1. Recall that a rational number is a number that can be expressed as a quotient of integers. That is, if $x$ is a rational number, then there exist two integers $m$ and $n$ such that $x = \frac{m}{n}$.

Using proof by contradiction, prove that if a number $y$ is irrational, then $\sqrt{y}$ is irrational.

Suppose, for the sake of contradiction, that $y$ is irrational and $\sqrt{y}$ is rational.

That is to say, we can write $\sqrt{y}$ as (for some unknown integers $m$ and $n$):

$$\sqrt{y} = \frac{m}{n}$$

Squaring both sides yields:

$$y = \frac{m \cdot m}{n \cdot n}$$

But a product of two integers is necessarily an integer. So $m \cdot m$ is an integer and $n \cdot n$ is an integer. Thus, $y$ is a quotient of integers, and thus it is a rational number. But this contradicts our assumption that $y$ is irrational.

Thus, by contradiction, we have shown that if $y$ is irrational then $\sqrt{y}$ is irrational.

Remarks for marking:
There are many other ways to solve this by contradiction. Most importantly, the solution should start by assuming the negation of the consequent. If the solution shows understanding of the general method of proof by contradiction and how to apply it to the problem, they should receive at least 6/10.

This problem is also solvable using proof by contrapositive (starting with the negation of the consequent and working to the negation of the antecedent). I would equally accept a proof by contrapositive solution here, which can be thought of as a special case of proof by contradiction.
2. Suppose we have the following first-order recurrence relation:

\[ a_n = 4a_{n-1} + 3 \]
\[ a_0 = 0 \]

Prove, using proof by induction, that for all \( n \geq 0 \):

\[ a_n = 4^n - 1 \]

Proof by induction:

Base case: \( n = 0 \).
We are given that \( a_0 = 0 \).
Plugging \( 0 \) into our closed-form solution for all \( n \), we get \( a_0 = 4^0 - 1 = 0 \).
Thus, our base case is satisfied.

Induction step:
Induction hypothesis: Assume that for some arbitrary \( k \geq 0 \), that the formula holds. That is:

\[ a_k = 4^k - 1 \]

Now, consider the recurrence relation for the case of \( k + 1 \):

\[ a_{k+1} = 4a_k + 3 \]

Now, using our induction hypothesis, we can substitute in our closed-form solution for \( k \):

\[ a_{k+1} = 4(4^k - 1) + 3 \]
\[ a_{k+1} = 4^{k+1} - 4 + 3 \]
\[ a_{k+1} = 4^{k+1} - 1 \]

Thus, our solution holds for \( k + 1 \) whenever it holds for an arbitrary \( k \). By the principle of mathematical induction, our closed-form solution holds for all \( n \geq 0 \).

Remarks for marking:
The proof by induction should always involve both a base case (in which the statement is shown to be true for a particular instance of \( n \)), and an induction step (where the statement is assumed to be true for an arbitrary \( k \) and shown to be true for \( k + 1 \)).

If a solution demonstrates an understanding of the basic form of an inductive proof, it should receive at least 6/10 (3 marks for the base case, 3 marks for the induction step).

The closer the solution is to a complete proof, the closer the mark should be to 10.

A correct proof without a base case should receive 7/10.

There are several ways to go from the assumption that the statement holds for an arbitrary \( k \) to the conclusion that the statement holds for \( k + 1 \). Any valid sequence of steps should be accepted equally.
3. Prove, using proof by smallest counter-example, that the following statement is true for all integers \( n \geq 1 \).

\[
\sum_{j=1}^{n} (2j+3) = n^2 + 4n
\]

Proof by smallest counter-example.

Suppose for the sake of contradiction, there exists a non-empty set \( X \) of counter-examples to this statement. Consider the smallest such counter-example \( x \in X \).

**Basis step:**
Substituting into this formula \( n = 1 \), we get for the left hand side:

\[
\sum_{j=1}^{1} (2j+3) = 2(1) + 3 = 5
\]

On the other hand, for the right hand side, we get:

\[
1^2 + 4 \cdot 1 = 5
\]

Thus, we conclude that \( x \neq 1 \).

Now consider the smallest counter-example \( x \). Since \( x \geq 2 \), we get that the statement must be true for \( x-1 \). That is:

\[
\sum_{j=1}^{x-1} (2j+3) = (x-1)^2 + 4(x-1)
\]

Now, we add to both sides the quantity \( 2x+3 \):

\[
\sum_{j=1}^{x-1} (2j+3) + 2x+3 = (x-1)^2 + 4(x-1) + 2x + 3
\]

\[
\sum_{j=1}^{x} (2j+3) = x^2 - 2x + 1 + 4x - 4 + 2x + 3
\]

\[
\sum_{j=1}^{x} (2j+3) = x^2 + 4x
\]

This shows that \( x \) satisfies the original statement, and thus is not a counter-example. This contradicts \( x \) being a counter-example \( \Rightarrow \). Thus, the set of counter-examples cannot have a least element, so by the well-ordering principle, it must be empty. That is, there are no counter-examples to the statement. The statement is true for all \( n \geq 1 \).

**Remarks for marking:**
The proof by smallest counter-example should always involve both a basis step (in which it is shown that the smallest counter-example is not a particular instance of \( n \)), and an “contradiction” step (where, given the
statement is true for \( x - 1 \), it is shown that \( x \) is not a counter-example, which contradicts that \( x \) is a counter-example).

If a solution demonstrates an understanding of the basic form of a proof by smallest counter-example, it should receive at least 6/10 (3 marks for the basis step, 3 marks for the “contradiction” step).

The closer the solution is to a complete proof, the closer the mark should be to 10.

A correct proof without a base case should receive 7/10.

There are several ways to show that the statement holds for \( x \) given that it holds for \( x - 1 \). Any valid sequence of steps should be accepted equally.
4. Suppose we have two sets $A = \{1,2,3,4,5\}$ and $B = \{11,12,13,14,15,16,17,18\}$.

a) How many possible different injective (one-to-one) functions are there from $A$ to $B$? Justify your answer.

b) How many possible different surjective (onto) functions are there from $A$ to $B$? Justify your answer.

(Hint: Remember what it means for a function to be injective (one-to-one) and surjective (onto). You may also need to use a counting argument.)

For part a), we remember that an injective function is a function $f : A \to B$ for which every element of $B$ is mapped to by at most one element of $A$. Or, written more formally: if $a \neq b$ then $f(a) \neq f(b)$.

So, we can think of our injective function allowing each element of $A$ to pick an element of $B$ without replacement.

For our specific example:
The element 1 can be mapped to any of the eight elements in $B$.
The element 2 can be mapped to any of the remaining seven elements in $B$.
The element 3 can be mapped to any of the remaining six elements in $B$.
The element 4 can be mapped to any of the remaining five elements in $B$.
The element 5 can be mapped to any of the remaining four elements in $B$.

That is to say, there are a total of $8 \times 7 \times 6 \times 5 \times 4$ ways that $f$ can map elements of $A$ to $B$ injectively.

So, there are a total of $\frac{8!}{(8-5)!} = 6720$ injective functions from $A$ to $B$.

For part b), we remember that an injective function is a function $f : A \to B$ for which every element of $B$ is mapped to by some element of $A$. Or, written more formally: $\forall b \in B$, there exists an $a \in A$ such that $f(a) = b$.

Since $f : A \to B$ is a function and $A$ has only five element but $B$ has eight elements, there is no possible way that every element of $B$ can be mapped to.

Thus, there are 0 surjective functions from $A$ to $B$.

Remarks for marking:
The solution in general to the part a) is $\frac{|A|!}{(|A| - |B|)!}$. The solution in general for part b) is zero if $|A| < |B|$.

Since there are no calculators on the test, if the solution is not expanded or there is an error in expanding the solution, do not deduct any marks.

If the solution shows an understanding of what it means for a function to be injective and surjective, it should receive at least 6/10. (3 marks for each of injective and surjective).
For both parts, the closer the argument is to being correct (both the counting argument and the argument that no surjective functions exist), the closer the mark should be to 10.

There are several ways to correctly argue the correct number of injective and surjective functions from \( A \) to \( B \). Any valid sequence of steps should be accepted equally. The arguments do not need to be too formal.
5. Suppose we have the following two permutations on the set $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$ represented in cycle notation.

$\pi = (1, 8)(2, 5, 6, 7, 3)(4)$

$\sigma = (1, 3, 5, 7)(2, 4, 6, 8)$

a) Compute the permutation $\sigma \circ \pi^{-1}$. Write your answer in cycle notation.

b) Write $\sigma$ as a composition of transpositions. Is it possible to write $\sigma$ using one fewer transposition than you just did? Explain.

For part a), let us first compute $\pi^{-1}$. We can do this directly from cycle notation.

$\pi^{-1} = (8, 1)(3, 7, 6, 5, 2)(4)$

Now, we compute $\sigma \circ \pi^{-1}$, using their representations in array notation:

$\pi^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 3 & 7 & 4 & 2 & 5 & 6 & 1 \end{bmatrix}$

Composing this with $\sigma$ yields:

$\sigma \circ \pi^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 3 & 7 & 4 & 2 & 5 & 6 & 1 \\ 2 & 5 & 1 & 6 & 4 & 7 & 8 & 3 \end{bmatrix}$

So, re-writing this in cycle notation gives us:

$\sigma \circ \pi^{-1} = (1, 2, 5, 4, 6, 7, 8, 3)$

For part b), we re-write $\sigma$ as a composition of transpositions in the following way, recalling that independent cycles can be written as independent compositions of transpositions:

$\sigma = (1, 7) \circ (1, 5) \circ (1, 3) \circ (2, 8) \circ (2, 6) \circ (2, 4)$

It is not possible to $\sigma$ as a composition of transpositions using one fewer transposition than above (i.e. we cannot write $\sigma$ as a composition of five transpositions). This is by our theorem that every transposition can only be written as either a composition of an odd number of transpositions or a composition of an even number of transpositions. Since we wrote $\sigma$ as a composition of six (an even number) transpositions, we cannot also write $\sigma$ as a composition of five (an odd number) transpositions.

Remarks for marking:
For part a), the solutions are fairly computational. There are a few methods for computing the inverse and composition of permutations by hand – any reasonable method should be accepted equally. Please be aware that any rearrangement of the independent cycles or cyclic re-ordering of the elements within each cycle is an equivalent permutation. These should all be accepted equally.
For part b), there are an infinite number of ways to write a permutation as a composition of transposition. The way used here is the one from the textbook, but any other equivalent decomposition should be accepted equally. The argument for writing \( \sigma \) with one fewer transposition does not need to prove anything, but should show understanding that permutations are exclusively even or odd.

The closer the computations and argument are to being correct, the closer the mark should be to 10.