SECTION 6.5 ➡ **Composite Integers with Primitive Roots**

By the end of this section you will be able to

- understand that not every positive integer has a primitive root
- determine which composite integers have primitive roots

In the last section we showed that *every* prime has a primitive root – Primitive Root Theorem (6.22).

In this section we will describe the composite integers which also have primitive roots.

For example:

The set of integers $\{2,\ 5\}$ are primitive roots modulo 9.

The set of integers $\{2,\ 5,\ 11,\ 14,\ 20,\ 23\}$ are primitive roots modulo 27.

The set of integers $\{3,\ 5,\ 7,\ 11,\ 23,\ 27,\ 29,\ 31\}$ are primitive roots modulo 34.

However there are *no* primitive roots moduli 8, 12, 15, 16, 20, 21, 24, 28, 30, 32, 33.

The aim of this section is to determine which *composite integers* have a primitive root.

6.5.1 Primitive Roots Modulo p^2

We examine the primitive roots modulo p^2 where p is an odd prime.

Example 6.27

Show that 2 is a primitive root of (a) 5 (b) $5^2 = 25$

Solution

(a) Since 5 is prime so $\phi(5) = 5 - 1 = 4$. Evaluating powers of 2 gives

$$2^1 \equiv 2,\ \ 2^2 \equiv 4,\ \ 2^3 \equiv 3,\ \ 2^4 \equiv 1 \pmod{5}$$

Hence 2 is a primitive root modulo 5.

(b) We have $\phi(25) = 5(5-1) = 20$. We only need to examine the indices of 2 which are positive divisors of $\phi(25) = 20$. *Why?*

Because by Corollary (6.5):

Let the integer a modulo n have order k. Then $k \mid \phi(n)$.

The positive divisors of 20 are 1, 2, 4, 5, 10 and 20. By using a calculator we find:

$$2^1 \equiv 2,\ \ 2^2 \equiv 4,\ 2^4 \equiv 16,\ \ 2^5 \equiv 7,\ \ 2^{10} \equiv 24,\ \ 2^{20} \equiv 1 \left(\text{mod } 25\right)$$

Hence 2 is a primitive root modulo 25 because the first index of 2 to give 1 modulo 25 is $\phi\left(25\right) = 20$.

We have the following results for primitive roots moduli 3^2, 5^2 and 7^2:

The integers $\left\{2,\ 5\right\}$ are primitive roots modulo $3^2 = 9$.

The integers $\left\{2,\ 3,\ 8,\ 12,\ 13,\ 17,\ 22,\ 23\right\}$ are primitive roots modulo $5^2 = 25$.

The integers $\left\{3,\ 5,\ 10,\ 12,\ 17,\ 24,\ 26,\ 33,\ 38,\ 40,\ 45,\ 47\right\}$ are primitive roots modulo $7^2 = 49$.

In this subsection we will show that modulo p^2 has primitive roots but to prove this we need a couple of results.

Lemma (6.23).

Let p be an odd prime. Then there is a primitive root r modulo prime p such that

$$r^{p-1} \not\equiv 1 \left(\text{mod } p^2\right)$$

In the previous example we had 2 is a primitive root of prime 5 and

$$2^{5-1} \equiv 2^4 \equiv 16 \not\equiv 1 \left(\text{mod } 5^2\right)$$

We can also show that 3 is a primitive root modulo 7 and

$$3^{7-1} \equiv 3^6 \equiv 43 \not\equiv 1 \left(\text{mod } 7^2\right)$$

The given statement claims that this is *not* just the case for these two examples but is generally true. We need to prove there is a primitive root r modulo prime p such that $r^{p-1} \not\equiv 1 \left(\text{mod } p^2\right)$.

Proof.

By the Primitive Root Theorem we know the prime p has a primitive root, r say. If $r^{p-1} \not\equiv 1 \left(\text{mod } p^2\right)$ then we are done. Suppose

$$r^{p-1} \equiv 1 \left(\text{mod } p^2\right) \qquad (*)$$

As r is a primitive root modulo p therefore $r + p$ is also a primitive root modulo p because $r + p \equiv r \left(\text{mod } p\right)$. We need to show that

$$\left(r + p\right)^{p-1} \not\equiv 1 \left(\text{mod } p^2\right)$$

We examine this primitive root $r + p$ modulo p.

Expanding $\left(r+p\right)^{p-1}$ by applying the binomial expansion (see Introductory Chapter) we have

$$\begin{aligned}\left(r+p\right)^{p-1} &\equiv r^{p-1}+\left(p-1\right)r^{p-2}p+\underbrace{0+\cdots+0}_{\text{All these are multiples of } p^2}\left(\operatorname{mod} p^2\right)\\ &\equiv r^{p-1}+\underbrace{p^2r^{p-2}}_{\equiv 0\left(\operatorname{mod} p^2\right)}-pr^{p-2}\left(\operatorname{mod} p^2\right)\\ &\equiv r^{p-1}-pr^{p-2}\equiv\underbrace{1}_{\text{by } (*)}-pr^{p-2}\left(\operatorname{mod} p^2\right)\end{aligned}$$

We have

$$\left(r+p\right)^{p-1}\equiv 1-pr^{p-2}\left(\operatorname{mod} p^2\right) \qquad (\ddagger)$$

Since r is a primitive root modulo p so $\gcd\left(r,\ p\right)=1$ which implies that

$$pr^{p-2}\not\equiv 0\left(\operatorname{mod} p^2\right)$$

Why?

Because if $pr^{p-2}\equiv 0\left(\operatorname{mod} p^2\right)$ then $r^{p-2}\equiv 0\left(\operatorname{mod} p\right)$. This *cannot* be the case because r is a primitive root modulo p. Therefore $pr^{p-2}\not\equiv 0\left(\operatorname{mod} p^2\right)$.

Substituting this $pr^{p-2}\not\equiv 0\left(\operatorname{mod} p^2\right)$ into the congruence (‡) gives

$$\left(r+p\right)^{p-1}\equiv 1-pr^{p-2}\not\equiv 1\left(\operatorname{mod} p^2\right)$$

Hence there is a primitive root $r+p$ of p such that $\left(r+p\right)^{p-1}\not\equiv 1\left(\operatorname{mod} p^2\right)$.

■

Lemma (6.24).

Let r be a primitive root modulo p. Then the order of r modulo p^2 is either $p-1$ or $\phi\left(p^2\right)=p\left(p-1\right)$.

Note that in the case of order is $\phi\left(p^2\right)=p\left(p-1\right)$, r is a primitive root modulo p^2.

Proof. See question 16 of Exercises 6.5.

Example 6.28

Determine a primitive root of 7. Determine the order of this primitive root modulo 49.

Solution

What is a primitive root of 7?

We first test powers of 2 modulo 7. Since $\phi\left(7\right)=6$ so we only need to find the powers of

2 which are *proper divisors* of 6 (these are 2 and 3):

$$2^2 \equiv 4\,,\ \ 2^3 \equiv 8 \equiv 1 \left(\text{mod } 7\right)$$

Since $2^3 \equiv 1 \left(\text{mod } 7\right)$ so 2 *cannot* be a primitive root modulo 7.

Evaluating powers of 3 modulo 7 gives

$$3^2 \equiv 9 \equiv 2 \left(\text{mod } 7\right) \quad \text{and} \quad 3^3 \equiv 2\times 3 \equiv 6 \left(\text{mod } 7\right)$$

Hence 3 is a primitive root modulo 7.

By the previous lemma the order of 3 modulo $7^2 = 49$ is $7-1=6$ or $7\left(7-1\right)=42$.

We first evaluate base 3 to index 6 modulo 49:

$$3^6 \equiv 43 \not\equiv 1 \left(\text{mod } 49\right)$$

Hence the order of 3 modulo 49 must be $7\left(7-1\right)=42$. (We don't need to check because the lemma says the order must be 6 or 42 and it is *not* 6.)

Since $\phi\left(49\right)=42$ so 3 is a primitive root modulo 49.

This example suggests that we can use the previous lemma to test whether a primitive root modulo p is also a primitive root modulo p^2.

This last lemma leads to the following result:

Theorem (6.25).

Let p be an odd prime. Then there is a primitive root modulo p^2.

We have already shown in the last section that a prime p has primitive roots. *What does this theorem claim?*

It claims that p^2 also has a primitive root provided p is an odd prime. For example $\left\{3,\ 5,\ 10,\ 12,\ 17,\ 24,\ 26,\ 33,\ 38,\ 40,\ 45,\ 47\right\}$ are primitive roots modulo $7^2 = 49$.

How do we prove this?

By using the previous lemma and showing that the order is $\phi\left(p^2\right)$.

Proof.

For primitive root of p^2 we must have the order equal to

$$\phi\left(p^2\right) = p\left(p-1\right)$$

Let p be an odd prime then by Lemma (6.23) there is a primitive root r of prime p such that

$$r^{p-1} \not\equiv 1 \left(\text{mod } p^2\right) \qquad (*)$$

From the previous lemma we have the order of r modulo p^2 is either $p-1$ or $p\left(p-1\right)$.

Case I The order of r is $p-1$.

Consider the primitive root $r+p$ modulo p. By the proof of the Lemma (6.24) we have

$$\left(r+p\right)^{p-1} \not\equiv 1 \left(\bmod\ p^2\right)$$

This $\left(r+p\right)^{p-1} \not\equiv 1 \left(\bmod\ p^2\right)$ implies that $r+p$ *cannot* have order $p-1$. By Lemma (6.24):

The order of r modulo p^2 is either $p-1$ or $\phi\left(p^2\right)=p\left(p-1\right)$.

Since $r+p$ is also a primitive root of p so the order of $r+p$ must be $\phi\left(p^2\right)=p\left(p-1\right)$. Hence in this case $r+p$ is a primitive root modulo p^2.

Case II Order of r is $p\left(p-1\right)$.

Clearly this r is a primitive root modulo p^2 because $\phi\left(p^2\right)=p\left(p-1\right)$.

■

Note that the primitive root modulo p^2 is the same primitive root r as p or it is $r+p$ (or both).

In most cases the primitive root modulo p will also be a primitive root modulo p^2. However, in a few cases the primitive root modulo p is *not* a primitive root modulo p^2. If this occurs, then $r+p$ is a primitive root modulo p^2.

For example, *all* the primitive roots of the odd primes 13, 17 and 19 are also primitive roots modulo 13^2, 17^2 and 19^2 respectively.

It is pretty hard to find a primitive root of prime p which is *not* a primitive root of p^2. However here is one example which you are asked to show in Exercises 6.5 question 12: 14 is a primitive root modulo 29 but 14 is *not* a primitive root modulo 29^2.

6.5.2 Primitive Roots of p^2

To show that modulo p^k has primitive roots we first prove the following:

Proposition (6.26).

Let p be an odd prime and r be a primitive root modulo p^2. Then we have

$$r^{p^{k-2}\left(p-1\right)} \not\equiv 1 \left(\bmod\ p^k\right) \text{ for every integer } k \geq 2.$$

How do we prove this proposition?

By mathematical induction.

Proof.

The given result is true for the base case $k=2$ because by Lemma (6.23) we have

$$r^{p-1} \not\equiv 1 \left(\text{mod } p^2\right)$$

Assume the given result is true for $k=m$, that is

$$r^{p^{m-2}(p-1)} \not\equiv 1 \left(\text{mod } p^m\right) \qquad (\ddagger)$$

We use this to prove the result for $k=m+1$, that is we need to show

$$r^{p^{m-1}(p-1)} \not\equiv 1 \left(\text{mod } p^{m+1}\right)$$

Note that $\phi\left(p^{m-1}\right) = p^{m-2}\left(p-1\right)$. Since r is a primitive root so $\gcd\left(r,\ \ p^{m-1}\right)=1$ and we can now apply Euler's theorem:

$$r^{p^{m-2}(p-1)} \equiv 1 \left(\text{mod } p^{m-1}\right)$$

By the definition of congruence there is an integer a such that

$$r^{p^{m-2}(p-1)} = 1 + ap^{m-1}$$

By assumption $(\ddagger)$ we know that $p \nmid a$ otherwise we would have $r^{p^{m-2}(p-1)} \equiv 1 \left(\text{mod } p^m\right)$.

Raising both sides to the power p gives

$$\left(r^{p^{m-2}(p-1)}\right)^p = \left(1+ap^{m-1}\right)^p$$

Expanding the right - hand side by using the binomial expansion we have

$$\begin{aligned}\left(r^{p^{m-2}(p-1)}\right)^p &= \left(1+ap^{m-1}\right)^p \\ &= 1 + pap^{m-1} + \underbrace{\frac{p\left(p-1\right)}{2!}\left(ap^{m-1}\right)^2 + \cdots + \left(ap^{m-1}\right)^p}_{\equiv 0 \left(\text{mod } p^{m+1}\right)} \\ &\equiv 1 + ap^m \left(\text{mod } p^{m+1}\right)\end{aligned}$$

Using the rules of indices on the left hand side we have

$$\left(r^{p^{m-2}(p-1)}\right)^p = r^{p^{m-2}(p-1)p} = r^{p^{m-1}(p-1)} \equiv 1 + ap^m \left(\text{mod } p^{m+1}\right)$$

We already have $p \nmid a$ therefore

$$r^{p^{m-1}(p-1)} \equiv 1 + ap^m \not\equiv 1 \left(\text{mod } p^{m+1}\right)$$

Hence we have shown what is required and this completes our proof.

■

Using these results we prove that *every* odd prime power has a primitive root.

Theorem (6.27).

Let p be an odd prime. Then there is a primitive root modulo p^k where $k \geq 1$.

How do we prove this result?

By contradiction.

Proof.

Every prime p has a primitive root by Primitive Root Theorem (6.22):

Every prime has a primitive root.

We are left to prove the given statement for p^k where $k \geq 2$.

Let r be a primitive root modulo p^2. By the previous Proposition (6.26) we have

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k} \qquad (\dagger)$$

The Euler totient function ϕ of p^k is

$$\phi\left(p^k\right) = p^{k-1}(p-1)$$

Applying Euler's Theorem (5.14):

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

On $n = p^k$ we have

$$r^{\phi\left(p^k\right)} \equiv r^{p^{k-1}(p-1)} \equiv 1 \pmod{p^k} \qquad (\dagger\dagger)$$

Suppose that d is a *proper divisor* of $p^{k-1}(p-1)$ such that

$$r^d \equiv 1 \pmod{p^k} \qquad (*)$$

By the definition of congruence there is an integer t such that

$$r^d = 1 + tp^k = 1 + \left(tp^{k-1}\right)p \text{ which implies } r^d \equiv 1 \pmod{p}$$

By applying Proposition (6.4):

Let a modulo n have order k. Then $a^h \equiv 1 \pmod{n} \Leftrightarrow k \mid h$

To the last calculation $r^d \equiv 1 \pmod{p}$ gives $(p-1) \mid d$ because r is a primitive root modulo p.

We are supposing that d is proper divisor of $p^{k-1}(p-1)$ so $d < p^{k-1}(p-1)$.

Therefore, d will be a factor of $p^{k-2}(p-1)$. *Why?*

If $d \mid p$ then $d \mid p^{k-1}$ which implies $d \mid p^{k-2}(p-1)$.

If $d \nmid p$ then $\gcd(d, \ p) = 1$ and so by using Euclid's Lemma (1.13):

If $a \mid (b \times c)$ with $\gcd(a, \ b) = 1$ then $a \mid c$.

On $d \mid p^{k-1}(p-1)$ implies $d \mid (p-1)$ which implies $d \mid p^{k-2}(p-1)$.

This $d \mid p^{k-2}(p-1)$ implies that there is an integer m such that

$$dm = p^{k-2}(p-1) \qquad (**)$$

Raising the congruence in (*) to the power m gives

$$\left(r^d\right)^m \equiv r^{dm} \equiv 1^m \equiv 1 \left(\text{mod } p^k\right)$$

From (**) we have

$$r^{dm} \equiv r^{p^{k-2}(p-1)} \equiv 1 \left(\text{mod } p^k\right)$$

This contradicts (†). This implies that we cannot have d is a *proper divisor* of $p^{k-1}(p-1)$. Hence r is a primitive root modulo p^k.

■

This theorem says that every odd prime power has a primitive root and it is given by:

Proposition (6.28).

Let r be a primitive root modulo p where p is an odd prime. Then either r or $r+p$ (or both) is a primitive root modulo p^k where $k \geq 1$.

Proof. See question 17 of Exercises 6.5.

We also have the following result:

Proposition (6.29).

Let p be an odd prime and r be a primitive root modulo p^2. Then r is a primitive root of every power of p.

Proof. See question 18 of Exercises 6.5.

We can use these propositions to test if a given integer is a primitive root of an odd prime power.

Example 6.29

Find a primitive root of $5^5 = 3125$.

Solution

In Example 27 we showed that 2 is a primitive root of $5^2 = 25$.

By the previous Proposition (6.29) we conclude that 2 is also a primitive root of $5^5 = 3125$.

6.5.3 Primitive Roots of Even Integers

Are there any other integers apart from the odd prime powers which also have primitive roots?

Yes, because integers like 6, 10, 14, 22 have primitive roots and these integers are *not* odd prime powers.

Next, we show that the *even* integer $2p^k$ where p is an odd prime also has primitive roots.

Proposition (6.30).

Let p be an odd prime. Then there is a primitive root of $2p^k$ where $k \geq 1$.

How do we prove this result?

By considering two cases of the primitive root – odd and even.

Proof.

Let r be a primitive root of p^k. (We know such an r exists by the last proposition.)

We consider two cases of the primitive root r;

Case I r is odd Case II r is even

<u>Case I</u> r is odd

The Euler phi function of $2p^k$ is given by

$$\begin{aligned}\phi(2p^k) &= \phi(2)\phi(p^k) \qquad [\text{Because } \phi \text{ multiplicative}]\\ &= 1 \times p^{k-1}(p-1) = p^{k-1}(p-1)\end{aligned}$$

We need to use Euler's Theorem (5.14):

$$a^{\phi(n)} \equiv 1 \pmod{n} \text{ provided } \gcd(a,\ n) = 1$$

Since we are considering the case where r is odd and it is a primitive root of p^k so $\gcd(r,\ 2p^k) = 1$ and we can apply Euler's Theorem:

$$r^{p^{k-1}(p-1)} \equiv 1 \pmod{2p^k}$$

Suppose d is a *proper divisor* of $p^{k-1}\left(p-1\right)$ such that

$$r^d \equiv 1 \left(\text{mod } 2p^k\right)$$

By the definition of congruence we have that there is an integer m which satisfies

$$r^d = 1 + 2p^k m = 1 + \left(2m\right)p^k$$

From this $r^d = 1 + \left(2m\right)p^k$ we have

$$r^d \equiv 1 \left(\text{mod } p^k\right)$$

This is a contradiction because r is a primitive root of p^k so there can be *no* proper divisor d of $\phi\left(2p^k\right) = p^{k-1}\left(p-1\right) = \phi\left(p^k\right)$ such that $r^d \equiv 1 \left(\text{mod } p^k\right)$.

Therefore r is a primitive root modulo $2p^k$.

Case II r is even

In this case $\gcd\left(r,\ 2p^k\right) = 2$. By Definition (6.10):

If $\gcd\left(a,\ n\right) = 1$ and a has order $\phi\left(n\right)$ then a is a **primitive root** of n.

This r which is an even primitive root of p^k *cannot* be a primitive root of $2p^k$.

The primitive root of $2p^k$ must be *odd*.

Let $\alpha = r + p^k$. Then $r + p^k \equiv r \left(\text{mod } p^k\right)$. This is a primitive root of p^k. *Why?*

Because

$$\alpha = r + p^k = \text{even} + \text{odd} = \text{odd}$$

We can now treat this as case I.

Hence this odd integer $\alpha = r + p^k$ is a primitive root of $2p^k$.

■

From this proof we have the following result:

Proposition (6.31).

Let p be an odd prime and $k \geq 1$. Then $2p^k$ has a primitive root. Additionally, if r is a primitive root modulo p^k then

(a) r is also a primitive root modulo $2p^k$ provided r is odd.

(b) $r + p^k$ is a primitive root modulo $2p^k$ provided r is even.

The following statement gives the integers which have *no* primitive roots:

Proposition (6.32).

(a) The integer 2^k where $k \geq 3$ has *no* primitive roots.

(b) Let $m > 2$ and $n > 2$ such that $\gcd\left(m, \quad n\right) = 1$. Then the integer mn has *no* primitive roots.

Proof. See questions 20 and 21 of Exercises 6.5.

Putting all these propositions together we have:

Proposition (6.33).

The positive integer $n > 1$ has a primitive root $\Leftrightarrow$ $n = 2, \ 4, \ p^k, \ 2p^k$ where p is an odd prime and $k \geq 1$.

Summary

In this section we have proved that every odd prime power p^k has a primitive root.

We also showed that apart from 2 and 4 the only even integers which have a primitive root are of the form $2p^k$ where p is an odd prime and $k \geq 1$.

The only integers which have primitive roots are 2, 4, p^k and $2p^k$.