# MAS114: Solutions to Exercises

Up to week 11

Note that the challenge problems are intended to be difficult! Doing any of them is an achievement. Please hand them in on a separate piece of paper if you attempt them.

## Sets, functions, logic

1. Learn the Greek alphabet: learn the names of all the lower-case letters

$$\alpha, \beta, \gamma, \delta, \epsilon, \zeta, \eta, \theta, \iota, \kappa, \lambda, \mu, \nu, \xi, o, \pi, \rho, \sigma, \tau, \upsilon, \phi, \chi, \psi, \omega.$$

*(They're among the commonest of the unfamiliar symbols that mathematicians use. If you're Greek or Cypriot, you have an advantage, but you should still get used to the way their names are pronounced in English.)*

**Solution** You're on your own with this one (but millions of primary school children in two countries have done it, so it can't be very difficult).

2. Which of the following rules define a function? For those that are functions, are they injective? Are they surjective? Are they bijective? Give brief explanations where necessary.

   (i) $f : \mathbb{N} \to \mathbb{R}$ defined by $f(n) = \sqrt{n}$;

   (ii) $g : \mathbb{Z} \to \mathbb{R}$ defined by $g(n) = \sqrt{n}$;

   (iii) $h : \mathbb{Z} \to \mathbb{N}$ defined by $h(n) = |n|$;

   (iv) $i : \mathbb{N} \to \mathbb{N}$ defined by taking $i(n) = 100 - n$.

   (v) $j : \mathbb{Z} \to \mathbb{Z}$ defined by $j(n) = -n$;

   (vi) $k : \mathbb{R} \to \mathbb{Z}$ defined by taking $k(x)$ to be the closest integer to $x$.

   **Solution**

   (i) This is a function, as every natural number has a real square root. It's injective, because every natural has a different square root. It's not surjective, for example because $1/2$ is not the square root of a natural number. Hence it's also not bijective.

   (ii) This is not a function, because $-1$ does not have a real square root.

(iii) This is a function: every integer has an absolute value which is a natural number. It's not injective, because $h(-1) = h(1) = 1$. But is surjective, since for every $n \in \mathbb{N}$, we have $h(n) = n$. It can't be bijective, as it isn't injective.

(iv) This is not a function: we have $i(101) = -1 \notin \mathbb{N}$.

(v) This is a function: every integer can be negated to give another integer. It's injective, since no two different integers have equal negations. It's surjective, since for any $n \in \mathbb{Z}$ we have $j(-n) = n$. Hence it's bijective too!

(vi) This is "almost" a function, but in fact it isn't. For example, there is no integer closest to $1/2$, as 0 and 1 are equally close.

3. (i) Write down an injective function from $\{1, \ldots, 10\}$ to $\{1, \ldots, 100\}$.

(ii) Write down a surjective function from $\{1, \ldots, 100\}$ to $\{1, \ldots, 10\}$.

(iii) Is there an injection from $\{1, \ldots, 100\}$ to $\{1, \ldots, 10\}$, or a surjection from $\{1, \ldots, 10\}$ to $\{1, \ldots, 100\}$?

**Solution**

(i) $f(n) = n$ will do (there are many others)!

(ii) One possibility is to take $g(n) = \lceil n/10 \rceil$ (that is, the smallest integer greater than or equal to $n/10$), so that

$$\begin{aligned} g(1) = g(2) = \cdots = g(10) = 1, \\ g(11) = g(12) = \cdots = g(20) = 2, \\ \ldots g(91) = g(92) = \cdots = g(100) = 10. \end{aligned}$$

There are many ways to describe this function, and many other functions which work.

(iii) No. For there to be an injection from $\{1, \ldots, 100\}$ to $\{1, \ldots, 10\}$, there would have to be 100 different objects in the codomain; for there to be a surjection from $\{1, \ldots, 10\}$ to $\{1, \ldots, 100\}$ there would have to be at most 10 elements in the codomain.

4. **(Challenge 1)** How many subsets are there of $\{1, 2, 3, \ldots, 19, 20\}$ which contain no two consecutive elements? (For example, $\{1, 4, 18\}$ is okay, but $\{1, 4, 17, 18\}$ is not okay since it contains the consecutives 17 and 18.)

5. Write down all the elements of each of the following sets:

(a) $\{a \in \mathbb{N} \mid a^2 < 9\}$;

(b) $\{a \in \mathbb{N} \mid a^2 \leq 9\}$;

(c) $\{a \in \mathbb{Z} \mid a^2 < 9\}$;

(d) $\{a \in \mathbb{Z} \mid a^2 \leq 9\}$.

**Solution** The sets are:

(a) $\{0, 1, 2\}$;

(b) $\{0, 1, 2, 3\}$;

(c) $\{-2, -1, 0, 1, 2\}$;

(d) $\{-3, -2, -1, 0, 1, 2, 3\}$.

6. Consider the following sets:

- $\{1, 2, 4\}$,
- $\{2, 3, 5\}$,
- $\{1, 2, 3, 4, 5\}$,
- $\{2\}$,
- $\{3, 4\}$.

1. Choose three different sets $X$, $Y$ and $Z$ from the above such that $X \cup Y = Z$.
2. Choose three different sets $X$, $Y$ and $Z$ from the above such that $X \cap Y = Z$.
3. Choose two different sets $X$, $Y$ from the above such that $X \cap Y = \emptyset$.

**Solution**

1. We have $\{1, 2, 4\} \cup \{2, 3, 5\} = \{1, 2, 3, 4, 5\}$.
2. We have $\{1, 2, 4\} \cap \{2, 3, 4\} = \{2\}$.
3. We have $\{2\} \cap \{3, 4\} = \emptyset$.

7. Suppose $U$ is a set. If $X$ is a subset of $U$, we'll write $\overline{X}$ for $U \backslash X$ for the duration of this question. *(This is common notation whenever we work at length with subsets of some particular set.)*

   Let $A$ and $B$ be subsets of $U$. Show that:

   (i) $\overline{A \cup B} = \overline{A} \cap \overline{B}$

   (ii) $\overline{A \cap B} = \overline{A} \cup \overline{B}$

   *(These are called De Morgan's laws. Remember, from lectures: the best way to prove two sets are equal is often to prove that each is contained in the other. So for each of these two you have two containments to prove: the left-hand side in the right-hand side, and vice versa.)*

**Solution**

(i) We'll show that each set is contained in the other, showing first that $\overline{A \cup B} \subset \overline{A} \cap \overline{B}$. Indeed, if $x \in \overline{A \cup B}$, then $x \in U$ and $x \notin A \cup B$. But that means that $x \notin A$ and $x \notin B$, or, equivalently, that $x \in \overline{A}$ and $x \in \overline{B}$. Hence $x \in \overline{A} \cap \overline{B}$, as required.

Now we'll show the converse containment, namely that $\overline{A} \cap \overline{B} \subset \overline{A \cup B}$. The argument above is reversible: if $x \in \overline{A} \cap \overline{B}$, then $x \in \overline{A}$ and $x \in \overline{B}$, and hence $x \notin A$ and $x \notin B$. This gives us that $x \notin A \cup B$, or equivalently that $x \in \overline{A \cup B}$.

These two containments show that the two sets are equal.

(ii) As before, we'll show that each set is contained in the other. We'll show first that $\overline{A \cap B} \subset \overline{A} \cup \overline{B}$. But, if $x \in \overline{A \cap B}$, then $x \in U$ and $x \notin A \cap B$. As a result, we have $x \notin A$ or $x \notin B$.

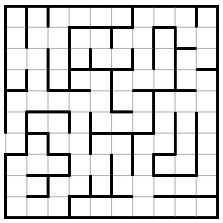
If $x \notin A$, then $x \in \overline{A}$ and hence $x \in \overline{A} \cup \overline{B}$. But if $x \notin B$, then $x \in \overline{B}$ and hence $x \in \overline{A} \cup \overline{B}$ all the same. This proves the first containment.

Now we'll show the other one: that $\overline{A} \cup \overline{B} \subset \overline{A \cap B}$. However, if $x \in \overline{A} \cup \overline{B}$, then $x \in U$, and $x \in \overline{A}$ or $x \in \overline{B}$.

If the former is true, $x \in \overline{A}$, then $x \notin A$ and so $x \notin A \cap B$, and so $x \in \overline{A \cap B}$. If the latter is true, then $x \notin B$ and so $x \notin A \cap B$ and so $x \in \overline{A \cap B}$ all the same.

This completes the proof.

8. **(Challenge 2)** I foolishly left my dog in a maze, and I'm not allowed in to retrieve him. The maze is a 10 m × 10 m grid, where some of the grid edges are walls and some aren't. I can't remember anything about where the walls are, but this picture shows an example of a similar maze.



My dog is very obedient, but not very clever. He understands the instructions "walk 1 m forwards", "turn 90° left", and "turn 90° right" but nothing else of any use. If I shout for him to walk forwards and that would result in him walking into a wall, he'll just do nothing for that order and wait patiently for the next one, wagging his tail.

I can't see into the maze, and have no idea whether my orders for him to walk forward are succeeding or not.

Is there a sequence of orders I could shout that would get him out of the maze, no matter what the maze looks like and no matter which square I left him at, and no matter which direction I left him facing?

9. An *even number* is an integer that can be written in the form $2k$ for some integer $k$. An *odd number* is one that can be written in the form $2k+1$ for some integer $k$. Using these definitions *and no other facts you may happen to know about odd or even numbers*, prove the following implications for integers $m$ and $n$:

   1. If $n$ is even, then $n^2$ is even.
   2. If $n$ and $m$ are odd, then $n + m$ is even.
   3. If $n$ and $m$ are odd, then $nm$ is odd.

   State the converse of each of the above implications. Do you think they are true or false?

**Solution** For the first part:

1. If $n$ is even, then $n = 2k$ for some integer $k$. That means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$, which is of the form $2l$. Hence $n^2$ is even.
2. If $n$ and $m$ are odd, then we can write $n = 2k + 1$ and $m = 2l + 1$ for some integers $k$ and $l$. That means that $n+m = (2k+1)+(2l+1) = 2k + 2l + 2 = 2(k + l + 1)$. This is of the form $2a$, so $n + m$ is even.
3. Again, if $n$ and $m$ are odd, then we can write $n = 2k+1$ and $m = 2l+1$ for some integers $k$ and $l$. That means that $nm = (2k + 1)(2l + 1) = 4kl + 2k + 2l + 1 = 2(2kl + k + l) + 1$. That means that $nm$ is odd.

For the converses:

1. The converse is "if $n^2$ is even, then $n$ is even", which is true.

2. The converse is "if $n+m$ is even, then $n$ and $m$ are odd". That need not be true, since we could have $n = 4$ and $m = 6$ (for example).
3. The converse is "if $nm$ is odd, then $n$ and $m$ are odd". That's true.

10. Which of these statements is true?

    1. $\forall x \in \mathbb{R}, (x^2 - 7x + 10 = 0) \Rightarrow (x = 2 \wedge x = 5)$
    2. $\forall x \in \mathbb{R}, (x^2 - 7x + 10 = 0) \Rightarrow (x = 2 \vee x = 5)$

    **Solution** It's the second one. It's not possible for $x$ to equal two and for $x$ to equal five.

    *(Nevertheless, students are fond of writing "$x = 2$ and $x = 5$" when they solve a quadratic equation, rather than the correct "$x = 2$ or $x = 5$".)*

11. Can you translate the following statements into English? Which are true and which are false?

    1. $\forall a, b, c \in \mathbb{R}, \exists x \in \mathbb{R} \quad \text{s.t.} \quad ax^2 + bx + c = 0.$
    2. $\forall a, b, c \in \mathbb{C}, \exists x \in \mathbb{C} \quad \text{s.t.} \quad ax^2 + bx + c = 0.$
    3. $\forall a, b, c \in \mathbb{R}, \exists x \in \mathbb{R} \quad \text{s.t.} \quad b^2 - 4ac \geq 0 \Rightarrow ax^2 + bx + c = 0.$

    **Solution**

    1. "Every quadratic equation with real coefficients has a real solution": this is false (because of equations with negative discriminant);
    2. "Every quadratic equation with complex coefficients has a complex solution": this is true;
    3. "Every quadratic equation with real coefficients and nonnegative discriminant has a real solution": this is true.

# Induction

12. Prove by induction that

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6},$$

    for all positive integers $n$.

    **Solution** This proof is by induction on $n$, as requested.

    For our base case, we show it's true for $n = 0$. In this case, the left-hand side is the sum of no integers, and is hence zero. The right-hand side is also zero, and so they're equal. (We could also have started from $n = 1$; and then both sides turn out to be 1.)

    Now we do the induction step: we assume that it's true for $n = k$, and we try deducing that it's true for $n = k + 1$.

In other words, we assume that

$$1^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{,}$$

and we try to prove that

$$1^2 + \cdots + (k+1)^2 = \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}.$$

But this is not too hard, since we have both

$$\begin{aligned}
&1 + \cdots + k^2 + (k+1)^2 \\
=&\left(1 + \cdots + k^2\right) + (k+1)^2 \\
=&\frac{k(k+1)(2k+1)}{6} + (k+1)^2 \quad \text{(by the induction step)} \\
=&\frac{k(k+1)(2k+1) + 6(k+1)^2}{6} \\
=&\frac{(2k^3 + 3k^2 + k) + (6k^2 + 12k + 6)}{6} \\
=&\frac{2k^3 + 9k^2 + 13k + 6}{6}
\end{aligned}$$

and also

$$\begin{aligned}
&\frac{(k+1)((k+1)+1)(2(k+1)+1)}{6} \\
=&\frac{(k+1)(k+2)(2k+3)}{6} \\
=&\frac{2k^3 + 9k^2 + 13k + 6}{6}.
\end{aligned}$$

Hence the two are equal, as required. This completes the induction proof.

13. **(Challenge 3)** Suppose that we have some positive integers (not necessarily distinct) whose sum is 100. How large can their product be? You should prove your answer is best.

14. Prove that for all natural numbers $n \geq 2$, we have

$$\left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right)\cdots\left(1 - \frac{1}{n^2}\right) = \frac{n+1}{2n}.$$

**Solution** Let's prove it by induction on $n$. Our base case is where $n = 2$, where we must prove

$$\left(1 - \frac{1}{2^2}\right) = \frac{2+1}{2 \times 2},$$

which is true since both sides are equal to $3/4$.

Now, for the induction step, we'll assume it true for $n = k$ and prove it for $n = k + 1$. So we're assuming

$$\left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right)\cdots\left(1 - \frac{1}{k^2}\right) = \frac{k+1}{2k},$$

and must prove

$$\left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right)\cdots\left(1 - \frac{1}{k^2}\right)\left(1 - \frac{1}{(k+1)^2}\right) = \frac{k+2}{2(k+1)}.$$

But

$$\begin{aligned}
&\left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right)\cdots\left(1 - \frac{1}{k^2}\right)\left(1 - \frac{1}{(k+1)^2}\right)\\
=&\left(\left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right)\cdots\left(1 - \frac{1}{k^2}\right)\right)\left(1 - \frac{1}{(k+1)^2}\right)\\
=&\frac{k+1}{2k}\left(1 - \frac{1}{(k+1)^2}\right)\\
=&\frac{k+1}{2k}\frac{(k+1)^2 - 1}{(k+1)^2}\\
=&\frac{k+1}{2k}\frac{k(k+2)}{(k+1)^2}\\
=&\frac{k+2}{2(k+1)},
\end{aligned}$$

as required. Note that, in the above, the second equation is due to the induction hypothesis. This completes the proof.

15. Prove carefully that $4^n < n!$ for all natural numbers $n \geq 10$.

    *(The quantity $n!$ denotes the* factorial *of $n$: the product of the natural numbers from 1 up to $n$.)*

    **Solution** We'll prove that $4^n < n!$ for all $n \geq 10$ by induction on $n$, starting with the base case of 10 itself.

    By calculating, we find that $4^{10} = 1048576$, while $10! = 3628800$, so $4^{10} < 10!$.

    Now, for our induction step, suppose that $4^k < k!$ for some $k \geq 10$; we'll show that $4^{k+1} < (k+1)!$. Indeed, we have

    $$4^{k+1} = 4.4^k < (k+1)k! = (k+1)!.$$

    Here the first equation is by definition of exponentiation. The inequality is because $4 < (k+1)$ (as $k \geq 10$ by assumption) and because of the induction hypothesis (that $4^k < k!$). And lastly, the final equation is by the definition of the factorial.

16. The sequence $a_0, a_1, \ldots$ is defined by the following rules:

    - $a_0 = 0$,

- $a_{2n+1} = 9a_n + 2$ for $n \geq 0$.
- $a_{2n} = 4a_n + 1$ for $n \geq 1$

Calculate the first few values $a_1, \ldots, a_5$ by hand. Prove by strong induction that $a_n \geq n^2$ for all $n$.

**Solution** The first few values are:

- $a_0 = 0$,
- $a_1 = 9a_0 + 2 = 2$,
- $a_2 = 4a_1 + 1 = 9$,
- $a_3 = 9a_1 + 2 = 20$,
- $a_4 = 4a_2 + 1 = 37$,
- $a_5 = 9a_2 + 2 = 82$.

We prove the statement that $a_n \geq n^2$ by strong induction on $n$, as follows. For our base case, we have $a_0 = 0 \geq 0^2$.

For the induction step, we assume that $a_k \geq k^2$ for all $k < n$, and we deduce it for $a_n$.

If $n$ is even, then it's equal to $2m$ for some $m$, and then

$$a_n = a_{2m} = 4a_m + 1 \geq 4m^2 + 1 \geq (2m)^2 = n^2.$$

Here we use the induction hypothesis, which tells us that $a_m \geq m^2$.

Similarly, if $n$ is odd, then it's equal to $2m + 1$ for some $m$, and then

$$a_n = a_{2m+1} = 9a_m + 2 \geq 9m^2 + 2 \geq 4m^2 + 4m + 1 = (2m + 1)^2 = n^2.$$

Again we use the induction hypothesis, which tells us that $a_m \geq m^2$.

Either way, we see that $a_n \geq n^2$, which concludes the induction step.

17. **(Challenge 4)** The *Fibonacci numbers* are a function $F : \mathbb{N} \to \mathbb{N}$ defined by $F(0) = 0$, $F(1) = 1$, and $F(n) = F(n-1) + F(n-2)$ for $n \geq 2$. So, for example, $F(2) = 1$, $F(3) = 2$, $F(4) = 3$, $F(5) = 5$, and so on.

    Is $F(2013)$ even or odd? Find an odd prime factor of $F(2013)$.

# Elementary number theory

18. For each of the following statements, either prove them or find a counterexample. Your proofs should proceed *directly from the definition of divisibility.*

    (i) Let $a, b, c$ be integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.

    (ii) Let $a, b, c$ be integers. If $a \mid b$ and $a \mid c$, then $a \mid b + c$.

    (iii) Let $a, b, c$ be integers. If $a \mid b + c$, then $a \mid b$ and $a \mid c$.

    (iv) Let $a, b, c$ be integers. If $a \mid b$ and $a \mid c$, then $a \mid bc$.

    (v) Let $a, b, c$ be integers. If $a \mid bc$, then $a \mid b$ and $a \mid c$.

    (vi) Let $a, b, c, d$ be integers. If $a \mid b$ and $c \mid d$, then $ac \mid bd$.

**Solution**

(i) This is true: to say that $a \mid b$ is to say that $am = b$ for some integer $m$. To say that $b \mid c$ is to say that $bn = c$ for some integer $c$. If both of these are true, then we have $amn = bn = c$, and hence $a \mid c$, as required.

(ii) This is true: if $a \mid b$ and $a \mid c$, we have that $am = b$ for some $m \in \mathbb{Z}$, and $an = c$ for some $n \in \mathbb{Z}$. This means that $a(m+n) = am + an = b + c$, and hence $a \mid b + c$.

(iii) This is false: consider that $2 \mid 2$, but $2 \nmid 1$ and $2 \nmid 1$.

(iv) This is true: since $b \mid bc$, it follows immediately from the first part.

(v) This is false: we have $4 \mid 4$, but $4 \nmid 2$ and $4 \nmid 2$.

(vi) This is true: if $a \mid b$ and $c \mid d$, then $am = b$ for some $m \in \mathbb{Z}$, and $cn = d$ for some $n \in \mathbb{Z}$. This means that $acmn = bd$, and so $ac \mid bd$ as required.

19. 1. Show that the product $n(n+1)(n+2)(n+3)$ of any four consecutive numbers is a multiple of 24.

    2. Show that, given any four numbers $a$, $b$, $c$, $d$ whatsoever, the product of their differences

    $$(a-b)(a-c)(a-d)(b-c)(b-d)(c-d)$$

    is a multiple of 12.

**Solution**

1. This can be done by a slow induction, but we do it more directly. Exactly one of every four consecutive numbers is a multiple of 4, and the number two less or two greater is a multiple of 2. Hence the product is a multiple of 8.

   Also, one of every three consective numbers is a multiple of 3, so the product is. Hence it's a multiple of 24.

2. First we show it a multiple of 4, and then a multiple of 3.

   If the numbers are all even or all odd, then all the differences are even, and so the product is a multiple of 4 (in fact, of 64). If three are even and one is odd, or one is even and three are odd, then the differences of the three that have the same parity are even, and so the product is a multiple of 4 (in fact, of 8). If two are even and two are odd, then the difference of the even pair and the difference of the odd pair are both even, so the product is a multiple of 4. So, in any case, it's a multiple of 4.

   Of the four numbers, some may be of the form $3k$, some of the form $3k+1$ and the rest of the form $3k+2$. There are at least two in the same category, and their difference is a multiple of 3.

   Hence the product is a multiple of 12.

20. Compute the following, showing your working:

    (a) $\gcd(896, 1200)$;

    (b) $\gcd(123456789, 987654321)$.

**Solution**

(a) We have

$$\begin{aligned}
\gcd(896, 1200) &= \gcd(1200, 896) \\
&= \gcd(1 \times 896 + 304, 896) \\
= \gcd(304, 896) &= \gcd(896, 304) \\
&= \gcd(2 \times 304 + 288, 304) \\
= \gcd(288, 304) &= \gcd(304, 288) \\
&= \gcd(1 \times 288 + 16, 288) \\
= \gcd(16, 288) &= \gcd(288, 16) \\
&= \gcd(18 \times 16 + 0, 16) \\
= \gcd(0, 16) &= 16.
\end{aligned}$$

(b) We have

$$\begin{aligned}
\gcd(123456789, 987654321) &= \gcd(987654321, 123456789) \\
&= \gcd(8 \times 123456789 + 9, 123456789) \\
= \gcd(9, 123456789) &= \gcd(123456789, 9) \\
&= \gcd(13717421 \times 9 + 0, 9) \\
= \gcd(0, 9) &= 9.
\end{aligned}$$

21. **(Challenge 5)** Show that any two numbers of the form $2^{2^n}+1$ are coprime (where $n$ is a nonnegative integer), and thus give an alternative proof that there are infinitely many primes.

22. Find all integer solutions to the following linear diophantine equations:

    (a) $10x + 17y = 88$;

    (b) $9x + 15y = 100$.

**Solution**

1. We can use Euclid to find that $\gcd(10, 17) = 1$. By working backwards through Euclid's algorithm one can find a solution to $10x + 17y = 1$ and multiply both sides by 88 to get a solution. However, one may prefer to spot that $10 \times 2 + 17 \times 4 = 88$.
   Suppose $(x, y)$ is another solution, we have

$$\begin{aligned}
10 \times 2 + 17 \times 4 &= 88 \\
10x + 17y &= 88,
\end{aligned}$$

   and so (by subtracting),

$$10(x - 2) + 17(y - 4) = 0.$$

   This means that $y - 4$ must be a multiple of 10, so $y - 4 = 10k$. But then $x - 2 = -17k$. Thus

$$x = 2 - 17k, \qquad y = 10k + 4.$$

We've shown that if $x$ and $y$ are solutions, then they're of these form; we should also check that any $x$ and $y$ of this form are solutions. But

$$10(2 - 17k) + 17(10k + 4) = 20 + 68 = 88,$$

so it does work, and so this is the general solution.

2. The greatest common divisor of 9 and 15 is 3, so the left-hand-side can never equal 100, which is not a multiple of 3. So there are no solutions.

23. Look again at the proof that if a prime $p$ divides $ab$, then $p$ divides $a$ or $b$. Simplify it to obtain a proof that, for any integers $n$, $a$, and $b$, if $n \mid ab$ and $\gcd(n, a) = 1$, then $n \mid b$.

**Solution** If $\gcd(n, a) = 1$, then there are integers $u$ and $v$ with $nu+av = 1$. Multiplying both sides by $b$, we get $nub+avb = b$. The integer $n$ divides the left-hand side since it divides $n$ and $ab$, so we have $n \mid b$.

24. Let $F(n)$ be the $n$th Fibonacci number. What is $\gcd(F(n), F(n + 1))$? Prove your answer by induction.

**Solution** We'll prove that $\gcd(F(n), F(n + 1)) = 1$ by induction on $n$.

or our base case $n = 0$, we have to prove that $\gcd(0, 1) = 1$, which is clearly true.

Now, let's assume it for $n = k$ and prove it for $n = k+1$. So we're assuming that $\gcd(F(k), F(k+1)) = 1$ and have to prove $\gcd(F(k+1), F(k+2)) = 1$.

But

$$\begin{aligned}
&\gcd(F(k + 1), F(k + 2)) \\
=&\gcd(F(k + 1), F(k) + F(k + 1)) \qquad \text{(by definition)} \\
=&\gcd(F(k + 1), F(k)) \qquad \text{(by the method of Euclid's algorithm)} \\
=&1 \qquad \text{(by the induction hypothesis).}
\end{aligned}$$

That's exactly what we needed to prove, so it completes the induction step.

25. **(Challenge 6)** Prove that there are infinitely many primes of the form $4n - 1$. *(Hint: Try thinking about numbers of the form $4p_1p_2 \dots p_k - 1$.)*

# Modular arithmetic

26. Find all solutions to the following congruence equations: in each case, either state that there are no solutions, or give them in the form $x \equiv a \pmod{b}$.

    (a) $6x \equiv 10 \pmod{14}$;

    (b) $6x \equiv 9 \pmod{14}$;

    (c) $5x \equiv 8 \pmod{14}$;

    (d) $7x \equiv 8 \pmod{14}$.

**Solution**

(a) We would like $10 - 6x = 14k$, or in other words, $6x + 14k = 10$. It's easy to check that $\gcd(6, 14) = 2$, and a solution is given by $k = 5$, $x = -10$.

Other solutions occur where $6(x+10) = 14(k-5)$, which is equivalent to $3(x + 10) = 7(k - 5)$. That happens when $3(x + 10)$ is a multiple of 7, which in turn is when $(x + 10)$ is a multiple of 7, which is when $x \equiv 4 \pmod 7$.

(b) We would like $6x+14k = 9$. But $\gcd(6, 14) = 2$, and so this equation has no solutions.

(c) We would like $5x + 14k = 8$. We have that $\gcd(5, 14) = 1$, and $-1 \times 14 + 3 \times 5 = 1$, so $k = -8, x = 24$ is a solution.

Other solutions happen when $5(x-24) = 14(k+8)$, which boils down to $x - 24$ being a multiple of 14, in other words $x \equiv 10 \pmod{14}$.

(d) We would like $7x + 14k = 8$. But $\gcd(7, 14) = 7$, and so there are no solutions.

27. Let $a_n = 2^{2^n-1}$.

    1. Show that each term is twice the square of the previous one.
    2. What is the behaviour of the sequence, modulo 7?

    **Solution**

    1. We have
    $$a_{n+1} = 2^{2^{n+1}-1} = 2^{(2^n-1)+(2^n-1)+1} = 2^{2^n+1}2^{2^n+1}2 = 2a_n^2.$$
    2. Firstly, $a_1 = 2^{2^1-1} = 2^1 = 2$. After that, we can use the above to calculate it:
        - $a_2 = 2a_1^2 = 8 \equiv 1 \pmod 7$;
        - $a_3 = 2a_2^2 \equiv 2 \times 1^1 \equiv 2 \pmod 7$.

        After this, since each only depends on the term before, they'll continue to alternate between being 1 and 2, modulo 7.

28. If $a^{31} \equiv 3 \pmod{47}$, show, by cubing both sides and applying Fermat's Little Theorem, that $a \equiv 27 \pmod{47}$.

    **Solution** Cubing both sides gives
    $$a^{93} = \left(a^{31}\right)^3 \equiv 3^3 = 27 \pmod{47}.$$
    However, $a^{46} \equiv 1 \pmod{47}$ by Fermat's Little Theorem, and then
    $$a^{93} = a^{46}a^{46}a \equiv 1 \cdot 1 \cdot a = a \pmod{47}.$$
    Hence $a \equiv 27 \pmod{47}$ as asked.

29. Find all solutions to the congruence equation
    $$143x \equiv 243 \pmod{343}.$$

**Solution** We seek solutions to

$$143x + 343k = 243.$$

We'll do it by taking the gcd, and working backwards, as usual.

We have

$$\begin{aligned}
\gcd(143, 343) &= \gcd(143, 2 \times 143 + 57) \\
&= \gcd(143, 57) = \gcd(57, 143) \\
&= \gcd(57, 2 \times 57 + 29) \\
&= \gcd(57, 29) = \gcd(29, 57) \\
&= \gcd(29, 1 \times 29 + 28) \\
&= \gcd(29, 28) = \gcd(28, 29) \\
&= \gcd(28, 1 \times 28 + 1) \\
&= \gcd(28, 1) = 1.
\end{aligned}$$

That means that

$$\begin{aligned}
1 &= 29 - 28 \\
&= 29 - (57 - 29) = 2(29) - 57 \\
&= 2(143 - 2(57)) - 57 = 2(143) - 5(57) \\
&= 2(143) - 5(343 - 2(143)) = 12(143) - 5(343).
\end{aligned}$$

So one way of getting $143x \equiv 1 \pmod{343}$ is to take $x = 12$; the general solution for that equation satisfies

$$143(x - 12) + 343(k - 5) = 0.$$

When this happens, we have $343 \mid (x - 12)$, and so $x = 12 + 343n$ for some $n$.

So the general solution to the equation we were given is to take $x \equiv 12 \cdot 243 \equiv 172 \pmod{343}$.

30. 1. Can you find values of $n$ satisfying the following equations?
    (a) $\varphi(n) = 10$ (there is only one solution);
    (b) $\varphi(n) = 20$ (there are five solutions).

**Solution**

1. $n = 11$ works.
2. $n = 25, 33, 44, 50, 66$ all work (and $n = 21$ doesn't!).

31. **(Challenge 7)** In 1994, Andrew Wiles, building on work of many other people, proved *Fermat's Last Theorem*, that there are no solutions to the equation

$$a^n + b^n = c^n,$$

where $a$, $b$, $c$ and $n$ are positive integers and $n > 2$.

Show that there *are* infinitely many solutions in positive integers to

$$a^{34} + b^{34} = c^{35}.$$

Then show that there are also infinitely many solutions in positive integers to

$$a^{51} + b^{52} = c^{53}.$$

32. Solve the following simultaneous congruence equations:

    (a) $x \equiv 5 \pmod 7$, $x \equiv 2 \pmod 6$;

    (b) $x \equiv 5 \pmod 8$, $x \equiv 2 \pmod 6$;

    (c) $x \equiv 5 \pmod 9$, $x \equiv 2 \pmod 6$;

    (d) $x \equiv 17 \pmod{41}$, $x \equiv 36 \pmod{43}$.

    **Solution**

    (a) The Chinese Remainder Theorem says that it is the same as some class modulo 42. In fact $x \equiv 26 \pmod{42}$.

    (b) No solution exists: one equation says that $x$ is even, and the other that $x$ is odd.

    (c) It can be found (by experimentation, for example), that $x \equiv 14 \pmod{18}$ is the general solution.

    (d) We find that $x = 41m + 17$ and $x = 43n + 36$. Hence, by identifying these and simplifying, $41m - 43n = 19$. The usual techniques solve this for us to get a solution $n = 12$, $m = 11$.

    Hence, by the Chinese Remainder Theorem, we have one solution mod $41 \times 43 = 1763$, and that's $x = 41 \times 12 + 17 = 509$: the solution is $x \equiv 509 \pmod{1763}$.

33. Here are some three-variable problems!

    1. Solve the simultaneous congruences

    $$\begin{aligned} n &\equiv 4 \pmod 9 \\ n &\equiv 7 \pmod{10} \\ n &\equiv 3 \pmod{11} \end{aligned}$$

    *(Hint: solve the first two, and then combine your solution with the last one).*

    2. Find all solutions to the equation

    $$10a + 12b + 15c = 1,$$

    where $a$, $b$ and $c$ are integers. *(Hint: find one solution, subtract as usual to find others, fix one variable and solve for the other two.)*

**Solution**

1. The methods of the lectures will combine the first pair of congruences to get $n \equiv 67 \pmod{90}$. By another use of the methods of the lectures, we can combine this with the third congruence to get $n \equiv 157 \pmod{990}$.
2. One solution is given by $a = -2$, $b = -2$, $c = 3$. If we subtract, that leaves us considering the equation

$$10(a+2) + 12(b+2) + 15(c-3) = 0.$$

For ease, we will let $u = a + 2$, $v = b + 2$ and $w = c - 3$, so we are interested in

$$10u + 12v + 15w = 0.$$

Suppose $u$ is fixed, so we're interested in

$$12v + 15w = -10u.$$

By considering the gcd, this is solvable only when $-10u$ is a multiple of three, which happens only when $u = 3k$ is a multiple of three. When it is, dividing out by the common factor, we have

$$4v + 5w = -10k.$$

One solution to this is given by $w = -10k$, $v = 10k$. Then, subtracting, we are considering the equation

$$4(v - 10k) + 5(w + 10k) = 0.$$

This has solutions whenever $4(v - 10k)$ is a multiple of 5, which happens exactly when $v - 10k$ is a multiple of 5. Say $v - 10k = 5l$. Then, substituting in, we get $4(v-10k) = 20l$, so $5(w+10k) = -20l$, so $w + 10k = -4l$.
Rearranging, this gives us

$$u = 3k, \qquad v = 10k + 5l, \qquad w = -10k - 4l,$$

and then substituting back gives

$$a = 3k - 2, \qquad v = 10k + 5l - 2, \qquad w = -10k - 4l + 3.$$

It can quickly be checked that this is indeed a solution.
*(Note that there are many, many ways of writing this solution: if yours looks different it may not be wrong: check it by substituting back in!)*

34. Show that $17 \mid (3^{32} - 2^{32})$ using Fermat's Little Theorem.

**Solution** Fermat's Little Theorem gives us that

$$3^{32} - 2^{32} = 3^{16}3^{16} - 2^{16}2^{16} \equiv 1 \cdot 1 - 1 \cdot 1 = 0 \pmod{17}.$$

35. **(Challenge 8)**

    (i) Show that 561 is not prime.

    (ii) Show that, even though 561 is not prime, if $\gcd(a, 561) = 1$, then $a^{560} \equiv 1 \pmod{561}$.

    *This shows that one possible converse of Fermat's Little Theorem is not true. Numbers with this property, of being composite but "apparently prime" from the point of view of Fermat's Little Theorem, are called* Carmichael numbers.

# The real numbers

36. Show that $\log_{10}(37)$ and $\sqrt[3]{2}$ are irrational numbers.

    **Solution**

    1. We'll prove it by contradiction. Suppose that $\log_{10}(37)$ is rational, and let $p$ and $q$ be integers (with $q$ positive) such that $p/q = \log_{10}(37)$. Then $10^{p/q} = 37$, so $10^p = (10^{p/q})^q = 37^q$. But the right-hand side is a multiple of 37 (since $q > 0$) and the left-hand side cannot be. This is a contradiction.
    2. Suppose not: suppose $\sqrt[3]{2} = p/q$, for some coprime integers $p$ and $q$. Then, cubing both sides, we get $2 = p^3/q^3$, and so $p^3 = 2q^3$.

       The right-hand side is a multiple of 2, and thus the left-hand side must be too, As a result, $p$ is even: an odd number cubes to an odd number. So we can write $p = 2r$ for some $r$. Then we substitute in to get $(2r)^3 = 8r^3 = 2q^3$ which cancels to get $4r^3 = q^3$. The left-hand side is even, too, and hence the right-hand side must be too. Hence $q$ is even, and so shares a factor (of 2) in common with $p$, which is a contradiction. Hence $\sqrt[3]{2}$ is irrational.

37. (a) Show directly from the definition of convergence that the sequence defined by

$$a_n = \frac{1 - \frac{1}{n}}{1 + \frac{1}{n}}$$

    converges to 1.

    (b) Show directly from the definition of convergence that the sequence defined by

$$b_n = \frac{(2n+1)(2n-1)}{n^2}$$

    converges to 4.

**Solution**

(a) We can simplify to get $a_n = \frac{n-1}{n+1} = 1 - \frac{2}{n+1}$. We aim to show that, for all $\epsilon$, there is some $N$ such that for all $n > N$ we have

$$|a_n - 1| < \epsilon,$$

but this rearranges to $\frac{2}{n+1} < \epsilon$. Hence if we take $N = \lceil 2/\epsilon - 1 \rceil$, then for $n > N$ we get $\frac{2}{n+1} < \frac{2}{2/\epsilon} = \epsilon$ as needed.

(b) The aim is to show that, for all $\epsilon$, there is some $N$ such that for all $n > N$ we have

$$|b_n - 4| < \epsilon.$$

But we have

$$\left|\frac{(2n+1)(2n-1)}{n^2} - 4\right| = \left|\frac{4n^2-1}{n^2} - 4\right|$$
$$= \left|4 - \frac{1}{n^2} - 4\right| = \left|-\frac{1}{n^2}\right| = \frac{1}{n^2}.$$

So the aim is to show that, for all $\epsilon$, there is some $N$ such that for all $n > N$ we have

$$\frac{1}{n^2} < \epsilon.$$

If we take $N = \lceil 1/\epsilon \rceil$, then for $n > N$ we have

$$\frac{1}{n^2} \leq \frac{1}{n} < \frac{1}{N} \leq \frac{1}{1/\epsilon} = \epsilon,$$

which is what we need.

38. **(Challenge 9)** Show that $\sqrt{3} + \sqrt{5} + \sqrt{7}$ is irrational.