1. (**3x4=12 marks**)

(a) The algorithm gives us

n	x	y	
78	1	0	r_1
72	0	1	r_2
6	1	-1	$r_3 = r_1 - r_2$
0	-12	13	$r_4 = r_3 - 12r_2$

From which we see that $\gcd(78, 72) = 6$ and $6 = 78 \cdot (1) + 72 \cdot (-1)$. Now $\gcd(78, 72) = 6$ does not divide 13 so there are no integer solutions.

(b) $\gcd(78, 72) = 6 \mid 12$ so there are integer solutions: $12 = 6 \cdot 2 = 78 \cdot (2) + 72 \cdot (-2)$. Hence the general solution is $x = -2 - t \cdot \frac{78}{6} = -2 - t \cdot 13, t \in \mathbb{Z}$.

(c) The algorithm gives us

n	x	y	
240	1	0	r_1
77	0	1	r_2
9	1	-3	$r_3 = r_1 - 3r_2$
5	-8	25	$r_4 = r_2 - 8r_3$
4	9	-28	$r_5 = r_3 - r_4$
0	-17	53	$r_6 = r_4 - r_5$

From this we see that $\gcd(77, 240) = 1 = 77 \cdot (53) + 240 \cdot (-17)$. $\gcd(77, 240) = 1 \mid 53$ so there are integer solutions: $53 = 1 \cdot 53 = 77 \cdot (53 \cdot 53) + 240 \cdot (-17 \cdot 53) = 77 \cdot (2809) + 240 \cdot (-17 \cdot 53)$. Hence the general solution is $x = 2809 - t \cdot \frac{240}{1} = 2809 - t \cdot 240t \in \mathbb{Z}$.

2. (**4 marks**) Solve the equation $\overline{53} = \overline{77} \cdot_{240} \overline{x}$ in $\mathbb{Z}_{240}$. Using the above solutions, we have $\overline{53} = \overline{77} \cdot_{240} \overline{x} \iff 53 = 77x + 240y$, so the solutions are $x = 2809 - t \cdot 240t$. Each of these is in the same equivalence class since they differ by a multiple of 240 and the representative solution in the range 0 ... 239 is $x = 2809 - 11 \cdot 240 = 169$.

3. (a) (**6 marks**) Checking each of the cases

x	$2x^2 - 3x \pmod{240}$
0	0
1	6
2	2
3	2
4	6
5	0
6	5

Hence the solutions are $x = 1, 4$.

(b) (**6 marks**) $28x \equiv 42 \pmod{70} \iff 4x \equiv 6 \pmod{10}$. Checking cases we have

x	$4x \pmod{10}$
0	0
1	4
2	8
3	2
4	6
5	0
6	4
7	8
8	2
9	6

Hence the solutions are $x = 4, 9$.

4. (**6 marks**) $(5n+6)(13n+7)(7n+8) \equiv 5n(n+1)(n+2) \equiv (-n)(n+1)(n+2) \pmod 6$. But given any three successive integers, there is at least one which is a multiple of 3 and at least one even number. Hence $n(n+1)(n+2) \mid 6$ so $(-n)(n+1)(n+2) \mid 6$ also.

5. (**5+5=10 marks**) We first divide $b(x)$ into $a(x)$, then divide the remainder into $b(x)$, and so on, until we get a remainder of 0.

$$\begin{array}{rrrrr}
 & 2 & & & \\ \cline{2-5}
x^3-7x-6 \;) & 2x^3 & -5x^2 & & -9 \\
 & 2x^3 & & -14x & -12 \\ \cline{2-5}
 & & -5x^2 & +14x & +3
\end{array}$$

so $a(x) = 2b(x) - 5x^2 + 14x + 3$, and then

$$\begin{array}{rrrrr}
 & \frac{-1}{5}x & -\frac{14}{25} & & \\ \cline{2-5}
-5x^2+14x+3 \;) & x^3 & & -7x & -6 \\
 & x^3 & -\frac{14}{5}x & -\frac{3}{5}x & \\ \cline{2-4}
 & \frac{14}{5}x^2 & -\frac{32}{5}x & -6 & \\
 & \frac{14}{5}x^2 & -\frac{14^2}{25}x & -\frac{42}{25} & \\ \cline{3-4}
 & & \frac{36}{25}x & -3\frac{36}{25} &
\end{array}$$

But now it is easy to see $x-3$ is a factor of $-5x^2+14x+3$ since $-5 \cdot 9 + 14 \cdot 3 + 3 = 0$.

Hence factorizing $-5x^2+14x+3 = -(x-3)(5x+1)$.

Note that for any $a(x), c(x) \in \mathbb{R}[x]$, and $k \in \mathbb{R} \setminus \{0\}$, $c(x) \mid a(x)$ if and only if $kc(x) \mid a(x)$. So, when we are applying the Euclidean Algorithm we may multiply or divide by constants to make the numbers nicer to deal with.

Now we have

n	x	y	
a	1	0	r_1
b	0	1	r_2
c	1	-2	$r_3 = r_1 - 2r_2$
d	$\frac{1}{5}x + \frac{14}{25}$	$1 - 2(\frac{1}{5}x + \frac{14}{25})$	$r_4 = r_2 - (\frac{1}{5}x + \frac{14}{25})r_3$
0	?	?	$r_5 = r_3 + \frac{25}{36}(5x+1)r_4$

Multiplying through by 25 to simplify the calculation we find that
$(5x + 14)(2x^3 - 5x^2 - 9) - (10x + 3)(x^3 - 7x - 6) = 36(x - 3)$ as expected.

6. (**6+6=12 marks**)

(a) Suppose $e * e = e$. Consider any $a \in G$ then $(e * e) * a = e * a$, so $e * (e * a) = e * a$, so $e * a = a$. Similarly $a * (e * e) = a * e$, so $(a * e) * e = a * e$, so $a * e = a$.

(b) If $\exists a : a * e = a$, then $\forall b \in G$, $b * a^{-1} * a * e = b * a^{-1} * a$ or $b * i * e = b * i$, or $b * e = b$. Hence $e * e = e$ and e is the identity by (a).

7. (**12 marks**) We will complete the following Cayley Table for $*$ as follows:

(a) $e * c = e \implies c = i$. We can thus fill in the row and column of c accordingly.

(b) Now $a * e$ has to equal a or c but there is already a in row 1, so $a * e = c$ and $d * e = a$.

(c) Now $a * e = c$, so $e * a = c$.

(d) Now in the last row $e * d$ can't be d so $e * b = d$ and $e * d = a$.

(e) Now $b * b = b * (e * e) = (b * e) * e = d * e = a$

(f) Now we can fill in the remaining entries by elimination.

$*$	a	b	c	d	e
a	d	e	a	b	c
b	e	a	b	c	d
c	a	b	c	d	e
d	b	c	d	e	a
e	c	d	e	a	b

8. (**12 marks**) Let $A = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$ be elements of K.

Then $AB = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}$, thus $AB \in K$.

Hence, K is closed under matrix multiplication.

Associativity is satisfied for multiplication of *all* matrices, not only for those in K.

The identity element is $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, since $IA = AI = \begin{pmatrix} 1 & x+0 \\ 0 & 1 \end{pmatrix} = A$ and it is a member of K.

The inverse of $A = \begin{pmatrix} 1 & \text{x} \\ 0 & 0 \end{pmatrix}$ is $A^{-1} = \begin{pmatrix} 1 & \text{-x} \\ 0 & 0 \end{pmatrix}$, since , since $A^{-1}A = AA^{-1} = \begin{pmatrix} 1 & x-x \\ 0 & 1 \end{pmatrix} = I$.

Thus K is a group.