Lecture 14 — Strong Mathematical Induction and the Well-Ordering Principle

Table of contents

Learning goals 1
Base cases, least elements and equivalence 2
Mathematical induction vs strong mathematical induction 2
The well-ordering principle for the integers 4
MI, SMI and the WOP on one example 6
Mathematical induction to prove a divisibility property 9
See also 10

Pre-work: Video 018 (Strong Mathematical Induction and the Well-Ordering Principle). See strong-induction-and-the-well-ordering-principle[1] for the principles themselves, the MI/SMI comparison and the worked examples; the questions worked below apply them. mathematical-induction[2] has the ordinary-induction template both methods share.

Learning goals

1. Gain fluency in applying the principles of **mathematical induction** and **strong mathematical induction**.
2. Further your understanding of how the **basis step** relates to the **inductive step** in mathematical induction and strong mathematical induction.
3. Appreciate the **equivalence** between mathematical induction, strong mathematical induction and the well-ordering principle for the integers.

[1] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf
[2] courses/math1061/mathematical-induction.pdf

Base cases, least elements and equivalence

Why does pre-class Q1 need 2 values for the basis step, not 3? Because the recurrence in that question, $b_n = b_{n-2} + b_{n-1}$, reaches back exactly **two** terms — so the inductive step consumes $P(k-1)$ and $P(k)$, and the basis step has to cover $P(1)$ and $P(2)$ for the chain to have somewhere to start. Worked in full below. Contrast the sequence $a_n = a_{n-1} - a_{n-3}$ further down, whose recurrence reaches back three terms and therefore needs three base cases.

In the well-ordering principle — non-empty set, fixed integer, a least element — is the least element an integer in the set or one outside it? In the set — a least element of S is a member of S that is $\leq$ every member of S, not a bound sitting outside it. (A lower bound *is* allowed to sit outside: the "fixed integer" in the statement is any integer below everything in S, and it need not belong to S — -1 plays that role for the set of squares below. The two ideas are easy to run together, and the difference is the whole content of the principle: bounds are cheap, a *least element* is what the WOP promises.) The terminology is unpacked in strong-induction-and-the-well-ordering-principle[3]; four sets are tested against the principle below and drawn together in one figure.

Why are mathematical induction, strong mathematical induction and the well-ordering principle for the integers all equivalent? Anything provable by one is provable by the other two — SMI becomes MI by rewording the predicate to accumulate every earlier case (Epp Q27 p. 279), and MI becomes the WOP by contradiction on the set of counterexamples (Epp Q31 p. 279). One example is proved all three ways; see the same note.

Mathematical induction vs strong mathematical induction

The two differ only in what the inductive step may assume, and correspondingly in how much the basis step must establish. Given the basis $P(2) \wedge P(3) \wedge P(4)$ and the SMI inductive step $\forall k \geq 4$, $(P(2) \wedge \cdots \wedge P(k)) \to P(k+1)$, we reach $P(6)$ in two applications — and in fact $P(n)$ for each integer $n \geq 2$, exactly as ordinary induction does from $P(2)$ alone. Side-by-side in strong-induction-and-the-well-ordering-principle[4].

Worked: $4 \mid b_n$ (pre-class Q1)

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 $n \geq 1$.

The recurrence reaches back two terms, so this **needs two base cases**. The proof is by **PSMI**. The first few terms:

[3] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf
[4] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf

$$b_3 = b_1 + b_2 = 4 + 12 = 16 \qquad b_4 = b_2 + b_3 = 12 + 16 = 28$$

The full proof by strong induction is in strong-induction-and-the-well-ordering-principle[5]. The point of the example: the inductive step uses both $P(k)$ and $P(k-1)$, which is exactly what ordinary induction cannot supply.

Worked: a recurrence that reaches back three terms

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 $n \geq 3$.

(a) Determine the value of a_4.

a_4 cannot be reached in one step, because the recurrence at $n = 4$ asks for a_3, which has not been computed yet. Two steps:

$$a_3 = a_2 - a_0 = 12 - 6 = 6 \qquad a_4 = a_3 - a_1 = 6 - 9 = -3$$

The sequence is not monotone and not positive — $6, 9, 12, 6, -3, \ldots$ — so nothing about "divisible by 3" can be read off a pattern of growth. It has to be proved.

(b) In a proof by strong mathematical induction that $3 \mid a_n$ for each integer $n \geq 0$, what would you need to prove in the basis step?

With $P(n)$ the predicate $3 \mid a_n$, the recurrence reaches back **three** terms, so the basis step needs **three cases**:

$$P(0) : \ 3 \mid a_0 \qquad P(1) : \ 3 \mid a_1 \qquad P(2) : \ 3 \mid a_2$$

The count is read straight off the recurrence: the term a_{n-3} means **3 cases**. It is the *deepest* back-reference that sets the number, not the number of terms on the right-hand side — strong-induction-and-the-well-ordering-principle[6] has a figure contrasting this recurrence with the one for b_n above.

This is the sequence used below to compare three separate proofs of $3 \mid a_n$ — by SMI, by MI, and by the WOP.

[5] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf
[6] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf

Every integer $n > 1$ is a product of primes

Proved by strong induction, splitting on whether $k+1$ is prime or composite; written out in strong-induction-and-the-well-ordering-principle[7]. Strong induction is required rather than ordinary induction **because r and s in the factorisation $k+1 = rs$ can be any integers from 2 to k** — the proof has no control over which, so it needs the inductive hypothesis at all of those values.

The prose proof leaves the induction machinery implicit. It is worth writing each part out in terms of a predicate:

Part of the proof	In terms of P
the theorem	$P(n)$: *n can be written as a product of primes*, for $n \geq 2$ (the same as $n > 1$)
the basis step	$P(2)$
the inductive step	$(P(2) \wedge P(3) \wedge \cdots \wedge P(k)) \to P(k+1)$
"$1 < r < k+1$ and $1 < s < k+1$"	$P(r) \wedge P(s)$, both taken from the conjunction above
"In either case…"	$P(2) \wedge \cdots \wedge P(k) \to P(k+1)$ again, closing the step

Naming the predicate first, then writing out the exact implication the inductive step owes you, is what turns the prose proof into the course's induction skeleton.

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.

Three conditions. The four sets below test them — one per condition, plus one case where they all hold. The one that is easiest to forget is **"of integers"**: a set can be non-empty and bounded below and still have no least element, as long as it is not a set of integers. The set of positive rationals below is exactly that case.

Worked: the integers congruent to $1 \bmod 4$ (pre-class Q2)

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

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

[7] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf

> 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, so we have a contradiction.

The middle clause is the step the contradiction turns on: $x - 4$ being smaller only matters once you know it's *in the set*.

The set is non-empty, but not bounded below — so the WOP never applied to it in the first place.

Worked: which of these sets has a least element?

For each statement, decide if it is true or false, and how you would demonstrate that it is true or false.

(a) The set of positive rational numbers has a least element.

False — proof by contradiction.

> Suppose $\frac{p}{q}$ is the smallest possible positive rational, where $p, q \in \mathbb{Z}^+$. Then
>
> $$0 < \frac{1}{2} \cdot \frac{p}{q} < \frac{p}{q}$$
>
> So $\frac{p}{2q}$ is a smaller positive rational — contradiction.

Halving is the useful move here: it produces a strictly smaller element that is still in the set, which is exactly what "no least element" needs. The trick is worth remembering on its own, because "multiply by a factor strictly between 0 and 1" is the standard way to defeat a claimed least element in a dense set.

$\mathbb{Q}^+$, the set of positive rationals, *is* non-empty and *is* bounded below — by 0. It satisfies two of the WOP's three conditions and still has no least element. What it fails is "**set of integers**": between $\frac{p}{q}$ and 0 there is always more room, whereas between an integer x and a fixed lower bound there is not. So (a) is not the "not bounded below" failure that (b) and the mod-4 set are; it is a different failure entirely, and it is the reason the principle is called the well-ordering principle *for the integers*.

(b) Every non-empty subset of the integers has a least element.

False — take $S = \mathbb{Z}^-$; the proof is by contradiction. (A contradiction can be marked inline with a crossed X, a lightning stroke or $\perp$; the three are alternatives — see math1061-diagram-notation[8].) $\mathbb{Z}^-$ is non-empty and made of integers, but it has no least element. This is precisely

[8] courses/math1061/math1061-diagram-notation.pdf

the "greater than some fixed integer" hypothesis of the WOP failing: $\mathbb{Z}^-$ is not bounded below.

(c) Every non-empty subset of the set of squares x^2 where $x \in \mathbb{Z}$ has a least element.

True.

> Let $S \subseteq \mathbb{Z}$ with $S \neq \emptyset$ be a set of such squares. For all $x \in \mathbb{Z}$ we have $0 \leq x^2 \in \mathbb{Z}$, so $-1 < x^2$ for every $x^2 \in S$. So by the WOP, S has a least element.

The fixed integer that bounds S below is -1 (or 0) — squares cannot be negative, which is what makes the WOP applicable here and not in (b). The proof does *not* have to say which element is least, or produce it. The WOP is an existence statement, and the whole argument is the three-line check that its hypotheses hold.

MI, SMI and the WOP on one example

The claim $3 \mid a_n$, for the sequence $a_n = a_{n-1} - a_{n-3}$ above, can be proved three times over — by SMI, by MI on the reworded predicate $Q(n) \equiv P(0) \wedge P(1) \wedge \cdots \wedge P(n)$, and by the WOP taking the least counterexample. All three proofs share the same algebraic core, $a_{k+1} = a_k - a_{k-2} = 3x - 3y = 3(x - y)$, and in the SMI and MI proofs that line is identical. They differ only in how the earlier cases are made available. All three are written out in strong-induction-and-the-well-ordering-principle[9].

Three details of those proofs, all recorded in that note:

- The MI proof's basis step is $n = 2$, not $n = 0$, because $Q(2)$ is the statement that packs all three of $3 \mid a_0$, $3 \mid a_1$, $3 \mid a_2$ into one predicate.
- The MI proof's last step concludes $Q(k+1)$, not $P(k+1)$. An induction run on Q must conclude $Q(k+1)$.
- The WOP proof's "least element k" is the **least counterexample**, which is the same information the strong inductive hypothesis carries, obtained a different way.

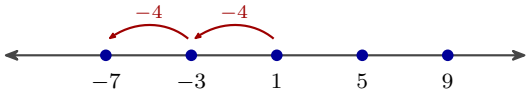
Worked: where the prime-factorisation proof uses the WOP

How does the following proof use the well-ordering principle for the integers?

> **Theorem:** every integer $n > 1$ can be written as a product of primes.
>
> **Proof:** suppose the theorem is false. Then there exists an integer $n > 1$ that is not a product of primes. Choose the smallest such number n. Since $n > 1$, then either n is prime or n is composite.

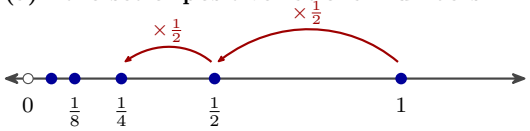
[9] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf

Q2 $S = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$**, the integers** $\equiv 1 \pmod 4$



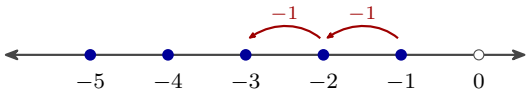
No least element. Whatever x you pick, $x - 4$ is still in S and is smaller. S is non-empty and made of integers, but it is **not bounded below** — so the WOP never applied to it.

2(a) the set of positive rational numbers



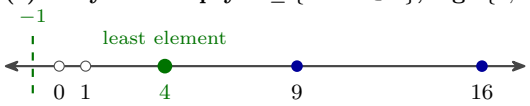
No least element. Halving $\frac{p}{q}$ gives $\frac{p}{2q}$, still positive and still rational. This set *is* bounded below (by 0) and non-empty — it fails only because it is **not a set of integers**, which the WOP requires.

2(b) $S = \mathbb{Z}^-$**, a non-empty subset of** $\mathbb{Z}$



No least element. Subtracting 1 always stays inside. Non-empty integers again, but **not bounded below** — the counterexample that disproves "every non-empty subset of $\mathbb{Z}$ has a least element".

2(c) any non-empty $S \subseteq \{x^2 : x \in \mathbb{Z}\}$**, e.g.** $\{4, 9, 16, \ldots\}$



Least element exists. Every square satisfies $0 \leq x^2$, so every member of S is greater than the fixed integer -1 (dashed). Non-empty, integers, bounded below: all three hypotheses hold, so the WOP delivers a least element.

Read the rows as the three hypotheses being tested one at a time. A set has no least element exactly when some move — -4, $\times\frac{1}{2}$, -1 — always produces a smaller member; the WOP says that for a non-empty, bounded-below set of *integers* no such move can exist.

Figure 1: Four sets tested against the well-ordering principle, and which of its conditions each one fails. A set has no least element exactly when some move always produces a smaller member still inside it — subtract 4, halve, subtract 1 — and each disproof is the exhibition of that move. The rows are drawn to scale: the mod-4 and negative-integer sets march off to the left forever, while the positive rationals stay bounded below by 0 and fail for a different reason, having no integrality to stop them accumulating. Open circles mark numbers not in the set. Each hop arrow is labelled by its operation.

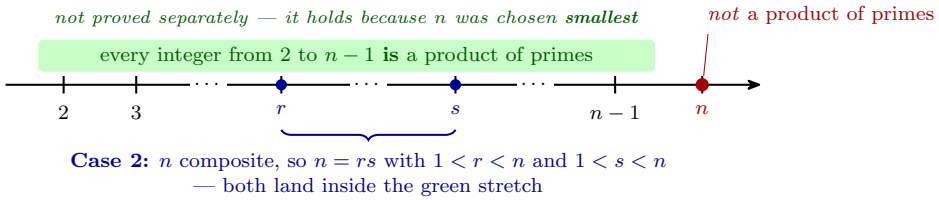
If n is prime, then n is a product of primes.

If n is composite, then $n = rs$ for some positive integers $r \neq 1$ and $s \neq 1$. This implies that $1 < r < n$ and $1 < s < n$. Because we chose n to be the smallest integer that is not a product of primes, both r and s (which are smaller) 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, and so $n = rs = p_1 p_2 \ldots p_a q_1 q_2 \ldots q_b$ is a product of primes also.

In either case, n is a product of primes, contradicting our choice of n. Therefore every integer $n > 1$ can be written as a product of primes.

At the step "choose the smallest such number n" — that is the well-ordering principle, and nothing else in the proof invokes it. Written in full, the step reads "**By the WOP we can** choose the smallest such number n". The proof has just established that the set of counterexamples is non-empty, and every member is an integer greater than 1, so the set is bounded below; the WOP is what licenses picking a least element out of it. Everything downstream ("because we chose n to be the smallest…") depends on that element existing.

The one WOP step: the counterexamples $\{\, n > 1 : n \text{ is not a product of primes} \,\}$ are integers, all greater than 1, and non-empty by assumption — so "choose the smallest such n" is legitimate. Nothing else in the proof uses the WOP.



So $r = p_1 p_2 \cdots p_a$ and $s = q_1 q_2 \cdots q_b$, hence $n = rs = p_1 p_2 \cdots p_a\, q_1 q_2 \cdots q_b$ — a product of primes.

Case 1: n prime — then n is a one-factor product of primes immediately.

Either way n *is* a product of primes, contradicting the choice of n.

Figure 2: The well-ordering proof that every integer n > 1 is a product of primes, drawn on the number line: the well-ordering principle is used once, and everything after it lives off that one step. The green stretch is not proved — it holds only because n was chosen smallest, and the whole proof consists of showing that the two factors of a composite n land inside it. Compare the same shape in the well-ordering proof of 3 | a_n: least counterexample, a stretch below it that is known to be fine, and a descent that lands inside that stretch. The r and s ticks are placed arbitrarily inside the range, since the argument fixes only that 1 < r, s < n.

Set this next to the strong-induction proof of the same theorem above and the two are the same argument turned inside out. Strong induction builds up: assume $P(2), \ldots, P(k)$, prove $P(k+1)$. The WOP version descends: assume some n fails, take the least such, and find that its factors — which are smaller, so they do *not* fail — hand you the very factorisation n was

supposed to lack. The green stretch in the figure is doing the job that "$P(2) \wedge \cdots \wedge P(k)$" does in the induction.

Mathematical induction to prove a divisibility property

Recall that for integers n and d with $d \neq 0$, $d \mid n$ if and only if there exists some integer a such that $n = da$ (see divisibility-and-factorisation[10]).

Worked: $5 \mid (7^n - 2^n)$

Prove that for each integer $n \geq 0$, $5 \mid (7^n - 2^n)$.

Let $P(n)$ be the predicate $5 \mid (7^n - 2^n)$.

Basis step ($P(0)$). When $n = 0$, $7^n - 2^n = 7^0 - 2^0 = 1 - 1 = 0 = 5 \times 0$. Therefore $5 \mid 0$, and so $P(0)$ is true.

Inductive step ($P(k) \to P(k+1)$). Suppose $P(k)$ is true for some $k \geq 0$. Then $5 \mid (7^k - 2^k)$, so there exists $b \in \mathbb{Z}$ such that $7^k - 2^k = 5b$. Thus $7^k = 5b + 2^k$.

Consider $P(k+1)$. Then

$$\begin{aligned} \text{LHS of } P(k+1) &= 7^{k+1} - 2^{k+1} = 7(7^k) - 2(2^k) \\ &= 7(5b + 2^k) - 2(2^k) \qquad \text{(by the inductive hypothesis } P(k)\text{)} \\ &= 5(7b) + (7-2)2^k = 5(7b + 2^k) \end{aligned}$$

Therefore $5 \mid (7^{k+1} - 2^{k+1})$, so $P(k) \to P(k+1)$. //

Conclusion. By the principle of mathematical induction, $5 \mid (7^n - 2^n)$ for each integer $n \geq 0$.

The idea: separate 7^k and 2^k out of $7^{k+1} - 2^{k+1}$, then use the inductive hypothesis to get rid of the 7^k. Replacing it with $5b + 2^k$ is what makes a factor of 5 appear; the two 2^k terms then collect into $(7-2)2^k$, which is another multiple of 5.

Two things about the shape of this one:

- **Ordinary induction, not strong.** Nothing here is a recurrence reaching back several terms — $P(k+1)$ is built out of $P(k)$ alone — so one base case is all it needs. It is the contrast to everything above it.

[10] courses/math1061/divisibility-and-factorisation.pdf

- **The end mark and the conclusion.** The double slash // closes the inductive step at "$P(k) \to P(k+1)$". The **Conclusion** line that follows, "by the principle of mathematical induction", completes the course's induction skeleton. (// is an end-of-proof mark; □ and no mark at all are also used — see math1061-diagram-notation[11], which records four options as sanctioned.)

See also

- strong-induction-and-the-well-ordering-principle[12] · mathematical-induction[13] · sequences-and-summations[14] · proof-techniques[15] · divisibility-and-factorisation[16]
- 2026-08-24-sequences-and-mathematical-induction[17] — Lecture 13
- practice-problems[18] — §18, with full worked solutions

[11] courses/math1061/math1061-diagram-notation.pdf
[12] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf
[13] courses/math1061/mathematical-induction.pdf
[14] courses/math1061/sequences-and-summations.pdf
[15] courses/math1061/proof-techniques.pdf
[16] courses/math1061/divisibility-and-factorisation.pdf
[17] courses/math1061/2026-08-24-sequences-and-mathematical-induction.pdf
[18] courses/math1061/practice-problems.pdf