Complete Solutions to Supplementary 8

1. We are asked to show that the product of 4 consecutive integers plus 1 is a square number.

Proof.

Let $a-1, a, a+1$ and $a+2$ be the four consecutive integers. The product is

$$\begin{aligned} n &= a\left(a-1\right)\left(a+1\right)\left(a+2\right) \\ &= a\left(a^2-1\right)\left(a+2\right) \\ &= a\left(a^3+2a^2-a-2\right) = a^4+2a^3-a^2-2a \end{aligned}$$

Therefore, the integer $n+1$ is given by

$$n+1 = a^4+2a^3-a^2-2a+1$$

Since we have a quartic (degree 4) we want to factorize this into a repeated quadratic so that it is a square number:

$$a^4+2a^3-a^2-2a+1 = \left(a^2+ka+m\right)^2$$

We need to find the numerical values of k and m. By expanding the quadratic we have

$$\begin{aligned} \left(a^2+ka+m\right)^2 &= \left(a^2+ka+m\right)\left(a^2+ka+m\right) \\ &= a^4+ka^3+ma^2+ka^3+k^2a^2+kam+ma^2+kam+m^2 \\ &= a^4+2ka^3+\left(2m+k^2\right)a^2+2kam+m^2 \\ &= a^4+2a^3-a^2-2a+1 \qquad \left[\text{From above}\right] \end{aligned}$$

Equating coefficients of a^3 in the last two lines gives $k=1$.

Equating coefficients of a^2 gives $2m+k^2 = 2m+1 = -1 \quad \Rightarrow \quad m=-1$.

Our quadratic is a^2+a-1, that is

$$n+1 = a^4+2a^3-a^2-2a+1 = \left(a^2+a-1\right)^2$$

Hence $n+1$ is a square number.

■

2. (i) We are required to prove that if $\gcd\left(x,\ \ y\right) = g$ then $\gcd\left(x^m,\ \ y^m\right) = g^m$.

Proof.

We first show that g^m is the gcd of x^m and y^m. *How?*

By mathematical induction.

For the case $m=1$ the result is true because we are given

$$\gcd\left(x,\ \ y\right) = g^1 = g$$

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

$$\gcd\left(x^k, \quad y^k\right) = g^k$$

Required to prove $\gcd\left(x^{k+1}, \quad y^{k+1}\right) = g^{k+1}$.

We have $g \mid x$ and by the above assumption $g^k \mid x^k$. By Theorem (1.2)(c):

> If $a \mid b$ and $c \mid d$ then $\left(a \times c\right) \mid \left(b \times d\right)$.

We have $\left(g^k \times g\right) \mid \left(x^k \times x\right)$ implies $g^{k+1} \mid x^{k+1}$.

Similarly $g^{k+1} \mid y^{k+1}$. Thus g^{k+1} is a common divisor of x^{k+1} and y^{k+1} so by mathematical induction we have g^m is a common divisor of x^m and y^m.

Let c be the gcd of x^m and y^m. We need to prove that $c = g^m$.

There are integers a and b such that

$$ca = x^m \text{ and } cb = y^m \quad (*)$$

Since g^m is a common divisor so $g^m \mid c$ which implies $g^m z = c$ for some integer z.

Substituting this

$$g^m z = c \qquad (\dagger)$$

into (*) yields

$$g^m za = x^m \text{ and } g^m zb = y^m$$

Thus we have $za = \left(\frac{x}{g}\right)^m$ and $zb = \left(\frac{y}{g}\right)^m$. The $\gcd\left(\left(\frac{x}{g}\right)^m, \quad \left(\frac{y}{g}\right)^m\right) = 1$. *Why?*

Because $\gcd\left(x, \quad y\right) = g$ and by Proposition (1.5):

> If $\gcd\left(x, \quad y\right) = g$ then $\gcd\left(\frac{x}{g}, \quad \frac{y}{g}\right) = 1$.

By Question 15(iii) of Exercises 1(c);

> If $\gcd\left(a, \quad b\right) = 1$ then $\gcd\left(a^n, \quad b^n\right) = 1$.

Therefore $\gcd\left(\left(\frac{x}{g}\right)^m, \quad \left(\frac{y}{g}\right)^m\right) = 1$. Substituting $za = \left(\frac{x}{g}\right)^m$ and $zb = \left(\frac{y}{g}\right)^m$ gives

$$\gcd\left(za, \quad zb\right) = 1 \text{ which implies that } z = 1.$$

Substituting this $z = 1$ into (†) gives us our result $c = g^m$.

This completes our proof.

■

(ii) We are asked to prove that if $a \times b = n^2$ and $\gcd\left(a, \quad b\right) = 1$ then both a and

b are squares.

Proof

We have

$$a = a \times \underbrace{\gcd\left(a, \quad b\right)}_{=1}$$

$$= \gcd\left(a^2, \quad a \times b\right) \quad \left[\text{By Proposition (1.11)} \quad m \times \gcd\left(a, \quad b\right) = \gcd\left(ma, \quad mb\right)\right]$$

$$\underbrace{=}_{\text{Using } a\times b=n^2} \gcd\left(a^2, \quad n^2\right) \underbrace{=}_{\text{By part (i)}} \left[\gcd\left(a, \quad n\right)\right]^2$$

Similarly we have

$$b = b \times \gcd\left(a, \quad b\right) = \gcd\left(b \times a, \quad b^2\right) = \gcd\left(n^2, \quad b^2\right) \underbrace{=}_{\text{By part (i)}} \left[\gcd\left(n, \quad b\right)\right]^2$$

Thus, both a and b are square numbers. This completes our proof.

■

3. We are asked to prove if any prime $p > 5$ can be written as $a^2 + 5b^2$ then $p \equiv 1$ or $9 \left(\text{mod } 20\right)$.

   Proof.

   We need to show that there is a solution a and b such that

   $$a^2 + 5b^2 \equiv 0 \left(\text{mod } p\right) \quad \Rightarrow \quad a^2 \equiv -5b^2 \left(\text{mod } p\right)$$

   provided $p \equiv 1$ or $9 \left(\text{mod } 20\right)$. This means we need find the primes p for which $-5b^2$ is a quadratic residue. Evaluating the Legendre symbol

   $$\left(\frac{-5b^2}{p}\right) = \left(\frac{-5}{p}\right) \times \underbrace{\left(\frac{b^2}{p}\right)}_{=1 \text{ because } b^2 \text{ is QR}} = \left(\frac{-5}{p}\right)$$

   By the result of question 21 of Supplementary 7:

   $$-5 \text{ is a QR of } p \text{ provided } p \equiv 1, 3, 7, 9 \left(\text{mod } 20\right).$$

   This means

   $$a^2 + 5b^2 \equiv 0 \left(\text{mod } p\right) \text{ where } p \text{ could be } p \equiv 1, 3, 7, 9 \left(\text{mod } 20\right)$$

   Testing each of these primes $p \equiv 1, 3, 7, 9 \left(\text{mod } 20\right)$ to check $a^2 + 5b^2 \equiv 0 \left(\text{mod } p\right)$. This $p \equiv 1, 3, 7, 9 \left(\text{mod } 20\right)$ means the prime p is 1, 3, 7 or 9 more than a multiple of 20 so we can write this as

   $$p = 20k_1 + 1, \quad 20k_2 + 3, \quad 20k_3 + 7, \quad 20k_4 + 9$$

   where k_j for $j = 1, 2, 3, 4$ are positive integers. First consider $p = 20k_1 + 1$:

$$p = 20k_1 + 1 = a^2 + 5b^2 \;\Rightarrow\; 5\left(4k_1 - b^2\right) = a^2 - 1 \equiv 0 \pmod 5$$

From the last result we have $a^2 \equiv 1 \pmod 5$ and 1 is a quadratic residue of 5 so $p = 20k_1 + 1$ can be written as $a^2 + 5b^2$.

Similarly we have for $p = 20k_2 + 3$:

$$p = 20k_2 + 3 = a^2 + 5b^2 \;\Rightarrow\; 5\left(4k_2 - b^2\right) = a^2 - 3 \equiv 0 \pmod 5$$

From the last result we have $a^2 \equiv 3 \pmod 5$ but evaluating the Legendre symbol

$$\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1 \quad \left[\text{Because } 3 \equiv 3 \pmod 8\right]$$

Hence 3 is a quadratic non - residue of 5 so $p = 20k_2 + 3$ *cannot* be written as $a^2 + 5b^2$.

Also for $p = 20k_3 + 7$:

$$p = 20k_3 + 7 = a^2 + 5b^2 \;\Rightarrow\; 5\left(4k_3 - b^2\right) = a^2 - 7 \equiv 0 \pmod 5$$

From the last result we have $a^2 \equiv 7 \pmod 5$ but evaluating the Legendre symbol

$$\left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1 \quad \left[\text{Because } 5 \equiv -3 \pmod 8\right]$$

Hence 7 is a quadratic non - residue of 5 so $p = 20k_3 + 7$ *cannot* be written as $a^2 + 5b^2$.

Investigating the last case $p = 20k_4 + 9$:

$$p = 20k_4 + 9 = a^2 + 5b^2 \;\Rightarrow\; 5\left(4k_4 - b^2\right) = a^2 - 9 \equiv 0 \pmod 5$$

Since $9 = 3^2$ so it is a quadratic residue of modulo 5 which implies that $p = 20k_3 + 9$ *can* be written as $a^2 + 5b^2$.

This completes our proof that $p \equiv 1$ or $9 \pmod{20}$.

■

4. We need to prove that if $n \equiv 7 \pmod 8$ then $n \neq x^2 + y^2 + z^2$. *How?*

Use proof by contradiction.

Proof.

Suppose $n = x^2 + y^2 + z^2$. Then by squaring each residue in modulo 8 we have $a^2 \equiv 0, 1$ or $4 \pmod 8$. *Why?*

Because we have $a \equiv 0, 1, 2, 3, 4, 5, 6, 7 \pmod 8$ which implies

$$\begin{aligned} a^2 &\equiv 0^2, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2 \pmod 8 \\ &\equiv 0, 1, 4, 1, 0, 1, 4, 1 \pmod 8 \end{aligned}$$

Therefore

$$\begin{aligned} n = x^2 + y^2 + z^2 &\equiv \{0, 1 \text{ or } 4\} + \{0, 1 \text{ or } 4\} + \{0, 1 \text{ or } 4\} \\ &\equiv 0, 1, 2, 3, 4, 5 \text{ or } 6 \pmod 8 \end{aligned}$$

Thus $n \not\equiv 7 \pmod 8$. This is contradiction because we are given $n \equiv 7 \pmod 8$.

Hence $n \neq x^2 + y^2 + z^2$. This completes our proof.

■

5. We prove this by using the given hint:

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{1}{4} n^2 (n+1)^2$$

and the following standard result which can be proved by induction:

$$1 + 2 + 3 + \cdots + n = \frac{1}{2} n(n+1) \qquad (\dagger)$$

Proof.

We have

$$\begin{aligned} 1^3 + 2^3 + 3^3 + \cdots + k^3 = \frac{1}{4} n^2 (n+1)^2 &= \left[\frac{1}{2} n(n+1)\right]^2 \\ &= \left[1 + 2 + 3 + \cdots + n\right]^2 \quad [\text{By } (\dagger)] \end{aligned}$$

Hence we have our result.

■

6. (a) We need to prove that every integer n which satisfies $n \equiv 3 \pmod 8$ can written as a sum of three non – zero squares.

Proof.

From $n \equiv 3 \pmod 8$ which implies that n is 3 more than a multiple of 8;

$n = 8k + 3$ where k is an integer. We prove the result by induction.

For $k = 1$ we have our result because

$$n = (8 \times 1) + 3 = 11 = 3^2 + 1^2 + 1^2$$

Assume the result is true for $k = k$, that is (our induction hypothesis):

$$n = 8k + 3 = a^2 + b^2 + c^2 \equiv 3 \pmod 8 \qquad (*)$$

We are given that $n \equiv 3 \pmod 8$ which implies that n is an odd integer. To be able to write this as a sum of three squares we must have the following:

$$n \equiv (odd)^2 + (odd)^2 + (odd)^2 \equiv 3 \pmod 8 \qquad (\ddagger)$$

Why?

The only other option is $n = (even)^2 + (even)^2 + (odd)^2 = odd$ but this gives

$$n \equiv (2m)^2 + (2l)^2 + (2s+1)^2$$
$$\equiv 4\underbrace{(m^2 + l^2 + s^2 + s)}_{\text{This bracket term can only be odd or even}} + 1 \equiv \underbrace{(0 \text{ or } 4)}_{\text{Because } 4\times(even)\equiv 0 \pmod 8 \text{ or } 4\times(odd)\equiv 4 \pmod 8} + 1 \equiv 1, 5 \pmod 8$$

In this case $n \not\equiv 3 \pmod 8$ which contradicts our given statement $n \equiv 3 \pmod 8$. Therefore we *cannot* have

$$n = (even)^2 + (even)^2 + (odd)^2 = odd.$$

Substituting $a = 2m+1$, $b = 2l+1$ and $c = 2s+1$ into (*) yields

$$8k + 3 = (2m+1)^2 + (2l+1)^2 + (2s+1)^2 \equiv 3 \pmod 8$$

We need to prove the result for $k+1$,

$$8(k+1) + 3 = x^2 + y^2 + z^2 \qquad (\dagger)$$

Considering the left – hand side of (†) we have

$$8(k+1) + 3 \equiv 8k + 3 + 8$$
$$\equiv (2m+1)^2 + (2l+1)^2 + (2s+1)^2 + 8$$
$$\equiv (2m+3)^2 + (2l+1)^2 + (2s+1)^2 - 8m \quad \left[\text{Because } (2m+3)^2 = 4m^2 + 12m + 9 = (2m+1)^2 + 8 + 8m\right]$$
$$\equiv (2m+3)^2 + (2l+1)^2 + (2s+1)^2 \pmod 8 \quad \left[\text{Because } -8m \equiv 0 \pmod 8\right]$$

Hence, we can write $8(k+1)+3$ as sum of three squares, so by mathematical induction we have our result. This completes our proof.

■

(b) See Example 6. Consider $n = 105$ then $105 \equiv 1 \pmod 8$ but

$$105 = 10^2 + 2^2 + 1^2$$

Hence an example where 105 is sum of three squares but $105 \not\equiv 3 \pmod 8$.

7. We need to *disprove* that $n = a^2 + b^2$ has *no* divisor d of the form $d \equiv 3 \pmod 4$. *How?*

By producing a counter example. Take $d = 7 \equiv 3 \pmod 4$ then

$$n = 7^2 + 7^2 = 98 \text{ and of course } 7 \mid 98 .$$

8. We are asked to prove that the odd prime p can be expressed as the sum of two squares $\Leftrightarrow$ $p \equiv 1$ or $5 \pmod 8$.

Proof.

$(\Rightarrow)$. Assume p can be written as sum of two squares, that is $p = a^2 + b^2$ say. We have $a^2 + b^2 \equiv 0 \pmod p$ which implies $a^2 \equiv -b^2 \pmod p$. By Proposition (7.11) of the last chapter:

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

We have that -1 is a quadratic residue of p provided $p \equiv 1 \pmod 4$. Hence there are integers a and b such that $a^2 + b^2 \equiv 0 \pmod p$ provided $p \equiv 1 \pmod 4$. Recall that this $p \equiv 1 \pmod 4$ means that the prime p is one more than a multiple of 4, that is $p = 4m + 1$ where m is a positive integer. However m can be odd or even.

If m is odd, $2l + 1$ then

$$p = 4m + 1 = 4(2l + 1) + 1 = 8l + 5 \equiv 5 \pmod 8$$

If m is even, $2l$ then

$$p = 4m + 1 = 4(2l) + 1 = 8l + 1 \equiv 1 \pmod 8$$

Hence p must satisfy $p \equiv 1$ or $5 \pmod 8$.

$(\Leftarrow)$. Now going the other way. We assume $p \equiv 1$ or $5 \pmod 8$ which means that p is 1 or 5 more than a multiple of 8, that is

$$p = 8k + 1 \text{ or } p = 8m + 5$$

where k and m are positive integers. We have

$$p = 8k + 1 = 4(2k) + 1 \equiv 1 \pmod 4 \text{ or}$$
$$p = 8m + 5 = 4(2m + 1) + 1 \equiv 1 \pmod 4$$

In either case we have $p \equiv 1 \pmod 4$. By Theorem (8.3):

> Every prime p satisfying $p \equiv 1 \pmod 4$ can be written as the sum of two squares.

Thus if $p \equiv 1$ or $5 \pmod 8$ then it can written as the sum of two squares.

■

9. (a) We are asked to prove that if p is an odd prime then there are integers x and y such that

$$x^2 + y^2 \equiv -4 \pmod p \text{ where } 0 \le x,\ y \le \frac{p-1}{2}$$

Proof.

Rewriting the given equation as $x^2 \equiv -4 - y^2 \pmod p$.

Repeat the proof of Lemma (8.11) with the sets S and T given by

$$S = \left\{0^2,\ 1^2,\ 2^2,\ \cdots,\ \left(\frac{p-1}{2}\right)^2\right\} \quad \left[\text{Subsituting } x = 0, 1, 2, 3, \cdots, \frac{p-1}{2} \text{ into } x^2\right]$$

$$T = \left\{-4 - 0^2, -4 - 1^2, \cdots, -1 - \left(\frac{p-1}{2}\right)^2\right\} \quad \left[\text{Substituting } y = 0,1, \cdots, \frac{p-1}{2} \text{ into } -4 - y^2\right]$$

There are $p+1$ integers in these sets so there must at least one integer which is in *both* sets by the Pigeonhole Principle. Hence there are integers x and y such that $x^2 + y^2 \equiv -4 \pmod p$.

■

(b) We need to find x and y such that

$$x^2 + y^2 \equiv -4 \pmod{19} \text{ where } 0 \le x, y \le (19-1)/2$$

We look for x and y such that $x^2 \equiv -4 - y^2 \pmod{19}$.

Using the sets of part (a) we have

$$\begin{aligned} S = \left\{0^2, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2,\ 9^2\right\} &\equiv \left\{0, 1, 4, 9, 16, 25, 36, 49, 64, 81\right\} \\ &\equiv \left\{0, 1, 4, 9, 16, 6, 17, 11, 7, 5\right\} \pmod{19} \end{aligned}$$

$$\begin{aligned} T &= \left\{-4, -4-1^2, -4-2^2, -4-3^2, -4-4^2, -4-5^2, -4-6^2, -4-7^2, -4-8^2, -4-9^2\right\} \\ &\equiv \left\{-4, -5,\ -8, -13, -20, -29, -40, -53, -68, -85\right\} \\ &\equiv \left\{15, 14,\ 11, 6, 18, 9, 17, 4, 8, 10\right\} \pmod{19} \end{aligned}$$

Which integers are common between the sets S and T?

$$4,\ 6,\ 9,\ 11 \text{ and } 17$$

The integer 4 is the third element in set S and third from last in T so we have

$$2^2 \equiv -4 - 7^2 \pmod{19}$$

We also have the solution $7^2 \equiv -4 - 2^2 \pmod{19}$.

Similarly we have the other 3 solutions:

$$5^2 \equiv -4 - 3^2 \pmod{19}$$

$$3^2 \equiv -4 - 5^2 \pmod{19} \quad \text{[By symmetry]}$$

The last solution 17 is

$$6^2 \equiv -4 - 4^2 \pmod{19}$$

The five solutions of $x^2 + y^2 \equiv -4 \pmod{19}$ are

$$\{x = 2, y = 7\}, \{x = 7, y = 2\}, \{x = 3, y = 5\}, \{x = 5, y = 3\}, \{x = 6, y = 6\}$$

10. We need to check that $r = 1\,766\,319\,049 + 226\,153\,980\sqrt{61}$ produces a solution to $x^2 - 61y^2 = 1$. Substituting $x = 1766319049,\ y = 226153980$ into $x^2 - 61y^2 = 1$ gives

$$x^2 - 61y^2 = 1766319049^2 - \left(61 \times 226153980^2\right) = 1$$

(My calculator showed that this was zero but checking this on Maple gave the above answer).

11. We are asked to prove that the quadratic Diophantine equation $x^2 - Ny^2 = -1$ has *no* solutions if $N \equiv 3 \pmod{4}$.

Proof.

Suppose there is a solution x and y such that $x^2 - Ny^2 = -1$. We have

$$x^2 = Ny^2 - 1 \equiv -1 \pmod{N}$$

This $x^2 \equiv -1 \pmod{N}$ implies that -1 is a quadratic residue of N where $N \equiv 3 \pmod{4}$. This $N \equiv 3 \pmod{4}$ implies that N is 3 more than a multiple of 4, that is $N = 4k + 3$ where k is an integer. By Proposition (7.24);

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{1}{2}(n-1)}$$

Substituting $N = 4k + 3$ into the index $\frac{1}{2}(N - 1)$ we have

$$\frac{1}{2}\big((4k + 3) - 1\big) = \frac{1}{2}(4k + 2) = 2k + 1 \text{ which is odd.}$$

Therefore the Legendre symbol $\left(\frac{-1}{N}\right) = -1$ so -1 is a quadratic non - residue of N. This is a contradiction because in the above hypothesis we had -1 is a

quadratic residue of N. Hence there are *no* solutions to $x^2 - Ny^2 = -1$ if $N \equiv 3 \pmod 4$.

■

12. We need to show that $x^2 - 11y^2 = -2$ has solutions but $x^2 - 11y^2 = 2$ does *not*. We can trial some integers for solutions of $x^2 - 11y^2 = -2$. Transposing this yields

$$x = \sqrt{11y^2 - 2}$$

Substituting $y = 1$ gives $x = \sqrt{11(1)^2 - 2} = 3$ therefore our seed solution for $x^2 - 11y^2 = 2$ is $x = 3$ and $y = 1$. Hence $x^2 - 11y^2 = -2$ has solutions.

We also need to show that $x^2 - 11y^2 = 2$ has *no* solutions. We have

$$x^2 = 2 + 11y^2 \equiv 2 \pmod{11}$$

Since $11 \equiv 3 \pmod 8$ so by Proposition (7.15):

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

The Legendre symbol $\left(\frac{2}{11}\right) = -1$ so 2 is a quadratic non – residue of 11 which implies that $x^2 \equiv 2 \pmod{11}$ has *no* solutions. Hence $x^2 - 11y^2 = 2$ has *no* solutions.

13. (a) We are asked to find the seed solution of $x^2 - 13y^2 = 3$. Transposing this to make x the subject we have

$$x = \sqrt{3 + 13y^2}$$

Substituting $y = 1$ into this yields $x = \sqrt{3 + (13 \times 1^2)} = \sqrt{16} = 4$. Therefore a solution of $x^2 - 13y^2 = 3$ is $x = 4$ and $y = 1$.

(b) We need to solve $x^2 - 13y^2 = -3$. Transposing to make x the subject

$$x = \sqrt{-3 + 13y^2}\ .$$

Trialling integer values for y until x is an integer gives

$$x = \sqrt{-3 + (13 \times 2^2)} = \sqrt{49} = 7\ .$$

A solution to $x^2 - 13y^2 = -3$ is $x = 7$ and $y = 2$.

(c) We need to solve $x^2 - 13y^2 = -1$. Transposing to make x the subject

$$x = \sqrt{-1 + 13y^2}\,.$$

Trialling integer values for y until x is an integer gives

$$x = \sqrt{-1 + \left(13 \times 5^2\right)} = \sqrt{324} = 18\,.$$

A solution to $x^2 - 13y^2 = -1$ is $x = 18$ and $y = 5$.

14. (a) We need to find the fundamental solution of $x^2 - 23y^2 = 1$. Transposing this equation gives $x = \sqrt{1 + 23y^2}$. Substituting various integer values for y until $\sqrt{1 + 23y^2}$ is a square number gives $x = \sqrt{1 + \left(23 \times 5^2\right)} = \sqrt{576} = 24$. Thus our fundamental solution of $x^2 - 23y^2 = 1$ is $x = 24$ and $y = 5$.

(b) We need to solve $x^2 - 59y^2 = -2$. Making x the subject gives

$$x = \sqrt{-2 + 59y^2}$$

Trialling integer values for y until we get an integer for x:

$$x = \sqrt{-2 + \left(59 \times 3^2\right)} = \sqrt{529} = 23$$

Our solution is $x = 23$ and $y = 3$.

(c) We need to find the least positive solution of $x^2 - 61y^2 = -4$. Repeating what we done above we have

$$x = \sqrt{-4 + 61y^2}$$

Trialling integer values for $y = 1, 2, 3, 4, 5$. We can stop at $y = 5$ because

$$x = \sqrt{-4 + \left(61 \times 5^2\right)} = \sqrt{1521} = 39$$

The least positive solution to $x^2 - 61y^2 = -4$ is $x = 39$ and $y = 5$.

15. (a) *How do we know that* $x^2 + y^2 = 245$ *has a solution?*

Factorizing $245 = 5 \times 7^2$ and $5 \equiv 1 \pmod 4$, $7 \equiv 3 \pmod 4$. However since 7 is to an even index we can convert this to a sum of two squares.

By question 23 of Exercises 7(a):

> If n is the product of r *distinct* primes p which satisfy $p \equiv 1 \pmod 4$ then the number of different ways n can be expressed as a sum of two squares is 2^{r-1}.

There prime decomposition of $245 = 5 \times 7^2$ and $5 \equiv 1 \pmod 4$, $7 \equiv 3 \pmod 4$.

Therefore 245 has $2^{1-1} = 2^0 = 1$ way of writing this as a sum of two squares.

We have

$$245 = 5\times 7^2$$
$$= \left(2^2+1^2\right)\times 7^2 = \left(2^2\times 7^2\right)+\left(1^2\times 7^2\right) = 14^2+7^2 \Rightarrow x=14,\ y=7.$$

(b) We need to write down the four solutions of $x^2+y^2=6409$ where $6409 = 13\times 17\times 29$. *How do we know we have 4 distinct solutions?*

Note that $13\equiv 17\equiv 29\equiv 1\left(\text{mod } 4\right)$ and so by the result of question 23 of Exercises 7(a):

> If n is the product of r *distinct* primes p which satisfy $p\equiv 1\left(\text{mod } 4\right)$ then the number of different ways n can be expressed as the sum of two squares is 2^{r-1}.

Since we have $r=3$ distinct primes; 13, 17 and 29 and they are all congruent to 1 modulo 4 so there are $2^{3-1}=2^2=4$ different ways of writing 6409 as the sum of two squares. Well $13=3^2+2^2$, $17=4^2+1^2$ and $29=5^2+2^2$. Applying the Conversion Identity (8.1):

$$\left(a^2+b^2\right)\left(c^2+d^2\right)=\left(ac-bd\right)^2+\left(ad+bc\right)^2$$

We have

$$\begin{aligned}13\times 17 &= \left(3^2+2^2\right)\left(4^2+1^2\right)\\ &= \left(\left(3\times 4\right)-\left(2\times 1\right)\right)^2+\left(\left(3\times 1\right)+\left(2\times 4\right)\right)^2 \quad \left[\text{By (8.1)}\right]\\ &= 10^2+11^2\end{aligned}$$

Now applying the Conversion Identity (8.1) to this $13\times 17=10^2+11^2$ with $29=5^2+2^2$ yields

$$\begin{aligned}6409 &= 13\times 17\times 29\\ &= \left(10^2+11^2\right)\times\left(5^2+2^2\right)\\ &= \left(\left(10\times 5\right)-\left(11\times 2\right)\right)^2+\left(\left(10\times 2\right)+\left(11\times 5\right)\right)^2\\ &= 28^2+75^2\end{aligned}$$

By changing the order of multiplication of $6409=13\times 17\times 29$ we obtain the other 3 sum of squares representation:

$$3^2+80^2,\ 35^2+72^2 \text{ and } 53^2+60^2.$$

16. (i) First we need to check that $r=221+27\sqrt{67}$ is a solution of $x^2-67y^2=-2$.

Substituting $x=221$ and $y=27$ into x^2-67y^2 gives

$$x^2-67y^2 = 221^2-\left(67\times 27^2\right)=-2.$$

(ii) Now we need to find r^2:

$$r^2 = \left(221 + 27\sqrt{67}\right)^2 = 221^2 + \left(2 \times 221 \times 27\sqrt{67}\right) + \left(27^2 \times 67\right)$$
$$= 97\ 684 + 11\ 934\sqrt{67}$$

Substituting $x = 97\ 684$ and $y = 11\ 934$ into $x^2 - 67y^2$ yields

$$x^2 - 67y^2 = 97\ 684^2 \ - \left(67 \times 11\ 934^2\right) = 4$$

(iii) We are asked to find $r^3 = r^2 \times r$. Using our answers to parts (i) and (ii) we have

$$r^3 = r^2 \times r = \left(97\ 684 + 11\ 934\sqrt{67}\right) \times \left(221 + 27\sqrt{67}\right)$$
$$= \left(97\ 684 \times 221\right) + \left[\left(97\ 684 \times 27\right) + \left(11\ 934 \times 221\right)\right]\sqrt{67} + \left(11\ 934 \times 27 \times 67\right)$$
$$= 43\ 176\ 770 + 5\ 274\ 882\sqrt{67}$$

Since $r^3 = 43\ 176\ 770 + 5\ 274\ 882\sqrt{67}$ so substituting $x = 43\ 176\ 770$ and $y = 5\ 274\ 882$ into $x^2 - 67y^2$ gives

$$x^2 - 67y^2 = 43\ 176\ 770^2 - \left(67 \times 5\ 274\ 882^2\right) = -8$$

(iv) From our results in parts (i), (ii) and (iii) our prediction is

$$r^n \text{ gives the solution to } x^2 - 67y^2 = \left(-2\right)^n$$

Proof.

We prove this by mathematical induction.

The base case $n = 1$ is clearly true by part (i).

Assume the result is true for $n = k$, that is

$$r^k \text{ gives the solution to } x^2 - 67y^2 = \left(-2\right)^k \qquad (*)$$

Required to prove that

$$r^{k+1} \text{ gives the solution to } x^2 - 67y^2 = \left(-2\right)^{k+1}$$

By the rules of indices we have $r^{k+1} = r^k \times r$ so by (*)

$$r^{k+1} = r^k \times r \text{ gives solutions to } x^2 - 67y^2 = \left(-2\right)^k \times \left(-2\right) = \left(-2\right)^{k+1}$$

Hence by mathematical induction we have our predicted result;

$$r^n \text{ gives the solution to } x^2 - 67y^2 = \left(-2\right)^n$$

This completes our proof.

■

17. We need to show that $x^3 = 2y^2 + 2$ has *no* solutions.

Proof.

Since the right – hand side of this $x^3 = 2y^2 + 2$ is even so x^3 must be even which implies that x is even. Therefore x^3 is a multiple of 8, that is $x^3 = 8k$ where k is an integer or in modular arithmetic we have

$$x^3 = 2y^2 + 2 \equiv 0 \pmod 8 \;\Rightarrow\; 2y^2 \equiv -2 \pmod 8$$

The gcd of 2 and 8 is 2 so dividing this last congruence by 2 gives

$$y^2 \equiv -1 \equiv 3 \pmod 4$$

However $y^2 \equiv 0,1,2 \pmod 4$ (you can easily check this) therefore $x^3 = 2y^2 + 2$ has *no* solutions.

■

18. (i) We need to check that $r = 170 + 39\sqrt{19}$ produces a solution of $x^2 - 19y^2 = 1$.

Substituting $x = 170, y = 39$ into $x^2 - 19y^2$ gives

$$170^2 - \left(19 \times 39^2\right) = 1$$

Hence r produces a solution of $x^2 - 19y^2 = 1$.

(ii) Evaluating

$$\begin{aligned} r^2 = \left(170 + 39\sqrt{19}\right)^2 &= 170^2 + \left(2 \times 170 \times 39\sqrt{19}\right) + \left(39^2 \times 19\right) \\ &= 57\,799 + 13\,260\sqrt{19} \end{aligned}$$

Checking that $x = 57\,799, y = 13\,260$ also produces a solution:

$$57\,799^2 - \left(19 \times 13\,260^2\right) = 1$$

Similarly we have

$$\begin{aligned} r^3 = r \times r^2 &= \left(170 + 39\sqrt{19}\right)\left(57\,799 + 13\,260\sqrt{19}\right) \\ &= 9\,825\,830 + 2\,254\,200\sqrt{19} + 2\,254\,161\sqrt{19} + \left(517\,140 \times 19\right) \\ &= 19\,651\,490 + 4\,508\,361\sqrt{19} \end{aligned}$$

Checking that $x = 19\,651\,490, y = 4\,508\,361$ produces a solution

$$19\,651\,490^2 - \left(19 \times 4\,508\,361^2\right) = 1$$

On my calculator I received an answer of 0 for this but when I checked on Maple it confirmed the above.

Now checking r^4 we have

$$r^4 = \left(r^2\right)^2 = \left(57\ 799 + 13\ 260\sqrt{19}\right)^2$$
$$= 57\ 799^2 + \left(2 \times 57\ 799 \times 13\ 260\sqrt{19}\right) + \left(13\ 260^2 \times 19\right)$$
$$= 3\ 340\ 724\ 401 + 1\ 532\ 829\ 480\sqrt{19} + 3\ 340\ 724\ 400$$
$$= 6\ 681\ 448\ 801 + 1\ 532\ 829\ 480\sqrt{19}$$

Substituting $x = 6\ 681\ 448\ 801,\ y = 1\ 532\ 829\ 480$ into $x^2 - 19y^2$ gives

$$6\ 681\ 448\ 801^2 - \left(19 \times 1\ 532\ 829\ 480^2\right) = 1$$

Again calculator gives 0 but Maple gives the correct answer of 1.

(iii) Finding approximations to $\sqrt{19}$ by using these solutions by evaluating $\frac{x}{y}$.

For r we substitute $x = 170,\ y = 39$ which gives

$$\frac{170}{39} - \sqrt{19} = 0.000\ 075\ 42$$

Similarly for r^2, r^3, r^4 we have

$$\frac{57\ 799}{13\ 260} - \sqrt{19} = 6.523 \times 10^{-10}$$

$$\frac{x}{y} = \frac{19\ 651\ 490}{4\ 508\ 361} - \sqrt{19} = 5.643 \times 10^{-15}$$

$$\frac{x}{y} = \frac{6\ 681\ 448\ 801}{1\ 532\ 829\ 480} - \sqrt{19} = 4.882 \times 10^{-20}$$

19. We are asked to solve $x^2 - 14y^2 = 1$. Transposing this to make x the subject:

$$x = \sqrt{1 + 14y^2}$$

Substituting $y = 4$ gives an integer value for $x = \sqrt{1 + \left(14 \times 4^2\right)} = 15$. Therefore our fundamental solution is $x = 15,\ y = 4$ and we write $r = 15 + 4\sqrt{14}$.

By using the binomial expansion we have

$$r^5 = \left(15 + 4\sqrt{14}\right)^5$$
$$= 15^5 + \left(5 \times 15^4 \times 4\sqrt{14}\right) + \left(10 \times 15^3 \times 4^2\left(14\right)\right) + \left[10 \times 15^2 \times 4^3\left(\sqrt{14}\right)^3\right]$$
$$+ \left(5 \times 15 \times 4^4\left(14\right)^2\right) + 4^5\left(\sqrt{14}\right)^5$$
$$= 12\ 082\ 575 + 3\ 229\ 204\sqrt{14}$$

The discrepancy between the solution r^5 and $\sqrt{14}$ is given by finding the difference $\dfrac{12\ 082\ 575}{3\ 229\ 204} - \sqrt{14} = 1.281 \times 10^{-14}$.

20. We need to write $\left(a^2 + nb^2\right)\left(c^2 + nd^2\right)$ as a sum of two squares. *How?*

Use the Conversion Identity (8.1):

$$\left(a^2 + b^2\right)\left(c^2 + d^2\right) = \left(ac - bd\right)^2 + \left(ad + bc\right)^2$$

Therefore

$$\begin{aligned}\left(a^2 + nb^2\right)\left(c^2 + nd^2\right) &= \left(a^2 + \left(\sqrt{n}b\right)^2\right)\left(c^2 + \left(\sqrt{n}d\right)^2\right) \quad \left[\text{Writing } n = \sqrt{n^2}\right] \\ &= \left(ac - nbd\right)^2 + \left[\left(a\sqrt{n}d\right) + \sqrt{n}bc\right]^2 \\ &= \left(ac - nbd\right)^2 + n\left[ad + bc\right]^2\end{aligned}$$

Hence $\left(a^2 + nb^2\right)\left(c^2 + nd^2\right) = x^2 + ny^2$ where $x = ac - nbd,\ y = ad + bc$.

21. We are asked to prove that if each of the integers $n_1, n_2, n_3, \cdots, n_k$ can be written as sum of two squares then their product can also be written as sum of two squares.

Proof.

We prove this result by mathematical induction.

Clearly $n_1 = a_1^{\,2} + b_1^{\,2}$ because we are given this.

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

$$n_1 \times n_2 \times n_3 \times \cdots \times n_m = a_m^{\,2} + b_m^{\,2} \qquad (*)$$

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

$$n_1 \times n_2 \times n_3 \times \cdots \times n_m \times n_{m+1} = \left(a_{m+1}\right)^2 + \left(b_{m+1}\right)^2$$

Rewriting the left – hand side and using (*) gives

$$\begin{aligned}n_1 \times n_2 \cdots \times n_m \times n_{m+1} &= \left(a_m^{\,2} + b_m^{\,2}\right) \times n_{m+1} \qquad \left[\text{By } (*)\right] \\ &= \left(a_m^{\,2} + b_m^{\,2}\right) \times \left(c^2 + d^2\right) \quad \left[\text{Because } n_{m+1} \text{ is sum of two squares}\right] \\ &= \left(a_m c - b_m d\right)^2 + \left(a_m d + b_m c\right)^2 \quad \left[\text{By Identity } (8.1)\right]\end{aligned}$$

It follows by mathematical induction that the product $n_1 \times n_2 \times n_3 \times \cdots \times n_k$ can be written as a sum of two squares.

■

22. (a) We are asked to prove that there are an infinitely many integer solutions of $x^2 - Ny^2 = z^2$ for any integer N.

Proof.

We want something similar to question 5(c) of Exercises 8.1:

$$\left(2mn\right)^2 + \left(n^2 - m^2\right)^2 = \left(n^2 + m^2\right)^2$$

We need a minus sign in the middle so let us expand $\left(a^2 + Nb^2\right)^2 - N\left(2ab\right)^2$:

$$\begin{aligned}\left(a^2 + Nb^2\right)^2 - N\left(2ab\right)^2 &= a^4 + 2a^2b^2N + N^2b^4 - 4a^2b^2N \\ &= a^4 - 2a^2b^2N + b^4N^2 \\ &= \left(a^2 - Nb^2\right)^2\end{aligned}$$

Let $x = a^2 + Nb^2,\ \ y = 2ab$ and $z = a^2 - Nb^2$ for any integers a and b.

Therefore we have infinitely many integer solutions to $x^2 - Ny^2 = z^2$.

■

(b) We also need to find the fundamental or seed solution of $x^2 - 230y^2 = 1$.

Transposing to make x the subject gives $x = \sqrt{1 + 230y^2}$. Substituting various integer values of y until x is an integer we find that

$$x = \sqrt{1 + \left(230 \times 6^2\right)} = 91$$

Hence $x = 91, y = 6$ is our seed solution.

23. We need to prove that the solution of Pell's equation $x^2 - \left(N^{2n} - 1\right)y^2 = 1$ where n is a natural number is $y = 1,\ \ x = N^n$.

Proof.

Substituting $y = 1,\ \ x = N^n$ into $x^2 - \left(N^{2n} - 1\right)y^2$ gives

$$\left(N^n\right)^2 - \left(N^{2n} - 1\right)1^2 = N^{2n} - N^{2n} + 1 = 1$$

Hence we have our required result.

■

24. We are required to prove that there are infinitely many integer solutions of $x^2 - \left(N^2 + 1\right)y^2 = 1$.

Proof.

Transposing the given equation yields

$$x^2 = 1 + \left(N^2 + 1\right)y^2 \qquad (*)$$

Since we are looking for integer solutions so $1+\left(N^2+1\right)y^2$ needs to be a square number. If we let $y=N$ this will *not* work because

$$1+\left(N^2+1\right)N^2=N^4+N^2+1$$

which is *not* a square number. Recall from our algebraic identities

$$\left(a+b\right)^2=a^2+2ab+b^2$$

This implies we need an even number in the middle. So, let us try $y=2N$:

$$\begin{aligned}1+\left(N^2+1\right)y^2&=1+\left(N^2+1\right)\left(2N\right)^2\\&=1+4N^2\left(N^2+1\right)=4N^4+4N^2+1=\left(2N^2+1\right)^2\end{aligned}$$

Therefore with $y=2N$ we have square number for $1+\left(N^2+1\right)y^2$. Substituting this into (*) gives

$$x^2=1+\left(N^2+1\right)y^2=\left(2N^2+1\right)^2\ \Rightarrow\ x=2N^2+1$$

So taking $x=2N^2+1$ and $y=2N$ for any integer N we have solutions of $x^2-\left(N^2+1\right)y^2=1$. Hence $x^2-\left(N^2+1\right)y^2=1$ has infinitely many solutions. ■

25. We need to prove that every prime $p>3$ that satisfies $p\equiv 1$ or $3\left(\text{mod } 8\right)\ \Leftrightarrow$ $p=x^2+2y^2$.

Proof.

$\left(\Leftarrow\right)$. If $p=x^2+2y^2$ then $x^2+2y^2\equiv 0\left(\text{mod } p\right)\ \Leftrightarrow\ x^2\equiv -2y^2\left(\text{mod } p\right)$. For this we have -2 is a quadratic residue of p because y^2 is a quadratic residue and product of QR with QR is a QR. By question 9 (ii) of Exercises 7(c):

If the odd prime p satisfies $p\mid\left(x^2+2\right)$ then $p\equiv 1,3\left(\text{mod } 8\right)$.

Hence $p\equiv 1$ or $3\left(\text{mod } 8\right)$.

$\left(\Rightarrow\right)$. We have $p\equiv 1$ or $3\left(\text{mod } 8\right)$ therefore $x^2\equiv -2y^2\left(\text{mod } p\right)$ has solutions and transposing this gives

$$x^2+2y^2\equiv 0\left(\text{mod } p\right)$$

We have $x^2+2y^2\equiv 0\left(\text{mod } p\right)\ \Rightarrow\ x^2+2y^2=kp$ where k is a positive integer.

We need to show that $k<p$.

If we chose $y=1$ then the quadratic congruence $x^2+2\equiv 0\left(\text{mod } p\right)$ which we can rewrite as $x^2\equiv -2\left(\text{mod } p\right)$ has solutions because we are given

$p \equiv 1$ or $3 \pmod 8$. By the symmetrical nature of the quadratic solutions we have $1 \le x \le \dfrac{p-1}{2}$. Therefore $1 \le x^2 \le \left(\dfrac{p-1}{2}\right)^2$. We are given that $p > 3$ therefore:

$$\frac{x^2+2}{p} \le \frac{\left(\dfrac{p-1}{2}\right)^2 + 2}{p} < \frac{\dfrac{p^2}{4}+2}{p} = \frac{p^2}{4p} + \frac{2}{p} = \frac{p}{4} + \frac{2}{p} < p$$

Hence $x^2 + 2 < p^2$. So there exists positive integers x and y such that

$$x^2 + 2y^2 = kp \text{ where } k < p.$$

By the Well Ordering Principle, WOP, let m be the least of these k's, that is

$$x^2 + 2y^2 = mp \text{ where } m \text{ is the least positive integer satisfying this.}$$

What do we need to show?

Required to prove that $m = 1$. *How?*

By contradiction. Suppose $m > 1$.

We define integers a and b such that

$$a \equiv x \pmod m \text{ and } b \equiv y \pmod m \text{ where } -\frac{m}{2} < a, b \le \frac{m}{2}.$$

Therefore

$$a^2 + 2b^2 \equiv x^2 + 2y^2 = mp \equiv 0 \pmod m \quad (*)$$

Thus, there is an integer n such that

$$a^2 + 2b^2 = mn \qquad (**)$$

Combining these together, (*) and (**), gives

$$\left(a^2 + 2b^2\right)\left(x^2 + 2y^2\right) = (mn)(mp) = m^2np$$

Now using the Conversion Identity (8.1) on the left – hand side yields

$$\left(a^2 + 2b^2\right)\left(x^2 + 2y^2\right) = \left(\left(\sqrt{2}b\right)^2 + a^2\right)\left(x^2 + \left(\sqrt{2}y\right)^2\right)$$

$$\underbrace{=}_{\text{By (8.1)}} \left(\sqrt{2}bx - \sqrt{2}ay\right)^2 + \left(2by + ax\right)^2 = m^2np \quad (\dagger)$$

Now we examine both terms inside the brackets $\left(\sqrt{2}bx - \sqrt{2}ay\right) = \sqrt{2}\left(bx - ay\right)$ and $\left(2by + ax\right)$:

$$\sqrt{2}\left(bx - ay\right) \equiv \sqrt{2}\left(yx - xy\right) \equiv 0 \pmod m$$

because $a \equiv x \pmod m$ and $b \equiv y \pmod m$. Similarly

$$2by + ax \equiv 2yy + xx \equiv 2y^2 + x^2 \equiv 0 \pmod m \qquad \text{[By (*)]}$$

Thus both $\sqrt{2}\left(bx-ay\right)$ and $2by+ax$ are multiples of m which implies that we can divide $\left(\dagger\right)$ by m^2 and get the following sum of two squares:

$$\left(\frac{2by+ax}{m}\right)^2+2\left(\frac{bx-ay}{m}\right)^2=np \qquad (\dagger\dagger)$$

From the above inequality $-\frac{m}{2}<a,b\le\frac{m}{2}$ we have

$$a^2+2b^2\le\left(\frac{m}{2}\right)^2+2\left(\frac{m}{2}\right)^2=\frac{3m^2}{4}<m^2$$

We have $-\frac{m}{2}<a,b\le\frac{m}{2}$ so by (**) and the above inequality we have

$$a^2+2b^2=mn<m^2 \;\Rightarrow\; n<m$$

We want to show that n is a positive integer. So far we have n is a non – negative integer.

If $n=0$ then from (**) we have

$$a^2+2b^2=m\times\left(0\right)=0 \text{ which implies } a=b=0\,.$$

From above $x\equiv a\equiv 0\left(\text{mod } m\right)$ and $y\equiv b\equiv 0\left(\text{mod } m\right)$ which implies that $m\mid x$ and $m\mid y$ respectively. Therefore

$$m^2\mid\left(x^2+y^2\right)\;\Rightarrow\; m^2\mid mp\;\Rightarrow\; m\mid p$$

We have $m<p$ so $m=1$ which is our required result.

If n is a positive integer then from $(\dagger\dagger)$ we have np is the sum of two squares and in the above calculation $n<m$. This is a contradiction. *Why?*

Because m was the least positive integer which is the sum of two squares and now we have found a smaller positive integer n. Our supposition that $m>1$ must be wrong so $m=1$ which implies $x^2+2y^2=mp=p$. Hence $p\equiv 1$ or $3\left(\text{mod } 8\right)$ can be written as x^2+2y^2.

■

26. We are asked to prove that every prime p that satisfies $p\equiv 1\left(\text{mod } 3\right)$ can be written as x^2+3y^2.

Proof.

Very similar proof to the previous question.

We need to show that there are solutions x and y such that

$$x^2+3y^2\equiv 0\left(\text{mod } p\right)\;\Rightarrow\; x^2\equiv -3y^2\left(\text{mod } p\right)$$

Clearly y^2 is a quadratic residue of p. *For what primes p is -3 a quadratic residue of p?*

By Question 5 of Exercises 7(d):

$$\left(\frac{-3}{p}\right)=\begin{cases} 1 & \text{if } p\equiv 1 \pmod 6 \\ -1 & \text{if } p\equiv 5 \pmod 6 \end{cases}$$

This implies that -3 is a quadratic residue of p provided $p\equiv 1 \pmod 6$.This $p\equiv 1 \pmod 6$ means that p is one more than a multiple of 6; $p=6k+1$ for some positive integer k. We have

$$p=6k+1=3(2k)+1\equiv 1 \pmod 3$$

Thus -3 is a quadratic residue of p such that $p\equiv 1 \pmod 3$. Evaluating the Legendre symbol

$$\left(\frac{-3y^2}{p}\right)\underbrace{=}_{\text{By the multiplicative propery of the Legendre symbol}}\left(\frac{-3}{p}\right)\times\underbrace{\left(\frac{y^2}{p}\right)}_{=1 \text{ Because } y^2 \text{ is a QR}}=\left(\frac{-3}{p}\right)=1$$

provided $p\equiv 1 \pmod 3$. Hence there are solutions to

$$x^2\equiv -3y^2 \quad\Rightarrow\quad x^2+3y^2\equiv 0 \pmod p$$

We have $x^2+3y^2\equiv 0 \pmod p \Rightarrow x^2+3y^2=kp$ where k is a positive integer. We need to show that $k<p$.

If we chose $y=1$ then the quadratic congruence $x^2+3\equiv 0 \pmod p$ which we can rewrite as $x^2\equiv -3 \pmod p$ has solutions because we are given $p\equiv 1 \pmod 3$. By the symmetrical nature of the quadratic solutions we have $1\le x\le \frac{p-1}{2}$. Therefore $1\le x^2\le \left(\frac{p-1}{2}\right)^2$. We are given that $p>3$ so

$$\frac{x^2+3}{p}\le\frac{\left(\frac{p-1}{2}\right)^2+3}{p}<\frac{\frac{p^2}{4}+3}{p}=\frac{p^2}{4p}+\frac{3}{p}=\frac{p}{4}+\frac{3}{p}<p$$

Hence $x^2+3<p^2$. So there exists positive integers x and y such that $x^2+3y^2=kp$ where $k<p$.

By the Well Ordering Principle, WOP, let m be the least of these *k's*, that is

$x^2+3y^2=mp$ where m is the least positive integer satisfying this.

What do we need to show?

Required to prove that $m=1$. *How?*

By contradiction. Suppose $m>1$.

We define integers a and b such that

$$a\equiv x\Big(\text{mod } m\Big) \text{ and } b\equiv y\Big(\text{mod } m\Big) \text{ where } -\frac{m}{2}<a,b\le\frac{m}{2}.$$

Therefore

$$a^2+3b^2\equiv x^2+3y^2=mp\equiv 0\Big(\text{mod } m\Big) \quad (*)$$

Thus, there is an integer n such that

$$a^2+3b^2=mn \qquad (**)$$

Combining these together, (*) and (**), gives

$$\Big(a^2+3b^2\Big)\Big(x^2+3y^2\Big)=\Big(mn\Big)\Big(mp\Big)=m^2np$$

Now using the Conversion Identity (8.1) on the left – hand side yields

$$\Big(a^2+3b^2\Big)\Big(x^2+3y^2\Big)=\left(\Big(\sqrt{3}b\Big)^2+a^2\right)\left(x^2+\Big(\sqrt{3}y\Big)^2\right)$$

$$\underbrace{\equiv}_{\text{By (8.1)}}\Big(\sqrt{3}bx-\sqrt{3}ay\Big)^2+\Big(3by+ax\Big)^2=m^2np \qquad (\dagger)$$

Now we examine both terms inside the brackets $\Big(\sqrt{3}bx-\sqrt{3}ay\Big)=\sqrt{3}\Big(bx-ay\Big)$ and $\Big(3by+ax\Big)$:

$$\sqrt{3}\Big(bx-ay\Big)\equiv\sqrt{3}\Big(yx-xy\Big)\equiv 0\Big(\text{mod } m\Big)$$

because $a\equiv x\Big(\text{mod } m\Big)$ and $b\equiv y\Big(\text{mod } m\Big)$. Similarly

$$3by+ax\equiv 3yy+xx\equiv 3y^2+x^2\equiv 0\Big(\text{mod } m\Big) \qquad \text{[By (*)]}$$

Thus both $\sqrt{3}\Big(bx-ay\Big)$ and $3by+ax$ are multiples of m which implies that we can divide $(\dagger)$ by m^2 and get the following sum of two squares:

$$\left(\frac{by+ax}{m}\right)^2+3\left(\frac{bx-ay}{m}\right)^2=np \qquad (\dagger\dagger)$$

From the above inequality $-\frac{m}{2}<a,b\le\frac{m}{2}$ we have

$$a^2+3b^2\le\left(\frac{m}{2}\right)^2+3\left(\frac{m}{2}\right)^2=m^2$$

If we have equality, that is $a=b=\frac{m}{2}$ then from (*)

$$m^2\equiv a^2+3b^2\equiv x^2+3y^2=mp\equiv 0\Big(\text{mod } mp\Big)$$

We have $m^2 \mid mp$ which implies $m \mid p$. From the start we have $m < p$ therefore $m = 1$ which is our required result.

If we have strict inequality, that is $-\frac{m}{2} < a, b < \frac{m}{2}$ then by (**) and the above inequality we have

$$a^2 + 3b^2 = mn < m^2 \quad \Rightarrow \quad n < m$$

We have n is a positive integer. From (††) we have np is the sum of two squares and in the above calculation $n < m$. This is a contradiction. *Why?* Because m was the least positive integer which is the sum of two squares and now we have found a smaller positive integer n. Our supposition that $m > 1$ must be wrong so $m = 1$ which implies $x^2 + 3y^2 = mp = p$. Hence $p \equiv 1 \pmod 3$ can be written as $x^2 + 3y^2$.

■