = 1$ and so d divides id'. It follows that d divides d'.

Thus the elements of order d in the group G are precisely the powers a^i of a where $i \leq d$ and $\gcd(d, i) = 1$. There are $\phi(d)$ such elements, which was what we were trying to prove. $\square$

The proof of the following is now immediate.

Corollary 0.3. *The group $\mathbb{U}_p$, where p is a prime, is cyclic.*

Let's have a look at an example. We study the generators of the cyclic group $\mathbb{U}_{13}$. This group has order 12. According to the theory, there will be $\phi(12)$ generators. We know that $\phi(12) = 4$. I claim that

2 is a generator. Let's see why. The top row gives the power of 2 and the bottom row gives the reduction mod 13.

2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}	2^{12}
2	4	8	3	6	12	11	9	5	10	7	1

These are all the (representatives) of the elements of $\mathbb{U}_{13}$. There are three other generators according to the theory: what are they? Check your answers.

It would be worth while developing this example and verifying that our claims in the theorem above are true.

There is in fact a complete classification of when the groups $\mathbb{U}_n$ are cyclic. I state this below but I shall not prove it in this course.

Theorem 0.4. *The group $\mathbb{U}_n$ is cyclic if and only if $n = 1, 2, 4, p^e$ or $2p^e$ where p is an odd prime.*

Show that $\mathbb{U}_{10}$ and $\mathbb{U}_{12}$ both have order 4 but only one of them is cyclic.

For historical reasons the generators of the groups $\mathbb{U}_p$ are called *primitive roots*. In the following table, the smallest primitive root in each case is given.

Prime	Primitive root
3	2
5	2
7	3
11	2
13	2
17	3
19	2
23	5
29	2