**MAT235 Assignment 3 Solutions**

**1.1:** $302 = 15 \times 19 + 17$. $\therefore$ the quotient is 15 and the remainder is 17.
**1.2:** $-302 = -16 \times 19 + 2$. $\therefore$ the quotient is -16 and the remainder is 2.
**1.3:** $0 = 0 \times 19 + 0$. $\therefore q = 0, r = 0$.
**1.4:** $2000 = 117 \times 17 + 11$. $\therefore q = 117, r = 11$.
**1.5:** $2001 = 117 \times 17 + 12$. $\therefore q = 117, r = 12$.
**1.6:** $2008 = 118 \times 17 + 2$. $\therefore q = 118, r = 2$.

**2:** As suggested in the hint, let $a \in \mathbb{Z}$ be an arbitrary integer and write $a = 4q + r$ for $r, q \in \mathbb{Z}$, $0 \leq r \leq 3$. Then $a^2 = (4q + r)^2 = 16q^2 + 8qr + r^2 = 4k' + r^2$, where $k' = 4q^2 + 2qr$. If $r$ is 0 or 1 we are done and if $r = 2$, then $4k' + 2^2 = 4(k' + 1) = 4k$. Finally, if $r = 3$, then $4k' + 3^2 = 4(k' + 2) + 1 = 4k + 1$. Hence $a^2$ can always be written as an integer multiple of 4, or 1 plus an integer multiple of 4.

**3:** Let $a = 2, b = c = 1$. Then clearly $a|(b + c)$ but $a \not| b$ and $a \not| c$.

**4:** Subbing the root $r$ into the given equation, we have $0 = r^2 + ar + b$. Rearranging, we get $-b = r^2 + ar = r(a + r)$. $\therefore r|b$ and the quotient is $-(a + r)$.

**5.1:** Suppose $(n, n + 2) = d$. Writing $n = dk$ and $n + 2 = dk'$, their difference can be written as $2 = n + 2 - n = d(k' - k)$. $\therefore d|2$ and we conclude the only possibilities for $d$ are 1 and 2 (Note that GCDs are always positive). To show both 1 and 2 are obtained for some $n$, check for $n \in \{1, 2\}$.
**5.2:** A similar argument as above shows $d = (n, n + 6)|6$. Hence $d \in \{1, 2, 3, 6\}$. Again, choose $n \in \{1, 2, 3, 6\}$ to show all such $d$ can be obtained.
**5.3:** Again let $d = (n, 2n + 1)$. Then $d$ divides the difference $2n + 1 - n = n + 1$. But now $d$ divides $n$ and $n + 1$, so $d$ divides the difference $n + 1 - n = 1$. Hence $d = 1$.

**6:** We argue similarly to (5.3). $a|n + 2$ and $a|2n + 18$, so $a$ divides $n + 16$. Applying differences again, we get $a|14$. Since $a$ is odd and greater then 1, we conclude $a = 7$. Choosing $n = 5$ shows that $a = 7$ is in fact possible.

**7.1:** We follow the Euclidean algorithm to find $(a, b)$ and to construct elements $u, v \in \mathbb{Z}$ such that $au + bv = (a, b)$.

$$\begin{aligned} 72 &= 1 \times 56 + 16 \\ 56 &= 3 \times 16 + 8 \\ 16 &= 2 \times 8 + 0 \end{aligned} \quad \Longrightarrow \quad \begin{aligned} 8 &= 56 - 3 \times 16 \\ &= 56 - 3(72 - 1 \times 56) \\ &= 4 \times 56 - 3 \times 72. \end{aligned}$$

$\therefore (56, 72) = 8$ and $u = 4, v = -3$.
**7.2:**

$$\begin{aligned} 138 &= 5 \times 24 + 18 \\ 24 &= 1 \times 18 + 6 \\ 18 &= 3 \times 6 \end{aligned} \quad \Longrightarrow \quad \begin{aligned} 6 &= 24 - 1 \times 18 \\ &= 24 - 1(138 - 5 \times 24) \\ &= 6 \times 24 - 138. \end{aligned}$$

$\therefore (24, 138) = 6$ and $u = 6, v = -1$.

**7.3:**

$$\begin{array}{lcl} 227 = 1 \times 143 + 84 & & 1 = 7 - 3 \times 2 \\ 143 = 1 \times 84 + 59 & & = 7 - 3(9-7) = -3 \times 9 + 4 \times 7 \\ 84 = 1 \times 59 + 25 & & = -3 \times 9 + 4(25 - 2 \times 9) = 4 \times 25 - 11 \times 9 \\ 59 = 2 \times 25 + 9 & \Longrightarrow & = 4 \times 25 - 11(59 - 2 \times 25) = -11 \times 59 + 26 \times 25 \\ 25 = 2 \times 9 + 7 & & = -11 \times 59 + 26(84 - 59) = 26 \times 84 - 37 \times 59 \\ 9 = 1 \times 7 + 2 & & = 26 \times 84 - 37(143 - 84) = -37 \times 143 + 63 \times 84 \\ 7 = 3 \times 2 + 1 & & = -37 \times 143 + 63(227 - 143) = 63 \times 227 - 100 \times 143 \end{array}$$

$\therefore (143, 227) = 1$ and $u = -100, v = 63$.

**7.4:**

$$\begin{array}{lcl} 314 = 1 \times 159 + 155 & & 1 = 4 - 1 \times 3 \\ 159 = 1 \times 155 + 4 & & = 4 - 1(155 - 38 \times 4) = -1 \times 155 + 39 \times 4 \\ 155 = 38 \times 4 + 3 & \Longrightarrow & = -1 \times 155 + 39(159 - 155) = 39 \times 159 - 40 \times 155 \\ 4 = 1 \times 3 + 1 & & 39 \times 159 - 40(314 - 159) = -40 \times 314 + 79 \times 159 \end{array}$$

$\therefore (314, 159) = 1$ and $u = -40, v = 79$.

**8:**Assume $a|c$ and $b|c$. In general it need not be the case that $(ab)|c$, for example take $a = b = 4$ and $c = 8$. However, suppose now that $(a, b) = 1$, we provide 2 proofs, one which requires the fundamental theorem of arithmetic and one that does not, that shows $ab|c$.

**Proof 1:** By the fundamental theorem of arithmetic, we can write $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$ and $b = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot ... \cdot q_t^{\beta_t}$, where the $p$'s and $q$'s are distinct primes and the $\alpha$'s and $\beta$'s are natural numbers. By the condition on the GCD, it follows that none of the $q$'s can be the same prime as any of the $p$'s (Make sure you understand why). Since $a|c$ and $b|c$, it follows that $c$ has a prime decomposition of the form

$$c = \prod_{i=a}^{k} p_i^{\alpha_i} \prod_{j=1}^{t} q_j^{\beta_j} \prod_s l_s^{\gamma_s}$$

where the final product is over some finite set of primes raised to positive integer powers, which may or may not include any of the primes dividing $a$ or $b$. Hence

$$c = ab \prod_s l_s^{\gamma_s}$$

and $\therefore (ab)|c$ when $(a, b) = 1$.

**Proof 2:** Since $(a, b) = 1$, we can find integers $u, v$ such that $1 = ua + vb$. Multiply both sides of this equation by $c$ to get $c = cua + cvb$. Using the fact that $c = d \times b = d' \times a$ for some integers $d, d'$, we can factor the right hand side of the above equation as $c = a(cu + d'vb) = a(b(du + d'v))$. Therefore $c = ab(du + d'v)$ and hence $ab|c$.

**9:** There are obviously different solutions to this problem. Here is a method that admits a bound that is on the same order as the best possible (it is however not the best possible bound).

Consider applying the Euclidean algorithm to the pair of integers $n \geq m > 0$. We can consider the output as a pair of finite sequences of non-negative integers $\{r_k\}_{k=1}^t$ and$\{q_j\}_{j=0}^{t-1}$, where we have $r_1 > r_2 > ... > r_t = 0$, each $q_i > 0$ and

$n = q_0 \times m + r_1$
$m = q_1 \times r_1 + r_2$
and for $k > 2$ we have
$r_{k-2} = q_{k-1} \times r_{k-1} + r_k$.

Consider the ratio $n/r_2$. Using the top two equations above, we can conclude that

$$\frac{n}{r_2} = \frac{q_0 m + r_1}{r_2} = \frac{q_0(q_1 r_1 + r_2) + r_1}{r_2} = q_0 + \frac{(q_0 q_1 + 1) r_1}{r_2} > 3$$

where the last inequality comes from the fact that each $q$ is a positive integer and because $r_1 > r_2$. Note further that this inequality must also hold if $n/r_2$ is replaced by $m/r_3$ or $r_j/r_{j+3}$ where this is defined because we can always shift our starting point from $n$ and $m$ to $r_j$ and $r_{j+1}$ and then apply the above argument.

It follows that $n/r_{3s+2} = n/r_2 \cdot r_2/r_5 \cdot ... \cdot r_{3(s-1)+2}/r_{3(s)+2} > 3^{s+1}$. On the other hand the Euclidean Algorithm terminates when $r_t = 0$ or equivalently, $r_t < 1$ since the $r$'s will always be integers. Hence if $s \in \mathbb{N}$ is such that $n/r_{3s+2} > n$, it follows that the algorithm must terminate in at most $3s + 2$ steps. $\therefore$ it suffices to find $s$ such that $n/r_{3s+2} > 3^{s+1} > n$, which is to say $s > \log n/\log 3 - 1$. Hence the Euclidean algorithm will terminate in less then $3 \log n/\log 3 + 2$ steps.