NB: Please deposit your solutions in the appropriate box **by 4 p.m. on the due date.** Late assignments or assignments placed into incorrect boxes will not be marked. Use a mathematics department cover sheet. These are available from outside the Resource Centre. PLEASE SHOW ALL WORKING. Also if we believe you have COPIED someone else's script or that you have let someone else COPY YOUR SCRIPT, then you will get NO MARKS.

1. Let $a, b, c \in \mathbb{Z}$. Prove that if $a \mid b$ and $b \mid c$ then $a \mid c$.

soln: $b \mid c$ means there is $\ell \in \mathbb{Z}$ so that $c = \ell b$ (a). $a \mid b$ means there is $k \in \mathbb{Z}$ so that $b = ka$. Substituting the last in (a) gives $c = k\ell a$. Since $k\ell \in \mathbb{Z}$ this shows that $a \mid c$. [4 marks]

2. Use the Euclidean algorithm to find the greatest common divisor of 2700 and 17,640. Show your working carefully.

soln:
$17,640 = 6 \cdot 2700 + 1440$
$2700 = 1 \cdot 1440 + 1260$
$1440 = 1 \cdot 1260 + 180$
$1260 = 7 \cdot 180$
So by the Euclidean algorithm $\gcd(2700, 17640) = 180$. [4 marks]

3. Prove the theorem from lectures:
If $a, b, q, r \in \mathbb{Z}$ and $a = bq + r$ then $\gcd(a, b) = \gcd(b, r)$.

soln: If $c \in \mathbb{Z}$ is a common divisor of b and r then clearly (or by an exercise in lectures) c is a divisor of $bq + r = a$. Since also c is a divisor of b we have (in summary) that

> $c \in \mathbb{Z}$ is a common divisor of b and r implies that c is a common divisor of a and b. (*)

[3 marks]
Now suppose c is a common divisor of a and b. Then in particular c is a divisor of b. Also since $r = a - bq$ we have $c \mid r$. So in summary,

> $c \in \mathbb{Z}$ is a common divisor of a and b implies that $c \in \mathbb{Z}$ is a common divisor of b and r. (**)

[3 marks]

From (*) and (**) we see that the pair (a, b) and the pair (c, d) have the *same set* of positive common divisors. The greatest element of this set (with respect to the relation $\mid$) is thus $\gcd(a, b)$ and $\gcd(c, d)$. [3 marks]

4. Let $a, b \in \mathbb{Z}$, not both zero, then the following statements are equivalent for a positive common divisor d of a and b:
(i) $c \leq d$ for all common divisors c of a and b.
(ii) $c \mid d$ for all common divisors c of a and b.

(a) That (ii)⇒(i) is true is *almost* immediate from some result in lectures. What is that result? Show something about d that enables us to use that result.
soln: Since a, b are not both zero the common divisor d cannot be zero. Thus (ii)⇒(i) follows at once from 5. of the 'Basic Properties'. That is
"If $a \mid b$ and $b \neq 0$ then $|a| \leq |b|$". [3 marks]

(b) Prove that (i)$\Rightarrow$(ii) is true *by the following steps.* (Throughout c is a common divisor of a and b.)

(a) Show that a is a common multiple of c and d.
(b) Show that b is a common multiple of c and d.
(c) Let $m = \operatorname{lcm}(d, c)$. Explain why $m \mid a$ and $m \mid b$.
(d) Explain why we can use the last results to conclude that $m \leq d$.
(e) On the other hand it is obvious that $d \leq m$. Why?
(f) Use the last two results to deduce that $c \mid d$.

soln:

c, d are both common divisors of a and b. In particular then:
(a) c, d are both divisors of a. That is $c \mid a$ and $d \mid a$ so a is a common multiple of c and d. [2 marks]
(b) c, d are both divisors of b. That is $c \mid b$ and $d \mid b$ so b is a common multiple of c and d. [2 marks]
(c) Let $m = \operatorname{lcm}(d, c)$. We just showed that a is a common multiple of c and d so $m \mid a$ (since by definition the lcm divides all other common multiples). Similarly from (b) we have that b is a common multiple of c and d. So $m \mid b$. [2 marks]
(d) In (c) we showed that m is a common divisor of a and b. By (i), which we are assuming, d is the largest common divisor (with respect to $\leq$). Thus $m \leq d$. [2 marks]
(e) On the other hand $m = \operatorname{lcm}(d, c)$ so $m \geq 0$ and $d \mid m$. thus $d \leq m$ (by 'Basic Property' 5). [2 marks]
(f) From (d) and (e) we have $d = m$. Of course $c \mid m$ as $m = \operatorname{lcm}(c, d)$. So $c \mid d$. [2 marks]

Total: 32 marks.