Complete Solutions to Exercises 3.5

1. We use the difference of two squares identity on each of the given integers:

$$a^2 - b^2 = \big(a - b\big)\big(a + b\big)$$

(a) We are given the integer 299. We need to find the ceiling function of the square root of 299:

$$\left\lceil \sqrt{299} \right\rceil = 18\,.$$

We have $18^2 - 299 = 25 = 5^2$. Re-arranging this gives us 299 as the difference of two squares:

$$299 = 18^2 - 5^2 = \big(18 - 5\big)\big(18 + 5\big) = 13 \times 23\,.$$

(b) This time we need to factorize 851. Finding the ceiling function of the square root of 851 gives $\left\lceil \sqrt{851} \right\rceil = 30$. Finding the difference between 30 squared and 851 yields

$$30^2 - 851 = 49 = 7^2$$

Hence we have $30^2 - 7^2 = 851$, so using the difference of two squares we have

$$851 = 30^2 - 7^2 = \big(30 - 7\big)\big(30 + 7\big) = 23 \times 37$$

(c) We are asked to factorize 10403. Taking the ceiling of the square root of 10403:

$$\left\lceil \sqrt{10403} \right\rceil = 102$$

Evaluating $102^2 - 10403 = 1 = 1^2$. Rewriting this we have:

$$\begin{aligned} 10403 &= 102^2 - 1^2 \\ &= \big(102 - 1\big)\big(102 + 1\big) \qquad \Big[\text{Using } \; a^2 - b^2 = \big(a - b\big)\big(a + b\big)\Big] \\ &= 101 \times 103 \end{aligned}$$

Therefore 10403 factorizes into 101×103. Note that both 101 and 103 are prime.

(d) We need to factorize 2479. Proceeding in the same manner as above:

$$\left\lceil \sqrt{2479} \right\rceil = 50$$

Finding the difference between 50 squared and 2479:

$$50^2 - 2479 = 21$$

Clearly 21 is *not* a perfect square. We trial the next integer after 50:

$$51^2 - 2479 = 122$$

Again 122 is *not* a perfect square so we increment by another integer:

$$52^2 - 2479 = 225 = 15^2$$

Re-arranging this we have $2479 = 52^2 - 15^2$. Using the difference of two squares identity:

$$\begin{aligned} 2479 = 52^2 - 15^2 &= \left(52 - 15\right)\left(52 + 15\right) \\ &= 37 \times 67 \end{aligned}$$

37 and 67 are *both* prime. Hence $2479 = 37 \times 67$.

2. (a) We are asked to factorize 9271. Let

$$a_1 = \left\lfloor \sqrt{9271} \right\rfloor = 97$$

Evaluating $a_1^{\,2} - 9271$ gives

$$a_1^{\,2} - 9271 = 97^2 - 9271 = 138$$

138 is *not* a perfect square. We trial the next a_2 which is the next integer after 97; $a_2 = 98$:

$$a_2^{\,2} - 9271 = 98^2 - 9271 = 333$$

Since $\sqrt{333} = 18.25\ \left(2\text{ dp}\right)$ so 333 is not a perfect square. We trial the next integer $a_3 = 99$:

$$a_3^{\,2} - 9271 = 99^2 - 9271 = 530$$

Again 530 is not a perfect square because $\sqrt{530} = 23.02\ \left(2\text{ dp}\right)$. We trial the next integer after 99 which is 100:

$$a_4^{\,2} - 9271 = 100^2 - 9271 = 729 \qquad (*)$$

As $\sqrt{729} = 27$. We can now stop because 729 is a perfect square. Rearranging (*) gives

$$100^2 - 729 = 100^2 - 27^2 = 9271$$

Using the difference of two squares to write out the factors of 9271:

$$\begin{aligned} 9271 = 100^2 - 27^2 &= \left(100 - 27\right)\left(100 + 27\right) \\ &= 73 \times 127 \end{aligned}$$

Since the question asks for the prime factors so we need to check that 73 and 127 are prime. *How?*

We use Corollary (2.10) of Chapter 2:

If $n > 1$ is composite then it has a prime divisor p such that $p \le \left\lfloor \sqrt{n} \right\rfloor$.

As 127 is larger of the two integers so we only need to examine the prime factors p such that $p \le \left\lfloor \sqrt{127} \right\rfloor = 11$. We need to test the primes below 11 and 11 itself.

Checking to see if each of the primes 2, 3, 5, 7 and 11 are proper divisors of 73 and 127, we find that they are not. Actually we *don't need* to check that 11 goes into 73 because the primes $\leq \left\lfloor \sqrt{73} \right\rfloor = 8$.

Therefore by the above corollary both 73 and 127 are prime. The prime factors of 9271 are 73 and 127 because $9271 = 73 \times 127$.

(b) We need to factorize 2146. This is an even number so 2 is clearly a factor of 2146. Dividing 2146 by 2 gives $\frac{2146}{2} = 1073$ so $2146 = 2 \times 1073$.

We try to write 1073 as difference of two squares. First we evaluate $\left\lfloor \sqrt{1073} \right\rfloor = 33$:

$$33^2 - 1073 = 16 = 4^2$$

Re-arranging this gives $1073 = 33^2 - 4^2$. Using the algebraic identity we have

$$1073 = 33^2 - 4^2 = \left(33 - 4\right)\left(33 + 4\right) = 29 \times 37$$

Putting all this together gives $2146 = 2 \times 1073 = 2 \times 29 \times 37$.

(c) We need to factorize 2 974 791. First note that if we add the digits of

$$2\ 974\ 791 \text{ we get } 2 + 9 + 7 + 4 + 7 + 9 + 1 = 39.$$

Clearly 3 divides into 39 so 3 is a factor of 2 974 791. We have

$$2\ 974\ 791 = 3 \times 991\ 597 \qquad (*)$$

We factorize 991 597 by using the fundamental algebraic identity – difference of two squares. First we evaluate $\left\lfloor \sqrt{991\ 597} \right\rfloor = 996$. Creating a table of values by starting the trial integers $a_1 = 996$:

a_k	$a_k^{\,2} - 991597$	$\sqrt{a_k^{\,2} - 99157}$
996	$996^2 - 991597 = 419$	20.47
997	$997^2 - 991597 = 2412$	49.11
998	$998^2 - 991597 = 4407$	66.39
999	$999^2 - 991597 = 6404$	80.02
1000	$1000^2 - 991597 = 8403$	73.51
1001	$1001^2 - 991597 = 10404$	102

From the last row we have

$$1001^2 - 991597 = 10404 = 102^2$$

Rearranging this we have

$$1001^2 - 102^2 = 991597$$

Expressing this as the difference of two squares yields

$$\begin{aligned} 991597 = 1001^2 - 102^2 &= \big(1001 - 102\big) \times \big(1001 + 102\big) \\ &= 899 \times 1103 \qquad (**) \end{aligned}$$

To find the factors of 899 and 1103 we have to use Corollary (2.10):

> If $n > 1$ is composite then it has a prime divisor p such that $p \le \left\lfloor \sqrt{n} \right\rfloor$.

Because 899 is one away from $30^2 = 900$ we can try to write 899 as a difference of two squares:

$$899 = 900 - 1 = 30^2 - 1^2$$

Applying difference of two squares gives

$$899 = 30^2 - 1^2 = \big(30 - 1\big) \times \big(30 + 1\big) = 29 \times 31$$

Now checking the other factor in (**), 1103. Let p be a prime divisor of 1103, then

$$p \le \left\lfloor \sqrt{1103} \right\rfloor = 33$$

The primes upto 33 are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29 and 31.

Clearly 2, 3 and 5 do not go into 1103. By using division you can check that the other primes up to 31 do not go into 1103. So 1103 is prime.

Therefore by (**)

$$991597 = 899 \times 1103 = 29 \times 31 \times 1103$$

By (*) we have

$$2974791 = 3 \times 991597 = 3 \times 29 \times 31 \times 1103$$

3. We are asked to show $\left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2 = n$.

Proof.

Using difference of two squares with $a = \frac{n+1}{2}$ and $b = \frac{n-1}{2}$ gives

$$\begin{aligned} a^2 - b^2 &= \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2 \\ &= \left[\frac{n+1}{2} + \frac{n-1}{2}\right] \times \left[\frac{n+1}{2} - \frac{n-1}{2}\right] = n \times \frac{\cancel{2}}{\cancel{2}} = n \end{aligned}$$

We have our required result.

■

4. Let $n = 1\,236\,519$ then we could try to use the fundamental identity of algebra - difference of two squares:

$$n = a^2 - b^2 = \big(a - b\big)\big(a + b\big)$$

If we can express $n = 1\,236\,519$ as $a^2 - b^2$ then we can use this fundamental identity. In order to use this we need to find the square root of $n = 1\,236\,519$ and then take the ceiling function of this number because we want to subtract. Let

$$a = \left\lceil \sqrt{1\,236\,519} \right\rceil = 1112$$

Since we are using the ceiling function so $a^2 = 1112^2 = 1\,236\,544$ is greater than $n = 1\,236\,519$. The difference is given by

$$a^2 - n = 1112^2 - 1\,236\,519 = 1\,236\,544 - 1236\,519 = 25 = 5^2$$

Rearranging this we have $\underbrace{1\,236\,544}_{1112^2} - \underbrace{25}_{5^2} = 1\,236\,519 = n$. Hence we have

$$\begin{aligned} n = 1236519 &= 1112^2 - 5^2 \\ &= \big(1112 - 5\big)\big(1112 + 5\big) \qquad \Big[\text{Using } n = a^2 - b^2 = \big(a - b\big)\big(a + b\big)\Big] \\ &= 1107 \times 1117 \qquad\qquad\qquad\qquad (*) \end{aligned}$$

Adding the digits of the first number $1 + 1 + 0 + 7 = 9$ and $9 \,\big|\, 9$ so 9 is factor of 1107:

$$\frac{1107}{9} = 123 \text{ or } 1107 = 9 \times 123 \qquad\qquad (\dagger)$$

Also 3 is factor of 123 because $1 + 2 + 3 = 6$ and $3 \,\big|\, 6$. We have $\dfrac{123}{3} = 41$:

$$123 = 3 \times 41$$

Putting this into (†) gives

$$1107 = 9 \times 123 = 9 \times 3 \times 41 = 3^3 \times 41$$

Need to find the factors of the other number in (*) which is 1117. Let p be a prime divisor of 1117. Then by Corollary (2.10):

If $n > 1$ is composite then it has a prime divisor p such that $p \le \left\lfloor \sqrt{n} \right\rfloor$.

We have $p \le \left\lfloor \sqrt{1117} \right\rfloor = 33$.

We need to test whether all the primes up to 33 which are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, and 31 go into 1117. You can check that none of these go exactly into 1117 so by the corollary we have 1117 is prime.

Putting all these results into (*) yields

$$1\,236\,519 = 1107 \times 1117 = 3^3 \times 41 \times 1117$$

5. (i) (a) We are asked to factorize 713. Finding the ceiling function of $\sqrt{713}$ gives

$$\left\lceil \sqrt{713} \right\rceil = 27$$

Evaluating $27^2 - 713 = 16 = 4^2$. Therefore $713 = 27^2 - 4^2$. Writing this as a difference of two squares:

$$\begin{aligned} 713 = 27^2 - 4^2 &= \big(27 - 4\big)\big(27 + 4\big) \\ &= 23 \times 31 \end{aligned}$$

(b) Similarly we factorize 1271. We have

$$\left\lceil \sqrt{1271} \right\rceil = 36$$

Therefore $36^2 - 1271 = 25 = 5^2$. Rewriting this we have

$$1271 = 36^2 - 5^2 = \big(36 - 5\big)\big(36 + 5\big) = 31 \times 41$$

(c) We need to factorize 403. We have

$$\left\lceil \sqrt{403} \right\rceil = 21$$

Evaluating $21^2 - 403 = 38$ and 38 is not a perfect square. Incrementing the integer

$$22^2 - 403 = 81 = 9^2$$

Rearranging this and factorizing gives

$$403 = 22^2 - 9^2 = \big(22 - 9\big)\big(22 + 9\big) = 13 \times 31$$

(ii) We need to solve the quadratic $403x^2 + 1271x + 713 = 0$. Replacing each of the coefficients with the factors evaluated in parts (a), (b) and (c) we have

$$403x^2 + 1271x + 713 = \big(13 \times 31\big)x^2 + \big(31 \times 41\big)x + \big(23 \times 31\big) = 0$$

What do you notice about the quadratic on the right-hand-side?

It has a common factor of 31. Taking this out yields the simpler quadratic:

$$13x^2 + 41x + 23 = 0$$

Using the formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

With $a = 13$, $b = 41$ and $c = 23$:

$$x = \frac{-41 \pm \sqrt{41^2 - \big(4 \times 13 \times 23\big)}}{2 \times 13}$$
$$= \frac{-41 \pm \sqrt{41^2 - 1196}}{26} = \frac{-41 \pm \sqrt{485}}{26} = \frac{-41 + \sqrt{485}}{26},\ \frac{-41 - \sqrt{485}}{26}$$

(iii) Using the factors found in part (i) we have the following simplification:

$$\frac{713}{1271} = \frac{23 \times \cancel{31}}{\cancel{31} \times 41} = \frac{23}{41},\quad \frac{403}{1271} = \frac{13 \times \cancel{31}}{\cancel{31} \times 41} = \frac{13}{41} \text{ and } \frac{403}{713} = \frac{13 \times \cancel{31}}{23 \times \cancel{31}} = \frac{13}{23} \qquad \left[\begin{array}{l}\text{Cancelling the}\\ \text{common factor 31}\end{array}\right]$$

6. We need to factorize $18\,861649$. First we find

$$\left\lceil \sqrt{18\ 861\ 649} \right\rceil = 4343$$

Resolving this into difference of two squares:

$$18\ 861\ 649 - 4343^2 = 0$$

Clearly a factor of 4343 is 43 and 43 is prime. So we have

$$\frac{4343}{43} = 101 \text{ which implies } 4343 = 43 \times 101.$$

Hence $18\ 861\ 649 = 4343^2 = \big(43 \times 101\big)^2 = 43^2 \times 101^2$. [Both 43 and 101 are prime.]

The solution of $x^2 - 18\ 861\ 649 = 0$ is $x = \sqrt{18861649} = \sqrt{4343^2} = \pm 4343$.

7. We need to factorize 3 397 301. Determining the ceiling function of the square root of 3 397 301 gives

$$\left\lceil \sqrt{3\ 397\ 301} \right\rceil = 1844$$

We have $1844^2 - 3\ 397\ 301 = 3035$ and 3035 is *not* a perfect square because $\sqrt{3035} = 55.09\ \big(2 \text{ dp}\big)$. We trial the next integer after 1844 which is 1845:

$$1845^2 - 3\ 397\ 301 = 6724 = 82^2$$

Rearranging this last evaluation into difference of two squares yields

$$\begin{aligned} 3\ 397\ 301 &= 1845^2 - 82^2 \\ &= \big(1845 - 82\big)\big(1845 + 82\big) \\ &= 1763 \times 1927 \qquad (\dagger) \end{aligned}$$

We are not asked to factorize them into prime factors so we can leave this factorization as $3\ 397\ 301 = 1763 \times 1927$.

Now we need to solve the given quadratic equation $x^2 + 164x - 3\ 397\ 301 = 0$.

Using the above factorization $3\ 397\ 301 = 1763 \times 1927$ we have

$$x^2 + 164x - 3\ 397\ 301 = x^2 + 164x - \left(1763 \times 1927\right)$$

Is there a combination of 1763 and 1927 which gives 164?

Yes if we subtract $1927 - 1763 = 164$. Hence we have

$$\begin{aligned} x^2 + 164x - 3397301 &= x^2 + 164x - \left(1763 \times 1927\right) \\ &= \left(x - 1763\right)\left(x + 1927\right) = 0 \quad \text{gives} \quad x = 1763, \quad x = -1927 \end{aligned}$$

Our two roots are $x = 1763, \ -1927$.

8. We are asked to factorize 53. Finding the ceiling function of $\sqrt{53}$ gives

$$\left\lceil \sqrt{53} \right\rceil = 8$$

Therefore $8^2 - 53 = 11$ and 11 is *not* a perfect square. Creating a table of values using this method yields

a_k	$a_k^{\,2} - 53$	Is $a_k^{\,2} - 53$ a perfect square?
8	$8^2 - 53 = 11$	No
9	$9^2 - 53 = 28$	No
10	$10^2 - 53 = 47$	No
11	$11^2 - 53 = 68$	No
12	$12^2 - 53 = 91$	No
13	$13^2 - 53 = 116$	No
⋮	⋮	⋮

You might have noticed that 53 is a prime number and so cannot be expressed as the difference of two squares.

In the next question we prove the only prime that can be written as the sum of two squares is 3.

9. We are asked to prove that the only prime of the form $n^2 - 1$ is 3.

Proof.

Since we can factorize $n^2 - 1$ as:

$$n^2-1=\big(n-1\big)\big(n+1\big)$$

The only condition where this $n^2-1=\big(n-1\big)\big(n+1\big)$ can be prime is when $n-1=1$. *Why?*

Because if $n-1\geq 2$ then $n^2-1=\big(n-1\big)\big(n+1\big)$ will be a composite number.

Therefore the only prime is $n-1=1$ which implies that $n=2$ and so

$$n^2-1=2^2-1=3$$

Hence 3 is the only prime of the form n^2-1.

■

10. (i) We need to show that 3^n-1 is *composite* for $n>1$.

Proof.

Writing the given expression 3^n-1 by using the hint

$$a^n-b^n=\big(a-b\big)\Big(a^{n-1}+a^{n-2}b+a^{n-3}b^2+\cdots+ab^{n-2}+b^{n-1}\Big)$$

With $a=3,\ b=1$

$$\begin{aligned}3^n-1&=\big(3-1\big)\big(3^{n-1}+3^{n-2}+\cdots+1\big)\\&=2\big(3^{n-1}+3^{n-2}+\cdots+1\big)\qquad\big[\text{even number}\big]\end{aligned}$$

Hence 3^n-1 has a factor of 2 for $n>1$ so it is a composite integer.

■

(ii) We are asked to prove x^n-1 is composite for both $x\geq 3$ and $n>1$.

Proof.

As part (i) replacing 3 with x. The factorization gives

$$x^n-1=\big(x-1\big)\big(x^{n-1}+x^{n-2}+\cdots+1\big)$$

Since $x\geq 3$ so $x-1\geq 2$ which means an integer ≥ 2 is a factor of x^n-1. Hence x^n-1 is a composite integer.

■

11. (a) Clearly 3 is a factor of 411 because $4+1+1=6$ and $3\,\big|\,6$. We have

$$\frac{411}{3}=137$$

We need to check whether 137 is prime or not. *How?*

Use Corollary (2.10):

> If $n>1$ is composite then it has a prime divisor p such that $p\leq\big\lfloor\sqrt{n}\big\rfloor$.

Let p be a prime divisor of 137 then by this corollary we have

$$p \le \left\lfloor \sqrt{137} \right\rfloor = 11 .$$

We need to see if any of the primes up to 11 go into 137. Clearly 2, 3 and 5 are not factors of 137. Also $\frac{137}{7} = 19.57 \ \left(2\text{dp}\right)$ and $\frac{137}{11} = 12.45 \left(2\text{dp}\right)$.

Since none of these primes go into 137 so 137 is prime. Hence $411 = 3 \times 137$.

(b) We are given the integer 2419. Taking the ceiling of $\sqrt{2419}$ gives

$$\left\lceil \sqrt{2419} \right\rceil = 50 .$$

Evaluating $50^2 - 2419 = 81 = 9^2$. Rearranging this we have

$$2419 = 50^2 - 9^2 = \left(50 - 9\right)\left(50 + 9\right) = 41 \times 59 .$$

Both 41 and 59 are prime so $2419 = 41 \times 59$.

(c) We need to factorize 17 947 into two primes. We have

$$\left\lceil \sqrt{17\ 947} \right\rceil = 134$$

Subtracting 17 947 from 134^2 gives $134^2 - 17947 = 9 = 3^2$. Rearranging this

$$\begin{aligned} 17947 = 134^2 - 3^2 &= \left(134 - 3\right) \times \left(134 + 3\right) \\ &= 131 \times 137 \end{aligned}$$

We need to check if both these numbers 131 and 137 are prime. By part (a) we know that 137 is prime. So we only need to test 131:

Again using the above corollary:

$$p \le \left\lfloor \sqrt{131} \right\rfloor = 11 \ \text{ where } p \text{ is a prime factor of 131.}$$

None of the primes 2, 3, 5, 7 and 11 go into 131 exactly so 131 is prime. Hence

$$17\ 947 = 131 \times 137$$

12. (a) We need to factorize 2201. The perfect square just larger than 2201 is

$$\left\lceil \sqrt{2201} \right\rceil = 47$$

Determining $a_k^{\,2} - 2201$:

a_k	$a_k^{\,2} - 2201$	Factors of $a_k^{\,2} - 2201$
47	$47^2 - 2201 = 8$	2^3
48	$48^2 - 2201 = 103$	103
49	$49^2 - 2201 = 200$	$2^3 \times 5^2$
50	$50^2 - 2201 = 299$	13×23
51	$51^2 - 2201 = 400$	20^2

From the last row we have

$$51^2 - 2201 = 20^2 \quad \Rightarrow \quad 51^2 - 20^2 = 2201$$

Therefore we have

$$\begin{aligned} 2201 &= 51^2 - 20^2 \\ &= \left(51-20\right)\times\left(51+20\right) = 31\times 71 \end{aligned}$$

Both 31 and 71 are prime so $2201 = 31\times 71$.

(b) We need to factorize 2189. The perfect square just larger than 2189 is

$$\left\lceil \sqrt{2189} \right\rceil = 47\,.$$

Determining $a_k^{\,2} - 2189$:

a_k	$a_k^{\,2} - 2189$	Factors of $a_k^{\,2} - 2189$
47	$47^2 - 2189 = 20$	$2^2\times 5$
48	$48^2 - 2189 = 115$	5×23
49	$49^2 - 2189 = 212$	$2^2\times 53$
50	$50^2 - 2189 = 311$	311
51	$51^2 - 2189 = 412$	$2^2\times 103$
52	$52^2 - 2189 = 515$	5×103

Writing each of the highlighted middle columns in modulo 2189 gives

$$47^2 \equiv 20 \equiv 2^2\times 5 \left(\text{mod } 2189\right)$$

$$51^2 \equiv 412 \equiv 2^2\times 103 \left(\text{mod } 2189\right)$$

$$52^2 \equiv 515 \equiv 5\times 103 \left(\text{mod } 2189\right)$$

Multiplying these gives

$$47^2\times 51^2\times 52^2 \equiv \left(2^2\times 5\right)\times\left(2^2\times 103\right)\times\left(5\times 103\right)$$

$$\left(47\times 51\times 52\right)^2 \equiv \left(2^2\times 5\times 103\right)^2 \left(\text{mod } 2189\right)$$

We use Theorem (3.26):

> $a^2 \equiv b^2 \left(\text{mod } n\right)$ and $a \not\equiv \pm b \left(\text{mod } n\right)$ then $\gcd\left(a-b,\ \ n\right)$ is a *non-trivial* factor of n.

So we need to check $a = 47\times 51\times 52 = 124644,\ \ b = 2^2\times 5\times 103 = 2060$ such that $a \not\equiv \pm b \left(\text{mod } 2189\right)$:

$$a = 124\,644 \equiv 2060 \left(\text{mod } 2189\right)$$

$$b \equiv 2060 \left(\text{mod } 2189\right)$$

Since $a \equiv b \equiv 2060 \left(\text{mod } 2189\right)$ we cannot use the above theorem (3.26).

We don't know how long this will take to find squares.

Now we could try subtracting the first perfect square from a multiple of 2189. Let us subtract various perfect squares from multiples of 2189:

$b_k = \left\lceil \sqrt{2189 \times k} \right\rceil$	$b_k^{\,2} - \left(2189 \times k\right)$	Factors of $b_k^{\,2} - \left(2189 \times k\right)$
$b_2 = \left\lceil \sqrt{2189 \times 2} \right\rceil = 67$	$67^2 - \left(2189 \times 2\right) = 111$	3×37
$b_3 = \left\lceil \sqrt{2189 \times 3} \right\rceil = 82$	$82^2 - \left(2189 \times 3\right) = 157$	157
$b_4 = \left\lceil \sqrt{2189 \times 4} \right\rceil = 94$	$94^2 - \left(2189 \times 4\right) = 80$	$2^4 \times 5$
$b_5 = \left\lceil \sqrt{2189 \times 5} \right\rceil = 105$	$105^2 - \left(2189 \times 5\right) = 80$	$2^4 \times 5$

We consider the first entry of the first table and penultimate entry of the bottom table:

$$47^2 - 2189 = 2^2 \times 5$$
$$94^2 - \left(2189 \times 4\right) = 2^4 \times 5$$

Writing both these results in terms of congruences:

$$47^2 \equiv 2^2 \times 5 \left(\text{mod } 2189\right)$$
$$94^2 \equiv 2^4 \times 5 \left(\text{mod } 2189\right)$$

Multiplying these results gives

$$47^2 \times 94^2 \equiv 2^2 \times 5 \times 2^4 \times 5$$
$$\equiv 2^6 \times 5^2$$
$$\left[47 \times 94\right]^2 \equiv \left[2^3 \times 5\right]^2 \left(\text{mod } 2189\right)$$

We use Theorem (3.26):

> $a^2 \equiv b^2 \left(\text{mod } n\right)$ and $a \not\equiv \pm b \left(\text{mod } n\right)$ then $\gcd\left(a - b, \quad n\right)$ is a *non-trivial* factor of n.

We have $a^2 \equiv b^2 \left(\text{mod } n\right)$ with $a = 47 \times 94,\ b = 2^3 \times 5 = 40$ and $n = 2189$ but we also need to check that $a \not\equiv \pm b \left(\text{mod } 2189\right)$:

$$a = 47 \times 94 \equiv 40 \equiv b \left(\text{mod } 2189\right)$$

Since $a \equiv b \left(\text{mod } 2189\right)$ we *cannot* use Theorem (3.26). We need to look for integers a and b such that $a^2 \equiv b^2 \left(\text{mod } 2189\right)$ and $a \not\equiv \pm b \left(\text{mod } 2189\right)$.

Notice that the last entry of the bottom table gives the same factors:

$$105^2 - \left(2189 \times 5\right) = 2^4 \times 5 \quad \text{implies} \quad 105^2 \equiv 2^4 \times 5 \left(\text{mod } \ 2189\right).$$

This time we can check whether we have $a \not\equiv \pm b \pmod{2189}$ with $a = 47 \times 105, b = 40$:

$$a = 47 \times 105 \equiv 557 \not\equiv \pm 40 \equiv b \pmod{2189}$$

Now we can use Theorem (3.26) because $a \not\equiv \pm b \pmod{2189}$. We have to find

$$\gcd(a - b, \quad n) = \gcd((47 \times 105) - 40, \quad 2189) = \gcd(4895, \quad 2189)$$

We apply the Euclidean algorithm to find this gcd:

$$\begin{aligned} 4895 &= (2 \times 2189) + 517 \\ 2189 &= (4 \times 517) + 121 \\ 517 &= (4 \times 121) + 33 \\ 121 &= (3 \times 33) + 22 \\ 33 &= (1 \times 22) + \boxed{11} \end{aligned}$$

Hence $\gcd(4895, \quad 2189) = 11$ so 11 is a factor of 2189. If we had been more observant we would have noticed that 11 is a factor of 2189 by using the test for divisibility by 11 which is given in question 33 of Exercises 3.1.

We have $\dfrac{2189}{11} = 199$. We need to find the factors of 199. Let p be a prime factor of 199, then by Corollary (2.10):

> If $n > 1$ is composite then it has a prime divisor p such that $p \le \lfloor \sqrt{n} \rfloor$.

We have $p \le \lfloor \sqrt{199} \rfloor = 15$. We need to test the primes below 15 which are 2, 3, 5, 7, 11 and 13. Clearly 2, 3 and 5 are not factors of 199. We only need to test 7, 11 and 13:

$$\frac{199}{7} = 28.43\,, \quad \frac{199}{11} = 18.09 \quad \text{and} \quad \frac{199}{13} = 15.31\,(2\text{dp})$$

By above corollary, we have 199 is a prime. Therefore the factors of 2189 are

$$2189 = 11 \times 199$$

(c) We are asked to factorize 9211. The perfect square just larger than this number is $\lceil \sqrt{9211} \rceil = 96$.

Evaluating $a_k^{\,2} - 9211$:

a_k	$a_k^{\,2} - 9211$	Factors of $a_k^{\,2} - 9211$
96	$96^2 - 9211 = 5$	5
97	$97^2 - 9211 = 198$	$2 \times 3^2 \times 11$
98	$98^2 - 9211 = 393$	3×131

99	$99^2 - 9211 = 590$	$2\times5\times59$
100	$100^2 - 9211 = 789$	3×263
101	$101^2 - 9211 = 990$	$2\times3^2\times5\times11$

Writing the shaded rows in modular arithmetic:

$$96^2 \equiv 5 \pmod{9211}$$

$$97^2 \equiv 2\times3^2\times11 \pmod{9211}$$

$$101^2 \equiv 2\times3^2\times5\times11 \pmod{9211}$$

Finding the product of these gives

$$\begin{aligned} 96^2\times97^2\times101^2 &\equiv 5\times\left(2\times3^2\times11\right)\times\left(2\times3^2\times5\times11\right) \\ &\equiv 2^2\times3^2\times3^2\times5^2\times11^2 \end{aligned}$$

$$\left[96\times97\times101\right]^2 \equiv \left[2\times3^2\times5\times11\right]^2 \pmod{9211}$$

Hence we have $\left[96\times97\times101\right]^2 \equiv \left[2\times3^2\times5\times11\right]^2 \pmod{9211}$. We need to check the conditions of Theorem (3.26):

> $a^2 \equiv b^2 \pmod{n}$ and $a \not\equiv \pm b \pmod{n}$ then $\gcd(a-b,\ n)$ is a factor of n.

We have $a^2 \equiv b^2 \pmod{n}$ with $a = 96\times97\times101,\ b = 2\times3^2\times5\times11$ and $n = 9211$ but we also need to check that $a \not\equiv \pm b \pmod{9211}$:

$$a = 96\times97\times101 \equiv 990 \pmod{9211}$$

$$b = 2\times3^2\times5\times11 \equiv 990 \pmod{9211}$$

We have $a \equiv b \pmod{9211}$ so we *cannot* use the above theorem.

Now we could try subtracting the first number from a *multiple* of 9211. Let us find $\left\lfloor\sqrt{2\times9211}\right\rfloor = 136$. Evaluating

$$136^2 - (2\times9211) = 74 = 2\times37\,.$$

We don't have a 37 as one of the factors in the above table.

We trial the next multiple of 9211:

$$\left\lfloor\sqrt{3\times9211}\right\rfloor = 167$$

We have $167^2 - (3\times9211) = 256 = 2^8 = \left(2^4\right)^2 = 16^2$. This is a useful result because we have a square number. Writing this $167^2 - (3\times9211) = 16^2$ in modular arithmetic:

$$167^2 \equiv 16^2 \pmod{9211}$$

We have $a^2 \equiv b^2 \pmod{n}$ with $a = 167,\ b = 16$ and $n = 9211$ but we also need to check that $a \not\equiv \pm b \pmod{9211}$:

$$a = 167 \equiv 167 \not\equiv \pm 16 \pmod{9211}$$

Using Theorem (3.26) we need to find

$$\gcd(a-b,\quad n) = \gcd(167-16,\quad 9211) = \gcd(151,\quad 9211)$$

First we could try to see if 151 goes into 9211:

$$\frac{9211}{151} = 61$$

Hence $\gcd(151,\quad 9211) = 151$ and from above we have

$$9211 = 61 \times 151\,.$$

13. We are asked to find the type of integer n which satisfies:

$$a^2 \equiv b^2 \pmod{n} \quad \Rightarrow \quad a \equiv \pm b \pmod{n}$$

This is true when n is a prime because by Proposition (3.14) (b):

$$a^2 \equiv b^2 \pmod{p} \text{ where } p \text{ is prime then } a \equiv \pm b \pmod{p}.$$

If n is composite, say $n = 15$, then the following is *false*:

$$1^2 \equiv 4^2 \pmod{15} \ \Rightarrow\ 1 \equiv \pm 4 \pmod{15}$$

14. (a) By using the hint we can write 9 999 as $10^4 - 1$ because $10^4 - 1 = 9999$.
Using difference of two squares gives

$$\begin{aligned} 9999 = 10^4 - 1 = \left(10^2\right)^2 - 1^2 &= \left(10^2 - 1\right)\left(10^2 + 1\right) \\ &= 99 \times 101 = 9 \times 11 \times 101 \end{aligned}$$

Hence $9999 = 9 \times 11 \times 101$.

(b) Similarly for 999 999 we have

$$\begin{aligned} 999999 = 10^6 - 1 = \left(10^3\right)^2 - 1^2 &= \left(10^3 - 1\right)\left(10^3 + 1\right) \\ &= 999 \times 1001 = 9 \times 111 \times 1001 \end{aligned}$$

Since $1+1+1=3$ and $3 \mid 3$ so 3 is a factor of 111:

$$\frac{111}{3} = 37 \quad \text{implies} \quad 111 = 3 \times 37$$

Clearly 11 is a factor of 1001 because $1 - 0 + 0 - 1 = 0$ and $11 \mid 0$. We have

$$1001 = 7 \times 11 \times 13$$

Therefore

$$\begin{aligned} 999999 &= 9\times 111\times 1001 \\ &= 3^2\times\left(3\times 37\right)\times\left(7\times 11\times 13\right) = 3^3\times 7\times 11\times 13\times 37 \end{aligned}$$

(c) (i) We need to factorize $R_4 = 1\,111$. We can rewrite this as

$$R_4 = 1\,111 = \frac{10^4-1}{9} = \frac{9999}{9} \qquad (*)$$

Now substituting the result of part (i), $9999 = 9\times 11\times 101$, into this (*) gives

$$R_4 = 1\,111 = \frac{9999}{9} = \frac{\cancel{9}\times 11\times 101}{\cancel{9}} = 11\times 101$$

Hence $R_4 = 11\times 101$.

(ii) Similarly we have

$$R_6 = 111\,111 = \frac{10^6-1}{9} = \frac{999999}{9}$$

Now substituting the result of part (ii), $999999 = 3^3\times 7\times 11\times 13\times 37$, into this yields

$$R_6 = 111\,111 = \frac{999999}{9} = \frac{\cancel{3^2}\times 3\times 7\times 11\times 13\times 37}{\cancel{9}} = 3\times 7\times 11\times 13\times 37$$

Hence $R_6 = 3\times 7\times 11\times 13\times 37$.

15. We are asked to factorize $8^8 - 1 = 16\,777\,215$. First apply the difference of two squares to this:

$$\begin{aligned} 8^8 - 1 &= \left(8^4-1\right)\left(8^4+1\right) \\ &= \left(8^2-1\right)\left(8^2+1\right)\left(8^4+1\right) \\ &= \left(63\right)\times\left(65\right)\times\left(8^4+1\right) \\ &= \left(7\times 9\right)\times\left(5\times 13\right)\times\left(8^4+1\right) \\ &= 3^2\times 5\times 7\times 13\times\left(4097\right) \end{aligned}$$

We need to factorize 4097. By using the results of chapter 2 we have

$$\left\lfloor\sqrt{4097}\right\rfloor = 64$$

Therefore if 4097 is composite it must have a prime factor less than 64. If we try 17 we find that $4097 = 17\times 241$. We also need to check if 241 is prime.

$$\left\lfloor\sqrt{241}\right\rfloor = 15$$

Hence 241 is prime because if any primes below 15 went into 241 then it would also be a factor of 4097 and it isn't. Hence $4097 = 17\times 241$. We have

$$16\,777\,215 = 8^8 - 1 = 3^2\times 5\times 7\times 13\times 17\times 241$$