

## Class activity, Week 9

### Primitive Roots and Quadratic Residues

In this activity, we first investigate some of the properties of the *primitive roots* you discovered in the pre-class. We will also see why having a primitive root modulo  $n$  allows us to put a specific structure on the elements modulo  $n$ , and when this happens. Then at the end, we will use the primitive roots to obtain some information about quadratic residues modulo  $p$ , i.e. those elements that are squares modulo  $p$ .

### Testing for Primitive Roots

Using the definition, to determine if  $g$  is a primitive root modulo  $n$ , we need to check that none of  $g^2, g^3, \dots, g^{\phi(n)-1}$  is congruent to 1 modulo  $n$ . But that is a lot of work! Instead, using the next proposition, we can significantly reduce the number of powers of  $g$  that we need to compute to find whether  $g$  is a primitive root.

**Proposition 1:** An integer  $g$  is a primitive root modulo  $n$  if and only if for every  $p$  dividing  $\phi(n)$

$$g^{\frac{\phi(n)}{p}} \not\equiv 1 \pmod{n}.$$

**proof:** Suppose  $g$  is a primitive root. Then, by definition,  $g^k \not\equiv 1 \pmod{n}$  for all  $1 \leq k < \phi(n) - 1$ . Since  $\frac{\phi(n)}{p} < \phi(n)$ ,  $g^{\frac{\phi(n)}{p}} \not\equiv 1 \pmod{n}$ .

Suppose now that  $g$  is an element for which

$$g^{\frac{\phi(n)}{p}} \not\equiv 1 \pmod{n}$$

for every  $p$  dividing  $\phi(n)$ , and assume that the order of  $g$  is  $r < \phi(n)$ . We will reach a contradiction.

From Corollary 2 of the week 8 class activity, we know that  $r | \phi(n)$ . Consider  $\frac{\phi(n)}{r}$ . There is a prime factor  $p$  of  $\frac{\phi(n)}{r}$  and an integer  $m$  such that  $pm = \frac{\phi(n)}{r}$ . Then  $rm = \phi(n)$ . But this is contradiction because

$$g^{\frac{\phi(n)}{p}} \equiv (g^r)^m \equiv 1 \pmod{n}.$$

Therefore,  $r = \phi(n)$  and  $g$  is a primitive root. □

**1.** Check that 2 is a primitive root modulo 101 in an efficient way. (Note: If you need to calculate large powers modulo 101, say  $2^{60}$ , you can do this in two steps:  $2^{15}$  and reduce modulo 101, and then take the fourth power of the reduced expression. You will need different powers than 60; I used 60 as an example.)

**2.** Find a primitive root modulo 18. (Hint: A primitive root  $g$  modulo  $n$  has to be relatively prime to  $n$  for otherwise order of  $g$  is not defined. So that cuts down the number of  $g$ 's to try.)

## Structure of $\mathbf{Z}_n^\times$

Given a modulus  $n$ , we let  $\mathbf{Z}_n^\times$  denote the set of all residue classes with integers relatively prime to  $n$ . These integers are those for which we can find the order and there are  $\phi(n)$  such integers. In this section, we will show that the set  $\mathbf{Z}_n^\times$  has a specific structure when there is a primitive root, as you guessed in problem 2 in the pre-class.

3. Suppose  $a$  has order  $k$  modulo  $n$ .

a. If  $a^i \equiv a^j \pmod{n}$ , what is the relation between  $i$  and  $j$ ?

b. Justify why  $a^0, a^1, a^2, \dots, a^{k-1}$  are all different modulo  $n$ .

Using the above problem with the special case of  $a$  being a primitive root, we obtain the first half of the following theorem:

**Theorem 1:** If  $g$  is a primitive root modulo  $n$ , then any integer relatively prime to  $n$  is congruent to  $g^i$  modulo  $n$  for some  $i$ . Conversely, if  $g$  is an integer for which any integer relatively prime to  $n$  is congruent to  $g^i$  for some  $i$ , then  $g$  is a primitive root.

**proof:** Suppose  $g$  is a primitive root. Then  $g$  has order  $\phi(n)$ . Using the above problem, this says that  $g^0, g^1, \dots, g^{\phi(n)-1}$  are all different modulo  $n$ . Also note that  $g^i$  are all relatively prime to  $n$  if  $g$  is. But there are only  $\phi(n)$  residue classes which are relatively prime to  $n$ , so the powers of  $g$  must cover all these residue classes.

Suppose now that  $g$  is an integer such that every integer relatively prime to  $n$  is congruent to  $g^i$  for some  $i$ . Suppose the order of  $g$  is  $k$ . Then, from the above problem, there are \_\_\_\_\_ different integers modulo  $n$  which are of the form  $g^i$ . But there are \_\_\_\_\_ integers modulo  $n$  which are relatively prime to  $n$ . Therefore, \_\_\_\_\_ and  $g$  is a primitive root. □

This theorem motivates another definition for a primitive root: An element  $g$  of  $\mathbf{Z}_n^\times$  is a *primitive root* if every element of  $\mathbf{Z}_n^\times$  is congruent to  $g^k$  for some power  $k$ . For this reason, a primitive root is also called a *generator* of  $\mathbf{Z}_n^\times$ . For those of you familiar with groups, this basically translates into saying that “if there is a primitive root,  $\mathbf{Z}_n^\times$  is a cyclic group with any primitive root being a generator.”

4. Check that 3 and 7 are primitive roots modulo 10, and express each in terms of the other.

## Number of Primitive Roots

The next question to consider is that in cases when a primitive root exists, how many primitive roots are there total? If  $g$  is a primitive root, then every element is of the form  $g^k$ . So the question then becomes, “for which powers  $k$  is  $g^k$  still a primitive root?”

5. Given: 2 is a primitive root modulo 11.

a. Describe what this means.

b. Find the order of  $2^4, 2^7, 2^9$  modulo 11, using the information on the order of 2.

c. Generalizing your observations from part b, determine for which  $k$  the order of  $2^k$  is 10, i.e. how many primitive roots are there modulo 11?

We consider now another example with a larger modulus  $n = 101$ . We know from earlier that 2 is a primitive root modulo 101. We know that  $2^4, 2^{25}, 2^{75}$  are not primitive roots because

$$(2^4)^{25} \equiv 1 \pmod{101}, (2^{25})^4 \equiv 1 \pmod{101}, (2^{75})^4 \equiv 1 \pmod{101}.$$

But  $2^3, 2^7, 2^9, 2^{11}, \dots$  are primitive roots. More generally,  $2^k$  is a primitive root as long as  $\gcd(k, 100) = 1$  (where  $100 = \phi(101)$  is the order of 2). There are  $\phi(100)$  such  $k$ 's.

**Theorem 2:** Suppose there is a primitive root  $g$  modulo  $n$ . Then  $g^k$  is also a primitive root if and only if  $\gcd(k, \phi(n)) = 1$ . Therefore, there are  $\phi(\phi(n))$  primitive roots modulo  $n$ .

The following theorem (whose proof is omitted) describes for which  $n$  we can expect to find a primitive root in general.

**Theorem 3:** A primitive root modulo  $n$  exists if and only if  $n$  is of the form  $2, 4, p^r, 2p^r$  where  $p$  is an odd prime and  $r \geq 1$ .

## Quadratic residues

Recall how we defined quadratic residues modulo  $p$  a prime: If  $x^2 \equiv a \pmod{p}$  has a solution, then  $a$  is a quadratic residue. If  $x^2 \equiv a \pmod{p}$  does not have a solution, then  $a$  is a *quadratic non-residue*. We let  $R$  denote the set of quadratic residues, and  $N$  denote the set of quadratic nonresidues.

**Theorem 3:** If  $p$  is an odd prime,  $|R| = |N| = (p-1)/2$ , where  $|\cdot|$  denotes set cardinality.

**proof:** In order to determine how many quadratic residues modulo  $p$  there are, we consider how many different squares we have modulo  $p$ . In fact, it is enough to count the number of  $x^2$ 's modulo  $p$  where  $x = 1, 2, \dots, (p-1)/2$  because  $i^2 = (-i)^2$ . Also note that,  $x^2 \not\equiv y^2 \pmod{p}$  for  $x \not\equiv y \pmod{p}$  and  $1 \leq x, y \leq (p-1)/2$ . If they were we would have  $p | x^2 - y^2 = (x-y)(x+y)$  and neither  $x-y$  nor  $x+y$  are divisible by  $p$  since  $1 \leq x-y, x+y \leq p-1$ . So, each  $x = 1, 2, \dots, (p-1)/2$  produces a unique square modulo  $p$ . Therefore, there are  $(p-1)/2$  quadratic residues. There are a total of  $p-1$  elements relatively prime to  $p$ , therefore  $|N| = p-1 - (p-1)/2 = (p-1)/2$ .  $\square$

**6.** There is another way to see why Theorem 3 is true using the primitive roots. Recall that for every prime  $p$  there is a primitive root modulo  $p$ . Let  $g$  be a primitive root modulo  $p$ .

**a.** Recall that every element modulo  $p$  can be written as  $g^i$  for some power  $i$ . What is the condition on  $i$  for the  $g^i$  to be a square? What is the condition for  $g^i$  to be a non-square?

**b.** Using part a, justify why  $|R| = |N| = (p-1)/2$ .

So, using this last problem, we see that if we have a primitive root at hand, then it is easy to find the squares modulo  $p$ . However, finding a primitive root is a lot of work too. If we have to determine whether one element  $a$  modulo a large prime  $p$  is a quadratic residue, then it is not worth the trouble to find a primitive root. Instead, can we use the idea of the primitive root without finding one explicitly?

**7.** Suppose  $g$  is a primitive root modulo  $p$ .

**a.** Let  $a$  be a quadratic residue modulo  $p$ . Using  $g$ , justify why  $a^{(p-1)/2} \equiv 1 \pmod{p}$ .

**b.** Let  $a$  be a quadratic nonresidue modulo  $p$ . Using  $g$ , justify why  $a^{(p-1)/2} \not\equiv 1 \pmod{p}$ .

c. Noting that  $a^{p-1} \equiv 1 \pmod{p}$ , justify why  $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$ . Therefore, using part b, show that  $a^{(p-1)/2} \equiv -1 \pmod{p}$  if  $a$  is a quadratic nonresidue.

**Theorem 4:** (Euler's criterion) Suppose that  $p$  is an odd prime and  $p \nmid a$ . Then the congruence  $x^2 \equiv a \pmod{p}$  has two solutions if  $a^{(p-1)/2} \not\equiv 1 \pmod{p}$  and no solution if  $a^{(p-1)/2} \equiv -1 \pmod{p}$ .

8. Using Euler's criterion, determine whether the following equations have solutions:

a.  $x^2 \equiv 5 \pmod{101}$

b.  $x^2 \equiv 7 \pmod{101}$

**Note:** It should be noted that the Euler's criterion does not tell us what the solution  $x$  is. It only tells us that there is a solution. However, the test is actually pretty efficient. For large numbers, there are various fast exponentiation methods which make the testing in Euler's criterion fast.