MATH342 Feedback and Solutions 2

1. The prime factorisation of 1008 is

$$1008 = 2^4 \times 3^2 \times 7.$$

So the divisors are $2^{n_1} \times 3^{n_2} \times 7^{n_3}$ where $0 \leq n_1 \leq 4$, $0 \leq n_2 \leq 2$ and $0 \leq n_3 \leq 1$. This gives $5 \times 3 \times 2$ possibilities. For the record the numbers are

$$1,\ 2,\ 4,\ 8,\ 16,\ 3,\ 6,\ 12,\ 24,\ 48,\ 9,\ 18,\ 36,\ 72,\ 144,\ 7,\ 14,\ 28,\ 56,\ 112,$$

$$21,\ 42,\ 84,\ 168,\ 336,\ 63,\ 126,\ 252,\ 504,\ 1008.$$

Most of the answers I had wrote down all the divisors It was OK to leave the divisors in factorised form $2^{n_1} \times 3^{n_2} \times 7^{n_3}$ *for* n_1, n_2 *and* n_3 *in the given ranges. I had some answers like " a number form* $\{1, 2, 4, 8, 16\}$ *times a number from* $\{1, 3, 9\}$ *times a number from* $\{1, 7\}$*". I found that perfectly clear and acceptable.*

2. a) $5 \times 3 + 7 \times (-2) = 1$. So $5 \times (3n) + 7 \times (-2n) = n$, for any $n \in \mathbb{Z}$.

Simple algebraic notation – just letters for general numbers – is always useful. I had some answers to the general case in words, some of which I found clear and some not. One person also found another form of the answer which was reasonably complete, to the effect that $5 \times 3 + 7 \times (-2) + (7 - 5) \times n = 2n + 1$*, giving any odd number. It is always good to use your initiative.*

b) We have

$$5 \times 2 + 7 \times 2 = 24,\ 5 \times 5 + 7 \times 0 = 25,\ 5 \times 1 + 7 \times 3 = 26,\ 5 \times 4 + 7 \times 1 = 27,\ 5 \times 0 + 7 \times 4 = 28.$$

Every integer $n \geq 24$ can be written in the form $m + 5k$ where m is an integer with $24 \leq m \leq 28$ and $k \in \mathbb{N}$. So then if $5a_1 + 7b_1 = m$ with a_1 and $b_1 \in \mathbb{N}$ we also have $a_1 + k \in \mathbb{N}$ and $5(a_1 + k) + 7b_1 = m + 5k$. *As invited, most solutions solved for* $24 \leq n \leq 28$*. Once again, simple use of algebraic notation is useful for explaining the general case effectively. Explanations in words alone are not always completely successful.*

c) Suppose that $35 = 5a_1 + 7b_1$ for a_1 and $b_1 \in Z_+$. Then $1 \leq a_1 \leq 6$ and $1 \leq b_1 \leq 4$. We also have $5 \times 7 = 35$. So $5(7 - a_1) - 7b_1 = 0$ and $5(7 - a_1) = 7b_1$. Since 5 and 7 are coprime (that is, the gcd is 1), we must have $7 \mid 7 - a_1$. This is impossible because $0 < 7 - a_1 < 7$. Alternatively we can use $5 \mid b_1$, which is also impossible, as $b_1 < 5$.

Most people realised that the obvious way of writing $35 = 5 \times 7$ *does not give a solution with both a and* $b \in \mathbb{Z}_+$*, but there is still some workk to be done to show that it is impossible to have both* $a \in \mathbb{Z}_+$ *and* $b \in \mathbb{Z}_+$*. The proof was expected to use the fact that* 5 *(or* 7*) is prime. If a prime divides a product of integers, it must divide one or other of these integers.*

To see that 40 can be written in the required form: $40 = 5 \times 1 + 7 \times 5$. So we can take $a = 1$ and $b = 5$.

3.

a) $x + 2 \equiv 1 \mod 4 \Leftrightarrow x \equiv 3 \mod 4$. It is also correct to say $x \equiv -1 \mod 4$.

b) $3x \equiv 2 \mod 5 \Leftrightarrow 2 \times 3x \equiv 2 \times 2 \mod 5 \Leftrightarrow x \equiv 4 \mod 5$.

c) $x^2 \equiv 1 \mod 3 \Leftrightarrow x \equiv 1 \mod 3$ or $x \equiv 2 \mod 3$. It is probably simplest to just check each of the three possibilities $x \equiv 0 \mod 3$, $x \equiv 1 \mod 3$ and $x \equiv 2 \mod 3$. Of course, if $x \equiv 0 \mod 3$ then $x^2 \equiv 0 \mod 3$.

d) Once again, until or unless we know more about the theory, the simplest thing is just to check for each of the five values of $x \mod 5$. We have:

$$x \equiv 0 \mod 5 \ \Rightarrow \ x^3 \equiv 0 \mod 5, \quad x \equiv 1 \mod 5 \ \Rightarrow \ x^3 \equiv 1 \mod 5,$$

$$x \equiv 2 \mod 5 \ \Rightarrow \ x^3 \equiv 8 \equiv 3 \mod 5,$$

$$x \equiv 3 \mod 5 \ \Rightarrow \ x^3 \equiv 27 \equiv 2 \mod 5,$$

$$x \equiv 4 \mod 5 \ \Rightarrow \ x^3 \equiv 64 \equiv 4 \mod 5.$$

So

$$x^3 \equiv 1 \mod 5 \ \Leftrightarrow \ x \equiv 1 \mod 5.$$

It is necessary to to check each of the 5 possible values in turn – until we know more theory (which we will do, soon).

e) To find a and b such that $183a + 257b = 1$,

$$\begin{array}{cc|c} 1 & 0 & 257 \\ 0 & 1 & 183 \end{array} \begin{array}{c} R_1 - R_2 \\ \rightarrow \end{array} \begin{array}{cc|c} 1 & -1 & 74 \\ 0 & 1 & 183 \end{array} \begin{array}{c} \rightarrow \\ R_2 - 2R_1 \end{array} \begin{array}{cc|c} 1 & -1 & 74 \\ -2 & 3 & 35 \end{array}$$

$$\begin{array}{c} R_1 - 2R_2 \\ \rightarrow \end{array} \begin{array}{cc|c} 5 & -7 & 4 \\ -2 & 3 & 35 \end{array} \begin{array}{c} \rightarrow \\ R_2 - 8R_1 \end{array} \begin{array}{cc|c} 5 & -7 & 4 \\ -42 & 59 & 3 \end{array} \begin{array}{c} R_1 - R_2 \\ \rightarrow \end{array} \begin{array}{cc|c} 47 & -66 & 1 \\ -42 & 59 & 3 \end{array}$$

So $183 \times (-66) + 257 \times 47 = 1$. This is enough to show that 183 and 257 are coprime. Since $-66 \equiv 191 \mod 257$, we have $183 \times 191 \equiv 1 \mod 257$. Since 183 and 257 are coprime, $x \equiv 191 \mod 257$ is the only solution to $183x \equiv 1 \mod 257$. It is also correct to write $x \equiv -66 \mod 257$ for the solution. *This was mostly well done, although not everyone realised that the final equation $183 \times (-66) + 257 \times 47 = 1$ is equivalent to $x \equiv -66 \mod 257$.*

4. We have

$$\gcd(6n+1, 6n-3) = \gcd(4, 6n-3).$$

Since $4 = 2 \times 2$ and $6n - 3$ is odd and not divisible by 2 we have $\gcd(4, 6n-3) = 1$. For the second part,

$$\gcd(5n+3, 3n+2) = \gcd(2n+1, 3n+2) = \gcd(2n+1, n+1) = \gcd(n, n+1) = \gcd(n, 1) = 1$$

Although the question did not say so, this is really just an application of the Euclidean algorithm: one application in the first part of the question and up to four applications in the second part (as I have written it).The point of the Euclidean algorithm is always to reduce the larger number of the pair to a number which is smaller than the other number in the pair. With the first part of the question is best to stop after just one application, because we know what the divisors of 4 are, and only 1 also divides any odd number. In principle we could continue the Euclidean algorithm in this part of the question but it is a bit awkward, and not necessary.

5. We prove by induction on n that if $p \mid \prod_{j=1}^{n} b_j$then $p \mid b_j$ for some $1 \leq j \leq i$. We are allowed to assume it is true for $n = 2$. Now let $n > 2$ and assume inductively that it is true for $n - 1$ replacing n. Write

$$\prod_{j=1}^{n} b_j = b_1 \times \prod_{j=1}^{-1} b_j \times_n$$

Since p is prime, $\gcd(p, b_n) = 1$ or $p \mid b_n$. If $\gcd(p, b_n) = 1$ then by the key property we have $p \mid \prod_{j=1}^{n-1} b_j$. So then by the inductive hypothesis we have $p \mid b_j$ for some $1 \leq j \leq n-1$. So in all cases $p \mid b_i$ for some $1 \leq i \leq n$.

This is an induction exercise, with base case $n = 2$. This is a step in the proof of the Fundamental Theorem of Arithmetic.