

# PRIMITIVE ROOTS

DAVID SAVTT

## 1. INTRODUCTION

Earlier in this course, we looked at tables of powers (mod  $p$ ), such as this table of powers (mod 7):

$a^k$	1	2	3	4	5	6
1	1	1	1	1	1	1
2	2	4	1	2	4	1
3	3	2	6	4	5	1
4	4	2	1	4	2	1
5	5	4	6	2	3	1
6	6	1	6	1	6	1

Our observation, which led us to uncover Fermat's Little Theorem, was that there are 6 rows in the table (one row for each residue class (mod 7) which is relatively prime to 7) and that the 6<sup>th</sup> column in the table consists entirely of 1's. In fact, we were able to prove Euler's generalisation of Fermat's Little Theorem, which says that if  $(a, n) = 1$ , then

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Restated in terms of our tables of powers, this says that in the table of powers (mod  $n$ ), in which there are  $\phi(n)$  rows (corresponding to the  $\phi(n)$  residue classes (mod  $n$ ) which are relatively prime to  $n$ ), the  $\phi(n)$ <sup>th</sup> column will consist entirely of 1's. However, this theorem is quite far from being an answer to any question we might ask about these tables of powers. For example, is the  $\phi(n)$ <sup>th</sup> column necessarily the *first* column which consists entirely of 1's? Quite evidently not, as the following table of powers (mod 8) demonstrates.

$a^k$	1	2	3	4
1	1	1	1	1
3	3	1	3	1
5	5	1	5	1
7	7	1	7	1

If  $a$  is odd, then  $a^2 \equiv 1 \pmod{8}$ , so the 2<sup>nd</sup> column consists entirely of 1's, whereas  $\phi(8) = 4$ . So, we can ask questions like: given  $n$ , can we decide which column will be the first to be all 1's? Can we characterise those  $n$  such that the answer to the previous question is  $\phi(n)$ ?

Turning our focus to individual rows of the above tables, what is the earliest point that a 1 can appear in any individual row? Looking at the (mod 7) table, 1 appears for the first time in the 1<sup>st</sup>, 3<sup>rd</sup>, 6<sup>th</sup>, 3<sup>rd</sup>, 6<sup>th</sup>, and 2<sup>nd</sup> column for  $a = 1, 2, 3, 4, 5$ , and 6 respectively, and we might guess that in general if 1 appears earliest in the  $d$ <sup>th</sup> column for some row, then  $d$  should be a divisor of  $\phi(n)$ . We might also notice that in the table (mod 7), there were two rows (the powers of 3 and of 5) in which every number from 1 to 6 appeared as a power, whereas in the table (mod 8), there were no such rows. If there exist such rows, how many of them are there? Could their non-existence (mod 8) be connected to the fact that (mod 8), the earliest column of 1's was not the  $\phi(8)$ <sup>th</sup> column?

Let us now turn to answering as many of these questions as we can.

## 2. THE ORDER OF A NUMBER (MOD N)

**Definition 1.** If  $(a, n) = 1$ , then the order of  $a \pmod{n}$ , denoted  $\text{ord}_n(a)$ , is defined to be the smallest positive integer  $k$  such that  $a^k \equiv 1 \pmod{n}$ . To put it another way, the order of  $a \pmod{n}$  is the first column in which 1 appears in the row of powers of  $a$  in the table of powers  $\pmod{n}$ .

This definition makes sense, because we certainly know that  $a^{\phi(n)} \equiv 1 \pmod{n}$ .

**Example 1.** For any  $n$ ,  $\text{ord}_n(1) = 1$ . Referring back to our table of powers  $\pmod{7}$ , we observe that  $\text{ord}_7(6) = 2$ ,  $\text{ord}_7(2) = \text{ord}_7(4) = 2$ , and  $\text{ord}_7(3) = \text{ord}_7(5) = 6$ .

As a first result, we can prove:

**Theorem 2.1.** If  $a^k \equiv 1 \pmod{n}$ , then  $\text{ord}_n(a)$  divides  $k$ .

*Proof.* Using the division algorithm, write  $k = q \cdot \text{ord}_n(a) + r$ , where  $r$  is a nonnegative integer smaller than  $\text{ord}_n(a)$ . This tells us that

$$a^k = a^{q \cdot \text{ord}_n(a) + r} = a^r (a^{\text{ord}_n(a)})^q \equiv a^r \cdot 1^q \equiv a^r \pmod{n}.$$

Since  $a^k \equiv 1 \pmod{n}$ , we therefore know that  $a^r \equiv 1 \pmod{n}$ . Since  $\text{ord}_n(a)$  is the smallest *positive* integer power of  $a$  which is  $1 \pmod{n}$ , and since  $r < \text{ord}_n(a)$ , it is therefore impossible for  $r$  to be positive. Consequently,  $r = 0$  and  $\text{ord}_n(a)$  divides  $k$ .  $\square$

The converse is evident, i.e. if  $\text{ord}_n(a)$  divides  $k$  then certainly  $a^k \equiv 1 \pmod{n}$ , so we can actually say that  $a^k \equiv 1 \pmod{n}$  if and only if  $\text{ord}_n(a)$  divides  $k$ . We can also now prove one of our earlier conjectures:

**Theorem 2.2.** If  $(a, n) = 1$ , then  $\text{ord}_n(a)$  divides  $\phi(n)$ .

*Proof.* By Euler's generalisation of Fermat's Little Theorem, we know that  $a^{\phi(n)} \equiv 1 \pmod{n}$ . The result then follows directly from the preceding theorem.  $\square$

We prove a useful result which allows us to calculate the order of  $a^k$  once we know the order of  $a$ .

**Theorem 2.3.** If  $(a, n) = 1$ , then  $\text{ord}_n(a^k) = \text{ord}_n(a) / (k, \text{ord}_n(a))$ .

*Proof.* We are trying to answer the question: for what  $l$  does  $(a^k)^l \equiv 1 \pmod{n}$ ? By Theorem 2.1, this congruence holds if and only if  $\text{ord}_n(a) \mid kl$ , and it follows from one of our results on divisibility and GCDs (specifically, question 10 on problem set 1) that this is the case if and only if  $\text{ord}_n(a) / (k, \text{ord}_n(a))$  divides  $l$ . Thus, the smallest positive value of  $l$  which makes  $(a^k)^l \equiv 1 \pmod{n}$  is  $\text{ord}_n(a) / (k, \text{ord}_n(a))$ , and so  $\text{ord}_n(a^k) = \text{ord}_n(a) / (k, \text{ord}_n(a))$ .  $\square$

**Example 2.** Using  $\text{ord}_7(3) = 6$ , we obtain  $\text{ord}_7(3^5) = 6 / (6, 5) = 6 / 1 = 6$ . Since  $3^5 \equiv 5 \pmod{7}$ , we conclude that  $\text{ord}_7(5) = 6$  as well.

Finally, we use the above result to prove a theorem which will be useful to us in the next section. The theorem states that if the orders of two elements are relatively prime, then the order of their product is the product of their orders, which allows us to construct elements of larger order from elements of smaller order.

**Theorem 2.4.** If  $\text{ord}_n(a)$  and  $\text{ord}_n(b)$  are relatively prime, then  $\text{ord}_n(ab) = \text{ord}_n(a) \cdot \text{ord}_n(b)$ .

*Proof.* If  $(ab)^k \equiv 1 \pmod{n}$ , then  $a^k \equiv b^{-k} \pmod{n}$ , so  $\text{ord}_n(a^k) = \text{ord}_n(b^{-k})$ . By Theorem 2.3, we therefore have

$$\text{ord}_n(a) / (k, \text{ord}_n(a)) = \text{ord}_n(b) / (-k, \text{ord}_n(b)).$$

Rewriting this as

$$\text{ord}_n(a) \cdot (-k, \text{ord}_n(b)) = \text{ord}_n(b) \cdot (k, \text{ord}_n(a)),$$

it follows that

$$\text{ord}_n(a) \mid \text{ord}_n(b) \cdot (k, \text{ord}_n(a)),$$

and using the fact that  $\text{ord}_n(a)$  and  $\text{ord}_n(b)$  are relatively prime we conclude that  $\text{ord}_n(a)$  divides  $(k, \text{ord}_n(a))$ , i.e.  $\text{ord}_n(a)$  divides  $k$ . Similarly,  $\text{ord}_n(b)$  divides  $k$ , and so in fact  $\text{ord}_n(a) \cdot \text{ord}_n(b)$  divides  $k$ . But certainly  $(ab)^{\text{ord}_n(a) \cdot \text{ord}_n(b)} \equiv 1 \pmod{n}$ , so as desired we obtain  $\text{ord}_n(ab) = \text{ord}_n(a) \cdot \text{ord}_n(b)$ .  $\square$

3. PRIMITIVE ROOTS

**Definition 2.** For a positive integer  $n$ , let  $A(n)$  be the maximum of  $\text{ord}_n(a)$  over all  $a$  with  $(a, n)=1$ .

**Example 3.**  $A(7) = 6$  and  $A(8) = 2$ .

Since  $\text{ord}_n(a)$  divides  $\phi(n)$  for any  $a$  relatively prime to  $n$ , it follows that  $A(n)$  also divides  $\phi(n)$ , and in particular  $A(n) \leq \phi(n)$ .

**Theorem 3.1.** If  $(a, n)=1$ , then  $\text{ord}_n(a)$  divides  $A(n)$ . In particular,  $a^{A(n)} \equiv 1 \pmod{n}$ , and so the  $A(n)$ <sup>th</sup> column in the table of powers  $(\text{mod } n)$  is the first column which consists entirely of 1's.

*Proof.* The second statement of the theorem follows immediately from the first statement. To prove the first statement, first observe that since  $\text{ord}_n(a)$  divides  $\phi(n)$  for any  $a$  relatively prime to  $n$ , any prime which divides  $\text{ord}_n(a)$  must also divide  $\phi(n)$ . This is a finite list of primes; call them  $p_1, \dots, p_l$ . Then  $\text{ord}_n(a)$  is always a product  $p_1^{\alpha_1} \cdots p_l^{\alpha_l}$ , and for each  $i$  we can select an  $a$  so that  $\alpha_i$  is as large as possible: in particular, choose  $a_i$  so that  $p_i^{A_i}$  is the power of  $p_i$  dividing  $\text{ord}_n(a_i)$ , and so that for any  $a$  the associated  $\alpha_i$  is  $\leq A_i$ .

Now, set  $b_i = a_i^{\text{ord}_n a_i / p_i^{A_i}}$ . By Theorem 2.3,

$$\text{ord}_n(b_i) = \frac{\text{ord}_n a_i}{\text{ord}_n a_i / p_i^{A_i}} = p_i^{A_i},$$

and so by repeated application of Theorem 2.4,

$$\text{ord}_n(b_1 \cdots b_l) = p_1^{A_1} \cdots p_l^{A_l}.$$

Given any  $a$  relatively prime to  $n$ , and writing  $\text{ord}_n(a) = p_1^{\alpha_1} \cdots p_l^{\alpha_l}$ , we know that  $\alpha_i \leq A_i$  (because  $A_i$  was defined to be the largest exponent of  $p_i$  in any of the orders  $\text{ord}_n(a)$ ). Therefore

$$\text{ord}_n(a) \mid \text{ord}_n(b_1 \cdots b_l)$$

for any  $a$  relatively prime to  $n$ . It follows that  $\text{ord}_n(b_1 \cdots b_l)$  is the largest of all the orders  $(\text{mod } n)$ , so  $A(n) = \text{ord}_n(b_1 \cdots b_l)$  and  $\text{ord}_n(a) \mid A(n)$  for any  $a$  relatively prime to  $n$ . □

So,  $A(n)$  is precisely the quantity we were so concerned with in the introduction: it's the number of the first column in the table of powers  $(\text{mod } n)$  which consists of all 1's.

**Definition 3.** An integer  $a$ , relatively prime to  $n$ , is called a primitive root  $(\text{mod } n)$  if the powers  $a^1, a^2, \dots, a^{\phi(n)}$  are all different  $(\text{mod } n)$ . Since adding a multiple of  $n$  to  $a$  doesn't change whether or not it's a primitive root  $(\text{mod } n)$ , we consider any two primitive roots  $(\text{mod } n)$  which differ by a multiple of  $n$  to be the same primitive root.

Since there are exactly  $\phi(n)$  different residue classes  $(\text{mod } n)$  which are relatively prime to  $n$ , and since if  $(a, n) = 1$  then the powers  $a^k$  are all also relatively prime to  $n$ , it follows that if  $a$  is a primitive root  $(\text{mod } n)$ , then the residue classes of  $a^1, a^2, \dots, a^{\phi(n)}$  must be *all* of the different residue classes  $(\text{mod } n)$  which are relatively prime to  $n$ . So, the row corresponding to  $a$  in the table of powers  $(\text{mod } n)$  is a row containing every possible residue class.

**Example 4.** 3 and 5 are the two primitive roots  $(\text{mod } 7)$ . There are no primitive roots  $(\text{mod } 8)$ .

**Theorem 3.2.** The integer  $a$  is a primitive root  $(\text{mod } n)$  if and only if  $\text{ord}_n(a) = \phi(n)$ .

*Proof.* If  $\text{ord}_n(a) < \phi(n)$ , then the residue class of 1 appears at least twice in the list of powers  $a^1, a^2, \dots, a^{\phi(n)}$ : in particular,  $a^{\text{ord}_n(a)} \equiv a^{\phi(n)} \equiv 1 \pmod{n}$ . So, these residue classes are not all different, and  $a$  cannot be a primitive root. On the other hand, if  $\text{ord}_n(a) = \phi(n)$ , could we have  $a^i \equiv a^j \pmod{n}$  with  $1 \leq i < j \leq \phi(n)$ ? No, because then we would find that  $a^{j-i} \equiv 1 \pmod{n}$ , contradicting the assumption that  $a^{\phi(n)}$  is the smallest power of  $a$  to be congruent to 1  $(\text{mod } n)$ . Thus,  $a$  is indeed a primitive root  $(\text{mod } n)$ . □

It immediately follows that:

**Theorem 3.3.** There exists a primitive root  $(\text{mod } n)$  if and only if  $A(n) = \phi(n)$ .

*Proof.* If  $A(n) = \phi(n)$ , then since  $A(n)$  is by definition the maximum of the orders (mod  $n$ ), there must exist  $a$  so that  $\text{ord}_n(a) = A(n) = \phi(n)$ . By the preceding result,  $a$  is a primitive root. Conversely, if  $a$  is a primitive root, then  $\text{ord}_n(a) = \phi(n)$ , so  $A(n) \leq \phi(n)$ . But  $A(n)$  is always at most  $\phi(n)$ , so indeed  $A(n) = \phi(n)$ .  $\square$

In the next section, we will study the existence (or, more accurately, non-existence) of primitive roots by studying  $A(n)$  and determining when  $A(n)$  could equal  $\phi(n)$ .

**Example 5.** Primitive roots (mod 9). Here is the table of powers (mod 9).

$a^k$	1	2	3	4	5	6
1	1	1	1	1	1	1
2	2	4	8	7	5	1
4	4	7	1	4	7	1
5	5	7	8	4	2	1
7	7	4	1	7	4	1
8	8	1	6	1	6	1

It is evident that 2 and 5 are the only primitive roots (mod 9). Now, suppose we were given the fact that 2 is a primitive root (mod 9), so that the powers  $2^1, 2^2, \dots, 2^6$  represent the distinct residue classes (mod 9) which are relatively prime to 9. Which of these could possibly also be primitive roots (mod 9)? Well,  $(2^2)^3 = 2^6 \equiv 1 \pmod{9}$ , so  $\text{ord}_9(2^2) \leq 3$ . Similarly,  $\text{ord}_9(2^4) \leq 3$  and  $\text{ord}_9(2^3) \leq 3$ , so the only possibility for another primitive root would be  $2^5 \equiv 5 \pmod{9}$ .

The above example suggests the following argument: suppose  $a$  and  $b$  are primitive roots (mod  $n$ ). Then  $b \equiv a^k \pmod{n}$  for some  $k$ , by the definition of a primitive root and the fact that  $b$  must be relatively prime to  $n$ . What, then, is  $\text{ord}_n(b)$ ? Well, by Theorem 2.3,

$$\text{ord}_n(b) = \text{ord}_n(a^k) = \text{ord}_n(a) / (k, \text{ord}_n(a)).$$

But since we've assumed that  $b$  and  $a$  are both primitive roots, we need  $\text{ord}_n(b) = \text{ord}_n(a) = \phi(n)$ , and  $(k, \text{ord}_n(a)) = (k, \phi(n)) = 1$ . Thus,  $k$  must be relatively prime to  $\phi(n)$ . On the other hand, if we start with a primitive root  $a$  and an integer  $k$  that's relatively prime to  $n$ , then reversing the preceding argument shows that  $\text{ord}_n(a^k) = \phi(n)$ , and so  $a^k$  is a primitive root as well. Therefore, we get a primitive root (mod  $n$ ) exactly for each integer between 1 and  $\phi(n)$  which is relatively prime to  $\phi(n)$ , and we have proved:

**Theorem 3.4.** If there are any primitive roots (mod  $n$ ), then there are exactly  $\phi(\phi(n))$  of them. Given one primitive root,  $a$ , the others can be obtained by taking powers  $a^k$  with  $(k, \phi(n)) = 1$ .

Notice that this argument *assumed* the existence of at least one primitive root (mod  $n$ ), and proceeded to count exactly the number of different primitive roots (mod  $n$ ). However, this argument does *not* say anything about whether or not any primitive roots exist (mod  $n$ ). For example, we now know that if there are any primitive roots (mod 27), then there are exactly  $\phi(\phi(27)) = \phi(18) = 6$  of them, but we don't know whether or not any exist. For curiosity's sake, let's see whether any do exist.

**Example 6.** Primitive roots (mod 27). Of all the residue classes (mod 27), can we think of a good guess as to which 6 could be primitive roots? Well, there are 2 primitive roots (mod 9), so there are 6 residue classes (mod 27) which reduce to a primitive root (mod 9), so it is sensible to guess that these classes – the classes of 2, 5, 11, 14, 20, and 23 – are our primitive roots.

There's a simple way of checking that these are indeed primitive roots, without calculating all  $18 = \phi(27)$  powers of them and checking that the 18<sup>th</sup> power is the first one to be congruent to 1. The method is based on the obvious fact that if  $x$  divides  $y$  and  $x < y$ , then there is some prime  $p$  dividing  $y$  so that  $x$  divides  $y/p$  as well. To apply this, we note that if  $\text{ord}_n(a) < \phi(n)$ , then there is some prime  $p$  such that  $\text{ord}_n(a)$  divides  $\phi(n)/p$ , and therefore  $a^{\phi(n)/p} \equiv 1 \pmod{n}$ . So, to check that  $a$  is a primitive root (mod  $n$ ), it suffices to check that no  $a^{\phi(n)/p}$  is congruent to 1 (mod  $n$ ).

In our case,  $\phi(27) = 18$ , which is divisible by the primes 2 and 3, so it would suffice to check that  $a^6$  and  $a^9$  are not congruent to 1 (mod 27). This is easily done: one checks that  $2^3, 5^3, 11^3, 14^3, 20^3$ , and  $23^3$  are all congruent either to 8 or 17 (mod 27), that  $8^2 = 64 \equiv 10 \pmod{27}$  and  $17^2 \equiv -10 \pmod{27}$ , and that  $8^3 \equiv 17^3 \equiv -1 \pmod{27}$ .

4. WHEN DO PRIMITIVE ROOTS (MOD  $N$ ) EXIST?

We begin with:

**Theorem 4.1.** If  $p$  is a prime, then there do exist primitive roots (mod  $p$ ).

*Proof.* If  $a$  is relatively prime to  $p$ , then, since  $\text{ord}_p(a)$  divides  $A(p)$ , it follows that  $a^{A(p)} \equiv 1 \pmod{p}$ . Thus, the polynomial  $x^{A(p)} - 1$  has  $p - 1$  roots (mod  $p$ ). However, we know that a polynomial of degree  $d$  has at most  $d$  roots (mod  $p$ ), because  $p$  is prime. Since the degree of  $x^{A(p)} - 1$  is  $A(p)$ , we conclude that  $A(p) \geq p - 1$ . But we already knew that  $A(p) \leq \phi(p) = p - 1$ , so we must have  $A(p) = \phi(p) = p - 1$ . By Theorem 3.3, there exist primitive roots (mod  $p$ ).  $\square$

It is natural, next, to look at whether or not there are primitive roots modulo the product of two primes.

**Example 7.** Primitive roots (mod 15). By the Chinese Remainder Theorem,  $a^k \equiv 1 \pmod{15}$  if and only if both  $a^k \equiv 1 \pmod{3}$  and  $a^k \equiv 1 \pmod{5}$ . Since  $a^k \equiv 1 \pmod{3}$  if and only if  $\text{ord}_3(a)$  divides  $k$ , and  $a^k \equiv 1 \pmod{5}$  if and only if  $\text{ord}_5(a)$  divides  $k$ , it follows that  $a^k \equiv 1 \pmod{15}$  if and only if  $\text{LCM}(\text{ord}_3(a), \text{ord}_5(a))$  divides  $k$ . Thus  $\text{ord}_{15}(a) = \text{LCM}(\text{ord}_3(a), \text{ord}_5(a))$ . However,  $\text{ord}_3(a)$  always divides  $\phi(3) = 2$ , and  $\text{ord}_5(a)$  always divides  $\phi(5) = 4$ , so in any case  $\text{ord}_{15}(a) = \text{LCM}(\text{ord}_3(a), \text{ord}_5(a))$  must divide 4. In particular,  $\text{ord}_{15}(a)$  cannot equal  $\phi(15) = 15(1 - \frac{1}{3})(1 - \frac{1}{5}) = 8$ , and therefore there are no primitive roots (mod 15).

In general, we have the following result, which is proved in exactly the same manner as the above example:

**Theorem 4.2.** If  $m$  and  $n$  are relatively prime integers, then  $A(mn) = \text{LCM}(A(m), A(n))$ .

*Proof.* If  $a$  is relatively prime to  $mn$ , then by the Chinese Remainder Theorem,  $a^k \equiv 1 \pmod{mn}$  if and only if both  $a^k \equiv 1 \pmod{m}$  and  $a^k \equiv 1 \pmod{n}$ , when in turn are true if and only if both  $\text{ord}_m(a) \mid k$  and  $\text{ord}_n(a) \mid k$ . Therefore,  $a^k \equiv 1 \pmod{mn}$  if and only if  $\text{LCM}(\text{ord}_m(a), \text{ord}_n(a)) \mid k$ , and so

$$\text{ord}_{mn}(a) = \text{LCM}(\text{ord}_m(a), \text{ord}_n(a)).$$

By Theorem 3.1,  $\text{ord}_m(a)$  divides  $A(m)$  and  $\text{ord}_n(a)$  divides  $A(n)$ , so certainly  $\text{LCM}(A(m), A(n))$  is a common multiple of  $\text{ord}_m(a)$  and  $\text{ord}_n(a)$ . Therefore, because  $\text{ord}_{mn}(a)$  is the *least* common multiple of  $\text{ord}_m(a)$  and  $\text{ord}_n(a)$ , we can conclude that  $\text{ord}_{mn}(a) \mid \text{LCM}(A(m), A(n))$  for any  $a$  relatively prime to  $mn$ . We conclude that  $A(mn)$  is a divisor of  $\text{LCM}(A(m), A(n))$ , and is thus at most  $\text{LCM}(A(m), A(n))$ .

It remains to show that  $A(mn)$  is actually equal to  $\text{LCM}(A(m), A(n))$ , not just a divisor. But we can certainly choose integers  $y$  and  $z$  such that  $\text{ord}_m(y) = A(m)$  and  $\text{ord}_n(z) = A(n)$  ( $y$  and  $z$  are simply any integers with the largest possible orders mod  $m$  and  $n$  respectively), and by the Chinese Remainder Theorem there exists  $x$  such that  $x \equiv y \pmod{m}$  and  $x \equiv z \pmod{n}$ . From the arguments in the first paragraph, it follows that

$$\text{ord}_{mn}(x) = \text{LCM}(\text{ord}_m(x), \text{ord}_n(x)) = \text{LCM}(\text{ord}_m(y), \text{ord}_n(z)) = \text{LCM}(A(m), A(n)),$$

and since  $A(mn)$  is the largest possible order (mod  $mn$ ) we therefore know that  $A(mn)$  is also at least  $\text{LCM}(A(m), A(n))$ .

Therefore,  $A(mn) = \text{LCM}(A(m), A(n))$ .  $\square$

**Example 8.**  $A(15) = \text{LCM}(A(3), A(5)) = \text{LCM}(2, 4) = 4$ . Similarly,  $A(40) = \text{LCM}(A(8), A(5)) = \text{LCM}(4, 4) = 4$ . So the largest order (mod 40) is 4.

If  $m$  and  $n$  are relatively prime but  $A(m)$  and  $A(n)$  are not relatively prime, then

$$\text{LCM}(A(m), A(n)) = \frac{A(m)A(n)}{(A(m), A(n))} < A(m) \cdot A(n) \leq \phi(m) \cdot \phi(n) = \phi(mn),$$

so  $A(mn) < \phi(mn)$  and therefore there do not exist any primitive roots (mod  $mn$ ). This allows us to prove the following:

**Theorem 4.3.** If  $n = pq$  is the product of two distinct odd primes, or if  $n = 4p$  is the product of 4 and an odd prime, then there are no primitive roots (mod  $n$ ).

*Proof.* In the case  $n = pq$  with  $p$  and  $q$  distinct odd primes,  $A(p) = p - 1$  and  $A(q) = q - 1$ , so 2 divides the GCD of  $A(p)$  and  $A(q)$ . Thus  $A(p)$  and  $A(q)$  aren't relatively prime, and so by the argument in the above paragraph there can't be any primitive roots (mod  $n$ ).

Similarly, in the case  $n = 4p$ ,  $A(4) = 2$  and  $A(p) = p - 1$  is divisible by 2, and again  $A(4)$  and  $A(p)$  aren't relatively prime.  $\square$

Finally, we conclude this section with a result which will give us most of the remaining cases:

**Theorem 4.4.** If  $a$  is a primitive root (mod  $n$ ) and if  $m$  divides  $n$ , then  $a$  is also a primitive root (mod  $m$ ). In particular, if there are no primitive roots (mod  $m$ ), then there can exist no primitive roots (mod  $n$ ).

*Proof.* The second statement of the theorem follows immediately from the first statement: if there were a primitive root (mod  $n$ ), we'd obtain one (mod  $m$ ), so the non-existence of primitive roots (mod  $m$ ) gives the non-existence of primitive roots (mod  $n$ ).

To prove the first statement, we want to show that every integer relatively prime to  $m$  is congruent (mod  $m$ ) to some power of  $a$ . (This, you'll recall, was the definition of a primitive root.) The trouble is that given an integer  $x$  relatively prime to  $m$ , it may *not* be the case that  $x$  is relatively prime to  $n$ , so we cannot prove the theorem by asserting that  $x$  is congruent (mod  $n$ ) to a power of  $a$ : that would only be true if  $x$  were relatively prime to  $n$ . Instead, what we will prove is that there exists  $c$  so that  $x + cm$  is relatively prime to  $n$ . Then, since  $a$  is a primitive root (mod  $n$ ), we know that there exists some  $k$  so that  $a^k \equiv x + cm \pmod{n}$ , in which case  $a^k \equiv x \pmod{m}$ . Thus, we will have established that  $x$  is indeed congruent to a power of  $a$  (mod  $m$ ).

So, let us proceed to show that there exists an integer  $c$  so that  $x + cm$  is relatively prime to  $n$ . Let  $p_1, \dots, p_l$  be the primes which divide  $n$  but do *not* divide  $m$ . Then  $m$  is invertible (mod  $p_i$ ) for each  $i$ , so let  $m_i$  be a multiplicative inverse of  $m$  (mod  $p_i$ ) for each  $i$ . Finally, using the Chinese Remainder Theorem, let  $c$  be a solution to the following system of congruences:

$$\begin{aligned} c &\equiv m_1(1 - x) \pmod{p_1} \\ c &\equiv m_2(1 - x) \pmod{p_2} \\ &\vdots \\ c &\equiv m_l(1 - x) \pmod{p_l} \end{aligned}$$

Then for each  $i$ ,

$$x + mc \equiv x + m \cdot m_i \cdot (1 - x) \equiv x + (1 - x) \equiv 1 \pmod{p_i},$$

and so  $x + mc$  is not divisible by  $p_i$  for any  $i$ . Thus, for this choice of  $c$ ,  $x + mc$  is not divisible by any of the primes which divide  $n$  but do not divide  $m$ . On the other hand, can  $x + mc$  be divisible by any of the primes which divide both  $n$  and  $m$ ? No, because if  $p$  divides  $x + mc$  and  $m$ , then  $p$  also divides  $x$ , contradicting the assumption that  $x$  and  $m$  are relatively prime. So, we've actually shown that this choice of  $x + mc$  is divisible by none of the primes which divide  $n$ , and therefore  $x + mc$  and  $n$  are relatively prime. This completes the proof.  $\square$

Recall that we already know that primitive roots (mod  $n$ ) don't exist in the following cases:

- (1) When  $n = pq$  is the product of two odd primes;
- (2) When  $n = 4p$  is the product of 4 and an odd prime;
- (3) When  $n = 8$ . (This was Example 4.)

By the theorem we have just proved, if  $n$  is *divisible* by the product of two odd primes, or by the product of 4 and an odd prime, or by 8, then there are no primitive roots (mod  $n$ ). This gives severe restrictions on  $n$ : if there exist primitive roots (mod  $n$ ), then  $n$  can be divisible by at most one odd prime, so its unique factorization must be of the form  $2^\alpha \cdot p^\beta$  for some odd prime  $p$ . If  $\beta > 0$ , then 4 cannot divide  $n$  either, so  $\alpha = 0$  or 1. And in any case 8 cannot divide  $n$ , so  $\alpha < 3$ . Thus, the only possibilities which remain are  $n = p^\beta$ ,  $n = 2 \cdot p^\beta$ , or  $n = 1, 2$ , or 4. We have therefore just shown:

**Theorem 4.5.** If there exist primitive roots (mod  $n$ ), then  $n$  is either 1, 2, 4, a power of an odd prime, or 2 times a power of an odd prime.

In the next section, we will prove that in all of these cases, primitive roots really do exist.

### 5. EXISTENCE OF PRIMITIVE ROOTS

We already know (by direct calculation) that there exist primitive roots modulo 1, 2, and 4. Suppose for a moment that there exist primitive roots (mod  $p^\beta$ ) with  $p$  an odd prime, so that  $A(p^\beta) = \phi(p^\beta) = p^{\beta-1}(p-1)$ . Then

$$A(2p^\beta) = \text{LCM}(A(2), A(p^\beta)) = \text{LCM}(1, \phi(p^\beta)) = \phi(p^\beta).$$

But  $\phi(2p^\beta) = \phi(2) \cdot \phi(p^\beta) = \phi(p^\beta)$ , so in fact  $A(2p^\beta) = \phi(2p^\beta)$ , and by Theorem 3.3 there must exist primitive roots (mod  $2p^\beta$ ).

All that remains, therefore, is to prove that there exist primitive roots modulo the powers of odd primes. Yet we know exactly where to look to find these primitive roots, for we know (Theorem 4.1) that there must exist primitive roots (mod  $p$ ) for each  $p$ , and Theorem 4.4 tells us that primitive roots modulo higher powers of  $p$  have to reduce (mod  $p$ ) to one of the primitive roots (mod  $p$ ).

To begin with, let us demonstrate the existence of primitive roots (mod  $p^2$ ). Given a primitive root  $a$  (mod  $p$ ), there are exactly  $p$  different residue classes (mod  $p^2$ ) which reduce (mod  $p$ ) to  $a$ ; we may select  $a, a+p, \dots, a+(p-1)p$  as representatives for these classes. We would like to know which of these  $p$  numbers, if any, are primitive roots (mod  $p^2$ ). What are the possibilities for the order of  $a+lp$  (mod  $p^2$ )? Well, if  $(a+lp)^k \equiv 1 \pmod{p^2}$ , then surely  $(a+lp)^k \equiv a^k \equiv 1 \pmod{p}$ . Since  $a$  is a primitive root (mod  $p$ ), this shows that  $p-1$  divides  $k$ . Thus,  $\text{ord}_{p^2}(a+lp)$  is divisible by  $p-1$ ; but this order also must divide  $\phi(p^2) = (p-1)p$ , so there are only two possibilities for  $\text{ord}_{p^2}(a+lp)$ :  $p-1$  or  $p(p-1)$ . Consequently, if we could show that  $(a+lp)^{p-1} \not\equiv 1 \pmod{p^2}$ , then we could conclude that  $\text{ord}_{p^2}(a+lp) = \phi(p^2)$  and that  $a+lp$  is a primitive root (mod  $p$ ).

Now, by the Binomial Theorem,

$$(a+lp)^{p-1} = a^{p-1} + \binom{p-1}{1} a^{p-2} pl + (\text{terms divisible by } p^2) \equiv a^{p-1} + p(p-1)la^{p-2} \pmod{p^2}.$$

Since  $(p-1)a^{p-2}$  is invertible (mod  $p$ ), we know that as  $l$  runs from 0 to  $p-1$ , the product  $l(p-1)a^{p-2}$  runs over a complete residue system (mod  $p$ ). So,  $p(p-1)la^{p-2}$  runs through every possible multiple of  $p$  (mod  $p^2$ ). Since  $a^{p-1} \equiv 1 + \text{some multiple of } p \pmod{p^2}$ , we conclude that  $(a+lp)^{p-1} \equiv 1 \pmod{p^2}$  for *exactly one* choice of  $l$ , and for the other  $p-1$  choices for  $l$ , we get that  $a+lp$  is a primitive root (mod  $p$ ).

We can check this argument against our previous work, for this argument gives us a new way of computing the number of primitive roots (mod  $p^2$ ): each primitive root (mod  $p$ ) lifts to  $p-1$  different primitive roots (mod  $p^2$ ), because we get one primitive root for each workable choice of  $l$ . So, the number of primitive roots (mod  $p^2$ ) should be  $p-1$  times the number of primitive roots (mod  $p$ ). This confirms our earlier calculation (Theorems 3.4) that the number of primitive roots (mod  $p$ ), if any, is  $\phi(\phi(p)) = \phi(p-1)$  and that the number of primitive roots (mod  $p^2$ ), if any, is  $\phi(\phi(p^2)) = \phi(p(p-1)) = \phi(p)\phi(p-1) = (p-1)\phi(p-1)$ .

Can we make this argument useful for higher powers of  $p$ ? Most certainly! Any primitive root (mod  $p^\beta$ ) must reduce to a primitive root (mod  $p^{\beta-1}$ ). Thus, given a primitive root  $a$  (mod  $p^{\beta-1}$ ), we get  $p$  potential primitive roots (mod  $p^\beta$ ):  $a, a+p^{\beta-1}, \dots, a+(p-1)p^{\beta-1}$ .

However the number of primitive roots (mod  $p^\beta$ ) should be

$$\phi(\phi(p^\beta)) = \phi(p^{\beta-1}(p-1)) = \phi(p-1)(p-1)p^{\beta-2},$$

while by a similar calculation the number of primitive roots (mod  $p^{\beta-1}$ ) should be  $\phi(p-1)(p-1)p^{\beta-3}$ . So the number of primitive roots (mod  $p^\beta$ ) should be exactly  $p$  times the number of primitive roots (mod  $p^{\beta-1}$ ). Consequently, we expect that *all* of  $a, a+p^{\beta-1}, \dots, a+(p-1)p^{\beta-1}$  will turn out to be primitive roots.

Turning to the proof that there exist primitive roots (mod  $p^\beta$ ) for  $\beta \geq 3$ , first select a primitive root  $a$  (mod  $p^{\beta-1}$ ). We wish to show that  $a$  is also a primitive root (mod  $p^\beta$ ). To do this, observe first that if  $a^k \equiv 1 \pmod{p^\beta}$ , then  $a^k \equiv 1 \pmod{p^{\beta-1}}$ , and since  $a$  is a primitive root (mod  $p^{\beta-1}$ ) we know that  $\phi(p^{\beta-1}) = (p-1)p^{\beta-2}$  must divide  $k$ .

Therefore,  $(p-1)p^{\beta-2}$  divides  $\text{ord}_{p^\beta}(a)$ . Since  $\text{ord}_{p^\beta}(a)$  divides  $\phi(p^\beta) = (p-1)p^{\beta-1}$ , there are, consequently, only two possibilities for  $\text{ord}_{p^\beta}(a)$ :  $(p-1)p^{\beta-1}$ , in which case  $a$  is a primitive root  $(\text{mod } p^\beta)$ , or  $(p-1)p^{\beta-2}$ , in which case it is not. So, to eliminate the second case and prove that  $a$  is indeed a primitive root, we need to show that  $a^{(p-1)p^{\beta-2}} \not\equiv 1 \pmod{p^\beta}$ .

Using the fact that  $a$  is a primitive root  $(\text{mod } p^{\beta-1})$  and the fact that  $\beta \geq 3$ , it follows from Theorem 4.4 that  $a$  is a primitive root  $(\text{mod } p^2)$ . Recalling our previous description of primitive roots  $(\text{mod } p^2)$ , we know that  $a^{p-1} \equiv 1 \pmod{p}$  but  $a^{p-1} \not\equiv 1 \pmod{p^2}$ , or, in other words,  $a^{p-1} = 1 + lp$  for some integer  $l$  not divisible by  $p$ . By the binomial theorem,

$$a^{(p-1)p^{\beta-2}} = (1 + lp)^{p^{\beta-2}} = 1 + \binom{p^{\beta-2}}{1}(lp) + \binom{p^{\beta-2}}{2}(lp)^2 + \dots$$

We want to show that  $(\text{mod } p^\beta)$ , every term in this binomial expansion except the first two is equal to zero. Since  $p > 2$ , it is evident that  $p^\beta$  divides

$$\binom{p^{\beta-2}}{2}(lp)^2 = \frac{1}{2}p^{\beta-2}(p^{\beta-2} - 1)p^2l^2.$$

Similarly, the general term of this binomial expansion is

$$\binom{p^{\beta-2}}{k}(lp)^k = \frac{1}{k!}p^{\beta-2}(p^{\beta-2} - 1) \dots (p^{\beta-2} - (k-1))p^k l^k.$$

The power of  $p$  dividing  $k!$  is equal to

$$\lfloor \frac{k}{p} \rfloor + \lfloor \frac{k}{p^2} \rfloor + \dots < \frac{k}{p} + \frac{k}{p^2} + \dots = \frac{k}{p-1},$$

(where  $\lfloor x \rfloor$  denotes the greatest integer less than or equal to  $x$ ). For  $p \geq 5$  and  $k \geq 3$ , and for  $p = 3$  and  $k \geq 4$ , it is easily verified that  $k - \frac{k}{p-1} \geq 2$ , and so the power of  $p$  dividing

$$\frac{1}{k!}p^{\beta-2}(p^{\beta-2} - 1) \dots (p^{\beta-2} - (k-1))p^k l^k$$

is at least

$$(\beta - 2) + k - \frac{k}{p-1} \geq \beta - 2 + 2 = \beta.$$

This last statement can be verified directly in the missing case  $p = 3, k = 3$ . Thus, this general term of the binomial expansion is indeed divisible by  $p^\beta$ , and so is congruent to 0  $(\text{mod } p^\beta)$ . Whew!

Where has this gotten us? Well, we started with

$$a^{(p-1)p^{\beta-2}} = (1 + lp)^{p^{\beta-2}} = 1 + \binom{p^{\beta-2}}{1}(lp) + \binom{p^{\beta-2}}{2}(lp)^2 + \dots$$

and now we know that  $(\text{mod } p^\beta)$  all the terms except the first two vanish, so

$$a^{(p-1)p^{\beta-2}} \equiv 1 + \binom{p^{\beta-2}}{1}(lp) \equiv 1 + lp^{\beta-1} \pmod{p^\beta}.$$

Since  $l$  is not divisible by  $p$ , this tells us definitively that

$$a^{(p-1)p^{\beta-2}} \not\equiv 1 \pmod{p^\beta}.$$

Therefore,  $a$  must have order  $(p-1)p^{\beta-1}$  and must be a primitive root  $(\text{mod } p^\beta)$ .

Notice, interestingly, that it follows from this proof that if  $a$  is a primitive root  $(\text{mod } p^2)$ , then  $a$  is also a primitive root  $(\text{mod } p^k)$  for any positive integer  $k$ . To summarize, we have proved:

**Theorem 5.1.** If  $p$  is an odd prime, then there exist primitive roots modulo  $p^\beta$  and  $2 \cdot p^\beta$  for any positive integer  $\beta$ . These numbers, together with 1, 2, and 4, are the only numbers modulo which there exist primitive roots. Furthermore, any primitive root  $a \pmod{p}$  lifts to  $p-1$  different primitive roots  $(\text{mod } p^2)$ , and any primitive root  $a \pmod{p^2}$  is also a primitive root  $(\text{mod } p^k)$  for any integer  $k$ .