Maths Exercise Sheet 6 Solutions

The solutions are mostly in the form of model answers, with some extra commentary in square brackets. Generally, and especially for questions that ask you to compute something, it is a good idea to write down more of your working than is in the model answers, and then to make it clear what your final answer is.

1. [**Numbers & Induction**]

   (a) $0, 5, 10, 25, 60, 145$ **[2 marks]**

   (b) Base case, $n = 0$:

   $$\begin{aligned}\gcd(a_0, a_1) &= \gcd(0, 5)\\ &= 5\end{aligned}$$

   as required.

   Inductive step: Suppose the statement is true for $n = k$. We will prove it for $n = k + 1$.

   $$\begin{aligned}\gcd(a_{k+1}, a_{k+2}) &= \gcd(a_{k+1}, 2a_{k+1} + a_k) && \text{by definition}\\ &= \gcd(a_{k+1}, 2a_{k+1} + a_k - a_{k+1}) && \text{first given fact}\\ &= \gcd(a_{k+1}, a_{k+1} + a_k)\\ &= \gcd(a_{k+1}, a_{k+1} + a_k - a_{k+1}) && \text{first given fact}\\ &= \gcd(a_{k+1}, a_k)\\ &= \gcd(a_k, a_{k+1}) && \text{second given fact}\\ &= 5 && \text{by induction hypothesis}\end{aligned}$$

   as required.

   [4 marks]

   (c) The possible values are $0, 1, 2$. For the actually possible residues, we can take the first three values of the sequence:

   $$a_0 = 0 \equiv 0 \pmod 4 \qquad a_1 = 5 \equiv 1 \pmod 4 \qquad a_2 = 10 \equiv 2 \pmod 4.$$

   It remains to argue why 3 never arises. The first six values of the sequence $a_n \texttt{ mod } 4$ are

   $$0, 1, 2, 1, 0, 1$$

   Since $a_{n+2} \equiv 2a_{n+1} + a_n \pmod 4$, each term in the sequence of residues is determined by the previous two. Since we started from $0, 1$ and ended up back at $0, 1$, the sequence of residues clearly just repeats the block $0, 1, 2, 1$ over and over. In particular, we never see a 3. **[4 marks]**

2. **[Numbers & Functions]**

(a) $0 \equiv 234 \pmod{234}$, therefore $55 \times 0 \equiv 55 \times 234 \pmod{234}$, which means $f(0) = f(234)$. **[2 marks]**

(b) Since $234 > 55$, we write $r_0 = 234$ and $r_1 = 55$. Then

$$\begin{aligned}234 &= 4 \times 55 + 14\\ 55 &= 3 \times 14 + 13\\ 14 &= 1 \times 13 + 1\\ 13 &= 13 \times 1 + 0\end{aligned}$$

So the r numbers are

$$\begin{aligned}r_0 &= 234\\ r_1 &= 55\\ r_2 &= 14\\ r_3 &= 13\\ r_4 &= 1\\ r_5 &= 0\end{aligned}$$

The algorithm outputs the last non-zero r_n, which is $r_4 = 1$. So $\gcd(234, 55) = 1$. **[4 marks]**

(c) Yes. We have just seen that 234 and 55 are coprime, which means that 55 has a reciprocal (mod 234), i.e. that there exists a number $c \in \mathbb{Z}$ with $55c \equiv 1 \pmod{234}$. So for any $i \in \{0, 1, \ldots, 233\}$,

$$\begin{aligned}f(ci) &\equiv 55ci \pmod{234}\\ &\equiv 1i \pmod{234}\\ &\equiv i \pmod{234}.\end{aligned}$$

But since $f(ci)$ is already in the range $0 \leq f(ci) < 234$, we have $f(ci) = i$.

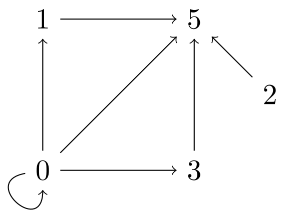
[We do not strictly need to compute a number c to answer this question, but for extra assurance we can do so by finding Bézout coefficients:

$$\begin{aligned}1 &= 14 - 13\\ &= 14 - (55 - 3 \times 14)\\ &= 4 \times 14 - 55\\ &= 4 \times (234 - 4 \times 55) - 55\\ &= 4 \times 234 - 17 \times 55\end{aligned}$$

from which we see that $c = -17$ is an example. Or, if you prefer a positive number, $c = 217$.] **[4 marks]**

3. **[Relations & Sets]**

Our working will be clearer if we first draw a diagram of R.



(a) No. Not every node in the diagram has a loop. For example $(1, 1) \notin R$ (or $\neg(1\ R\ 1)$). **[1 mark]**

(b) No. Not every edge in the diagram has a backward companion (there are edges "$\rightarrow$" that are not part of a "$\leftrightarrows$"). For example, $(0, 1) \in R$, but $(1, 0) \notin R$. **[1 mark]**

(c) Yes. The diagram has no back-and-forth edges "$\leftrightarrows$" (loops don't count). The only time we have $(a, b), (b, a) \in R$ is when $a = b = 0$. So R does satisfy $x\ R\ y \wedge y\ R\ x \implies x = y$. **[2 marks]**

(d) Yes. The only length 2 paths to check are $0\ R\ 1\ R\ 5$ and $0\ R\ 3\ R\ 5$, but the 'shortcut' for both, $0\ R\ 5$, is already in the relation.
[Arguably, we should also check length 2 paths like $0\ R\ 0\ R\ 1$, but there is no need to consider such because they cannot lead to counterexamples to transitivity, because the 'shortcut' $0\ R\ 1$ is already included in the path. So there would be no penalty for not mentioning them here.] **[3 marks]**

(e) Uncountable. Let us inject $P(\mathbb{N})$ into it the set with:

$$\begin{aligned} P(\mathbb{N}) &\to \{A \in P(\mathbb{N} \times \mathbb{N}) \mid R \subseteq A\} \\ S &\mapsto R \cup \{(6, n) \mid n \in S\}. \end{aligned}$$

This is an injection because the '6' in the first component of the pair mean that none of the pairs arising from S clash with those in R, so we can recover S from its image ("different S's are mapped to different relations").
[There are lots of ways to do this question. Another is to inject $P(\mathbb{N} \times \mathbb{N})$ into it, e.g.:

$$\begin{aligned} P(\mathbb{N} \times \mathbb{N}) &\to \{A \in P(\mathbb{N} \times \mathbb{N}) \mid R \subseteq A\} \\ S &\mapsto R \cup \{(m + 6, n + 6) \mid (m, n) \in S\}. \end{aligned}$$

This relies on $P(\mathbb{N} \times \mathbb{N})$ being uncountable, which it is because it is a powerset of an infinite set. It would generally be fine to rely on this fact unless the question is specifically asking for a proof.]

4. [**Numbers & Induction**]

(a) We use ('strong') induction. We want to prove the statement for $n \in \mathbb{N}$, so we will assume the statement is true for all $k < n$. We case-split on whether $n = 0$, or $n = 2k+1$, or $n = 2k+2$.

- If $n = 0$, then $b_0 = 10 \equiv 1 \pmod 3$, as required (no induction hypothesis required).
- If $n = 2k+1$, then $b_n = 3b_k + 1 \equiv 1 \pmod 3$, (no induction hypothesis required).
- If $n = 2k+2$, then $b_n = b_{k+1}$, where $k+1 < 2k+2 = n$. So by induction hypothesis, $b_n = b_k \equiv 1 \pmod 3$.

[5 marks]

(b) The possible values are $S = \{0, 1, 3, 4\}$. First, all these values are possible, because

$$\begin{aligned} b_0 &= 10 \\ &\equiv 0 \pmod 5 \\ b_1 &= 31 \\ &\equiv 1 \pmod 5 \\ b_3 &= 94 \\ &\equiv 4 \pmod 5 \\ b_7 &= 3 \times 94 + 1 \\ &\equiv 3 \times 4 + 1 \pmod 5 \\ &\equiv 3 \pmod 5 \end{aligned}$$

Now we show by (strong) induction that $b_n \mathbin{\texttt{mod}} 5 \in S$ for all $n \in \mathbb{N}$. Suppose the statement is true for all $k < n$.

- If $n = 0$, then $b_0 = 10$ so $b_0 \mathbin{\texttt{mod}} 5 = 0 \in S$, as required (no induction hypothesis required).
- If $n = 2k+1$, then $b_n \equiv 3b_k + 1 \pmod 5$, where $k < n$. So, by induction hypothesis, $b_k \in S$. But if $m \in S$ then $(3m+1) \mathbin{\texttt{mod}} 5 \in S$:

  $$\begin{aligned} 3 \times 0 + 1 &= 1 \\ 3 \times 1 + 1 &= 4 \\ 3 \times 3 + 1 &\equiv 0 \pmod 5 \\ 3 \times 4 + 1 &\equiv 3 \pmod 5. \end{aligned}$$

  So it follows that $b_n \mathbin{\texttt{mod}} 5 \in S$.
- If $n = 2k+2$, then $b_n = b_{k+1}$. By induction hypothesis, $b_k \in S$, so also $b_n \in S$.

Since $b_n \in S$ for all $n \in \mathbb{N}$, this means we never have $b_n \mathbin{\texttt{mod}} 5 = 2$.

[5 marks]

5. **[Real Numbers & Functions]**

(a) $(\frac{\sqrt{5}}{3})^2 = \frac{5}{9}$, and $0^2 = 0 < \frac{5}{9} < 1 = 1^2$. **[2 marks]**

(b) We will set out our working in a table. Let $a_0 = 0$, $b_0 = 1$, and continue by interval bisection following the method and notation from lectures/notes.

n	a_n	b_n	c_n	c_n^2	c_n^2 vs $\frac{5}{9}$
0	0	1	$\frac{1}{2}$	$\frac{1}{4}$	$<$
1	$\frac{1}{2}$	1	$\frac{3}{4}$	$\frac{9}{16}$	$>$
2	$\frac{1}{2}$	$\frac{3}{4}$			

For the final column we have checked:

- $\frac{1}{4} = \frac{9}{36}$ and $\frac{5}{9} = \frac{20}{36}$, so $<$.
- $\frac{9}{16} = \frac{81}{144}$ and $\frac{5}{9} = \frac{80}{144}$, so $>$.

So $\frac{1}{2} < \frac{\sqrt{5}}{3} < \frac{3}{4}$. Since $\frac{1}{2} = \frac{2}{4}$, the answer is $m = 2$.

[Potentially, you could use a calculator to find $\frac{\sqrt{5}}{3} \approx 0.7453559925$, which puts it between $\frac{1}{2}$ and $\frac{3}{4}$. This is not a sufficient answer. As the question did not specify any particular method other than asking for proof, it would be acceptable to find the answer with a calculator and then subsequently prove $\frac{1}{2} < \frac{\sqrt{5}}{3} < \frac{3}{4}$ with a calculation:

$$\left(\frac{1}{2}\right)^2 = \frac{1}{4} = \frac{9}{36} < \frac{20}{36} = \frac{5}{9} = \left(\frac{\sqrt{5}}{3}\right)^2$$

$$\left(\frac{3}{4}\right)^2 = \frac{9}{16} = \frac{81}{144} > \frac{80}{144} = \frac{5}{9} = \left(\frac{\sqrt{5}}{3}\right)^2 .]$$

[3 marks]

(c) If x is in either $\mathbb{Q}$ or $\mathbb{R}$, then $x\sqrt{5} \in \mathbb{R}$, so we do get functions $\mathbb{Q} \to \mathbb{R}$ and $\mathbb{R} \to \mathbb{R}$. If $x \in \mathbb{Q}$, then $x\sqrt{5} \in \mathbb{R}$ but it is not necessarily in $\mathbb{Q}$. For example, when $x = 1$, we get $\sqrt{5}$, which is irrational.

[There is no need to prove that $\sqrt{5}$ is irrational unless directly asked. It is virtually the same proof as for $\sqrt{2}$.]

[2 marks]

(d) It is injective for both. If $x\sqrt{5} = y\sqrt{5}$, where $x, y \in \mathbb{R}$, then because $\sqrt{5}$ is non-zero we can divide by it to get $x = y$. This also goes for the special case $x, y \in \mathbb{Q}$.

For $\mathbb{R} \to \mathbb{R}$, it is also surjective. To see that any $y \in \mathbb{R}$ is in the image, note that $\frac{y}{\sqrt{5}} \in \mathbb{R}$ and $\frac{y}{\sqrt{5}} \mapsto \sqrt{5} \times \frac{y}{\sqrt{5}} = y$.

For $\mathbb{Q} \to \mathbb{R}$, it is not surjective. For example, 1 is not in the image, because to have $x \mapsto 1$ we would need $x = \frac{1}{\sqrt{5}}$, but this is not in $\mathbb{Q}$. **[3 marks]**

6. **[Numbers]**

(a) Since $54 > 35$, we write $r_0 = 54$ and $r_1 = 35$. Then

$$\begin{aligned}54 &= 35 + 19\\ 35 &= 19 + 16\\ 19 &= 16 + 3\\ 16 &= 5 \times 3 + 1\\ 3 &= 3 \times 1 + 0\end{aligned}$$

So the r numbers are

$$\begin{aligned}r_0 &= 54\\ r_1 &= 35\\ r_2 &= 16\\ r_3 &= 3\\ r_4 &= 1\\ r_5 &= 0\end{aligned}$$

The algorithm outputs the last non-zero r_n, which is $r_4 = 1$. So $\gcd(35, 54) = 1$.

[4 marks]

(b) We'll find Bézout coefficients.

$$\begin{aligned}1 &= 16 - 5 \times 3\\ &= 16 - 5 \times (19 - 16)\\ &= 6 \times 16 - 5 \times 19\\ &= 6 \times (35 - 19) - 5 \times 19\\ &= 6 \times 35 - 11 \times 19\\ &= 6 \times 35 - 11 \times (54 - 35)\\ &= 17 \times 35 - 11 \times 54\end{aligned}$$

Following the usual pattern, we set

$$N = 3 \times 17 \times 35 - 2 \times 11 \times 54 = 597.$$

So 597 is one possible value of x.

[Reminder: the pattern for solving this sort of problem is that you take the residue you want modulo 54, which is 3, and put it in front of the *other* modulus, 35. Similarly, the residue you want modulo 35, which is 2, you put in front of the other modulus, 54.]

[It's a good idea, but not necessary for the marks if the above working was followed correctly, to check that 597 does work.] **[4 marks]**

(c) Since 35 and 54 are coprime, the solutions repeat every $35 \times 54 = 1890$. So the full set of solutions is

$$\{597 + 1890k \mid k \in \mathbb{Z}\}.$$

[You don't need to repeat the justification for this to get the marks if you wrote down the correct set above, but as reminder: if x is another solution to the simultaneous congruences, then

- $x - 597 \equiv 0 \pmod{35}$, and
- $x - 597 \equiv 0 \pmod{54}$.

So $35 \mid (x - 597)$ and $54 \mid (x - 597)$. Since 35 and 54 are coprime, their product also divides $x - 597$. So $x - 597 = 1890k$ for some $k \in \mathbb{Z}$, (and any such x is a solution), as required.]

[2 marks]