Primitive Roots

Reading

- Section 10.3

Practice Problems

10.3 1, 2, 3, 4, 5, 6, 7, 11
10.3 (Challenge, Optional) 15-23 (These problems examine the primitive root theorem when the modulus is not prime)

Notes

Primitive Roots: Definition

We have shown in previous sections that the order of each element must divide $\phi(n)$. Elements that achieve this largest possible value are special:

> Let p be prime and $\bar{a} \in \mathbb{Z}_p$. We say that $\bar{a}$ is a **primitive root** in $\mathbb{Z}_p$, or a *primitive root modulo* p, if $ord(\bar{a}) = p - 1$.
>
> If $\bar{a}$ is a primitive root, then $1, \bar{a}, \bar{a}^2, \ldots, \bar{a}^{p-2}$ are all distict elements, all reduced residues, and since there are $\phi(p) = p - 1$ of them they must be all the reduced residues. We say that the primitive root **generates** all reduced residues.

The main result of this section will be that there is always a primitive root, a very nontrivial result.

Find primitive roots modulo 17 and modulo 19.

Primitive Root Theorem

The **Primitive Root Theorem** is fairly straightforward:

> Let p be a prime. Then there exists a primitive root modulo p.

Its proof will take many steps. The two main steps are as follows:

- We first show there are elements of order q^s, where $q^s | p - 1$ and q is a prime.
- We then show that if a, b are two elements with relatively prime orders, then the order of ab is the product, i.e. $ord(ab) = ord(a)ord(b)$.
- We finally combine these two parts to get to our result.

Lemma 1 (existence of elements of prime power order)

Suppose p is prime and $q^s | p-1$. Then there is an element of order q^s in $\mathbb{Z}_p$.

Let us proceed with the proof:

- Since $q^s | p-1 = \phi(p)$, our previous work says that the equation $x^{q^s} = 1$ has q^s solutions.
- Similarly, the equation $x^{q^{s-1}} = 1$ has q^{s-1} solutions, all of which are also solutions of the previous equation.
- Since $q^s > q^{s-1}$, there must be a solution of the first equation that does not solve the other question.
- So there is an element $\bar{a}$ such that $\bar{a}^{q^s} = \bar{1}$ such that $\bar{a}^{q^{s-1}} \neq 1$.
- All we need is to show that $\bar{a}$ has order exactly q^s.
  - The order must divide q^s, so it must be q^k for some $k \leq s$.
  - If $k < s$ this would have led to $a^{q^{s-1}} = 1$, which is not true.
  - So q^s is the first power of $\bar{a}$ that could equal 1.

Let us do a demonstration of this:

Consider $p = 37$. Then $p - 1 = 36 = 2^2 3^2$. This lemma tells us that there must be elements of each of the order 1, 2, $2^2 = 4$, 3, $3^2 = 9$.

We focus on orders 2 and 2^2 for now. $36 = -1$ is of course of order 2. Note that $6^2 = 36$, so 6 has order 4. The four solutions to the equation $x^4 = 1$ would therefore be $1, 36 = -1, 6, -6 = 31$.

Now we want to look for elements of orders 3 and 3^2. A simple way to do so is to take any element and raise it to the 4-th power. Since $a^{36} = 1$, then for each element we have $(a^4)^9 = 1$. So if $a^4 \neq 1$ this is a good place to start.

To do this, we start with 2, then $2^4 = 16$. We know for sure that $16^9 = 1$, so we check $16^3 = 4096 = 26$. This is not 1. Therefore we found an element 16 of order 9. We also found an element, 26, of order 3.

So in total we have:

a	ord
1	1
36	2
6	4
16	9
26	3

Now we proceed to the second claim.

Lemma 2 (product of elements of relatively prime orders)

Let $\bar{a}, \bar{b} \in \mathbb{Z}_n$ be reduced residues whose orders $ord(\bar{a})$ and $ord(\bar{b})$ are relatively prime. Then the order of $\bar{a}\bar{b}$ is equal to $ord(\bar{a}) \cdot ord(\bar{b})$ i.e.:

$$ord(\bar{a}\bar{b}) = ord(\bar{a}) \cdot ord(\bar{b})$$

Let us proceed with the proof:

- Suppose $ord(\bar{a}) = r$ and $ord(\bar{b}) = s$.
- Then first of all it is clear that $(\bar{a}\bar{b})^{rs} = \bar{a}^{rs}\bar{b}^{rs} = \bar{1}$.
- Now suppose that for some power k we have $(\bar{a}\bar{b})^k = \bar{1}$. We will show that rs divides k. This will finish the proof.
  - Raising to r-th power we see that $(\bar{a}\bar{b})^{rk} = \bar{1}$.
  - This becomes $\bar{b}^{rk} = \bar{1}$.
  - So we must have $s|rk$.
  - Since s and r are relatively prime, then $s|k$.
  - A similar argument, starting with raising to the s-th power, will tell us that $r|k$.
  - Since s and r are relatively prime, it must therefore be the case that $sr|k$.

Let us continue our illustration from before. We have that 6 has order 4 and 16 has order 9, therefore $6 \cdot 16 = 22$ must have order $6 \cdot 9 = 36$. And we just found our primitive root! To confirm that, you will need to verify that $ord(22) = 36$ by excluding all other possibilities.

It should be noted that this is not the only primitive root, in fact there are exactly $\phi(36) = 12$ primitive roots. But that's a topic for later.

Proof of Primitive Root Theorem We now bring it all together.

- Suppose $p - 1 = q_1^{s_1} q_2^{s_2} \cdots q_m^{s_m}$, where the q_i are distict primes.
- By our previous lemma there are elements $x_1, x_2, \ldots, x_m$ with respective orders $q_1^{s_1}, q_2^{s_2}, \ldots, q_m^{s_m}$.
- By our other previous lemma, iterated m times, their product $x_1 x_2 \cdots x_m$ would have order equal to the product of the orders, namely $p - 1$.
- That is our primitive root.

Counting the Primitive Roots Now that we know primitive roots exist, we can determine exactly how many there are. From previous sections, we have:

Let p be prime and $\bar{a}$ be a primitive root modulo p. Then:

- For any j we have $\bar{a}^j = \frac{p-1}{\gcd(j,p-1)}$.
- $\bar{a}^j$ is a primitive root if and only if j is relatively prime to $p - 1$.
- There are exactly $\phi(p - 1)$ primitive roots.

Let us demonstrate this in our example with $p = 37$. We already found one primitive root, 22. We now find all primitive roots. They would be all the elements of the form 22^j where $\gcd(j, 36) = 1$. Let us find some of these elements:

j	x
1	22
5	13
7	2
11	18

There is a total of $\phi(36) = \phi(2^2)\phi(3^2) = 12$ such elements.