Complete Solutions to Exercises 6.5

1. (i) We need to show that 3 is a primitive root of both 5 and $5^2 = 25$.

   Since $\phi(5) = 4$ so we only need to find powers of 3 which are proper factors of 4; that is 2. We have

   $$3^2 \equiv 9 \equiv 4 \pmod{5}$$

   As $3^2 \equiv 4 \not\equiv 1 \pmod{5}$ so 3 is a primitive root of modulo 5.

   We also need to show that 3 is also a primitive root of $5^2 = 25$.

   The Euler phi function of 25 is $\phi(5^2) = 5(5-1) = 20$.

   By Lemma (6.24):

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

   Just need to show that the order of 3 modulo 25 is *not* $5-1=4$. We have

   $$3^4 \equiv 81 \equiv 6 \not\equiv 1 \pmod{25}$$

   By the above Lemma (6.24) the order of 3 modulo 25 must be

   $$\phi(5^2) = 5(5-1) = 20$$

   Therefore 3 is a primitive root of modulo 25.

   (ii) This time we need to show that 8 is a primitive root of 5 and 25.

   In part (i) we showed that 3 is a primitive root of 5 so 8 is also a primitive root of 5 because $8 \equiv 3 \pmod{5}$.

   Just need to show that 8 is a primitive root of modulo 25.

   Again by the above Lemma (6.24) we need to show that $8^4 \not\equiv 1 \pmod{25}$.

   $$8^4 \equiv (8^2)^2 \equiv 14^2 \equiv 196 \equiv -4 \not\equiv 1 \pmod{25}$$

   Since $8^4 \not\equiv 1 \pmod{25}$ so the order of 8 modulo 25 is

   $$\phi(5^2) = 5(5-1) = 20$$

   Hence 8 is a primitive root of modulo 25.

2. Note that $27 = 3^3$. We only need to find a primitive root of 3^2. *Why?*

   Because by Proposition (6.29):

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

To find a primitive root of 3^2 we use Lemma (6.24):

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

2 is a primitive root of modulo 3. By this Lemma the order of 2 modulo 3^2 can only be $3-1=2$ or $\phi\left(3^2\right)=3\left(3-1\right)=6$.

$$2^2 \equiv 4 \not\equiv 1 \pmod{9}$$

Hence the order of 2 modulo 9 must be 6 so it is a primitive root of modulo $3^2=9$.

By Proposition (6.29) we have 2 is a primitive root of modulo $27=3^3$.

We need to find another primitive root of 27.

By Proposition (6.28):

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

By this proposition we have that 2 or $2+3=5$ is a primitive root of 27.

Using the above Lemma (6.24) we test the index $3-1=2$:

$$5^2 \equiv 25 \not\equiv 1 \pmod{9}$$

Hence the order of 5 is $\phi\left(3^2\right)=3\left(3-1\right)=6$ so it is a primitive root of 9.

By the above Proposition (6.28) we conclude that 5 is a primitive root of modulo 27.

3. Since $11^2=121$ so we find a primitive root of 11 because by Proposition (6.28):

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

So first we find a primitive root r of 11.

We have $\phi\left(11\right)=10$. The factors of 10 are 1, 2, 5 and 10. We only need to find indices 2 and 5 as index 10 will always give us 1 modulo 11 because of Euler's Theorem.

Using base 2 we have

$$2^2 \equiv 4,\ \ 2^5 \equiv 32 \equiv 10 \not\equiv 1 \pmod{11}$$

Hence 2 is a primitive root of 11. Let us test if 2 is also a primitive root of $11^2=121$. *How?*

We use Lemma (6.24):

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

Evaluating the index $11-1=10$:

$$2^{10}\equiv 1024\equiv 56\not\equiv 1\left(\text{mod } 121\right)$$

Hence the order of 2 modulo 11^2 is $\phi\left(11^2\right)=11\left(11-1\right)=110$.

Therefore 2 is a primitive root of modulo $11^2=121$.

4. We need to verify that 10 is a primitive root of $7^2=49$.

   First we find a primitive root of 7 and then we use this to show that 10 is a primitive root of $7^2=49$.

   We have already shown in Example 28 that 3 is a primitive root of modulo 7.

   Note that

   $$10\equiv 3\left(\text{mod } 7\right)$$

   This $10\equiv 3\left(\text{mod } 7\right)$ implies that 10 is also a primitive root of modulo 7.

   To show that 10 is also a primitive root of $7^2=49$ we find the order of 10 modulo 49. By Lemma (6.24):

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

   The order of 10 modulo 49 must be $7-1=6$ or $\phi\left(7^2\right)=7\left(7-1\right)=42$.

   We have

   $$10^6\equiv\left(10^2\right)^3\equiv 100^3\equiv 2^3\equiv 8\not\equiv 1\left(\text{mod } 49\right)$$

   Hence the order of 10 modulo 49 must be 42 so 10 is a primitive root of modulo 49.

   Note that $343=7^3$ and by Proposition (6.29):

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

   Hence 10 is a primitive root of $7^3=343$.

5. We need to show that 47 is a primitive root of 49.

   This is established by showing that

   $$47^{7-1}\equiv 47^6\not\equiv 1\left(\text{mod } 49\right)$$

47 is too large a residue to work with. Since $47 \equiv -2 \pmod{49}$ and it is easier to work with -2 rather than 47 we have

$$47^6 \equiv (-2)^6 \equiv 64 \not\equiv 1 \pmod{49}$$

Since $47^6 \not\equiv 1 \pmod{7^2}$ so the order of 47 is $\phi(7^2) = 7(7-1) = 42$. This implies that 47 is a primitive root of modulo $7^2 = 49$.

6. (i) Note that $81 = 3^4$. We know that 2 is a primitive root of 3.

One shortcut would be to show that 2 is also a primitive root of $3^2 = 9$ because by Proposition (6.29):

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

We use Lemma (6.24) to show that 2 is a primitive root of $3^2 = 9$:

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

We have

$$2^{3-1} = 2^2 \equiv 4 \not\equiv 1 \pmod{9}$$

Hence 2 is a primitive root of modulo $3^2 = 9$. So by the above Proposition (6.29) we conclude that 2 is also a primitive root of modulo $3^4 = 81$.

(ii) This time we need to show that 5 is a primitive root of 81.

Since $5 \equiv 2 \pmod{3}$ so 5 is a primitive root of modulo 3.

We need to show that 5 is also a primitive root of $3^2 = 9$.

$$5^{3-1} = 5^2 \equiv 7 \not\equiv 1 \pmod{9}$$

Hence 5 is a primitive root of $3^2 = 9$.

By Proposition (6.29) we have that 5 is a primitive root of $3^4 = 81$.

(iii) We need to show that 79 is *not* a primitive root of 81. We have

$$79 \equiv 1 \pmod{3}$$

1 is *not* a primitive root of modulo 3 so 79 cannot be a primitive root of modulo 3.

Hence 79 is *not* a primitive root of modulo 81.

7. (a) Since $10 = 2 \times 5$ which is of the form $2p^k$ where $p = 5$ and $k = 1$ so it has a primitive root because by Proposition (6.32):

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

We need to find a primitive root of modulo 10. We use Proposition (6.31):

If r is a primitive root of 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.

We have already established 2 is a primitive root of 5. We don't need to check that 2 is a primitive root of 10. *Why?*

Because 2 is even so 2 is not a primitive root of 10.

By the above Proposition (6.31) we have $2 + 5 = 7$ is a primitive root of 10.

[3 is also a primitive root of 10.]

(b) As $12 = 2^2 \times 3$ so it has *no* primitive roots. [It is *not* of the form $2p^k$.]

(c) Since $50 = 2 \times 5^2$ so it is of the form $2p^k$ so it has primitive roots. We know that 2 is a primitive root of modulo 5.

Again 2 being even it *cannot* be a primitive root of 50 because of the above Proposition (6.31).

Hence a primitive root of 50 is $2 + 5^2 = 27$.

(d) Since $100 = 2^2 \times 5^2$ so it has *no* primitive roots.

(e) Since $98 = 2 \times 49 = 2 \times 7^2$ so it has a primitive root. We have already established that 3 is a primitive root of 7. As 3 is odd so 3 is also a primitive root of 98.

(f) We know that $18 = 2 \times 3^2$ so it has a primitive root. Again we have already established that 2 is a primitive root of 3. Since 2 is even so by Proposition (6.31)(b) we have $2 + 3^2 = 11$ is a primitive root of 18.

(g) We have $22 = 2 \times 11$ which is of the form $2p^k$ so it has a primitive root.

What is a primitive root of the odd prime 11?

You can show that 2 is a primitive root of 11. Since 2 is even so

$$2 + 11 = 13 \text{ is a primitive root of modulo } 22$$

(h) Note that $118 = 2 \times 59$ and 59 is an odd prime. We need to first find a primitive root of 59.

The Euler phi function of 59 is

$$\phi(59) = 59 - 1 = 58$$

Factorizing 58 gives $58 = 2\times 29$. Evaluating the first power, 2, with base 2 gives $2^2 \equiv 4 \pmod{59}$. We also need to find the second power, 29, with base 2. Working out powers of 2 we have

$$2^6 = 64 \equiv 5 \pmod{59}$$

By the division algorithm we have

$$29 = (6\times 4) + 5$$

Hence

$$2^{29} \equiv 2^{(6\times 4)+5} \equiv \left(2^6\right)^4 \times 2^5 \equiv 5^4 \times 32 \equiv 625\times 32 \equiv 58 \equiv -1 \pmod{59}$$

This $2^{29} \equiv -1 \not\equiv 1 \pmod{59}$ implies that 2 is a primitive root of 59.

Since 2 is even so $2 + 59 = 61$ is a primitive root of 118.

8. We can easily show that 2 is a primitive root of modulo 25. *How many incongruent primitive roots does 25 have?*

By question 18 of the Supplementary Problems on Chapter 6:

If n has a primitive root then it has exactly $\phi(\phi(n))$ incongruent primitive roots.

We have

$$\phi(\phi(25)) = \phi(20) = \phi(2^2\times 5) = \phi(2^2)\times\phi(5) = 2\times 4 = 8$$

There are 8 incongruent primitive roots of modulo 25.

To find the primitive roots of modulo 25 we use Lemma (6.24):

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

To determine whether an integer $r + p$ is a primitive root of 25.

Let us check if $2 + 5 = 7$ is a primitive root of 25.

$$7^{5-1} = 7^4 \equiv 1 \pmod{25}$$

This $7^4 \equiv 1 \pmod{25}$ implies 7 is *not* a primitive root of 25.

Let us next trial $7 + 5 = 12$:

$$12^4 \equiv 11 \not\equiv 1 \pmod{25}$$

Hence 12 is a primitive root of modulo 25.

Adding another 5 gives $12 + 5 = 17$:

$$17^4 \equiv 21 \not\equiv 1 \pmod{25}$$

Hence 17 is a primitive root of modulo 25.

The last of these is $17+5=22$:

$$22^4 \equiv 5 \not\equiv 1 \pmod{25}$$

Hence 22 is a primitive root of modulo 25.

So far we have 4 primitive roots of modulo 25 and these are 2, 12, 17 and 22.

There are 4 more.

We have shown in the main text that 3 is also a primitive root of 5. Let us see if this is also a primitive root of 25:

$$3^4 \equiv 81 \equiv 6 \not\equiv 1 \pmod{25}$$

Hence 3 is a primitive root of modulo 25.

Next we test $3+5=8$:

$$8^4 \equiv 21 \not\equiv 1 \pmod{25}$$

Therefore 8 is also a primitive root of 25.

Now we test $8+5=13$:

$$13^4 \equiv 11 \not\equiv 1 \pmod{25}$$

13 is also a primitive root of 25.

Next we test $13+5=18$:

$$18^4 \equiv 1 \pmod{25}$$

This $18^4 \equiv 1 \pmod{25}$ implies that 18 is *not* a primitive root of 25.

Now we test $18+5=23$:

$$23^4 \equiv 16 \not\equiv 1 \pmod{25}$$

Hence 23 is a primitive root of 25.

Collecting all 8 of the *incongruent* primitive roots of modulo 25:

$$\left\{2,\ 3,\ 8,\ 12,\ 13,\ 17,\ 22,\ 23\right\}$$

9. We have shown in Example 28 that 3 is a primitive root of 49.

By question 18 of the Supplementary Problems on Chapter 6:

> If n has a primitive root then it has exactly $\phi\left(\phi\left(n\right)\right)$ incongruent primitive roots.

The number of incongruent primitive roots of modulo 49 are

$$\phi\left(\phi\left(49\right)\right)=\phi\left(\phi\left(7^2\right)\right)=\phi\left(7\left(6\right)\right)=\phi\left(42\right)=\phi\left(6\right)\phi\left(7\right)=2\times 6=12$$

We have 12 incongruent primitive roots of modulo 49.

3 is one of these primitive roots.

We use Lemma (6.24):

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

We need to determine whether an integer $r+p$ is also a primitive root of $49=7^2$.

We test $3+7=10$ to the index $7-1=6$:

$$10^6 \equiv 8 \not\equiv 1 \pmod{49}$$

Hence 10 is a primitive root of 49.

Now we test $10+7=17$:

$$17^6 \equiv 22 \not\equiv 1 \pmod{49}$$

Therefore 17 is also a primitive root of 49.

Continuing in this manner by adding 7 each time we have the following congruences:

$$24^6 \equiv 36 \not\equiv 1 \pmod{49}$$

$$\begin{aligned} 31^6 &\equiv 1 \pmod{49} \\ 38^6 &\equiv \left(-11\right)^6 \equiv 15 \not\equiv 1 \pmod{49} \\ 45^6 &\equiv \left(-4\right)^6 \equiv 29 \not\equiv 1 \pmod{49} \end{aligned}$$

Out of these 24, 38 and 45 are primitive roots of modulo 49. So far we have

3, 10, 17, 24, 38 and 45 incongruent primitive roots modulo 49

We can show that 5 is also a primitive root of 49.

This time adding a multiple of 7 to 5 gives the integers

$$12,\ 19,\ 26,\ 33,\ 40,\ 47$$

Testing each of these integers to the index $7-1=6$:

$$\begin{aligned} 12^6 &\equiv 22 \not\equiv 1 \pmod{49} \\ 19^6 &\equiv 1 \pmod{49} \\ 26^6 &\equiv 29 \not\equiv 1 \pmod{49} \\ 33^6 &\equiv 8 \not\equiv 1 \pmod{49} \\ 40^6 &\equiv 36 \not\equiv 1 \pmod{49} \\ 47^6 &\equiv 15 \not\equiv 1 \pmod{49} \end{aligned}$$

Similarly we have 12, 26, 33, 40 and 47 are primitive roots of modulo 49.

Collecting all the primitive roots of modulo 49 we have that

$$\left\{3,\ 5,\ 10,\ 12,\ 17,\ 24,\ 26,\ 33,\ 38,\ 40,\ 45,\ 47\right\}$$

These are all the 12 incongruent primitive roots of modulo 49.

10. We need to find all the incongruent primitive roots of modulo 54. First we show that 54 does have primitive roots.

Since $54 = 2 \times 27 = 2 \times 3^3$ which is of the form $2p^k$ so 54 does have primitive roots. The Euler phi function of 54 is given by

$$\phi(54) = \phi(2 \times 3^3) = \phi(2) \times \phi(3^3) = 1 \times \left[3^2(3-1)\right] = 18$$

How many primitive roots does 54 have?

By question 18 of the Supplementary Problems on Chapter 6:

> If n has a primitive root then it has exactly $\phi(\phi(n))$ incongruent primitive roots.

Evaluating $\phi(\phi(54))$ we have

$$\phi(\phi(54)) = \phi(18) = \phi(2 \times 9) = \phi(2) \times \phi(9) = 1 \times (3 \times 2) = 6$$

Modulo 54 has 6 incongruent primitive roots.

How do we find all 6 incongruent primitive roots of modulo 54?

By using Proposition (6.31):

> If r is a primitive root of 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.

In our case $p = 3$ because $54 = 2 \times 3^3$.

In the hint we are given that $\{2, 5, 11, 14, 20, 23\}$ are primitive roots of modulo 27.

In this list $\{2, 5, 11, 14, 20, 23\}$ the integers 5, 11 and 23 are odd so by the above proposition they are primitive roots of modulo $54 = 2 \times 3^3$.

2 is even so $2 + 3^3 = 29$ is a primitive root of modulo 54.

Similarly 14 is even so $14 + 3^3 = 41$ is a primitive root of modulo 54.

Also 20 is even so $20 + 3^3 = 47$ is a primitive root of modulo 54.

The incongruent primitive roots of modulo 54 are

$$\left\{5, 11, 23, 29, 41, 47\right\}$$

11. We need to find all the incongruent primitive roots of modulo 38.

Since $38 = 2\times 19$ so it has primitive roots because it is of the form $2p^k$.

How many primitive roots does modulo 38 have?

By question 18 of the Supplementary Problems on Chapter 6:

> If n has a primitive root then it has exactly $\phi\left(\phi\left(n\right)\right)$ incongruent primitive roots.

Therefore modulo 38 has

$$\begin{aligned}\phi\left(\phi\left(38\right)\right) &= \phi\left(\phi\left(2\times 19\right)\right)\\ &= \phi\left(\phi\left(2\right)\times\phi\left(19\right)\right)\\ &= \phi\left(\phi\left(19\right)\right) = \phi\left(18\right) = \phi\left(2\times 3^2\right) = 3\left(3-1\right) = 6\end{aligned}$$

Hence modulo 38 has 6 incongruent primitive roots.

We first find a primitive root of modulo 19 as in this case we have $p = 19$.

You can check that 2 is a primitive root of modulo 19.

We can find the other primitive roots of modulo 19 by using Proposition (6.18):

> Let r be a primitive root of modulo p where p is prime. Then $r^m \left(\text{mod } p\right)$ is also a primitive root of modulo p provided $\gcd\left(m,\ \ p-1\right) = 1$.

We use $r = 2$ to find the other primitive roots of modulo 19.

Also $p - 1 = 19 - 1 = 18$. We only consider the m values which are relatively prime to 18. These are 5, 7, 11, 13 and 17:

$$2^5 \equiv 32 \equiv 13\left(\text{mod } 19\right)$$

$$2^7 \equiv 128 \equiv 14\left(\text{mod } 19\right)$$

$$2^{11} \equiv 15\left(\text{mod } 19\right)$$

$$2^{13} \equiv 3\left(\text{mod } 19\right)$$

$$2^{17} \equiv 10\left(\text{mod } 19\right)$$

Thus the primitive roots of modulo 19 are 2, 3, 10, 13, 14 and 15.

How do we find the 6 incongruent primitive roots of modulo 38?

By using Proposition (6.31):

> If r is a primitive root of 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.

Since the primitive roots of modulo 19 are 2, 3, 10, 13, 14 and 15 so the odd ones amongst this list are also primitive roots of modulo 38, that is 3, 13 and 15 are primitive roots of modulo 38.

Since 2 is even so with $r = 2,\ p = 19$ we have $r + p = 2 + 19 = 21$ is a primitive root of modulo 38.

Also 10 is even so $10 + 19 = 29$ is a primitive root of modulo 38.

Finally 14 is even so $14 + 19 = 33$ is a primitive root of modulo 38.

All the incongruent primitive roots of modulo 38 are

$$\left\{3,\ 13,\ 15,\ 21,\ 29,\ 33\right\}$$

12. We first need to show that 14 is a primitive root of modulo 29. The Euler phi function of the prime 29 is 28. The proper divisors of 28 are 2, 4, 7 and 14:

$$14^2 \equiv 22 \left(\text{mod } 29\right)$$

$$14^4 \equiv 22^2 \equiv 20 \left(\text{mod } 29\right)$$

$$14^7 \equiv 14^4 \times 14^3 \equiv 20 \times 2744 \equiv 12 \left(\text{mod } 29\right)$$

$$14^{14} \equiv \left(14^7\right)^2 \equiv 12^2 \equiv 144 \equiv 28 \left(\text{mod } 29\right)$$

Hence 14 is a primitive root of modulo 29.

We also need to show that 14 is *not* a primitive root of modulo 29^2. *How do we show this?*

By Lemma (6.24):

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

We need to show that the order of 14 modulo 29^2 is $29 - 1 = 28$. By evaluating powers of 14 we have

$$14^{28} \equiv \left(14^4\right)^2 \equiv 28^2 \equiv 1 \left(\text{mod } 29^2\right)$$

Hence 14 *cannot* be a primitive root of modulo 29^2.

By Proposition (6.28):

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

A primitive root of modulo 29^2 is $14 + 29 = 43$.

13. We can easily establish that 2 is a primitive root of modulo 13. We need to find a primitive root of $2\times 13^4 = 57122$. *How?*

By using Proposition (6.31):

If r is a primitive root of 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.

We need to check that $r=2$ is a primitive root of modulo 13^2. *How?*

By Lemma (6.24);

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

The order of 2 modulo 13^2:

$$2^{12}\equiv 40 \not\equiv 1 \left(\text{mod } 13^2\right)$$

Hence 2 is a primitive root of modulo 13^k. Since 2 is even so

$$2+13^4 = 28563 \text{ is a primitive root of modulo } 2\times 13^4 = 57122$$

14. Since $34 = 2\times 17$ so it has primitive roots because it is of the form $2p^k$.

We first find all the incongruent primitive roots of prime 17.

Testing 2 for a primitive root:

We have $\phi\left(17\right)=16$ and the only proper factors of 16 are 2, 4 and 8:

$$2^2\equiv 4,\ \ 2^4\equiv 16,\ \ 2^8\equiv 1\left(\text{mod } 17\right)$$

Hence 2 *cannot* be a primitive root of modulo 17 because $2^8\equiv 1\left(\text{mod } 17\right)$.

Let us now trial 3:

$$3^2\equiv 9,\ \ 3^4\equiv 13,\ \ 3^8\equiv 16\left(\text{mod } 17\right)$$

Hence 3 is a primitive root of modulo 17.

Now we use 3 as a base to find the other primitive roots of 17. *Why?*

Because by using Proposition (6.18):

Let r be a primitive root of modulo p where p is prime. Then $r^m\left(\text{mod } p\right)$ is also a primitive root of modulo p provided $\gcd\left(m,\ \ p-1\right)=1$.

In our case we have $p-1=17-1=16$. The integers below 16 which are relatively prime to 16 are all odd integers (1, 3, 5, 7, 9, 11, 13 and 15) up to 15 (inclusive).

$$3^3 \equiv 10 \pmod{17}$$
$$3^5 \equiv 5 \pmod{17}$$
$$3^7 \equiv 11 \pmod{17}$$
$$3^9 \equiv 14 \pmod{17}$$
$$3^{11} \equiv 7 \pmod{17}$$
$$3^{13} \equiv 12 \pmod{17}$$
$$3^{15} \equiv 6 \pmod{17}$$

Thus the primitive roots of modulo 17 are $\{3, 5, 6, 7, 10, 11, 12, 14\}$.

How do we find the primitive roots of modulo 34?

By using Proposition (6.31):

> If r is a primitive root of 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 odd integers amongst the above list are 3, 5, 7 and 11 so they are also primitive roots of modulo $2 \times 17 = 34$.

For the even integers 6, 10, 12 and 14 we add 17 in each case:

$$6 + 17 = 23$$
$$10 + 17 = 27$$
$$12 + 17 = 29$$
$$14 + 17 = 31$$

These are also primitive roots of modulo 34.

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

15. We need to show that 3 is a primitive root of 343. First note that $343 = 7^3$.

This is similar to question 14 of the last Exercises (6.4) but this time we use the theory developed in this section.

You can easily verify that 3 is a primitive root of modulo 7. Then by Proposition (6.28):

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

Either 3 or $3+7=10$ is a primitive root of $343=7^3$. We want to show that 3 is a primitive root of modulo 343.

Therefore we need to show that the order of 3 modulo 343 is equal to

$$\phi\left(343\right)=\phi\left(7^3\right)=343-49=294$$

The positive divisors of 294 are $\{1, 2, 3, 6, 7, 14, 21, 42, 49, 98, 147, 294\}$.

Clearly the indices 1, 2, 3, of base 3 are *not* going to work. We try the next index:

$$3^6\equiv 729\equiv 43\not\equiv 1\left(\text{mod } 343\right)$$

Using this to evaluate the next index 7 gives

$$3^7\equiv 3^6\times 3\equiv 43\times 3\equiv 129\not\equiv 1\left(\text{mod } 343\right)$$

Using these results obtained to find the remaining indices (apart from the last one which we know is going to give us 1 modulo 343 because of Euler's Theorem):

$$3^{14}\equiv\left(3^7\right)^2\equiv 129^2\equiv 16641\equiv 177\not\equiv 1\left(\text{mod } 343\right)$$

$$3^{21}\equiv\left(3^6\right)^3\times 3^3\equiv 43^3\times 27\equiv 2\,146\,689\equiv 195\not\equiv 1\left(\text{mod } 343\right)\qquad(\ddagger)$$

$$3^{42}\equiv 195^2\equiv 38\,025\equiv 295\equiv -48\not\equiv 1\left(\text{mod } 343\right)\qquad(*)$$

$$3^{49}\equiv 3^{42}\times 3^7\equiv -48\times 129\equiv -6192\equiv 325\equiv -18\not\equiv 1\left(\text{mod } 343\right)\qquad(**)$$

$$3^{98}\equiv\left(3^{49}\right)^2\equiv\left(-18\right)^2\equiv 324\equiv -19\not\equiv 1\left(\text{mod } 343\right)$$

$$3^{147}\equiv 3^{98}\times 3^{49}\equiv\left(-19\right)\times\left(-18\right)\equiv 342\equiv -1\not\equiv 1\left(\text{mod } 343\right)$$

Therefore the order of 3 modulo 343 is $\phi\left(343\right)=294$ which implies that it is a primitive root of modulo 343.

(ii) We are asked to solve the quadratic $x^2\equiv 295\left(\text{mod } 343\right)$. Using the rules of indices with respect to the base 3 we have

$$2\ ind_3\left(x\right)\equiv ind_3\left(295\right)\left(\text{mod } 294\right)$$

From (*) in part (i) we have $ind_3\left(195\right)=42$, substituting this into the above

$$2\ ind_3\left(x\right)\equiv 42\left(\text{mod } 294\right)$$

We have 2 *incongruent* solutions because the $\gcd(2,\ 294)=2$ and $2 \mid 42$

$$\begin{aligned} 2\ ind_3(x) \equiv 42 \pmod{294} \quad &\Rightarrow \quad ind_3(x) \equiv 21 \pmod{147} \\ &\Rightarrow \quad ind_3(x) \equiv 21,\ 21+147 \equiv 21,\ 168 \pmod{294} \end{aligned}$$

From the last line $ind_3(x) \equiv 21,\ 168 \pmod{294}$ we deduce that

$$x \equiv 3^{21},\ 3^{168} \pmod{343}$$

From (‡) we have $x \equiv 3^{21} \equiv 195 \pmod{343}$. Evaluating the other index by using the the results obtained in part (i) we have

$$x \equiv 3^{168} \equiv 3^{147} \times 3^{21} \equiv (-1) \times 195 \equiv -195 \equiv 148 \pmod{343}$$

The other solution is $x \equiv -148 \equiv 195 \pmod{343}$.

Our solutions to the given quadratic $x^2 \equiv 295 \pmod{343}$ are

$$x \equiv 148, 195 \pmod{343}$$

(iii) We are asked to solve $x^7 \equiv 325 \pmod{343}$. Taking indices to base 3:

$$7\ ind_3(x) \equiv ind_3(325) \pmod{294}$$

By (**) of part (i) we have $ind_3(325) = 49$. Substituting this gives

$$7\ ind_3(x) \equiv ind_3(325) \equiv 49 \pmod{294}$$

The $\gcd(7,\ 294)=7$ and $7 \mid 49$ so we have 7 incongruent solutions to the given equation. Simplifying this $7\ ind_3(x) \equiv 49 \pmod{294}$ yields

$$ind_3(x) \equiv 7 \pmod{42}$$

By definition of congruence we have

$$ind_3(x) \equiv 7 \pmod{42} \quad \Leftrightarrow \quad ind_3(x) = 7 + 42k$$

Since we know that we have 7 incongruent solutions so substituting $k = 0, 1, \cdots, 6$ gives

$$\begin{aligned} ind_3(x) &\equiv 7, 7+42, 7+2(42), 7+3(42), 7+4(42), 7+5(42), 7+6(42) \\ &\equiv 7, 49, 91, 133, 175, 217, 259 \pmod{294} \end{aligned}$$

Therefore the solutions are given by

$$x \equiv 3^7, 3^{49}, 3^{91}, 3^{133}, 3^{175}, 3^{217}, 3^{259} \pmod{343}$$

Using the results of part (i) for the first two indices we have

$$x \equiv 3^7 \equiv 129,\ 3^{49} \equiv 325 \pmod{343}$$

By using (*) and (**) we can find the next index:

$$x \equiv 3^{91} \equiv 3^{42} \times 3^{49} \equiv (-48)\times(-18) \equiv 864 \equiv 178 \pmod{343}:$$

The next index $3^{133} \pmod{343}$ is a bit cumbersome to evaluate, let skip this and find this at the end. For the next three congruences $x \equiv 3^{175}, 3^{217}, 3^{259} \pmod{343}$ we can use the last computation in part (i) which is $3^{147} \equiv -1 \pmod{343}$. Breaking each of the indices 175, 217 and 259 we have

$$x \equiv 3^{175} \equiv 3^{147} \times 3^{28} \equiv (-1)\times\left(3^{14}\right)^2 \equiv -(177)^2 \equiv -31\,329 \equiv 227 \pmod{343}$$
$$x \equiv 3^{217} \equiv 3^{147} \times 3^{49} \times 3^{21} \equiv (-1)\times(-18)\times 195 \equiv 3510 \equiv 80 \pmod{343}$$
$$x \equiv 3^{259} \equiv 3^{147} \times 3^{98} \times 3^{14} \equiv (-1)\times(-19)\times 177 \equiv 3363 \equiv 276 \pmod{343}$$

Let us now evaluate the one we left earlier:

$$x \equiv 3^{133} \equiv 3^{98} \times 3^{21} \times 3^{14} \equiv (-19)\times 195 \times 177 \equiv -655\,785 \equiv 31 \pmod{343}$$

Our solutions are $x \equiv 31, 80, 129, 178, 227, 276, 325 \pmod{343}$.

16. Lemma (6.24) claims:

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

Proof.

Let r have order k modulo p^2 that is

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

Since $\phi\left(p^2\right) = p(p-1)$ so by Corollary (6.5):

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

We have

$$k \mid \phi\left(p^2\right) \quad \Rightarrow \quad k \mid p(p-1) \qquad (\dagger)$$

We show that either $k = p-1$ or $k = p(p-1)$.

Suppose $k = dp$ where d is a proper divisor of $p-1$ then

$$r^k \equiv r^{dp} \equiv 1 \pmod{p^2}$$

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

$$r^{dp} \equiv 1 \pmod{p^2} \quad \Rightarrow \quad r^{dp} = 1 + mp^2 = 1 + (mp)p$$

From the last calculation we have

$$r^{dp} = 1 + (mp)p \text{ implies that } r^{dp} \equiv (r^d)^p \equiv 1 \pmod{p}$$

However $r^d \not\equiv 1 \pmod{p}$ because d is a proper divisor of $p-1$ and we are given that r is a primitive root of p.

Hence $(r^d)^p \equiv 1 \pmod{p}$ is *impossible* because by Corollary (4.2):

$$n^p \equiv n \pmod{p}$$

We have $(r^d)^p \equiv r \not\equiv 1 \pmod{p}$. This is clearly a contradiction so $k \neq dp$ where d is a proper divisor of $p-1$.

From this $k \neq dp$ we have $\gcd(k, \; p) = 1$.

From (†) we have $k \mid p(p-1)$. Using Euclid's Lemma (1.13):

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

On $k \mid p(p-1)$ gives $k \mid (p-1)$. Required to show that $k = p-1$.

From (*) we have

$$r^k \equiv 1 \pmod{p^2} \text{ which implies } r^k \equiv 1 \pmod{p}$$

We are given that r is a primitive root of p so the lowest index to give 1 modulo p is $p-1$, that is $r^{p-1} \equiv 1 \pmod{p}$.

By Proposition (6.4):

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

We have $(p-1) \mid k$.

In the above we had $k \mid (p-1)$ and now $(p-1) \mid k$ so $k = p-1$.

Hence either $k = p-1$ or $k = p(p-1)$.

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

■

17. The given proposition (6.28):

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

Proof.

For $k = 1$ we have the given primitive root r of modulo p.

For $k \geq 2$:

The proof of this follows from Theorem (6.27):

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

From the proof of Theorem (6.25) we have:

(I) The primitive root of p^2 is the same primitive root r as the odd prime p or it is $r + p$ (or both).

(II) Also from the proof of Theorem (6.27) we showed that the primitive root of modulo p^2 is also a primitive root of p^k.

Combining these two results (I) and (II) gives the required result.

■

18. We are asked to show that:

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

Proof.

In the proof of Theorem (6.27) we showed that the primitive root of modulo p^2 is also a primitive root of p^k.

■

19. We are asked to show that p^k and $2p^k$ have the same number of *incongruent* primitive roots provided p is an odd prime.

Proof.

By the main propositions in the text we have that both p^k and $2p^k$ have primitive roots.

By question 18 of the Supplementary Problems on Chapter 6:

> If n has a primitive root then it has exactly $\phi\left(\phi\left(n\right)\right)$ incongruent primitive roots.

We show that $\phi\left(p^k\right) = \phi\left(2p^k\right)$.

Since p is an odd prime so $\gcd\left(2,\ p^k\right) = 1$. Using the multiplicative property of the Euler phi function we have

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

Since $\phi\left(p^k\right)=\phi\left(2p^k\right)$ so by the above proposition we have that p^k and $2p^k$ have the same number of *incongruent* primitive roots.

■

20. We are asked to prove that 2^k where $k \geq 3$ has *no* primitive roots.

How to we prove this result?

By using the hint which says use mathematical induction on k.

Proof.

Base Case

First we prove there are *no* primitive roots of integer $2^3=8$. This is our base case.

Let r be odd because $\gcd\left(r,\ \ 8\right)=1$ for r to be considered as a primitive root.

Let $r=2m+1$ where m is an integer.

Now we can evaluate $\phi\left(2^3\right)$ by Proposition (5.4):

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

We have

$$\phi\left(2^3\right)=2^2\left(2-1\right)=4$$

The only proper factor of 4 is 2. Let us check to see that r to the index 2 does *not* give 1 modulo 8:

$$r^2=\left(2m+1\right)^2=4m^2+4m+1=4m\left(m+1\right)+1 \qquad (*)$$

Note that $m\left(m+1\right)=\text{even}$. Writing $m\left(m+1\right)=2n$ for some integer n.

Substituting this into (*) gives

$$r^2=4m\left(m+1\right)+1=4\left(2n\right)+1=8n+1\equiv 1\left(\text{mod } 8\right)$$

Since the index 2 of r gives 1 modulo 8 so r cannot be a primitive root of modulo 8.

Hence $2^3=8$ has *no* primitive roots.

Induction Hypothesis

Assume the given result is true for $k=m$:

That is 2^m has *no* primitive roots. This implies that there is a proper factor d of 2^{m-1}, that is $d \mid 2^{m-1}$, such that for all residues r which are relatively prime to 2^m we have

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

Induction Step

Required to prove that 2^{m+1} has *no* primitive roots.

By the above Proposition (5.4) we have

$$\phi\left(2^{m+1}\right) = 2^m$$

Let r be a residue which is relatively prime to 2^{m+1}.

From (*) we have an integer k such that

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

If k is even then we are done because $k = 2l$ for some integer l and

$$r^d = 1 + \left(2^m\right)2l = 1 + 2^{m+1}l \;\Rightarrow\; r^d \equiv 1 \left(\text{mod } 2^{m+1}\right)$$

Where d is a proper divisor of $\phi\left(2^{m+1}\right) = 2^m$ because $d \mid 2^{m-1}$.

If k is odd, $k = 2n + 1$ say, then by substituting this into ($\ddagger$) gives

$$r^d = 1 + \left(2^m\right)k = 1 + 2^m\left(2n+1\right) = 1 + 2^m + 2^{m+1}n$$

Writing this $r^d = 1 + 2^m + 2^{m+1}n$ as congruence modulo 2^{m+1} gives

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

Squaring both sides of this congruence yields

$$\begin{aligned}\left(r^d\right)^2 &\equiv \left(1+2^m\right)^2\\ r^{2d} &\equiv 1 + 2\left(2^m\right) + \left(2^m\right)^2\\ &\equiv 1 + 2^{m+1} + 2^{2m}\\ &\equiv 1 + 2^{m+1}\left(1 + 2^{m-1}\right)\\ &\equiv 1\left(\text{mod } 2^{m+1}\right)\end{aligned}$$

As d is a proper divisor of 2^{m-1} therefore $2d \mid 2^m$.

So $2d$ is a proper divisor of $\phi\left(2^{m+1}\right) = 2^m$. Since in the above derivation we have $r^{2d} \equiv 1\left(\text{mod } 2^{m+1}\right)$ so r *cannot* be a primitive root of modulo 2^{m+1}.

Hence by mathematical induction we have 2^k where $k \geq 3$ has *no* primitive roots.

■

21. We need to prove that mn has *no* primitive roots given $\gcd(m, \ n) = 1$.

Proof.

Since we are given that $\gcd(m, \ n) = 1$ so $\phi(mn) = \phi(m)\phi(n)$.

By Euler's Theorem (5.14):

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

Let $\gcd(r, \ m) = \gcd(r, \ n) = 1$. Then by Euler's Theorem we have

$$r^{\phi(m)} \equiv 1 \pmod{m} \qquad (*)$$

$$r^{\phi(n)} \equiv 1 \pmod{n} \qquad (**)$$

By Proposition (5.10):

$$\boxed{\phi(l) \text{ is an even integer for } l > 2}$$

Therefore both $\phi(m)$ and $\phi(n)$ are divisible by 2.

Raise the congruence in (*) to the power of $\frac{\phi(n)}{2}$:

$$\left(r^{\phi(m)}\right)^{\frac{\phi(n)}{2}} \equiv r^{\frac{\phi(m)\phi(n)}{2}} \equiv 1 \pmod{m}$$

Similarly raising the congruence in (**) to the power of $\frac{\phi(m)}{2}$ gives

$$\left(r^{\phi(n)}\right)^{\frac{\phi(m)}{2}} \equiv r^{\frac{\phi(n)\phi(m)}{2}} \equiv 1 \pmod{n}$$

We have $r^{\frac{\phi(m)\phi(n)}{2}} \equiv 1 \pmod{m}$ and $r^{\frac{\phi(n)\phi(m)}{2}} \equiv 1 \pmod{n}$.

We need to use the result; that given $\gcd(k_1, \ k_2) = 1$ then

$$\boxed{a \equiv b \pmod{k_1} \text{ and } a \equiv b \pmod{k_2} \text{ implies } a \equiv b \pmod{k_1 k_2}}$$

Therefore applying this to $r^{\frac{\phi(m)\phi(n)}{2}} \equiv 1 \pmod{m}$ and $r^{\frac{\phi(n)\phi(m)}{2}} \equiv 1 \pmod{n}$ gives

$$r^{\frac{\phi(m)\phi(n)}{2}} \equiv 1\left(\text{mod } mn\right)$$

Hence r *cannot* be a primitive root of mn.

■

22. We are asked to prove that if r is a primitive root of odd prime p and

$$\left(r+mp\right)^{p-1} \not\equiv 1\left(\text{mod } p^2\right) \quad \Rightarrow \quad r+mp \text{ is a primitive root of } p^k$$

Proof.

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 we are given that $\left(r+mp\right)^{p-1} \not\equiv 1\left(\text{mod } p^2\right)$ so the order of $r+mp$ must be $\phi\left(p^2\right)=p\left(p-1\right)$. Therefore $r+mp$ is a primitive root of p^2.

By Proposition (6.29):

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

We have $r+mp$ is a primitive root of p^k for $k \geq 1$.

This completes our proof.

■

23. Required to prove that $n=2^i p^j$ for $i \geq 2$ and $j \geq 1$ has *no* primitive roots.

Proof.

If $p=2$ then $n=2^i p^j=2^{i+j}$ and $i+j \geq 3$. By result of question 3:

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

Hence $n=2^i p^j$ has *no* primitive roots.

If p is odd then $\gcd\left(2^i,\ p^j\right)=1$ and $\phi\left(2^i\right)>2,\ \phi\left(p^j\right)>2$. So by Proposition (6.32) (b):

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

Applying this we have $n=2^i p^j$ has *no* primitive roots.

This completes our proof.

■

24. We need to show that given $r^m \equiv 1 \pmod{n}$ then in general $m \nmid \phi(n)$.

By the hint let $n = 15$ then with $m = 12$:

$$2^{12} \equiv 1 \pmod{15}$$

Also

$$\phi(15) = \phi(3 \times 5) = \phi(3) \times \phi(5) = 2 \times 4 = 8$$

We have $m = 12$ and $12 \nmid 8$ implies $12 \nmid \phi(15)$.

25. We have shown in question 8 that 2 is a primitive root of $5^2 = 25$. Also in question 8 we showed that $2 + 5 = 7$ is *not* a primitive root of modulo 25.

26. See solution to question 14 of the previous Exercises 6.4. Replace the prime p with n.

27. First we show that 3 is a primitive root of modulo $5^2 = 25$. We have already shown in question 1 that 3 is a primitive root of modulo $5^2 = 25$.

By using Proposition (6.31):

If r is a primitive root of 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.

With $r = 2$ and $p^2 = 5^2$ we have 3 is a primitive root of modulo 50.

Also

$$\phi(50) = \phi(2 \times 5^2) = \phi(2)\phi(5^2) = 1 \times 20 = 20$$

Since 3 is a primitive root of modulo 50 so

$$3^{20} \equiv 1 \pmod{50} \qquad (*)$$

Let $N = 3^{3^8} + 1$. We want to find the least positive integer x such that

$$N = 3^{3^8} + 1 \equiv x \pmod{50}$$

Note that $3^{3^8} = 3^{\left(3^8\right)}$ so $3^8 = 6561$. We have

$$3^{3^8}+1 \equiv 3^{3561}+1 \pmod{50} \qquad (**)$$

Writing the index 3561 as a multiple of 20 and any remainder we have

$$3561 = (178 \times 20) + 1$$

Therefore

$$3^{3^8} \equiv 3^{3561} \equiv 3^{(178\times 20)+1} \equiv \left(3^{20}\right)^{178} 3 \equiv 3 \pmod{50}$$

Putting this result into (*) gives

$$3^{3^8}+1 \equiv 3+1 \equiv 4 \pmod{50}$$

The least positive residue is $x \equiv 4 \pmod{50}$.