Discrete Mathematics

Exercises 4 – Solutions with Commentary

Marcelo Fiore   Ohad Kammar   Dima Szamozvancev

4. On induction

4.1. Basic exercises

1. Prove that for all natural numbers $n \geq 3$, if n distinct points on a circle are joined in consecutive order by straight lines, then the interior angles of the resulting polygon add up to $180 \cdot (n-2)$ degrees.

   We prove this property $P(n)$ of all $n \geq 3$ by mathematical induction from basis 3.

   Base case: $n = 3$. Three connected points on a circle must form a triangle: since they are distinct, they cannot be collinear. The sum of internal angles of a triangle is $180°$, which is $180 \cdot (3-2)$ degrees.

   Inductive case: $n = k + 1$. Assume that ⒤ $P(k)$ holds and take an arbitrary polygon constructed from $k + 1$ points $A_1, \dots, A_{k+1}$ on a circle. The $(k+1)$-gon can be separated into a k-gon and a triangle with a line segment connecting A_1 and A_k. By the induction hypothesis ⒤, the interior angles of the k-gon add up to $S_k = 180 \cdot (k-2)$ degrees. The sum of angles of the whole polygon is $S_{k+1} = S_k + \angle A_k A_1 A_{k+1} + \angle A_1 A_{k+1} A_k + \angle A_1 A_k A_{k+1}$, where the angle terms belong to the triangle $\triangle A_1 A_k A_{k+1}$. Since its interior angles must add up to $180°$, we have the expression for the sum of internal angles of the $(k+1)$-gon:

   $$S_{k+1} = S_k + 180° = 180 \cdot (k-2) + 180° = 180 \cdot ((k+1)-2)$$
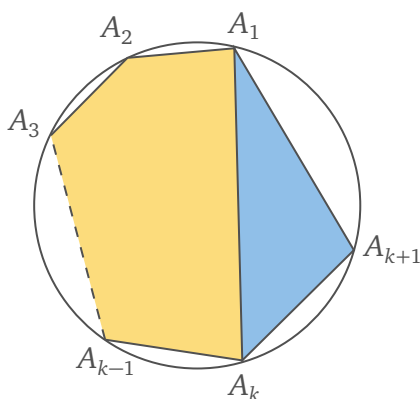
   ♪ While the formula holds for any polygon, working with points on a circle makes the inductive proof easier, since we never need to worry about three points being on the same line and only making up one side.

   ♪ It may be tempting to approach the inductive step by starting with a k-gon, then *adding* a new point to turn it into a $(k+1)$-gon and increasing the sum of internal angles by $180°$. The problem with this is that we are *given* a $(k+1)$-gon to start with, and its vertices are

predetermined: we need to split it up into a triangle and a k-gon, no matter what the points are. This distinction is fairly minor in this case and doesn't cause any difficulties (any line segment connecting two vertices one point apart will split do the job), but remembering what parameters we have control over vs. what we are given (that is, what we need to assume as being arbitrary) is very important in proofs, especially inductive ones. We will see examples of this throughout this sheet.

2. Prove that, for any positive integer n, a $2^n \times 2^n$ square grid with any one square removed can be tiled with L-shaped pieces consisting of 3 squares.

We prove the property $P(n)$ of all $n \geq 1$ by mathematical induction from basis 1:

$$P(n) = \forall 0 \leq i, j \leq n. \text{ a } 2^n \times 2^n \text{ grid } A \text{ with square } A_{i,j} \text{ missing can be tiled}$$

Base case: $n = 1$. Take a $2^1 \times 2^1 = 2 \times 2$ grid and assume one of the squares is missing. This must be one of the following four situations, depending on which one of the 4 squares was removed:

All resulting shapes can be tiled with one L-shaped piece consisting of three squares.

Inductive step: $n = k + 1$. Assume ⒣ $P(k)$: a $2^k \times 2^k$ grid with any square missing can be tiled with L-shaped pieces. Take a $2^{k+1} \times 2^{k+1}$ grid with any one square missing. The grid can be split into four $2^k \times 2^k$ quarters which we label by A, B, C and D; assume, without loss of generality, that the missing square is in quarter A at position $A_{i,j}$. By the ⒣ applied to i and j, the quarter A can be tiled with $A_{i,j}$ missing. Next, we use the ⒣ applied to $i = k$ and $j = 1$ to tile quarter B with the bottom left square missing. Similarly, we tile C and D with two applications of the induction hypothesis (⒣$(1, k)$ and ⒣$(1, 1)$, respectively) with the top right and left corners missing. The three missing corners form an L-shaped hole of 3 squares in the middle of the $2^{k+1} \times 2^{k+1}$ grid, which can be filled in with one additional tile. This leaves only one missing square $A_{i,j}$ with the rest of the grid tiled with L-shaped pieces, so we are done.
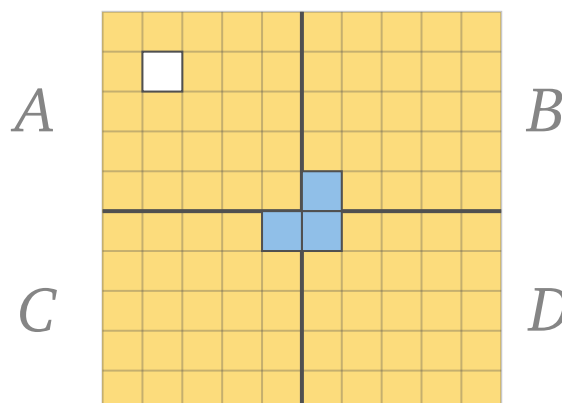
♪ This is an example of an inductive proof where the proposition $P(n)$ is itself a universally quantified statement: we state property for all grid size parameters n, and within a particular grid of size $2^n \times 2^n$, for all possible grid cells that could be missing. Thus, after case-splitting on n, we still have a universally quantified proof obligation; however, in the inductive case, we also have a universally quantified inductive assumption.

While the general pattern for proofs like this is just an instance of the standard induction principle, it is worth analysing nevertheless:

To prove a property of the form

$$\forall n \in \mathbb{N}. \ \forall x \in A. \ P(n, x)$$

it is sufficient to prove

$$\forall x \in A. \ P(0, x) \quad \text{and} \quad \forall k \in \mathbb{N}. \ (\forall y \in A. \ P(k, y)) \implies (\forall x \in A. \ P(k + 1, x))$$

The base case – which is usually seen as the "trivial" step – is now itself a universally quantified statement which may not necessarily be easy to establish. Indeed, if the inner quantification is over natural numbers as well, we may end up having to do *another* inductive proof of $\forall m \in \mathbb{N}. \ P(0, m)$ if a direct proof ("Let m be an arbitrary natural number and prove $P(0, m)\dots$") is not possible.

The inductive step highlights the interplay between the two quantifications. Unwrapping the formula, we get three assumptions: an arbitrary natural number k, an arbitrary element $x \in A$, and a *proof* that $P(k, y)$ holds for any choice of $y \in A$. In the process of the proof, this induction hypothesis can be applied to any element $y \in A$, be it $x \in A$, a value computed from x, or any other value arbitrarily chosen by us. There is a significant difference between the inductive step above, and a formula such as

$$\forall k \in \mathbb{N}. \ \forall x \in A. \ P(k, x) \implies P(k + 1, x)$$

which leaves us no flexibility in "tailoring" the IH to our needs by choosing an appropriate value for x.

The question above had an inner universal quantification over the position of the missing cell, so the proof cannot depend on any particular choice of position in the $2^{k+1} \times 2^{k+1}$ grid. However, we do have control over the position of the missing cell when applying the induction hypothesis to the $2^k \times 2^k$ quarter grids: we can essentially think of the Ⓘ as a "function" from coordinates (i, j) to the proof of "tileability". To complete the inductive step, we first apply the IH to the coordinates of the actual hole in the $2^{k+1} \times 2^{k+1}$ within the A quarter, then select the appropriate locations for the holes in the quarters B, C and D to leave an L-shaped hole in the middle. We apply the Ⓘ both to the unknown values (i, j) given to us by the universal quantifier on the LHS of the implication, as well as values that we select deliberately to create space for an extra L-shaped tile.

♪ The phrase "without loss of generality" is often used to reduce repetition or make simplifying assumptions that do not change the strength of the result. It is usually understood that if the assumption is violated, it can be altered in an obvious way to make the rest of the proof go through. It is important to ensure that the assumption really doesn't affect the generality of the statement: saying things like "w.l.o.g., assume n is even/nonzero/a power of two" is sometimes tempting, but it's rarely clear how the proof could be extended to numbers which are odd/zero/not a power of two, and proving these cases may require entirely different approaches to the one considered. Above, we assumed w.l.o.g. that the hole is in quarter A so we don't need to repeat the proof for all four quarters. The proofs would not be exactly the same (e.g. if the hole was in quarter B, the IH would need to be applied to the $(i - k, j)$ coordinates of the $2^k \times 2^k$ grid), but it's clear that the general idea would work in each case.

♪ The proof above doesn't just show that a tiling is possible, it gives a concrete algorithm for constructing it. Proofs like this are – unsurprisingly – called *constructive* proofs (also known as *effective* proofs to avoid confusion with constructive mathematics), as opposed to *nonconstructive* or *pure existence* proofs which show that a mathematical object exists, but doesn't give a concrete example or way of computing one. Constructive proofs by induction naturally give rise to recursive algorithms, where the application of the ⓘⒽ corresponds to a recursive call. Of course, when implementing the recursive algorithm, we don't have the luxury of saying that "without loss of generality, assume the user will never call the function with the hole outside of quarter A" – we have to explicitly handle all four possibilities and slightly different recursive calls to cover any possible input.

4.2. Core exercises

1. Establish the following:

   (a) For all positive integers m and n,

   $$(2^n - 1) \cdot \sum_{i=0}^{m-1} 2^{i \cdot n} = 2^{m \cdot n} - 1$$

   The first thing to note is that an inductive proof is not really necessary. Indeed, for arbitrary positive integers m and n, one can calculate that

   $$(2^n - 1) \cdot \sum_{i=0}^{m-1} 2^{i \cdot n} = \sum_{i=0}^{m-1} 2^{(i+1) \cdot n} - \sum_{i=0}^{m-1} 2^{i \cdot n}$$

   $$= \sum_{i=1}^{m-1} 2^{i \cdot n} + 2^{((m-1)+1) \cdot n} - 2^{0 \cdot n} - \sum_{i=1}^{m-1} 2^{i \cdot n}$$

   $$= 2^{m \cdot n} - 1$$

   However, as it is very instructive, two inductive proofs follow. Note the different,

though subtle, ways in which the inductive hypothesis is used in each proof.

For the *first proof*, we show

$$\forall m \in \mathbb{Z}^+. \ P(m)$$

for $P(m)$ the statement

$$\forall n \in \mathbb{Z}^+. \ (2^n - 1) \cdot \sum_{i=0}^{m-1} 2^{i \cdot n} = 2^{m \cdot n} - 1$$

by the Principle of Induction.

Base case: $m = 1$. The statement $P(1)$ amounts to

$$\forall n \in \mathbb{Z}^+. \ (2^n - 1) \cdot 2^{i \cdot n} = 2^{1 \cdot n} - 1$$

which is vacuously true.

Inductive step: $m = k + 1$. Let k be an arbitrary positive integer, and assume that the Inductive Hypothesis $P(k)$ holds for it; i.e. that

$$\forall n \in \mathbb{Z}^+. \ (2^n - 1) \cdot \sum_{i=0}^{k-1} 2^{i \cdot n} = 2^{k \cdot n} - 1 \qquad \text{(IH)}_1$$

We need show that $P(k + 1)$ follows; i.e. that

$$\forall n \in \mathbb{Z}^+. \ (2^n - 1) \cdot \sum_{i=0}^{(k+1)-1} 2^{i \cdot n} = 2^{(k+1) \cdot n} - 1$$

To this end, we let l be an arbitrary positive integer and proceed to show that

$$(2^l - 1) \cdot \sum_{i=0}^{k} 2^{i \cdot l} = 2^{(k+1) \cdot l} - 1 \qquad \text{①}$$

Indeed, instantiating the (IH)_1, we have that

$$(2^l - 1) \cdot \sum_{i=0}^{k-1} 2^{i \cdot l} = 2^{k \cdot l} - 1 \qquad \text{②}$$

and so that

$$(2^l - 1) \cdot \sum_{i=0}^{k} 2^{i \cdot l} = \left((2^l - 1) \cdot \sum_{i=0}^{k-1} 2^{i \cdot l} \right) + (2^l - 1) \cdot 2^{k \cdot l}$$

$$= 2^{k \cdot l} - 1 + (2^l - 1) \cdot 2^{k \cdot l} \qquad \text{(by ②)}$$

$$= 2^{(k+1) \cdot l} - 1$$

establishing ① as required. $\qquad\qquad \square$

For the *second proof*, to show

$$\forall n \in \mathbb{Z}^+. \ \forall m \in \mathbb{Z}^+. \ (2^n - 1) \cdot \sum_{i=0}^{m-1} 2^{i \cdot n} = 2^{m \cdot n} - 1$$

we let l be an arbitrary positive integer and prove

$$\forall m \in \mathbb{Z}^+. \ Q(l, m)$$

for $Q(l, m)$ the statement

$$(2^l - 1) \cdot \sum_{i=0}^{m-1} 2^{i \cdot l} = 2^{m \cdot l} - 1$$

by the Principle of Induction.

Base case: $m = 1$. The statement $Q(l, 1)$ amounts to

$$(2^l - 1) \cdot 2^{0 \cdot l} = 2^{1 \cdot l} - 1$$

which is vacuously true.

Inductive step: $m = k + 1$. Let k be an arbitrary positive integer, and assume that the Inductive Hypothesis $Q(l, k)$ holds for it; i.e. that

$$(2^l - 1) \cdot \sum_{i=0}^{k-1} 2^{i \cdot l} = 2^{k \cdot l} - 1 \qquad \text{ⒾⒽ}_2$$

We need show that $Q(l, k + 1)$ follows; i.e. that

$$\mathbb{Z}^+ (2^l - 1) \cdot \sum_{i=0}^{(k+1)-1} 2^{i \cdot l} = 2^{(k+1) \cdot l} - 1 \qquad ①$$

Indeed,

$$(2^l - 1) \cdot \sum_{i=0}^{k} 2^{i \cdot l} = \left((2^l - 1) \cdot \sum_{i=0}^{k-1} 2^{i \cdot l} \right) + (2^l - 1) \cdot 2^{k \cdot l}$$

$$= 2^{k \cdot l} - 1 + (2^l - 1) \cdot 2^{k \cdot l} \qquad \text{(by ⒾⒽ}_2\text{)}$$

$$= 2^{(k+1) \cdot l} - 1$$

establishing ① as required.

🎵 The core of the proof is the same in both cases; the difference is how they set up the induction hypothesis. The first proof includes the quantification over n in the ⒾⒽ$_1$ and applies it to the arbitrary l in the proof to get a specific instance ②. The second proof fixes this l right from the start, introducing it as a new arbitrary variable in the standard manner of proving universal quantification. Then, the predicate to be established by inductively is "parameterised" by this l, so the statement $Q(l, m)$

doesn't actually need a nested quantification. Despite $⑩_2$ not containing a universal quantification, the proof only requires it at the specific l we already introduced. This makes the second proof slightly simpler, but it would not work if we ever needed the induction hypothesis at any other value of n.

(b) Suppose k is a positive integer that is not prime. Then $2^k - 1$ is not prime.

Let k be an arbitrary positive integer. We consider two cases:

- $k = 1$. The statement holds because $2^1 - 1 = 1$ is not prime.

- $k \geq 2$. Assume that $k \geq 2$ is not prime. Hence, it is of the form $m \cdot n$ for natural numbers m, n greater than or equal 2. It follows from the previous item that $2^k - 1 = 2^{m \cdot n} - 1 = (2^n - 1) \cdot \sum_{i=0}^{m-1} 2^{i \cdot n}$; and, since $2^n - 1 \geq 2^2 - 1 = 3$ and $\sum_{i=0}^{m-1} 2^{i \cdot n} \geq 1 + 4 = 5$, we have that $2^k - 1$ has a non-trivial decomposition. Hence it is not prime.

2. Prove that

$$\forall n \in \mathbb{N}.\ \forall x \in \mathbb{R}.\ x \geq -1 \implies (1+x)^n \geq 1 + n \cdot x$$

We prove $\forall n \in \mathbb{N}.\ P(n)$ for $P(n)$ the statement

$$\forall x \in \mathbb{R}.\ x \geq -1 \implies (1+x)^n \geq 1 + n \cdot x$$

by the Principle of Induction.

Base case: $n = 0$. The statement $P(0)$ reduces to

$$\forall x \in \mathbb{R}.\ x \geq -1 \implies 1 \geq 1$$

and holds vacuously.

Inductive step: $n = k+1$. Let k be an arbitrary natural number, and assume $P(k)$; i.e. assume the Inductive Hypothesis

$$\forall x \in \mathbb{R}.\ x \geq -1 \implies (1+x)^k \geq 1 + k \cdot x \qquad ⑩$$

We need show that $P(k+1)$ also holds; i.e. that

$$\forall x \in \mathbb{R}.\ x \geq -1 \implies (1+x)^{k+1} \geq 1 + (k+1) \cdot x$$

To this end, we let y be an arbitrary real number, assume further that

$$y \geq -1 \qquad ①$$

and proceed to show that

$$(1+y)^{k+1} \geq 1 + (k+1) \cdot y \qquad ②$$

From $\text{\textcircled{IH}}$, by instantiation and Modus Ponens using $\text{\textcircled{1}}$, one concludes that

$$(1 + y)^k \geq 1 + k \cdot y$$

and from this, since by $\text{\textcircled{1}}$ we have $1 + y \geq 0$, it follows that

$$(1 + y)^{k+1} = (1 + y)^k \cdot (1 + y) \geq (1 + k \cdot y) \cdot (1 + y) = 1 + (k+1) \cdot y + k \cdot y^2$$

Thus, from the fact that $k \cdot y^2 \geq 0$, $\text{\textcircled{2}}$ holds.

3. Recall that the Fibonacci numbers F_n for $n \in \mathbb{N}$ are defined recursively by $F_0 = 0$, $F_1 = 1$, and $F_{n+2} = F_n + F_{n+1}$ for $n \in \mathbb{N}$.

   a) Prove Cassini's Identity: For all $n \in \mathbb{N}$,

   $$F_n \cdot F_{n+2} = F_{n+1}{}^2 + (-1)^{n+1}$$

   We prove

   $$\forall n \in \mathbb{N}.\ F_n \cdot F_{n+2} = F_{n+1}{}^2 + (-1)^{n+1}$$

   by the Principle of Induction.

   Base case: $n = 0$. We have that

   $$F_0 \cdot F_2 = F_1{}^2 + (-1)^1$$

   because $F_0 = 0$ and $F_1 = 1$.

   Inductive step: $n = k + 1$. For any natural number k, assume the Induction Hypothesis

   $$F_n \cdot F_{k+2} = F_{k+1}{}^2 + (-1)^{k+1}$$

   which can be rearranged to the following form by subtracting $(-1)^{k+1}$:

   $$F_{k+1}{}^2 = (-1)^k + F_n \cdot F_{k+2} \qquad\qquad \text{\textcircled{IH}}$$

   We need show that

   $$F_{k+1} \cdot F_{(k+1)+2} = F_{(k+1)+1}{}^2 + (-1)^{(k+1)+1}$$

   i.e. that

   $$F_{k+1} \cdot F_{k+3} = F_{k+2}{}^2 + (-1)^k$$

   for which one calculates as follows:

   $$
   \begin{aligned}
   F_{k+1} \cdot F_{k+3} &= F_{k+1}{}^2 + F_{k+1} \cdot F_{k+2} &&(F_{k+3} = F_{k+1} + F_{k+2})\\
   &= (-1)^k + F_n \cdot F_{k+2} + F_{k+1} \cdot F_{k+2} &&(\text{by } \text{\textcircled{IH}})\\
   &= (-1)^k + F_{k+2}{}^2 &&(F_{k+2} = F_k + F_{k+1})
   \end{aligned}
   $$

   b) Prove that for all natural numbers k and n,

   $$F_{n+k+1} = F_{n+1} \cdot F_{k+1} + F_n \cdot F_k$$

We prove that

$$\forall k \in \mathbb{N}. \ P(k)$$

for $P(k)$ the statement

$$\forall n \in \mathbb{N}. \ F_{n+k+1} = F_{n+1} \cdot F_{k+1} + F_n \cdot F_k$$

by the Principle of Induction.

Base case: We need show that

$$\forall n \in \mathbb{N}. \ F_{n+1} = F_{n+1} \cdot F_1 + F_n \cdot F_0$$

which holds because $F_1 = 1$ and $F_0 = 0$.

Inductive step: For an arbitrary natural number k, assume the Induction Hypothesis

$$\forall n \in \mathbb{N}. \ F_{n+k+1} = F_{n+1} \cdot F_{k+1} + F_n \cdot F_k \qquad \text{(IH)}$$

We need show that

$$\forall n \in \mathbb{N}. \ F_{n+(k+1)+1} = F_{n+1} \cdot F_{(k+1)+1} + F_n \cdot F_{k+1}$$

i.e. that

$$\forall n \in \mathbb{N}. \ F_{n+k+2} = F_{n+1} \cdot F_{k+2} + F_n \cdot F_{k+1} \qquad \text{①}$$

To this end, we let m be an arbitrary natural number and proceed to show the equivalent identity:

$$F_{(m+1)+k+1} = F_{m+1} \cdot F_{k+2} + F_m \cdot F_{k+1} \qquad \text{②}$$

Indeed, instantiating the universally-quantified Induction Hypothesis ⒤ for the natural number $m + 1$, one has that

$$F_{(m+1)+k+1} = F_{(m+1)+1} \cdot F_{k+1} + F_{m+1} \cdot F_k$$

from which one further calculates as follows:

$$
\begin{aligned}
& F_{(m+1)+1} \cdot F_{k+1} + F_{m+1} \cdot F_k \\
= {} & F_m \cdot F_{k+1} + F_{m+1} \cdot F_{k+1} + F_{m+1} \cdot F_k & (F_{(m+1)+1} = F_m + F_{m+1}) \\
= {} & F_m \cdot F_{k+1} + F_{m+1} \cdot F_{k+2} & (F_{k+2} = F_k + F_{k+1})
\end{aligned}
$$

to conclude ②.

♪ This is an example of a proposition that could also be established by nested induction: rather than show ① directly for an arbitrary $n \in \mathbb{N}$, we could do another base case for $n = 0$ and inductive case for $n = m + 1$. It's not always obvious when this is required, but quite often results in a lengthier, but simpler proof.

♪ If either of k or n is positive, this identity gives a way of expanding F_{n+k} as a sum of products of Fibonacci numbers – a useful property whenever the index is a sum.

c) Deduce that $F_n \mid F_{l \cdot n}$ for all natural numbers n and l.

> We prove that
> $$\forall l \in \mathbb{N}.\ P(l)$$
> for $P(l)$ the statement
> $$\forall n \in \mathbb{N}.\ F_n \mid F_{l \cdot n}$$
> by the Principle of Induction.
>
> **Base case**: We need to show that
> $$\forall n \in \mathbb{N}.\ F_n \mid F_{0 \cdot n}$$
> i.e. that
> $$\forall n \in \mathbb{N}.\ F_n \mid 0$$
> which holds because we know that every integer divides 0 from §1.2.1(b).
>
> **Inductive step**: For an arbitrary natural number l, assume the Induction Hypothesis
> $$\forall n \in \mathbb{N}.\ F_n \mid F_{l \cdot n} \qquad\qquad \text{(IH)}$$
> We need to show that
> $$\forall n \in \mathbb{N}.\ F_n \mid F_{(l+1) \cdot n}$$
> i.e. that
> $$\forall n \in \mathbb{N}.\ F_n \mid F_{l \cdot n + n}$$
> To this end, let $n \in \mathbb{N}$ be an arbitrary natural number. We first consider the case when $n = 0$: we have $F_0 \mid F_{l \cdot 0 + 0}$ from the fact that $0 \mid 0$ (see §1.2.1(a)). Otherwise, we can express $F_{l \cdot n + n}$ as $F_{l \cdot n + (n-1)+1}$ and expand using §4.2.3(b) as follows:
>
> $$\begin{aligned} & F_{l \cdot n + (n-1)+1} \\ = {}& F_{l \cdot n + 1} \cdot F_{(n-1)+1} + F_{l \cdot n} \cdot F_{n-1} && \text{(by §4.2.3(b))} \\ = {}& F_{l \cdot n + 1} \cdot F_n + k \cdot F_n \cdot F_{n-1} && \text{(by (IH), } \exists k \in \mathbb{Z}.\ F_{l \cdot n} = k \cdot F_n\text{)} \\ = {}& F_n \cdot (F_{l \cdot n + 1} + k \cdot F_{n-1}) \end{aligned}$$
>
> Thus, $F_{(l+1) \cdot n} = k' \cdot F_n$ for $k' = F_{l \cdot n + 1} + k \cdot F_{n-1}$, showing that $F_n \mid F_{(l+1) \cdot n}$, as required.
>
> ♪ Words like "deduce" and "conclude" are a dead giveaway that you should be using properties you showed in a previous part of the question, so you should always try to transform the proposition or play around with your assumptions until a previous lemma could be applied – this step often takes care of the "hard part" of the proof. In this exercise the inductive step gave us $F_{l \cdot n + n}$; since the index is a sum of two natural numbers with n positive, we notice that the previous identity can be applied to expand the term into two more "manageable" subterms.

d) Prove that $\gcd(F_{n+2}, F_{n+1})$ terminates with output 1 in n steps for all positive integers n.

We prove that

$$\forall n \in \mathbb{N}.\ \gcd(F_{n+2}, F_{n+1}) \text{ terminates with output 1 in } n \text{ steps}$$

by the Principle of Induction.

Base case: We need to show that

$$\gcd(F_3, F_2) \text{ terminates with output 1 in 1 step}$$

Since $F_3 = 2$ and $F_2 = 1$ and $1 \mid 2$, the algorithm terminates with the base case of $F_2 = 1$ after one step.

Inductive step: For an arbitrary natural number k, assume the Induction Hypothesis

$$\gcd(F_{k+2}, F_{k+1}) \text{ terminates with output 1 in } k \text{ steps} \qquad \text{(IH)}$$

We need to prove that

$$\gcd(F_{k+3}, F_{k+2}) \text{ terminates with output 1 in } k+1 \text{ steps}$$

By the definition of Fibonacci numbers, $F_{k+3} = F_{k+2} + F_{k+1}$. Since $F_{k+2} \geq F_{k+1}$, this is a valid quotient-remainder decomposition of F_{k+3} so by the Division Theorem we have that $\text{quo}(F_{k+3}, F_{k+2}) = 1$ and $\text{rem}(F_{k+3}, F_{k+2}) = F_{k+1}$. As F_{k+1} is positive, $F_{k+2} \nmid F_{k+3}$ and $\gcd(F_{k+3}, F_{k+2})$ steps to $\gcd(F_{k+2}, \text{rem}(F_{k+3}, F_{k+2})) = \gcd(F_{k+2}, F_{k+1})$. By the (IH), this terminates with output 1 in k steps; thus, starting with the additional computation step, $\gcd(F_{k+3}, F_{k+2})$ terminates with output 1 in $k+1$ steps.

e) Deduce also that:

   (i) for all positive integers $n < m$, $\gcd(F_m, F_n) = \gcd(F_{m-n}, F_n)$,

and hence that:

   (ii) for all positive integers m and n, $\gcd(F_m, F_n) = F_{\gcd(m,n)}$.

Firstly, we prove the following statement equivalent to (i):

For all positive integers n and natural numbers k,

$$\gcd(F_{n+k+1}, F_n) = \gcd(F_{k+1}, F_n)$$

We make use of the following corollary/restatement of Theorem 61, which allows us to use properties of Euclid's Algorithm in reasoning about gcds:

For all positive integers m and n, $\gcd(m, n) = \gcd(m, n)$.

In particular, we can adapt the recursive case of the definition of $\gcd$ into:

$$\forall m, n \in \mathbb{Z}^+.\ \gcd(m, n) = \gcd(\text{rem}(m, n), n) \qquad \text{①}$$

and the previous part §4.2.3(d) (shifted to positive integers) into:

$$\forall m \in \mathbb{Z}^+.\ \gcd(F_{m+1}, F_m) = 1 \qquad \text{②}$$

Now, let n be a positive integer and k a natural number. Then,

$$\begin{aligned}
\gcd(F_{n+k+1}, F_n) &= \gcd(F_{n+1} \cdot F_{k+1} + F_n \cdot F_k, F_n) && \text{(by §4.2.3(b))} \\
&= \gcd(\mathrm{rem}(F_{n+1} \cdot F_{k+1} + F_n \cdot F_k, F_n), F_n) && \text{(by ①)} \\
&= \gcd(F_{n+1} \cdot F_{k+1}, F_n) && \text{(by §2.1.3(a))} \\
&= \gcd(F_{k+1}, F_n) && \text{(by §3.2.2 and ②)}
\end{aligned}$$

Secondly, we prove the following statement from which (ii) follows:

for all positive integers l, $P(l)$

where $P(l)$ is the statement:

for all positive integers m, n,
if `gcd0`(n, m) terminates in l steps then $\gcd(F_m, F_n) = F_{\gcd(m,n)}$

for `gcd0` the function from §3.3.3. The proof is by the Principle of Induction.

Base case: Let m, n be arbitrary positive integers. Assume that `gcd0`(m, n) terminates in 1 step. Then $m = n$ and $\gcd(F_m, F_n) = F_m = F_{\gcd(m,n)}$.

Inductive step: Let l be an arbitrary positive integer, and assume the Induction Hypothesis $P(l)$. Further, let m, n be arbitrary positive integers, and assume that `gcd0`(m, n) terminates in $l + 1$ steps Then, for $p = \min(m, n)$ and $q = \max(m, n)$, `gcd0`$(m, n) = $ `gcd0`$(p, q - p)$ and `gcd0`$(p, q - p)$ terminates in l steps. Thus, by the Induction Hypothesis, we have that $\gcd(F_{q-p}, F_p) = F_{\gcd(q-p,p)}$. Finally, since by the previous item, $\gcd(F_m, F_n) = \gcd(F_q, F_p) = \gcd(F_{q-p}, F_p)$ and $F_{\gcd(q-p,p)} = F_{\gcd(q,p)} = F_{\gcd(m,n)}$ we are done.

♪ One can intuitively deduce that property (ii) holds because we are performing the simplified Euclid's Algorithm (with repeated subtraction rather than remainder) on the indices of the Fibonacci number via a repeated application of property (i). This is indeed the case, but formulating this into a proof is far from obvious. Given that this is an exercise sheet on inductive proofs, we could try doing induction on m or n, only to notice that we can't make use of the inductive hypothesis in any meaningful way. Indeed, the "repetition" that we're trying to capture has nothing to with the numerical value of m or n directly, but rather the number of times we have to apply property (i) to compute their gcd. Given $m, n \in \mathbb{Z}^+$, we either cannot apply (i) because m and n are equal, or we can apply it once to get $\gcd(F_{m-n}, F_n)$, recursively apply it l more times to get $F_{\gcd(m-n,n)}$, and then "unapply" one step of `gcd0` to get $F_{\gcd(m,n)}$.

Extracting a strong enough induction hypothesis from this intuition is still nontrivial and requires us to explicitly refer to the termination of `gcd0`. Moreover, m and n

are universally quantified in the induction statement and the required property $\gcd(F_m, F_n) = F_{\gcd(m,n)}$ is made dependent on a termination hypothesis that refers to the induction variable l, rather than relating the two with a conjunction. This means that when proving the inductive case, we can *assume* that $\texttt{gcd0}(n, m)$ terminates in more than one step, and execute one step of the algorithm manually by applying property (i). It may take several attempts to construct sufficiently strong induction hypotheses, and as this exercise shows, they are not always as direct as case-analysing on a positive/nonnegative integer that is quantified over in the proposition.

f) Show that for all positive integers m and n, $(F_m \cdot F_n) \mid F_{m \cdot n}$ if $\gcd(m, n) = 1$.

Since m and n are coprime, §4.2.3(e) gives:

$$\gcd(F_m, F_n) = F_{\gcd(m,n)} = F_1 = 1$$

implying that F_m and F_n are themselves coprime. From §4.2.3(c) we know that $F_m \mid F_{m \cdot n}$ and $F_n \mid F_{m \cdot n}$. This, together with coprimality of F_m and F_n and §3.2.2 implies that $F_m \cdot F_n \mid F_{m \cdot n}$, as required.

g) Conjecture and prove theorems concerning the following sums for any natural number n:

(i) $\sum_{i=0}^{n} F_{2 \cdot i}$

After some test cases we conjecture the following identity:

$$\sum_{i=0}^{n} F_{2 \cdot i} = F_{2n+1} - 1$$

and prove it by the Principle of Induction.

Base case: $n = 0$. The sum consists of a single term $F_{2 \cdot 0} = F_0 = 0$, which equals $F_{2 \cdot 0 + 1} - 1 = F_1 - 1 = 0$.

Inductive step: $n = k + 1$. We assume the Induction Hypothesis

$$\sum_{i=0}^{k} F_{2 \cdot i} = F_{2k+1} - 1 \qquad \text{(IH)}$$

and prove that

$$\sum_{i=0}^{k+1} F_{2 \cdot i} = F_{2(k+1)+1} - 1$$

We can calculate as follows:

$$\sum_{i=0}^{k+1} F_{2 \cdot i} = F_{2 \cdot (k+1)} + \sum_{i=0}^{k} F_{2 \cdot i}$$
$$= F_{2k+2} + F_{2k+1} - 1 \qquad \text{(by (IH))}$$
$$= F_{2k+3} - 1 = F_{2(k+1)+1} - 1$$

(ii) $\sum_{i=0}^{n} F_{2 \cdot i + 1}$

We conjecture the following identity:

$$\sum_{i=0}^{n} F_{2 \cdot i+1} = F_{2n+2}$$

and prove it by the Principle of Induction.

Base case: $n = 0$. The sum consists of a single term $F_{2 \cdot 0+1} = F_1 = 1$, which equals $F_{2 \cdot 0+2} = F_2 = 1$.

Inductive step: $n = k + 1$. We assume the Induction Hypothesis

$$\sum_{i=0}^{k} F_{2 \cdot i+1} = F_{2k+2} \qquad \text{(IH)}$$

and prove that

$$\sum_{i=0}^{k+1} F_{2 \cdot i+1} = F_{2(k+1)+2}$$

We can calculate as follows:

$$\sum_{i=0}^{k+1} F_{2 \cdot i+1} = F_{2 \cdot (k+1)+1} + \sum_{i=0}^{k} F_{2 \cdot i+1}$$

$$= F_{2k+3} + F_{2k+2} \qquad \text{(by IH)}$$

$$= F_{2k+4} = F_{2(k+1)+2}$$

(iii) $\sum_{i=0}^{n} F_i$

We conjecture the following identity:

$$\sum_{i=0}^{n} F_i = F_{n+2} - 1$$

We can prove this by induction as before. Instead, we derive it from the previous two results by case-analysis on n:

Case $n = 2k$. If k is 0, the sum is $0 = F_{0+2} - 1$. Otherwise, the sum consists of the first k even Fibonacci numbers plus the first $(k-1)$ odd Fibonacci numbers:

$$\sum_{i=0}^{2k} F_i = \left(\sum_{i=0}^{k} F_{2 \cdot i} \right) + \left(\sum_{i=0}^{k-1} F_{2 \cdot i+1} \right) = F_{2k+1} + F_{2k} - 1 = F_{2k+2} - 1$$

Case $n = 2k + 1$. The sum consists of the sum of the first k even Fibonacci numbers plus the first k odd Fibonacci numbers:

$$\sum_{i=0}^{2k} F_i = \left(\sum_{i=0}^{k} F_{2 \cdot i} \right) + \left(\sum_{i=0}^{k} F_{2 \cdot i+1} \right) = F_{2k+1} - 1 + F_{2k+2} = F_{(2k+1)+2} - 1$$

4.3. Optional exercises

1. Recall the `gcd0` function from §3.3.3. Use the Principle of Mathematical Induction from basis 2 to formally establish the following correctness property of the algorithm:

> For all natural numbers $l \geq 2$, we have that for all positive integers m, n, if $m + n \leq l$ then `gcd0`(m, n) terminates.

As suggested, we proceed by Mathematical Induction from basis 2.

Base case: We need show that for all positive integers m, n, if $m + n \leq 2$ then `gcd0`(m, n) terminates. To this end, we let m and n be arbitrary positive integers, and assume that $m + n \leq 2$. Then, $m = n = 1$ and `gcd0`(m, n) terminates.

Inductive step: Let l be an arbitrary natural number greater than or equal 2, and assume the Induction Hypothesis

> For all positive integers m, n, if $m + n \leq l$ then `gcd0`(m, n) terminates.   (IH)

We need show that for all positive integers m, n, if $m+n \leq l+1$ then `gcd0`(m, n) terminates. To this end, we let a, b be arbitrary positive integers, assume that $a + b \leq l + 1$, and proceed to prove that `gcd0`(a, b) terminates.

We consider three cases.

- If $a = b$, then `gcd0`(a, b) terminates.

- If $a < b$, then `gcd0`$(a, b) = $ `gcd0`$(a, b - a)$. Moreover, by the Inductive Hypothesis (IH), we have that

$$\text{if } a + (b - a) \leq l \text{ then } \texttt{gcd0}(a, b - a) \text{ terminates,}$$

and since

$$a + (b - a) = b \ \leq \ l + 1 - a \ \leq \ l$$

it follows that `gcd0`$(a, b - a)$ terminates and therefore that so does `gcd0`(a, b).

- If $b < a$, then `gcd0`$(a, b) = $ `gcd0`$(a, a - b)$. Moreover, by the Inductive Hypothesis (IH), we have that

$$\text{if } b + (a - b) \leq l \text{ then } \texttt{gcd0}(a, a - b) \text{ terminates,}$$

and since

$$b + (a - b) = a \ \leq \ l + 1 - b \ \leq \ l$$

it follows that `gcd0`$(a, a - b)$ terminates and therefore that so does `gcd0`(a, b).

2. The set of *univariate polynomials* (over the rationals) on a variable x is defined as that of arithmetic expressions equal to those of the form $\sum_{i=0}^{n} a_i \cdot x^i$, for some $n \in \mathbb{N}$ and some *coefficients* $a_0, a_1, \ldots, a_n \in \mathbb{Q}$.

    (a) Show that if $p(x)$ and $q(x)$ are polynomials then so are $p(x) + q(x)$ and $p(x) \cdot q(x)$.

Let $p(x) = \sum_{i=0}^{m} a_i \cdot x^i$ and $q(x) = \sum_{j=0}^{n} b_j \cdot x^j$ be polynomials, and assume without loss of generality that $m > n$. For simplicity, we extend the coefficients a_i and b_j to all natural indices, with $a_i = 0$ for $m < i$ and $b_j = 0$ for $n < j$. Then, the sum $p(x) + q(x)$ is a polynomial (of degree m) because it is of the form:

$$p(x) + q(x) = \sum_{i=0}^{m} (a_i + b_i) \cdot x^i$$

where the coefficients $a_i + b_i$ are rational numbers since $\mathbb{Q}$ is closed under addition.

For the product $p(x) \cdot q(x)$, we calculate using the distributivity of multiplication over addition:

$$
\begin{aligned}
p(x) \cdot q(x) &= \left(\sum_{i=0}^{m} a_i \cdot x^i \right) \cdot \left(\sum_{j=0}^{n} b_j \cdot x^j \right) \\
&= \sum_{i=0}^{m} \left(a_i \cdot x^i \cdot \sum_{j=0}^{n} b_j \cdot x^j \right) \\
&= \sum_{i=0}^{m} \sum_{j=0}^{n} a_i \cdot x^i \cdot b_j \cdot x^j \\
&= \sum_{i=0}^{m} \sum_{j=0}^{n} a_i \cdot b_j \cdot x^{i+j}
\end{aligned}
$$

The number of terms in the sum of a fixed degree d will be equal to the number of ways one can construct d as a sum of an $i \leq m$ and a $j \leq n$; for example there will be at most one term of degree 0 or $m + n$, two terms of degree $1 = 1 + 0 = 0 + 1$ and $m + n - 1 = m + (n - 1) = (m - 1) + n$, three of degree 2 and $m + n - 2$ and so on. Terms of the same degree can be combined, with their coefficients getting added together. Using our extended coefficient indexing, the coefficient of the term of degree k can be concisely expressed as:

$$c_k = \sum_{j=0}^{k} a_j \cdot b_{k-j}$$

As expected, $c_0 = a_0 \cdot b_0$ (the constant terms), $c_{m+n} = a_0 \cdot b + m + n + \cdots + a_m \cdot b_n + \cdots + a_{m+n} b_0 = 0 + \cdots + a_m \cdot b_n + \cdots + 0$ (most of the coefficients are "out of range" and are 0) and $c_n = a_0 \cdot b_n + a_1 \cdot b_{n-1} + \cdots + a_n \cdot b_0$ (n nonzero coefficients). Since these are all rational numbers, the product of two polynomials is indeed a polynomial (of degree $m + n$) because it is of the form:

$$p(x) \cdot q(x) = \sum_{k=0}^{m+n} c_k \cdot x^k$$

(b) Deduce as a corollary that, for all $a, b \in \mathbb{Q}$, the linear combination $a \cdot p(x) + b \cdot q(x)$ of two polynomials $p(x)$ and $q(x)$ is a polynomial.

Every rational number a can be seen as a polynomial of degree 0, with its only coefficient being a. Thus, $a \cdot p(x)$ is a product of polynomials and hence is a polynomial. The sum of two such expressions is still a polynomial, so we can conclude that the linear combination $a \cdot p(x) + b \cdot q(x)$ of two polynomials for $a, b \in \mathbb{Q}$ is a polynomial.

(c) Show that there exists a polynomial $p_2(x)$ such that $p_2(n) = \sum_{i=0}^{n} i^2 = 0^2 + 1^2 + \cdots + n^2$ for every $n \in \mathbb{N}$.[1]

Hint: Note that for every $n \in \mathbb{N}$,

$$(n+1)^3 = \sum_{i=0}^{n}(i+1)^3 - \sum_{i=0}^{n} i^3$$

The required polynomial is

$$p_2(n) = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n$$

We show that this is a sum of squares for any $n \in \mathbb{N}$ by induction.

Base case: $n = 0$. The polynomial reduces to 0, which is the sum of the square number $0 = 0^2$.

Inductive step: $n = k + 1$. Assume the Induction Hypothesis:

$$p_2(k) = \frac{1}{3}k^3 + \frac{1}{2}k^2 + \frac{1}{6}k = \sum_{i=0}^{k} i^2 \qquad \text{(IH)}$$

We need to prove that

$$p_2(k+1) = \sum_{i=0}^{k+1} i^2$$

The polynomial expands as follows:

$$
\begin{aligned}
p_2(k+1) &= \frac{1}{3}(k+1)^3 + \frac{1}{2}(k+1)^2 + \frac{1}{6}(k+1) \\
&= \frac{1}{3}k^3 + k^2 + k + \frac{1}{3} + \frac{1}{2}k^2 + k + \frac{1}{2} + \frac{1}{6}k + \frac{1}{6} \\
&= \left(\frac{1}{3}k^3 + \frac{1}{2}k^2 + \frac{1}{6}k \right) + k^2 + 2k + \frac{1}{3} + \frac{1}{2} + \frac{1}{6} \\
&= \sum_{i=0}^{k} i^2 + (k^2 + 2k + 1) \qquad \text{(by (IH))} \\
&= \sum_{i=0}^{k} i^2 + (k+1)^2 = \sum_{i=0}^{k+1} i^2
\end{aligned}
$$

Thus $p_2(k+1)$ is the sum of consecutive squares, as required.

---

[1] Chapter 2.5 of *Concrete Mathematics* by R.L. Graham, D.E. Knuth and O. Patashnik looks at this in great detail.

♪ As is usual with existence proofs, the hard work is done behind the scenes and we start off the formal proof by magically producing a witness that just so happens to satisfy the required property. The required witness for the existence was calculated from the supplied hint:

$$(n+1)^3 = \sum_{i=0}^{n}(i+1)^3 - \sum_{i=0}^{n}i^3$$

$$= \sum_{i=0}^{n}(i^3 + 3i^2 + 3i + 1) - \sum_{i=0}^{n}i^3$$

$$= \left(\sum_{i=0}^{n}3i^2 + 3i + 1\right) + \sum_{i=0}^{n}i^3 - \sum_{i=0}^{n}i^3$$

$$= \sum_{i=0}^{n}3i^2 + 3i + 1 = 3 \cdot \sum_{i=0}^{n}i^2 + \sum_{i=0}^{n}3i + 1$$

Rearranging, we get that

$$\sum_{i=0}^{n}i^2 = \frac{1}{3}\left((n+1)^3 - \sum_{i=0}^{n}3i + 1\right)$$

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

$$= \frac{1}{3}n^3 + n^2 + n + \frac{1}{3} - \frac{1}{3}n - \frac{1}{3} - \frac{1}{2}n^2 + \frac{1}{2}n$$

$$= \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n$$

Now, we suspect that this is the right answer, but the formal proof should start with the statement of the answer followed by a proof that it satisfies the required property. This is especially important in this case, when the proposed witness was calculated using the (unverified) hint; separately proving that the polynomial is a sum of squares makes our answer independent of the hint. The formal proof may well be done using a different technique (in this case, induction), but it should not present any unpleasant surprises since our proposed witness is almost certainly correct.

Of course, the statement for this question is a rather obfuscated way of saying "find a formula for the sum of the first n square numbers". You may already have it memorised as

$$\sum_{i=0}^{n}i^2 = \frac{n(n+1)(2n+1)}{6}$$

Multiplying things out indeed leads to the formula for the polynomial $p_2(n)$ we had above. Even if we recognise this shortcut (instead of deriving it from the hint), we still need to prove that the formula works – this is still best accomplished using induction.

(d) Show that, for every $k \in \mathbb{N}$, there exists a polynomial $p_k(x)$ such that, for all $n \in \mathbb{N}$, $p_k(n) = \sum_{i=0}^{n}i^k = 0^k + 1^k + \cdots + n^k$.

Hint: Generalise the hint above, and the similar identity

$$(n+1)^2 = \sum_{i=0}^{n}(i+1)^2 - \sum_{i=0}^{n}i^2$$

For $k \in \mathbb{N}$, $P(k)$ be the statement

> There exists a polynomial $p_k(x)$ such that, for all $n \in \mathbb{N}$, $p_k(n) = \sum_{i=0}^{n} i^k$.

We prove this by the Principle of Strong Induction.

Base case: The polynomial needs to satisfy $p_0(n) = \sum_{i=0}^{n} i^0$; since $i^0 = 1$, this is simply equal to $p_0(n) = n + 1$, which is a polynomial.

Inductive step: Assume the Strong Induction Hypothesis: for all $0 \le l \le k$,

$$\text{there exists a polynomial } p_l(x) \text{ such that, for all } n \in \mathbb{N}, \ p_l(n) = \sum_{i=0}^{n} i^l. \qquad \text{(IH)}_S$$

We need to show that $P(k+1)$ holds, that is

> there exists a polynomial $p_{k+1}(x)$ such that, for all $n \in \mathbb{N}$, $p_{k+1}(n) = \sum_{i=0}^{n} i^{k+1}$

The required witness of existence is

$$p_{k+1}(n) = \frac{1}{k+2}\left((n+1)^{k+2} - \sum_{j=0}^{k} \binom{k+2}{j} \cdot p_j(n) \right) \qquad \text{(E)}$$

This is indeed a polynomial since:

- $p_j(n)$ is a polynomial for all $0 \le j \le k$ by the Strong Induction Hypotheses, and $\sum_{j=0}^{k} \binom{k+2}{j} p_j(n)$ is a linear combination of polynomials which is a polynomial;

- $(n+1)^{k+1}$ can be expanded using the Binomial Theorem into a sum of powers of n with binomial coefficients, so it too is a polynomial;

- the sum of two polynomials is a polynomial, and $\frac{1}{k+2}$ is a rational coefficient.

We prove that $p_{k+1}(n) = \sum_{i=0}^{n} i^{k+1}$ for all $n \in \mathbb{N}$ by induction on n.

Base case: As before, $p_{k+1}(0) = 0$.

Inductive step: Assume the Induction Hypothesis

$$p_{k+1}(n) = \sum_{i=0}^{n} i^{k+1} \qquad \text{(IH)}$$

and prove that

$$p_{k+1}(n+1) = \sum_{i=0}^{n+1} i^{k+1}$$

First, we note the following two calculations:

$$(n+2)^{k+2} = ((n+1)+1)^{k+2} = \sum_{i=0}^{k+2} \binom{k+2}{i}(n+1)^i \qquad \text{(Binomial Theorem)}$$

$$= (n+1)^{k+2} + (k+2) \cdot (n+1)^{k+1} + \sum_{i=0}^{k} \binom{k+2}{i}(n+1)^i \quad \text{(extract two summands)}$$

$$\sum_{j=0}^{k} \binom{k+2}{j} \cdot p_j(n+1)$$

$$= \sum_{j=0}^{k} \binom{k+2}{j} \cdot \sum_{a=0}^{n+1} a^j = \sum_{a=0}^{n+1}\sum_{j=0}^{k} \binom{k+2}{j} \cdot a^j \qquad \text{(by ⒤$_S$ and distributivity)}$$

$$= \sum_{j=0}^{k} \binom{k+2}{j} \cdot (n+1)^j + \sum_{a=0}^{n}\sum_{j=0}^{k} \binom{k+2}{j} \cdot a^j \qquad \text{(extract last summand)}$$

Combining the two, we have that

$$(n+2)^{k+2} - \sum_{j=0}^{k} \binom{k+2}{j} \cdot p_j(n+1)$$

$$= (n+1)^{k+2} + (k+1) \cdot (n+1)^{k+1} - \sum_{a=0}^{n}\sum_{j=0}^{k} \binom{k+2}{j} \cdot a^j \qquad \qquad ①$$

Now we are ready to expand the polynomial of the inductive step:

$$p_{k+1}(n+1)$$

$$= \frac{1}{k+2}\left((n+2)^{k+2} - \sum_{j=0}^{k} \binom{k+2}{j} \cdot p_j(n+1) \right)$$

$$= \frac{1}{k+2}\left((n+1)^{k+2} + (k+2) \cdot (n+1)^{k+1} - \sum_{a=0}^{n}\sum_{j=0}^{k} \binom{k+2}{j} \cdot a^j \right) \qquad \text{(by ①)}$$

$$= \frac{1}{k+2}\left((n+1)^{k+2} - \sum_{a=0}^{n}\sum_{j=0}^{k} \binom{k+2}{j} \cdot a^j \right) + (n+1)^{k+1}$$

$$= \frac{1}{k+2}\left((n+1)^{k+2} - \sum_{j=0}^{k} \binom{k+2}{j} \cdot \sum_{a=0}^{n} a^j \right) + (n+1)^{k+1}$$

$$= \frac{1}{k+2}\left((n+1)^{k+2} - \sum_{j=0}^{k} \binom{k+2}{j} \cdot p_j(n) \right) + (n+1)^{k+1} \qquad \text{(by ⒤$_S$)}$$

$$= p_{k+1}(n) + (n+1)^{k+1} = \sum_{i=0}^{n} i^{k+1} + (n+1)^{k+1} = \sum_{i=0}^{n+1} i^{k+1} \qquad \text{(by Ⓔ and ⒤)}$$

Thus, we have shown (by the nested Mathematical Induction) that our definition of

$p_{k+1}(n)$ by Ⓔ indeed satisfies $p_{k+1}(n) = \sum_{i=0}^{n} i^{k+1}$ for all $n \in \mathbb{N}$. Then, by the outer Strong Induction, we can conclude that there exists a polynomial $p_k(n)$ for all $k \in \mathbb{N}$ that satisfies $p_k(n) = \sum_{i=0}^{n} i^k$ for all $n \in \mathbb{N}$.

♪ Once again, we found the witness Ⓔ by calculating backwards from the (conjectured) generalisation of the hint

$$(n+1)^k = \sum_{i=0}^{n}(i+1)^k - \sum_{i=0}^{n} i^k$$

We *could* prove that this holds, but we can also use it without proof to derive the witness, as long as we then formally show that the witness is correct. Given that the property is only used behind the scenes as an "educated guess", it will not invalidate the proof even if the conjecture is actually incorrect. The calculation of the witness is as follows:

$$(n+1)^{k+2} = \sum_{m=0}^{n}(m+1)^{k+2} - \sum_{m=0}^{n} m^{k+2}$$

$$= \left(\sum_{m=0}^{n}\sum_{j=0}^{k+2}\binom{k+2}{j} \cdot m^j\right) - \sum_{m=0}^{n} m^{k+2} \qquad \text{(Binomial Theorem)}$$

$$= \left(\sum_{j=0}^{k+2}\sum_{m=0}^{n}\binom{k+2}{j} \cdot m^j\right) - \sum_{m=0}^{n} m^{k+2} \qquad \text{(commute summation)}$$

$$= \sum_{j=0}^{k+1}\sum_{m=0}^{n}\binom{k+2}{j} \cdot m^j \qquad \text{(subtract last summand)}$$

$$= \sum_{m=0}^{n}\binom{k+2}{k+1} \cdot m^{k+1} + \sum_{j=0}^{k}\sum_{m=0}^{n}\binom{k+2}{j} \cdot m^j \qquad \text{(extract last summand)}$$

$$= (k+2)\sum_{m=0}^{n} m^{k+1} + \sum_{j=0}^{k}\binom{k+2}{j} \cdot \sum_{m=0}^{n} m^j \qquad \text{(binom. coefficient)}$$

$$= (k+2)\sum_{m=0}^{n} m^{k+1} + \sum_{j=0}^{k}\binom{k+2}{j} \cdot p_j(n) \qquad (\text{ⒾⒽ}_S)$$

We rearrange this to get $\sum_{m=0}^{n} m^{k+1}$ and set that as the witness formula for $p_{k+1}(n)$.

♪ This proof is a rather involved example of a nested, mixed induction proof: we do strong induction over $k \in \mathbb{N}$ and mathematical induction over $n \in \mathbb{N}$ when proving that our proposed witness Ⓔ for $p_{k+1}(n)$ (the inductive case of the outer induction) is correct. The strong induction hypothesis ⒾⒽ_S is used throughout the proof, both in the derivation of the witness and the proof of its correctness.

♪ Note that we haven't actually constructed a closed-form expression for $p_k(n)$, but a recursive algorithm for computing it from formulae for lower degrees. Importantly, we established that the recursive expression is indeed a polynomial using the clos-

ure properties proved in earlier parts. This is sufficient to prove that there exists a polynomial expression for $\sum_{i=0}^{n} i^k$, but of course one has to do quite some additional work to extract the degree and the coefficients of the polynomial from the recursive construction. The general, closed-form expression is known as Faulhaber's Formula and features the Bernoulli numbers, a rather irregular-looking sequence of rational numbers used throughout mathematics; for instance, $B_{14} = \frac{7}{6}, B_{15} = 0, B_{16} = -\frac{3617}{510}$.