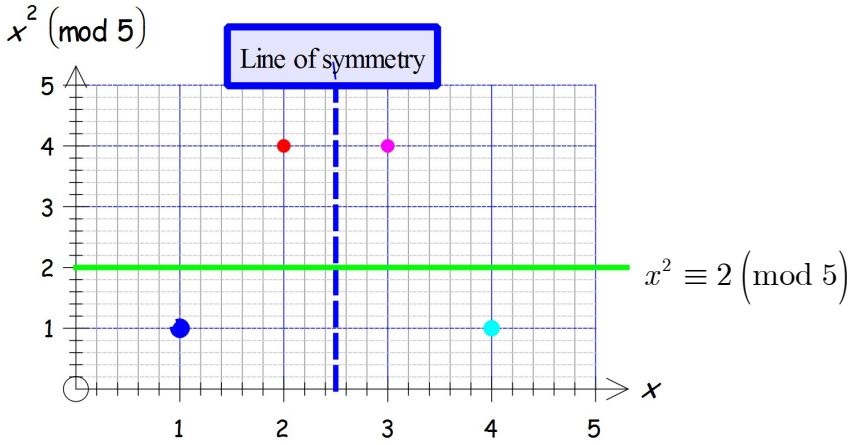
Complete Solutions to Exercise 7.1

1. In each case we create a table and then plot the appropriate graph:

   (a) We are given $p = 5$ so our least positive residues are $x = 1,\ 2,\ 3$ and 4:

x	1	2	3	4
$x^2 \pmod 5$	1	4	4	1

   Plotting this graph gives



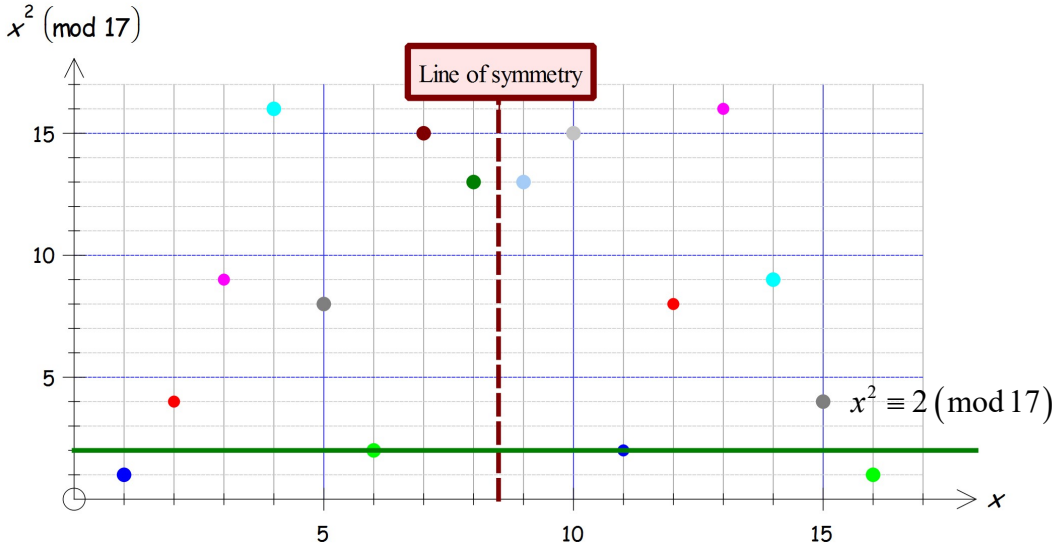
   As we can see from the graph and table there is *no* solution to $x^2 \equiv 2 \pmod 5$.

   Therefore, we *cannot* solve the Diophantine equation $x^2 = 2 + 5y$.

   (b) This time $p = 17$ so our table is

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

   Plotting the graph:



   Using the above graph or table we have

$$x^2 \equiv 2 \pmod{17} \quad \Rightarrow \quad x \equiv 6 \pmod{17} \quad \text{and} \quad x \equiv 11 \pmod{17}$$

Now we need to solve the Diophantine equation

$$x^2 = 2 + 17y\,.$$

Substituting the simplest of these solutions for x we have $x = 6,\ x = 11$ gives

$$6^2 = 2 + 17y \ \Rightarrow \ y = \frac{36-2}{17} = 2$$

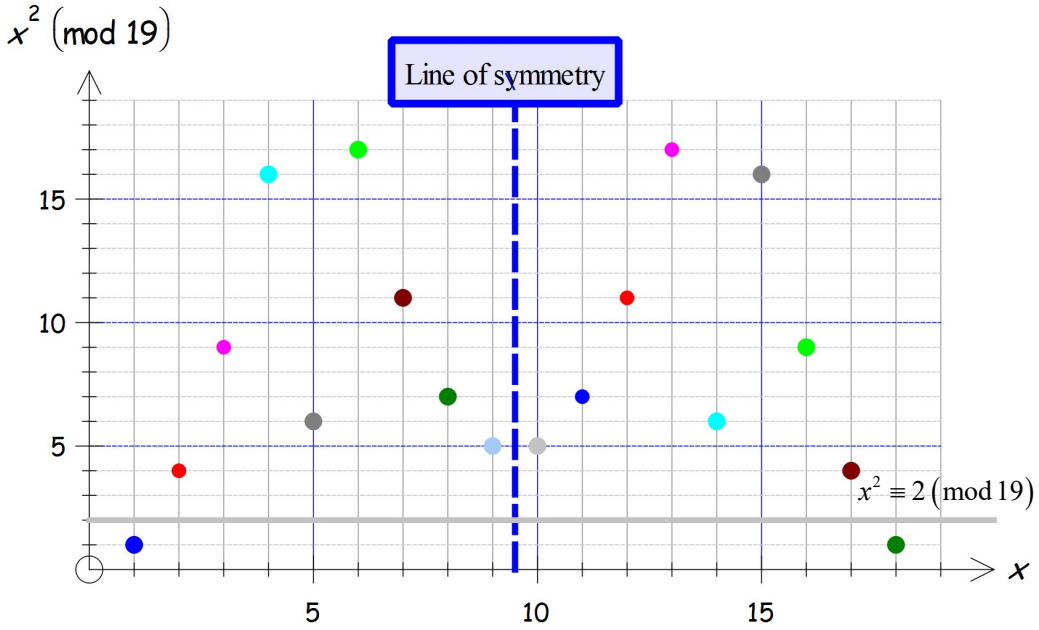
$$11^2 = 2 + 17y \ \Rightarrow \ y = \frac{121-2}{17} = 7$$

Our solutions are $\{x = 6,\ y = 2\}$ and $\{x = 11,\ y = 7\}$.

(c) Similarly for $p = 19$ we have:

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

Plotting this graph gives:



As we can see from the graph and table that there are *no* solutions to $x^2 \equiv 2 \pmod{19}$.

Hence the Diophantine equation $x^2 = 2 + 19y$ has no solutions.

2. In each case we use the Proposition (7.4):

$$\frac{p-1}{2} \text{ quadratic residues.}$$

(a) Substituting $p = 1223$ into this formula gives that there are

$$\frac{1223-1}{2} = 611 \text{ quadratic residues of } 1223.$$

(b) Similarly, there are exactly $\frac{3571-1}{2} = 1785$ quadratic residues of 3571.

(c) Also, there are $\frac{104\ 729-1}{2} = 52\ 364$ quadratic residues of 104 729.

(d) Repeating this we have $\frac{179\ 424\ 673-1}{2} = 89\ 712\ 336$ quadratic residues of 179 424 673.

3. We need to use Euler's Criterion (7.5) to determine whether the given residues are quadratic residues:

$$a \text{ is a quadratic residue of } p \Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

We are given the prime $p = 37$ so $\frac{p-1}{2} = \frac{37-1}{2} = 18$.

(a) In this case we need to evaluate $6^{18} \pmod{37}$. We have

$$6^2 \equiv 36 \equiv -1 \pmod{37}.$$

Therefore using the rules of indices we have

$$6^{18} \equiv \left(6^2\right)^9 \equiv \left(-1\right)^9 \equiv -1 \pmod{37}.$$

Since $6^{18} \equiv -1 \pmod{37}$ so by Euler's Criterion, 6 is a quadratic non-residue of 37.

(b) Similarly, we need to find the least positive residue of $2^{18} \pmod{37}$. Evaluating a simple power of 2 gives

$$2^5 \equiv 32 \equiv -5 \pmod{37}.$$

Writing the index 18 as a multiple of 5 plus any remainder we have

$$18 = \left(3 \times 5\right) + 3.$$

Therefore, we have

$$\begin{aligned} 2^{18} &\equiv 2^{(3\times5)+3} \equiv \left(2^5\right)^3 \times 2^3 \\ &\equiv \left(-5\right)^3 \times 8 \equiv -125 \times 8 \equiv -14 \times 8 \equiv -112 \equiv -1 \pmod{37} \end{aligned}$$

Since $2^{18} \equiv -1 \pmod{37}$ so 2 is a quadratic non-residue of 37.

(c) This time we need to evaluate $12^{18} \pmod{37}$. First we find $12^2 \pmod{37}$:

$$12^2 \equiv 144 \equiv -4 \pmod{37}$$

Evaluating powers of -4:

$$\left(-4\right)^2 \equiv 16 \left(\text{mod } 37\right)$$

$$\left(-4\right)^3 \equiv -64 \equiv -\left(-10\right) \equiv 10 \left(\text{mod } 37\right)$$

$$\left(-4\right)^4 \equiv -4 \times 10 \equiv -40 \equiv -3 \left(\text{mod } 37\right)$$

Since -3 is a smaller number let us use this result; $\left(-4\right)^4 \equiv -3 \left(\text{mod } 37\right)$. We have

$$\begin{aligned} 12^{18} \equiv \left(12^2\right)^9 &\equiv \left(-4\right)^9 \\ &\equiv \left(-4\right)^8 \times \left(-4\right) \\ &\equiv \left[\left(-4\right)^4\right]^2 \times \left(-4\right) \equiv \left(-3\right)^2 \times \left(-4\right) \equiv -36 \equiv 1 \left(\text{mod } 37\right) \end{aligned}$$

Hence 12 is a quadratic residue of 37 because $12^{18} \equiv 1 \left(\text{mod } 37\right)$.

(d) We need to find the least positive residue of $5^{18} \left(\text{mod } 37\right)$. Finding a simpler index of 5:

$$5^2 \equiv 25 \equiv -12 \left(\text{mod } 37\right).$$

We have

$$5^{18} \equiv \left(5^2\right)^9 \equiv \left(-12\right)^9 \left(\text{mod } 37\right) \qquad (*)$$

For the residue -12 we can use the results of part (c).

$$\begin{aligned} \left(-12\right)^9 &\equiv \left(-12\right)^8 \times \left(-12\right) \\ &\equiv \left(12^2\right)^4 \times \left(-12\right) \\ &\equiv \left(-4\right)^4 \times \left(-12\right) \equiv \left(-3\right) \times \left(-12\right) \equiv 36 \equiv -1 \left(\text{mod } 37\right) \end{aligned}$$

Using this result in (*) gives

$$5^{18} \equiv \left(-12\right)^9 \equiv -1 \left(\text{mod } 37\right).$$

Hence 5 is a quadratic non-residue of 37.

4. To find the square root of $a \left(\text{mod } p\right)$ means we need to solve $x^2 \equiv a \left(\text{mod } p\right)$.

We need to first determine if the given residues are quadratic residues. *How?*

By using Euler's Criterion (7.5):

$$a \text{ is a quadratic residue of } p \;\Leftrightarrow\; a^{\frac{p-1}{2}} \equiv 1 \left(\text{mod } p\right)$$

In each case $p = 17$ so $\dfrac{p-1}{2} = \dfrac{17-1}{2} = 8$.

(a) We first need to find the least positive residue of $2^8 \pmod{17}$. Well we have

$$2^4 \equiv 16 \equiv -1 \pmod{17}.$$

Therefore

$$2^8 \equiv \left(2^4\right)^2 \equiv \left(-1\right)^2 \equiv 1 \pmod{17}$$

By Euler's Criterion, 2 is a quadratic residue of 17 because $2^8 \equiv 1 \pmod{17}$. This means that $x^2 \equiv 2 \pmod{17}$ has solutions. Squaring $x = 1,\ 2,\ 3,\ 4,\ 5$ does *not* give 2 modulo 17. Squaring $x = 6$ gives

$$6^2 \equiv 36 \equiv 2 \pmod{17}$$

Hence $x \equiv 6 \pmod{17}$ is one solution. By Proposition (3.14) (b):

$$a^2 \equiv b^2 \pmod{p} \ \Leftrightarrow\ a \equiv \pm b \pmod{p}$$

We have the two solutions given by:

$$x^2 \equiv 6^2 \ \Leftrightarrow\ x \equiv \pm 6 \equiv 6, -6 \equiv 6, 11 \pmod{17}.$$

The two square roots of $2 \pmod{17}$ are $x \equiv 6, 11 \pmod{17}$.

(b) We have been given $x^2 \equiv 16 \pmod{17}$. Note that

$$x^2 \equiv 16 \equiv 4^2 \pmod{17}.$$

We have

$$x^2 \equiv 4^2 \ \Rightarrow\ x \equiv \pm 4 \equiv 4, -4 \equiv 4, 13 \pmod{17}.$$

Square roots of $16 \pmod{17}$ are $x \equiv 4, 13 \pmod{17}$.

(c) This time we are given $x^2 \equiv 5 \pmod{17}$. Again, we first test to see if there are solutions. We need to find the least positive residue of $5^8 \pmod{17}$:

$$5^2 \equiv 25 \equiv 8 \pmod{17}.$$

Remember $8 = 2^3$ so

$$5^8 \equiv \left(5^2\right)^4 \equiv 8^4 \equiv \left(2^3\right)^4 \equiv \left(2^4\right)^3 \pmod{17} \qquad (*)$$

Recall (from part(a)) that $2^4 \equiv -1 \pmod{17}$. Substituting this into (*) yields

$$5^8 \equiv \left(2^4\right)^3 \equiv \left(-1\right)^3 \equiv -1 \pmod{17}.$$

Since $5^8 \equiv -1 \pmod{17}$ so 5 is a quadratic non-residue which implies $x^2 \equiv 5 \pmod{17}$ has no solutions.

The square roots of $5 \pmod{17}$ do *not* exist.

5. In each case we need to complete the square on the given residues.

(a) We need to solve $x^2 + 2x + 2 \equiv 0 \pmod{23}$. Completing the square, we have

$$x^2 + 2x + 2 \equiv x^2 + 2x + 1 + 1 \equiv (x+1)^2 + 1 \equiv 0 \pmod{23}.$$

Subtracting 1 from both sides gives

$$(x+1)^2 \equiv -1 \pmod{23}.$$

Let $y = x + 1$ then we need to solve $y^2 \equiv -1 \pmod{23}$.

The prime p is 23 so we first need to find

$$(-1)^{\frac{p-1}{2}} \equiv (-1)^{\frac{23-1}{2}} \equiv (-1)^{11} \equiv -1 \pmod{23}.$$

This means there are *no* solutions to $y = (x+1)^2 \equiv -1 \pmod{23}$ so there are *no* solutions to the given congruence $x^2 + 2x + 2 \equiv 0 \pmod{23}$.

(b) Now we need to solve the quadratic congruence $x^2 + 4x + 2 \equiv 0 \pmod{23}$.

Completing the square gives

$$x^2 + 4x + 2 \equiv \underbrace{x^2 + 4x + 4}_{=(x+2)^2} - 2 \equiv (x+2)^2 - 2 \equiv 0 \pmod{23}.$$

Adding 2 to both sides yields

$$(x+2)^2 \equiv 2 \pmod{23}.$$

Let $y = x + 2$ so we need to solve the quadratic congruence

$$y^2 \equiv 2 \pmod{23}.$$

First, we need to see if 2 is a quadratic residue of 23 by applying Euler's Criterion. This means we must find the least positive residue of $2^{11} \pmod{23}$.

Evaluating some simple powers of 2:

$$2^5 \equiv 32 \equiv 9 \pmod{23}, \; 2^6 \equiv 64 \equiv -5 \pmod{23}$$

We have

$$2^{11} \equiv 2^{6+5} \equiv 2^6 \times 2^5 \equiv -5 \times 9 \equiv -45 \equiv -22 \equiv 1 \pmod{23}$$

Hence, we have solutions to $y^2 \equiv 2 \pmod{23}$. We have two solutions to this quadratic congruence. Trying $y = 5$ gives

$$5^2 \equiv 25 \equiv 2 \pmod{23}.$$

We need to find the other solution which is given by $-5 \equiv 18 \pmod{23}$.

We have the solutions $y \equiv 5 \pmod{23}$ and $y \equiv 18 \pmod{23}$. Remember we need to find x where $y = x + 2$. Subtracting 2 from both these congruences gives

$$x + 2 \equiv 5 \pmod{23} \quad \Rightarrow \quad x \equiv 3 \pmod{23}$$
$$x + 2 \equiv 18 \pmod{23} \quad \Rightarrow \quad x \equiv 16 \pmod{23}$$

The two solutions to the given congruence $x^2 + 4x + 2 \equiv 0 \pmod{23}$ are

$$x \equiv 3,\ 16 \pmod{23}$$

(c) We are required to solve $x^2 + 6x + 5 \equiv 0 \pmod{23}$. Completing the square gives

$$\begin{aligned} x^2 + 6x + 5 &\equiv x^2 + 6x + 9 - 4 \\ &\equiv (x+3)^2 - 4 \equiv 0 \pmod{23} \end{aligned}$$

Adding 4 to both sides yields

$$(x+3)^2 \equiv 4 \pmod{23}$$

Let $y = x + 3$ so we must solve $y^2 \equiv 4 \pmod{23}$. Clearly trying $y = 2$ is going to work because $2^2 \equiv 4 \pmod{23}$. Hence one of the solutions is $y \equiv 2 \pmod{23}$. We need to find the other solution. Therefore

$$y \equiv \pm 2 \equiv 2, -2 \equiv 2, 21 \pmod{23}.$$

Hence, we have $y \equiv 2 \pmod{23}$ and $y \equiv 21 \pmod{23}$. Substituting $y = x + 3$ gives

$$x + 3 \equiv 2 \pmod{23} \quad \Rightarrow \quad x \equiv -1 \equiv 22 \pmod{23}$$
$$x + 3 \equiv 21 \pmod{23} \quad \Rightarrow \quad x \equiv 18 \pmod{23}$$

Our two solutions to $x^2 + 6x + 5 \equiv 0 \pmod{23}$ are $x \equiv 18,\ 22 \pmod{23}$.

6. We need to prove that -1 is a quadratic residue of an odd prime $p \Leftrightarrow p \equiv 1 \pmod{4}$.

Proof.

$(\Leftarrow)$. Let $p \equiv 1 \pmod{4}$ so $p = 1 + 4k$ where k is an integer. Using Euler's Criterion (7.5):

$$a \text{ is a quadratic residue of } p \ \Leftrightarrow \ a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Applying this with $a = -1$ gives

$$\left(-1\right)^{\frac{p-1}{2}} \equiv \left(-1\right)^{\frac{4k+1-1}{2}} \equiv \left(-1\right)^{2k} \equiv 1 \left(\text{mod } p\right)$$

Hence -1 is a quadratic residue of p.

$\left(\Rightarrow\right)$. Let -1 be a quadratic residue of p. By Euler's Criterion we have

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

This implies that $\dfrac{p-1}{2}$ must be even or $\dfrac{p-1}{2} = 2m$ where m is an integer. Making p the subject of the formula gives $p - 1 = 4m$ which implies $p \equiv 1 \left(\text{mod } 4\right)$.

This completes our proof.

■

7. (a) We are required to prove that if a is a quadratic residue then $p - a$ is a quadratic residue $\Leftrightarrow$ $p \equiv 1 \left(\text{mod } 4\right)$.

Proof.

This is very similar to the proof of the previous question.

$\left(\Leftarrow\right)$. Let $p \equiv 1 \left(\text{mod } 4\right)$ so $p = 1 + 4k$ where k is an integer. Using Euler's Criterion (7.5):

$$a \text{ is a quadratic residue of } p \Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \left(\text{mod } p\right)$$

Applying this

$$\begin{aligned}\left(p-a\right)^{\frac{p-1}{2}} &\equiv \left(-a\right)^{\frac{p-1}{2}} \\ &\equiv \left(-1\right)^{\frac{p-1}{2}} a^{\frac{p-1}{2}} \equiv \underbrace{\left(-1\right)^{\frac{4k+1-1}{2}}}_{\equiv 1} a^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \underbrace{\equiv}_{\substack{\text{Because } a \text{ is a} \\ \text{quadratic residue of } p}} 1 \left(\text{mod } p\right)\end{aligned}$$

By Euler's Criterion $p - a$ is a quadratic residue of p.

$\left(\Rightarrow\right)$. Let $p - a$ be a quadratic residue of p. By Euler's Criterion we have

$$\begin{aligned}\left(p-a\right)^{\frac{p-1}{2}} &\equiv \left(-a\right)^{\frac{p-1}{2}} \\ &\equiv \left(-1\right)^{\frac{p-1}{2}} a^{\frac{p-1}{2}} \\ &\equiv \left(-1\right)^{\frac{p-1}{2}} 1 \qquad \left[\text{Because } a \text{ is a quadratic residue}\right] \\ &\equiv \left(-1\right)^{\frac{p-1}{2}} \equiv 1 \qquad \left[\text{Because } p-a \text{ is a quadratic residue}\right]\end{aligned}$$

This implies that $\dfrac{p-1}{2}$ must be even or $\dfrac{p-1}{2} = 2m$ where m is an integer. Making p the subject of the formula gives $p - 1 = 4m$ which implies $p \equiv 1 \left(\text{mod } 4\right)$.

This completes our proof.

■

(b) In this case we need to prove:

If a is a quadratic residue then $p-a$ is a quadratic non-residue $\Leftrightarrow$ $p \equiv 3 \pmod 4$.

Proof.

$(\Leftarrow)$. Let $p \equiv 3 \pmod 4$ so $p = 3 + 4k$ where k is an integer. Using Euler's Criterion (7.5):

$$a \text{ is a quadratic residue of } p \;\Leftrightarrow\; a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

Applying this

$$\begin{aligned}
(p-a)^{\frac{p-1}{2}} &\equiv (-a)^{\frac{p-1}{2}} \\
&\equiv (-1)^{\frac{p-1}{2}} a^{\frac{p-1}{2}} \\
&\equiv (-1)^{\frac{4k+3-1}{2}} a^{\frac{p-1}{2}} \\
&\equiv (-1)^{2k+1} a^{\frac{p-1}{2}} \equiv (-1) \underbrace{1}_{\substack{\text{Because } a \text{ is a} \\ \text{quadratic residue of } p}} \equiv -1 \pmod p
\end{aligned}$$

By Euler's Criterion $p-a$ is a quadratic non-residue of p.

$(\Rightarrow)$. Let $p-a$ be a quadratic non- residue of p. By Euler's Criterion we have

$$\begin{aligned}
(p-a)^{\frac{p-1}{2}} &\equiv (-a)^{\frac{p-1}{2}} \\
&\equiv (-1)^{\frac{p-1}{2}} a^{\frac{p-1}{2}} \\
&\equiv (-1)^{\frac{p-1}{2}} 1 \qquad \left[\text{Because } a \text{ is a quadratic residue}\right] \\
&\equiv (-1)^{\frac{p-1}{2}} \equiv -1 \qquad \left[\text{Because } p-a \text{ is a quadratic non-residue}\right]
\end{aligned}$$

This implies that $\dfrac{p-1}{2}$ must be odd or $\dfrac{p-1}{2} = 2m+1$ where m is an integer.

Making p the subject of the formula gives

$$p - 1 = 4m + 2 \quad \Rightarrow \quad p = 4m + 3$$

which gives $p \equiv 3 \pmod 4$.

This completes our proof.

■

8. We need to show that $ax^2 + bx + c \equiv 0 \pmod p$ where $p \nmid a$ can be written as $y^2 \equiv m \pmod p$.

Proof.

Multiply both sides of the given quadratic congruence by $4a$ yields

$$4a^2x^2 + 4abx + 4ac \equiv 0\Big(\text{mod } p\Big).$$

Completing the square on this gives

$$\begin{aligned} 4a^2x^2 + 4abx + 4ac &\equiv \Big(2ax + b\Big)^2 + 4ac - b^2 \\ &\equiv \Big(2ax + b\Big)^2 \equiv b^2 - 4ac\Big(\text{mod } p\Big) \end{aligned}$$

Let $y = 2ax + b$ then $y^2 = \Big(2ax + b\Big)^2$ and let $m = b^2 - 4ac$.

We have $y^2 \equiv m\Big(\text{mod } p\Big)$.

■

We solve each of the given quadratic congruences using the above established formula.

(a) We are given $2x^2 + 2x + 1 \equiv 0\Big(\text{mod } 29\Big)$ so substituting $a = 2,\ b = 2,\ c = 1$ into $y = 2ax + b = 4x + 2$ and $m = b^2 - 4ac = 4 - \Big(4 \times 2 \times 1\Big) = -4$ yields

$$y^2 \equiv -4\Big(\text{mod } 29\Big) \equiv 25\Big(\text{mod } 29\Big).$$

This $y^2 \equiv 25 \equiv 5^2\Big(\text{mod } 29\Big)$ implies $y \equiv \pm 5 \equiv 5,\ 24\Big(\text{mod } 29\Big)$. We have

$$\begin{aligned} y = 4x + 2 \equiv 5 \ &\Rightarrow\ 4x \equiv 3 \ \Rightarrow\ x \equiv 8\Big(\text{mod } 29\Big) \\ y = 4x + 2 \equiv 24 \ &\Rightarrow\ 4x \equiv 22 \ \Rightarrow\ x \equiv 20\Big(\text{mod } 29\Big) \end{aligned}$$

Our solutions are $x \equiv 8,\ 20\ \Big(\text{mod } 29\Big)$.

(b) This time we are asked to solve $5x^2 + 9x + 4 \equiv 0\Big(\text{mod } 101\Big)$. Again using the above derived formula with $a = 5, b = 9, c = 4$:

$$y = 2ax + b = 10x + 9\,,\ m = b^2 - 4ac = 81 - \Big(4 \times 5 \times 4\Big) = 1\,.$$

Using $y^2 \equiv m\Big(\text{mod } 101\Big)$ gives

$$y^2 \equiv 1\Big(\text{mod } 101\Big) \ \Rightarrow\ y \equiv \pm 1\Big(\text{mod } 101\Big).$$

Thus, we need to solve $10x + 9 \equiv 1\Big(\text{mod } 101\Big) \ \Rightarrow\ 10x \equiv -8 \equiv 93\Big(\text{mod } 101\Big)$.

We can rewrite the last congruence as a linear Diophantine equation:

$$10x \equiv 93\Big(\text{mod } 101\Big) \ \Rightarrow\ 10x = 93 + 101y \ \Rightarrow\ 10x - 101y = 93$$

10 and 101 are relatively prime so we can solve

$$\begin{aligned} 10x - 101y = 1 \ &\Rightarrow\ x = -10,\ \ y = -1 \\ 10x - 101y = 93 \ &\Rightarrow\ x = -930,\ \ y = -93 \end{aligned}$$

Therefore $x = -930 \equiv 80 \pmod{101}$. One of our solutions is $x \equiv 80 \pmod{101}$.

Similarly computing the other solution for $y \equiv -1 \equiv 100 \pmod{101}$:

$$10x + 9 \equiv 100 \pmod{101} \;\Rightarrow\; 10x \equiv 91 \pmod{101}$$

Writing the equivalent linear Diophantine equation $10x - 101y = 91$. We have

$$10x - 101y = 1 \;\Rightarrow\; x = -10,\; y = -1$$
$$10x - 101y = 91 \;\Rightarrow\; x = -910,\; y = -91$$

Our other solution is $x \equiv -910 \equiv 100 \pmod{101}$. The solutions to

$$5x^2 + 9x + 4 \equiv 0 \pmod{101} \text{ are } x \equiv 80,\; 100 \pmod{101}$$

(c) We are asked to solve $7x^2 + 9x + 3 \equiv 0 \pmod{41}$. Again using the above formula with $a = 7, b = 9, c = 3$ gives

$$y = 2ax + b = 14x + 9\,,\; m = b^2 - 4ac = 81 - (4 \times 7 \times 3) = -3\,.$$

We need to solve $y^2 \equiv -3 \pmod{41}$. We first need to check that -3 is a quadratic residue of 41 by using Euler's Criterion (7.5):

$$a \text{ is a quadratic residue of } p \;\Leftrightarrow\; a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Computing $(-3)^{\frac{41-1}{2}} \equiv (-3)^{20} \equiv x \pmod{41}$. Evaluating simpler powers of -3:

$$(-3)^4 \equiv 81 \equiv 40 \equiv -1 \pmod{41}.$$

Therefore, using this we have

$$(-3)^{20} \equiv (-3)^{4\times 5} \equiv \left[(-3)^4\right]^5 \equiv (-1)^5 \equiv -1 \pmod{41}.$$

Hence by Euler's Criterion we conclude that $y^2 \equiv -3 \pmod{41}$ has *no* solutions so there are *no* solutions to the given equation $7x^2 + 9x + 3 \equiv 0 \pmod{41}$.

(d) We need to solve $2x^2 + 20x + 49 \equiv 0 \pmod{61}$.

Substituting $a = 2, b = 20, c = 49$ into $y = 2ax + b = 4x + 20$ and

$$m = 20^2 - (4 \times 2 \times 49) = 8\,.$$

We need to solve $y^2 \equiv 8 \pmod{61}$. We first need to check that 8 is a quadratic residue of 61 by using Euler's Criterion (7.5):

$$a \text{ is a quadratic residue of } p \;\Leftrightarrow\; a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Computing $8^{\frac{61-1}{2}} \equiv 8^{30} \equiv x \pmod{61}$. Computing powers of 8:

$$8^2 \equiv 64 \equiv 3 \pmod{61} \text{ and } 3^4 \equiv \left(3^2\right)^2 \equiv 9^2 \equiv 81 \equiv 20 \pmod{61}.$$

We use this result $3^4 \equiv 20 \pmod{61}$ to evaluate $8^{30} \equiv x \pmod{61}$.

$$\begin{aligned} 8^{30} \equiv \left(8^2\right)^{15} \equiv 3^{15} \equiv \left(3^4\right)^3 \times 3^3 \equiv 20^3 \times 27 \\ \equiv 20^2 \times 20 \times 27 \equiv 34 \times 52 \equiv 1768 \equiv 60 \equiv -1 \pmod{61} \end{aligned}$$

By Euler's criterion we know 8 is a quadratic *non* residue so there is *no* solution to $y^2 \equiv 8 \pmod{61}$ which implies $2x^2 + 20x + 49 \equiv 0 \pmod{61}$ has *no* solutions.

9. We need to prove that $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ provided $p \nmid a$. *How?*

We use Fermat's Little Theorem (4.1):

$$n^{p-1} \equiv 1 \pmod{p}$$

Proof.

Let $x = a^{\frac{p-1}{2}}$ then

$$x^2 = \left(a^{\frac{p-1}{2}}\right)^2 = a^{p-1} \equiv 1 \pmod{p} \quad \left[\text{By Fermat's Little Theorem}\right]$$

Now using Lemma (4.3):

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

We have $x \equiv \pm 1 \pmod{p}$. Therefore $x = a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. This completes our proof.

■

10. We need to prove that if a is a quadratic residue of p then a is *not* a primitive root of p.

Proof.

Let a be a quadratic residue of p. By Euler's Criterion we have

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Suppose a is a primitive root of p. By the definition of the primitive root (6.10):

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

In our case we are dealing with primes p so $\phi(p) = p-1$. Since a is a primitive root so $a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$. This is a contradiction because from above we have $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Hence our supposition a is a primitive root of p must be wrong so a is *not* a primitive root of p.

■

11. (a) We need to prove the product of two quadratic non-residues is a quadratic residue.

Proof.

Let a and b both be quadratic non – residues of p. By Euler's Criterion we have

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p} \text{ and } b^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Multiplying these together gives

$$a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (-1)(-1) \pmod{p}$$
$$(ab)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Since $(ab)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ so ab is a quadratic residue of p. This completes our proof.

■

(b) This time we need to prove the product of a quadratic residue and quadratic non-residue is a quadratic non – residue.

Proof.

Let a be a quadratic residue and b be a quadratic non – residues of p. We have

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \text{ and } b^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Multiplying these together gives

$$a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv 1(-1) \pmod{p}$$
$$(ab)^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

Therefore $(ab)^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ implies that ab is a quadratic non - residue of p. Hence the product of a quadratic residue and quadratic non-residue is a quadratic non – residue.

■

(c) We are required to prove that the square of a quadratic residue of p is a quadratic residue.

Proof.

By $x^2 \equiv a^2 \pmod{p} \Leftrightarrow x \equiv \pm a \pmod{p}$ which completes our proof.

■

12. We are asked to show that if a is a quadratic residue modulo p where $p \equiv 3 \pmod{4}$ then the quadratic congruence $x^2 \equiv a \pmod{p}$ has the solutions $x \equiv \pm a^{\frac{p+1}{4}} \pmod{p}$.

Proof.

We are given that a is a quadratic residue modulo p so by Euler's Criterion (7.5):

$$a \text{ is a quadratic residue of } p \Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

We have $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Multiplying this by a gives

$$a \times a^{\frac{p-1}{2}} \equiv a^{1+\frac{p-1}{2}} \equiv a^{\frac{p+1}{2}} \equiv a \equiv x^2 \pmod{p} \qquad (*)$$

We are also given that $p \equiv 3 \pmod{4}$ which implies $p = 3 + 4k$. Therefore we can write the above index as

$$\frac{p+1}{2} = \frac{3+4k+1}{2} = 2(k+1).$$

Substituting this $\frac{p+1}{2} = 2(k+1)$ into (*) yields

$$x^2 \equiv a^{\frac{p+1}{2}} \equiv a^{2(k+1)} \equiv \left(a^{k+1}\right)^2 \pmod{p}.$$

We have $x^2 \equiv \left(a^{k+1}\right)^2 \pmod{p}$. By Proposition (3.14) (b):

$$a^2 \equiv b^2 \pmod{p} \Leftrightarrow a \equiv \pm b \pmod{p}$$

Applying this to $x^2 \equiv \left(a^{k+1}\right)^2 \pmod{p}$ implies $x \equiv \pm a^{k+1} \pmod{p}$. From above we have $p = 3 + 4k$ which implies that

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

Substituting this $k+1 = \frac{p+1}{4}$ into $x \equiv \pm a^{k+1} \pmod{p}$ gives us our result:

$$x \equiv \pm a^{\frac{p+1}{4}} \pmod{p}$$

This completes our proof.

■

(a) We need to solve $x^2 \equiv 3 \pmod{83}$. First, we need to establish whether 3 is a quadratic residue modulo 83. *How?*

Use Euler's Criterion with $a = 3$, $p = 83$:

$$3^{\frac{83-1}{2}} \equiv 3^{41} \equiv x \pmod{83}.$$

We need to find x where x is the least positive residue. From the powers of 3:

$$3^4 \equiv 81 \equiv -2 \pmod{83}.$$

Using this result we have

$$3^{41} \equiv 3^{40} \times 3 \equiv \left(3^4\right)^{10} \times 3 \equiv \left(-2\right)^{10} \times 3 \equiv 1024 \times 3 \equiv 28 \times 3 \equiv 84 \equiv 1 \pmod{83}$$

Hence 3 is a quadratic residue modulo 83. Since $83 \equiv 3 \pmod{4}$ so we can use the result proven above which says that $x \equiv \pm a^{\frac{p+1}{2}} \pmod{p}$:

$$x \equiv \pm 3^{\frac{83+1}{4}} \equiv \pm 3^{21} \equiv \pm\left[\left(3^4\right)^5 \times 3\right] \equiv \pm\left[\left(-2\right)^5 \times 3\right] \equiv \pm\left[-32 \times 3\right] \equiv \pm\left[-96\right] \equiv \pm\left(-13\right) \equiv \pm 70 \pmod{83}$$

Hence, we have the solutions $x \equiv 13, 70 \pmod{83}$.

(b) We are asked to solve $x^2 \equiv 2 \pmod{\left(2^{13} - 1\right)}$. First we check that 2 is a quadratic residue modulo $2^{13} - 1$. By Euler's Criterion we need to find x in

$$2^{\frac{2^{13}-1-1}{2}} \equiv 2^{4095} \equiv x \pmod{2^{13} - 1}.$$

Clearly by the definition of congruence we have

$$2^{13} \equiv 1 \pmod{\left(2^{13} - 1\right)} \qquad (\dagger)$$

Also $13 \times 315 = 4095$ therefore $2^{4095} \equiv 1 \pmod{2^{13} - 1}$ which implies that 2 is a quadratic residue modulo $2^{13} - 1$. Additionally, $2^{13} - 1 \equiv 3 \pmod{4}$ which means we can use the above result that we proved. Substituting $a = 2$ and $p = 2^{13} - 1$ into $x \equiv \pm a^{\frac{p+1}{4}} \pmod{p}$ yields

$$x \equiv \pm 2^{\frac{2^{13}-1+1}{4}} \equiv \pm 2^{\frac{2^{13}}{2^2}} \equiv \pm 2^{2^{11}} \equiv \pm 2^{2048} \pmod{2^{13} - 1}.$$

We want to use (†) which means we need to write the index of 2048 as a multiple of 13 and any remainder:

$$2048 = \left(157 \times 13\right) + 7.$$

Therefore, we have

$$x \equiv \pm 2^{2048} \equiv \pm 2^7 \equiv \pm 128 \equiv 128, \;\; 8063 \pmod{2^{13}-1}.$$

(c) We need to solve $x^2 \equiv 5 \pmod{127}$. Again, we first test whether 5 is a quadratic residue modulo 127 by using Euler's Criterion:

$$5^{\frac{127-1}{2}} \equiv 5^{63} \equiv x \pmod{127}.$$

We can use $5^3 \equiv 125 \equiv -2 \pmod{127}$ and $2^7 \equiv 128 \equiv 1 \pmod{27}$. Combining these we have

$$5^{63} \equiv 5^{3\times 21} \equiv \left(5^3\right)^{21} \equiv \left(-2\right)^{21} \equiv \left(-1\right)^{21} \times 2^{(7\times 3)} \equiv \left(-1\right) \times \underbrace{\left(2^7\right)}_{\equiv 1 \pmod{128}}{}^3 \equiv -1 \pmod{127}.$$

Therefore by Euler's Criterion we conclude that 5 is a quadratic non – residue modulo 127 which implies that $x^2 \equiv 5 \pmod{127}$ has *no* solutions.

13. We are asked to prove that the multiplicative inverse of a quadratic residue of p is also a quadratic residue of p.

Proof.

Let a be a quadratic residue of p so by Euler's Criterion we have

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \qquad (\dagger)$$

Let b be the multiplicative inverse of a modulo p. This implies

$$ab \equiv 1 \pmod{p} \qquad (*)$$

We need to prove that $b^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Taking the congruence in (*) to the power $\dfrac{p-1}{2}$ gives

$$(ab)^{\frac{p-1}{2}} \equiv \underbrace{a^{\frac{p-1}{2}}}_{\substack{\equiv 1 \pmod{p} \\ \text{by } (\dagger)}} b^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Hence we have $b^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ so by Euler's Criterion we conclude that b is a quadratic residue of p. So the multiplicative inverse of a quadratic residue is also a quadratic residue of p.

■