## Complete Solutions to Exercises 8.1

1. (a) 36 is already a square number so $36 = 6^2 + 0^2$.

   (b) 37 is one more than 36 so $37 = 6^2 + 1^2$.

   (c) Again 101 is 1 more than 100 which is $10^2$ so $101 = 10^2 + 1^2$.

   (d) We have $170 = 169 + 1 = 13^2 + 1^2$.

   (e) The sum of squares for 229 is harder to spot but can be done by inspection:

   $$229 = 225 + 4 = 15^2 + 2^2$$

2. (a) Note that $256 = 16^2 = 16^2 + 0^2$.

   (b) Since 281 is close to 256, we find that the difference between these numbers, 281 and 256, is $25 = 5^2$. So $281 = 256 + 25 = 16^2 + 5^2$.

   (c) 512 is a power of 2; that is $2^9 = 512$. We have

   $$\begin{aligned} 512 = 2^9 = 2^8 \times 2 &= \left(2^4\right)^2 \times \left(1^2 + 1^2\right) \\ &= 16^2 \times \left(1^2 + 1^2\right) = 16^2 + 16^2 \end{aligned}$$

   (d) Again 2048 is a power of 2 integer; $2^{11} = 2048$. Writing this as the sum of two squares gives

   $$2048 = 2^{11} = \left(2^5\right)^2 \times 2 = 32^2 \times \left(1^2 + 1^2\right) = 32^2 + 32^2.$$

3. For this question we can use the Sum of Squares Theorem (8.5):

   > $n = p_1 \times p_2 \times \cdots \times p_r \times N^2$ can be expressed as sum of two squares provided every prime $p_j$ satisfies $p_j = 2$ or $p_j \equiv 1 \pmod 4$ for $j = 1, \cdots, r$.

   If we want to use this theorem we need to first factorize our given integer.

   (a) Since 202 is an even number so 2 is a factor. The factorization of 202 into its primes is given by

   $$202 = 2 \times 101$$

   Since our primes satisfy $p_j = 2$ or $p_j \equiv 1 \pmod 4$ so we can write this integer as the sum of two squares:

   $$202 = 2 \times 101 = \left(1^2 + 1^2\right) \times \left(10^2 + 1^2\right)$$

   *How do we convert* $\left(1^2 + 1^2\right) \times \left(10^2 + 1^2\right)$ *into sum of two squares?*

   By using the Conversion Identity (8.1):

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

Applying this to $\left(1^2+1^2\right)\times\left(10^2+1^2\right)$ gives

$$\begin{aligned}\left(1^2+1^2\right)\times\left(10^2+1^2\right) &= \left(\left[1\times 10\right]-\left[1\times 1\right]\right)^2+\left(\left[1\times 1\right]+\left[1\times 10\right]\right)^2\\ &= 9^2+11^2\end{aligned}$$

Hence $202 = 9^2+11^2$.

(b) Factorizing $205 = 5\times 41$. Since $5\equiv 41\equiv 1\pmod 4$ so we can convert 205 into sum of two squares:

$$\begin{aligned}205 &= 5\times 41\\ &= \left(2^2+1^2\right)\times\left(25+16\right)\\ &= \left(2^2+1^2\right)\times\left(5^2+4^2\right)\end{aligned}$$

Now we need to rewrite $205 = \left(2^2+1^2\right)\times\left(5^2+4^2\right)$ as the sum of two squares. Using the identity (8.1) we have

$$\begin{aligned}205 &= \left(2^2+1^2\right)\times\left(5^2+4^2\right)\\ &= \left(\left[2\times 5\right]-\left[1\times 4\right]\right)^2+\left(\left[2\times 4\right]+\left[1\times 5\right]\right)^2 \qquad \left[\text{By (8.1)}\right]\\ &= 6^2+13^2\end{aligned}$$

(c) We need to convert 180 to sum of two squares. Factorizing 180 gives

$$\begin{aligned}180 &= 4\times 9\times 5\\ &= 2^2\times 3^2\times 5\\ &= 5\times\left(2\times 3\right)^2 = 5\times 6^2\end{aligned}$$

This $180 = 5\times 6^2$ is in the correct format, $n = p_1\times p_2\times\cdots\times p_r\times N^2$, of using the Sum of Squares Theorem. Since $p_1 = 5\equiv 1\pmod 4$ so we can write 180 as the sum of two squares:

$$180 = 5\times 6^2 = \left(2^2+1^2\right)\times 6^2 = 12^2+6^2$$

4. (a) We need to convert 2016 into sum of two squares. The prime factorization of 2016 is given by:

$$\begin{aligned}2016 = 2\times 1008 &= 2\times 2\times 504\\ &= 2^2\times 2\times 252\\ &= 2^3\times 2\times 126\\ &= 2^4\times 2\times 63 = 2^5\times 9\times 7 = 2^5\times 3^2\times 7\end{aligned}$$

By Corollary (8.8):

> $n = p_1\times p_2\times\cdots\times p_r\times N^2$ *cannot* be expressed as sum of two squares $\Leftrightarrow$ it has *a* prime factor $p_j\equiv 3\pmod 4$.

Since $7 \equiv 3 \left(\text{mod } 4\right)$ and 7 is to the index 1 so $2016 = 2^5 \times 3^2 \times 7$ *cannot* be expressed as the sum of two squares.

(b) The prime factorization of 2015 is given by

$$2015 = 5 \times 13 \times 31$$

Since $31 \equiv 3 \left(\text{mod } 4\right)$ so by the above corollary we conclude that 2015 *cannot* be expressed as the sum of two squares.

(c) We need to convert 2017 into sum of two squares. We are informed that 2017 is prime so we only need to test if it satisfies $p \equiv 1 \left(\text{mod } 4\right)$:

$$2017 \equiv 1 \left(\text{mod } 4\right)$$

Hence we can write 2017 as the sum of two squares. Taking the square root of 2017 as suggested in the hint we have

$$\sqrt{2017} = 44.911 \left(3\text{dp}\right)$$

Taking the floor function of this

$$\left\lfloor \sqrt{2017} \right\rfloor = \left\lfloor 44.911 \right\rfloor = 44$$

Finding the difference between 2017 and 44 squared we have

$$2017 - 44^2 = 81 = 9^2$$

Rearranging this so that 2017 is the subject gives

$$2017 = 9^2 + 44^2 .$$

(d) This time we are required to express 2018 $\left(2 \times 1009\right)$ as the sum of two squares. First we need to test whether 1009 is congruent to 1 modulo 4:

$$1009 \equiv 1 \left(\text{mod } 4\right).$$

Therefore we can write 2018 as the sum of two squares. Using the other part of the hint we have

$$1009 - 28^2 = 225 = 15^2 .$$

Rearranging this gives $1009 = 28^2 + 15^2$. Substituting this $1009 = 28^2 + 15^2$ into $2018 = 2 \times 1009$ yields

$$\begin{aligned} 2018 &= 2 \times 1009 \\ &= 2 \times \left(28^2 + 15^2\right) \\ &= \left(1^2 + 1^2\right) \times \left(28^2 + 15^2\right) \end{aligned}$$

Applying 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

$$\begin{aligned}2018 &= \left(1^2+1^2\right)\times\left(28^2+15^2\right)\\ &= \left(\left[1\times 28\right]-\left[1\times 15\right]\right)^2+\left(\left[1\times 15\right]+\left[1\times 28\right]\right)^2\\ &= 13^2+43^2\end{aligned}$$

(e) We are given $2019 = 3\times 673$ and as 3 is a factor of 2019 so we *cannot* express 2019 as the sum of two squares. *Why not?*

Because by Corollary (8.8):

> $n = p_1\times p_2\times\cdots\times p_r\times N^2$ *cannot* be expressed as sum of two squares $\Leftrightarrow$ it has *a* prime factor $p_j \equiv 3\left(\text{mod } 4\right)$.

We have $3\equiv 3\left(\text{mod } 4\right)$ so 2019 *cannot* be converted into sum of two squares.

(f) The prime factorization of 2020 is given by

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

Since the primes 5 and 101 in this factorization satisfy

$$5\equiv 101\equiv 1\left(\text{mod } 4\right),$$

so we can express 2020 as the sum of two squares:

$$5\times 101 = \left(2^2+1^2\right)\times\left(10^2+1^2\right)$$

Using 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

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

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

$$\begin{aligned}2020 &= 2^2\times 5\times 101\\ &= 2^2\times\left(19^2+12^2\right)\\ &= \left(2\times 19\right)^2+\left(2\times 12\right)^2 = 38^2+24^2\end{aligned}$$

Hence we can write 2020 as $38^2+24^2$.

5. (a) We have

$$\left(3n\right)^2+\left(4n\right)^2 = 9n^2+16n^2 = 25n^2 = \left(5n\right)^2.$$

(b) We have

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

(c) Similarly, we have

$$\left(2mn\right)^2+\left(n^2-m^2\right)^2=4m^2n^2+n^4-2m^2n^2+m^4=n^4+2m^2n^2+m^4=\left(n^2+m^2\right)^2.$$

6. We are asked to prove that $2^n$ is sum of two squares.

*Proof.*

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

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

So we can write this as the sum of two squares.

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

$$2^n=2^{2m+1}=\left(2^m\right)^2 2=\left(2^m\right)^2\left(1^2+1^2\right)=\left(2^m\right)^2+\left(2^m\right)^2.$$

Again we can express $2^n$ is sum of two squares.

Since $n$ can only be odd or even so we have completed our proof.

■

7. We need to prove that $n^k$ where $k$ is an even positive integer can be written as sum of two squares.

*Proof.*

Since we are given that $k$ is an even positive integer, so let $k=2m$. Therefore by using the rules of indices we have

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

Hence $n^k$ where $k$ is an even positive integer can be expressed as the sum of two squares.

■

8. We need to prove that $k^2n$ can be expressed as the sum of two squares provided $n$ can be represented by sum of two squares.

*Proof.*

We are given that $n$ can be expressed as the sum of two squares, so

$$n=a^2+b^2.$$

Therefore

$$k^2 n = k^2\left(a^2 + b^2\right) = \left(ka\right)^2 + \left(kb\right)^2.$$

Hence $k^2 n$ can be expressed as the sum of two squares.

■

9. We are asked to prove;

> Let $p$ be prime such that $p \equiv 1 \pmod 4$ and $k$ be a natural number. Then we can write $n = p^k$ as the sum of two squares.

*Proof.*

Since we are given the prime $p \equiv 1 \pmod 4$ so we can express this as the sum of two squares; $p = a^2 + b^2$. If $k$ is even, say $k = 2m$ then we are done because

$$n = p^k = p^{2m} = \left(p^m\right)^2 = \left(p^m\right)^2 + 0^2.$$

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

$$\begin{aligned} n = p^k &= p^{2m+1} \\ &= p\left(p^m\right)^2 = \left(a^2 + b^2\right)\left(p^m\right)^2 \\ &= a^2\left(p^m\right)^2 + b^2\left(p^m\right)^2 = \left(ap^m\right)^2 + \left(bp^m\right)^2 \end{aligned}$$

Hence $n = p^k$ can be written as the sum of two squares.

■

10. We are asked to prove that if $p \equiv 1 \pmod 4$ then there exists positive integers $x$ and $y$ such that $x^2 + y^2 = kp$ where $k < p$ and it is a positive integer.

*Proof.*

We assume $p \equiv 1 \pmod 4$ which implies $-1$ is a quadratic residue of $p$ thus $\left(\frac{-1}{p}\right) = 1$. From the quadratic congruence $x^2 \equiv -y^2 \pmod p$ we know that $y^2$ is a quadratic residue of $p$. The product of QR with QR gives us a QR, so $-y^2$ is a quadratic residue of $p$. Hence $x^2 \equiv -y^2 \pmod p$ has solutions so there are integers $x$ and $y$ such that $x^2 + y^2 \equiv 0 \pmod p$. Hence $x^2 + y^2 = kp$. We also need to show that $0 < k < p$.

If we chose $y = 1$ then the quadratic congruence $x^2 + 1 \equiv 0 \pmod p$ which we can rewrite as $x^2 \equiv -1 \pmod p$ has solutions because we are given

$p \equiv 1 \pmod 4$. By the symmetrical nature of the quadratic solutions we have $1 \le x \le \dfrac{p-1}{2}$. Therefore $1 \le x^2 \le \left(\dfrac{p-1}{2}\right)^2$. Examining

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

Hence $x^2 + 1 < p^2$. So there exists positive integers $x$ and $y$ such that $x^2 + y^2 = kp$ where $k < p$.

■

11. We need to prove that any integer $n > 1$ can be written as

$$n = p_1 \times p_2 \times \cdots \times p_r \times N^2$$

*Proof.*

Let $n > 1$. By the Fundamental Theorem of Arithmetic (2.5):

> Every integer $n$ greater than 1 is either a prime or can be written uniquely as a product of primes apart from the order in the following manner:
>
> $$n = p_1^{k_1} \times p_2^{k_2} \times p_3^{k_3} \times \cdots \times p_l^{k_l}$$

So by this theorem we can write any integer greater than 1 as

$$n = p_1^{k_1} \times p_2^{k_2} \times p_3^{k_3} \times \cdots \times p_l^{k_l}$$

(If $n$ is prime then we can write this as $n = p_1$.)

Consider an arbitrary index $k_j$ where $j = 1, \cdots, l$.

Now the index $k_j$ can only be odd or even.

Let us first take the case where $k_j$ is odd. Let $k_j = 2m+1$ where $m$ is an integer $\ge 0$. Then by using the rules of indices we have

$$p_j^{k_j} = p_j^{2m+1} = p_j \times \left(p_j^{m}\right)^2$$

If the index $k_j$ is even, $k_j = 2m$ say, where $m \ge 1$ is an integer, then

$$p_j^{k_j} = p_j^{2m} = \left(p_j^{m}\right)^2$$

Writing the integer $n = p_1^{k_1} \times p_2^{k_2} \times p_3^{k_3} \times \cdots \times p_l^{k_l}$ so that all the primes which have an odd index are written first. Assume there are $r$ of these primes with an odd index;

$$p_1,\ p_2, \cdots,\ p_r$$

Therefore we have

$$
\begin{aligned}
n &= p_1^{k_1} \times p_2^{k_2} \times p_3^{k_3} \times \cdots \times p_l^{k_l} \\
&= \underbrace{p_1^{2m_1+1} \times p_2^{2m_2+1} \times \cdots \times p_r^{2m_r+1}}_{\text{primes with an odd index}} \times \underbrace{\left(p_{r+1}^{2m_{r+1}} \times \cdots \times p_l^{2l}\right)}_{\text{primes with an even index}} \\
&\underbrace{=}_{\substack{\text{using the} \\ \text{rules of indices}}} p_1 \times p_2 \times \cdots \times p_r \times \left(p_1^{2m_1} \times p_2^{2m_2} \times \cdots \times p_r^{2m_r}\right) \times \left(p_{r+1}^{2m_{r+1}} \times \cdots \times p_l^{2l}\right) \\
&= p_1 \times p_2 \times \cdots \times p_r \times \left(p_1^{m_1} \times p_2^{m_2} \times \cdots \times p_r^{m_r}\right)^2 \times \left(p_{r+1}^{m_{r+1}} \times \cdots \times p_l^{l}\right)^2 \\
&\underbrace{=}_{\text{rearranging}} p_1 \times p_2 \times \cdots \times p_r \times \left(p_1^{m_1} \times p_2^{m_2} \times \cdots \times p_r^{m_r} \times p_{r+1}^{m_{r+1}} \times \cdots \times p_l^{l}\right)^2 \\
&= p_1 \times p_2 \times \cdots \times p_r \times N^2 \quad \text{where } N = p_1^{m_1} \times p_2^{m_2} \times \cdots \times p_r^{m_r} \times p_{r+1}^{m_{r+1}} \times \cdots \times p_l^{l}
\end{aligned}
$$

Hence every positive integer $n$ greater than 1 can be written as

$$n = p_1 \times p_2 \times \cdots \times p_r \times N^2$$

This completes our proof.

■

12. We need to prove the identity:

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

*Proof.*

Expanding the left - hand side of the given statement gives

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

Expanding the right - hand side yields

$$
\begin{aligned}
\left(ac + bd\right)^2 + \left(ad - bc\right)^2 &= a^2c^2 + 2abcd + b^2d^2 + \left(a^2d^2 - 2abcd + b^2c^2\right) \\
&= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2
\end{aligned}
$$

Since both sides are equal, so the given identity holds.

■

13. In each case we use the Conversion Identity (8.1):

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

(a) We need to write $5^2$ as the sum of two non-zero squares:

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

(b) Now we need to convert $17^2$ into the sum of two non-zero squares

$$\begin{aligned} 17^2 = 17\times 17 &= \left(4^2+1^2\right)\times\left(4^2+1^2\right) \\ &= \left(\left[4\times 4\right]-\left[1\times 1\right]\right)^2+\left(\left[4\times 1\right]+\left[1\times 4\right]\right)^2 \qquad \left[\text{By (8.1)}\right] \\ &= 15^2+8^2 \end{aligned}$$

(c) Similarly for $29^2$ we have

$$\begin{aligned} 29^2 = 29\times 29 &= \left(5^2+2^2\right)\times\left(5^2+2^2\right) \\ &= \left(\left[5\times 5\right]-\left[2\times 2\right]\right)^2+\left(\left[5\times 2\right]+\left[2\times 5\right]\right)^2 \qquad \left[\text{By (8.1)}\right] \\ &= 21^2+20^2 \end{aligned}$$

Hence we can write $29^2$ as $20^2+21^2$.

(d) From the solution to question 3(a) we have $202 = 9^2+11^2$:

$$\begin{aligned} 202^2 = \left(9^2+11^2\right)^2 &= \left(9^2+11^2\right)\times\left(9^2+11^2\right) \\ &= \left(\left[9\times 9\right]-\left[11\times 11\right]\right)^2+\left(\left[9\times 11\right]+\left[11\times 9\right]\right)^2 \qquad \left[\text{By (8.1)}\right] \\ &= \left(-40\right)^2+198^2 = 40^2+198^2 \end{aligned}$$

14. We need to show $\left(a^2+b^2\right)^2 = \left(a^2-b^2\right)^2+\left(2ab\right)^2$.

*Proof.*

Squaring $a^2+b^2$ and using the Conversion Identity (8.1) we have

$$\begin{aligned} \left(a^2+b^2\right)^2 &= \left(a^2+b^2\right)\times\left(a^2+b^2\right) \\ &= \left(\left[a\times a\right]-\left[b\times b\right]\right)^2+\left(\left[a\times b\right]+\left[b\times a\right]\right)^2 \qquad \left[\text{By Identity (8.1)}\right] \\ &= \left(a^2-b^2\right)^2+\left(2ab\right)^2 \end{aligned}$$

We have our required result. ∎

15. We are asked to show that

if $\gcd\left(x,\ \ y\right)=1$ and $x^2+y^2=z^2$ then $\gcd\left(x,\ \ z\right)=\gcd\left(y,\ \ z\right)=1$.

*Proof.*

By contradiction.

Suppose $\gcd\left(x,\ \ z\right)=g>1$ then there are integers $a$ and $b$ such that

$$ga = x,\ \ gb = z\,.$$

Substituting this into $x^2+y^2=z^2$ gives

$$\left(ga\right)^2+y^2=\left(gb\right)^2 \ \Rightarrow\ y^2=g^2\left(a^2+b^2\right) \ \Rightarrow\ g^2 \mid y^2 \ \Rightarrow\ g \mid y$$

We have $g \mid y$ and from our supposition $\gcd\left(x,\ \ z\right)=g>1$ we have

$$g \mid x$$

Hence $g \mid x$ and $g \mid y$ therefore $\gcd(x, \ y) \geq g > 1$. This is a contradiction because we are given $\gcd(x, \ y) = 1$. Hence $\gcd(x, \ z) = 1$ and similarly $\gcd(y, \ z) = 1$. This completes our proof.

■

16. We need to find the unknowns $x$ and $y$ such that $x^2 + y^2 = 178$.
For this we need to write 178 as sum of two squares; $x^2 + y^2$.
Factorizing 178 gives $178 = 2 \times 89$. Since the prime 89 satisfies

$$89 \equiv 1 \pmod 4,$$

so we can express $178 = 2 \times 89$ as the sum of two squares. Converting 89 into sum of two squares gives

$$89 = 64 + 25 = 8^2 + 5^2.$$

Therefore

$$\begin{aligned} 178 = 2 \times 89 &= \left(1^2 + 1^2\right) \times \left(8^2 + 5^2\right) \\ &= \left(\left[1 \times 8\right] - \left[1 \times 5\right]\right)^2 + \left(\left[1 \times 5\right] + \left[1 \times 8\right]\right)^2 \\ &= 3^2 + 13^2 \end{aligned}$$

Since $3^2 + 13^2 = 178$ so $x = 3$ and $y = 13$ or vice-versa.

17. We are asked to express $1105 = 5 \times 13 \times 17$ as the sum of two squares in 4 different ways. First we need to establish that we can write $1105 = 5 \times 13 \times 17$ as the sum of two squares. Since

$$5 \equiv 13 \equiv 17 \equiv 1 \pmod 4$$

So we can write this 1105 as the sum of two squares.
<u>First sum of square representation</u>:
Converting the first two multiples of $1105 = 5 \times 13 \times 17$ into sum of squares

$$5 = 2^2 + 1^2 \text{ and } 13 = 3^2 + 2^2$$

Using the identity (8.1):

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

On $5 \times 13 = \left(2^2 + 1^2\right) \times \left(3^2 + 2^2\right)$ gives

$$\begin{aligned}5\times 13 &= \left(2^2+1^2\right)\times\left(3^2+2^2\right)\\ &= \left(\left[2\times 3\right]-\left[1\times 2\right]\right)^2+\left(\left[2\times 2\right]+\left[1\times 3\right]\right)^2\\ &= 4^2+7^2\end{aligned}$$

Substituting this $5\times 13 = 4^2+7^2$ into the above integer $1105 = 5\times 13\times 17$ gives

$$\begin{aligned}1105 &= \underbrace{5\times 13}_{=4^2+7^2}\times 17\\ &= \left(4^2+7^2\right)\times 17\\ &= \left(4^2+7^2\right)\times\left(4^2+1^2\right) \qquad (\dagger)\\ &= \left(\left[4\times 4\right]-\left[7\times 1\right]\right)^2+\left(\left[4\times 1\right]+\left[7\times 4\right]\right)^2\\ &= 9^2+32^2\end{aligned}$$

So one sum of two square representation of 1105 is $9^2+32^2$.

<u>Second sum of square representation</u>:

Using the above evaluation in (†) but changing the order of the integers:

$$\begin{aligned}1105 &= \left(4^2+7^2\right)\times\left(4^2+1^2\right)\\ &= \left(7^2+4^2\right)\times\left(4^2+1^2\right) \qquad \left[\text{Changing the integers in the first bracket}\right]\\ &= \left(\left[7\times 4\right]-\left[4\times 1\right]\right)^2+\left(\left[7\times 1\right]+\left[4\times 4\right]\right)^2\\ &= 24^2+23^2\end{aligned}$$

<u>Third sum of square representation</u>:

From the first representation we have

$$5 = 2^2+1^2,\ 13 = 3^2+2^2 \text{ and } 17 = 4^2+1^2$$

Changing the order of multiplication we have

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

Substituting this $13\times 17 = 10^2+11^2$ into $1105 = 5\times 13\times 17$ gives

$$\begin{aligned}1105 &= 5\times\left(13\times 17\right)\\ &= \left(1^2+2^2\right)\times\left(10^2+11^2\right)\\ &= \left(\left[1\times 10\right]-\left[2\times 11\right]\right)^2+\left(\left[1\times 11\right]+\left[2\times 10\right]\right)^2\\ &= \left(-12\right)^2+31^2 = 12^2+31^2\end{aligned}$$

<u>Fourth sum of square representation</u>:

Changing the order of multiplication

$$1105 = 5\times 17\times 13$$

Using the previous derivations gives

$$5 = 2^2 + 1^2,\ 17 = 4^2 + 1^2 \text{ and } 13 = 3^2 + 2^2$$

Putting these into $1105 = 5 \times 17 \times 13$ yields

$$\begin{aligned} 1105 &= 5 \times 17 \times 13 \\ &= \left[\left(2^2 + 1^2\right) \times \left(4^2 + 1^2\right)\right] \times \left(2^2 + 3^2\right) \\ &= \left[\left(\left[2 \times 4\right] - \left[1 \times 1\right]\right)^2 + \left(\left[2 \times 1\right] + \left[1 \times 4\right]\right)^2\right] \times \left(2^2 + 3^2\right) \\ &= \left[7^2 + 6^2\right] \times \left(2^2 + 3^2\right) \\ &= \left(14 - 18\right)^2 + \left(21 + 12\right)^2 \\ &= \left(-4\right)^2 + 33^2 = 4^2 + 33^2 \end{aligned}$$

The four different sum of two squares of 1105 are

$$9^2 + 32^2,\ 24^2 + 23^2,\ 12^2 + 31^2 \text{ and } 4^2 + 33^2$$

18. We are asked to prove that if $n = p \times q$ where $p \equiv q \equiv 1 \pmod 4$ then we can write $n$ as sum of two squares.

*Proof.*

As we are given that $p \equiv q \equiv 1 \pmod 4$ so we can write these as sum of two squares. Let $p = a^2 + b^2$ and $q = c^2 + d^2$. Applying the 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

$$n = p \times q = \left(a^2 + b^2\right) \times \left(c^2 + d^2\right) \underbrace{=}_{\text{By (8.1)}} \left(ac - bd\right)^2 + \left(ad + bc\right)^2$$

Hence, we can write $n = p \times q$ where $p \equiv q \equiv 1 \pmod 4$ as the sum of two squares.

■

19. (a) The integer 6 *cannot* be converted into sum of two squares because the prime decomposition of $6 = 2 \times 3$ and $3 \equiv 3 \pmod 4$ so by Corollary (8.8):

> $n = p_1 \times p_2 \times \cdots \times p_r \times N^2$ *cannot* be expressed as sum of two squares $\Leftrightarrow$ it has *a* prime factor $p_j \equiv 3 \pmod 4$.

Hence 6 cannot be written as the sum of two squares.

(b) We are asked to show that if $n \equiv 3$ or $6 \pmod 9$ then $n$ *cannot* be expressed as the sum of two squares.

*Proof.*

Consider each case; $n \equiv 3 \pmod 9$ and then $n \equiv 6 \pmod 9$.

Case I: $n \equiv 3 \pmod 9$

By the definition of congruence we have

$$n = 9k + 3 \text{ where } k \text{ is an integer}$$

We can rewrite this by factorizing

$$n = 9k + 3 = 3(3k + 1)$$

Since the prime 3 is a factor of $n$ and 3 cannot be a factor of $3k + 1$ so $n$ can only have one 3 in its prime decomposition. By Corollary (8.8):

> $n = p_1 \times p_2 \times \cdots \times p_r \times N^2$ *cannot* be expressed as sum of two squares $\Leftrightarrow$ it has *a* prime factor $p_j \equiv 3 \pmod 4$.

We conclude that $n$ *cannot* be expressed as the sum of two squares.

Case II: $n \equiv 6 \pmod 9$

Similarly in this case we have

$$n = 9k + 6 = 3(3k + 2)$$

The integer $n$ only has one 3 in its prime factorization so by the above Corollary (8.8) we can say that $n$ *cannot* be written as the sum of two squares.

■

(c) We are asked to prove that if $n \equiv 6, 12, 24, 30 \pmod{36}$ then $n$ *cannot* be expressed as the sum of two squares.

*Proof.*

By the definition of congruence we can write each of these integers as

$$n = 36k + 6,\ 36k + 12,\ 36k + 24 \text{ and } 36k + 30 \text{ for some integer } k.$$

Factorizing these gives

$$\begin{aligned} n &= 6(6k + 1),\ 6(6k + 2),\ 6(6k + 4) \text{ and } 6(6k + 5) \\ &= 2 \times 3 \times (6k + 1),\ 2 \times 3 \times (6k + 2),\ 2 \times 3 \times (6k + 4) \text{ and } 2 \times 3 \times (6k + 5) \end{aligned}$$

In each of these cases there is only one 3 in the factorization of $n$ so $n$ *cannot* be expressed as the sum of two squares because $3 \equiv 3 \pmod 4$.

■

(d) We need to show that if $n \equiv 18 \pmod{36}$ then we cannot necessarily write this as the sum of two squares.

By the definition of congruence we have

$$n = 36k + 18 = 9\left(4k + 2\right) = 3^2\left(4k + 2\right) = 2 \times 3^2 \times \left(2k + 1\right)$$

If $2k + 1 = 3m$ where $m$ is *not* a multiple of 3 then we cannot write

$$n = 2 \times 3^2 \times \left(2k + 1\right)$$

as the sum of two squares. *Why not?*

Because

$$n = 2 \times 3^2 \times \left(2k + 1\right) = 2 \times 3^2 \times 3m = 2 \times 3^3 \times m$$

So by Corollary (8.8):

> $n = p_1 \times p_2 \times \cdots \times p_r \times N^2$ *cannot* be expressed as sum of two squares $\Leftrightarrow$ it has *a* prime factor $p_j \equiv 3 \left(\text{mod } 4\right)$.

We conclude that $n$ *cannot* be expressed as the sum of two squares.

Note that if $2k + 1 \equiv 1 \left(\text{mod } 4\right)$ then we can write $n \equiv 18 \left(\text{mod } 36\right)$ as the sum of two squares.

The question says explain why we *cannot* say $n \equiv 18 \left(\text{mod } 36\right)$. From the above discussion we see that we can sometimes but we just cannot conclude this for every $n \equiv 18 \left(\text{mod } 36\right)$.

20. We need to prove that if $n = 2 \times p^e \times q^k$ where $p \equiv 3 \left(\text{mod } 4\right)$, $e$ is even, $q \equiv 1 \left(\text{mod } 4\right)$ and $k$ is any natural number then $n$ can be expressed as sum of two squares.

*Proof.*

We are given that $n = 2 \times p^e \times q^k$ where $e$ is an even integer. By Corollary (8.8):

> $n = p_1 \times p_2 \times \cdots \times p_r \times N^2$ *cannot* be expressed as sum of two squares $\Leftrightarrow$ it has *a* prime factor $p_j \equiv 3 \left(\text{mod } 4\right)$.

As we are given that $p \equiv 3 \left(\text{mod } 4\right)$ and is to an even power $p^e$ in

$$n = 2 \times p^e \times q^k$$

So, by this corollary we can say that $n$ can be written as the sum of two squares.

■

21. (a) We need to disprove the given statement which is:

If $m$ is the sum of two squares and $m \mid n$ then $n$ is also the sum of two squares.

Let $m = 5$ and $n = 15$ then $5 \mid 15$ but $15 = 3 \times 5$ *cannot* be written as the sum of two squares.

(b) We are asked to disprove;

If both $m$ and $n$ are sum of two squares then $m + n$ is also the sum of two squares.

Let $m = 5$ and $n = 2$ then both of these can be expressed as the sum of two squares; $5 = 2^2 + 1^2$ and $2 = 1^2 + 1^2$. However

$$m + n = 5 + 2 = 7 \equiv 3 \pmod 4$$

Since $7 \equiv 3 \pmod 4$ so it *cannot* be expressed as the sum of two squares.

(c) We are given that $n_1$, $n_2$ and $n_3$ cannot be expressed as the sum of two squares so by Corollary (8.8):

> $n = p_1 \times p_2 \times \cdots \times p_r \times N^2$ *cannot* be expressed as sum of two squares $\Leftrightarrow$ it has *a* prime factor $p_j \equiv 3 \pmod 4$.

Let $n_1 = 3$, $n_2 = 7$ and $n_3 = 15$ then

$$n_1 + n_2 + n_3 = 3 + 7 + 15 = 25 = 5^2 + 0^2$$

Hence $n_1 + n_2 + n_3$ can be written as the sum of two squares.

22. (i) We need to prove:

A prime $p$ which satisfies $p \equiv 1 \pmod 4$ can be written *uniquely* as the sum of two squares.

*Proof.*

Let $p \equiv 1 \pmod 4$ and suppose there are two ways of expressing this prime as sum of two squares

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

where $a \geq 1$, $b \geq 1$, $c \geq 1$ and $d \geq 1$. Required to prove

$$a = c,\ b = d \text{ or } a = d,\ b = c$$

By the Conversion Identity (8.1) we have

$$p^2 = \left(a^2 + b^2\right) \times \left(c^2 + d^2\right) \underbrace{=}_{\text{By (8.1)}} \left(ac - bd\right)^2 + \left(ad + bc\right)^2 \qquad (\dagger)$$

By using the other sum of squares identity given in question 12:

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

Re-arranging the equation in (*) we have

$$p - a^2 = b^2 \quad \text{and} \quad p - c^2 = d^2$$

Multiplying the first equation by $d^2$ and the second by $b^2$ gives

$$\left(p - a^2\right)d^2 = b^2d^2 \quad \text{and} \quad b^2\left(p - c^2\right) = b^2d^2$$

Equating these two yields (because both are equal to $b^2d^2$)

$$\begin{aligned} \left(p - a^2\right)d^2 &= b^2\left(p - c^2\right) \\ pd^2 - a^2d^2 &= b^2p - b^2c^2 \qquad \left[\text{Expanding}\right] \end{aligned}$$

Collecting like terms and factorizing

$$\begin{aligned} pd^2 - b^2p &= a^2d^2 - b^2c^2 \\ p\left(d^2 - b^2\right) &\underbrace{=}_{\substack{\text{By Difference} \\ \text{of two squares}}} \left(ad - bc\right) \times \left(ad + bc\right) \qquad (**) \end{aligned}$$

From this last line we have $p \mid \left(ad - bc\right) \times \left(ad + bc\right)$. By Proposition (2.2):

> If $p$ is prime and $p \mid \left(a \times b\right)$ then $p \mid a$ or $p \mid b$.

Applying this proposition to $p \mid \left(ad - bc\right) \times \left(ad + bc\right)$ gives

$$p \mid \left(ad - bc\right) \text{ or } p \mid \left(ad + bc\right)$$

Consider the first case $p \mid \left(ad - bc\right)$. From this

$$p \mid \left(ad - bc\right) \text{ implies } p^2 \mid \left(ad - bc\right)^2.$$

By (††) we must have $ad - bc = 0$. *Why?*

Because $p^2m = \left(ad - bc\right)^2$ and $\left(ac + bd\right)^2 \geq 1$ (we are given $a \geq 1,\ b \geq 1,\ c \geq 1$ and $d \geq 1$):

$$\begin{aligned} p^2 = \left(ac + bd\right)^2 + \left(ad - bc\right)^2 &= \left(ac + bd\right)^2 + p^2m \qquad \left[\text{By } (\dagger)\right] \\ p^2\left(1 - m\right) &\underbrace{=}_{\text{Rearranging}} \left(ac + bd\right)^2 \quad \Rightarrow \quad m = 0. \end{aligned}$$

Substituting $m = 0$ into $p^2m = \left(ad - bc\right)^2$ implies $ad - bc = 0$.

Substituting this $ad - bc = 0$ into (**) yields

$$p\left(d^2 - b^2\right) = 0 \ \Rightarrow\ d^2 - b^2 = 0 \ \Rightarrow\ d^2 = b^2 \ \Rightarrow\ d = b \quad \left[\text{Because } d \geq 1,\ b \geq 1\right]$$

Substituting this $d = b$ into (*) gives

$$p = a^2 + d^2 = c^2 + d^2 \ \Rightarrow\ a^2 = c^2 \ \Rightarrow\ a = c \quad \left[\text{Because } a \geq 1,\ c \geq 1\right]$$

Hence, we have $a = c,\ b = d$ so the representation is unique.

Consider the second case $p \mid \big(ad + bc\big)$. Similarly we have

$$p^2 \mid \big(ad + bc\big)^2$$

Using this $p^2 \mid \big(ad + bc\big)^2$ in (†) we have

$$ac - bd = 0 \qquad (\ddagger)$$

because

$$p^2 = \big(ac - bd\big)^2 + \big(ad + bc\big)^2$$

From (*) $p = a^2 + b^2 = c^2 + d^2$ we have

$$\underbrace{\big(p - a^2\big)}_{=b^2} c^2 = b^2 \underbrace{\big(p - d^2\big)}_{=c^2} \qquad \Big[\text{Because } b^2c^2 = b^2c^2\Big]$$

Again rearranging this by expansion and factorization gives

$$\begin{aligned} pc^2 - a^2c^2 &= pb^2 - b^2d^2 \\ p\big(c^2 - b^2\big) &= a^2c^2 - b^2d^2 \underbrace{=}_{\substack{\text{Difference of} \\ \text{two squares}}} \big(ac - bd\big)\big(ac + bd\big) \end{aligned}$$

From (‡) we have $ac - bd = 0$. Putting this into the above yields

$$p\big(c^2 - b^2\big) = 0 \ \Rightarrow\ c^2 = b^2 \ \Rightarrow\ c = b$$

Substituting $c = b$ into (*) gives

$$a^2 + c^2 = c^2 + d^2 \ \Rightarrow\ a^2 = d^2 \ \Rightarrow\ a = d$$

We have $a = d,\ b = c$.

Again the sum of squares representation is unique.

This completes our proof.

■

(ii) We need to prove that

An odd prime $p$ can be written as sum of two squares *uniquely* $\Leftrightarrow$

$p \equiv 1\big(\text{mod } 4\big)$.

*Proof.*

Uniqueness has been proved in part (i).

($\Leftarrow$). By Theorem (8.3):

> Every prime $p \equiv 1\big(\text{mod } 4\big)$ can be written as the sum of two squares.

We can write $p$ has sum of two squares.

($\Rightarrow$). Let the prime $p$ satisfy $p = a^2 + b^2$.

Then by question 2 of Exercises 1(b):

> The square of any integer is of the form $4m$ or $4m+1$.

Applying this we have

$$p = a^2 + b^2 \equiv 0, 1+0, 1 \equiv 0, 1, 2 \pmod 4$$

We are assuming $p$ is an odd prime so $p \not\equiv 0, 2 \pmod 4$. Hence $p \equiv 1 \pmod 4$.

This completes our proof.

■

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

By mathematical induction.

*Proof.*

If there is only one prime in $n$, say $n = p$ where $p \equiv 1 \pmod 4$ then by the result of the previous question, there is only one way to write $n$ as the sum of two squares. Hence $2^{1-1} = 2^0 = 1$. Our result holds for the base case.

Assume that the result is also true for $r = k$;

This means that if $n$ has $k$ distinct primes which satisfy $p \equiv 1 \pmod 4$ then there are $2^{k-1}$ different ways of expressing $n$ as the sum of two squares.

Required to prove that if $n$ has $k+1$ distinct primes which satisfy $p \equiv 1 \pmod 4$ then there are $2^k$ different ways of expressing $n$ as sum of two squares.

We have $n = \left(p_1 \times p_2 \times \cdots \times p_k\right) \times p_{k+1}$. We can write

$$p_1 \times p_2 \times \cdots \times p_k = a^2 + b^2 \quad \text{[As sum of two squares.]}$$

Also we can write $p_{k+1}$ as sum of two squares

$$p_{k+1} = c^2 + d^2$$

Therefore

$$\begin{aligned} n &= \left(p_1 \times p_2 \times \cdots \times p_k\right) \times p_{k+1} \\ &= \left(a^2 + b^2\right) \times \left(c^2 + d^2\right) \end{aligned}$$

Applying the Conversion Identity (8.1) and the identity given in question 12 to this $n = \left(a^2 + b^2\right) \times \left(c^2 + d^2\right)$ yields

$$\begin{aligned} n &= \left(a^2 + b^2\right) \times \left(c^2 + d^2\right) \\ &= \left(ac - bd\right)^2 + \left(ad + bc\right)^2 \qquad \left[\text{By (8.1)}\right] \\ &= \left(ac + bd\right)^2 + \left(ad - bc\right)^2 \qquad \left[\text{By result of question 12}\right] \end{aligned}$$

Now each of these squares integers are distinct. *Why?*

Suppose $ac-bd=ac+bd$ then we have $0=2bd$ which gives $b=0$ or $d=0$.

This is impossible as the given primes $p$'s are distinct and this would imply that

$$p_1\times p_2\times\cdots\times p_k=a^2 \text{ or } p_{k+1}=c^2.$$

Similarly if $ac-bd=ad-bc$ then

$$a\left(c-d\right)=b\left(d-c\right)=-b\left(c-d\right) \Rightarrow a=-b \quad \left[\text{Cancelling } \left(c-d\right)\right]$$

This $a=-b$ is impossible because we would have

$$p_1\times p_2\times\cdots\times p_k=a^2+b^2=2b^2.$$

Remember *all* the primes satisfy $p\equiv 1\left(\text{mod } 4\right)$ so are odd.

As all the primes in this decomposition are odd so

$$\left(ac-bd\right)^2\neq\left(ad+bc\right)^2$$
$$\left(ac+bd\right)^2\neq\left(ad-bc\right)^2$$

Hence we can express $n=\left(p_1\times p_2\times\cdots\times p_k\right)\times p_{k+1}$ as the sum of two different squares which are given above by:

$$\begin{aligned} n&=\left(ac-bd\right)^2+\left(ad+bc\right)^2\\ &=\left(ac+bd\right)^2+\left(ad-bc\right)^2\end{aligned}$$

By our above assumption of the mathematical induction step we know that

$p_1\times p_2\times\cdots\times p_k$ can be expressed as $2^{k-1}$ different sum of squares

Writing each sum of squares as

$$p_1\times p_2\times\cdots\times p_k=a_j^{\,2}+b_j^{\,2} \text{ for } j=1,\cdots,2^{k-1}.$$

We can express $n=\left(p_1\times p_2\times\cdots\times p_k\right)\times p_{k+1}$ in the following 2 sum of squares for each $j=1,\cdots,2^{k-1}$:

$$\begin{aligned} n&=\left(a_jc-b_jd\right)^2+\left(a_jd+b_jc\right)^2\\ &=\left(a_jc+b_jd\right)^2+\left(a_jd-b_jc\right)^2\end{aligned}$$

Hence there are $2^{k-1}\times 2=2^k$ different ways of expressing $n$ as the sum of two squares.

Therefore by mathematical induction we have our required result.

■

24. We are asked to prove:

Let $n = p_1 \times p_2 \times \cdots \times p_r \times N^2$ where $p$'s are distinct primes. If $n$ can be expressed as sum of two squares then *none* of these primes $p_j$ satisfies $p_j \equiv 3 \pmod 4$ for $j = 1, \cdots, r$.

*Proof.*

Assume that $n$ can be expressed as sum of two squares;

$$n = a^2 + b^2 = p_1 \times p_2 \times \cdots \times p_r \times N^2 \qquad (*)$$

If $n = N^2$ then we don't have any of these primes so the result holds.

Suppose $p$ is an odd prime amongst $p_1,\ p_2,\ \cdots,\ p_r$ such that

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

Let $g = \gcd(a,\ b)$ then there are integers $x$ and $y$ such that

$$gx = a \text{ and } gy = b.$$

Then from (*) we have

$$\begin{aligned} n &= a^2 + b^2 \\ &= g^2x^2 + g^2y^2 = g^2\left(x^2 + y^2\right) \ \Rightarrow\ g^2 \mid n \end{aligned}$$

Since $n = p_1 \times p_2 \times \cdots \times p_r \times N^2$ so $g^2 \mid N^2$ because the primes $p$ are distinct so

$$\gcd\left(p_1 \times p_2 \times \cdots \times p_r,\ g^2\right) = 1.$$

Therefore $x^2 + y^2$ must be a multiple of $p$. *Why?*

Because from above we have

$$\begin{aligned} g^2\left(x^2 + y^2\right) &= n = p_1 \times p_2 \times \cdots \times p_r \times N^2 \\ \Rightarrow\ x^2 + y^2 &= \frac{p_1 \times p_2 \times \cdots \times p_r \times N^2}{g^2} \text{ and } \frac{N^2}{g^2} = \text{integer} \\ \Rightarrow\ x^2 + y^2 &= p_1 \times p_2 \times \cdots \times p_r \times (\text{integer}) \text{ where } p \text{ is amongst the } p_j\text{'s} \end{aligned}$$

Therefore we have

$$x^2 + y^2 \equiv 0 \pmod p \qquad (*)$$

Since $\gcd(x,\ y) = 1$. *Why?*

Because by Proposition (1.5):

If $\gcd(a,\ b) = g$ then $\gcd\left(\frac{a}{g},\ \frac{b}{g}\right) = 1$.

From this $\gcd(x,\ y) = 1$ and $x^2 + y^2 \equiv 0 \pmod p$ either $\gcd(x,\ p) = 1$ or $\gcd(y,\ p) = 1$. *Why?*

Because otherwise $p$ would be a common factor of $x$ and $y$. This cannot be the case because $\gcd\left(x,\quad y\right)=1$.

Without loss of generality let $\gcd\left(x,\quad p\right)=1$. Therefore $x\left(\text{mod } p\right)$ has a multiplicative inverse $x'$ say:

$$x\times x'\equiv 1\left(\text{mod } p\right)$$

Multiplying the congruence in (*) by $\left(x'\right)^2$ gives

$$x^2\left(x'\right)^2+y^2\left(x'\right)^2\equiv\underbrace{\left(x\times x'\right)^2}_{\equiv 1\left(\text{mod } p\right)}+\left(y\times x'\right)^2$$

$$\equiv 1+\left(y\times x'\right)^2\equiv 0\left(\text{mod } p\right)$$

Re-arranging this we have

$$\left(y\times x'\right)^2\equiv -1\left(\text{mod } p\right)$$

Hence we have $-1$ is a quadratic residue of modulo $p$.

By the following result of quadratic residue from the last chapter, question 6 of Exercises 7(a):

$$-1 \text{ is a QR of } p \Leftrightarrow p\equiv 1\left(\text{mod } 4\right).$$

From this we have $p\equiv 1\left(\text{mod } 4\right)$ because $-1$ is a quadratic residue of modulo $p$. We have a contradiction to our supposition that $p\equiv 3\left(\text{mod } 4\right)$.

Hence *none* of the primes $p_j$ satisfies $p_j\equiv 3\left(\text{mod } 4\right)$ for $j=1,\cdots,r$.

This completes our proof.

■

25. We need to prove the following:

Let $n=p_1\times p_2\times\cdots\times p_r\times N^2$ where $p$'s are distinct primes. Then $n$ *cannot* be expressed as sum of two squares $\Leftrightarrow$ it has a prime factor $p_j\equiv 3\left(\text{mod } 4\right)$.

*Proof.*

By combining Theorems (8.5) and (8.7) we have

Let $n$ be a positive integer given by $n=p_1\times p_2\times\cdots\times p_r\times N^2$ where the $p$'s are distinct primes. Then $n$ can be expressed as sum of two squares $\Leftrightarrow$ every prime $p_j$ satisfies $p_j=2$ or $p_j\equiv 1\left(\text{mod } 4\right)$ for $j=1,\cdots,r$.

If for some $j$ in $j = 1, \cdots, r$ there is a prime $p_j \equiv 3 \left(\text{mod } 4\right)$ then by the contrapositive of these theorems we have our result.

This completes our proof.

■