DEPARTMENT OF MATHEMATICS

MATHS 255	Solutions to Assignment 8	Due: 14 May 2003

1. 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.

$$\begin{array}{rrrrrr}
 & & x & +5 & & \\ \cline{2-6}
x^2-4x+4 &) & x^3 & +x^2 & -2x & -8 \\
 & & x^3 & -4x^2 & +4x & \\ \cline{2-5}
 & & & 5x^2 & -6x & -8 \\
 & & & 5x^2 & -20x & +20 \\ \cline{4-6}
 & & & & 14x & -28
\end{array}$$

so $a(x) = (x+5)b(x) + (14x-28)$, and then

$$\begin{array}{rrrrr}
 & & \frac{1}{14}x & -\frac{1}{7} & \\ \cline{2-5}
14x-28 &) & x^2 & -4x & +4 \\
 & & x^2 & -2x & \\ \cline{2-4}
 & & & -2x & +4 \\
 & & & -2x & +4 \\ \cline{4-5}
 & & & & 0
\end{array}$$

So we have $b(x) = (\frac{1}{14}x - \frac{1}{7})(14x-28)$. The last non-zero remainder was $14x-28$, so $14x-28$ is a greatest common divisor of $a(x)$ and $b(x)$.

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. After the first long division above, we could have divided $\frac{1}{14}(14x-28) = (x-2)$ into $b(x)$ instead. which would have given us $b(x) = (x-2)(x-2)$, and the greatest common divisor we found would be $x-2$ instead of $14x-28$.

2. (a) Putting $u(x) = 0$ and $v(x) = 0$ gives $0 = a(x)u(x) + b(x)v(x)$, so $0 \in S$, and therefore $\deg 0 = -\infty \in T$.

(b) We know that if $A \subseteq \mathbb{Z}$, $A \neq \emptyset$ and A is bounded below then A has a least element. We certainly have $T' \subseteq \mathbb{Z}$, and T' is bounded below by 0, so we only need to show that $T' \neq \emptyset$, in other words to show there is some $c(x) \in S$ with $c(x) \neq 0$. Putting $u(x) = 1$, $v(x) = 0$ we get $a(x)u(x) + b(x)v(x) = a(x)$, so $a(x) \in S$. We assumed that $a(x) \neq 0$, so $\deg a(x) \neq -\infty$, so $\deg a(x) \in T'$. Thus $T' \neq \emptyset$, so it has a least element, n say.

(c) Since $n \in T'$, there is some $d(x) \in S$ with $\deg d(x) = n$. Thus there exist $u_d(x), v_d(x)$ with

$$d(x) = a(x)u_d(x) + b(x)v_d(x). \tag{1}$$

Using the Division Algorithm to divide $d(x)$ into $a(x)$, there exist $q_a(x)$ and $r_a(x)$ with

$$a(x) = q_a(x)d(x) + r_a(x) \tag{2}$$

and $\deg r_a(x) < \deg d(x)$. Substituting (1) into (2) and rearranging, we get

$$a(x) = q_a(x)(a(x)u_d(x) + b(x)v_d(x)) + r_a(x),$$

so $r_a(x) = a(x)(1 - q_a(x)u_d(x)) + b(x)(-q_a(x)v_d(x))$, so $r_a(x) \in S$.

(d) Since $r_a(x) \in S$, $\deg r_a(x) \in T$. However, $\deg r_a(x) < n$, so $\deg r_a(x) \notin T'$. This must mean that $\deg r_a(x) = -\infty$, so $r_a(x) = 0$. Thus (2) becomes $a(x) = q_a(x)d(x)$, so $d(x) \mid a(x)$.

(e) Similarly, we can write

$$b(x) = q_b(x)d(x) + r_b(x) \tag{3}$$

with $\deg r_b(x) < \deg d(x)$. We can substitute (1) into (3) and rearrange to get

$$b(x) = q_b(x)(a(x)u_d(x) + b(x)v_d(x)) + r_b(x),$$

so $r_b(x) = a(x)(-q_b(x)u_d(x)) + b(x)(1-q_b(x)v_d(x))$, so $r_b(x) \in S$. Again, since $\deg r_b(x) \in T \backslash T'$ we must have $r_b(x) = 0$ so $b(x) = q_b(x)d(x)$, so $d(x) \mid b(x)$.

(f) Suppose $c(x)$ is a common divisor of $a(x)$ and $b(x)$, so there exist $s(x)$ and $t(x)$ with $a(x) = s(x)c(x)$ and $b(x) = t(x)c(x)$. Substituting these into (1) gives

$$d(x) = s(x)c(x)u_d(x) + t(x)c(x)v_d(x) = c(x)(s(x)u_d(x) + t(x)v_d(x)),$$

so $c(x) \mid d(x)$.

3. Let $G = \{\alpha, \beta, \gamma, \delta, \varepsilon\}$. Given that $*$ is a group operation on G, we will complete the following Cayley Table for $*$:

(a) From $\alpha * \beta = \beta$, we know that α must be the identity element for G. This lets us fill in the row α and the column α.

(b) We now have β, δ and γ already appearing in row β, so $\beta * \varepsilon$ must be either α or ε. But we also already have ε in column ε, so $\beta * \varepsilon$ must be α.

(c) We now have $\beta * \varepsilon = e$, so $\varepsilon * \beta = e$, i.e. $\varepsilon * \beta = \alpha$.

(d) Column β already contains β, δ and α, so the remaining two entries must be γ and ε. γ already appears in row γ, so we must have $\gamma * \beta = \varepsilon$ and $\delta * \beta = \gamma$.

(e) We have

$$\delta * \delta = (\beta * \beta) * \delta = \beta * (\beta * \delta) = \beta * \gamma = \varepsilon.$$

(f) Looking at column γ, the two remaining entries are α and β: row ε already contains α so $\varepsilon * \delta = \beta$ and $\gamma * \delta = \alpha$. Now $\delta * \varepsilon$ is α or β, and it cannot be α, so $\delta * \varepsilon = \beta$ and $\delta * \gamma = \alpha$. Similarly $\gamma * \varepsilon$ is β or δ, and it is not β, so $\gamma * \varepsilon = \delta$ and $\gamma * \gamma = \beta$. Thus $\varepsilon * \gamma = \delta$ and $\varepsilon * \varepsilon = \gamma$. The final Cayley Table we obtain is

$*$	α	β	γ	δ	ε
α	α	β	γ	δ	ε
β	β	δ	ε	γ	α
γ	γ	ε	β	α	δ
δ	δ	γ	α	ε	β
ε	ε	α	δ	β	γ