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.

   Proof by induction:

   When $n = 3$, the 3 points on the circle join up to form a triangle.
   The interior angles of a triangle sum to $180°$.

   $$\begin{aligned} &180 \cdot (3-2) \\ =&180 \cdot 1 \\ =&180 \end{aligned} \tag{1}$$

   So the statement holds for $n = 3$.

   Assume that the statement holds for $n = k$.
   Joining $k+1$ points on the circle forms a shape with $k+1$ sides.
   If we join the k^{th} point and the 0^{th} point then we see that the $k+1$ sided shape can be decomposed into a k sided shape and a triangle.
   Since we have not changed the outer part of the shape, the sum of the interior angles is unchanged.
   By assumption the sum of the interior angles in the k sided shape is $180 \cdot (k-2)$. The sum of the interior angles of a triangle is 180. So the sum of the interior angles of the $k+1$ sided shape is:

   $$\begin{aligned} &180 \cdot (k-2)° + 180° \\ =&180 \cdot ((k+1)-2)° \end{aligned} \tag{2}$$

   So if the statement holds for $n = k$ then it also holds for $n = k+1$. Since the statement holds for $n = 3$, by induction it must also hold for all $n \geq 3$.

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

   Proof by induction:

   At $n = 0$: At $n = 0$ the grid is sized 1×1. If you remove 1 square then there are 0 squares to fill with L-shaped pieces. Hence the grid has been filled with L-shaped pieces.

   Assume that we can fill the grid with L-shaped pieces after removing one piece at $n = k$.
   Since we can fill the grid with L-shaped pieces after removing one piece at $n = k$, there is one empty piece. So if we have three $2^k \times 2^k$ grids, then there are three empty pieces.
   We can place the three $2^k \times 2^k$ grids next to each other (in an L-shape) so that the three gaps are next to each other in an L-shape. We can hence place a L-shaped block in there and connect them. We now place another $2^k \times 2^k$ grid so that the four grids are now in a square. This square has side length $2 \cdot 2^k = 2^{k+1}$ and height $2 \cdot 2^k = 2^{k+1}$.
   Therefore it is a square grid of size $2^{k+1} \times 2^{k+1}$.

   So if the statement holds for $n = k$ then it also holds for $n = k+1$. Since it holds for $n = 0$, by induction it must also hold for all $n \in \mathbb{N}$.

4.2 Core exercises

1. Establish the following

(a) For all positive integers m and n,

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

$$\begin{aligned}
&(2^n - 1) \cdot \sum_{i=0}^{m-1} 2^{i \cdot n} = (2^n - 1) \cdot (2^{m \cdot n - n} + 2^{m \cdot n - 2 \cdot n} + \cdots + 1) \iff \\
&(2^n - 1) \cdot \sum_{i=0}^{m-1} 2^{i \cdot n} = 2^n \cdot 2^{m \cdot n - n} + 2^n \cdot 2^{m \cdot n - 2 \cdot n} + \cdots + 2^n \cdot 1 - 2^{m \cdot n - n} - 2^{m \cdot n - 2 \cdot n} - \cdots - 1 \iff \\
&(2^n - 1) \cdot \sum_{i=0}^{m-1} 2^{i \cdot n} = 2^{m \cdot n} + 2^{m \cdot n - n} + \cdots + 2^n - 2^{m \cdot n - n} - 2^{m \cdot n - 2 \cdot n} - \cdots - 1 \iff \\
&(2^n - 1) \cdot \sum_{i=0}^{m-1} 2^{i \cdot n} = 2^{m \cdot n} + 2^{m \cdot n - n} - 2^{m \cdot n - n} + \cdots + 2^n - 2^n - 1 \iff \\
&(2^n - 1) \cdot \sum_{i=0}^{m-1} 2^{i \cdot n} = 2^{m \cdot n} - 1 \text{ as required}
\end{aligned} \tag{4}$$

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

$$\begin{aligned}
k \text{ is not prime} &\iff \\
\exists m, n \in \mathbb{Z}^+ : k = m \cdot n &\iff \\
\exists m, n \in \mathbb{Z}^+ : 2^k - 1 = 2^{m \cdot n} - 1 &\iff \\
\exists m, n \in \mathbb{Z}^+ : 2^k - 1 = (2^n - 1) \cdot \sum_{i=0}^{m-1} 2^{i \cdot n} \text{ using (4)} &\iff \\
\exists n \in \mathbb{Z}^+ : 2^n - 1 | 2^k - 1 &\iff \\
2^k \text{ is not prime as required}
\end{aligned} \tag{5}$$

2. Prove that

$$\forall n \in \mathbb{N} : \forall x \in \mathbb{R} : x \geq -1 \implies (1 + x)^n \geq 1 + n \cdot x \tag{6}$$

At $n = 0$

$$\begin{aligned}
&(1 + x)^n \\
=&1 \\
\geq&1 + 0 \cdot x
\end{aligned} \tag{7}$$

So the expression holds true at $n = 0$.

Assume the expression holds at $n = k$. So $(1 + x)^k \geq 1 + k \cdot x$

$$\begin{aligned}
(1 + x)^{k+1} &= (1 + x) \cdot (1 + x)^k \\
&\geq (1 + x) \cdot (1 + k \cdot x) \\
&= 1 + k \cdot x + x + k \cdot x^2 \\
&= 1 + (k + 1) \cdot x + x^2 \\
&\geq 1 + (k + 1) \cdot x \text{ since } \forall x \in \mathbb{Z} : x^2 \geq 0
\end{aligned} \tag{8}$$

So if the expression holds at $n = k$ then by it also holds at $n = k + 1$. Since the expression holds for $n = 0$, by induction, it must also hold for all $n \in \mathbb{N}$. As required.

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) Provve Cassani's Identity: for all $n \in \mathbb{N}$,

$$F_n \cdot F_{n+2} = F_{n+1}^2 + (-1)^{n+1} \tag{9}$$

   At $n = 0$:

$$\begin{aligned} & F_n \cdot F_{n+2} \\ =& 0 \cdot 1 \\ =& 0 \\ =& 1 - 1 \\ =& F_2^2 + (-1)^{n+1} \end{aligned} \tag{10}$$

   So the expression holds true for $n = 0$.

   Assume that the expression holds true for $n = k$.

$$\begin{aligned} F_k \cdot F_{k+2} = F_{k+1}^2 + (-1)^{k+1} \iff \\ (F_{k+2} - F_{k+1}) \cdot (F_{k+3} - F_{k+1}) = F_{k+1}^2 + (-1)^{k+1} \iff \\ F_{k+2} \cdot F_{k+3} - F_{k+2} \cdot F_{k+1} - F_{k+1} \cdot F_{k+3} + F_{k+1}^2 = F_{k+1}^2 + (-1)^{k+1} \iff \\ F_{k+2} \cdot (F_{k+3} - F_{k+1}) - F_{k+1} \cdot F_{k+3} = (-1)^{k+1} \iff \\ F_{k+2}^2 - F_{k+1} \cdot F_{k+3} = (-1)^{k+1} \iff \\ -F_{k+1} \cdot F_{k+3} = -F_{k+2}^2 + (-1)^{k+1} \iff \\ F_{k+1} \cdot F_{k+3} = F_{k+2}^2 + (-1)^{k+2} \end{aligned} \tag{11}$$

   So if the expression is true at $n = k$ then it is also true at $n = k + 1$. Since the expression is true for $n = 0$, by induction it must also be true for all $n \in \mathbb{N}$.

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

$$F_{n+k+1} = F_{n+1} \cdot F_{k+1} + F_n \cdot F_k \tag{12}$$

   At $n = 0$:

$$\begin{aligned} & F_{n+k+1} \\ =& F_{k+1} \\ & F_{n+1} \cdot F_{k+1} + F_n \cdot F_k \\ =& F_1 \cdot F_{k+1} + F_0 \cdot F_k \\ =& 1 \cdot F_{k+1} + 0 \cdot F_k \\ =& F_{k+1} \end{aligned} \tag{13}$$

   So the statement is true for $n = 0$.

At $n = 1$.

$$\begin{aligned} & F_{n+k+1} \\ =& F_{k+2} \\ & F_{n+1} \cdot F_{k+1} + F_n \cdot F_k \\ & F_2 \cdot F_{k+1} + F_1 \cdot F_k \\ =& 1 \cdot F_{k+1} + 1 \cdot F_k \\ =& F_{k+1} + F_k \\ =& F_{k+2} \end{aligned} \tag{14}$$

So the statement is true for $n = 1$.

Assume that it is also true for arbitrary k at $n = i$ and $n = i - 1$.

$$\begin{aligned} \text{Assume: } F_{i+k} &= F_i \cdot F_{k+1} + F_{i-1} \cdot F_k \\ \text{Assume: } F_{i+k+1} &= F_{i+1} \cdot F_{k+1} + F_i \cdot F_k \\ F_{i+k+1} + F_{i+k} &= F_{i+1} \cdot F_{k+1} + F_i \cdot F_{k+1} + F_i \cdot F_k + F_{i-1} F_k \iff \\ F_{i+k+2} &= (F_{i+1} + F_i) \cdot F_{k+1} + (F_i + F_{i-1}) \cdot F_k \iff \\ F_{i+k+2} &= F_{i+2} \cdot F_{k+1} + F_{i+1} \cdot F_k \iff \\ F_{(i+1)+k+1} &= F_{(i+1)+1} \cdot F_{k+1} + F_{(i+1)} \cdot F_k \end{aligned} \tag{15}$$

So if the statement holds for $n = i$ and $n = i - 1$ at arbitrary k then it also holds for arbitrary k and $n = i + 1$.

An analagous proof can be made for k.

Since the statement is true for $n, k \in \{0, 1\}$ and the truth of the statement at $n = i - 1$ and $n = i$ implies the proof of the statement at $n = i + 1$ and the truth of the statement at $k = j - 1$ and $k = j$ implies the proof of the statement at $k = j + 1$ we can conclude by multivariate induction that the statement is true for all $n, k \in \mathbb{N}$.

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

$$F_{n \cdot l} = F_n \cdot F_{n+l} \iff \tag{16}$$

At $n = 0$ for constant l:

$$\begin{aligned} & F_n = 0 \land F_{l \cdot n} = F_0 = 0 \iff \\ & 0|0 \iff \\ & F_n | F_{l \cdot n} \end{aligned} \tag{17}$$

Assume that the identity also holds at $n = k$:

$$\begin{aligned} \text{Assume: } & F_k | F_{l \cdot k} \iff \\ \exists a \in \mathbb{Z} : & a \cdot F_k = F_{l \cdot k} \\ & \text{Using (12):} \\ & F_{l \cdot (k+1)} = F_{l \cdot k} \cdot F_{k+1} + F_{l \cdot k - 1} \cdot F_k \iff \\ \exists a \in \mathbb{Z} : & F_{l \cdot (k+1)} = a \cdot F_k \cdot F_{k+1} + F_{l \cdot k - 1} \cdot F_k \iff \\ \exists a \in \mathbb{Z} : & F_{l \cdot (k+1)} = F_k (a \cdot F_{k+1} + F_{l \cdot k - 1}) \iff \\ & F_k | F_{l \cdot (k+1)} \end{aligned} \tag{18}$$

So if the expression holds at $n = k$ then it also holds at $n = k + 1$. Since the expression holds at $n = 0$; by induction it must also hold for all $n \in \mathbb{N}$. As required.

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

At $n = 0$:

$$\begin{aligned} &\gcd(F_2, F_1) \\ =&\gcd(1, 1) \\ =&1 \end{aligned} \tag{19}$$

So the expression holds at $n = 1$

Assume it also holds for $n = k$.

$$\begin{aligned} \text{Assume: } \gcd(F_{k+2}, F_{k+1}) = 1 &\iff \\ \gcd(F_{k+2}, F_{k+1} + F_{k+2}) = 1 &\iff \\ \gcd(F_{k+2}, F_{k+3}) = 1 &\iff \\ \gcd(F_{k+3}, F_{k+2}) = 1 & \end{aligned} \tag{20}$$

So if the expression for $n = k$ then it also holds for $n = k+1$. Since $\gcd(F_2, F_1) = 1$, by induction it must also hold for all $n \in \mathbb{Z}^+$.

Let # signify the number of steps until termination.

At $n = 0$:

$$\begin{aligned} \#\gcd(F_2, F_1) &= \#\gcd(1, 1) \\ &= 0 \end{aligned} \tag{21}$$

So it terminates in 0 steps. So the algorithm terminates in n steps for $n = 0$.

Assume that it terminates in k steps for $n = k$:

$$\begin{aligned} &\text{Assume: } \#\gcd(F_{k+2}, F_{k+1}) = k \\ &\quad \#\gcd(F_{(k+1)+2}, F_{(k+1)+1}) = \#\gcd(F_{k+3}, F_{k+2}) \iff \\ &\quad \#\gcd(F_{(k+1)+2}, F_{(k+1)+1}) = \#\gcd(F_{k+2}, F_{k+3} - F_{k+2}) + 1 \iff \\ &\quad \#\gcd(F_{(k+1)+2}, F_{(k+1)+1}) = \#\gcd(F_{k+2}, F_{k+1}) + 1 \iff \\ &\quad \#\gcd(F_{(k+1)+2}, F_{(k+1)+1}) = (k + 1) \iff \end{aligned} \tag{22}$$

So if $\#\gcd(F_{k+2}, F_{k+1}) = k$ then $\#\gcd(F_{k+3}, F_{k+2}) = k+1$. Since $\#\gcd(F_2, F_1) = 0$, by induction the algorithm must terminate in n steps for all $n \in \mathbb{N}$.

$$\text{So } \gcd(F_{n+2}, F_{n+1}) \text{ terminates with output 1 in } n \text{ steps for all positive integers } n \text{ as required.} \tag{23}$$

(e) Deduce also that:

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

$$\begin{aligned} \text{Using (12): } F_m = F_{n+1} \cdot F_{m-n} + F_n \cdot F_{m-n-1} &\iff \\ \gcd(F_m, F_n) = \gcd(F_{n+1} \cdot F_{m-n} + F_n \cdot F_{m-n-1}, F_n) &\iff \\ \gcd(F_m, F_n) = \gcd(F_{n+1} \cdot F_{m-n}, F_n) &\iff \\ (\text{Using (23): } \gcd(F_{n+1}, F_n) = 1) \wedge (\gcd(a, c) = 1 \implies \gcd(a \cdot b, c) = \gcd(b, c)) &\iff \\ \gcd(F_m, F_n) = \gcd(F_{m-n}, F_n) \text{ as required} & \end{aligned} \tag{24}$$

and hence that:

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

If initially we start with F_{m_0} and F_{n_0} then at the next stage we will have F_{m_1} and F_{n_1} where m_1 and n_1 are the next stages in gcd0. Since we know that gcd0 will terminate when $m = n = \gcd(m, n)$: we know that $\gcd(F_m, F_n)$ will terminate when $m = n = \gcd(m, n)$. So $\gcd(F_n, F_m) = F_{\gcd(n,m)}$ as required.

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

$$\begin{gathered}\gcd(m,n) = 1 \iff \\ \gcd(F_m, F_n) = 1 \text{ by (e)(ii)} \iff \\ (F_m \cdot F_n)|F_{m\cdot n} \implies \\ F_m|F_{m\cdot n} \wedge F_n|F_{m\cdot n}\end{gathered} \tag{25}$$

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

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

Prove:

$$\sum_{i=0}^{n} F_{2\cdot i} = F_{2\cdot n+1} - 1 \tag{26}$$

At $n = 0$:

$$\begin{gathered}\sum_{i=0}^{n} F_{2\cdot i} = 0 \iff \\ \sum_{i=0}^{n} F_{2\cdot i} = 1 - 1 \iff \\ \sum_{i=0}^{n} F_{2\cdot i} = F_1 - 1 \iff \\ \sum_{i=0}^{n} F_{2\cdot i} = F_{2\cdot n+1} - 1\end{gathered} \tag{27}$$

So the expression is true at $n = 0$.

Assume that it is also true at $n = k$:

$$\begin{gathered}\sum_{i=0}^{k} F_{2\cdot i} = F_{2\cdot k+1} - 1 \iff \\ \sum_{i=0}^{k} F_{2\cdot i} + F_{2\cdot(k+1)} = F_{2\cdot k+1} + F_{2\cdot k+2} - 1 \iff \\ \sum_{i=0}^{k} F_{2\cdot i} + F_{2\cdot(k+1)} = F_{2\cdot k+1} + F_{2\cdot k+2} - 1 \iff \\ \sum_{i=0}^{k+1} F_{2\cdot i} = F_{2\cdot k+3} - 1 \iff \\ \sum_{i=0}^{k+1} F_{2\cdot i} = F_{2\cdot(k+1)+1} - 1\end{gathered} \tag{28}$$

So if the expression holds at $n = k$ then it also holds at $n = k + 1$. Since the expression holds at $n = 0$ then by induction it must also hold for all $n \in \mathbb{N}$ as required.

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

$$\sum_{i=0}^{n} F_{2\cdot i+1} = F_{2\cdot n+2} - 1 \tag{29}$$

At $n = 0$:

$$\begin{aligned}\sum_{i=0}^{n} F_{2\cdot i+1} &= 1 \iff \\ \sum_{i=0}^{n} F_{2\cdot i+1} &= F_2 \iff \\ \sum_{i=0}^{n} F_{2\cdot i+1} &= F_{2\cdot n+2}\end{aligned} \tag{30}$$

So the expression is true at $n = 0$.

Assume that it is also true at $n = k$:

$$\begin{aligned}\sum_{i=0}^{k} F_{2\cdot i+1} &= F_{2\cdot k+2} \iff \\ \sum_{i=0}^{k} F_{2\cdot i+1} + F_{2\cdot(k+1)+1} &= F_{2\cdot k+2} + F_{2\cdot(k+1)+1} \iff \\ \sum_{i=0}^{k+1} F_{2\cdot i+1} &= F_{2\cdot(k+1)+2}\end{aligned} \tag{31}$$

So if the expression holds at $n = k$ then it also holds at $n = k + 1$. Since the expression holds at $n = 0$ then by induction it must also hold for all $n \in \mathbb{N}$ as required.

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

$$\sum_{i=0}^{n} F_i = F_{2\cdot n+3} - 1 \tag{32}$$

$$\begin{aligned}\sum_{i=0}^{n} F_i &= \sum_{i=0}^{n} F_{2\cdot i} + \sum_{i=0}^{n} F_{2\cdot i+1} \iff \\ \sum_{i=0}^{n} F_i &= (F_{2\cdot n+1} - 1) + F_{2\cdot n+2} \text{ using (26), (29)} \iff \\ \sum_{i=0}^{n} F_i &= (F_{2\cdot n+1} + F_{2\cdot n+2}) - 1 \iff \\ \sum_{i=0}^{n} F_i &= F_{2\cdot n+3} - 1 \iff\end{aligned} \tag{33}$$

As required.

4.3 Optional exercises

1. 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 $\text{gcd0}(m, n)$ terminates.

At $l = 2$:

$$\begin{aligned} m, n \in \mathbb{Z}^+ \wedge m + n \leq 2 \implies \\ m, n = 1 \implies \\ \text{gcd0}(m, n) = 1 \end{aligned} \tag{34}$$

So the property is correct for $l = 2$

Assume that the property is also correct for $l = k$:

$$\text{Assume: } \forall m, n \in \mathbb{Z}^+ : m + n \leq k \implies \exists g \in \mathbb{Z} : \text{gcd0}(m, n) = g \tag{35}$$

So for $l = k + 1$:

$$\begin{aligned} & m + n < k + 1 \vee m + n = k + 1 \iff \\ & m + n \leq k \vee m + n = k + 1 \end{aligned} \tag{36}$$

From the assumption we know that if $m + n \leq k$ then gcd0 terminates.
So we need only consider the case where $m + n = k + 1$.

We can divide this into two cases: $m = n \vee m \neq n$.

Case $m = n$:

$$m = n \implies \text{gcd0}(m, n) = m \tag{37}$$

So in the first case the algorithm terminates.

Case $m \neq n$:
Without loss of generality assume that $m > n$.

$$\text{gcd0}(m, n) = \text{gcd0}(n, m - n) \tag{38}$$

However, since $n \geq 1$: $n + m - n \leq k$ and so by assumption gcd0 must terminate for this input.

So if gcd0 terminates for $m+n \leq k$ then it must also terminate for $m+n \leq k+1$. Since gcd0 terminates for $l = 2$, by induction it must terminate for all $l \geq 2$ as required.

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 $a_0, a_1, \cdots, a_n \in \mathbb{Q}$.

   (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 $p(x)$ have degree m such that $p(x) = \sum_{i=0}^{m} c_i \cdot x^i$ and $q(x)$ have degree n such that $q(x) = \sum_{i=0}^{n} d_i \cdot x^i$.
   Without loss of generality, assume that $m \geq n$.
   Let $q'(x) = \sum_{i=0}^{m} e_i \cdot x^i$ such that $(e_i \leq n \implies e_i = d_i) \wedge (e_i > n \implies c_i = 0)$.
   Therefore $q'(x)$ is the same as $q(x)$.

$$\begin{aligned} & p(x) + q(x) \\ = & p(x) + q'(x) \\ = & \sum_{i=0}^{m} c_i \cdot x^i + \sum_{i=0}^{m} e_i \cdot x^i \\ = & \sum_{i=0}^{m} (c_i + e_i) \cdot x^i \end{aligned} \tag{39}$$

Which is the formula for a univariate polynomial where $a_i = c_i + e_i$. So if $p(x)$ and $q(x)$ are univariate polynomials, then $p(x) + q(x)$ is also a univariate polynomial. As required.

$$\begin{aligned}
p(x) \cdot q(x) &= \sum_{i=0}^{m} c_i \cdot x^i \cdot \sum_{j=0}^{n} d_j \cdot x^j \iff \\
p(x) \cdot q(x) &= \sum_{i=0}^{m} \sum_{j=0}^{n} c_i \cdot d_j \cdot x^{i+j} \iff \\
p(x) \cdot q(x) &= \sum_{i=0}^{m} f_i(x) \text{ where } f_i(x) \text{ is a univariate polynomial}
\end{aligned} \tag{40}$$

Using (39) we know that the sum of univariate polynomials is also a univariate polynomial. Hence $p(x) \cdot q(x)$ is also a univariate polynomial. As required.

(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.

Let $p(x)$ have degree m such that $p(x) = \sum_{i=0}^{m} c_i \cdot x^i$ and $q(x)$ have degree n such that $q(x) = \sum_{i=0}^{n} d_i \cdot x^i$.
Without loss of generality, assume that $m \geq n$.
Let $q'(x) = \sum_{i=0}^{m} e_i \cdot x^i$ such that $(e_i \leq n \implies e_i = d_i) \wedge (e_i > n \implies c_i = 0)$.
Therefore $q'(x)$ is the same as $q(x)$.

$$\begin{aligned}
&a \cdot p(x) + b \cdot q(x) \\
=&a \cdot p(x) + b \cdot q'(x) \\
=&a \cdot \sum_{i=0}^{m} c_i \cdot x^i + b \cdot \sum_{i=0}^{m} e_i \cdot x^i \\
=&\sum_{i=0}^{m} a \cdot c_i \cdot x^i + \sum_{i=0}^{m} b \cdot e_i \cdot x^i \\
=&\sum_{i=0}^{m} (a \cdot c_i + b \cdot e_i) \cdot x^i
\end{aligned} \tag{41}$$

Which is the formula for a univariate polynomial where $a_i = a \cdot c_i + b \cdot e_i$. So if $p(x)$ and $q(x)$ are univariate polynomials, then $a \cdot p(x) + b \cdot q(x)$ is also a univariate polynomial. As required.

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

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

At $n = 0$:

$$\begin{aligned}
&\frac{n}{6}(n+1)(2 \cdot n + 1) \\
=&\frac{0}{6} \cdot 1 \cdot 1 \\
=&0 \\
&\sum_{i=0}^{0} i^2 \\
=&0
\end{aligned} \tag{42}$$

So the expression holds true at $n = 0$.

Assume that the expression also holds true at $n = k$.

$$\begin{aligned}
\sum_{i=0}^{k} i^2 &= \frac{k}{6}(k+1)\cdot(2\cdot k+1) \\
\sum_{i=0}^{k+1} i^2 &= \frac{k}{6}(k+1)\cdot(2\cdot k+1)+(k+1)^2 \\
\sum_{i=0}^{k+1} i^2 &= \frac{1}{6}(k+1)\cdot(k\cdot(2\cdot k+1)+6\cdot(k+1)) \\
\sum_{i=0}^{k+1} i^2 &= \frac{1}{6}(k+1)\cdot(2\cdot k^2+k+6\cdot k+6) \\
\sum_{i=0}^{k+1} i^2 &= \frac{1}{6}(k+1)\cdot(2\cdot k^2+7\cdot k+6) \\
\sum_{i=0}^{k+1} i^2 &= \frac{1}{6}(k+1)\cdot(2\cdot k+3)\cdot(k+2) \\
\sum_{i=0}^{k+1} i^2 &= \frac{k+1}{6}(k+2)\cdot(2\cdot k+3) \\
\sum_{i=0}^{k+1} i^2 &= \frac{k+1}{6}((k+1)+1)\cdot(2\cdot(k+1)+1)
\end{aligned} \tag{43}$$

So if the expression is true at $n = k$ then by induction it is also true at $n = k+1$. Since the expression is also true at $n = 0$, by induction it must be true for all $n \in \mathbb{N}$. So there exists a polynomial $p_2(x)$ such that $p_2(n) = \sum_{i=0}^{n} i^2$.

Since $\sum_{i=0}^{n} i^2 = \frac{n}{6}(n+1)(2\cdot n+1)$ is a polynomial that satisfies $p_2(n) = \sum_{i=0}^{n} i^2$ – there must be a polynomial that satisfies $p_2(n) = \sum_{i=0}^{n} i^2$

(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

$$(n+1)^2 = \sum_{i=0}^{n}(i+1)^2 - \sum_{i=0}^{n} i^2 \tag{44}$$

$$(n+1)^k = \sum_{i=0}^{n}(i+1)^k - \sum_{i=0}^{n} i^k \tag{45}$$

So if $p_k(n)$ is a polynomial, then $p_k(n+1)$ is also s polynomial.

Hence there exists a polynomial $p_k(x)$ such that for all $n \in \mathbb{N} : p_k(n) = \sum^(n)_{i=0} i^k$.

I'm fully aware that this does not constitute a proper proof – I just didn't know how to prove it formally.