Complete Solutions to Exercises 6.4

1. In order to find the primitive roots of the given prime we use Proposition (6.18):

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

(a) First we need to find a primitive root of 7. Recall we only need to try the positive factors of $\phi(7)=6$. *Why?*

Because of Corollary (6.5):

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

The only positive factors of 6 are 1, 2, 3 and 6.

We could try 2:

$$2^1 \equiv 2,\ \ 2^2 \equiv 4,\ \ 2^3 \equiv 8 \equiv 1 \pmod{7}.$$

Since $2^3 \equiv 1 \pmod{7}$ which implies that the order of 2 modulo 7 is 3 and *not* 6 so it *cannot* be a primitive root of modulo 7.

Next we try 3:

$$3^1 \equiv 3,\ \ 3^2 \equiv 2,\ \ 3^3 \equiv 27 \equiv -1 \pmod{7}.$$

As none of these indices give 1 modulo 7 so the order must be 6 which means that 3 is a primitive root of modulo 7.

We need to find the integers which are relatively prime to $\phi(7)=6$. The only integers below 6 which are relatively prime to 6 are 1 and 5. Therefore

$$3^1 \equiv 3,\ \ 3^5 \equiv 5 \pmod{7}.$$

Hence 3 and 5 are the only incongruent primitive roots of modulo 7.

(b) We are asked to find the primitive roots of modulo 11.

First we find the Euler phi function of 11; $\phi(11)=10$. The only positive factors of 10 are 1, 2, 5 and 10.

Let us see if 2 is a primitive root of modulo 11:

$$2^1 \equiv 2,\ \ 2^2 \equiv 4,\ \ 2^5 \equiv 10 \pmod{11}.$$

Since none of these indices (1, 2 and 5) gives 1 modulo 11 so the order of 2 modulo 11 must be 10. Therefore 2 is a primitive root of modulo 11.

How do we find the other primitive roots of modulo 11?

Use the above Proposition (6.18). In order to use this proposition we need to find which integers are relatively prime to $\phi(11) = 10$. These are

$$1, 3, 7 \text{ and } 9.$$

Taking 2 to these indices gives

$$2^1 \equiv 2,\ 2^3 \equiv 8,\ 2^7 \equiv 7 \text{ and } 2^9 \equiv 6 \pmod{11}.$$

The incongruent primitive roots of modulo 11 are 2, 6, 7 and 8.

(c) We need to find the incongruent primitive roots of 17.

We attack this problem in a similar manner to the previous two.

Evaluating the Euler totient function of 17 gives

$$\phi(17) = 16.$$

The positive factors of 16 are 1, 2, 4, 8 and 16.

Let us first trial the powers of 2 with these indices, 1, 2, 4, 8 and 16:

$$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^4 \equiv 16,\ 2^8 \equiv 1 \pmod{17}$$

The order of 2 modulo 17 is 8 not 16 so 2 is *not* a primitive root of modulo 17.

Next let us trial powers (1, 2, 4 and 8) of 3:

$$3^1 \equiv 3,\ 3^2 \equiv 9,\ 3^4 \equiv 13,\ 3^8 \equiv 16 \pmod{17}.$$

Therefore the order of 3 modulo 17 is 16 which implies that 3 is a primitive root of modulo 17.

We use powers of 3 to find the other primitive roots of 17. We only use the powers which are relatively prime to $\phi(17) = 16$. *Which positive integers below 16 are relatively prime to 16?*

$$1, 3, 5, 7, 9, 11, 13 \text{ and } 15.$$

Evaluating these powers with base 3 gives

$$3^1 \equiv 3,\ 3^3 \equiv 10,\ 3^5 \equiv 5,\ 3^7 \equiv 11,\ 3^9 \equiv 14,\ 3^{11} \equiv 7,$$
$$3^{13} \equiv 12 \text{ and } 3^{15} \equiv 6 \pmod{17}$$

The primitive roots of modulo 17 are 3, 5, 6, 7, 10, 11, 12 and 14.

(d) This time we are asked to find the primitive roots of 23.

We have $\phi(23) = 22$ and the factors of 22 are 1, 2, 11 and 22.

First we see if 2 is a primitive root of 23:

$$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^{11} \equiv 1 \pmod{23}.$$

Therefore 2 *cannot* be a primitive root of modulo 23.

Now we trial 3:

$$3^1 \equiv 3,\ 3^2 \equiv 9,\ 3^{11} \equiv 1 \pmod{23}.$$

Similarly, 3 *cannot* be a primitive root of modulo 23.

Now we trial the next prime, 5:

$$5^1 \equiv 5,\ \ 5^2 \equiv 2,\ \ 5^{11} \equiv 22 \pmod{23}.$$

The order of 5 modulo 23 must be 22 because none of the other factors produce 1 modulo 23. Hence 5 is a primitive root of modulo 23.

We need to find the other primitive roots of modulo 23. These are given by the powers of 5 which are relatively prime to $\phi(23) = 22$. The positive integers ≤ 22 which are relatively prime to 22 are

$$1,\ 3,\ 5,\ 7,\ 9,\ 13,\ 15,\ 17,\ 19 \text{ and } 21.$$

Evaluating these powers with base 5 yields:

$$5^1 \equiv 5,\ \ 5^3 \equiv 10,\ \ 5^5 \equiv 20,\ \ 5^7 \equiv 17,\ \ 5^9 \equiv 11,\ \ 5^{13} \equiv 21,$$
$$5^{15} \equiv 19,\ \ 5^{17} \equiv 15,\ \ 5^{19} \equiv 7 \text{ and } 5^{21} \equiv 14 \pmod{23}$$

The primitive roots of 23 are 5, 7, 10, 11, 14, 15, 17, 19, 20 and 21.

2. (a) We need to solve $x^3 \equiv 1 \pmod{7}$. Since 7 is prime so $\phi(7) = 6$ and $3 \mid 6$ so we have 3 incongruent solutions.

From solution to question 1(a) we know 3 is a primitive root of 7. Evaluating powers of 3 we have

$$3^1 \equiv 3,\ \ 3^2 \equiv 2,\ \ 3^3 \equiv 6,\ \ 3^4 \equiv 4,\ \ 3^5 \equiv 5,\ \ 3^6 \equiv 1 \pmod{7}$$

Creating a table gives

Integer a	1	2	3	4	5	6
$\text{ind}_3(a)$	6	2	1	4	5	3

Applying the rules of indices to $x^3 \equiv 1 \pmod{7}$ converts to linear form:

$$3\ \text{ind}_3(x) \equiv \text{ind}_3(1) \pmod{6}.$$

From the table we have $\text{ind}_3(1) = 6$. Substituting this into the above yields

$$3\ \text{ind}_3(x) \equiv 6 \pmod{6}.$$

The $\gcd(3,\ 6) = 3$. Dividing the above congruence by 3 gives

$$\text{ind}_3(x) \equiv 2 \pmod{2}.$$

Solving this

$$\text{ind}_3(x) \equiv 2,\ \ 4 \text{ and } 6 \pmod{6}$$

Using the above table in the reverse direction we have

$$x \equiv 2,\ 4,\ 1 \pmod 7$$

Our solution in ascending order is $x \equiv 1,\ 2,\ 4 \pmod 7$.

(b) This time we need to solve $x^4 \equiv 1 \pmod{13}$.

The Euler phi function of 13 is 12 because 13 is prime. Moreover as $4 \mid 12$ so we have 4 incongruent solutions to $x^4 \equiv 1 \pmod{13}$.

2 is a primitive root of 13 and we created a table for the indices in Example 19:

a	1	2	3	4	5	6	7	8	9	10	11	12
$\text{ind}_2(a)$	12	1	4	2	9	5	11	3	8	10	7	6

Applying the rules of indices on $x^4 \equiv 1 \pmod{13}$ gives

$$4\ \text{ind}_2(x) \equiv \text{ind}_2(1) \pmod{12}$$
$$4\ \text{ind}_2(x) \equiv 12 \pmod{12} \qquad (*)$$

Evaluating the gcd of 4 and 12 we have $\gcd(4,\ 12) = 4$ and $4 \mid 4$. Dividing the congruence in (*) by 4 gives

$$\text{ind}_2(x) \equiv 3 \pmod 3.$$

Hence we have

$$\text{ind}_2(x) \equiv 3,\ 6,\ 9,\ 12 \pmod{12}.$$

Locating these values in the bottom row of the above table and reading off the corresponding integers in the top row we have

$$x \equiv 8,\ 12,\ 5,\ 1 \pmod{13}.$$

Placing our solutions into ascending order gives $x \equiv 1,\ 5,\ 8,\ 12 \pmod{13}$.

(c) Similarly, we solve $x^{11} \equiv 1 \pmod{23}$. We have $11 \mid \phi(23)$ because $\phi(23) = 22$. Therefore there are exactly 11 *incongruent* solutions to

$$x^{11} \equiv 1 \pmod{23}.$$

In question 1(d) we established that 5 was a primitive root of modulo 23.

By evaluating powers of 5 we get the following table:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\text{ind}_5(a)$	22	2	16	4	1	18	19	6	10	3	9	20	14	21	17	8

a	17	18	19	20	21	22
$\text{ind}_5(a)$	7	12	15	5	13	11

Using the rules of indices on $x^{11} \equiv 1 \pmod{23}$ yields

$$11 \operatorname{ind}_5(x) \equiv \operatorname{ind}_5(1) \pmod{22}$$
$$11 \operatorname{ind}_5(x) \equiv 22 \pmod{22}$$

The $\gcd(11,\ 22) = 11$ and $11 \mid 22$ so dividing the above congruence by 11:

$$\operatorname{ind}_5(x) \equiv 2 \pmod{2}.$$

From this $\operatorname{ind}_5(x) \equiv 2 \pmod{2}$ we have

$$\operatorname{ind}_5(x) \equiv 2,\ 4,\ 6,\ 8,\ 10,\ 12,\ 14,\ 16,\ 18,\ 20,\ 22 \pmod{22}.$$

Again, locating these integers in the bottom row of the above table and reading off the corresponding entries in the first row we have

$$x \equiv 2,\ 4,\ 8,\ 16,\ 9,\ 18,\ 13,\ 3,\ 6,\ 12,\ 1 \pmod{23}.$$

Writing this in ascending order gives

$$x \equiv 1,\ 2,\ 3,\ 4,\ 6,\ 8,\ 9,\ 12,\ 13,\ 16 \text{ and } 18 \pmod{23}.$$

3. We need to solve $x^d - 1 \equiv 0 \pmod{19}$ for each d which is a factor of $\phi(19)$.

$$\phi(19) = 18 \quad [\text{Because } 19 \text{ is prime}]$$

The positive factors d of 18 are 1, 2, 3, 6, 9 and 18.

By evaluating powers of 2 we obtain the following table:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\operatorname{ind}_2(a)$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

Hence 2 is a primitive root of 19.

For $d = 1$:

In this case we have a unique solution $x \equiv 1 \pmod{19}$.

For $d = 2$:

In this case we have *two incongruent* solutions. Substituting $d = 2$ into the given congruence yields

$$x^2 \equiv 1 \pmod{19}.$$

Applying Lemma (4.3):

$$x^2 \equiv 1 \pmod{p} \iff x \equiv \pm 1 \pmod{p}$$

To $x^2 \equiv 1 \pmod{19}$ gives

$$x \equiv \pm 1 \equiv 1,\ 18 \pmod{19}$$

Our two incongruent solutions to $x^2 \equiv 1 \pmod{19}$ are $x \equiv 1,\ 18 \pmod{19}$.

For $d = 3$:

In this case we have *three incongruent* solutions. Substituting $d = 3$ into the given congruence yields

$$x^3 \equiv 1 \pmod{19}.$$

Applying the rules of indices we have

$$3 \operatorname{ind}_2(x) \equiv \operatorname{ind}_2(1) \pmod{18}$$
$$3 \operatorname{ind}_2(x) \equiv 18 \pmod{18}$$

Dividing the last congruence by 3 gives

$$\operatorname{ind}_2(x) \equiv 6 \pmod{6}$$

Hence

$$\operatorname{ind}_2(x) \equiv 6,\ 12,\ 18 \pmod{18}$$

Using the above table we have

$$x \equiv 7,\ 11,\ 1 \pmod{19}$$

Our three incongruent solutions to $x^3 \equiv 1 \pmod{19}$ are $x \equiv 1,\ 7,\ 11 \pmod{19}$.

For $d = 6$ and $d = 9$:

Carbon copying the above arguments we have the following results:

$$x^6 \equiv 1 \pmod{19} \text{ implies } x \equiv 1,\ 7,\ 8,\ 11,\ 12,\ 18 \pmod{19}$$

$$x^9 \equiv 1 \pmod{19} \text{ implies } x \equiv 1,\ 4,\ 5,\ 6,\ 7,\ 9,\ 11,\ 16,\ 17 \pmod{19}$$

For $d = 18$ we have the 18 least positive residues of modulo 19:

$$x^{18} \equiv 1 \pmod{19} \text{ implies}$$

$$x \equiv 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18 \pmod{19}$$

When $d = 18 = \phi(19)$ so we have the converse of *FLT*; that is all the solutions $x \pmod{19}$ such that $19 \nmid x$.

4. We are required to prove that if d is even then $p-1$ is a solution to $x^d - 1 \equiv 0 \pmod{p}$ where p is prime.

Proof.

We are given that d is even, so let $d = 2m$ where m is an integer. Note that

$$p-1 \equiv -1 \pmod{p}.$$

Therefore using this we have

$$x^d \equiv x^{2m} \equiv (-1)^{2m} \equiv 1 \pmod{p}$$

Hence the integer $p-1$ satisfies $x^d - 1 \equiv 0 \pmod{p}$ so it is a solution.

This completes our proof.

■

5. (a) We are asked to find $x \equiv 1+2+2^2+2^3+2^4+2^5 \pmod{7}$. The powers of 2 modulo 7 are given by

$$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 1,\ 2^4 \equiv 2,\ 2^5 \equiv 4 \pmod{7}.$$

Therefore

$$x \equiv 1+2+4+1+2+4 \equiv 0 \pmod{7}.$$

(b) We need to find $x \equiv 1+3+3^2+3^3+3^4+3^5 \pmod{7}$.

We have evaluated the powers of 3 in question 2(a):

$$3^1 \equiv 3,\ 3^2 \equiv 2,\ 3^3 \equiv 6,\ 3^4 \equiv 4,\ 3^5 \equiv 5,\ 3^6 \equiv 1 \pmod{7}.$$

Substituting these into the above gives

$$\begin{aligned} x &\equiv 1+3+3^2+3^3+3^4+3^5 \\ &\equiv 1+3+2+6+4+5 \equiv 21 \equiv 0 \pmod{7} \end{aligned}$$

(c) We need to find $x \equiv 1+3+3^2+3^3+3^4+3^5+3^6+3^7+3^8+3^9 \pmod{11}$.

The powers of 3 modulo 11 are

$$3^1 \equiv 3,\ 3^2 \equiv 9,\ 3^3 \equiv 5,\ 3^4 \equiv 4,\ 3^5 \equiv 1,\ 3^6 \equiv 3,\ 3^7 \equiv 9,\ 3^8 \equiv 5,\ 3^9 \equiv 4 \pmod{11}.$$

Substituting these into the given congruence yields

$$\begin{aligned} x &\equiv 1+3+3^2+3^3+3^4+3^5+3^6+3^7+3^8+3^9 \\ &\equiv 1+3+9+5+4+1+3+9+5+4 \\ &\equiv 0 \pmod{11} \end{aligned}$$

(d) This time we need to find the least non-negative residue x in

$$x \equiv 1+2+2^2+2^3+2^4+2^5+2^6+2^7+2^8+2^9+2^{10}+2^{11} \pmod{13}.$$

We evaluated the powers of 2 modulo 13 in Example 19:

$$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^4 \equiv 3,\ 2^5 \equiv 6,\ 2^6 \equiv 12,$$
$$2^7 \equiv 11,\ 2^8 \equiv 9,\ 2^9 \equiv 5,\ 2^{10} \equiv 10,\ 2^{11} \equiv 7,\ 2^{12} \equiv 1 \pmod{13}$$

Substituting these into the above congruence gives

$$\begin{aligned} x &\equiv 1+2+2^2+2^3+2^4+2^5+2^6+2^7+2^8+2^9+2^{10}+2^{11} \pmod{13} \\ &\equiv 1+2+4+8+3+6+12+11+9+5+10+7 \\ &\equiv 78 \equiv 0 \pmod{13} \end{aligned}$$

In all our answers we have zero modulo prime.

6. We are required to prove if $p \nmid r$ and $r \not\equiv 1 \pmod{p}$ then

$$1+r+r^2+\cdots+r^{p-3}+r^{p-2} \equiv 0 \pmod{p}$$

where p is an odd prime.

Proof.

We are given that $p \nmid r$ so by Fermat's Little Theorem (*FlT*) we have

$$r^{p-1} \equiv 1 \pmod{p} \quad \Leftrightarrow \quad r^{p-1}-1 \equiv 0 \pmod{p}.$$

We can factorize $r^{p-1}-1$ as

$$r^{p-1}-1 = (r-1)(r^{p-2}+r^{p-3}+\cdots+r+1).$$

Substituting this into $r^{p-1}-1 \equiv 0 \pmod{p}$ gives

$$r^{p-1}-1 \equiv (r-1)(r^{p-2}+r^{p-3}+\cdots+r+1) \equiv 0 \pmod{p} \qquad (\ddagger)$$

By Proposition (3.14) (a):

> If $a \times b \equiv 0 \pmod{p}$ where p is prime then $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.

Applying this proposition to (‡) gives

$$r-1 \equiv 0 \pmod{p} \text{ or } r^{p-2}+r^{p-3}+\cdots+r+1 \equiv 0 \pmod{p}.$$

We are given that $r \not\equiv 1 \pmod{p}$. Therefore we must have

$$r^{p-2}+r^{p-3}+\cdots+r+1 \equiv 0 \pmod{p}.$$

This completes our proof. ∎

The second part requires us to evaluate

$$1+r+r^2+\cdots+r^{p-3}+r^{p-2} \equiv x \pmod{p} \text{ provided } r \equiv 1 \pmod{p}$$

If $r \equiv 1 \pmod{p}$ then $r^m \equiv 1 \pmod{p}$ so

$$\begin{aligned} 1+r+r^2+\cdots+r^{p-3}+r^{p-2} &\equiv 1+\underbrace{1+\cdots+1+1}_{=p-2} \\ &\equiv 1+p-2 \\ &\equiv p-1 \pmod{p} \end{aligned}$$

∎

7. We are asked to prove Proposition (6.18) which is given by:

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

Proof.

We are given that r is a primitive root of modulo p so the order of r modulo p is $\phi(p) = p-1$.

Since we are given that $\gcd(m, \quad p-1) = 1$ so by Corollary (6.9):

> Let a modulo n have order k, then a^s has order $k \quad \Leftrightarrow \quad \gcd(s, \ k) = 1$.

We have the order of r^m is also $\phi(p) = p-1$. Hence r^m is a primitive root of modulo p. This completes our proof.

■

8. We need to show that $r_1 \times r_2$ is *not* necessarily a primitive root modulo p.

Only need to produce a counter example.

From Example 24 we have 2, 3, 10, 13, 14 and 15 are primitive roots modulo 19.

Let $r_1 = 2$ and $r_2 = 3$ then $r_1 \times r_2 = 2 \times 3 = 6$ but 6 is *not* a primitive root modulo 19.

9. We are asked to find the order of negative residues modulo 19.

The Euler phi function of 19 is $\phi(19) = 18$.

(a) We need to find the order of $-2 \pmod{19}$.

We are given that 2 is a primitive root modulo 19. Therefore

$$2^{18} \equiv 1 \pmod{19}.$$

Rewriting the index 18 we have

$$\left(2^9\right)^2 \equiv 1 \pmod{19}.$$

By Lemma (4.3):

$$x^2 \equiv 1 \pmod{p} \quad \Leftrightarrow \quad x \equiv \pm 1 \pmod{p}$$

Applying this result to $\left(2^9\right)^2 \equiv 1 \pmod{19}$ gives

$$2^9 \equiv 1 \pmod{19} \text{ or } 2^9 \equiv -1 \pmod{19}.$$

We *cannot* have $2^9 \equiv 1 \pmod{19}$. *Why not?*

Because 2 is a primitive root of 19. Hence we have

$$2^9 \equiv -1 \pmod{19}$$

Multiplying both sides of this by -1 yields

$$(-1)2^9 \equiv (-2)^9 \equiv 1 \pmod{19}$$

Hence the order of $-2 \pmod{19}$ is 9.

(b) We evaluate the order of $-3 \pmod{19}$ along similar lines of part (a).

Since 3 is a primitive root of 19 so

$$3^{18} \equiv 1 \pmod{19}.$$

We have

$$(3^9)^2 \equiv 1 \pmod{19}.$$

Again, using Lemma (4.3) given above:

$$3^9 \equiv 1 \pmod{19} \quad \text{or} \quad 3^9 \equiv -1 \pmod{19}.$$

Clearly, we cannot have $3^9 \equiv 1 \pmod{19}$ because 3 is a primitive root modulo 19. Therefore, we must have $3^9 \equiv -1 \pmod{19}$. Multiplying this by -1 gives

$$(-3)^9 \equiv (-1) \times (-1) \equiv 1 \pmod{19}.$$

The order of $-3 \pmod{19}$ is 9.

(c), (d), (e) and (f). The order is evaluated similar to parts (a) and (b) and the order in each case is 9.

10. We are asked to prove $-r$ has order $\dfrac{p-1}{2}$ given that r is a primitive root and prime $p \equiv 3 \pmod{4}$.

Proof.

Since r is a primitive root of p so

$$r^{p-1} \equiv 1 \pmod{p}.$$

We have

$$\left(r^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod{19}.$$

Applying Lemma (4.3) to this congruence:

$$x^2 \equiv 1 \pmod{p} \;\Leftrightarrow\; x \equiv \pm 1 \pmod{p}$$

gives

$$r^{\frac{p-1}{2}} \equiv 1 \pmod{p} \quad \text{or} \quad r^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Clearly we cannot have $r^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ because r is a primitive root modulo p. Therefore we must have $r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Multiplying this by -1 gives

$$(-1)r^{\frac{p-1}{2}} \equiv -1 \times (-1) \equiv 1 \pmod{p} \qquad (\ddagger)$$

We are given that $p \equiv 3 \pmod{4}$ so

$$p - 3 = 4k \;\Rightarrow\; p - 1 = 2 + 4k \;\Rightarrow\; \frac{p-1}{2} = 1 + 2k.$$

Hence the index $\frac{p-1}{2} = 1 + 2k$ in $(\ddagger)$ is odd so we can write $-1 = (-1)^{\frac{p-1}{2}}$.

Rewriting the congruence in $(\ddagger)$ as

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

We have $(-r)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ and need to show this index $\frac{p-1}{2}$ is the order of $-r$.

Suppose the order of $-r$ is m where $m < \frac{p-1}{2}$. We have

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

By Proposition (6.4):

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

Applying this proposition to $(-r)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ gives $m \mid \frac{p-1}{2}$.

Squaring the index in (*) yields

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

Rewriting $-r = -1 \times r$ into the above congruence gives

$$(-r)^{2m} \equiv (-1 \times r)^{2m} \equiv (-1)^{2m} r^{2m} = r^{2m} \equiv 1 \pmod{p}.$$

In the above we have $m < \frac{p-1}{2}$ which implies $2m < p-1$. We have a contradiction because the order of r is $p-1$ but in the above we have

$$r^{2m} \equiv 1 \pmod{p} \text{ where } 2m < p-1.$$

Our supposition that the order of $-r$ is m where $m < \dfrac{p-1}{2}$ must be wrong.

Hence the order of $-r$ is $\dfrac{p-1}{2}$. This completes our proof.

■

11. You need to notice that in each case we have a primitive root. Observe that

$-3 \equiv 14 \pmod{17}$, $-5 \equiv 12 \pmod{17}$, $-6 \equiv 11 \pmod{17}$,

$-7 \equiv 10 \pmod{17}$, $-10 \equiv 7 \pmod{17}$, $-11 \equiv 6 \pmod{17}$,

$-12 \equiv 5 \pmod{17}$ and $-14 \equiv 3 \pmod{17}$.

We are given that 3, 5, 6, 7, 10, 11, 12 and 14 are primitive roots modulo 19 therefore -3, -5, -6, -7, -10, -11, -12 and -14 are also the same primitive roots modulo 17 but in a *different* order.

The order of -3, -5, -6, -7, -10, -11, -12 and -14 modulo 17 is

$$\phi(17) = 16.$$

12. We need to prove that that $-r$ is also a primitive root modulo p given that r is a primitive root modulo p where $p \equiv 1 \pmod{4}$.

Proof.

We use proof by contradiction.

Suppose $-r$ is *not* a primitive root modulo p but r is. Then

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

where $m \mid (p-1)$ but $m < p-1$.

We consider two cases of m.

Case I m is even

If m is even, $m = 2k$, then substituting this into (*) yields

$$\begin{aligned}(-r)^m &= (-r)^{2k} = (-1 \times r)^{2k} \\ &= (-1)^{2k} \times r^{2k} = r^{2k} \equiv 1 \pmod{p}\end{aligned}$$

This is impossible because r is a primitive root modulo p so it has order $p-1$ not $m = 2k < p-1$. Therefore m cannot be even.

Case II m is odd

Let m be odd. We are given that $p \equiv 1 \pmod 4$ so for some integer n we have

$$p - 1 = 4n\,.$$

Combining these two results, $m \mid (p-1)$ and $p - 1 = 4n$, we have

$$m \mid 4n\,.$$

In this case we are considering m to be odd, therefore $\gcd(m,\ 4) = 1$ and so by Euclid's Lemma (1.13):

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

We have $m \mid n$. Since m and n are positive integers so $m \le n$.

Additionally we have $2m \mid 4n$ where $2m < 4n$ because $2 < 4$.

Squaring the congruence in (*) gives

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

Rewriting this index $-r$ in this congruence

$$(-r)^{2m} = (-1 \times r)^{2m} = (-1)^{2m} \times r^{2m} = r^{2m} \equiv 1 \pmod p$$

This is also impossible because $2m < 4n$ and $4n$ is the order of r modulo p.

Hence we cannot have an odd m.

Since m cannot be even or odd so such a m does not exist. Therefore the order of $-r$ is $p-1$ which means that $-r$ is a primitive root modulo p.

This completes our proof.

■

13. We are asked to find $x \equiv 2 \times 3 \times 10 \times 13 \times 14 \times 15 \pmod{19}$:

$$x \equiv 2 \times 3 \times 10 \times 13 \times 14 \times 15 \equiv 163800 \equiv 1 \pmod{19}.$$

14. We are asked to prove that the multiplicative inverse of $r \pmod p$ is *also* a primitive root of modulo p.

Proof.

We are given that r is a primitive root of modulo p therefore the $\gcd\left(r, \quad p\right) = 1$ which implies that the inverse of $r\left(\text{mod } p\right)$ exists.

Let $t\left(\text{mod } p\right)$ be the inverse of $r\left(\text{mod } p\right)$. Then

$$rt \equiv 1\left(\text{mod } p\right) \qquad (*)$$

Suppose the order of $t\left(\text{mod } p\right)$ is n where $n < p-1$. From this we have

$$t^n \equiv 1\left(\text{mod } p\right).$$

Taking the congruence in (*) to the index n:

$$\left(rt\right)^n \equiv r^n t^n \equiv 1^n \equiv 1\left(\text{mod } p\right).$$

Substituting the previous congruence $t^n \equiv 1\left(\text{mod } p\right)$ into this last congruence gives

$$r^n \times t^n \equiv r^n \times 1 \equiv r^n \equiv 1\left(\text{mod } p\right).$$

This $r^n \equiv 1\left(\text{mod } p\right)$ is impossible because we are given that r is a primitive root of p so the order of r is $p-1$ but in the above we have $r^n \equiv 1\left(\text{mod } p\right)$ where $n < p-1$.

Therefore our supposition the order of $t\left(\text{mod } p\right)$ is n where $n < p-1$ is wrong and the order of $t\left(\text{mod } p\right)$ is $p-1$ which means that t is a primitive root of modulo p. This completes our proof.

■

15. We are required to prove that the product of all the *incongruent* primitive roots of a prime p are congruent to $1\left(\text{mod } p\right)$. *How do we prove this result?*

By using the statement of the previous question.

Proof.

If the prime, $p = 2$ then the only primitive root of 2 is 1 and

$$1 \equiv 1\left(\text{mod } p\right).$$

We have our given result.

Now let p be an odd prime. By the Primitive Root Theorem (6.22):

> Every prime p has a primitive root and there are $\phi\left(p-1\right)$ primitive roots of p.

There are $\phi\left(p-1\right)$ primitive roots of p. By Proposition (5.10):

> For $n > 2$, $\phi\left(n\right)$ is an even integer.

Therefore p has an even number of primitive roots. Let these be

$$r_1,\ r_2,\ \cdots,\ r_n,\ \cdots,\ r_{2n}.$$

where the multiplicative inverse of $r_j \pmod p$ is $r_{2j} \pmod p$ in this list because by the previous question the inverse of $r_j \pmod p$ is also a primitive root. For each j from 1 to n we have

$$r_j \times r_{2j} \equiv 1 \pmod p.$$

Therefore the product

$$r_1 \times r_2 \times \cdots \times r_n \times \cdots \times r_{2n} \equiv 1 \pmod p.$$

Thus we have our required result. ■

16. (i) First the Fermat prime $F_3 = 2^{2^3} + 1 = 257$ and we are told it is prime. Therefore $\phi(257) = 256$ and the positive divisors of 256 are

$$\{1, 2, 4, 8, 16, 32, 64, 128, 256\}.$$

We need to evaluate each of these as an index to the base 3. Clearly the first three indices are not going to give 1 modulo 257 and the last index, 256, will definitely give 1 modulo 257 because of Euler's Theorem. Checking the remaining indices gives

$$3^8 \equiv 6561 \equiv 136 \not\equiv 1 \pmod{257}$$

$$3^{16} \equiv \left(3^8\right)^2 \equiv 136^2 \equiv 18\,496 \equiv 249 \equiv -8 \not\equiv 1 \pmod{257}$$

$$3^{32} \equiv \left(3^{16}\right)^2 \equiv (-8)^2 \equiv 64 \not\equiv 1 \pmod{257}$$

$$3^{64} \equiv \left(3^{16}\right)^4 \equiv (-8)^4 \equiv 4096 \equiv 241 \equiv -16 \not\equiv 1 \pmod{257} \qquad (\dagger)$$

$$3^{128} \equiv \left(3^{64}\right)^2 \equiv (-16)^2 \equiv 256 \equiv -1 \not\equiv 1 \pmod{257} \qquad (\ddagger)$$

Hence 3 is a primitive root of modulo $F_3 = 257$.

(ii) We need to solve the quadratic $x^2 \equiv -1 \pmod{257}$. Using indices to the base 3 gives

$$2 \operatorname{ind}_3(x) \equiv \operatorname{ind}_3(-1) \pmod{256}.$$

Using (‡) from part (i) we have $\operatorname{ind}_3(-1) = 128$. Substituting this yields

$$2\,\mathrm{ind}_3\left(x\right) \equiv 128 \left(\mathrm{mod}\ 256\right) \qquad (*)$$

The $\gcd\left(2,\ \ 256\right) = 2$ and $2 \mid 128$ so we have two incongruent solutions of the given quadratic. Dividing both sides by 2 of (*) gives

$$\mathrm{ind}_3\left(x\right) \equiv 64 \left(\mathrm{mod}\ 128\right) \ \Rightarrow\ \mathrm{ind}_3\left(x\right) = 64,\ \ 64 + 128 = 64,\ \ 192$$

Hence the solutions are given by

$$x \equiv 3^{64},\ \ 3^{192} \left(\mathrm{mod}\ 257\right)$$

The first of these was evaluated (†) in part (i). One solution is

$$3^{64} \equiv 241 \left(\mathrm{mod}\ 257\right)$$

By Proposition (3.14) (b) we have

$$a^2 \equiv b^2 \left(\mathrm{mod}\ p\right) \ \Leftrightarrow\ a \equiv \pm b \left(\mathrm{mod}\ p\right)$$

The other solution of $x^2 \equiv -1 \left(\mathrm{mod}\ 257\right)$ is given by $x \equiv -241 \equiv 16 \left(\mathrm{mod}\ 257\right)$.

Our solutions to the quadratic are $x \equiv 16,\ \ 241 \left(\mathrm{mod}\ 257\right)$.

17. (i) We need to show that 2 is a primitive root of 243. First note that $243 = 3^5$. Therefore we need to show that the order of 2 modulo 243 is equal to

$$\phi\left(243\right) = \phi\left(3^5\right) = 3^5 - 3^4 = 162\,.$$

The positive divisors of 162 are $\{1,\ 2,\ 3,\ 6,\ 9,\ 18,\ 27,\ 54,\ 81,\ 162\}$. Clearly the indices 1, 2, 3, 6 of base 2 are *not* going to work. We try the next index:

$$2^9 \equiv 512 \equiv 26 \not\equiv 1 \left(\mathrm{mod}\ 243\right) \qquad (‡)$$

Using this to evaluate the next index 18 gives

$$2^{18} \equiv \left(2^9\right)^2 \equiv 26^2 \equiv 676 \equiv 190 \not\equiv 1 \left(\mathrm{mod}\ 243\right).$$

Again using the result obtained in (‡) to find the remaining indices (apart from the last one which we know is going to give us 1 modulo 243 because of Euler's Theorem):

$$2^{27} \equiv \left(2^9\right)^3 \equiv 26^3 \equiv 17\ 576 \equiv 80 \not\equiv 1 \left(\mathrm{mod}\ 243\right) \qquad (†)$$

$$2^{54} \equiv \left(2^{27}\right)^2 \equiv 80^2 \equiv 82 \not\equiv 1 \left(\mathrm{mod}\ 243\right) \qquad (*)$$

$$2^{81} \equiv \left(2^{27}\right)^3 \equiv 80^3 \equiv 512\,000 \equiv 242 \not\equiv 1 \left(\mathrm{mod}\ 243\right)$$

Therefore the order of 2 modulo 243 is $\phi\left(243\right) = 162$ which implies that it is a primitive root of modulo 243.

(ii) We are asked to solve the quadratic $x^2 \equiv 82 \left(\mathrm{mod}\ 243\right)$. Using the rules of indices with respect to the base 2 we have

$$2\ \mathrm{ind}_2\left(x\right) \equiv \mathrm{ind}_2\left(82\right) \left(\mathrm{mod}\ 162\right)$$

From (*) in part (i) we have $\mathrm{ind}_2\left(82\right) = 54$, substituting this into the above

$$2\ \mathrm{ind}_2\left(x\right) \equiv 54 \left(\mathrm{mod}\ 162\right)$$

We have 2 *incongruent* solutions because the $\gcd\left(2,\ \ 162\right) = 2$ and $2 \mid 54$;

$$2\ \mathrm{ind}_2\left(x\right) \equiv 54 \left(\mathrm{mod}\ 162\right) \underbrace{\Rightarrow}_{\text{simplifying}} \mathrm{ind}_2\left(x\right) \equiv 27 \left(\mathrm{mod}\ 81\right)$$

$$\Rightarrow \quad \mathrm{ind}_2\left(x\right) \equiv 27,\ \ 27 + 81 \equiv 27,\ \ 108 \left(\mathrm{mod}\ 162\right)$$

From the last line $\mathrm{ind}_2\left(x\right) \equiv 27,\ \ 108 \left(\mathrm{mod}\ 162\right)$ we deduce that

$$x \equiv 2^{27},\ \ 2^{108} \left(\mathrm{mod}\ 243\right)$$

From (†) we have the first value of x that is $x \equiv 2^{27} \equiv 80 \left(\mathrm{mod}\ 243\right)$. Since we are given a quadratic equation $x^2 \equiv 82 \left(\mathrm{mod}\ 243\right)$ so the other solution is

$$x \equiv -80 \equiv 163 \left(\mathrm{mod}\ 243\right).$$

Our solutions to the given quadratic $x^2 \equiv 82 \left(\mathrm{mod}\ 243\right)$ are

$$x \equiv 80, 163 \left(\mathrm{mod}\ 243\right).$$

18. We need to prove that if $d \mid \left(p-1\right)$ and $p \nmid x$ then

$$x^d - 1 \equiv 0 \left(\mathrm{mod}\ p\right) \text{ where } p \text{ is prime}$$

has exactly d incongruent solutions.

Proof.

We are given that $d \mid \left(p-1\right)$ so there is an integer m such that

$$dm = p - 1$$

From the given congruence $x^d - 1 \equiv 0 \pmod{p}$ we have

$$x^d \equiv 1 \pmod{p}.$$

Taking this $x^d \equiv 1 \pmod{p}$ to the power of m gives

$$\left(x^d\right)^m \equiv x^{dm} \equiv x^{p-1} \equiv 1 \pmod{p} \qquad (*)$$

All the members of the reduced residue system modulo p satisfy the congruence (*). This implies that this congruence (*) has exactly $p-1$ incongruent solutions because there are $p-1$ members which belong to the reduced residue system modulo p namely $\{1,\ 2,\ 3, \cdots,\ p-1\}$. Factorizing this congruence by using the well-known identity:

$$a^{rs} - 1 = \left(a^r - 1\right)\left(a^{r(s-1)} + a^{r(s-2)} + \cdots + a + 1\right)$$

gives

$$x^{dm} - 1 = \left(x^d - 1\right)\left(x^{d(m-1)} + x^{d(m-2)} + \cdots + x + 1\right) \equiv 0 \pmod{p} \qquad (\ddagger)$$

So this congruence has exactly $p-1$ incongruent solutions.

By Proposition (3.14) (a):

$$a \times b \equiv 0 \pmod{p} \text{ implies } a \equiv 0 \pmod{p} \text{ or } b \equiv 0 \pmod{p}$$

Applying this to (‡) gives

$$\left(x^d - 1\right) \equiv 0 \pmod{p} \quad \text{or} \quad \left(x^{d(m-1)} + x^{d(m-2)} + \cdots + x + 1\right) \equiv 0 \pmod{p}.$$

By the given result of Lagrange we have that the second bracket on the right hand side $\left(x^{d(m-1)} + x^{d(m-2)} + \cdots + x + 1\right) \equiv 0 \pmod{p}$ has at most $d(m-1)$ incongruent solutions. The total number of incongruent solutions of (‡) is $p-1$ therefore

$$x^{dm} - 1 = \underbrace{\left(x^d - 1\right)}_{\text{Let } s \text{ be the least number of solutions}} \underbrace{\left(x^{d(m-1)} + x^{d(m-2)} + \cdots + x + 1\right)}_{\leq d(m-1) \text{ solutions}} \equiv 0 \pmod{p}.$$

We have

$$s + d(m-1) = p - 1 = dm$$

$$s = dm - d(m-1) = dm - dm + d = d$$

The least number of solutions of $\left(x^d - 1\right) \equiv 0 \pmod{p}$ is $s = d$. Applying Lagrange's result to $\left(x^d - 1\right) \equiv 0 \pmod{p}$ gives that the number of incongruent solutions of this congruence must be less than or equal to d.

Hence $\left(x^d - 1\right) \equiv 0 \left(\text{mod } p\right)$ has exactly d incongruent solutions.

This completes our proof.

■

19. We need to show the converse of Fermat's Little Theorem:

$$\text{If } a^{p-1} \equiv 1 \left(\text{mod } p\right) \text{ then } p \nmid a \,.$$

Proof.

We are given that p is prime so by Primitive Root Theorem (6.22):

> Every prime p has a primitive root.

Let r be a primitive root of p. Taking the indices to the base r of

$$a^{p-1} \equiv 1 \left(\text{mod } p\right).$$

gives $\text{ind}_r \left(a^{p-1}\right) \equiv \text{ind}_r \left(1\right) \left(\text{mod } p-1\right)$. Using the rules yields

$$\left(p-1\right) \text{ind}_r \left(a\right) \equiv \text{ind}_r \left(1\right) \left(\text{mod } p-1\right).$$

Clearly $r^0 \equiv 1 \left(\text{mod } p\right)$ so $\text{ind}_r \left(1\right) = 0$. Substituting this into the above

$$\left(p-1\right) \text{ind}_r \left(a\right) \equiv 0 \left(\text{mod } p-1\right).$$

The $\gcd\left(p-1, \quad p-1\right) = p-1$ and $\left(p-1\right) \mid 0$ because $\left(p-1\right) \times 0 = 0$. Hence, we have $p-1$ incongruent solutions and dividing by $p-1$ gives

$$\text{ind}_r \left(a\right) \equiv 0 \left(\text{mod } 1\right).$$

Therefore $\text{ind}_r \left(a\right) = 1, 2, 3, 4, \cdots, p-1$ which is the reduced residue system modulo p.

Therefore $a \equiv r^0, \; r^1, r^2, \cdots, r^{p-1}$. Since r is in the reduced residue system so r^m is also in the reduced residue system modulo p by Proposition (6.11). This completes our proof.

■

20. We are asked to prove Wilson's Theorem by using primitive roots:

If p is prime then $\left(p-1\right)! \equiv -1 \left(\text{mod } p\right)$.

Proof.

Let p be prime so it has a primitive root r because by the Primitive Root (6.22):

> Every prime p has a primitive root and there are $\phi\left(p-1\right)$ incongruent primitive roots.

By Proposition (6.11):

If r is a primitive root of n, then

$$r,\ r^2,\ r^3,\ \cdots,\ r^{\phi(n)}$$

are congruent modulo n to $r_1,\ r_2,\ r_3,\ \cdots,\ r_{\phi(n)}$ in some order.

These r_j's where $1 \le j \le \phi(n)$ are members of the reduced residue system modulo n. In our case we have $n = p$ where p is prime so the reduced residue system of p are integers $\{1, 2, 3, \cdots, p-1\}$ modulo p. Recall that $\phi(p) = p - 1$.

Therefore, we have

$$r \times r^2 \times r^3 \times \cdots \times r^{p-1} \equiv 1 \times 2 \times 3 \times \cdots \times (p-1) \equiv (p-1)! \pmod{p}.$$

On the left – hand side we use the rules of indices and the following result:

$$1 + 2 + 3 + \cdots + m = \frac{1}{2} m(m+1).$$

Hence, we have

$$\begin{aligned} r \times r^2 \times r^3 \times \cdots \times r^{p-1} &\equiv r^{1+2+3+\cdots+(p-1)} \\ &\equiv r^{\frac{1}{2}p(p-1)} \\ &\equiv \left(r^p\right)^{\frac{1}{2}(p-1)} \equiv (p-1)! \pmod{p} \qquad (*) \end{aligned}$$

Applying Corollary (4.2):

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

Gives $r^p \equiv r \pmod{p}$. Substituting this into (*) yields

$$\left(r^p\right)^{\frac{1}{2}(p-1)} \equiv r^{\frac{1}{2}(p-1)} \equiv (p-1)! \pmod{p} \qquad (\ddagger)$$

By *FlT* (4.1) we have $r^{p-1} \equiv 1 \pmod{p}$. Therefore

$$r^{p-1} \equiv \left(r^{\frac{1}{2}(p-1)}\right)^2 \equiv 1 \pmod{p}.$$

By Lemma (4.3):

$$x^2 \equiv 1 \pmod{p} \quad \Leftrightarrow \quad x \equiv \pm 1 \pmod{p}$$

Applying this on $\left(r^{\frac{1}{2}(p-1)}\right)^2 \equiv 1 \pmod{p}$ gives

$$r^{\frac{1}{2}(p-1)} \equiv \pm 1 \pmod{p}.$$

However, as r is a primitive root of p so $r^{\frac{1}{2}(p-1)} \not\equiv 1 \pmod{p}$ which implies

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

Substituting this into (‡) gives

$$(p-1)! \equiv r^{\frac{1}{2}(p-1)} \equiv -1 \pmod{p}.$$

This completes our proof.

■

21. We need to solve $x^6 = 1 + 13y$ which is equivalent to $x^6 \equiv 1 \pmod{13}$. By Example 19 we have that 2 is a primitive root of modulo 13. So, taking ind_2 of both sides of this congruence gives

$$\begin{aligned} \text{ind}_2\left(x^6\right) &\equiv \text{ind}_2\left(1\right) \pmod{12} \\ 6 \times \text{ind}_2\left(x\right) &\equiv \text{ind}_2\left(1\right) \pmod{12} \qquad \left[\text{Linear Form}\right] \end{aligned}$$

Since 2 is a primitive root of 13 so $\text{ind}_2\left(1\right) = \phi\left(13\right) = 13 - 1 = 12$. Putting this into the above yields

$$6 \times \text{ind}_2\left(x\right) \equiv 12 \pmod{12} \qquad (*)$$

The $\gcd\left(6,\ 12\right) = 6$ and $6 \mid 12$ so we have 6 incongruent solutions. Dividing (*) by 6 gives

$$\text{ind}_2\left(x\right) \equiv 2 \equiv 0 \pmod{2}.$$

Hence $\text{ind}_2\left(x\right) \equiv 2 \equiv 0 \pmod{2}$ which means that we have an even integer;

$$\begin{aligned} \text{ind}_2\left(x\right) &\equiv 2,\ 4,\ 6,\ 8,\ 10,\ 12 \pmod{12} \\ x &\equiv 2^2,\ 2^4,\ 2^6,\ 2^8,\ 2^{10},\ 2^{12} \pmod{13} \\ &\equiv 4,\ 3,\ 12,\ 9,\ 10,\ 1 \pmod{13} \end{aligned}$$

Our solutions are $x \equiv 1,\ 3,\ 4,\ 9,\ 10,\ 12 \pmod{13}$.

Finding the y values for these x by transposing $x^6 = 1 + 13y$ to

$$y = \frac{x^6 - 1}{13} \qquad (**)$$

Substituting $x = 1,\ 3,\ 4,\ 9,\ 10,\ 12$ into (**) yields

$$y = \frac{1^6 - 1}{13} = 0,\ \frac{3^6 - 1}{13} = 56,\ \frac{4^6 - 1}{13} = 315,\ \frac{9^6 - 1}{13} = 40\ 880,$$
$$\frac{10^6 - 1}{13} = 76\ 923,\ \frac{12^6 - 1}{13} = 229\ 691$$

Our solutions are

$$\{x=1,\, y=0\},\ \{x=3,\, y=56\},\ \{x=4,\ y=315\},\ \{x=9,\, y=40\ 880\},$$
$$\{x=10,\, y=76\ 923\},\ \{x=12,\ y=229\ 691\}$$

22. (a) We use Proposition (6.18) to find all the primitive roots of 61:

> Let r be a primitive root modulo p where p is prime. Then $r^m \pmod p$ is also a primitive root modulo p provided $\gcd(m,\ p-1)=1$.

We are given that 2 is a primitive root of 61. Let $r=2$ and m be an integer which is relatively prime to $\phi(61)=61-1=60$. *How many of these integers are there?*

$\phi(60)=12$ and these 12 integers are

$$m\in\{1,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47,\ 49,\ 53,\ 59\}$$

Evaluating 2^m for each of these integer values we have

$$2^1\equiv 2\pmod{61}$$
$$2^7\equiv 128\equiv 6\pmod{61}$$
$$2^{11}\equiv 6\times 16\equiv 96\equiv 35\pmod{61}$$
$$2^{13}\equiv 35\times 4\equiv 140\equiv 18\pmod{61}$$
$$2^{17}\equiv 18\times 16\equiv 288\equiv 44\pmod{61}$$
$$2^{19}\equiv 4\times 44\equiv 176\equiv 54\pmod{61}$$
$$2^{23}\equiv 54\times 16\equiv 864\equiv 10\pmod{61}$$
$$2^{29}\equiv 10\times 2^6\equiv 10\times 64\equiv 10\times 3\equiv 30\pmod{61}$$
$$2^{31}\equiv 4\times 30\equiv 120\equiv 59\pmod{61}$$
$$2^{37}\equiv 2^6\times 59\equiv 64\times(-2)\equiv -6\equiv 55\pmod{61}$$
$$2^{41}\equiv 2^4\times(-6)\equiv 16\times(-6)\equiv -96\equiv 26\pmod{61}$$
$$2^{43}\equiv 4\times 26\equiv 104\equiv 43\pmod{61}$$
$$2^{47}\equiv 16\times 43\equiv 688\equiv 17\pmod{61}$$
$$2^{49}\equiv 4\times 17\equiv 68\equiv 7\pmod{61}$$
$$2^{53}\equiv 16\times 7\equiv 112\equiv 51\pmod{61}$$
$$2^{59}\equiv 2^6\times 51\equiv 64\times(-10)\equiv -30\equiv 31\pmod{61}$$

Hence all the primitive roots of 61 in ascending order are given by

$$\left\{2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, \ 55, 59\right\}.$$

(b) We need to show that $x^2 = r + 61y$ has no solutions where r is one of the primitive roots of part (a).

Proof.

We convert the Diophantine equation $x^2 = r + 61y$ to modular arithmetic;

$$x^2 \equiv r \left(\text{mod } 61\right).$$

We know 61 is prime so it has a primitive root, say r. Taking indices to the base r of this gives the linear form;

$$2 \times \text{ind}_r\left(x\right) \equiv \text{ind}_r\left(r\right)\left(\text{mod } 60\right).$$

The $\gcd\left(2, \ \ 60\right) = 2$ but $\text{ind}_r\left(r\right) = 1$ because $r^1 \equiv r\left(\text{mod } 60\right)$. We have $2 \not| 1$ so $x^2 \equiv r\left(\text{mod } 61\right)$ has *no* solutions.

■

(c) We need to show that $x^2 = r + py$ has *no* solutions.

Proof.

Converting this $x^2 = r + py$ into modular form gives

$$x^2 \equiv r\left(\text{mod } p\right).$$

We are given that p is an odd prime so it has a primitive root, r say. Taking indices to the base r of this equation yields

$$\text{ind}_r\left(x^2\right) \equiv \text{ind}_r\left(r\right)\left(\text{mod } p-1\right) \ \Rightarrow \ 2\ \text{ind}_r\left(x\right) \equiv 1\left(\text{mod } p-1\right).$$

Since p is an odd prime so $\gcd\left(2, \ \ p-1\right) = 2$ and $2 \not| 1$ so $x^2 \equiv r\left(\text{mod } p\right)$ has *no* solution. This completes our proof.

■