Strong Induction and the Well-Ordering Principle

Table of contents

Strong mathematical induction 1
How many base cases? 2
The well-ordering principle for the integers 5
MI, SMI and the WOP are equivalent 5
See also 8

Strong mathematical induction, the well-ordering principle for the integers, and the sense in which these two and ordinary induction are all the same tool. See mathematical-induction[1] for ordinary induction and the four-step proof template both methods share.

Strong mathematical induction

Let $P(n)$ be a predicate written in terms of some integer n. The difference from ordinary induction is entirely in what the inductive step is allowed to assume: **every** earlier case, not just the immediately preceding one — and, to pay for that, a basis step that establishes several cases rather than one.

	Ordinary induction (MI)	Strong induction (SMI)
Basis step	$P(2)$	$P(2) \wedge P(3) \wedge P(4)$
Inductive step	$\forall k \in \mathbb{Z}$ with $k \geq 2$, if $P(k)$ then $P(k+1)$	$\forall k \in \mathbb{Z}$ with $k \geq 4$, if $P(2) \wedge P(3) \wedge \cdots \wedge P(k)$ then $P(k+1)$
Conclusion	$P(n)$ for each integer $n \geq 2$	$P(n)$ for each integer $n \geq 2$

Both reach the same conclusion by the same kind of chain. For MI, $P(5)$ follows from $P(2)$ by three applications of the implication; for SMI with the basis above, $P(6)$ follows in two.

[1] courses/math1061/mathematical-induction.pdf

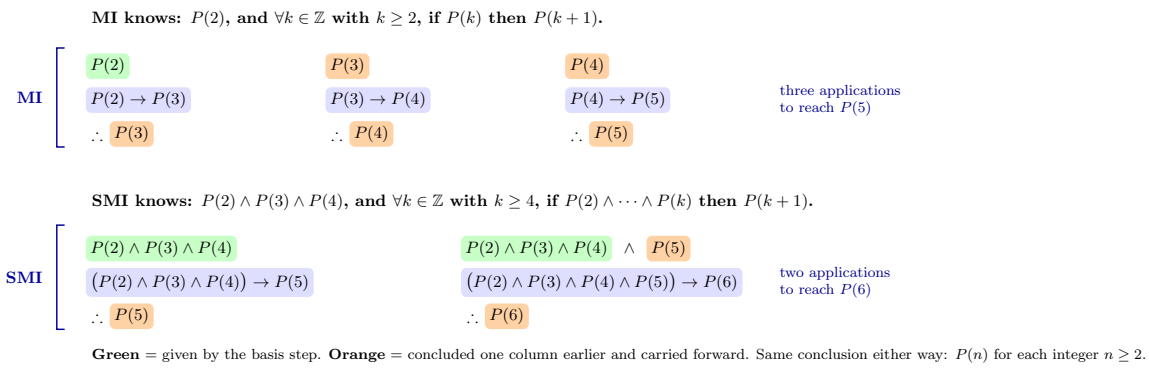


Figure 1: Mathematical induction and strong mathematical induction as chains of inferences. Each column is an argument — premises stacked, conclusion prefixed by $\therefore$, no rule line. MI climbs one rung at a time from a single base case; SMI starts from three base cases and each step may lean on everything established so far, which is why it lands on P(6) in two moves rather than four. Colour tracks one expression as it moves: green is what the basis step supplies, orange is a statement concluded one column earlier and carried forward. There are no arrows between columns — the repeated colour alone shows where a statement moves.

How many base cases?

As many as the inductive step reaches back for. This is the whole reason the basis step of an SMI proof is not a single case, and the answer to "why two values and not three?"

Count *how far back* the recurrence reaches, not how many terms it uses — those differ. $a_n = a_{n-1} - a_{n-3}$ uses only two earlier terms, but the deepest is three positions back, so all three of $P(0), P(1), P(2)$ must be established or the step could reach for an unproven case.

If the basis step establishes fewer cases than the inductive step consumes, the chain has a hole in it: the first few applications of the inductive step would reach for a case nobody ever proved.

Worked example — a two-term recurrence

Suppose $b_1, b_2, b_3, \ldots$ is defined by $b_1 = 4$, $b_2 = 12$, and $b_n = b_{n-2} + b_{n-1}$ for each integer $n \geq 3$. Prove that $4 \mid b_n$ for each integer $n \geq 1$.

> *Proof.* Let $P(n)$ be the predicate $4 \mid b_n$.
>
> **Basis step.** We know that $b_1 = 4$ and $b_2 = 12$. Since $4 \mid 4$ and $4 \mid 12$, $P(1)$ is true and $P(2)$ is true.

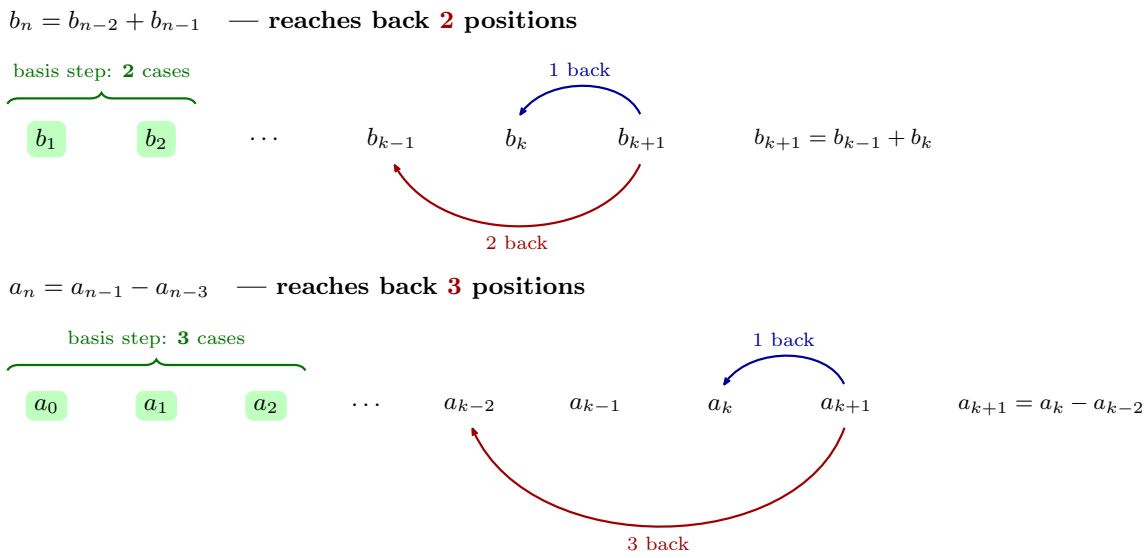


Figure 2: How many base cases a strong induction needs, on the two sequences worked below: b_n = b_{n-2} + b_{n-1} and a_n = a_{n-1} − a_{n-3}. Both use exactly two earlier terms, so counting terms gives the wrong answer; what settles it is the longest arrow. Reaching two positions back means the basis step must cover two cases; reaching three means three. The terms sit in a row, and each short curved arrow is labelled with what it does.

Inductive hypothesis. Suppose $k \geq 2$ is an integer and that $P(1), P(2), \ldots, P(k)$ are true. Since $P(k)$ is true, $b_k = 4x$ for some $x \in \mathbb{Z}$. Since $P(k-1)$ is true, $b_{k-1} = 4y$ for some $y \in \mathbb{Z}$.

Inductive step. Consider $n = k + 1$:

$$\begin{aligned} b_{k+1} = b_{k-1} + b_k &= 4y + 4x \qquad \text{(by the inductive hypothesis)} \\ &= 4(y + x) \end{aligned}$$

Thus $4 \mid b_{k+1}$, so $P(k+1)$ is true.

Therefore, by PSMI, for each integer $n \geq 1$, $4 \mid b_n$. □

Note where strong induction actually earns its keep: the step uses $P(k)$ **and** $P(k-1)$. Ordinary induction only hands you $P(k)$, which is not enough to say anything about b_{k-1}.

Worked example — every integer $n > 1$ is a product of primes

Theorem. Every integer $n > 1$ can be written as a product of primes.

Proof. Let $P(n)$ be the predicate *n can be written as a product of primes*, for $n \geq 2$.

Basis step. $n = 2$ is prime and thus is a product of primes, so $P(2)$ is true.

Inductive step. Suppose that for some integer $k \geq 2$, every integer $2, 3, \ldots, k$ can be written as a product of primes — that is, $P(2) \wedge P(3) \wedge \cdots \wedge P(k)$. We now need to prove that $k + 1$ is a product of primes. Since $k + 1 > 1$, either $k + 1$ is prime or $k + 1$ is composite.

- *Case 1: $k + 1$ is prime.* Then $k + 1$ is a product of primes.
- *Case 2: $k + 1$ is composite.* Then $k + 1 = rs$ for some positive integers $r \neq 1$ and $s \neq 1$. This implies $1 < r < k + 1$ and $1 < s < k + 1$. So by the inductive hypothesis — specifically $P(r)$ and $P(s)$ — both r and s are products of primes. Let $r = p_1 p_2 \ldots p_a$ and $s = q_1 q_2 \ldots q_b$ where the p_i and q_j are primes; thus $k + 1 = rs = p_1 p_2 \ldots p_a q_1 q_2 \ldots q_b$ is a product of primes.

In either case, $k + 1$ is a product of primes.

Therefore, by SMI, every integer $n > 1$ can be written as a product of primes. □

Why strong induction and not ordinary induction? Because r and s can be *any* integers from 2 to k — the factorisation gives no control over which — so the proof needs the inductive hypothesis available at all of those values, not just at k.

The well-ordering principle for the integers

> Let S be a **non-empty** set of integers, each of which is **greater than some fixed integer**. Then S has a **least element**.

Four pieces of terminology, all load-bearing:

- **non-empty** — the empty set has no least element, trivially.
- **of integers** — not of rationals or reals. This clause is not decoration: the positive rationals are non-empty *and* bounded below by 0, and still have no least element, because between any candidate and 0 there is always another one (halve it). See 2026-08-27-strong-induction-and-well-ordering[2].
- **greater than some fixed integer** — S must be bounded below. Without this the principle fails: $\mathbb{Z}^-$ is a non-empty set of integers with no least element.
- **a least element** — an element *of* S that is $\leq$ every element of S. It lives inside the set, not outside it.

Example — integers congruent to $1 \bmod 4$

True or false? The set of all integers congruent to $1 \bmod 4$ has a least element.

False. The set is $\{\dots, -7, -3, 1, 5, 9, \dots\}$.

> Suppose this set did have a least element, call it x. Then, since $x \equiv 1 \pmod 4$, we have $x - 4 \equiv 1 \pmod 4$, so $x - 4$ is also in the set. But $x - 4$ is smaller than x — a contradiction. $\square$

The set is non-empty, but it fails the "bounded below" condition, so the well-ordering principle simply does not apply to it.

MI, SMI and the WOP are equivalent

Anything provable by one is provable by the other two. Two of the translations:

SMI $\to$ MI: reword the statement. A strong-induction proof of $P(n)$ becomes an ordinary-induction proof of the *accumulated* predicate

$$Q(n) \;\equiv\; P(0) \wedge P(1) \wedge \cdots \wedge P(n)$$

Assuming $Q(k)$ in ordinary induction gives you exactly what assuming $P(0), \dots, P(k)$ gave you in strong induction. (Epp, Q27 p. 279.)

[2] courses/math1061/2026-08-27-strong-induction-and-well-ordering.pdf

MI → WOP: argue by contradiction. Suppose the set of integers $\geq a$ for which $P(n)$ is *false* is non-empty. It is bounded below by a, so by the WOP it has a least element; derive a contradiction from that least element. (Epp, Q31 p. 279.)

The same theorem, three ways

Suppose $a_0, a_1, a_2, \ldots$ is defined by $a_0 = 6$, $a_1 = 9$, $a_2 = 12$ and $a_n = a_{n-1} - a_{n-3}$ for each integer $n \geq 3$. Prove that for all integers $n \geq 0$, $3 \mid a_n$.

By SMI.

Let $P(n)$ be the predicate $3 \mid a_n$.

Basis step. $a_0 = 6$, $a_1 = 9$ and $a_2 = 12$. Since $3 \mid 6$, $3 \mid 9$ and $3 \mid 12$, $P(0)$, $P(1)$ and $P(2)$ are true.

Inductive hypothesis. Suppose $k \geq 2$ is an integer and that $P(0), P(1), \ldots, P(k)$ are true. Since $P(k-2)$ is true, $a_{k-2} = 3y$ for some $y \in \mathbb{Z}$; since $P(k)$ is true, $a_k = 3x$ for some $x \in \mathbb{Z}$.

Inductive step. Consider $n = k+1$: $a_{k+1} = a_k - a_{k-2} = 3x - 3y = 3(x-y)$. Thus $3 \mid a_{k+1}$, so $P(k+1)$ is true.

Therefore, by PSMI, for each integer $n \geq 0$, $3 \mid a_n$. □

By MI, on the reworded predicate.

Let $Q(n)$ be the predicate $3 \mid a_j$ *for all integers* j *where* $0 \leq j \leq n$ — that is, $Q(n) \equiv P(0) \wedge P(1) \wedge \cdots \wedge P(n)$.

Basis step. Consider $n = 2$. Since $3 \mid a_0$, $3 \mid a_1$ and $3 \mid a_2$, $Q(2)$ is true.

Inductive hypothesis. Suppose $k \geq 2$ is an integer and that $Q(k)$ is true. Since $Q(k)$ is true and $k \geq 2$, $a_k = 3x$ and $a_{k-2} = 3y$ for some $x, y \in \mathbb{Z}$.

Inductive step. Consider $n = k+1$: $a_{k+1} = a_k - a_{k-2} = 3x - 3y = 3(x-y)$. Thus $3 \mid a_{k+1}$. Since $Q(k)$ already gives $3 \mid a_i$ for every $0 \leq i \leq k$, adding $3 \mid a_{k+1}$ gives $Q(k+1)$.

(That last step is the point of rewording the predicate: $Q(k+1)$ is a conjunction over *all* indices up to $k+1$, so it needs $Q(k)$ **and** the new case — $3 \mid a_{k+1}$ alone would not establish it.)

Therefore, by PMI, for each integer $n \geq 0$, $3 \mid a_n$. □

The two proofs have the *same* algebraic core: the line $a_{k+1} = a_k - a_{k-2} = 3x - 3y = 3(x - y)$ is identical in each. All the reworded predicate does is let a single assumption, $Q(k)$, carry the several earlier facts the algebra needs.

Two details of the MI proof are easy to get wrong:

- **The basis is $n = 2$, not $n = 0$.** $Q(2)$ already asserts $3 \mid a_0$, $3 \mid a_1$ *and* $3 \mid a_2$, so verifying $Q(2)$ discharges all three of the SMI proof's base cases in one statement. Three base cases have not disappeared; they have been packed into one predicate.
- **The step concludes $Q(k+1)$, not $P(k+1)$.** An ordinary induction on Q has to deliver $Q(k+1)$, and $3 \mid a_{k+1}$ on its own does not — it needs $Q(k)$ alongside it.

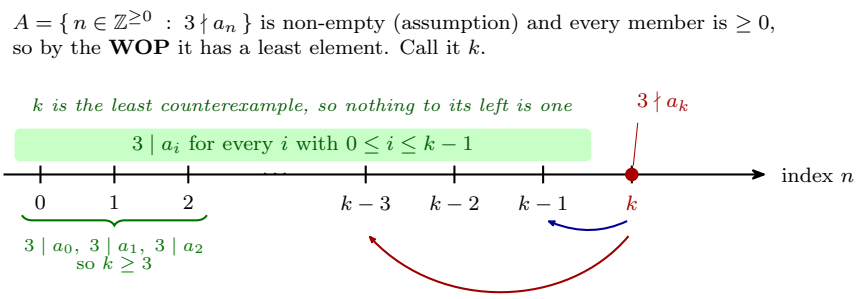
The conjunction in Q starts at $P(0)$, not $P(1)$. The predicate is $3 \mid a_j$ *for all integers j where* $0 \le j \le n$, so $Q(2) \equiv P(0) \wedge P(1) \wedge P(2)$ — which is also what the basis step checks.

By the WOP, by contradiction.

> Suppose the statement is false, so there exists an integer $n \ge 0$ such that 3 does not divide a_n. Let
>
> $$A = \{\, n \in \mathbb{Z}^{\ge 0} \;:\; 3 \nmid a_n \,\}$$
>
> By the WOP and our assumption, A has a least element — the smallest n for which $3 \nmid a_n$. Call it k. Thus $3 \nmid a_k$, but $3 \mid a_i$ for all $0 \le i \le k-1$.
>
> Note that $k \ge 3$, since a_0, a_1 and a_2 are all divisible by 3.
>
> Thus $a_{k-1} = 3x$ and $a_{k-3} = 3y$ for some $x, y \in \mathbb{Z}$, so
>
> $$a_k = a_{k-1} - a_{k-3} = 3x - 3y = 3(x - y)$$
>
> Thus $3 \mid a_k$, which is a contradiction.
>
> Therefore, for each integer $n \ge 0$, $3 \mid a_n$. $\square$

Reading the WOP proof next to the SMI one: "let k be the least counterexample" plays the role of the inductive hypothesis (everything below k works), and "$3 \mid a_k$, contradiction" plays the role of the inductive step. Drawn on the index line, the whole proof is one picture:

Note which term the WOP proof reaches for. The SMI proof used a_k and a_{k-2} to build a_{k+1}; the WOP proof is standing at k rather than at $k+1$, so the same recurrence reads $a_k = a_{k-1} - a_{k-3}$ and it reaches for a_{k-1} and a_{k-3}. Same recurrence, index shifted by one — and that shift is why the "$k \ge 3$" line has to be there.



Both arrows land inside the green stretch (this is what $k \geq 3$ buys), so $a_{k-1} = 3x$ and $a_{k-3} = 3y$ for some $x, y \in \mathbb{Z}$:

$$a_k = a_{k-1} - a_{k-3} = 3x - 3y = 3(x-y) \quad \text{— so } 3 \mid a_k \text{ after all. Contradiction.}$$

Figure 3: The well-ordering proof of 3 | a_n as a picture of its own least counterexample. Everything to the left of k is green not because it was proved, but because k was chosen least — that single step is the only place the WOP is used, and it is exactly what the strong inductive hypothesis supplies in the SMI proof. The least element here is the smallest number that gives a contradiction. k 3 is what guarantees both arrows land inside the green stretch, since a_{k-3} has to be a term of the sequence at all.

Spotting a WOP proof

A proof is using the well-ordering principle whenever it says **"choose the smallest such n"** about a set it has just argued is non-empty. That phrase is not free — it is the WOP being invoked, and it needs the set to be non-empty and bounded below.

For instance, the primes theorem above can be rewritten as a contradiction proof: suppose some integer $n > 1$ is not a product of primes; by the WOP, choose the smallest such n; then n is prime (done) or $n = rs$ with $1 < r, s < n$, and both r and s *are* products of primes precisely because n was chosen smallest — contradicting the choice of n. Structurally it is the SMI proof with the induction turned inside out.

See also

- mathematical-induction[3] · proof-techniques[4] · sequences-and-summations[5]

[3] courses/math1061/mathematical-induction.pdf
[4] courses/math1061/proof-techniques.pdf
[5] courses/math1061/sequences-and-summations.pdf

- recursive-definitions[6] · solving-recurrence-relations[7] — where a two-term recurrence forces the strong hypothesis
- trees[8] — strong induction on the number of vertices: a tree with n vertices has $n-1$ edges
- 2026-08-27-strong-induction-and-well-ordering[9] — Lecture 14
- practice-problems[10] — §18, with full worked solutions

[6] courses/math1061/recursive-definitions.pdf
[7] courses/math1061/solving-recurrence-relations.pdf
[8] courses/math1061/trees.pdf
[9] courses/math1061/2026-08-27-strong-induction-and-well-ordering.pdf
[10] courses/math1061/practice-problems.pdf