Complete Solutions to Supplementary Problems 7

1. This is straightforward because $196 = 14^2$ so we have

$$x^2 \equiv 196 \equiv 14^2 \;\Leftrightarrow\; x \equiv \pm 14 \equiv 14, 197 \pmod{211}$$

Hence the given quadratic congruence has the solutions $x \equiv 14, 197 \pmod{211}$.

2. (a) We need to solve $5x^2 + 2x \equiv 20 \pmod{101}$. Subtracting 20 from both sides

$$5x^2 + 2x - 20 \equiv 0 \pmod{101}$$

Multiplying this congruence by 20 and simplifying yields

$$\begin{aligned} 100x^2 + 40x - 400 &\equiv 0 \pmod{101} \\ -x^2 + 40x - 400 &\equiv 0 \pmod{101} \qquad \left[\text{Because } 100 \equiv -1 \pmod{101}\right] \\ -\left(x^2 - 40x + 400\right) \equiv -\left(x - 20\right)^2 &\equiv 0 \pmod{101} \\ x - 20 \equiv 0 \pmod{101} \;\Rightarrow\; x &\equiv 20 \pmod{101} \end{aligned}$$

Our solution to $5x^2 + 2x \equiv 20 \pmod{101}$ is $x \equiv 20 \pmod{101}$.

(b) We are given the quadratic $x^2 - x - 6 \equiv 0 \pmod{103}$. Factorizing this

$$x^2 - x - 6 \equiv (x-3)(x+2) \equiv 0 \pmod{103}$$

Using Proposition (3.14)(a):

> (a) If $a \times b \equiv 0 \pmod{p}$ then $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.

On $(x-3)(x+2) \equiv 0 \pmod{103}$ gives

$$x - 3 \equiv 0 \text{ or } x + 2 \equiv 0 \;\Rightarrow\; x \equiv 3, -2 \equiv 3,\ 101 \pmod{103}$$

Hence our solution to $x^2 - x - 6 \equiv 0 \pmod{103}$ is $x \equiv 3,\ 101 \pmod{103}$.

3. We are asked to solve $x^2 \equiv 7 \pmod{787}$. We use the result of question 12 of Exercises 7.1:

> If a is a quadratic residue of p where $p \equiv 3 \pmod{4}$ then the quadratic congruence $x^2 \equiv a \pmod{p}$ has the solutions $x \equiv \pm a^{\frac{p+1}{4}} \pmod{p}$.

First $787 \equiv 3 \pmod 4$ and now we need to test if 7 is a quadratic residue of 787.

How?

We evaluate the Legendre symbol $\left(\frac{7}{787}\right)$ by using Corollary (7.17):

$$\left(\frac{p}{q}\right) = \begin{cases} \left(q/p\right) & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -\left(q/p\right) & \text{if both } p \equiv 3 \pmod 4 \text{ and } q \equiv 3 \pmod 4 \end{cases}$$

We have

$$\left(\frac{7}{787}\right) \underbrace{=}_{\text{Because } 7 \equiv 787 \equiv 3 \pmod 4} -\left(\frac{787}{7}\right)$$

$$\underbrace{=}_{\text{Because } 787 \equiv 3 \pmod 7} -\left(\frac{3}{7}\right) \underbrace{=}_{\text{Because } 7 \equiv 3 \pmod 4} \overbrace{-(-)}^{=+}\left(\frac{7}{3}\right) \underbrace{=}_{\text{Because } 7 \equiv 1 \pmod 3} \left(\frac{1}{3}\right) = 1$$

Hence 7 is a quadratic residue of 787. Now we are in a position to use the above result of question 12 of Exercises 7.1. We have

$$x \equiv \pm 7^{\frac{787+1}{4}} \equiv \pm 7^{197} \pmod{787} \qquad (\dagger)$$

Computing some simpler powers of 7 gives

$$7^4 \equiv 2401 \equiv 40 \pmod{787}$$

$$7^8 \equiv 40^2 \equiv 26 \pmod{787}$$

$$7^{16} \equiv 26^2 \equiv 676 \pmod{787}$$

$$7^{17} \equiv 7 \times 676 \equiv 10 \pmod{787}$$

We use this last result $7^{17} \equiv 10 \pmod{787}$ to reduce our calculations:

$$7^{18} \equiv 7 \times 10 \equiv 70 \pmod{787}$$

$$7^{35} \equiv 7^{17} \times 7^{18} \equiv 10 \times 70 \equiv 700 \pmod{787}$$

$$7^{51} \equiv \left(7^{17}\right)^3 \equiv 10^3 \equiv 1000 \equiv 213 \pmod{787}$$

$$7^{68} \equiv \left(7^{17}\right)^4 \equiv 10^4 \equiv 10000 \equiv 556 \pmod{787}$$

$$7^{85} \equiv \left(7^{17}\right)^5 \equiv 10^5 \equiv 100\,000 \equiv 51 \pmod{787}$$

We use these results to evaluate $x \equiv \pm 7^{197} \pmod{787}$.

$$x \equiv \pm 7^{197} \equiv \pm 7^{(2\times 85)+27} \equiv \pm\left[\left(7^{85}\right)^2 \times 7^{27}\right]$$
$$\equiv \pm\left[51^2 \times 7^{17+10}\right]$$
$$\equiv \pm\left[2601 \times 10 \times 7^{10}\right] \equiv \pm\left[2601 \times 10 \times 26 \times 49\right] \equiv \pm 105 \pmod{787}$$

Hence our solution to the given quadratic $x^2 \equiv 7 \pmod{787}$ is

$$x \equiv \pm 105 \equiv 105,\ -105 \equiv 105,\ 682 \pmod{787}$$

We also need to solve the Diophantine equation $x^2 = 7 + 787y$.

Because $x \equiv 105,\ 682 \pmod{787}$ we have an infinite number of solutions but we choose the simplest of these which is $x = 105,\ 682$.

Substituting these into $x^2 = 7 + 787y$ and transposing gives

$$105^2 = 7 + 787y \ \Rightarrow\ y = \frac{105^2 - 7}{787} = 14$$

$$682^2 = 7 + 787y \ \Rightarrow\ y = \frac{682^2 - 7}{787} = 591$$

Hence $x = 105, y = 14$ and $x = 682,\ y = 591$.

4. (a) In order to compute the square root of $3 \pmod{131}$ we have to solve

$$x^2 \equiv 3 \pmod{131}.$$

First, we need to test whether 3 is a quadratic residue of 131. *How?*

By evaluating the Legendre symbol

$$\left(\frac{3}{131}\right) \underbrace{=}_{\text{Because } 3\equiv 131 \pmod 4} -\left(\frac{131}{3}\right) \underbrace{=}_{\text{Because } 131\equiv 2 \pmod 3} -\left(\frac{2}{3}\right)$$

Testing for the integer 2 is given by

(7.15) $$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

Since $3 \equiv 3 \pmod 8$ so

$$\left(\frac{3}{131}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1$$

Hence 3 is a quadratic residue of 131 so the square root of $3 \pmod{131}$ exists.

Also $131 \equiv 3 \pmod 4$ so we can use the result of question 12 of Exercises 7.1:

If a is a quadratic residue of p where $p \equiv 3 \pmod 4$ then the quadratic congruence $x^2 \equiv a \pmod p$ has the solutions $x \equiv \pm a^{\frac{p+1}{4}} \pmod p$.

Applying this result we have

$$x \equiv \pm 3^{\frac{131+1}{4}} \equiv \pm 3^{33} \pmod{131}$$

Evaluating some low powers of 3:

$$3^4 \equiv 81 \equiv -50 \pmod{131}$$

$$3^8 \equiv \left(3^4\right)^2 \equiv \left(-50\right)^2 \equiv 2500 \equiv 11 \pmod{131}$$

$$3^{16} \equiv \left(3^8\right)^2 \equiv 11^2 \equiv 121 \equiv -10 \pmod{131}$$

Expressing the index 33 as a multiple of 16 and any remainder gives

$$\begin{aligned} x \equiv \pm 3^{33} &\equiv \pm\left[3^{32} \times 3\right] \equiv \pm\left[\left(3^{16}\right)^2 \times 3\right] \\ &\equiv \pm\left[\left(-10\right)^2 \times 3\right] \equiv \pm\left[300\right] \equiv \pm 38 \pmod{131} \end{aligned}$$

The square roots of $3 \pmod{131}$ are $x \equiv \pm 38 \equiv 38,\ 93 \pmod{131}$.

(b) To find the square root of $11 \pmod{127}$ means we need to solve

$$x^2 \equiv 11 \pmod{127}$$

First, we need to check whether 11 is a quadratic residue of modulo 127. This means we must evaluate the Legendre symbol $\left(\frac{11}{127}\right)$. *How?*

We use the Corollary (7.17):

$$\left(\frac{p}{q}\right) = \begin{cases} \left(q/p\right) & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -\left(q/p\right) & \text{if both } p \equiv 3 \pmod 4 \text{ and } q \equiv 3 \pmod 4 \end{cases}$$

Therefore

$$\left(\frac{11}{127}\right) \underbrace{=}_{\text{Because } 11 \equiv 127 \equiv 3 \pmod 4} -\left(\frac{127}{11}\right) \underbrace{=}_{\text{Because } 127 \equiv 6 \pmod{11}} -\left(\frac{6}{11}\right) = -\left(\frac{2}{11}\right) \times \left(\frac{3}{11}\right) \quad \left[\begin{matrix}\text{By multiplicative} \\ \text{property}\end{matrix}\right]$$

Testing for the integer 2 is given by:

(7.15) $$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

Since $11 \equiv 3 \pmod 8$ so $\left(\frac{2}{11}\right) = -1$ and evaluating the other Legendre symbol

$$\left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) \underbrace{\equiv}_{\text{by (7.15)}} -(-1) = 1$$

Substituting $\left(\frac{2}{11}\right) = -1$ and $\left(\frac{3}{11}\right) = 1$ into the above calculation yields

$$\left(\frac{11}{127}\right) = -\left(\frac{2}{11}\right) \times \left(\frac{3}{11}\right) = -(-1) \times 1 = 1$$

Hence 11 is a quadratic residue of 127 so the square root of $11 \pmod{127}$ exists.

Now we must find it. *How?*

Since $127 \equiv 3 \pmod 4$ so we use the result of question 12 of Exercises 7.1:

> If a is a quadratic residue of p where $p \equiv 3 \pmod 4$ then the quadratic congruence $x^2 \equiv a \pmod p$ has the solutions $x \equiv \pm a^{\frac{p+1}{4}} \pmod p$.

This gives

$$x \equiv \pm 11^{\frac{127+1}{4}} \equiv \pm 11^{32} \pmod{127} \qquad (\dagger)$$

Evaluating some simpler powers of 11:

$$11^2 \equiv 121 \equiv -6 \pmod{127}$$

$$11^4 \equiv (-6)^2 \equiv 36 \pmod{127}$$

$$11^5 \equiv 36 \times 11 \equiv 396 \equiv 15 \pmod{127}$$

$$11^{10} \equiv 15^2 \equiv 225 \equiv 98 \pmod{127}$$

$$11^{12} \equiv 98 \times (-6) \equiv -588 \equiv 47 \pmod{127}$$

$$11^{13} \equiv 47 \times 11 \equiv 517 \equiv 9 \pmod{127}$$

Using a combination of these powers with the rules of indices to evaluate x in (†) gives

$$x \equiv \pm 11^{32} \equiv \pm\left[\left(11^{13}\right)^2 \times 11^5 \times 11\right] \equiv \pm\left[9^2 \times 15 \times 11\right] \equiv \pm 13\ 365 \equiv \pm 30 \pmod{127}$$

Hence the square roots of $11 \pmod{127}$ are

$$x \equiv \pm 30 \equiv 30,\ -30 \equiv 30,\ 97 \pmod{127}$$

(c) In order to compute the square root of $3 \pmod{251}$ we have to solve

$$x^2 \equiv 3 \pmod{251}.$$

First, we need to test whether 3 is a quadratic residue of 251. *How?*

By evaluating the Legendre symbol

$$\left(\frac{3}{251}\right) \underset{\text{Because } 3\equiv 251 \pmod 4}{=\!=} -\left(\frac{251}{3}\right) \underset{\text{Because } 251\equiv 2 \pmod 3}{=\!=} -\left(\frac{2}{3}\right)$$

Testing for the integer 2 is given by

(7.15) $$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

Since $3 \equiv 3 \pmod 8$ so

$$\left(\frac{3}{251}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1$$

Hence 3 is a quadratic residue of 251 so the square root of $3 \pmod{251}$ exists.

Also $251 \equiv 3 \pmod 4$ so we can use the result of question 12 of Exercises 7.1:

If a is a quadratic residue of p where $p \equiv 3 \pmod 4$ then the quadratic congruence $x^2 \equiv a \pmod p$ has the solutions $x \equiv \pm a^{\frac{p+1}{4}} \pmod p$.

Applying this result we have

$$x \equiv \pm 3^{\frac{251+1}{4}} \equiv \pm 3^{63} \pmod{251}$$

Evaluating some low powers of 3:

$$3^5 \equiv 243 \equiv -8 \pmod{251}$$

$$3^{10} \equiv \left(3^5\right)^2 \equiv (-8)^2 \equiv 64 \pmod{251}$$

$$3^{15} \equiv \left(3^5\right)^2 \times 3^5 \equiv 64 \times (-8) \equiv -512 \equiv 241 \equiv -10 \pmod{251}$$

Expressing the index 63 as a multiple of 15 and any remainder gives

$$\begin{aligned} x \equiv \pm 3^{63} &\equiv \pm\left[3^{60} \times 3^3\right] \equiv \pm\left[\left(3^{15}\right)^4 \times 27\right] \\ &\equiv \pm\left[(-10)^4 \times 27\right] \equiv \pm[270\,000] \equiv \pm 175 \pmod{251} \end{aligned}$$

The square roots of $3 \pmod{251}$ are

$$x \equiv \pm 175 \equiv 175,\ -175 \equiv 175,\ 76 \pmod{251}.$$

5. (a) We need to compute the Legendre symbol $\left(\frac{751}{919}\right)$. We use Corollary (7.17):

$$\left(\frac{p}{q}\right)=\begin{cases}\left(q/p\right) & \text{if } p\equiv 1\left(\text{mod } 4\right) \text{ or } q\equiv 1\left(\text{mod } 4\right)\\ -\left(q/p\right) & \text{if both } p\equiv 3\left(\text{mod } 4\right) \text{ and } q\equiv 3\left(\text{mod } 4\right)\end{cases}$$

We have

$$\left(\frac{751}{919}\right)\underbrace{=}_{\text{Because } 751\equiv 919\equiv 3\left(\text{mod } 4\right)}-\left(\frac{919}{751}\right)\underbrace{=}_{\text{Because } 919\equiv 168\left(\text{mod } 751\right)}-\left(\frac{168}{751}\right)$$

$$\underbrace{=}_{\text{By the multiplicative property and } 8\times 3\times 7=168}-\left(\frac{8}{751}\right)\times\left(\frac{3}{751}\right)\times\left(\frac{7}{751}\right)$$

$$\underbrace{=}_{\text{By } 2^3=2^2\times 2}-\underbrace{\left(\frac{2^2}{751}\right)}_{=1}\times\left(\frac{2}{751}\right)\times\left[-\left(\frac{751}{3}\right)\right]\times\left[-\left(\frac{751}{7}\right)\right]$$

$$=-\left(\frac{2}{751}\right)\times\left[-\underbrace{\left(\frac{1}{3}\right)}_{=1}\right]\times\left[-\left(\frac{2}{7}\right)\right]$$

$$=-\left(\frac{2}{751}\right)\times\left(\frac{2}{7}\right)\qquad\left[\text{Because } -\times-\times-=-\right]$$

Testing for the integer 2 is given by:

$$(7.15)\qquad \left(\frac{2}{p}\right)=\begin{cases}1 & \text{if } p\equiv\pm 1\left(\text{mod } 8\right)\\ -1 & \text{if } p\equiv\pm 3\left(\text{mod } 8\right)\end{cases}$$

Since $751\equiv 7\equiv -1\left(\text{mod } 8\right)$ so $\left(\frac{2}{751}\right)=\left(\frac{2}{7}\right)=1$ and substituting this into the above

$$\left(\frac{751}{919}\right)=-\left(\frac{2}{751}\right)\times\left(\frac{2}{7}\right)=-1\times 1=-1$$

Since $\left(\frac{751}{919}\right)=-1$ so the quadratic congruence $x^2\equiv 715\left(\text{mod } 919\right)$ has *no* solutions

or the square root of $715\left(\text{mod } 919\right)$ does *not* exist.

(b) We need to evaluate the Legendre symbol $\left(\frac{123}{4567}\right)$.

$$\left(\frac{123}{4567}\right)=\left(\frac{3\times 41}{4567}\right)=\left(\frac{3}{4567}\right)\times\left(\frac{41}{4567}\right)\qquad (*)$$

Computing each of the Legendre symbols on the right – hand side:

$$\left(\frac{3}{4567}\right)\underbrace{=}_{\text{Because } 4567\equiv 3\left(\text{mod } 4\right)}-\left(\frac{4567}{3}\right)\underbrace{=}_{\text{Because } 4567\equiv 1\left(\text{mod } 3\right)}-\left(\frac{1}{3}\right)=-1\qquad\left[\begin{array}{l}\text{Because 1 is a}\\ \text{quadratic residue}\end{array}\right]$$

The other Legendre symbol is

$$\left(\frac{41}{4567}\right)\underbrace{=}_{\text{because } 41\equiv 1\left(\text{mod } 4\right)}\left(\frac{4567}{41}\right)\underbrace{=}_{\text{because } 4567\equiv 16\left(\text{mod } 41\right)}\left(\frac{16}{41}\right)=\left(\frac{4^2}{41}\right)=1$$

Substituting these evaluations into (*) gives

$$\left(\frac{123}{4567}\right)=\left(\frac{3}{4567}\right)\times\left(\frac{41}{4567}\right)=\left(-1\right)\times 1=-1$$

Hence the quadratic congruence $x^2\equiv 123\left(\text{mod } 4567\right)$ is *not* solvable.

(c) We need to evaluate $\left(\dfrac{7892}{1\,234\,567\,891}\right)$. Using the given hint and the multiplicative property of the Legendre symbol we have

$$\left(\frac{7892}{1\,234\,567\,891}\right)=\underbrace{\left(\frac{2^2}{1\,234\,567\,891}\right)}_{=1}\times\left(\frac{1973}{1\,234\,567\,891}\right)=\left(\frac{1973}{1\,234\,567\,891}\right)\qquad(*)$$

Using Corollary (7.17):

$$\left(\frac{p}{q}\right)=\begin{cases}\left(q/p\right) & \text{if } p\equiv 1\left(\text{mod } 4\right) \text{ or } q\equiv 1\left(\text{mod } 4\right)\\ -\left(q/p\right) & \text{if both } p\equiv 3\left(\text{mod } 4\right) \text{ and } q\equiv 3\left(\text{mod } 4\right)\end{cases}$$

On right – hand side gives

$$\left(\frac{1973}{1\,234\,567\,891}\right)\underbrace{=}_{\text{Because } 1973\equiv 1\left(\text{mod } 4\right)}\left(\frac{1\,234\,567\,891}{1973}\right)=\left(\frac{628}{1973}\right)$$
$$=\left(\frac{2^2\times 157}{1973}\right)=\underbrace{\left(\frac{2^2}{1973}\right)}_{=1}\times\left(\frac{157}{1973}\right)=\left(\frac{157}{1973}\right)\qquad(\dagger)$$

Using Corollary (7.17) to reduce the calculation further

$$\left(\frac{157}{1973}\right)\underbrace{=}_{\text{Because } 173\equiv 1\left(\text{mod } 4\right)}\left(\frac{1973}{157}\right)\underbrace{=}_{\text{Because } 1973\equiv 89\left(\text{mod } 157\right)}\left(\frac{89}{157}\right)$$
$$\underbrace{=}_{\text{Because } 89\equiv 1\left(\text{mod } 4\right)}\left(\frac{157}{89}\right)$$
$$\underbrace{=}_{\text{Because } 157\equiv 68\left(\text{mod } 89\right)}\left(\frac{68}{89}\right)$$
$$=\underbrace{\left(\frac{2^2}{89}\right)}_{=1}\times\left(\frac{17}{89}\right)=\left(\frac{17}{89}\right)=\left(\frac{89}{17}\right)\underbrace{=}_{89\equiv 4\left(\text{mod } 17\right)}\left(\frac{4}{17}\right)=\left(\frac{2^2}{17}\right)=1$$

Substituting this $\left(\dfrac{157}{1973}\right)=1$ into $(\dagger)$ gives

$$\left(\frac{1973}{1\,234\,567\,891}\right)=\left(\frac{157}{1973}\right)=1\,.$$

Putting this $\left(\frac{1973}{1\,234\,567\,891}\right)=1$ into (*) yields

$$\left(\frac{7892}{1\,234\,567\,891}\right)=\left(\frac{1973}{1\,234\,567\,891}\right)=1.$$

Hence 7892 is a quadratic residue of 1 234 567 891, that is the quadratic

$$x^2\equiv 7892\left(\mathrm{mod}\ 1\,234\,567\,891\right) \text{ has solutions.}$$

6. We are asked to find the first primitive root of modulo 97. We are given that 97 is prime so $\phi\left(97\right)=96$. The prime factorization of 96 is $96=2^5\times 3$ and the factors of 96 are 1, 2, 3, 4, 6, 8, 12, 16, 24, 32, 48 and 96.
We only need to test the 32 and 48 as the index since all the others (1, 2, 3, 4, 6, 8, 12, 16, 24) are factors of 48.

If r is a primitive root of modulo 97 then $r^{32}\not\equiv 1\left(\mathrm{mod}\ 97\right)$ and $r^{48}\not\equiv 1\left(\mathrm{mod}\ 97\right)$.

Note that if $p=97$ then

$$\frac{p-1}{2}=\frac{97-1}{2}=48$$

We trial $r=2$ and test $2^{48}\equiv x\left(\mathrm{mod}\ 97\right)$. This is given by Euler's criterion because Euler's Criterion says:

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

Hence, we test the Legendre symbol $\left(\frac{2}{97}\right)$. Since $97\equiv 1\left(\mathrm{mod}\ 8\right)$ so 2 is a quadratic residue of 97 because

(7.15) $$\left(\frac{2}{p}\right)=\begin{cases}1 & \text{if } p\equiv\pm 1\left(\mathrm{mod}\ 8\right)\\ -1 & \text{if } p\equiv\pm 3\left(\mathrm{mod}\ 8\right)\end{cases}$$

Therefore $2^{48}\equiv 1\left(\mathrm{mod}\ 97\right)$ so 2 cannot be a primitive root of modulo 97. We don't need to test whether $2^{32}\equiv 1\left(\mathrm{mod}\ 97\right)$ because 2 cannot be a primitive root of 97.

Next, we trial $r=3$ and evaluate the Legendre symbol $\left(\frac{3}{97}\right)$.

$$\left(\frac{3}{97}\right)\underbrace{=}_{\text{Because } 97\equiv 1\left(\mathrm{mod}\ 4\right)}\left(\frac{97}{3}\right)\underbrace{=}_{\text{Because } 97\equiv 1\left(\mathrm{mod}\ 3\right)}\left(\frac{1}{3}\right)=1$$

Therefore 3 is a quadratic residue which implies that $3^{48} \equiv 1 \pmod{97}$ so 3 *cannot* be a primitive root of 97.

Clearly $r = 4$ is not a primitive root of modulo 97 because 4 is a square number so it is a quadratic residue of 97 which implies $4^{48} \equiv 1 \pmod{97}$.

Now we trial $r = 5$:

$$\left(\frac{5}{97}\right) \underset{\text{Because } 97 \equiv 1 \pmod 4}{=} \left(\frac{97}{5}\right) \underset{\text{Because } 97 \equiv 2 \pmod 5}{=} \left(\frac{2}{5}\right) = -1$$

Hence 5 is a quadratic non – residue of 97. This time we need to test

$$5^{32} \equiv x \pmod{97}$$

because 5 could be a first primitive root of 97.

$$5^3 \equiv 125 \equiv 28 \pmod{97}$$

$$5^6 \equiv \left(5^3\right)^2 \equiv 28^2 \equiv 784 \equiv 8 \pmod{97}$$

Using these to evaluate $5^{32} \equiv x \pmod{97}$:

$$5^{32} \equiv 5^{30} \times 5^2 \equiv \left(5^6\right)^5 \times 25 \equiv 8^5 \times 25 \equiv 819\,200 \equiv 35 \pmod{97} \qquad (\ddagger)$$

Since $5^{32} \equiv 35 \not\equiv 1 \pmod{97}$ so 5 is a primitive root of 97.

We need to use this primitive 5 to find the square root of $35 \pmod{97}$ which means we need to solve $x^2 \equiv 35 \pmod{97}$. Since the result $(\ddagger)$ shows

$$5^{32} \equiv 35 \pmod{97}$$

and we are asked to solve $x^2 \equiv 35 \pmod{97}$ so let $x = 5^{16}$. Then

$$x^2 \equiv 35 \pmod{97} \;\Rightarrow\; x \equiv \pm 5^{16} \pmod{97}.$$

Therefore the square roots of $35 \pmod{97}$ are given by

$$\begin{aligned} x \equiv \pm 5^{16} &\equiv \pm\left[\left(5^6\right)^2 \times 5^4\right] \\ &\equiv \pm\left[8^2 \times 625\right] \equiv \pm\left[64 \times 43\right] \equiv \pm 2752 \equiv \pm 36 \equiv 36, -36 \equiv 36, 61 \pmod{97} \end{aligned}$$

Hence the solutions to $x^2 \equiv 35 \pmod{97}$ are $x \equiv 36,\ 61 \pmod{97}$ which implies that the square roots of $35 \pmod{97}$ are $36,\ 61 \pmod{97}$.

7. We are asked to find a primitive root of modulo 101. We are given that 101 is prime so $\phi\left(101\right)=100$. The prime factorization of 100 is $100=2^2\times5^2$ and the positive factors of 100 are 1, 2, 4, 5, 10, 20, 25, 50 and 100.

We only need to test 20 and 50 as the index because 1, 2, 5, 10 and 25, are factors of 50 and 4 is a factor of 20.

If r is a primitive root of modulo 101 then $r^{20}\not\equiv1\left(\mathrm{mod}\,101\right)$ and $r^{50}\not\equiv1\left(\mathrm{mod}\,101\right)$.

Note that if $p=101$ then

$$\frac{101-1}{2}=50$$

We trial $r=2$ and test $2^{50}\equiv x\left(\mathrm{mod}\,101\right)$. This is given by Euler's criterion:

a is a quadratic residue of $p \Leftrightarrow a^{\frac{p-1}{2}}\equiv1\left(\mathrm{mod}\ p\right)$.

Hence, we test the Legendre symbol $\left(\frac{2}{101}\right)$. Since $101\equiv5\left(\mathrm{mod}\,8\right)$ so 2 is a quadratic non - residue of 101 because

(7.15) $$\left(\frac{2}{p}\right)=\begin{cases}1 & \text{if } p\equiv\pm1\left(\mathrm{mod}\,8\right)\\ -1 & \text{if } p\equiv\pm3\left(\mathrm{mod}\,8\right)\end{cases}$$

Therefore $2^{50}\equiv-1\not\equiv1\left(\mathrm{mod}\,101\right)$ so 2 could be a primitive root of modulo 101. We need to test whether $2^{20}\equiv1\left(\mathrm{mod}\,101\right)$ because if this is true then 2 *cannot* be a primitive root of 101. Computing a simpler power of 2:

$$2^{10}\equiv1024\equiv14\left(\mathrm{mod}\,101\right)\qquad(\S)$$

$$2^{20}\equiv\left(2^{10}\right)^2\equiv14^2\equiv196\equiv95\not\equiv1\left(\mathrm{mod}\,101\right)$$

Since $2^{20}\equiv95\not\equiv1\left(\mathrm{mod}\,101\right)$ and $2^{50}\equiv-1\not\equiv1\left(\mathrm{mod}\,101\right)$ so 2 is a primitive root of 101.

(a) We need to solve the non – linear Diophantine equation $x^2-101y=14$. We can express this as a quadratic congruence $x^2\equiv14\left(\mathrm{mod}\,101\right)$ and solve this. Using the primitive root 2 of modulo 101 we have, by using index to the base 2:

$$\mathrm{ind}_2\left(x^2\right)\equiv\mathrm{ind}_2\left(14\right)\left(\mathrm{mod}\,100\right)$$
$$2\times\mathrm{ind}_2\left(x\right)\equiv\mathrm{ind}_2\left(14\right)\left(\mathrm{mod}\,100\right)$$

By the above calculation (§) we have $\mathrm{ind}_2\left(14\right)=10$. Putting this in gives

$$2\times \text{ind}_2\left(x\right)\equiv 10\left(\text{mod } 100\right) \;\Rightarrow\; \text{ind}_2\left(x\right)\equiv 5\left(\text{mod } 50\right) \;\Rightarrow\; \text{ind}_2\left(x\right)\equiv 5,\; 55\left(\text{mod } 100\right)$$

Therefore, from the last calculation $\text{ind}_2\left(x\right)\equiv 5,\; 55\left(\text{mod } 100\right)$ we have

$$x\equiv 2^5,\; 2^{55}\left(\text{mod } 101\right)$$

Again, we don't need to work out $x\equiv 2^{55}\left(\text{mod } 101\right)$ because the square roots of $14\left(\text{mod } 101\right)$ are given by

$$x\equiv \pm 2^5 \equiv \pm 32\equiv 32,\; 69\left(\text{mod } 101\right)$$

Substituting the simplest of these $x\equiv 32,\; 69\left(\text{mod } 101\right)$ which is $x=32, 69$ into the given Diophantine equation $x^2-101y=14$ gives

$$y=\frac{x^2-14}{101}=\frac{32^2-14}{101},\; \frac{69^2-14}{101}=10,\; 47$$

Two solutions to the given Diophantine equation are

$$\left\{x=32,\; y=10\right\} \text{ and } \left\{x=69,\; y=47\right\}.$$

(b) We need to solve the non – linear Diophantine equation $x^2-101y=22$. We can express this as a quadratic congruence $x^2\equiv 22\left(\text{mod } 101\right)$ and solve this. Using the primitive root 2 of modulo 101 we have

$$2\times \text{ind}_2\left(x\right)\equiv \text{ind}_2\left(22\right)\left(\text{mod } 100\right) \qquad (\ddagger)$$

We need to find a power of 2 which gives 22 modulo 101. Evaluating powers of 2 gives

$$2^{11}\equiv 2^{10}\times 2\equiv 14\times 2\equiv 28\left(\text{mod } 101\right)$$

$$2^{12}\equiv 2^{11}\times 2\equiv 28\times 2\equiv 56\left(\text{mod } 101\right)$$

$$2^{13}\equiv 2^{12}\times 2\equiv 56\times 2\equiv 11\left(\text{mod } 101\right)$$

Since $22=2\times 11$ so by using the last computation we have

$$2^{14}\equiv 2^{13}\times 2\equiv 11\times 2\equiv 22\left(\text{mod } 101\right)$$

As $2^{14}\equiv 22\left(\text{mod } 101\right)$ so $\text{ind}_2\left(22\right)=14$. Substituting this into (‡) gives

$$2\times \text{ind}_2\left(x\right)\equiv 14\left(\text{mod } 100\right)$$

We can solve this congruence because $2\,|\,14$. Dividing by 2 yields

$$\text{ind}_2\left(x\right)\equiv 7\left(\text{mod } 50\right) \;\Rightarrow\; \text{ind}_2\left(x\right)\equiv 7,\ 57\left(\text{mod } 100\right)$$

From this $\text{ind}_2\left(x\right)\equiv 7,\ 57\left(\text{mod } 100\right)$ we have

$$x\equiv 2^7,\ 2^{57}\equiv\pm 2^7\equiv\pm 128\equiv\pm 27\equiv 27,\ 74\left(\text{mod } 101\right)$$

The simplest of these is $x=27,\ 74$, substituting these into $x^2-101y=22$ and re-arranging gives

$$y=\frac{x^2-22}{101}=\frac{27^2-22}{101},\ \frac{74^2-22}{101}=7,\ 54$$

Hence our solutions to the given Diophantine equation $x^2-101y=22$ are

$$\left\{x=27,\ y=7\right\} \text{ and } \left\{x=74,\ y=54\right\}$$

(c) We need to solve the non – linear Diophantine equation $x^2-101y=44$. We need to solve $2\times\text{ind}_2\left(x\right)\equiv\text{ind}_2\left(44\right)\left(\text{mod } 100\right)$. From calculation of part (b) we have $2^{14}\equiv 2^{13}\times 2\equiv 11\times 2\equiv 22\left(\text{mod } 101\right)$ therefore

$$2^{15}\equiv 2^{14}\times 2\equiv 22\times 2\equiv 44\left(\text{mod } 101\right)$$

Hence $\text{ind}_2\left(44\right)=15$ and substituting this into $2\times\text{ind}_2\left(x\right)\equiv\text{ind}_2\left(44\right)\left(\text{mod } 100\right)$:

$$2\times\text{ind}_2\left(x\right)\equiv 15\left(\text{mod } 100\right)$$

However, the $\gcd\left(2,\ 100\right)=2$ and $2\not|\ 15$ so the above congruence has no solutions. This means that 44 is a quadratic non – residue of 101.

The given Diophantine equation $x^2-101y=44$ has *no* solutions.

8. We need to show that $\left(\frac{-1}{p}\right)=\left(-1\right)^{\frac{p^2-1}{4}}$ is false. *How?*

Produce an example where this result is false.

Let $p=11$ then

$$\left(\frac{-1}{11}\right)=\left(-1\right)^{\frac{11^2-1}{4}}=\left(-1\right)^{30}=1.$$

Hence this implies that -1 is a quadratic residue of 11.

Since $11\equiv 3\left(\text{mod } 4\right)$ so by applying Proposition (7.11):

$$\left(\frac{-1}{p}\right)=\begin{cases}1 & \text{if } p\equiv 1\pmod 4\\ -1 & \text{if } p\equiv 3\pmod 4\end{cases}$$

We have $\left(\frac{-1}{11}\right)=-1$ which implies that -1 is a quadratic non – residue of 11.

9. We need to find the primes $p>3$ for which 3 is a quadratic residue modulo p.

We consider the Legendre symbol $\left(\frac{3}{p}\right)$. By using Corollary (7.17):

$$\left(\frac{p}{q}\right)=\begin{cases}\left(q/p\right) & \text{if } p\equiv 1\pmod 4 \text{ or } q\equiv 1\pmod 4\\ -\left(q/p\right) & \text{if both } p\equiv 3\pmod 4 \text{ and } q\equiv 3\pmod 4\end{cases}$$

Any odd prime p satisfies $p\equiv 1$ or $3\pmod 4$. Considering these two cases.

Case I: If $p\equiv 1\pmod 4$ then $\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)$ and this is equal to 1 provided $p\equiv 1\pmod 3$ because

$$\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)=\left(\frac{1}{3}\right)=1 \text{ as 1 is always a quadratic residue.}$$

Hence one solution that gives 3 is a quadratic residue of p is when p satisfies both the conditions

$$p\equiv 1\pmod 4 \text{ and } p\equiv 1\pmod 3$$

Using the result of Chinese Remainder Theorem of question 8(c) of Exercises 3.4:

$$a\equiv b\pmod{m_k} \;\Leftrightarrow\; a\equiv b\pmod{\left[m_1,\ m_2,\ \cdots,\ m_n\right]}$$

Hence $p\equiv 1\pmod{3\times 4}\equiv 1\pmod{12}$.

Case II: If $p\equiv 3\pmod 4$ then $\left(\frac{3}{p}\right)=-\left(\frac{p}{3}\right)$. *How can 3 be a quadratic residue of p?*

When $\left(\frac{p}{3}\right)=-1$ and this is the case when $p\equiv 2\pmod 3$ because

(7.15) $$\left(\frac{2}{p}\right)=\begin{cases}1 & \text{if } p\equiv \pm 1\pmod 8\\ -1 & \text{if } p\equiv \pm 3\pmod 8\end{cases}$$

Hence

$$\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1 \text{ provided } p \equiv 3\left(\text{mod } 4\right) \text{ and } p \equiv 2\left(\text{mod } 3\right)$$

We need to find prime p which satisfies both these conditions. Using the Chinese Remainder Theorem formula:

(3.23) $$x = a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 + \cdots + a_rN_rx_r$$

We have

$$p \equiv a_1x_1N_1 + a_2N_2x_2 \ \left(\text{mod } 3\times 4\right) \qquad (*)$$

We have $N_1 = 3,\ N_2 = 4$ and

$$3x_1 \equiv 1\left(\text{mod } 4\right) \ \Rightarrow \ x_1 = 3$$

$$4x_2 \equiv 1\left(\text{mod } 3\right) \ \Rightarrow \ x_2 = 1$$

Substituting $N_1 = 3,\ N_2 = 4,\ x_1 = 3,\ x_2 = 1,\ a_1 = 3,\ a_2 = 2$ into (*) gives

$$p \equiv \left(3\times 3\times 3\right) + \left(2\times 4\times 1\right) \equiv 35 \equiv -1 \ \left(\text{mod } 12\right)$$

Hence 3 is a quadratic residue of p provided $p \equiv -1 \ \left(\text{mod } 12\right)$.

Summarizing both these results we have 3 is a quadratic residue or we can find the square root of $3\left(\text{mod } p\right)$ if and only if $p \equiv \pm 1\left(\text{mod } 12\right)$.

(ii) (a) We need to factorize $306^2 - 3 = 93\,633$. Clearly 3 is a factor and

$$\frac{93\,633}{3} = 31\,211 \text{ or } 93\,633 = 3\times 31\,211.$$

Since the integer looks like $x^2 - 3$ so other odd prime factors p must satisfy $p \equiv \pm 1\left(\text{mod } 12\right)$. The first few primes of this format are 11, 13, 23, 37, 47, 59, 61, … . Trialling these primes gives

$$\frac{31\,211}{11} = 2837.36\left(2\text{dp}\right)$$

$$\frac{31\,211}{13} = 2400.85\left(2\text{dp}\right)$$

$$\frac{31\,211}{23} = 1357$$

Hence $31\,211 = 23\times 1357$. We still need to factorize 1357. Again it must have prime factors which satisfy $p \equiv \pm 1\left(\text{mod } 12\right)$ and also it has to have a prime

factor which is less than or equal to $\left\lfloor\sqrt{1357}\right\rfloor = 36$ and the only prime left to trial is 23 again:

$$\frac{1357}{23} = 59 \quad \Rightarrow \quad 1357 = 23 \times 59$$

Putting all this together we have

$$\begin{aligned} 306^2 - 3 &= 93\,633 \\ &= 3 \times 31\,211 \\ &= 3 \times 23 \times 1357 = 3 \times 23 \times 23 \times 59 = 3 \times 23^2 \times 59 \end{aligned}$$

Our prime factorization of $306^2 - 3 = 93\,633$ is $3 \times 23^2 \times 59$.

(b) We are asked to factorize $214^2 - 3 = 45\,793$. Again the odd prime factors p of this number 45 793 satisfy $p \equiv \pm 1 \left(\mathrm{mod}\, 12\right)$. The first few primes of this format are 11, 13, 23, 37,… . Trialling the first of these, 11, gives

$$\frac{45\,793}{11} = 4163 \quad \text{or} \quad 45\,793 = 4163 \times 11.$$

By the 11 test we know 11 does not go into 4163 so we trial the next prime of the above format which is 13:

$$\frac{4163}{13} = 320.23\,(2\mathrm{dp})$$

So, 13 is not a factor so we trial the next prime which is 23:

$$\frac{4163}{23} = 181 \quad \text{which implies} \quad 4163 = 23 \times 181.$$

We only need to factorize 181. Well $\left\lfloor\sqrt{181}\right\rfloor = 13$ and any prime factor of 181 must also satisfy $p \equiv \pm 1 \left(\mathrm{mod}\, 12\right)$ but none of them do as we have checked above, so 181 is prime. Hence

$$214^2 - 3 = 45\,793 = 11 \times 4163 = 11 \times 23 \times 181.$$

(c) We asked to factorize $602^2 - 3 = 362\,401$. Let p be a prime factor of this number then $p \equiv \pm 1 \left(\mathrm{mod}\, 12\right)$. Trialling the first few primes of this format which are 11, 13, 23, 37, 47, 59, 61, … . Clearly 11 is not a factor of $362\,401$ because of the well – known 11 test which we established in Chapter 3. The next prime is 13 and we have

$$\frac{362\,401}{13} = 27\,877 \text{ implies } 362\,401 = 13 \times 27\,877$$

Trialling 13 again gives

$$\frac{27\ 877}{13} = 2144.38\left(2\text{dp}\right)$$

Trying the next few primes 23, 37, 47, 59 we find that these are *not* factors. However, trying 61 gives

$$\frac{27\ 877}{61} = 457 \text{ which implies } 27\ 877 = 61\times 457$$

Now $\left\lfloor\sqrt{457}\right\rfloor = 21$ and none of the primes which are $\pm 1\left(\text{mod}\,12\right)$ and below 21, that is 11 and 13 go into 457 otherwise they would have been factors earlier on. Hence 457 is prime. Therefore

$$602^2 - 3 = 362\ 401 = 13\times 27\ 877 = 13\times 61\times 457$$

10. In order to solve the given Diophantine equations we first solve the equivalent quadratic congruence.

(a) We are asked to solve $x^2 + 11y = 5$ which we can rewrite as

$$x^2 = 5 - 11y = 5 + 11\left(-y\right) \text{ implies } x^2 \equiv 5\left(\text{mod}\,11\right)$$

First, we test whether 5 is a quadratic residue of modulo 11 by computing the Legendre symbol $\left(\frac{5}{11}\right)$:

$$\left(\frac{5}{11}\right) = \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1 \quad \left[\text{Because 1 is always a QR}\right]$$

Therefore 5 is a quadratic residue of 11 and by trial and error we have

$$x^2 \equiv 5\left(\text{mod}\,11\right) \Rightarrow x \equiv \pm 4 \equiv 4, 7\left(\text{mod}\,11\right)$$

Substituting $x = 4$ and $x = 7$ into the above quadratic $x^2 = 5 + 11\left(-y\right)$ gives

$$4^2 = 16 = 5 + 11\left(-y\right) \Rightarrow y = \frac{5-16}{11} = -1$$

$$7^2 = 49 = 5 + 11\left(-y\right) \Rightarrow y = \frac{5-49}{11} = -4$$

Hence a pair of solutions are $x = 4,\ y = -1$ and $x = 7,\ y = -4$.

(b) Similarly, we solve $x^2 + 23y = 2$. Rewriting this

$$x^2 = 2 - 23y = 2 + 23\left(-y\right)$$

Computing the Legendre symbol $\left(\frac{2}{23}\right)$ by using

(7.15) $$\left(\frac{2}{p}\right)=\begin{cases}1 & \text{if } p\equiv\pm1\left(\text{mod } 8\right)\\ -1 & \text{if } p\equiv\pm3\left(\text{mod } 8\right)\end{cases}$$

With $23\equiv-1\left(\text{mod } 8\right)$ so 2 is a quadratic residue of 23. Clearly

$$5^2\equiv25\equiv2\left(\text{mod } 23\right)$$

Therefore, our solutions are $x\equiv\pm5\equiv5,\ 18\left(\text{mod } 23\right)$.

Substituting $x=5,\ 18$ into $x^2=2+23\left(-y\right)$ and transposing gives

$$5^2=25=2+23\left(-y\right)\ \Rightarrow\ y=\frac{2-25}{23}=-1$$

$$18^2=324=2+23\left(-y\right)\ \Rightarrow\ y=\frac{2-324}{23}=-14$$

Particular solutions are $x=5,\ y=-1$ and $x=18,\ y=-14$.

(c) Solving $x^2+53y=-1$ in a similar manner. Re-arranging this

$$x^2=-1+53\left(-y\right)$$

Since $53\equiv1\left(\text{mod } 4\right)$ so by Proposition (7.11):

$$\left(\frac{-1}{p}\right)=\begin{cases}1 & \text{if } p\equiv1\left(\text{mod } 4\right)\\ -1 & \text{if } p\equiv3\left(\text{mod } 4\right)\end{cases}$$

We conclude that $\left(\frac{-1}{53}\right)=1$ which implies that -1 is a quadratic residue of 53.

We can solve the quadratic congruence $x^2\equiv-1\left(\text{mod } 53\right)$. First we need to find a primitive root of 53. We have $\phi\left(53\right)=52$ and the positive factors of 52 are 1, 2, 4, 13, 26 and 52. We only need to test the factors 4 and 26 as 26 includes 2 and 13.

We trial $r=2$. We need to show that $2^{26}\not\equiv1\left(\text{mod } 53\right)$ and $2^4\not\equiv1\left(\text{mod } 53\right)$.

Clearly $2^4\equiv8\not\equiv1\left(\text{mod } 53\right)$ so we are left to evaluate $2^{26}\equiv x\left(\text{mod } 53\right)$. We have

$$2^6\equiv64\equiv11\left(\text{mod } 53\right)$$

$$2^{12}\equiv11^2\equiv121\equiv15\left(\text{mod } 53\right)\qquad(\ddagger)$$

$$2^{24}\equiv15^2\equiv225\equiv13\left(\text{mod } 53\right)$$

Using this last result, we have

$$2^{26}\equiv2^{24}\times2^2\equiv13\times4\equiv52\equiv-1\not\equiv1\left(\text{mod } 53\right)\qquad(*)$$

Therefore 2 is a primitive root of 53.

By (*) we have $2^{26} \equiv -1 \pmod{53}$ and we need to solve $x^2 \equiv -1 \pmod{53}$. Let $x = 2^{13}$ then

$$x^2 \equiv 2^{26} \equiv -1 \pmod{53} \Rightarrow x \equiv \pm 2^{13} \pmod{53}.$$

By (‡) we have

$$2^{12} \equiv 15 \pmod{53} \Rightarrow 2^{13} \equiv 2 \times 15 \equiv 30 \pmod{53}$$

Our two solutions are $x \equiv \pm 30 \equiv 30, -30 \equiv 30, 23 \pmod{53}$. Writing our solutions in ascending order gives $x \equiv 23, 30 \pmod{53}$.

Substituting $x = 23, 30$ into $x^2 = -1 + 53(-y)$ and transposing yields

$$23^2 = 529 = -1 + 53(-y) \Rightarrow y = \frac{-1-529}{53} = -10$$

$$30^2 = 900 = -1 + 53(-y) \Rightarrow y = \frac{-1-900}{53} = -17$$

Particular solutions are $x = 23, y = -10$ and $x = 30, \ y = -17$.

11. (a) We are asked to prove there are infinitely many primes of the form $8k + 3$.

Proof.

Let n be any natural number. Consider the number

$$N = \left[3 \times 5 \times 7 \times \cdots \times (2n+1)\right]^2 + 2 \qquad (*)$$

The product in N is odd therefore we have $N \equiv 3 \pmod{8}$. If *all* the prime divisors of N are of the form $8k \pm 1$ then so is N (you can easily show this by mathematical induction). Hence N has a prime divisor p which satisfies $p \equiv \pm 3 \pmod{8}$. We have

$$N \equiv 0 \pmod{p} \Rightarrow N = \left[3 \times 5 \times \cdots \times (2n+1)\right]^2 + 2 \equiv 0 \pmod{p}$$
$$\Rightarrow \left[3 \times 5 \times \cdots \times (2n+1)\right]^2 \equiv -2 \pmod{p}$$

We need to show that the only primes p which satisfy this quadratic

$$\left[3 \times 5 \times 7 \times \cdots \times (2n+1)\right]^2 \equiv -2 \pmod{p}$$

are of the form $p \equiv 3 \pmod{8}$ because we want to show infinitely many primes of the form $8k + 3$.

By question 9 of Exercises 7.3 the Legendre symbol

$$\left(\frac{-2}{p}\right)=\begin{cases}1 & \text{if } p\equiv 1 \text{ or } 3\pmod 8\\ -1 & \text{if } p\equiv -1 \text{ or } -3\pmod 8\end{cases}$$

Hence the prime p which is a divisor of N is of the form $p\equiv 3\pmod 8$ or $p=8k+3$. Now this p is greater than n in (*) and n is an arbitrary natural number so we can find primes of the form $p=8k+3$ greater than any natural number. This completes our proof.

■

(b) We are asked to prove there are infinitely many primes of the form $8k-3$.

Proof.

Let n be any natural number and consider the number

$$N=\left[3\times 5\times 7\times\cdots\times(2n+1)\right]^2+4$$

The square term in N is odd because it is the product of odd numbers. Therefore

$$N=\left[3\times 5\times 7\times\cdots\times(2n+1)\right]^2+4\equiv 5\equiv -3\pmod 8$$

N has a prime divisor p which satisfies $p\equiv\pm 3\pmod 8$. *Why?*

Suppose *all* the prime factors p of $N\equiv -3\pmod 8$ satisfy $p\equiv\pm 1\pmod 8$ then

$$(8k\pm 1)(8m\pm 1)=64km\pm 8(k+m)+1=8\ell+1,$$

which implies that $N\equiv 1\pmod 8$ which it isn't.

We have

$$N=\left[3\times 5\times\cdots\times(2n+1)\right]^2+4\equiv 0\pmod p\ \Rightarrow\ \left[3\times 5\times\cdots\times(2n+1)\right]^2\equiv -4\pmod p$$

Now the primes for which -4 is a quadratic residue is when the Legendre symbol $\left(\frac{-4}{p}\right)=1$. Thus

$$\left(\frac{-4}{p}\right)=\left(\frac{-1}{p}\right)\times\left(\frac{4}{p}\right)=\left(\frac{-1}{p}\right)\times\underbrace{\left(\frac{2^2}{p}\right)}_{=1}=\left(\frac{-1}{p}\right).$$

Now by Proposition (7.11):

> Let p be an odd prime. Then $\left(\frac{-1}{p}\right)=\begin{cases}1 & \text{if } p\equiv 1\pmod 4\\ -1 & \text{if } p\equiv 3\pmod 4\end{cases}$.

Hence $p\equiv 1\pmod 4$ and from above we have $p\equiv\pm 3\pmod 8$. Combining these together, $p\equiv 1\pmod 4$ and $p\equiv\pm 3\pmod 8$, gives $p\equiv -3\pmod 8$ because

$$p \equiv 3 \pmod 8 = 8k+3 \equiv 3 \pmod 4 .$$

Since $p > n$ for any arbitrary n we have an infinitely many primes of the form $p \equiv -3 \pmod 8$ or $8k-3$.

■

12. We are asked to show that if p is a prime of the form $4k+3$ and a, b are integers such that $a^2 + b^2 \equiv 0 \pmod p$ then $a \equiv b \equiv 0 \pmod p$.

Proof.

Suppose $b \not\equiv 0 \pmod p$ which implies $p \nmid b$. From $a^2 + b^2 \equiv 0 \pmod p$ we have

$$a^2 \equiv -b^2 \pmod p$$

The Legendre symbol

$$\left(\frac{-b^2}{p}\right) = \left(\frac{-1}{p}\right) \times \underbrace{\left(\frac{b^2}{p}\right)}_{=1 \text{ because } b^2 \text{ is a QR}} = \left(\frac{-1}{p}\right) \underbrace{=}_{\text{Because } p \equiv 3 \pmod 4} -1$$

The last step follows from the fact that we are given $p = 4k+3 \equiv 3 \pmod 4$ and by Proposition (7.11):

> Let p be an odd prime. Then $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$.

Hence $-b^2$ is a quadratic non – residue of p. There are *no* solutions to

$$a^2 \equiv -b^2 \pmod p$$

Therefore, there are *no* solutions to $a^2 + b^2 \equiv 0 \pmod p$ or $a^2 + b^2 \not\equiv 0 \pmod p$.

This is a contradiction because we are given $a^2 + b^2 \equiv 0 \pmod p$. So $b \equiv 0 \pmod p$.

Similarly, we have $a \equiv 0 \pmod p$.

■

13. (a) We need to write 313 as sum of two squares but we first need to check that this is congruent to 1 modulo 4:

$$313 \equiv 1 \pmod 4$$

Thus, we can express 313 as sum of two squares;

$$313 = a^2 + b^2 \;\Rightarrow\; b = \sqrt{313 - a^2}$$

We substitute integer values for a in this $b = \sqrt{313 - a^2}$ and stop once b is an integer:

$$b = \sqrt{313 - 2^2} = \sqrt{309}$$
$$b = \sqrt{313 - 3^2} = \sqrt{304}$$
$$b = \sqrt{313 - 4^2} = \sqrt{297}$$
$$b = \sqrt{313 - 5^2} = \sqrt{288}$$
$$b = \sqrt{313 - 6^2} = \sqrt{277}$$
$$b = \sqrt{313 - 7^2} = \sqrt{264}$$
$$b = \sqrt{313 - 8^2} = \sqrt{249}$$
$$b = \sqrt{313 - 9^2} = \sqrt{232}$$
$$b = \sqrt{313 - 10^2} = \sqrt{213}$$
$$b = \sqrt{313 - 11^2} = \sqrt{192}$$
$$b = \sqrt{313 - 12^2} = \sqrt{169} = 13$$

Therefore $313 = 12^2 + 13^2$. We will describe a more systematic way to write a given integer as the sum of two squares in the next chapter.

(b) Similarly, we have $1237 \equiv 1 \pmod 4$ so we express 1237 as the sum of two squares. By transposing

$$1237 = a^2 + b^2 \;\Rightarrow\; b = \sqrt{1237 - a^2}$$

Using brute force calculation, we have

$$b = \sqrt{1237 - 9^2} = 34$$

Therefore $1237 = 9^2 + 34^2$.

(c) First $1249 \equiv 1 \pmod 4$ so we can express 1249 as the sum of two squares:

$$1249 = a^2 + b^2 \;\Rightarrow\; b = \sqrt{1249 - a^2}$$

By substituting various integers for a we have

$$b = \sqrt{1249 - 15^2} = 32$$

Therefore $1249 = 15^2 + 32^2$.

14. We need to show that there are integers a, b such that $p = a^2 + 2b^2 \Leftrightarrow$ $p \equiv 1 \text{ or } 3 \pmod 8$.

Proof.

Assume there are integers a, b such that $p = a^2 + 2b^2$. Thus, we have

$$a^2 + 2b^2 \equiv 0 \pmod p \Rightarrow a^2 \equiv -2b^2 \pmod p.$$

From the last step $a^2 \equiv -2b^2 \pmod p$ we have $-2b^2$ is a quadratic residue of the prime p. The Legendre symbol of this $\left(\frac{-2b^2}{p}\right) = 1$ therefore

$$\left(\frac{-2b^2}{p}\right) = \left(\frac{-2}{p}\right) \times \underbrace{\left(\frac{b^2}{p}\right)}_{=1} = \left(\frac{-2}{p}\right) = 1$$

Hence -2 is a quadratic residue of modulo p. By question 9(ii) of Exercises 7.3:

If $p \mid (x^2 + 2)$ then $p \equiv 1, 3 \pmod 8$.

We conclude that $p \equiv 1 \text{ or } 3 \pmod 8$.

(a) Since $p = 211 \equiv 3 \pmod 8$ we have -2 is a quadratic residue of 211.

Writing 211 as $p = a^2 + 2b^2$ by first transposing gives

$$a^2 + 2b^2 = 211 \Rightarrow b = \sqrt{\frac{211 - a^2}{2}}$$

Substituting odd integers for a because if a is even then 211 take away even is odd and we need to divide by 2. Trialling $a = 1, 3, 5, 7, 9, 11, 13$ and stopping when b is an integer, we have

$$b = \sqrt{\frac{211 - 1^2}{2}} = \sqrt{\frac{210}{2}} = \sqrt{105}$$

$$b = \sqrt{\frac{211 - 3^2}{2}} = \sqrt{\frac{202}{2}} = \sqrt{101}$$

$$b=\sqrt{\frac{211-5^2}{2}}=\sqrt{\frac{186}{2}}=\sqrt{93}$$

$$b=\sqrt{\frac{211-7^2}{2}}=\sqrt{\frac{162}{2}}=\sqrt{81}=9$$

Hence we have $a=7, b=9$ and checking this $7^2+2\left(9\right)^2=211$.

(b) Similarly, we have $1019\equiv 3\left(\text{mod } 8\right)$ this means we can write $1019=a^2+2b^2$ but we need to find a and b. We have

$$a^2+2b^2=1019 \;\Rightarrow\; b=\sqrt{\frac{1019-a^2}{2}}$$

Again, substituting odd integers for a we find that when $a=21$ we have

$$b=\sqrt{\frac{1019-21^2}{2}}=\sqrt{289}=17$$

Therefore $1019=21^2+2\left(17\right)^2$.

(c) We have $1249\equiv 1\left(\text{mod } 8\right)$ so we can write 1249 as a^2+2b^2. Finding a and b by brute force calculation:

$$a^2+2b^2=1249 \;\Rightarrow\; b=\sqrt{\frac{1249-a^2}{2}}$$

Substituting odd numbers for a and stopping once b is an integer, we have

$$b=\sqrt{\frac{1249-31^2}{2}}=\sqrt{144}=12$$

We have $1249=31^2+2\left(12\right)^2$.

15. We are asked to show that $\left(\frac{-2}{p}\right)=\left(-1\right)^{\frac{\left(p+5\right)\left(p-1\right)}{8}}$.

Proof.

By the multiplicative property of the Legendre symbol we have

$$\left(\frac{-2}{p}\right)=\left(\frac{-1\times 2}{p}\right)=\left(\frac{-1}{p}\right)\times\left(\frac{2}{p}\right)=\underbrace{\left(-1\right)^{\frac{p-1}{2}}}_{\text{By Question 8 of Exercises 7(b)}}\times\underbrace{\left(-1\right)^{\frac{p^2-1}{8}}}_{\text{By Corollary (7.18)}}$$

$$\underbrace{=}_{\text{By the rules of indices}}\left(-1\right)^{\frac{p-1}{2}+\frac{p^2-1}{8}}$$

$$=\left(-1\right)^{\frac{4p-4+p^2-1}{8}}=\left(-1\right)^{\frac{p^2+4p-5}{8}}=\left(-1\right)^{\frac{\left(p+5\right)\left(p-1\right)}{8}}$$

Substituting $p = 1\,000\,003$ into the given result $\left(\frac{-2}{p}\right) = (-1)^{\frac{(p+5)(p-1)}{8}}$ yields

$$\left(\frac{-2}{1\,000\,003}\right) = (-1)^{\frac{(1\,000\,003+5)\times(1\,000\,003-1)}{8}} = (-1)^{\frac{(1\,000\,008)\times(1\,000\,002)}{8}} \underbrace{=}_{\substack{\text{Because 1 000 008 is a mutiple of 8} \\ \text{and 1 000 002 is even}}} 1$$

Hence -2 is a quadratic residue of 1 000 003.

16. We are asked to prove that $x^4 \equiv -1 \pmod{p}$ has a solution $\Leftrightarrow p \equiv 1 \pmod{8}$.

Proof.

$(\Leftarrow)$ Let $p \equiv 1 \pmod{8}$ then $p = 8k + 1$ for some positive integer k. We need to prove that the quartic congruence $x^4 \equiv -1 \pmod{p}$ has solutions.

By *FlT*;

$$a^{p-1} \equiv 1 \pmod{p} \text{ provided } p \nmid a$$

Substituting $p = 8k + 1$ into *FlT* we have

$$a^{8k} \equiv 1 \pmod{p} \Rightarrow \left(a^{4k}\right)^2 \equiv 1 \pmod{p}$$

By Lemma (4.3):

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

Applying this Lemma to $\left(a^{4k}\right)^2 \equiv 1 \pmod{p}$ gives

$$a^{4k} \equiv \pm 1 \equiv 1, -1 \pmod{p}$$

Let $x = a^k$ is a solution to $x^4 = a^{4k} \equiv -1 \pmod{p}$.

$(\Rightarrow)$. Assume that $x^4 \equiv -1 \pmod{p}$ has a solution. Since p is an odd prime so $p \equiv \pm 1 \pmod{8}$ or $p \equiv \pm 3 \pmod{8}$. We need to show that $p \equiv 1 \pmod{8}$.

We use proof by contradiction by dismissing the cases $p \equiv -1 \pmod{8}$ and $p \equiv \pm 3 \pmod{8}$.

Suppose $p \equiv -1 \pmod{8}$ then $p = 8m - 1$ for some positive integer m.

By *FlT* we have for $p \nmid x$;

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

By Lemma (4.3):

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

We have

$$x^{4m-1} \equiv \left(x^4\right)^m x^{-1} \equiv \left(-1\right)^m x^{-1} \equiv -1 \pmod{p} \text{ implies } x^{-1} \equiv \left(-1\right)^{1-m} \equiv \pm 1 \pmod{p}$$

This is impossible because $x \not\equiv \pm 1 \pmod{p}$. *Why?*

If $x \equiv \pm 1 \pmod{p}$ then $x^4 \equiv 1 \not\equiv -1 \pmod{p}$ and $\pm 1 \pmod{p}$ are the only residues which are self-invertible. Hence $p \not\equiv -1 \pmod{8}$.

Now suppose $p \equiv \pm 3 \pmod{8}$. WLOG assume $p \equiv 3 \pmod{8}$ then $p = 8m + 3$ for some positive integer m.

By *FlT* we have for $p \nmid x$:

$$x^{p-1} \equiv x^{8m+2} \equiv \left(x^{4m+2}\right)^2 \equiv 1 \pmod{p}$$

By Lemma (4.3):

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

We have

$$x^{4m+2} \equiv \left(x^4\right)^m x^2 \equiv \left(-1\right)^m x^2 \equiv -1 \pmod{p} \text{ implies } x^2 \equiv \left(-1\right)^{1-m} \equiv \pm 1 \pmod{p}$$

This $x^2 \equiv \pm 1 \pmod{p}$ is impossible because we are assuming $x^4 \equiv -1 \pmod{p}$ so $x^2 \not\equiv \pm 1 \pmod{p}$.

Hence $p \not\equiv 3 \pmod{8}$ and similarly $p \not\equiv -3 \pmod{8}$.

Thus $p \equiv 1 \pmod{8}$ and this completes our proof.

■

(a) We are asked to factorize $12^4 + 1 = 20\,737$. By the above result

$$x^4 \equiv -1 \pmod{p} \text{ has a solution } \Leftrightarrow p \equiv 1 \pmod{8}.$$

We deduce that the odd prime factors p of 20 737 satisfy $p \equiv 1 \pmod 8$. Listing some of these factors 17, 41, 73, 89, ….

Dividing 20 737 by each of these we find that

$$\frac{20\ 737}{89} = 233$$

The $\left\lfloor \sqrt{233} \right\rfloor = 15$ and no prime below 15 is of the form $p \equiv 1 \pmod 8$. Hence 233 is prime and we have

$$12^4 + 1 = 20\ 737 = 89 \times 233$$

(b) This time we are asked to factorize $22^4 + 1 = 234\ 257$. The odd prime factors p of this number satisfy $p \equiv 1 \pmod 8$. Going through the list given in part (a) we have

$$\frac{234\ 257}{73} = 3209\,.$$

Testing whether 3209 is prime we need to find $\left\lfloor \sqrt{3209} \right\rfloor = 56$. Neither of the primes 17 or 41 go into 234 257 so they cannot be factors of 3209. Hence 3209 is prime and $22^4 + 1 = 234\ 257 = 73 \times 3209$.

(c) Factorizing $50^4 + 1 = 6\ 250\ 001$ by examining the primes of the form $p \equiv 1 \pmod 8$ which are 17, 41, 73, 89, 97, 113, 137, 193, 233, 241, 257,…

Trialling these primes as divisors of 6 250 002 we see that

$$\frac{6\ 250\ 001}{97} = 64\ 433$$

Again testing 64 433 to see if it is a prime:

$$\left\lfloor \sqrt{64\ 433} \right\rfloor = 253$$

We know need to see if the remaining primes ≥ 97 are factors of 64 433. None of the numbers in the list are factors so 64 433 is prime. Thus, we obtain

$$6\ 250\ 001 = 97 \times 64\ 433\,.$$

17. (i) *Proof.*

The Legendre symbol

$$\left(\frac{12}{p}\right)=\left(\frac{2^2\times 3}{p}\right)=\left(\frac{2^2}{p}\right)\times\left(\frac{3}{p}\right)=1\times\left(\frac{3}{p}\right)=\left(\frac{3}{p}\right)$$

Hence the primes for which 12 is a quadratic residue or quadratic non – residue is the same as the ones for which 3 is a QR or NR.

By Question 11(i) of Exercises 7.3 we have

$$\left(\frac{12}{p}\right)=\begin{cases}1 & \text{if } p\equiv\pm 1\left(\text{mod } 12\right)\\ -1 & \text{if } p\equiv\pm 5\left(\text{mod } 12\right)\end{cases}$$

■

(ii) (a) We need to factorize $151^2-12=22\ 789$. By part (i) we know the odd prime factors greater than 3 have the form $p\equiv\pm 1\left(\text{mod } 12\right)$.

Prime factors of this form are 11, 13, 23, 37, 47, … . We have

$$\frac{22\ 789}{13}=1753$$

We don't know whether 1753 is composite or prime. We have

$$\left\lfloor\sqrt{1753}\right\rfloor=41$$

None of the above primes go into 1753 so 1753 is prime. Thus

$$151^2-12=22\ 789=41\times 1753$$

(b) Similarly factorizing $2003^2-12=4\ 011\ 997$ we have

$$2003^2-12=4\ 011\ 997=11^2\times 71\times 467$$

18. (i) We need to prove that every primitive root of odd prime p is a quadratic non – residue of p.

Proof.

By the primitive root theorem (6.22) we have that the odd prime p has a primitive root, r say. Required to prove

$$x^2\equiv r\left(\text{mod } p\right) \text{ has } no \text{ solutions.}$$

Converting this $x^2\equiv r\left(\text{mod } p\right)$ to linear form by taking indices to the base r we obtain

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

The $\gcd\left(2,\ \ p-1\right)=2$ because we are given that p is an odd prime.

By Proposition (6.14):

$$\text{ind}_r(r) = 1$$

Now $2 \not| 1$ therefore $x^2 \equiv r \pmod{p}$ has *no* solutions because by Proposition (3.16):

$cx \equiv b \pmod{n}$ has exactly g solutions provided $g \mid b$ where $g = \gcd(c, n)$.

This completes our proof.

■

(ii) This time we show there is a quadratic non – residue of odd prime p which is *not* a primitive root of p. *How?*

Produce a counter example.

Let $p = 13$ and $r = 8$ then

$$8^2 \equiv 64 \equiv -1 \pmod{13} \text{ implies } 8^4 \equiv (-1)^2 \equiv 1 \pmod{13}$$

Hence $r = 8$ is *not* a primitive root of 13. Now we need to show that 8 is a quadratic non – residue of 13. *How?*

By evaluating the Legendre symbol $\left(\frac{8}{13}\right)$:

$$\left(\frac{8}{13}\right) = \left(\frac{2^3}{13}\right) = \underbrace{\left(\frac{2^2}{13}\right)}_{=1} \times \left(\frac{2}{13}\right) = \left(\frac{2}{13}\right) \qquad (*)$$

Since $13 \equiv -3 \pmod{8}$ so by

(7.15) $$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \equiv \pm 3 \pmod{8} \end{cases}$$

we obtain $\left(\frac{2}{13}\right) = -1$. From (*) we conclude that $\left(\frac{8}{13}\right) = \left(\frac{2}{13}\right) = -1$ so 8 is a quadratic non – residue of 13.

■

19. We need to prove that the square roots of $a \pmod{p}$ are given by $\pm r^n$ for some positive integer n.

Proof.

We are given that a is a quadratic residue of p so the quadratic congruence

$$x^2 \equiv a \pmod{p}$$

which implies that the square roots of $a \pmod{p}$ exist. Since p is prime so it has a primitive root by Primitive Root Theorem (6.22):

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

Call the primitive root r say. Taking indices and converting the quadratic congruence to linear form we have

$$2 \times \operatorname{ind}_r(x) \equiv \operatorname{ind}_r(a) \pmod{p-1} \qquad (*)$$

Since a is a quadratic residue so by the result of question 12 of Exercises 7.2:

> r^{2n} is a quadratic residue of p

Therefore $r^{2n} = a$ and substituting this into (*) gives

$$2 \times \operatorname{ind}_r(x) \equiv \operatorname{ind}_r(r^{2n}) \pmod{p-1}$$
$$2 \times \operatorname{ind}_r(x) \equiv 2n \times \underbrace{\operatorname{ind}_r(r)}_{=1 \text{ by Proposition (6.14)}} \equiv 2n \pmod{p-1}$$

Since p is odd prime so $\gcd(2,\ p-1) = 2$ and $2 \mid 2n$. The solutions are given by

$$\operatorname{ind}_r(x) \equiv n \pmod{\frac{p-1}{2}} \ \Rightarrow\ \operatorname{ind}_r(x) \equiv n,\ n + \frac{p-1}{2} \pmod{p-1}$$

From the right – hand side derivation we have

$$x \equiv r^n,\ r^{n+\frac{p-1}{2}} \underbrace{\equiv}_{\text{By the rules of indices}} r^n,\ r^n \times r^{\frac{p-1}{2}} \pmod{p} \qquad (\dagger)$$

Since r is a primitive root of p so $p \nmid r$ and by Proposition (7.6):

> $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ provided $p \nmid a$.

We have $r^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ and substituting this into (†) yields

$$x \equiv r^n,\ r^n(\pm 1) \equiv \pm r^n \pmod{p}$$

Therefore, the solutions of $x^2 \equiv a \pmod{p}$ are $x \equiv \pm r^n \pmod{p}$ so the square roots of $a \pmod{p}$ are $\pm r^n \pmod{p}$. This completes our proof.

■

20. We are asked to show that $x^3 - 5 = y^2$ has *no* solution.

Proof.

We proof this by contradiction. Suppose there is a solution, that is there are integers x and y such that $x^3 - 5 = y^2$.

The integer x can only be even or odd.

If x is even, then $x^3 \equiv 0 \pmod{8}$ and so

$$y^2 = x^3 - 5 \equiv -5 \equiv 3 \pmod{8}$$

However, $y^2 \not\equiv 3 \pmod{8}$ because 3 is a QNR of $p \equiv 3 \pmod{8}$.

If x is odd, then

$$x^3 - 5 = x^3 - 1 - 4 = y^2 \;\Rightarrow\; x^3 - 1 = (x-1)(x^2 + x + 1) = y^2 + 4$$

Since x is odd so x^2 is odd, and $x^2 + x + 1$ is odd.

Let p be a prime that divides $x^2 + x + 1$ then $p \mid (y^2 + 4)$ which implies

$$y^2 \equiv -4 \equiv (-1) \times 4 \pmod{p}.$$

Clearly 4 is a quadratic residue of p because $2^2 = 4$. Since y is a solution to the given equation so -1 must be a quadratic residue of p which implies $p \equiv 1 \pmod{4}$. *Why?*

By question 6 of Exercises 7.1:

$$-1 \text{ is a QR of } p \Leftrightarrow p \equiv 1 \pmod{4}.$$

Since $p \mid (x^2 + x + 1)$ so

$$x^2 + x + 1 \equiv 1 \pmod{4}$$

If $x \equiv 1 \pmod{4}$ then $x^2 + x + 1 \equiv 3 \pmod{4}$ which is impossible. Therefore

$x \equiv 3 \pmod 4$. Now we have

$$y^2 + 4 \equiv (x-1)(x^2 + x + 1) \equiv (3-1) \times (3^2 + 3 + 1) \equiv 26 \equiv 2 \pmod 4$$

Hence $y^2 + 4$ is even but the odd prime p satisfies $p \mid (y^2 + 4)$. This is impossible. Thus, there is *no* solution to the non – linear Diophantine equation $x^3 - 5 = y^2$.

■

21. We are asked to prove that -5 is a QR for $p \equiv 1, 3, 7, 9 \pmod{20}$.

Proof.

Let p be an odd prime. The Legendre symbol

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right) \times \left(\frac{5}{p}\right) \qquad (\ddagger)$$

By looking at the brief solutions of question 18 of Exercises 7.4 we have

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 5 \\ -1 & \text{if } p \equiv \pm 2 \pmod 5 \end{cases}$$

Also by Proposition (7.11):

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

The Legendre symbol in (‡) is equal to 1 if

$$\left(\frac{5}{p}\right) = \left(\frac{-1}{p}\right) = 1 \text{ or } \left(\frac{5}{p}\right) = \left(\frac{-1}{p}\right) = -1.$$

Considering the first case where both 5 and -1 are quadratic residues we have $p \equiv \pm 1 \equiv 1, 4 \pmod 5$ and $p \equiv 1 \pmod 4$. If $p \equiv 1 \pmod 5$ and $p \equiv 1 \pmod 4$ then by question 8(a) of Exercises 3.4:

$$x \equiv M \pmod p \text{ and } x \equiv M \pmod q \text{ implies } x \equiv M \pmod{pq}$$

We obtain $p \equiv 1 \pmod{20}$.

If $p \equiv 4 \pmod 5$ and $p \equiv 1 \pmod 4$ then by the Chinese Remainder Theorem

$$p \equiv a_1 x_1 N_1 + a_2 x_2 N_2 \left(\text{mod } N_1 N_2\right) \quad (*)$$

All these symbols are defined in the section on the Chinese Remainder Theorem.

$N_1 = 4, N_2 = 5$ and

$$4x_1 \equiv 1\left(\text{mod } 5\right) \quad \Rightarrow \quad x_1 = 4$$

$$5x_2 \equiv 1\left(\text{mod } 4\right) \quad \Rightarrow \quad x_2 = 1$$

Substituting $a_1 = 4,\ \ a_2 = 1$ and the above evaluations into (*) gives

$$\begin{aligned} p &\equiv \left(4 \times 4 \times 4\right) + \left(5 \times 1 \times 1\right)\left(\text{mod } \left(4 \times 5\right)\right) \\ &\equiv 64 + 5 \equiv 69 \equiv 9\left(\text{mod } 20\right) \end{aligned}$$

Hence -5 is a quadratic residue if the odd prime p satisfies $p \equiv 9\left(\text{mod } 20\right)$.

Now considering the case where both 5 and -1 are quadratic non – residues.

This is if $p \equiv \pm 2 \equiv 2,\ \ 3\left(\text{mod } 5\right)$ and $p \equiv 3\left(\text{mod } 4\right)$.

Arguing along similar lines we have $p \equiv 3\left(\text{mod } 5\right)$ and $p \equiv 3\left(\text{mod } 4\right)$ then by the result of question 8 of Exercises 3.4:

$$p \equiv 3\left(\text{mod } 20\right)$$

Also if $p \equiv 2\left(\text{mod } 5\right)$ and $p \equiv 3\left(\text{mod } 4\right)$ then by applying the Chinese Remainder Theorem we have $p \equiv 7\left(\text{mod } 20\right)$.

Thus, by combining all these different combinations we have -5 is a QR for $p \equiv 1, 3, 7, 9\left(\text{mod } 20\right)$. This completes our proof.

■