Complete Solutions to Exercises 8.2

1. For this question we use the sum of four squares identity (8.10):

$$\left(a^2+b^2+c^2+d^2\right)\times\left(x^2+y^2+z^2+w^2\right)=\left(ax+by+cz+dw\right)^2+\left(ay-bx+cw-dz\right)^2 \\ +\left(az-bw-cx+dy\right)^2+\left(aw+bz-cy-dx\right)^2$$

(a) Factorizing $35=5\times7$ and writing each of these integers as sum of four squares:

$$5=2^2+1^2+0^2+0^2 \quad \text{and} \quad 7=2^2+1^2+1^2+1^2$$

Using the above four square identity we have

$$\begin{aligned}5\times7&=\left(2^2+1^2+0^2+0^2\right)\times\left(2^2+1^2+1^2+1^2\right)\\&=\left(\left[2\times2\right]+\left[1\times1\right]+\left[0\times1\right]+\left[0\times1\right]\right)^2+\left(\left[2\times1\right]-\left[1\times2\right]+\left[0\times1\right]-\left[0\times1\right]\right)^2\\&\quad+\left(\left[2\times1\right]-\left[1\times1\right]-\left[0\times2\right]+\left[0\times1\right]\right)^2+\left(\left[2\times1\right]+\left[1\times1\right]-\left[0\times1\right]-\left[0\times2\right]\right)^2\\&=5^2+0^2+1^2+3^2\end{aligned}$$

Therefore $35=5^2+3^2+1^2+0^2$. (Only need 3 non – zero squares.)

(b) We need to convert 49 into sum of four squares. We know that

$$49=7\times7 \quad \text{and} \quad 7=2^2+1^2+1^2+1^2$$

Applying the four squares identity (8.10) we have

$$\begin{aligned}7\times7&=\left(2^2+1^2+1^2+1^2\right)\times\left(2^2+1^2+1^2+1^2\right)\\&=\left(\left[2\times2\right]+\left[1\times1\right]+\left[1\times1\right]+\left[1\times1\right]\right)^2+\left(\left[2\times1\right]-\left[1\times2\right]+\left[1\times1\right]-\left[1\times1\right]\right)^2\\&\quad+\left(\left[2\times1\right]-\left[1\times1\right]-\left[1\times2\right]+\left[1\times1\right]\right)^2+\left(\left[2\times1\right]+\left[1\times1\right]-\left[1\times1\right]-\left[1\times2\right]\right)^2\\&=7^2+0^2+0^2+0^2\quad\left(\text{Only need 1 square.}\right)\end{aligned}$$

(c) Factorizing 945 and using the rules of indices gives

$$945=3^3\times5\times7=3^2\times15\times7 \qquad (*)$$

Now we just need to write 15×7 as sum of four squares:

$$7=2^2+1^2+1^2+1^2 \text{ and } 15=3^2+2^2+1^2+1^2$$

Using the four square identity (8.10) on 7 and 15 we have

$$\begin{aligned}7\times15&=\left(2^2+1^2+1^2+1^2\right)\times\left(3^2+2^2+1^2+1^2\right)\\&=\left(\left[2\times3\right]+\left[1\times2\right]+\left[1\times1\right]+\left[1\times1\right]\right)^2+\left(\left[2\times2\right]-\left[1\times3\right]+\left[1\times1\right]-\left[1\times1\right]\right)^2\\&\quad+\left(\left[2\times1\right]-\left[1\times1\right]-\left[1\times3\right]+\left[1\times2\right]\right)^2+\left(\left[2\times1\right]+\left[1\times1\right]-\left[1\times2\right]-\left[1\times3\right]\right)^2\\&=10^2+1^2+0^2+\left(-2\right)^2=10^2+2^2+1^2+0^2\end{aligned}$$

Substituting this $7\times15=10^2+2^2+1^2+0^2$ into (*) yields

$$\begin{aligned}945 &= 3^2 \times \left(10^2 + 2^2 + 1^2 + 0^2\right) \\ &= \left(3\times 10\right)^2 + \left(3\times 2\right)^2 + \left(3\times 1\right)^2 + \left(3\times 0\right)^2 \\ &= 30^2 + 6^2 + 3^2 + 0^2\end{aligned}$$

(d) Factorizing $310 = 10\times 31$ and writing each of these integers as sum of four squares:

$$10 = 3^2 + 1^2 + 0^2 + 0^2 \text{ and } 31 = 5^2 + 2^2 + 1^2 + 1^2$$

Applying (8.10) to $310 = 10\times 31$ gives

$$\begin{aligned}10\times 31 &= \left(3^2 + 1^2 + 0^2 + 0^2\right)\times\left(5^2 + 2^2 + 1^2 + 1^2\right) \\ &= \left(\left[3\times 5\right] + \left[1\times 2\right] + \left[0\times 1\right] + \left[0\times 1\right]\right)^2 + \left(\left[3\times 2\right] - \left[1\times 5\right] + \left[0\times 1\right] - \left[0\times 1\right]\right)^2 \\ &\quad + \left(\left[3\times 1\right] - \left[1\times 1\right] - \left[0\times 5\right] + \left[0\times 2\right]\right)^2 + \left(\left[3\times 1\right] + \left[1\times 1\right] - \left[0\times 2\right] - \left[0\times 5\right]\right)^2 \\ &= 17^2 + 1^2 + 2^2 + 4^2 = 17^2 + 4^2 + 2^2 + 1^2\end{aligned}$$

Therefore 310 as sum of four squares is $17^2 + 4^2 + 2^2 + 1^2$.

(e) The factorization of 465 is

$$465 = 3\times 5\times 31 = 15\times 31$$

The sum of four squares of 15 and 31 are given by

$$15 = 3^2 + 2^2 + 1^2 + 1^2 \text{ and } 31 = 5^2 + 2^2 + 1^2 + 1^2$$

Putting these into (8.10) yields

$$\begin{aligned}15\times 31 &= \left(3^2 + 2^2 + 1^2 + 1^2\right)\times\left(5^2 + 2^2 + 1^2 + 1^2\right) \\ &= \left(\left[3\times 5\right] + \left[2\times 2\right] + \left[1\times 1\right] + \left[1\times 1\right]\right)^2 + \left(\left[3\times 2\right] - \left[2\times 5\right] + \left[1\times 1\right] - \left[1\times 1\right]\right)^2 \\ &\quad + \left(\left[3\times 1\right] - \left[2\times 1\right] - \left[1\times 5\right] + \left[1\times 2\right]\right)^2 + \left(\left[3\times 1\right] + \left[2\times 1\right] - \left[1\times 2\right] - \left[1\times 5\right]\right)^2 \\ &= 21^2 + \left(-4\right)^2 + \left(-2\right)^2 + \left(-2\right)^2 = 21^2 + 4^2 + 2^2 + 2^2\end{aligned}$$

Hence 465 as sum of four squares is $21^2 + 4^2 + 2^2 + 2^2$.

(f) We have $143 = 11\times 13$ and

$$11 = 3^2 + 1^2 + 1^2 + 0^2;\ 13 = 3^2 + 2^2 + 0^2 + 0^2$$

Using identity (8.10) we have

$$\begin{aligned}11\times 13 &= \left(3^2 + 1^2 + 1^2 + 0^2\right)\times\left(3^2 + 2^2 + 0^2 + 0^2\right) \\ &= \left(\left[3\times 3\right] + \left[1\times 2\right] + \left[1\times 0\right] + \left[0\times 0\right]\right)^2 + \left(\left[3\times 2\right] - \left[1\times 3\right] + \left[1\times 0\right] - \left[0\times 0\right]\right)^2 \\ &\quad + \left(\left[3\times 0\right] - \left[1\times 0\right] - \left[1\times 3\right] + \left[0\times 2\right]\right)^2 + \left(\left[3\times 0\right] + \left[1\times 0\right] - \left[1\times 2\right] - \left[0\times 3\right]\right)^2 \\ &= 11^2 + 3^2 + \left(-3\right)^2 + \left(-2\right)^2 \\ &= 11^2 + 3^2 + 3^2 + 2^2\end{aligned}$$

Hence $143 = 11^2 + 3^2 + 3^2 + 2^2$.

2. (a) We are given $3072 = 2^{10} \times 3$ and $3 = 1^2 + 1^2 + 1^2 + 0^2$ so by applying the rules of indices we have

$$\begin{aligned} 3072 &= 2^{10} \times 3 \\ &= \left(2^5\right)^2 \times \left(1^2 + 1^2 + 1^2 + 0^2\right) \\ &= 32^2 \times \left(1^2 + 1^2 + 1^2 + 0^2\right) \\ &= 32^2 + 32^2 + 32^2 + 0^2 \end{aligned}$$

Hence $3072 = 32^2 + 32^2 + 32^2 + 0^2$. (Only three non – zero squares.)

(b) We are asked to convert $4992 = 2^7 \times 3 \times 13$ into sum of four squares. Rewriting the given integer and using the rules of indices we have

$$\begin{aligned} 4992 &= 2^6 \times \underbrace{2 \times 3}_{=6} \times 13 \\ &= \left(2^3\right)^2 \times 6 \times 13 \\ &= 8^2 \times 6 \times 13 \qquad (\dagger) \end{aligned}$$

Writing 6 and 13 as sum of four squares gives

$$6 = 2^2 + 1^2 + 1^2 + 0^2 \text{ and } 13 = 3^2 + 2^2 + 0^2 + 0^2$$

Expressing 6×13 as sum of four squares gives

$$\begin{aligned} 6 \times 13 &= \left(2^2 + 1^2 + 1^2 + 0^2\right) \times \left(3^2 + 2^2 + 0^2 + 0^2\right) \\ &= \left(\left[2 \times 3\right] + \left[1 \times 2\right] + \left[1 \times 0\right] + \left[0 \times 0\right]\right)^2 + \left(\left[2 \times 2\right] - \left[1 \times 3\right] + \left[1 \times 0\right] - \left[0 \times 0\right]\right)^2 \\ &+ \left(\left[2 \times 0\right] - \left[1 \times 0\right] - \left[1 \times 3\right] + \left[0 \times 2\right]\right)^2 + \left(\left[2 \times 0\right] + \left[1 \times 0\right] - \left[1 \times 2\right] - \left[0 \times 3\right]\right)^2 \\ &= 8^2 + 1^2 + \left(-3\right)^2 + \left(-2\right)^2 = 8^2 + 3^2 + 2^2 + 1^2 \end{aligned}$$

Substituting this $6 \times 13 = 8^2 + 3^2 + 2^2 + 1^2$ into (†) gives

$$\begin{aligned} 4992 &= 8^2 \times 6 \times 13 \\ &= 8^2 \times \left(8^2 + 3^2 + 2^2 + 1^2\right) \\ &= \left(8 \times 8\right)^2 + \left(8 \times 3\right)^2 + \left(8 \times 2\right)^2 + \left(8 \times 1\right)^2 \\ &= 64^2 + 24^2 + 16^2 + 8^2 \end{aligned}$$

Hence 4992 as sum of four squares is $64^2 + 24^2 + 16^2 + 8^2$.

(c) 2015 factorizes into $5 \times 13 \times 31$. We can write

$$5 \times 13 = 65 = 8^2 + 1^2 + 0^2 + 0^2 \text{ so } 2015 = 5 \times 13 \times 31 = 65 \times 31$$

Also $31 = 5^2 + 2^2 + 1^2 + 1^2$. Putting these 65 and 31 together as sum of four squares and using identity (8.10) gives

$$\begin{aligned}65\times 31 &= \left(8^2+1^2+0^2+0^2\right)\times\left(5^2+2^2+1^2+1^2\right)\\ &= \left(\left[8\times 5\right]+\left[1\times 2\right]+\left[0\times 1\right]+\left[0\times 1\right]\right)^2+\left(\left[8\times 2\right]-\left[1\times 5\right]+\left[0\times 1\right]-\left[0\times 1\right]\right)^2\\ &\quad+\left(\left[8\times 1\right]-\left[1\times 1\right]-\left[0\times 5\right]+\left[0\times 2\right]\right)^2+\left(\left[8\times 1\right]+\left[1\times 1\right]-\left[0\times 2\right]-\left[0\times 1\right]\right)^2\\ &= 42^2+11^2+7^2+9^2\end{aligned}$$

Hence $2015 = 42^2+11^2+9^2+7^2$.

(d) We need to express 2016 into sum of four squares. Factorizing 2016 and using the rules of indices we have

$$\begin{aligned}2016 &= 2^5\times 3^2\times 7\\ &= \left(2^2\times 3\right)^2\times 2\times 7\\ &= 12^2\times 2\times 7 = 12^2\times 14\end{aligned}$$

Now 14 as sum of four squares is $14 = 3^2+2^2+1^2+0^2$. Substituting this $14 = 3^2+2^2+1^2+0^2$ into the above derivation yields

$$\begin{aligned}2016 &= 12^2\times\left(3^2+2^2+1^2+0^2\right)\\ &= \left(12\times 3\right)^2+\left(12\times 2\right)^2+\left(12\times 1\right)^2+\left(12\times 0\right)^2\\ &= 36^2+24^2+12^2+0^2\end{aligned}$$

(e) We need to convert 2020 into sum of four squares. We have

$$2020 = 2^2\times 5\times 101 \qquad (*)$$

We express 5 and 101 as sum of four squares

$$5 = 2^2+1^2+0^2+0^2 = 2^2+1^2 \text{ and } 101 = 10^2+1^2+0^2+0^2 = 10^2+1^2.$$

Since we have $5 = 2^2+1^2$ and $101 = 10^2+1^2$ we can use the Conversion Identity (8.1):

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

We have

$$\begin{aligned}5\times 101 &= \left(2^2+1^2\right)\times\left(10^2+1^2\right)\\ &= \left(20-1\right)^2+\left(2+10\right)^2\\ &= 19^2+12^2\end{aligned}$$

Substituting this $5\times 101 = 19^2+12^2$ into (*) gives

$$\begin{aligned}2020 &= 2^2\times\left(19^2+12^2\right)\\ &= 38^2+24^2\end{aligned}$$

We can write 2020 as sum of four squares as $38^2+24^2+0^2+0^2$.

3. (a) Factorizing 217 gives 7×31. Writing 7 and 31 as sum of four squares:

$$7 = 2^2 + 1^2 + 1^2 + 1^2 \text{ and } 31 = 5^2 + 2^2 + 1^2 + 1^2$$

Using identity (8.10):

$$\begin{aligned}\left(a^2+b^2+c^2+d^2\right)\times\left(x^2+y^2+z^2+w^2\right) &= \left(ax+by+cz+dw\right)^2 + \left(ay-bx+cw-dz\right)^2 \\ &\quad + \left(az-bw-cx+dy\right)^2 + \left(aw+bz-cy-dx\right)^2\end{aligned}$$

Gives

$$\begin{aligned}7\times 31 &= \left(2^2+1^2+1^2+1^2\right)\times\left(5^2+2^2+1^2+1^2\right) \\ &= \left(\left[2\times 5\right]+\left[1\times 2\right]+\left[1\times 1\right]+\left[1\times 1\right]\right)^2 + \left(\left[2\times 2\right]-\left[1\times 5\right]+\left[1\times 1\right]-\left[1\times 1\right]\right)^2 \\ &\quad + \left(\left[2\times 1\right]-\left[1\times 1\right]-\left[1\times 5\right]+\left[1\times 2\right]\right)^2 + \left(\left[2\times 1\right]+\left[1\times 1\right]-\left[1\times 2\right]-\left[1\times 5\right]\right)^2 \\ &= 14^2 + \left(-1\right)^2 + \left(-2\right)^2 + \left(-4\right)^2 = 14^2 + 4^2 + 2^2 + 1^2\end{aligned}$$

Therefore $217 = 14^2 + 4^2 + 2^2 + 1^2$.

(b) We need to convert 819 into sum of four squares. We have the prime factorization of 819:

$$819 = 3^2 \times 7 \times 13 \qquad (\ddagger)$$

Now $7 = 2^2 + 1^2 + 1^2 + 1^2$ and $13 = 3^2 + 2^2 + 0^2 + 0^2$. Using (8.10):

$$\begin{aligned}\left(a^2+b^2+c^2+d^2\right)\times\left(x^2+y^2+z^2+w^2\right) &= \left(ax+by+cz+dw\right)^2 + \left(ay-bx+cw-dz\right)^2 \\ &\quad + \left(az-bw-cx+dy\right)^2 + \left(aw+bz-cy-dx\right)^2\end{aligned}$$

We have

$$\begin{aligned}7\times 13 &= \left(2^2+1^2+1^2+1^2\right)\times\left(3^2+2^2+0^2+0^2\right) \\ &= \left(\left[2\times 3\right]+\left[1\times 2\right]+\left[1\times 0\right]+\left[1\times 0\right]\right)^2 + \left(\left[2\times 2\right]-\left[1\times 3\right]+\left[1\times 0\right]-\left[1\times 0\right]\right)^2 \\ &\quad + \left(\left[2\times 0\right]-\left[1\times 0\right]-\left[1\times 3\right]+\left[1\times 2\right]\right)^2 + \left(\left[2\times 0\right]+\left[1\times 0\right]-\left[1\times 2\right]-\left[1\times 3\right]\right)^2 \\ &= 8^2 + 1^2 + \left(-1\right)^2 + \left(-5\right)^2 \\ &= 8^2 + 5^2 + 1^2 + 1^2\end{aligned}$$

Substituting this $7\times 13 = 8^2 + 5^2 + 1^2 + 1^2$ into $(\ddagger)$ gives

$$\begin{aligned}819 &= 3^2 \times 7 \times 13 \\ &= 3^2 \times \left(8^2 + 5^2 + 1^2 + 1^2\right) \\ &= 24^2 + 15^2 + 3^2 + 3^2\end{aligned}$$

(c) We are asked to convert $2109 = 3\times 19\times 37$ into sum of four squares. We have $3\times 19 = 57 = 7^2 + 2^2 + 2^2 + 0^2$ and $37 = 6^2 + 1^2 + 0^2 + 0^2$. Now using identity (8.10) on 57×37 gives

$$\begin{aligned}57\times 37 &= \left(7^2+2^2+2^2+0^2\right)\times\left(6^2+1^2+0^2+0^2\right)\\ &= \left(\left[7\times 6\right]+\left[2\times 1\right]+\left[2\times 0\right]+\left[0\times 0\right]\right)^2+\left(\left[7\times 1\right]-\left[2\times 6\right]+\left[2\times 0\right]-\left[0\times 0\right]\right)^2\\ &\quad+\left(\left[7\times 0\right]-\left[2\times 0\right]-\left[2\times 6\right]+\left[0\times 1\right]\right)^2+\left(\left[7\times 0\right]+\left[2\times 0\right]-\left[2\times 1\right]-\left[0\times 6\right]\right)^2\\ &= 44^2+\left(-5\right)^2+\left(-12\right)^2+\left(-2\right)^2\\ &= 44^2+12^2+5^2+2^2\end{aligned}$$

Hence $2109 = 44^2+12^2+5^2+2^2$.

4. (i) The prime factorization of 343 is 7^3 and by the rules of indices we have

$$7^3 = 7^2\times 7 \text{ and } 7 = 2^2+1^2+1^2+1^2$$

Multiplying these gives

$$\begin{aligned}7^2\times 7 &= 7^2\times\left(2^2+1^2+1^2+1^2\right)\\ &= \left[7\times 2\right]^2+\left[7\times 1\right]^2+\left[7\times 1\right]^2+\left[7\times 1\right]^2\\ &= 14^2+7^2+7^2+7^2\end{aligned}$$

We have $343 = 14^2+7^2+7^2+7^2$.

(ii) We need to convert $2401 = 7^4$ into sum of four squares.

Easier to tackle this problem by using the rules of indices because

$$2401 = 7^4 = \left(7^2\right)^2 = 49^2 = 49^2+0^2+0^2+0^2$$

(iii) Applying the rules of indices gives $16\,807 = 7^5 = 7^4\times 7$. Using the result of part (ii) $7^4 = 49^2+0^2+0^2+0^2$ and the rules of indices on this $7^4\times 7$ gives

$$\begin{aligned}7^4\times 7 &= 49^2\times\left(2^2+1^2+1^2+1^2\right)\\ &= \left(49\times 2\right)^2+\left(49\times 1\right)^2+\left(49\times 1\right)^2+\left(49\times 1\right)^2\\ &= 98^2+49^2+49^2+49^2\end{aligned}$$

Therefore $16\,807 = 98^2+49^2+49^2+49^2$.

We need to predict a formula for converting 7^n into sum of four squares.

If n is even, $n = 2m$ say then by the rules of indices we have

$$7^n = 7^{2m} = \left(7^m\right)^2 = \left(7^m\right)^2+0^2+0^2+0^2$$

If n is odd, $n = 2m+1$ say then

$$\begin{aligned}7^n = 7^{2m+1} = \left(7^m\right)^2\times 7 &= \left(7^m\right)^2\times\left(2^2+1^2+1^2+1^2\right)\\ &= \left(2\times 7^m\right)^2+\left(7^m\right)^2+\left(7^m\right)^2+\left(7^m\right)^2\end{aligned}$$

Combining both of these we have

$$7^n = \begin{cases} \left(7^m\right)^2 + 0^2 + 0^2 + 0^2 & \text{if } n = 2m \\ \left(2\times 7^m\right)^2 + \left(7^m\right)^2 + \left(7^m\right)^2 + \left(7^m\right)^2 & \text{if } n = 2m+1 \end{cases}$$

For the general formula we have:

If n is even, $n = 2m$ say, then

$$x^n = x^{2m} = \left(x^m\right)^2 = \left(x^m\right)^2 + 0^2 + 0^2 + 0^2$$

If n is odd, $n = 2m+1$ say, then

$$\begin{aligned} x^n = x^{2m+1} = \left(x^m\right)^2 \times x &= \left(x^m\right)^2 \times \left(a^2 + b^2 + c^2 + d^2\right) \\ &= \left(ax^m\right)^2 + \left(bx^m\right)^2 + \left(cx^m\right)^2 + \left(dx^m\right)^2 \end{aligned}$$

Combining both of these we have

$$x^n = \begin{cases} \left(x^m\right)^2 + 0^2 + 0^2 + 0^2 & \text{if } n = 2m \\ \left(ax^m\right)^2 + \left(bx^m\right)^2 + \left(cx^m\right)^2 + \left(dx^m\right)^2 & \text{if } n = 2m+1 \end{cases}$$

5. (a) We need to convert $6a^2b^2$ into sum of four squares. Rewriting this $6a^2b^2$ as

$$\begin{aligned} 6a^2b^2 &= 4a^2b^2 + a^2b^2 + a^2b^2 + 0^2 \\ &= \left(2ab\right)^2 + \left(ab\right)^2 + \left(ab\right)^2 + 0^2 \end{aligned}$$

(b) We are asked to convert $7a^2b^2$ into sum of four squares. Well

$$7 = 2^2 + 1^2 + 1^2 + 1^2$$

Substituting this $7 = 2^2 + 1^2 + 1^2 + 1^2$ into $7a^2b^2$ gives

$$\begin{aligned} 7a^2b^2 &= \left(2^2 + 1^2 + 1^2 + 1^2\right)a^2b^2 \\ &= \left(2ab\right)^2 + \left(ab\right)^2 + \left(ab\right)^2 + \left(ab\right)^2 \end{aligned}$$

(c) We need to write na^2b^2 as sum of four squares. By Lagrange's Sum of Four Squares Theorem (8.14).

> *Every* positive integer can be expressed as sum of *four* squares.

We can write the integer n as sum of four squares:

$$n = x^2 + y^2 + z^2 + w^2$$

Substituting this $n = x^2 + y^2 + z^2 + w^2$ into na^2b^2 gives

$$\begin{aligned} na^2b^2 &= \left(x^2 + y^2 + z^2 + w^2\right)a^2b^2 \\ &= x^2a^2b^2 + y^2a^2b^2 + z^2a^2b^2 + w^2a^2b^2 \\ &= \left(xab\right)^2 + \left(yab\right)^2 + \left(zab\right)^2 + \left(wab\right)^2 \end{aligned}$$

6. We found some of the solutions to $x^2 + y^2 \equiv -1 \pmod{19}$ in Example 7 which were the following:

$$\{x \equiv 1,\ y \equiv 6 \pmod{19}\}, \{x \equiv 8,\ y \equiv 7 \pmod{19}\}, \{x \equiv 3,\ y \equiv 3 \pmod{19}\},$$
$$\{x \equiv 7,\ y \equiv 8 \pmod{19}\} \text{ and } \{x \equiv 6,\ y \equiv 1 \pmod{19}\}$$

By symmetry we have that if $x = a$ is a solution then so is $x = -a$ because

$$x^2 = a^2 = (-a)^2$$

From the above solution $\{x \equiv 1,\ y \equiv 6 \pmod{19}\}$ we have

$$\{x \equiv -1 \equiv 18,\ y \equiv 6 \pmod{19}\}, \{x \equiv 1,\ y \equiv -6 \equiv 13 \pmod{19}\} \text{ and}$$
$$\{x \equiv -1 \equiv 18,\ y \equiv -6 \equiv 13 \pmod{19}\}$$

From $\{x \equiv 8,\ y \equiv 7 \pmod{19}\}$ we have the solutions

$$\{x \equiv -8 \equiv 11,\ y \equiv 7 \pmod{19}\}, \{x \equiv 8,\ y \equiv -7 \equiv 12 \pmod{19}\} \text{ and}$$
$$\{x \equiv -8 \equiv 11,\ y \equiv -7 \equiv 12 \pmod{19}\}$$

From $\{x \equiv 3,\ y \equiv 3 \pmod{19}\}$ we have the solutions

$$\{x \equiv -3 \equiv 16,\ y \equiv 3 \pmod{19}\}, \{x \equiv 3,\ y \equiv -3 \equiv 16 \pmod{19}\} \text{ and}$$
$$\{x \equiv -3 \equiv 16,\ y \equiv -3 \equiv 16 \pmod{19}\}$$

From $\{x \equiv 7,\ y \equiv 8 \pmod{19}\}$ we have

$$\{x \equiv -7 \equiv 12,\ y \equiv 8 \pmod{19}\}, \{x \equiv 7,\ y \equiv -8 \equiv 11 \pmod{19}\} \text{ and}$$
$$\{x \equiv -7 \equiv 12,\ y \equiv -8 \equiv 11 \pmod{19}\}$$

From $\{x \equiv 6,\ y \equiv 1 \pmod{19}\}$ we have

$$\{x \equiv -6 \equiv 13,\ y \equiv 1 \pmod{19}\}, \{x \equiv 6,\ y \equiv -1 \equiv 18 \pmod{19}\} \text{ and}$$
$$\{x \equiv -6 \equiv 13,\ y \equiv -1 \equiv 18 \pmod{19}\}$$

All the solutions to the given equation are:

$$\{x = 1, y = 6\}, \{x = 1, y = 13\}, \{x = 3, y = 3\}, \{x = 3, y = 16\},$$
$$\{x = 6, y = 1\}, \{x = 6, y = 18\}, \{x = 7, y = 8\}, \{x = 7, y = 11\},$$
$$\{x = 8, y = 7\}, \{x = 8, y = 12\}, \{x = 11, y = 7\}, \{x = 11, y = 12\},$$
$$\{x = 12, y = 8\}, \{x = 12, y = 11\}, \{x = 13, y = 1\}, \{x = 13, y = 18\},$$
$$\{x = 16, y = 3\}, \{x = 16, y = 16\}, \{x = 18, y = 6\}, \{x = 18, y = 13\}$$

7. We need to solve

$$x^2 + y^2 \equiv -1 \pmod{13} \text{ which implies } x^2 \equiv -1 - y^2 \pmod{13}$$

We find *all* the incongruent solutions to this equation by reproducing Example 7 and using symmetry. The sets S, T, S' and T' are as defined in Example 7.

In this case we have $p = 13$ so $\dfrac{p-1}{2} = \dfrac{13-1}{2} = 6$. Therefore there are $6 + 1 = 7$ integers in each set;

$$S = \left\{0^2, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2\right\} = \left\{0, 1, 4, 9, 16, 25, 36\right\} \pmod{13}$$

$$\begin{aligned} T &= \left\{-1-0^2, -1-1^2, -1-2^2, -1-3^2, -1-4^2, -1-5^2, -1-6^2,\right\} \\ &= \left\{-1, -2, -5, -10, -17, -26, -37\right\} \pmod{13} \end{aligned}$$

The least non-negative residues modulo 13 of these sets are given by

$$S' = \left\{0,\ 1,\ 4,\ 9,\ 3,\ 12,\ 10\right\}$$

$$T' = \left\{12,\ 11,\ 8,\ 3,\ 9,\ 0,\ 2\right\}$$

There are four integers, 0, 3, 9 and 12, which are in *both* sets S' and T'. If we take the integer 0 which is common to both these sets then from the set S this corresponds to 0^2 the first element in S. The integer 0 is the sixth element in T' and it corresponds to the sixth element in the set T which is $-1-5^2$. Therefore we have

$$0^2 \equiv -1 - 5^2 \pmod{13} \quad \text{implies} \quad \{x = 0,\ y = 5\}$$

By symmetry we also have $y \equiv -5 \equiv 8 \pmod{13}$ so our solution is

$$\{x = 0,\ y = 8\}$$

Similarly for the remaining integers 3, 9 and 12 we have:

<u>For integer 3</u>: $\quad 4^2 \equiv -1 - 3^2 \pmod{13} \quad \text{implies} \quad \{x = 4,\ y = 3\}$

By symmetry we also have the solutions

$$\left\{x \equiv -4 \equiv 9,\ y \equiv 3 \pmod{13}\right\}, \quad \left\{x \equiv 4,\ y \equiv -3 \equiv 10 \pmod{13}\right\} \text{ and}$$

$$\left\{x \equiv -4 \equiv 9,\ y \equiv -3 \equiv 10 \pmod{13}\right\}$$

We can write these as

$$\{x = 4,\ y = 3\}, \{x = 9,\ y = 3\}, \{x = 4,\ y = 10\} \text{ and}$$

$$\{x = 9,\ y = 10\}$$

<u>For integer 9</u>: $\quad 3^2 \equiv -1 - 4^2 \pmod{13} \quad \text{implies} \quad \left\{x \equiv 3,\ y \equiv 4 \pmod{13}\right\}$

By symmetry we also have

$$\left\{x \equiv -3 \equiv 10,\ \ y \equiv 4 \left(\text{mod } 13\right)\right\},\ \left\{x \equiv 3,\ \ y \equiv -4 \equiv 9 \left(\text{mod } 13\right)\right\} \text{ and}$$

$$\left\{x \equiv -3 \equiv 10,\ \ y \equiv -4 \equiv 9 \left(\text{mod } 13\right)\right\}$$

We can write these as

$$\{x = 3,\ y = 4\},\ \{x = 10,\ y = 4\},\ \{x = 3,\ y = 9\} \text{ and}$$

$$\{x = 10,\ y = 9\}$$

For integer 12: $5^2 \equiv -1 - 0^2 \left(\text{mod } 13\right)$ implies $\left\{x \equiv 5,\ \ y \equiv 0 \left(\text{mod } 13\right)\right\}$

By symmetry we have

$$\left\{x \equiv -5 \equiv 8,\ \ y \equiv 0 \left(\text{mod } 13\right)\right\}$$

We have $\{x = 5,\ y = 0\},\ \{x = 8,\ y = 0\}$.

Hence *all* our solutions are given by

$\{x = 0,\ y = 5\},\ \{x = 0,\ y = 8\},\ \{x = 3,\ y = 4\},\ \{x = 3,\ y = 9\},$
$\{x = 4,\ y = 3\},\ \{x = 4,\ y = 10\},\ \{x = 5,\ y = 0\},\ \{x = 8,\ y = 0\},$
$\{x = 9,\ y = 3\},\ \{x = 9,\ y = 10\},\ \{x = 10,\ y = 4\},\ \{x = 10,\ y = 9\}$

8. We can write $2 = 1^2 + 1^2 + 0^2 + 0^2$. We have

$$2x = \left(1^2 + 1^2 + 0^2 + 0^2\right) \times \left(a^2 + b^2 + c^2 + d^2\right)$$

Applying four squares identity (8.10):

$$\left(a^2 + b^2 + c^2 + d^2\right) \times \left(x^2 + y^2 + z^2 + w^2\right) = \left(ax + by + cz + dw\right)^2 + \left(ay - bx + cw - dz\right)^2 + \left(az - bw - cx + dy\right)^2 + \left(aw + bz - cy - dx\right)^2$$

To $2x$ gives

$$\begin{aligned} 2x &= \left(a^2 + b^2 + c^2 + d^2\right) \times \left(1^2 + 1^2 + 0^2 + 0^2\right) \\ &= \left(\left[a \times 1\right] + \left[b \times 1\right] + 0 + 0\right)^2 + \left(\left[a \times 1\right] - \left[b \times 1\right] + 0 - 0\right)^2 \\ &\quad + \left(0 - 0 - \left[c \times 1\right] + \left[d \times 1\right]\right)^2 + \left(0 + 0 - \left[c \times 1\right] - \left[d \times 1\right]\right)^2 \\ &= \left(a + b\right)^2 + \left(a - b\right)^2 + \left(d - c\right)^2 + \left[\left(-1\right)\left(c + d\right)\right]^2 \\ &= \left(a + b\right)^2 + \left(a - b\right)^2 + \left(d - c\right)^2 + \left(c + d\right)^2 \qquad \left[\text{Because } \left(-1\right)^2 = 1\right] \end{aligned}$$

(i) We are given $1984 = 40^2 + 16^2 + 8^2 + 8^2$ and need to convert

$$\begin{aligned} 3968 &= 2 \times 1984 \\ &= 2 \times \left(40^2 + 16^2 + 8^2 + 8^2\right) = \left(40^2 + 16^2 + 8^2 + 8^2\right) \times \underbrace{\left(1^2 + 1^2 + 0^2 + 0^2\right)}_{=2} \end{aligned}$$

Using the above result $2x = (a+b)^2 + (a-b)^2 + (d-c)^2 + (c+d)^2$ with

$$a = 40,\ \ b = 16,\ \ c = 8 \ \text{ and } \ d = 8$$

Gives

$$\begin{aligned} 3968 &= 2 \times 1984 \\ &= (40+16)^2 + (40-16)^2 + (8-8)^2 + (8+8)^2 \\ &= 56^2 + 24^2 + 0^2 + 16^2 \end{aligned}$$

Thus $3968 = 56^2 + 24^2 + 16^2 + 0^2$.

(ii) We need to convert $992 = \dfrac{1984}{2}$ into sum of four squares. Using the given hint we have

$$992 = \frac{1984}{2} = \frac{2 \times 1984}{2 \times 2} = \frac{3968}{2^2}$$

We have

$$\begin{aligned} 992 = \frac{3968}{2^2} &= \frac{1}{2^2} \times \left(56^2 + 24^2 + 16^2 + 0^2\right) \qquad \left[\text{By Part (i)}\right] \\ &= \left(\frac{56}{2}\right)^2 + \left(\frac{24}{2}\right)^2 + \left(\frac{16}{2}\right)^2 + \left(\frac{0}{2}\right)^2 \\ &= 28^2 + 12^2 + 8^2 + 0^2 \end{aligned}$$

Hence $992 = 28^2 + 12^2 + 8^2 + 0^2$.

9. We need to show that $n > 169$ can be written as the sum of *five positive* squares.

Proof.

By the given hint we have $n = m + 169$. By Lagrange's Sum of Four Squares Theorem (8.14):

> *Every* positive integer can be expressed as sum of *four* squares.

We can write $m = a^2 + b^2 + c^2 + d^2$ where $a \geq 0,\ \ b \geq 0,\ \ c \geq 0$ and $d \geq 0$.

Substituting this $m = a^2 + b^2 + c^2 + d^2$ into $n = m + 169 = m + 13^2$ gives

$$n = a^2 + b^2 + c^2 + d^2 + 13^2 \qquad (*)$$

If all of these $a \geq 0,\ \ b \geq 0,\ \ c \geq 0$ and $d \geq 0$ are *positive* then we are done because we have five positive square integers.

We *cannot* have $a = b = c = d = 0$. *Why not?*

Because we are given $n > 169$.

We need to consider three cases;

Case I: One of these $a \geq 0,\ b \geq 0,\ c \geq 0$ and $d \geq 0$ is zero.

Case II: Two of these $a \geq 0,\ b \geq 0,\ c \geq 0$ and $d \geq 0$ are zero.

Case III: Three of these $a \geq 0,\ b \geq 0,\ c \geq 0$ and $d \geq 0$ are zero.

In each case we rewrite 13^2 as sum of two, three and four squares respectively.

Case I: Without loss of generality let $d = 0$ and $a > 0,\ b > 0,\ c > 0$.

Substituting this $d = 0$ into (*)

$$\begin{aligned} n &= a^2 + b^2 + c^2 + 0^2 + 13^2 \\ &= a^2 + b^2 + c^2 + 13^2 \\ &= a^2 + b^2 + c^2 + \underbrace{12^2 + 5^2}_{=13^2=169} \end{aligned}$$

Hence n is sum of five *positive* squares.

Case II: Without loss of generality let $c = d = 0$ and $a > 0,\ b > 0$.

Substituting this $c = d = 0$ into (*) gives

$$\begin{aligned} n &= a^2 + b^2 + 0^2 + 0^2 + 13^2 \\ &= a^2 + b^2 + 13^2 \\ &= a^2 + b^2 + \underbrace{12^2 + 4^2 + 3^2}_{=13^2} \end{aligned}$$

Thus n is sum of five *positive* squares.

Case III: Without loss of generality let $b = c = d = 0$ and $a > 0$. Substituting this $b = c = d = 0$ into (*) yields

$$\begin{aligned} n &= a^2 + 13^2 \\ &= a^2 + \underbrace{10^2 + 8^2 + 2^2 + 1^2}_{=13^2} \end{aligned}$$

Thus n is sum of five *positive* squares.

This completes our proof.

■

10. From the previous question we have

$$169 = 12^2 + 5^2,\ 169 = 12^2 + 4^2 + 3^2 \text{ and } 169 = 10^2 + 8^2 + 2^2 + 1^2$$

Thus 169 does *not* have a unique representation in terms of four squares.

11. *How do we prove the given result?*

By contradiction.

Proof.

Suppose $8m+7$ can be written as sum of three squares. Rewriting the given expression using $8=3^2-1^2$ and $7=2^2+1^2+1^2+1^2$ gives

$$\begin{aligned} 8m+7 &= \underbrace{\left(3^2-1^2\right)}_{=8}m+2^2+\underbrace{1^2+1^2+1^2}_{=3\times 1^2} \\ &= 3^2m+2^2+\left(3-m\right)1^2 \qquad \left[\text{Re-arranging}\right] \end{aligned}$$

Our supposition says that this $8m+7=3^2m+2^2+\left(3-m\right)1^2$ is sum of three squares. Therefore we must have

$$m=x^2 \quad \text{and} \quad 3-m=y^2 \text{ where } x \text{ and } y \text{ are integers.}$$

From these simultaneous equations $m=x^2$ and $3-m=y^2$ we have

$$3-m=3-x^2=y^2 \quad \Rightarrow \quad 3=x^2+y^2$$

This $3=x^2+y^2$ implies there are integers x and y such that $x^2+y^2=3$.

This is impossible because there are *no* integers x and y such that

$$x^2+y^2=3$$

We have a contradiction so our supposition $8m+7$ can be written as sum of three squares must be wrong.

Hence $8m+7$ *cannot* be written as sum of three squares. This completes our proof.

■

12. We are asked to prove:

> A positive integer which looks like $4^n\left(8m+7\right)$ *cannot* be expressed as a sum of three squares.

How do we prove this?

By mathematical induction.

Proof.

For $n=1$ we have

$$4^n\left(8m+7\right)=4\left(8m+7\right)=2^2\left(8m+7\right)$$

Now by the result of the last question we have $8m+7$ *cannot* be written as the sum of three squares so $2^2\left(8m+7\right)$ *cannot* be written as the sum of three squares. *Why not?*

Suppose $2^2\left(8m+7\right)$ can be written as the sum of three squares;

$$2^2\left(8m+7\right)=x^2+y^2+z^2$$

Since 2^2 is a factor of the left hand side so all three x, y and z must have factors of 2. Dividing $2^2\left(8m+7\right)=x^2+y^2+z^2$ by 2^2 gives

$$8m+7=\frac{1}{2^2}\left(x^2+y^2+z^2\right)=\left(\frac{x}{2}\right)^2+\left(\frac{y}{2}\right)^2+\left(\frac{z}{2}\right)^2$$

Now $\frac{x}{2}$, $\frac{y}{2}$ and $\frac{z}{2}$ are integers. This implies that $8m+7$ can be written as the sum of three squares which contradicts the result of the previous question.

Assume that the given result holds for $n=k$;

$4^k\left(8m+7\right)$ cannot be written as the sum of three squares

Required to prove the result for $n=k+1$;

$4^{k+1}\left(8m+7\right)$ cannot be written as the sum of three squares

Expanding $4^{k+1}\left(8m+7\right)$ gives

$$4^{k+1}\left(8m+7\right)=4^k4\left(8m+7\right)=2^24^k\left(8m+7\right)$$

By our induction hypothesis we know $4^k\left(8m+7\right)$ *cannot* be written as the sum of three squares. Therefore

$4^{k+1}\left(8m+7\right)=2^24^k\left(8m+7\right)$ *cannot* be written as sum of three squares

So by mathematical induction we have our result. Hence $4^n\left(8m+7\right)$ *cannot* be written as the sum of three squares.

■

13. We need to prove:

$$\left(a^2+b^2+c^2+d^2\right)\times\left(x^2+y^2+z^2+w^2\right)=\left(ax+by+cz+dw\right)^2+\left(ay-bx+cw-dz\right)^2$$
$$+\left(az-bw-cx+dy\right)^2+\left(aw+bz-cy-dx\right)^2$$

Proof.

Expanding the right hand side and simplifying gives us the required result.

■

14. We are asked to prove:

> Every prime can be expressed as the sum of four squares.

Proof.

Let p be prime. If $p=2$ then

$$2=1^2+1^2+0^2+0^2$$

We have our result.

Let p be an odd prime. By Corollary (8.12):

There exists a positive integer m with $m < p$ such that mp can be written as a sum of four squares.

We have

$$mp = a^2 + b^2 + c^2 + d^2 \text{ where } m < p \qquad (\dagger)$$

Let m be the least positive integer so that mp can be written as the sum of four squares.(Such an m exists by the well ordering principles which states that – every non-empty set of positive integers has a least element.)

Required to prove that m is equal to 1.

Suppose m is even.

Since mp is even so we *cannot* have an odd number of odd integers amongst a, b, c and d otherwise $a^2 + b^2 + c^2 + d^2$ would be odd. Therefore all four are even or two are odd and two are even or all four are odd.

Without loss of generality let

$$a \equiv b \pmod 2 \text{ and } c \equiv d \pmod 2$$

Consider

$$\left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 \underbrace{=}_{\text{Expanding}} \frac{a^2+b^2+c^2+d^2}{2} = \frac{mp}{2} = \left(\frac{m}{2}\right)p$$

This *cannot* be correct because $\frac{m}{2} < m$ and m was the least positive integer such that a multiple of p is the sum of four squares.

Hence m must be odd. Now we need to show that m is equal to 1.

Suppose $m > 1$.

Let x, y, z and w be non-negative integers such that

$$a \equiv x \pmod m,\ b \equiv y \pmod m,\ c \equiv z \pmod m \text{ and } d \equiv w \pmod m \qquad (\ddagger)$$

and these integers x, y, z and w satisfy $-\frac{m}{2} < x, y, z \text{ and } w < \frac{m}{2}$.

We have

$$a^2 + b^2 + c^2 + d^2 \equiv x^2 + y^2 + z^2 + w^2 \pmod m$$

Recall from above we have $mp = a^2 + b^2 + c^2 + d^2$ so this is congruent to 0 modulo m. Thus we have

$$a^2 + b^2 + c^2 + d^2 \equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod m \qquad (\ddagger\ddagger)$$

By the definition of congruence we have

$$x^2 + y^2 + z^2 + w^2 = mn \text{ where } n \text{ is non-negative} \qquad (*)$$

Since $-\frac{m}{2} < x, y, z$ and $w < \frac{m}{2}$ so

$$0 \le x^2 + y^2 + z^2 + w^2 < 4 \times \frac{m^2}{4} = m^2$$

From (*) we have the inequality

$$0 \le mn < m^2 \quad \text{which implies} \quad 0 \le n < m$$

We cannot have $n = 0$. *Why not?*

Suppose $n = 0$ then from (*)

$$x^2 + y^2 + z^2 + w^2 = 0 \;\Rightarrow\; x = y = z = w = 0$$

From (‡) we have

$$a \equiv x \equiv 0 \left(\text{mod } m\right),\ b \equiv y \equiv 0 \left(\text{mod } m\right),\ c \equiv z \equiv 0 \left(\text{mod } m\right) \text{ and}$$
$$d \equiv w \equiv 0 \left(\text{mod } m\right)$$

Therefore

$$mp = a^2 + b^2 + c^2 + d^2 = m^2 k \text{ or } m^2 \mid mp$$

From $m^2 \mid mp$ we have $m \mid p$. This $m \mid p$ *cannot* be true because from the start we have $1 < m < p$. Hence $n \neq 0$ [Not equal].

So $1 \le n < m$.

Multiplying the equations in (†) and (*) gives

$$mp \times mn = \left(a^2 + b^2 + c^2 + d^2\right) \times \left(x^2 + y^2 + z^2 + w^2\right)$$

Applying the sum of squares identity (8.10) to this product gives

$$\begin{aligned}\left(mp\right) \times \left(mn\right) &= \left(a^2 + b^2 + c^2 + d^2\right) \times \left(x^2 + y^2 + z^2 + w^2\right) \\ &= \left(ax + by + cz + dw\right)^2 + \left(ay - bx + cw - dz\right)^2 \\ &\quad + \left(az - bw - cx + dy\right)^2 + \left(aw + bz - cy - dx\right)^2\end{aligned}$$

On the right hand side we have a sum of four squares. Let us write each of the terms in the bracket as a single symbol. So let

$$\begin{aligned} r &= ax + by + cz + dw \\ s &= ay - bx + cw - dz \\ t &= az - bw - cx + dy \\ u &= aw + bz - cy - dx \end{aligned}$$

Substituting this into the above equation gives

$$\left(mp\right) \times \left(mn\right) = m^2 \times np = r^2 + s^2 + t^2 + u^2 \qquad (***)$$

Note that from (‡) and (‡‡) we have

$$r = ax + by + cz + dw \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \left(\text{mod } m\right)$$

Similarly $s \equiv 0 \pmod{m}$, $t \equiv 0 \pmod{m}$ and $u \equiv 0 \pmod{m}$.

This means that r, s, t and u are *all* divisible by m. Additionally

$$r^2,\ s^2,\ t^2 \text{ and } u^2 \text{ are divisible by } m^2$$

Dividing the equation in (***) by m^2 gives

$$np = \frac{1}{m^2}\left(r^2 + s^2 + t^2 + u^2\right) = \left(\frac{r}{m}\right)^2 + \left(\frac{s}{m}\right)^2 + \left(\frac{t}{m}\right)^2 + \left(\frac{u}{m}\right)^2$$

Where $n < m$. *Why is* $n < m$ *?*

Because from above we have $1 \le n < m$. We have now expressed np as sum of four squares. This contradicts that m is the least integer such that mp is the sum of four squares. Hence $m = 1$. Therefore

$$a^2 + b^2 + c^2 + d^2 = mp = 1 \times p = p$$

This is our required result and so completes our proof.

■