

2.3 Definition by Recursion

Since school we have defined powers by two clauses: $u^0 = 1$, and $u^{n+1} = u^n u$. Sums $a_1 + \dots + a_n$, factorials and many sequences are defined the same way: a starting value, and a rule that produces the next value from the last. *Logic and Proof*, Chapter 4 used induction to prove facts about such objects, such as $3^n \geq 2n + 1$ in *Logic and Proof*, Example (An inequality by induction). But induction proves facts about a function that **already exists**, and here the function is what we want to obtain. This section proves that two such clauses always define exactly one function on $\mathbb{N}$, and then uses the theorem to define sums, products and powers properly and to prove their first laws.

2.3.1 Definitions that define something

Logic and Proof, Chapter 4 met the same question for formulas. A recursive definition on formulas gives a value for each atom and a rule for each way of building a compound formula, and *Logic and Proof*, Theorem 4.3.4 showed that such clauses define exactly one function, because unique readability leaves no choice of clause. On $\mathbb{N}$ the clauses are simpler: one starting value at 0, and one rule for passing from n to $n + 1$. What we want to prove is this.

A starting value and a rule for the next value determine exactly one sequence.

Theorem 2.3.1. Recursion Theorem

Let X be a set, let $a \in X$, and let $g: \mathbb{N} \times X \rightarrow X$ be a function. Then there is **exactly one** function $f: \mathbb{N} \rightarrow X$ such that

$$f(0) = a \quad \text{and} \quad f(n+1) = g(n, f(n)) \quad \text{for every } n \in \mathbb{N}.$$

In words: a is the starting value, and g is the rule that turns the stage n and the current value $f(n)$ into the next value. The rule may look at n as well as at $f(n)$: the factorial needs this, since $(n+1)! = (n+1) \cdot n!$ is $g(n, x) = (n+1)x$ at $x = n!$. The hypothesis that g maps into X is what lets the rule be applied again at the next stage. The conclusion has two halves: **existence** (some f obeys the two equations) and **uniqueness** (no two different functions do).

Idea. Uniqueness is an ordinary induction: two solutions agree at 0, and if they agree at n , the second equation makes them agree at $n + 1$. Existence is harder, because induction cannot produce f ; it can only prove statements. So we prove by induction a statement about finite pieces of f . The roadmap:

- ① **Uniqueness**, by induction on n .
- ② **Claim:** for every $n \in \mathbb{N}$ there is exactly one function on $\{0, \dots, n\}$ obeying the two equations wherever they make sense (a **partial solution**). Its graph is the graph of the previous one with one pair added.
- ③ **Glue:** collect the graphs of all partial solutions in one set $\mathcal{S}$ and take the union. The partial solutions agree where they overlap, so the union is the graph of a function on all of $\mathbb{N}$, and that function obeys the equations.

Before reading on: self-explain the Claim's inductive step.

Proof. For $n \in \mathbb{N}$, the set $\{0, \dots, n\} = \{k \in \mathbb{N} : k \leq n\}$ of Section 2.1 contains 0, since $0 \leq n$ by Lemma 2.1.1 (a). Call a function $h: \{0, \dots, n\} \rightarrow X$ a **partial solution up to n** if $h(0) = a$ and $h(k+1) = g(k, h(k))$ for every $k \in \mathbb{N}$ with $k+1 \leq n$. (For such k , both k and $k+1$ lie in $\{0, \dots, n\}$, so the equation makes sense.)

Step 1 (uniqueness). Let $f, f': \mathbb{N} \rightarrow X$ both satisfy the two equations, and let $P(n)$ be “ $f(n) = f'(n)$ ”. $P(0)$ holds, since $f(0) = a = f'(0)$. If $P(n)$ holds, then

$$f(n+1) = g(n, f(n)) = g(n, f'(n)) = f'(n+1),$$

so $P(n+1)$ holds. By Logic and Proof, Axiom 4.2.1, $f(n) = f'(n)$ for every $n \in \mathbb{N}$. The two functions have the same domain and the same codomain, so $f = f'$ by Proposition 1.4.1.

Step 2.

Claim. For every $n \in \mathbb{N}$ there is exactly one partial solution up to n .

Proof of Claim. We use Logic and Proof, Axiom 4.2.1 on n .

Base case. By Lemma 2.1.1 (a), every $k \in \mathbb{N}$ has $k \geq 0$, so $k \leq 0$ holds only for $k = 0$, and $\{0, \dots, 0\} = \{0\}$. The graph $\{(0, a)\}$ with codomain X is a function on $\{0\}$, since $a \in X$: the input 0 has the one output a . It is a partial solution up to 0: its value at 0 is a , and the second condition is vacuous, because $k+1 \geq 1 > 0$ for every $k \in \mathbb{N}$. Any partial solution up to 0 has value a at 0, so it equals this one by Proposition 1.4.1.

Inductive step. Let $n \in \mathbb{N}$, and suppose there is exactly one partial solution up to n ; call it f_n , with graph G_n . Let

$$G_{n+1} := G_n \cup \{(n+1, g(n, f_n(n)))\}.$$

First, $\{0, \dots, n+1\} = \{0, \dots, n\} \cup \{n+1\}$: a natural number $k \leq n+1$ is either $n+1$ or less than $n+1$, and then $k \leq n$, since no natural number lies strictly between n and $n+1$ (Lemma 2.1.1 (e)). Also $n+1 \notin \{0, \dots, n\}$, since $n+1 > n$.

We check the clauses of Definition 1.4.1 for G_{n+1} on $\{0, \dots, n+1\}$ with codomain X . Every pair of G_{n+1} lies in $\{0, \dots, n+1\} \times X$, because g takes values in X . (Fn1): an input $k \leq n$ has the output $f_n(k)$ in G_n , and the input $n+1$ has the output $g(n, f_n(n))$. (Fn2): the pairs with first coordinate $k \leq n$ all lie in G_n , since the added pair has first coordinate $n+1 \neq k$, and G_n satisfies (Fn2); the only pair with first coordinate $n+1$ is the added one, since the first coordinates in G_n are at most n . So $f_{n+1} := (G_{n+1}, X)$ is a function on $\{0, \dots, n+1\}$, and it agrees with f_n on $\{0, \dots, n\}$.

It is a partial solution up to $n+1$. Its value at 0 is $f_n(0) = a$. Let $k \in \mathbb{N}$ with $k+1 \leq n+1$, so $k \leq n$. If $k < n$, then $k+1 \leq n$ by Lemma 2.1.1 (e), and $f_{n+1}(k+1) = f_n(k+1) = g(k, f_n(k)) = g(k, f_{n+1}(k))$, because f_n is a partial solution. If $k = n$, then $f_{n+1}(n+1) = g(n, f_n(n)) = g(n, f_{n+1}(n))$ by the choice of the added pair.

It is the only one. Let h be a partial solution up to $n+1$. Its restriction $h|_{\{0, \dots, n\}}$ (Section 1.4) is a partial solution up to n , because the conditions on it are among the conditions on h . By the induction hypothesis it is f_n . So $h(k) = f_n(k) = f_{n+1}(k)$ for $k \leq n$, and

$$h(n+1) = g(n, h(n)) = g(n, f_n(n)) = f_{n+1}(n+1).$$

By Proposition 1.4.1, $h = f_{n+1}$. This proves the claim.

For each $n \in \mathbb{N}$, let f_n be the partial solution up to n , and G_n its graph. If $m \leq n$, then $\{0, \dots, m\} \subseteq \{0, \dots, n\}$, and the restriction of f_n to $\{0, \dots, m\}$ is a partial solution up to m , so by the claim it is f_m . In terms of graphs,

$$G_m = G_n \cap (\{0, \dots, m\} \times X) \subseteq G_n \quad (m \leq n).$$

Step 3 (existence). Let

$$\mathcal{S} := \{G \in \mathcal{P}(\mathbb{N} \times X) : G \text{ is the graph of a partial solution up to some } n \in \mathbb{N}\},$$

a set by Definition 1.1.3 and Definition 1.2.2. By the claim, the elements of $\mathcal{S}$ are exactly the graphs G_n . Let $F := \bigcup \mathcal{S}$ (Definition 1.2.4), so a pair lies in F if and only if it lies in some G_n ; in particular $F \subseteq \mathbb{N} \times X$. We check the clauses of Definition 1.4.1 for F .

(Fn1): for $n \in \mathbb{N}$, the pair $(n, f_n(n))$ lies in $G_n \in \mathcal{S}$, hence in F .

(Fn2): let $(k, y) \in F$ and $(k, y') \in F$, say $(k, y) \in G_m$ and $(k, y') \in G_n$. If $m \leq n$, then $G_m \subseteq G_n$, so both pairs lie in G_n , and $y = y'$ because G_n satisfies (Fn2). If $n < m$, the same argument with m and n exchanged gives $y = y'$.

So $f := (F, X)$ is a function $\mathbb{N} \rightarrow X$. For $m \geq n$, the pair $(n, f_m(n))$ lies in $G_m \subseteq F$, so $f(n) = f_m(n)$. Hence $f(0) = f_0(0) = a$, and for every $n \in \mathbb{N}$,

$$f(n+1) = f_{n+1}(n+1) = g(n, f_{n+1}(n)) = g(n, f(n)),$$

where the middle equation holds because f_{n+1} is a partial solution. This proves existence, and with Step 1, the theorem. ■

The starting value was used in both halves: Step 1 needs $f(0) = f'(0)$ as its base case, and Step 2 needs it to fix the first partial solution. The set $\mathcal{S}$ is cut out of a power set by a condition, so no family $n \mapsto f_n$ had to be formed before the union was taken. No choice is made anywhere: at every stage the claim leaves exactly one candidate. From now on, a definition of the form “ $f(0) := a$, $f(n+1) := g(n, f(n))$ ” is legitimate whenever $a \in X$ and g is a function $\mathbb{N} \times X \rightarrow X$, and we say that f is **defined by recursion**.

Remark. Because the rule may depend on n , the theorem also covers constructions in which the step uses outside data indexed by n . *Analysis on the Real Line*, Chapter 1 builds closed intervals I_{n+1} from I_n and the $(n+1)$ -st number of a given list in exactly this way, with no choice principle involved. The values may be sets as well as numbers. With $X = \mathcal{P}(\mathbb{N})$, $A_0 := \mathbb{N}$ and $A_{n+1} := A_n \setminus \{n\}$ define a sequence of sets of the kind Section 1.2 promised, and an induction that follows the same two clauses shows $A_n = \{k \in \mathbb{N} : k \geq n\}$: the base is Lemma 2.1.1 (a), and the step removes n from $\{k : k \geq n\}$, leaving $\{k : k > n\} = \{k : k \geq n+1\}$ by Lemma 2.1.1 (e).

2.3.2 Starting elsewhere, looking two steps back

Two variants come up constantly. Sequences are often indexed from 1, as in Section 1.4, and some recursions use the two previous values. Both reduce to the theorem.

Corollary 2.3.2. Recursion from a Base

Let n_0 be an integer, $D := \{n \in \mathbb{Z} : n \geq n_0\}$, X a set, $a \in X$, and $g: D \times X \rightarrow X$ a function. Then there is exactly one function $f: D \rightarrow X$ with $f(n_0) = a$ and $f(n+1) = g(n, f(n))$ for every $n \in D$.

Idea. Rename the index: $k = n - n_0$ turns D into $\mathbb{N}$ and the recursion on D into one on $\mathbb{N}$, where [Theorem 2.3.1](#) applies.

Proof. For $k \in \mathbb{N}$, the number $n_0 + k$ is an integer (Proposition 2.1.2 (a)) and $n_0 + k \geq n_0$ (Lemma 2.1.1 (a)), so it lies in D . Conversely, for $n \in D$, $n - n_0$ is an integer (Proposition 2.1.2 (a)) and ≥ 0 , so $n - n_0 \in \mathbb{N}$ by Proposition 2.1.2 (b). Define $g': \mathbb{N} \times X \rightarrow X$ by $g'(k, x) := g(n_0 + k, x)$. By [Theorem 2.3.1](#) there is exactly one $f': \mathbb{N} \rightarrow X$ with $f'(0) = a$ and $f'(k+1) = g(n_0 + k, f'(k))$ for every $k \in \mathbb{N}$.

Existence. Let $t: D \rightarrow \mathbb{N}$, $t(n) := n - n_0$, and $f := f' \circ t$ (Definition 1.4.2). Then $f(n_0) = f'(0) = a$, and for $n \in D$, with $k = n - n_0$,

$$f(n+1) = f'(k+1) = g(n_0 + k, f'(k)) = g(n, f(n)).$$

Uniqueness. If $\tilde{f}: D \rightarrow X$ also satisfies both equations, then $k \mapsto \tilde{f}(n_0 + k)$ satisfies the equations that define f' , so it is f' by the uniqueness in [Theorem 2.3.1](#). Hence $\tilde{f}(n) = f'(n - n_0) = f(n)$ for every $n \in D$, and $\tilde{f} = f$ by Proposition 1.4.1. ■

The renaming is the move that gave induction from a base (Theorem 2.2.1). The corollary covers every sequence $(a_n)_{n \geq 1}$ given by a first term and a rule, and *Analysis on the Real Line*, Chapter 1's intervals, which are listed from 1.

Corollary 2.3.3. Two-Step Recursion

Let X be a set, $a, b \in X$, and $h: \mathbb{N} \times (X \times X) \rightarrow X$ a function (Definition 1.3.2); write $h(n, x, y)$ for $h(n, (x, y))$. Then there is exactly one function $f: \mathbb{N} \rightarrow X$ with

$$f(0) = a, \quad f(1) = b, \quad f(n+2) = h(n, f(n), f(n+1)) \quad \text{for every } n \in \mathbb{N}.$$

Idea. A rule that looks two steps back is a rule that looks one step back at **pairs**. Carry the pair $(f(n), f(n+1))$ along: the next pair is $(f(n+1), f(n+2))$, and both of its entries are computed from the current pair.

Proof. Define $G: \mathbb{N} \times (X \times X) \rightarrow X \times X$ by $G(n, (x, y)) := (y, h(n, x, y))$. By [Theorem 2.3.1](#) with the set $X \times X$ and the starting value (a, b) , there is exactly one $p: \mathbb{N} \rightarrow X \times X$ with $p(0) = (a, b)$ and $p(n+1) = G(n, p(n))$. Write $p(n) = (p_1(n), p_2(n))$. The equation $p(n+1) = (p_2(n), h(n, p_1(n), p_2(n)))$ gives, by the characteristic property of pairs (Definition 1.3.1),

$$p_1(n+1) = p_2(n), \quad p_2(n+1) = h(n, p_1(n), p_2(n)).$$

Let $f(n) := p_1(n)$. Then $f(0) = a$, $f(1) = p_2(0) = b$, and

$$f(n+2) = p_2(n+1) = h(n, p_1(n), p_2(n)) = h(n, f(n), f(n+1)).$$

For uniqueness, let f' satisfy the three equations, and let $p'(n) := (f'(n), f'(n+1))$. Then $p'(0) = (a, b)$ and

$$p'(n+1) = (f'(n+1), h(n, f'(n), f'(n+1))) = G(n, p'(n)),$$

so $p' = p$ by the uniqueness in [Theorem 2.3.1](#), and $f'(n) = p_1(n) = f(n)$ for every n . By Proposition 1.4.1, $f' = f$. ■

2.3.3 Sums, products and powers

The symbols $\sum$ and $\prod$ are recursive definitions, and so are powers. Writing them as instances of [Theorem 2.3.1](#) settles what they mean at the edges: the empty sum, the empty product and u^0 .

Definition 2.3.1. Finite Sums and Products

Let $(a_k)_{k \geq 1}$ be a sequence of real numbers. The **sums** $\sum_{k=1}^n a_k$ and **products** $\prod_{k=1}^n a_k$, for $n \in \mathbb{N}$, are defined by recursion:

$$\begin{aligned} \sum_{k=1}^0 a_k &:= 0, & \sum_{k=1}^{n+1} a_k &:= \sum_{k=1}^n a_k + a_{n+1}, \\ \prod_{k=1}^0 a_k &:= 1, & \prod_{k=1}^{n+1} a_k &:= \left(\prod_{k=1}^n a_k \right) a_{n+1}. \end{aligned}$$

The **factorial** of $n \in \mathbb{N}$ is $n! := \prod_{k=1}^n k$. For integers $m \leq n+1$ and reals a_k given for every integer $k \geq m$,

$$\sum_{k=m}^n a_k := \sum_{i=1}^{n-m+1} a_{m-1+i}, \quad \prod_{k=m}^n a_k := \prod_{i=1}^{n-m+1} a_{m-1+i}.$$

In words: a sum starts at 0 and adds one term at each stage; a product starts at 1 and multiplies by one term at each stage. The sum is [Theorem 2.3.1](#) with $X = \mathbb{R}$, $a = 0$ and $g(n, x) = x + a_{n+1}$, a function $\mathbb{N} \times \mathbb{R} \rightarrow \mathbb{R}$ because $n+1 \geq 1$ is an index of the sequence (Lemma 2.1.1 (a), (NS)); the product is $a = 1$, $g(n, x) = xa_{n+1}$. The letter k is a dummy: $\sum_{k=1}^n a_k$ and $\sum_{j=1}^n a_j$ are the same number. In the general form, $n-m+1$ is an integer ≥ 0 , hence in $\mathbb{N}$ (Proposition 2.1.2 (b)), and the terms a_{m-1+i} , for $i \geq 1$, run through $a_m, a_{m+1}, \dots$; when $m = 1$ it gives the first form back.

The edge cases are the point of the definition. The **empty sum** is 0 and the **empty product** is 1: $\sum_{k=m}^{m-1} a_k = 0$ and $0! = 1$. These are the only values that make the recursive clause true at the first stage for every sequence, since $\sum_{k=1}^1 a_k$ should be a_1 and $\prod_{k=1}^1 a_k$ should be a_1 . So $1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$.

Three consequences are used constantly, and each is a short check from the definition.

- **Finite lists.** $\sum_{k=1}^n a_k$ depends only on $a_1, \dots, a_n$. Precisely: if two sequences agree at $1, \dots, N$, their sums up to n agree for every $n \leq N$. Induct on n with the property “if $n \leq N$, the two sums up to n are equal”. The base is $0 = 0$. In the step, $n+1 \leq N$ gives $n \leq N$, so the sums up to n agree, and the added terms a_{n+1} agree because $1 \leq n+1 \leq N$. So a finite list $a_1, \dots, a_N$ is summed by extending it in any way, say by $a_k := 0$ for $k > N$, and the result does not depend on the extension. The same holds for products, and for the general bounds with $a_m, \dots, a_n$.
- **Shifting the index.** For every integer p , $\sum_{k=m}^n a_k = \sum_{k=m+p}^{n+p} a_{k-p}$, because both sides unfold to $\sum_{i=1}^{n-m+1} a_{m-1+i}$. *Analysis on the Real Line*, Chapter 1’s estimate of $y^k - x^k$ uses the shift $p = 1$.
- **Splitting off the last term.** For $m \leq n+1$, $\sum_{k=m}^{n+1} a_k = \sum_{k=m}^n a_k + a_{n+1}$. Unfold the left side to $\sum_{i=1}^{n-m+2} a_{m-1+i}$ and apply the recursive clause; its last term is $a_{m-1+(n-m+2)} = a_{n+1}$.

Definition 2.3.2. Powers

Let $u \in \mathbb{R}$. The **powers** u^n , for $n \in \mathbb{N}$, are defined by recursion:

$$u^0 := 1, \quad u^{n+1} := u^n u.$$

This is [Theorem 2.3.1](#) with $X = \mathbb{R}$, $a = 1$ and $g(n, x) = xu$. So $u^1 = u^0 u = u$, and $u^2 = uu$. The definition gives $0^0 = 1$, in line with the empty product: $u^n = \prod_{k=1}^n u$, since both sides obey the same two clauses and so agree by the uniqueness in [Theorem 2.3.1](#). Only exponents in $\mathbb{N}$ are defined here; roots $a^{1/n}$ come in *Analysis on the Real Line*, Chapter 1.

A sequence that approaches $\sqrt{2}$. Let $X := (0, \infty)$ and $g(n, x) := \frac{1}{2}(x + 2/x)$. Before writing a recursion, check that g maps X into X : for $x > 0$, $2/x$ is defined and positive, so $x + 2/x > 0$, and half of it is positive. By [Theorem 2.3.1](#), $a_0 := 2$ and $a_{n+1} := \frac{1}{2}(a_n + 2/a_n)$ define a sequence in $(0, \infty)$. Because the check was made on g , no separate induction is needed to show $a_n > 0$ before dividing by it. The first values are

$$a_0 = 2, \quad a_1 = \frac{1}{2}(2 + 1) = \frac{3}{2}, \quad a_2 = \frac{1}{2}\left(\frac{3}{2} + \frac{4}{3}\right) = \frac{17}{12},$$

and $(17/12)^2 = 289/144$, which exceeds 2 by $1/144$. That the sequence converges to $\sqrt{2}$ is a question for *Analysis on the Real Line*, Chapter 2, where recursively defined sequences become objects of study.

A two-step example. By [Corollary 2.3.3](#), $a_0 = 2$, $a_1 = 3$ and $a_{n+2} = 3a_{n+1} - 2a_n$ define a unique sequence of reals ($X = \mathbb{R}$, $h(n, x, y) = 3y - 2x$), and its first values are 2, 3, 5, 9, 17. These are $2^n + 1$. To prove it, induct on the **pair** statement $Q(n)$: “ $a_n = 2^n + 1$ and $a_{n+1} = 2^{n+1} + 1$ ”. $Q(0)$ is $2 = 1 + 1$ and $3 = 2 + 1$. If $Q(n)$ holds, its second half is the first half of $Q(n+1)$, and

$$a_{n+2} = 3(2^{n+1} + 1) - 2(2^n + 1) = 2 \cdot 2^{n+1} + 1 = 2^{n+2} + 1,$$

where $2 \cdot 2^n = 2^n \cdot 2 = 2^{n+1}$ and $2 \cdot 2^{n+1} = 2^{n+1} \cdot 2 = 2^{n+2}$ by [Definition 2.3.2](#) (and commutativity). So Logic and Proof, Axiom 4.2.1 gives $Q(n)$ for every n , and in particular $a_n = 2^n + 1$. The induction carries a pair because the recursion does: the proof follows the clauses of the definition.

Warning. A recursion needs its starting values, and its rule must stay inside X . “ $a_{n+2} = a_{n+1} + a_n$ ” alone defines nothing: $0, 1, 1, 2, \dots$ and $2, 1, 3, 4, \dots$ both obey it, and [Corollary 2.3.3](#) asks for a_0 and a_1 . And “ $a_0 = 2, a_{n+1} = 1/(a_n - 1)$ ” is not a definition by recursion: $a_1 = 1$, and then a_2 would be $1/0$. The rule $x \mapsto 1/(x - 1)$ is not a function from any set X containing 2 into X , since X would have to contain its value 1, where the rule is undefined.

Quick check. Compute $\prod_{k=1}^4 (1 + \frac{1}{k})$, and say why the answer is so simple.

Solution. Each factor is $1 + \frac{1}{k} = \frac{k+1}{k}$, so the product is

$$\frac{2}{1} \cdot \frac{3}{2} \cdot \frac{4}{3} \cdot \frac{5}{4} = 5.$$

Each numerator cancels the next denominator: the product **telescopes**. In general $\prod_{k=1}^n \frac{k+1}{k} = n+1$, by induction on n : the empty product is $1 = 0+1$, and $(n+1) \cdot \frac{n+2}{n+1} = n+2$.

2.3.4 Recursion, then induction

A function defined by recursion is studied by induction, and the induction follows the clauses of the definition: the base case uses the starting value, the step uses the rule. The laws of powers are the first example.

Proposition 2.3.4. Laws of Powers

Let $u, v \in \mathbb{R}$ and $m, n \in \mathbb{N}$.

- (a) $u^{m+n} = u^m u^n$.
- (b) $(u^m)^n = u^{mn}$.
- (c) $(uv)^n = u^n v^n$.
- (d) If $u \in \mathbb{Z}$, then $u^n \in \mathbb{Z}$; if $u \in \mathbb{N}$, then $u^n \in \mathbb{N}$.
- (e) If $u > 0$, then $u^n > 0$. If $u > 1$ and $m < n$, then $u^m < u^n$.

Idea. Each part is an induction on n from 0, with m fixed. The base case is $u^0 = 1$ in some form, and the step peels one factor off with $u^{n+1} = u^n u$ and applies the induction hypothesis to u^n . For the second half of (e), write $n = m + j$ with $j \geq 1$ and use (a).

Proof.

- (a) Fix m and induct on n . For $n = 0$: $u^{m+0} = u^m = u^m \cdot 1 = u^m u^0$. Suppose $u^{m+n} = u^m u^n$. Since $m+n \in \mathbb{N}$ (Lemma 2.1.1 (b)), [Definition 2.3.2](#) applies at $m+n$, and

$$u^{m+(n+1)} = u^{(m+n)+1} = u^{m+n} u = u^m u^n u = u^m u^{n+1},$$

where the third equation is the induction hypothesis and the last is [Definition 2.3.2](#). By Logic and Proof, Axiom 4.2.1, (a) holds for every n .

- (b) Fix m . For $n = 0$: $(u^m)^0 = 1 = u^0 = u^{m \cdot 0}$. If $(u^m)^n = u^{mn}$, then $(u^m)^{n+1} = (u^m)^n u^m = u^{mn} u^m = u^{mn+m} = u^{m(n+1)}$, using (a) with the exponents $mn, m \in \mathbb{N}$ (Lemma 2.1.1 (b)).
- (c) $(uv)^0 = 1 = 1 \cdot 1 = u^0 v^0$. If $(uv)^n = u^n v^n$, then $(uv)^{n+1} = (uv)^n uv = u^n v^n uv = (u^n u)(v^n v) = u^{n+1} v^{n+1}$.
- (d) $u^0 = 1 = 0 + 1$ lies in $\mathbb{N}$ by $((\mathbb{N})0)$ and (NS), and $\mathbb{N} \subseteq \mathbb{Z}$. If $u^n \in \mathbb{Z}$ and $u \in \mathbb{Z}$, then $u^{n+1} = u^n u \in \mathbb{Z}$ by Proposition 2.1.2 (a). For $u \in \mathbb{N}$ the same induction works with Lemma 2.1.1 (b) in place of Proposition 2.1.2.
- (e) Let $u > 0$. Then $u^0 = 1 > 0$, and if $u^n > 0$, then $u^{n+1} = u^n u > 0$ as a product of positive numbers. Now let $u > 1$. First, $u^j > 1$ for every integer $j \geq 1$ (such j lies in $\mathbb{N}$ by Proposition 2.1.2 (b), so u^j is defined), by Theorem 2.2.1 with base 1: $u^1 = u > 1$, and if $u^j > 1$, then $u^{j+1} = u^j u > 1 \cdot u > 1$, multiplying $u^j > 1$ by $u > 0$. Let $m < n$. Then $j := n - m \in \mathbb{N}$ by Lemma 2.1.1 (d), and $j \neq 0$, so $j \geq 1$ by Lemma 2.1.1 (a). By (a), $u^n = u^{m+j} = u^m u^j > u^m$, multiplying $u^j > 1$ by $u^m > 0$.

■

Some instances that earlier chapters used on trust: $(t^2)^2 = t^4$ is (b) with $m = n = 2$; $2^{s+t} = 2^s 2^t$ is (a); $n \mapsto 2^n$ is strictly increasing on $\mathbb{N}$ by (e); and an integer power of an integer is an integer by (d). For $(-1)^n$: by (b), $(-1)^{2k} = ((-1)^2)^k = 1^k = 1$, where $1^k = 1$ by the induction $1^{k+1} = 1^k \cdot 1$; and $(-1)^{2k+1} = (-1)^{2k}(-1) = -1$. Every $n \in \mathbb{N}$ is $2k+r$ with $k \in \mathbb{Z}$ and $r \in \{0, 1\}$ (Theorem 2.2.3 with divisor 2, and Proposition 2.1.2 (c) for $r \leq 1$), and $k \geq 0$: if $k < 0$, then $k \leq -1$ (Proposition 2.1.2 (c)), so $n = 2k+r \leq -2+1 < 0$, contradicting $n \geq 0$ (Lemma 2.1.1 (a)). So $k \in \mathbb{N}$ by Proposition 2.1.2 (b), n is $2k$ or $2k+1$, and $(-1)^n$ is 1 for even n and -1 for odd n .

The next two formulas are proved the same way; each is a recursion (the sum) followed by an induction whose step splits off the last term.

Proposition 2.3.5. Sum of the First Natural Numbers

For every $n \in \mathbb{N}$, $\sum_{k=1}^n k = \frac{n(n+1)}{2}$.

Proof. For $n = 0$, both sides are 0: the left by the empty sum, the right since $0 \cdot 1 = 0$. If the formula holds for n , then by [Definition 2.3.1](#)

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

which is the formula for $n+1$. By Logic and Proof, Axiom 4.2.1 it holds for every $n \in \mathbb{N}$.

■

Proposition 2.3.6. Geometric Sum

Let $r \in \mathbb{R}$ with $r \neq 1$. For every $n \in \mathbb{N}$,

$$\sum_{k=1}^n r^{k-1} = \frac{1 - r^n}{1 - r}.$$

Proof. The terms are defined: for $k \geq 1$, $k - 1 \in \mathbb{N}$ by Lemma 2.1.1 (c), so r^{k-1} is given by Definition 2.3.2, and the term added at stage $n + 1$ is $r^{(n+1)-1} = r^n$. The right side is defined because $1 - r \neq 0$. For $n = 0$, both sides are 0, since $r^0 = 1$. If the formula holds for n , then, by Definition 2.3.1 and the induction hypothesis,

$$\begin{aligned} \sum_{k=1}^{n+1} r^{k-1} &= \frac{1 - r^n}{1 - r} + r^n = \frac{1 - r^n + r^n - r^{n+1}}{1 - r} \\ &= \frac{1 - r^{n+1}}{1 - r}, \end{aligned}$$

where $r^n(1 - r) = r^n - r^{n+1}$ by Definition 2.3.2. By Logic and Proof, Axiom 4.2.1 the formula holds for every $n \in \mathbb{N}$. ■

For $r = 1$ the sum is n , since every term is 1; that is the case the hypothesis excludes, where the right side would divide by 0.

The next inequality is the most used estimate of a power in analysis. Its proof shows a hypothesis doing exactly one job.

Theorem 2.3.7. Bernoulli's Inequality

Let $x \in \mathbb{R}$ with $x \geq -1$. Then $(1 + x)^n \geq 1 + nx$ for every $n \in \mathbb{N}$.

Idea. Induct on n . To pass from n to $n + 1$, multiply the induction hypothesis by $1 + x$; the product $(1 + nx)(1 + x) = 1 + (n + 1)x + nx^2$ is at least $1 + (n + 1)x$, because the extra term nx^2 is non-negative. Multiplying an inequality by $1 + x$ keeps its direction only if $1 + x \geq 0$, and that is what $x \geq -1$ says.

Proof. For $n = 0$: $(1 + x)^0 = 1 \geq 1 = 1 + 0 \cdot x$. Suppose $(1 + x)^n \geq 1 + nx$. Since $x \geq -1$, we have $1 + x \geq 0$, and multiplying the induction hypothesis by $1 + x$ gives

$$\begin{aligned} (1 + x)^{n+1} &= (1 + x)^n(1 + x) \geq (1 + nx)(1 + x) \\ &= 1 + (n + 1)x + nx^2 \geq 1 + (n + 1)x, \end{aligned}$$

where the first equation is Definition 2.3.2 and the last step uses $nx^2 \geq 0$, true because $n \geq 0$ (Lemma 2.1.1 (a)) and $x^2 \geq 0$. By Logic and Proof, Axiom 4.2.1 the inequality holds for every $n \in \mathbb{N}$. ■

The hypothesis $x \geq -1$ appears in the proof once, in the sentence “since $x \geq -1$, we have $1 + x \geq 0$ ”, and it cannot simply be dropped: for $x = -4$ and $n = 3$, $(1 + x)^3 = (-3)^3 = -27$, while $1 + 3x = -11$, and $-27 < -11$. Exercise C2 below shows that the statement can survive at some $x < -1$ even though the proof does not.

The last result of this subsection is not about a recursive definition, but its induction runs over lists, and it is the fact *Analysis on the Real Line*, Chapter 1 needs about finite sets. A **maximum** of a set $A \subseteq \mathbb{R}$ is an element $M \in A$ with $a \leq M$ for every $a \in A$; a **minimum** is an element $m \in A$ with $m \leq a$ for every $a \in A$. For reals $x_1, \dots, x_n$, we write $\{x_1, \dots, x_n\} := \{x_k : k \in \{1, \dots, n\}\}$.

Proposition 2.3.8. Finite Sets Have a Maximum

For every integer $n \geq 1$ and all reals $x_1, \dots, x_n$, the set $\{x_1, \dots, x_n\}$ has a maximum and a minimum.

Idea. Add the elements one at a time. The maximum of the longer list is the old maximum or the new element, whichever is larger, and comparing the two is all the step needs.

Proof. Let $P(n)$ be “for all reals $x_1, \dots, x_n$, the set $\{x_1, \dots, x_n\}$ has a maximum”. We prove $P(n)$ for every $n \geq 1$ by Theorem 2.2.1 with base 1.

Base case. $\{x_1\}$ has the maximum x_1 .

Inductive step. Let $n \geq 1$, suppose $P(n)$, and let $x_1, \dots, x_{n+1}$ be reals. Since $\{1, \dots, n+1\} = \{1, \dots, n\} \cup \{n+1\}$ (Lemma 2.1.1 (e), as in the proof of Theorem 2.3.1), the set $B := \{x_1, \dots, x_{n+1}\}$ is $A \cup \{x_{n+1}\}$, where $A := \{x_1, \dots, x_n\}$. By $P(n)$, applied to the list $x_1, \dots, x_n$, the set A has a maximum M . By trichotomy, $x_{n+1} \leq M$ or $M < x_{n+1}$.

Case 1: $x_{n+1} \leq M$. Then $M \in A \subseteq B$, and every element of B is an element $a \in A$, with $a \leq M$, or is $x_{n+1} \leq M$. So M is a maximum of B .

Case 2: $M < x_{n+1}$. Then $x_{n+1} \in B$, and every $a \in A$ satisfies $a \leq M < x_{n+1}$. So x_{n+1} is a maximum of B .

In both cases $P(n+1)$ holds. By Theorem 2.2.1, $P(n)$ holds for every $n \geq 1$.

For the minimum, apply the result to $-x_1, \dots, -x_n$: if $-x_j$ is a maximum of $\{-x_1, \dots, -x_n\}$, then $-x_k \leq -x_j$, that is $x_j \leq x_k$, for every k , so x_j is a minimum of $\{x_1, \dots, x_n\}$.

■

The base is 1, not 0: for $n = 0$ the set is $\emptyset$, which has neither a maximum nor a minimum, since both must be elements. The proof used only order properties of $\leq$: any two elements are comparable (trichotomy), $\leq$ is reflexive and transitive, and $x \mapsto -x$ reverses $\leq$. All of these hold in any ordered field, so the proof works word for word there; that is the setting in which *Analysis on the Real Line*, Chapter 1 uses it. Passing from a finite **set** to a list $x_1, \dots, x_n$ that enumerates it is what “finite” will mean in Chapter 3.

2.3.5 When the claim is too weak to carry its step

Sometimes the statement we want is true, but it cannot be proved by induction as it stands: its inductive step does not go through. The cure looks paradoxical. We prove **more**.

Example. Proving more to prove anything

Prove that $\sum_{k=1}^n \frac{1}{k^2} < 2$ for every integer $n \geq 1$.

Solution. The direct attempt fails. Let $S_n := \sum_{k=1}^n 1/k^2$, so $S_{n+1} = S_n + 1/(n+1)^2$ by Definition 2.3.1. The base $S_1 = 1 < 2$ holds. For the step, all we may assume is $S_n < 2$, and that is too little: it allows $S_n = 2 - \frac{1}{2(n+1)^2}$, and then $S_n + \frac{1}{(n+1)^2} > 2$. The values of S_n never come so close to 2, but the induction hypothesis cannot know that.

Prove more. We prove $P(n)$: “ $S_n \leq 2 - \frac{1}{n}$ ” for every $n \geq 1$, by Theorem 2.2.1 with base 1. It implies the claim, since $2 - \frac{1}{n} < 2$.

Base case. $S_1 = 1 = 2 - \frac{1}{1}$.

Inductive step. Let $n \geq 1$ and suppose $S_n \leq 2 - \frac{1}{n}$. Then

$$S_{n+1} = S_n + \frac{1}{(n+1)^2} \leq 2 - \frac{1}{n} + \frac{1}{(n+1)^2}.$$

It remains to show $-\frac{1}{n} + \frac{1}{(n+1)^2} \leq -\frac{1}{n+1}$, that is, $\frac{1}{(n+1)^2} \leq \frac{1}{n} - \frac{1}{n+1} = \frac{1}{n(n+1)}$. Both denominators are positive, and $n(n+1) \leq (n+1)^2$ because $n \leq n+1$ and $n+1 > 0$; so the inequality holds. Hence $S_{n+1} \leq 2 - \frac{1}{n+1}$, which is $P(n+1)$.

By Theorem 2.2.1, $S_n \leq 2 - \frac{1}{n} < 2$ for every $n \geq 1$.

The stronger statement carries its own step because its hypothesis says **how far** below 2 the sum is, and that margin pays for the next term. When a step fails, ask what the hypothesis would need to say, and prove that instead. Exercise C3 below uses it twice over, proving two identities together because neither carries its own one-step induction.

2.3.6 Exercises

2.3.6.1 A. Check your understanding

Exercise. A1

These questions are about the proof of Theorem 2.3.1.

- Why does uniqueness need only an induction, while existence needs the claim about partial solutions?
- In Step 3, which property of the graphs G_n makes $\bigcup \mathcal{S}$ satisfy (Fn2), and which part of the proof supplies it?
- Run the construction for $X = \mathbb{R}$, $a = 1$ and $g(n, x) = (n+1)x$: write the graphs G_0 , G_1 , G_2 . Which familiar function is f ?
- State the idea of the proof in two sentences.

- (e) Write $\sum_{k=1}^n a_k$ and $n!$ as instances of [Theorem 2.3.1](#): name X , a and g for each.

Solution.

- (a) Uniqueness is a statement about two functions that are **given**: it compares their values, and comparing values at $n + 1$ through the values at n is an induction. Existence asks for a function that is not given. Induction proves statements and does not build objects, so the proof proves a statement (the claim) whose content is that the finite pieces exist and are unique, and then builds f from them as a union.
- (b) The graphs agree where they overlap: $G_m \subseteq G_n$ for $m \leq n$, more precisely $G_m = G_n \cap (\{0, \dots, m\} \times X)$. This comes from the **uniqueness** half of the claim: the restriction of f_n to $\{0, \dots, m\}$ is a partial solution up to m , so it is f_m . With it, two pairs $(k, y) \in G_m$ and $(k, y') \in G_n$ lie in the larger graph, whose (Fn2) gives $y = y'$. So it verifies (Fn2) of Definition 1.4.1 for $\bigcup \mathcal{S}$.
- (c) $G_0 = \{(0, 1)\}$. Then $g(0, 1) = 1 \cdot 1 = 1$, so $G_1 = \{(0, 1), (1, 1)\}$. Then $g(1, 1) = 2 \cdot 1 = 2$, so $G_2 = \{(0, 1), (1, 1), (2, 2)\}$. The function f is $n \mapsto n!$: by [Definition 2.3.1](#), $0! = 1$ and $(n + 1)! = n!(n + 1) = g(n, n!)$, so $n \mapsto n!$ satisfies both equations, and by the uniqueness in [Theorem 2.3.1](#) it is f .
- (d) For each n , induction shows that there is exactly one function on $\{0, \dots, n\}$ obeying the equations, and these pieces extend one another. Their union is the required function, and an induction on n shows there is no other.
- (e) The sum: $X = \mathbb{R}$, $a = 0$, $g(n, x) = x + a_{n+1}$. The factorial: $X = \mathbb{R}$ (or $\mathbb{N}$), $a = 1$, $g(n, x) = (n + 1)x$, as in (c).

2.3.6.2 B. Practice

Exercise. B1: Sum of cubes

Prove that $\sum_{k=1}^n k^3 = \left(\frac{n(n+1)}{2}\right)^2$ for every $n \in \mathbb{N}$.

Solution. For $n = 0$, both sides are 0 (the empty sum, and $0^2 = 0$). Suppose the formula holds for n . By [Definition 2.3.1](#) and the induction hypothesis,

$$\begin{aligned} \sum_{k=1}^{n+1} k^3 &= \frac{n^2(n+1)^2}{4} + (n+1)^3 = (n+1)^2 \frac{n^2 + 4n + 4}{4} \\ &= \frac{(n+1)^2(n+2)^2}{4} = \left(\frac{(n+1)(n+2)}{2}\right)^2, \end{aligned}$$

which is the formula for $n + 1$. By Logic and Proof, Axiom 4.2.1 the formula holds for every $n \in \mathbb{N}$. (Compare [Proposition 2.3.5](#): the sum of the first n cubes is the square of the sum of the first n numbers.)

Exercise. B2: Starting at the right place

Logic and Proof, Chapter 4 observed, in the warning after Logic and Proof, Example (An

inequality by induction), that “ $2^n \geq n^2$ ” fails at $n = 3$ and holds again from $n = 4$ on. Prove that $2^n \geq n^2$ for every integer $n \geq 4$, using Theorem 2.2.1. Say why the base must be 4 and not 3.

Solution. Let $P(n)$ be “ $2^n \geq n^2$ ”; we use Theorem 2.2.1 with $n_0 = 4$.

Base case. $2^4 = 16 \geq 16 = 4^2$.

Inductive step. Let $n \geq 4$ and suppose $2^n \geq n^2$. Then $2^{n+1} = 2 \cdot 2^n \geq 2n^2$ by Definition 2.3.2 and the hypothesis. Moreover $2n^2 \geq (n+1)^2$, because $2n^2 - (n+1)^2 = n^2 - 2n - 1 = (n-1)^2 - 2$, and $(n-1)^2 \geq 9 > 2$ for $n \geq 4$. Hence $2^{n+1} \geq (n+1)^2$.

By Theorem 2.2.1, $2^n \geq n^2$ for every $n \geq 4$.

The base cannot be 3, because $P(3)$ is false: $2^3 = 8 < 9 = 3^2$. The step is valid from $n = 3$ on, since $(n-1)^2 - 2 \geq 2$ for $n \geq 3$, but it is useless at 3, where its hypothesis is false. At $n = 2$ the step fails $((2-1)^2 - 2 = -1)$, which is why the true $P(2)$ does not lead to $P(3)$.

Exercise. B3: A closed form

The sequence $a_0 := 0$, $a_{n+1} := 2a_n + 1$ is defined by Theorem 2.3.1. Compute its first five values, guess a formula for a_n , and prove it.

Solution. The values are 0, 1, 3, 7, 15: one less than 1, 2, 4, 8, 16. We prove $a_n = 2^n - 1$ for every $n \in \mathbb{N}$. For $n = 0$: $a_0 = 0 = 2^0 - 1$. If $a_n = 2^n - 1$, then

$$a_{n+1} = 2(2^n - 1) + 1 = 2^{n+1} - 1,$$

using $2 \cdot 2^n = 2^{n+1}$ (Definition 2.3.2). By Logic and Proof, Axiom 4.2.1, $a_n = 2^n - 1$ for every $n \in \mathbb{N}$. The induction follows the two clauses of the definition: the base case is the starting value, the step is the rule.

2.3.6.3 C. Going deeper

Exercise. C1: Powers of two

Prove that every $n \in \mathbb{Z}_{>0}$ can be written as $2^k q$ with $k \in \mathbb{N}$ and q odd (that is, $q = 2j + 1$ for an integer j). Below, the proof is started; the second half is blank. *Name the move, then complete it.*

Suppose not. Then the set F of $n \in \mathbb{Z}_{>0}$ that cannot be written in this form is non-empty, and $F \subseteq \mathbb{N}$; let m be its least element. Then $m \geq 1$, and m is not odd, since otherwise $m = 2^0 m$ would be of the required form. _____

Why is the statement made for $n \geq 1$ only?

Solution. The move is the **smallest counterexample** of Section 2.2: suppose the claim fails, take the least failure by well-ordering (Theorem 2.1.3), and produce a smaller failure.

Completion. By Theorem 2.2.3 with divisor 2, every integer is even or odd; m is not odd, so $m = 2m'$ for an integer m' . Since $m > 0$, $m' = m/2 > 0$, so $m' \in \mathbb{Z}_{>0}$ (Proposition 2.1.2 (b)), and $m' < 2m' = m$. As m is the least element of F , $m' \notin F$, so $m' = 2^k q$ with $k \in \mathbb{N}$ and q odd. Then

$$m = 2 \cdot 2^k q = 2^{k+1} q$$

by Definition 2.3.2, and $k+1 \in \mathbb{N}$ by (NS). So m has the required form, contradicting $m \in F$. Hence $F = \emptyset$, and every $n \in \mathbb{Z}_{>0}$ is $2^k q$ with q odd.

The restriction to $n \geq 1$ is needed: $0 = 2^k q$ forces $q = 0$, since $2^k > 0$ (Proposition 2.3.4 (e)), and $0 = 2 \cdot 0$ is even, not odd (Theorem 2.2.3: not both). So 0 is a genuine counterexample, and in the proof it is excluded by taking $m \in \mathbb{Z}_{>0}$, which is what makes $m' > 0$.

Marking scheme. (10 points) - 2: names the move (smallest counterexample) and says that the least element m exists by well-ordering (Theorem 2.1.3). - 2: from “ m is not odd” concludes $m = 2m'$ with $m' \in \mathbb{Z}$, citing even-or-odd. - 3: shows $m' \in \mathbb{Z}_{>0}$ and $m' < m$, so $m' \notin F$. - 2: writes $m = 2^{k+1} q$ with $k+1 \in \mathbb{N}$ and reaches the contradiction. - 1: explains why $n = 0$ is excluded. Fatal errors (0 for the step): concluding $m' \notin F$ (or applying the induction hypothesis to m') without having shown both $m' < m$ and $m' \geq 1$; missing either one is fatal. A reader who restarts by Theorem 2.2.2 with base 1 earns the points for the other steps (the induction hypothesis at m' replaces “ $m' \notin F$ ”), but not the 2 points for naming the move.

Exercise. C2: Bernoulli beyond its hypothesis

- Show that $(1+x)^n \geq 1+nx$ holds for $x = -2$ and every $n \in \mathbb{N}$.
- Say which line of the proof of Theorem 2.3.7 fails at $x = -2$, and why the statement survives anyway.
- At $x = -4$, find the first n where the inequality fails, and the first n where the step “ $P(n) \Rightarrow P(n+1)$ ” fails.

Solution.

- At $x = -2$ the claim is $(-1)^n \geq 1-2n$. By the remark after Proposition 2.3.4, $(-1)^n$ is 1 or -1 . For $n = 0$ the claim reads $1 \geq 1$. For $n \geq 1$, $1-2n \leq -1 \leq (-1)^n$.
- The line “multiplying the induction hypothesis by $1+x$ ” fails. At $x = -2$ the multiplier is $1+x = -1 < 0$, and multiplying $(1+x)^n \geq 1+nx$ by a negative number **reverses** it: we get $(1+x)^{n+1} \leq (1+nx)(1+x)$, the wrong direction. The rest of the proof ($nx^2 \geq 0$) still holds. The statement survives because (a) proves it by a different argument, which uses the special values $(-1)^n = \pm 1$. A proof that fails does not make its conclusion false.
- At $x = -4$: $n = 0$ gives $1 \geq 1$; $n = 1$ gives $-3 \geq -3$; $n = 2$ gives $9 \geq -7$; $n = 3$ gives $-27 \geq -11$, false. So the first failure is $n = 3$. The step $P(n) \Rightarrow P(n+1)$ holds for $n = 0$ and $n = 1$ (both sides are true) and fails at $n = 2$, where $P(2)$ is true and $P(3)$ false.

Exercise. C3: Two identities at once

Use [Corollary 2.3.3](#) to define the sequence $F_0 := 0$, $F_1 := 1$, $F_{n+2} := F_{n+1} + F_n$; name X , a , b and h . Then prove, for every $n \in \mathbb{N}$, the statement $P(n)$:

$$F_{2n+1} = F_n^2 + F_{n+1}^2 \quad \text{and} \quad F_{2n+2} = F_{n+1}(F_n + F_{n+2}).$$

Check $P(0)$, $P(1)$ and $P(2)$ numerically first.

Solution (Hint 1). Neither identity carries its own one-step inductive step: passing from F_{2n+1} to F_{2n+3} needs F_{2n+2} , which is the other identity. Prove both together, and use $F_n + F_{n+1} = F_{n+2}$ to merge terms.

Solution (Hint 2). In the step, start with $F_{2n+3} = F_{2n+2} + F_{2n+1}$ and substitute both halves of $P(n)$.

Solution. The definition. [Corollary 2.3.3](#) with $X = \mathbb{R}$, $a = 0$, $b = 1$ and $h(n, x, y) = x + y$ gives exactly one sequence with $F_0 = 0$, $F_1 = 1$ and $F_{n+2} = F_n + F_{n+1}$. Its first values are 0, 1, 1, 2, 3, 5, 8.

Small cases. $P(0)$: $F_1 = 1 = 0^2 + 1^2$ and $F_2 = 1 = 1 \cdot (0 + 1)$. $P(1)$: $F_3 = 2 = 1^2 + 1^2$ and $F_4 = 3 = 1 \cdot (1 + 2)$. $P(2)$: $F_5 = 5 = 1^2 + 2^2$ and $F_6 = 8 = 2 \cdot (1 + 3)$.

Proof. We use Logic and Proof, Axiom 4.2.1. $P(0)$ was checked. Suppose $P(n)$. Using the recursion and then both halves of $P(n)$,

$$\begin{aligned} F_{2n+3} &= F_{2n+2} + F_{2n+1} \\ &= F_{n+1}F_n + F_{n+1}F_{n+2} + F_n^2 + F_{n+1}^2 \\ &= F_n(F_n + F_{n+1}) + F_{n+1}F_{n+2} + F_n^2 \\ &= F_{n+2}(F_n + F_{n+1}) + F_{n+1}^2 = F_{n+2}^2 + F_{n+1}^2, \end{aligned}$$

where the last two lines use $F_n + F_{n+1} = F_{n+2}$ twice. This is the first half of $P(n+1)$. For the second half,

$$\begin{aligned} F_{2n+4} &= F_{2n+3} + F_{2n+2} \\ &= F_{n+1}^2 + F_{n+2}^2 + F_{n+1}F_n + F_{n+1}F_{n+2} \\ &= F_{n+1}(F_{n+1} + F_n) + F_{n+2}^2 + F_{n+1}F_{n+2} \\ &= F_{n+2}(2F_{n+1} + F_{n+2}) = F_{n+2}(F_{n+1} + F_{n+3}), \end{aligned}$$

using the first half of $P(n+1)$ just proved, the second half of $P(n)$, $F_{n+1} + F_n = F_{n+2}$, and finally $F_{n+1} + F_{n+2} = F_{n+3}$. So $P(n+1)$ holds, and by Logic and Proof, Axiom 4.2.1 $P(n)$ holds for every $n \in \mathbb{N}$.

The second identity is written with F_{n+2} rather than in the form $F_{2n} = F_n(F_{n-1} + F_{n+1})$, so that both identities make sense on all of $\mathbb{N}$ and no F_{-1} is needed. The two identities hold together, and together they carry a one-step induction that neither carries alone: this is “prove more” ([Example \(Proving more to prove anything\)](#)) in the form of a pair, as in the two-step example after [Definition 2.3.2](#). (A two-step induction can prove the first identity alone; see the marking scheme.)

Marking scheme. (10 points) - 2: defines the sequence by [Corollary 2.3.3](#), naming X , a , b and h . - 1: checks the base case $P(0)$, both halves. - 3: proves the first identity at $n + 1$ (or for all n): $F_{2n+3} = F_{n+1}^2 + F_{n+2}^2$. - 3: proves the second identity at $n + 1$ (or for all n): $F_{2n+4} = F_{n+2}(F_{n+1} + F_{n+3})$. - 1: concludes by induction (one-step or two-step), with a hypothesis that covers every value the step uses. Alternative route: 3 for proving $F_{2n+1} = F_n^2 + F_{n+1}^2$ alone by a two-step induction (via $F_{k+2} = 3F_k - F_{k-2}$ for $k \geq 2$ and the matching recursion for $F_n^2 + F_{n+1}^2$, with both bases $n = 0, 1$ checked), and 3 for deriving the second identity as $F_{2n+2} = F_{2n+3} - F_{2n+1} = F_{n+2}^2 - F_n^2 = F_{n+1}(F_n + F_{n+2})$. Fatal errors (0 for the step): inducting on one identity alone while using the other at n unproved; using the identities at $n + 1$ to prove themselves.