# Maths Exercise Sheet 4 Solutions
# Reals (and revision)

---

You do not have to answer all questions, but try to answer as many as you can.
Questions marked with one or more asterisks go beyond the scope of the course in difficulty or topic.

1. Which of the following functions are injective/surjective/bijective?

   (a) $n \mapsto -n : \mathbb{Z} \to \mathbb{Z}$.
   Bijective.

   (b) $x \mapsto x^2 : [0, \infty) \cap \mathbb{Q} \to [0, \infty) \cap \mathbb{Q}$.
   Injective because if $x^2 = y^2$ then $x = \pm y$, so $x = y$ if $x, y \geq 0$. Not surjective because, e.g., 2 is not the square of any rational number.

   (c) $x \mapsto x^2 : [0, \infty) \to [0, \infty)$.
   Bijective.

   (d) $x \mapsto \frac{1}{x} : (0, \infty) \to \mathbb{R}$.
   Injective but not surjective: the image is only $(0, \infty)$.

   (e) $x \mapsto x^7 - x : \mathbb{R} \to \mathbb{R}$.
   Not injective because, e.g., both 0 and 1 are mapped to 0. It is surjective because it is a polynomial of odd degree.

   *(f) $x \mapsto \log(|x|) : \mathbb{R} \backslash \{0\} \to \mathbb{R}$.
   It doesn't matter what base you take for the logarithm here (different logarithms only differ by a constant factor). Not injective since, for any $x \in \mathbb{R} \backslash \{0\}$, $x$ and $-x$ have the same image. It is surjective: it is surjective even when restricted to $(0, \infty)$ e.g. because log is the inverse to a (bijective) function $\exp : \mathbb{R} \to (0, \infty)$.

   *(g) $x \mapsto \sin x : [-t, t] \to [-1, 1]$
   (determine for each $t \in [0, \infty)$)
   It is injective for $t \leq \frac{\pi}{2}$, surjective for $t \geq \frac{\pi}{2}$, and so bijective for $t = \frac{\pi}{2}$.

2. Consider the following functions $f, g : \mathbb{R} \to \mathbb{R}$ given by

$$f(x) = 2x + 1 \qquad\qquad g(x) = x^2 - 2.$$

   Compute formulas for the composites $f \circ g$ and $g \circ f$.

$$(f \circ g)(x) = 2x^2 - 3 \qquad\qquad (g \circ f)(x) = 4x^2 + 4x - 1$$

3. Define two sequences $(p_n)$, $(q_n)$ of natural numbers by

$$p_0 = 1 \qquad q_0 = 0 \qquad p_{n+1} = p_n + 2q_n \qquad q_{n+1} = p_n + q_n$$

(a) Prove by induction that $p_n^2 - 2q_n^2 = (-1)^n$.
Base case:

$$\begin{aligned} p_0^2 - 2q_0 &= 1^2 - 2 \times 0^2 \\ &= 1 \\ &= (-1)^0. \end{aligned}$$

For the inductive step, suppose $p_k^2 - 2q_k^2 = (-1)^k$. We calculate:

$$\begin{aligned} p_{k+1}^2 - 2q_{k+1}^2 &= (p_k + 2q_k)^2 - 2(p_k + q_k)^2 \\ &= (p_k^2 + 4p_kq_k + 4q_k^2) - 2(p_k^2 + 2p_kq_k + q_k^2) \\ &= 2q_k^2 - p_k^2 \\ &= -(-1)^k \\ &= (-1)^{k+1} \end{aligned}$$

as required.

(b) Deduce that $|\sqrt{2} - \frac{p_n}{q_n}| < \frac{1}{2q_n^2}$ for $n > 0$.
By an easy induction, both $p_n \geq q_n > 0$ for $n > 0$. In particular, when $n > 0$, $q_n > 0$ so we can divide by it in what follows. We have

$$(p_n^2 - 2q_n^2) = (p_n - \sqrt{2}q_n)(p_n + \sqrt{2}q_n)$$

hence

$$(\tfrac{p_n}{q_n} - \sqrt{2})(p_n + \sqrt{2}q_n) = \frac{(-1)^n}{q_n}$$

whence

$$\left|\sqrt{2} - \frac{p_n}{q_n}\right| \leq \frac{1}{q_n(p_n + \sqrt{2}q_n)} < \frac{1}{2q_n^2}$$

The numbers of the sequence $(q_n)$ are called the *Pell numbers* (`https://oeis.org/A000129`) and the equation $x^2 - 2y^2 = 1$ a special case of *Pell's equation*. The sequence of fractions $\frac{p_n}{q_n}$ is an ancient method of approximating $\sqrt{2}$. Since $q_{n+1} \geq 2q_n$, the above shows that the guaranteed precision of the approximations quadruples or better with each step, which is twice the rate of the interval bisection method.

4. Find $n \in \mathbb{N}$ such that $|\frac{n}{8} - \sqrt{5}| < \frac{1}{16}$. Now write down the first 6 binary digits of $\sqrt{5}$.
[You should not use the square root function on a calculator.]

We build up iteratively.

- For a denominator of $2^0$, we evidently have $2 < \sqrt{5} < 3$, because $4 < 5 < 9$.
- The midpoint is $\frac{5}{2}$, where $(\frac{5}{2})^2 = \frac{25}{4} > 5$, so $2 < \sqrt{5} < \frac{5}{2}$.
- The midpoint is $\frac{9}{4}$, where $(\frac{9}{4})^2 = \frac{81}{16} > 5$, so $2 < \sqrt{5} < \frac{9}{4}$.
- The midpoint is $\frac{17}{8}$, where $(\frac{17}{8})^2 = \frac{289}{64} < 5$, so $\frac{17}{8} < \sqrt{5} < \frac{9}{4}$.

It remains to decide which of $\frac{17}{8}$ and $\frac{9}{4} = \frac{18}{8}$ that $\sqrt{5}$ is closer to. The midpoint is $\frac{35}{16}$ where $(\frac{35}{16})^2 = \frac{1225}{256} < 5$. So the closer number is $\frac{9}{4} = \frac{18}{8}$.

So the final answer is $\underline{n = 18}$.

For the second part, we computed that $\frac{35}{16}$ was the largest fraction with denominator 16 below $\sqrt{5}$. Since $35 = 100011_2$, we can deduce that the binary expansion begins $\sqrt{5} = 10.0011\ldots_2$. (Be careful to put the binary point in the right place).

5. Let $X$ be a set and let $R \subseteq X \times X$ be a relation on $X$. Suppose that $R$ is symmetric and transitive. Consider the subset $D \subseteq X$ given by

$$D = \{x \in X \mid x \; R \; x\}.$$

   (a) Show that $R \subseteq D \times D$.

   Suppose $x \; R \; y$. We have to show that $x, y \in D$. But $R$ is symmetric, so we have $y \; R \; x$. $R$ is transitive, and $x \; R \; y$ and $y \; R \; x$, therefore $x \; R \; x$. Similarly $y \; R \; y$.

   (b) As a relation on $D$, show that $R$ is an equivalence relation. $R$ is reflexive, since if $x \in D$, then by definition $(x, x) \in R$. $R$ is symmetric: if $x, y \in D$ then also $x, y \in X$, so $x \; R \; y$ implies $y \; R \; x$. Transitivity is similarly inherited.

   A relation $R$ satisfying symmetry and transitivity is called a *partial equivalence relation*. Given a partial equivalence relation $R$ on a set $X$, we can define the quotient $X/R$ to be the set of equivalence classes of the relation $R$ consider as an equivalence relation on the subset $D$ as above of 'reflexive elements'. This sometimes has notational advantages. For example, we could define $\mathbb{Q}$ as the quotient of $\mathbb{Z}^2$ by a certain *partial* equivalence relations.

* 6. Show that the set

$$A = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

   is closed under $+, -, \times, \div$ in $\mathbb{R}$.
   ['Closed under an operation $\odot$' means that, whenever $x, y \in A$ then also $x \odot y \in A$.]

   Addition:

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$$

   where $(a + b), (b + d) \in \mathbb{Q}$ provided $a, b, c, d \in \mathbb{Q}$, as required.

   For subtraction, it suffices to observe that the negative of $a + b\sqrt{2} \in A$ is $(-a) + (-b)\sqrt{2} \in A$.

   Multiplication:

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$$

   as required.

   For division, we have to check that the reciprocal of non-zero $a + b\sqrt{2} \in A$ is also in $A$. But

$$(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$$

   is not 0 unless $a = b = 0$. So if $a + b\sqrt{2} \in A$ is non-zero then $\frac{a}{a^2-2b^2} + \frac{b}{a^2-2b^2}\sqrt{2} \in A$ is its reciprocal.

** 7. A compression algorithm is *lossless* if the original data can be exactly reconstructed. A new lossless compression algorithm promises that no compressed file is larger than the original. Prove that in this case the 'compression' algorithm actually leaves every file exactly the same size. [You may model a 'file' as a vector $v \in \{0, 1\}^N$ where $N \in \mathbb{N}$ is considered to be the *size* of the file.]

   The behaviour of a compression algorithm is a function $f : \{v : v \text{ a file}\} \to \{v : v \text{ a file}\}$. It is *lossless* iff $f$ is an injection. Assuming $f$ never makes a file larger, we show by induction on $n$ that $f$ restricts to a bijection $\{\text{files of size} \leq n\} \to \{\text{files of size} \leq n\}$.

   Base case: There is one file of size 0, the empty file. It cannot be made smaller than empty, and it is not made larger, so $f$ must send the empty file to itself.

   Inductive step: Suppose $f$ restricts to a bijection $\{\text{files of size} \leq k\} \to \{\text{files of size} \leq k\}$. Since $f$ is both lossless and does not increase file size, it restricts to an *injection*

$$\{\text{files of size} \leq k + 1\} \to \{\text{files of size} \leq k + 1\}$$

which further restricts to a *bijection*

$$\{\text{files of size} \leq k\} \to \{\text{files of size} \leq k\}.$$

By injectivity, no file of size $k+1$ can be mapped to a file of size of $\leq k$, since those files are already in the image of some files of size $\leq k$. Thus $f$ restricts to an injection

$$\{\text{files of size } k+1\} \to \{\text{files of size } k+1\}.$$

But an injection from a finite set to itself must be a bijection. Thus $f$ must have been a bijection $\{\text{files of size} \leq k+1\} \to \{\text{files of size} \leq k+1\}$.

*** 8. Let $p$ be a prime number greater than 2. Show that

$$|\{x^2 \mid x \in \mathbb{Z}_p\}| = \frac{1}{2}(p+1).$$

The possible values of $x^2 \bmod p$ for $x \in \mathbb{Z}$ are called *quadratic residues*.

Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be given by $f(x) = x^2$. For $x, y \in \mathbb{Z}_p$, $f(x) = f(y)$ iff $p \mid (x-y)(x+y)$, i.e. iff $x = \pm y$ (this is where we use primality). Hence, for each $z \in \mathbb{Z}_p$, there are three possibilities for $f^{-1}(\{z\})$.

- If $z = 0$ then $f^{-1}(\{0\}) = \{0\}$ is a singleton.
- If $z \neq 0$, then either
  - $f^{-1}(\{z\}) = \emptyset$, or
  - $f^{-1}(\{z\})$ has precisely two elements. This step would break for $p = 2$, because in $\mathbb{Z}_2$ we have $1 = -1$, so $f^{-1}(\{1\})$ would have only one element.

Hence,

$$\begin{aligned} |\mathbb{Z}_p| &= 1 + 2|\{x^2 \mid x \in \mathbb{Z}_p, x \neq 0\}| \\ &= 2|\{x^2 \mid x \in \mathbb{Z}_p\}| - 1. \end{aligned}$$

But $|\mathbb{Z}_p| = p$, so rearranging we get $|\{x^2 \mid x \in \mathbb{Z}_p\}| = \frac{1}{2}(p+1)$.