1 Collette has been asked to prove that:

'If n is any integer which is not divisible by 5, then $n2$ divided by 5 always leaves a remainder of either 1 or 4'.

a Collette begins her proof by using the division theorem to consider the possible forms which n can take. She correctly states:

First possible form: $n = 5t + 1$ **(3 marks)**

b Find all of the other possible forms for n using a similar format.

By considering each of the separate possible forms for n, prove, by exhaustion, that the given statement is correct. **(5 marks)**

2 Consider the two integers **X** = 831 and **Y** = 2827.

a Applying your knowledge of divisibility tests, show that neither **X** nor **Y** are prime. **(2 marks)**

b Two integers are coprime if their greatest common factor = 1.

Using the Euclidean algorithm, determine whether **X** and **Y** are coprime. **(4 marks)**

3 The greatest common factor of 252 and 105 is defined as the integer d.

a Using back substitution, find integer values x and y which satisfy the Bezout's identity:

$$252x + 105y = d$$

(5 marks)

b The solutions you have found in part **a** are not unique.

Labelling your solutions as x_0 and y_{02}, pairs of alternative solutions may be found as follows:

$$x_{n+1} = x_n + 105 \quad \text{and} \quad yx_{n+1} = yx_n - 252$$

where $n \in \square$

i Find two more pairs of integer values which satisfy the same identity. **(1 mark)**

ii By substitution, or otherwise, prove by induction that this process always **works.** **(2 marks)**

4 Two integers, a and b, are known to be congruent, modulo $\boldsymbol{n}$, where $n \in \mathbb{Z}$.

a Show algebraically that

i $a \equiv b \,(\text{mod}) \Rightarrow a - b = \text{kn}$, where $k \in \mathbb{Z}$ **(2 marks)**

ii $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$ **(2 marks)**

b Given $p_1 \equiv q_1 \pmod{n}$ and $p_2 \equiv q_2 \pmod{n}$, and that $b \equiv a \Rightarrow a \equiv b$, prove that

i $p_1 + p_2 \equiv q_1 + q_2 \pmod{n}$ **(2 marks)**

ii $p_1 p_2 \equiv q_1 q_2 \pmod{n}$ **(3 marks)**

5 **a** Peter has discovered that 82 and 723 are coprime.

He now believes that the equation below has a solution for all possible integer values of $\boldsymbol{q}$.

$$82p \equiv q \pmod{723},$$

where $p \in \mathbb{Z}$

i Using appropriate and precise mathematical language, define Q, the set of all possible non-congruent integer values for q. **(2 marks)**

ii State, with reason, why Peter is correct regarding the given equation. **(1 mark)**

b Solve the equation $21x \equiv 12 \pmod{159}$, where $\{x \in \mathbb{Z} : x < 159\}$ **(5 marks)**

c Using Fermat's Little Theorem, show that $235 + 1 \equiv 0 \pmod{11}$ **(3 marks)**

6 The set $\mathbf{R}_n$ comprises all of the unique residuals for modulo $\boldsymbol{n}$.

$S_m \subset R_n$, such that S_m comprises $\boldsymbol{m}$ unique members of $\mathbf{R}_n$ and $0 < m < n$.

a When $\boldsymbol{n} = 8$, find how many different subsets exist which all satisfy the criteria for $\mathbf{S}_6$. **(2 marks)**

b Show that the total number of subsets, $\boldsymbol{T}$, containing 3 or fewer elements of $\mathbf{R}_n$ is given by the formula

$$T = \frac{n(n^2 + 5)}{6}$$

(6 marks)