NUMBER & ALGEBRA

Chapter 3

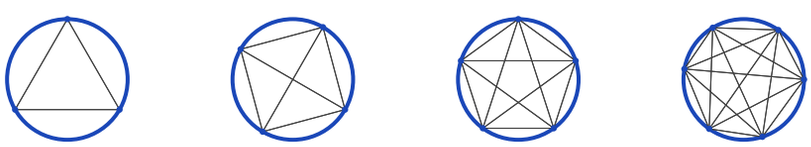
Proofs

3

SYLLABUS 1.6 1.15

Mark some points on a circle. Join every pair of points with a straight line. Then count the regions inside the circle. Place the points carefully, so that no three lines cross at the same spot. The first few cases give 1 region, then 2, then 4, then 8, then 16.

The pattern seems clear: each new point doubles the number of regions, so six points should give 32. In fact six points give **31**.



3 points, **4 regions** 4 points, **8 regions** 5 points, **16 regions** 6 points, **31 regions**

Figure 3.1 Every pair of points is joined by a chord (a straight line between two points on the circle), and no three chords meet at one point.

Five cases followed the doubling rule and the sixth did not. Nothing in the first five cases showed that the rule would fail, and no number of agreeing cases could have shown that it was true.

This is the difference between seeing a pattern and knowing that it always holds. A pattern is a guess. The word for such a guess is a **conjecture**: a statement believed true but not yet proved. The doubling rule was a conjecture, and the sixth case disproved it.

A **proof** is an argument in which each step follows from the one before, so the conclusion cannot be false. One proof covers every case at once, however many points you take.

By the end of this chapter you will be able to prove an identity by changing one side into the other, and prove a statement directly from definitions. You will also disprove a statement with a single counterexample, argue by contradiction, and prove a result about every positive integer by induction. These methods show that a formula or an identity is true in every case, not only in the cases you have checked. You will use them again for sums, derivatives and complex numbers.

© 2026 Hasan Khan Free for personal and classroom use www.bettermath.org

3.1 Deductive Proof

A proof is a chain of logical steps. It starts from things already accepted, such as definitions, results proved earlier, and the rules of algebra, and it ends at the statement you want to establish. Each step must follow with certainty from the steps before it. If the chain is correct, the conclusion is not just likely. It cannot be false.

A **mathematical statement** (or **proposition**) is a sentence that is either true or false, such as "7 is prime" or "$2^{10} > 1000$".

This is **deductive** reasoning: you apply general principles to reach a specific, guaranteed result. A familiar example is not mathematical at all:

- Every human being is mortal. (a general principle)
- Socrates is a human being. (a specific case)
- Therefore Socrates is mortal. (the conclusion)

The conclusion is not a guess, and no amount of further evidence could improve it. If the first two statements are true, the third cannot be false. Mathematics uses arguments of exactly this shape:

- Every multiple of 4 is even.
- The number 132 is a multiple of 4.
- Therefore 132 is even.

Notice that you did not divide 132 by 2 to check. The conclusion followed from the two statements above it.

The circle problem went in the opposite direction: there, a few particular cases were used to guess a general rule. Reasoning in that direction, from examples to a general claim, is called induction in the everyday sense of the word, and it can lead to a false conclusion. Deduction from true starting statements cannot.

Despite its name, *mathematical* induction (§3.4) is a form of deduction: it proves a rule for every positive integer from two facts that have been proved.

3.1.1 Equality versus identity

Before you prove a statement about an equation, you must know which kind of statement it is. The equals sign is used for two very different claims: that two expressions are equal for some values of the variable, or for every value.

DEFINITION 3.1 **Equation and identity**

An **equation** states that two expressions are equal. Solving it means finding every value of the variable for which it is true. An **identity** is an equation that is true for *every* value for which both sides are defined. An identity is written with the symbol $\equiv$:

$$(x+1)^2 \equiv x^2 + 2x + 1.$$

The equation $x^2 = 4$ is true only when $x = 2$ or $x = -2$. The identity $(x+1)^2 \equiv x^2 + 2x + 1$ is true for every real x. Solving an equation means finding the values that make it true; proving an identity means showing that no value makes it false.

The three-bar symbol $\equiv$ means the claim is "for all x", not "find x". The IB formula booklet and the rest of these notes write identities with $=$. There, the wording and the context tell you which kind of statement it is. This section uses $\equiv$ because the difference matters here.

You will meet one important identity in trigonometry:

$$\sin^2 x + \cos^2 x \equiv 1.$$

It is proved and used in Ch. 8.

3.1.2 Proving an identity

The two sides of an identity have names. The expression to the left of the $\equiv$ sign is the **left-hand side**, written **LHS**. The expression to the right is the **right-hand side**, written **RHS**.

To prove an identity you take one side and transform it, step by step, into the other, using only valid algebra. Start from the more complicated side and simplify it: write down that side, change it one line at a time, and finish with the other. Write the labels LHS and RHS in your working, so the direction of the argument is clear to the marker. If a side contains a fraction, first state the values for which it is defined; the identity is claimed for those values only.

When the proof is finished, check it with numbers. Substitute simple values into both sides; if the two sides differ, there is an error. A check is not a proof, because it covers one case only, but a failed check shows that something is wrong.

CAUTION Do not start by assuming the identity is true and then manipulate both sides until you reach something obvious like $0 = 0$. Reaching a true statement proves nothing about the starting line unless every step can be reversed. For example, start from the false statement $-1 = 1$ and square both sides: the result, $1 = 1$, is true. Squaring cannot be reversed, so the true result says nothing about the start. Transform *one* side into the other instead.

EXAMPLE 3.1

Prove that $(a+b)^2-(a-b)^2 \equiv 4ab$.

SOLUTION

Start from the LHS and expand each square:

$$\text{LHS} = (a+b)^2-(a-b)^2 = (a^2+2ab+b^2)-(a^2-2ab+b^2).$$

Now remove the brackets. Take care with the signs in the second bracket:

$$= a^2+2ab+b^2-a^2+2ab-b^2 = 4ab = \text{RHS}. \quad \blacksquare$$

Check at $a=3$, $b=2$: the left side is $25-1=24$ and the right side is $4(3)(2)=24$.

EXAMPLE 3.2

Show that $\frac{1}{4}+\frac{1}{12}=\frac{1}{3}$, and prove the algebraic generalisation

$$\frac{1}{m+1}+\frac{1}{m^2+m} \equiv \frac{1}{m}.$$

SOLUTION

The numerical case is direct: $\frac{1}{4}+\frac{1}{12}=\frac{3}{12}+\frac{1}{12}=\frac{4}{12}=\frac{1}{3}$. Notice it is the claimed identity at $m=3$: $m+1=4$ and $m^2+m=12$.

Both fractions need $m \neq 0$ and $m \neq -1$, so the identity is claimed for those values only; checking where the expressions are defined is part of the argument. For the general statement, start from the left side and factorise the second denominator, $m^2+m=m(m+1)$:

$$\frac{1}{m+1}+\frac{1}{m(m+1)}=\frac{m}{m(m+1)}+\frac{1}{m(m+1)}=\frac{m+1}{m(m+1)}=\frac{1}{m}. \quad \blacksquare$$

One calculation confirmed a single case. The algebra covers every $m \neq 0, -1$ at once. Examination questions often use this "verify, then generalise" structure.

3.1.3 Proving a general statement

Many proofs are not about identities. They are about claims such as "the sum of two odd numbers is even". For these, the first step is to write the general object in algebra, so that one expression stands for every case at once.

The table below lists the standard forms. In every row, k and n are integers.

In words	In algebra
an even number	$2k$
an odd number	$2k+1$, or $2k-1$
two consecutive integers	n and $n+1$
three consecutive integers	$n-1$, n, $n+1$
two consecutive even numbers	$2k$ and $2k+2$
two consecutive odd numbers	$2k+1$ and $2k+3$
a multiple of 3	$3k$
a number that leaves remainder 1 when divided by 3	$3k+1$
a square number	k^2
a rational number	p/q, with p, q integers and $q \neq 0$

Choosing the right form matters. To prove a statement about *any* two odd numbers, use $2a+1$ and $2b+1$ with two different letters. Writing $2a+1$ twice would **only prove the statement for two *equal* odd numbers**.

When no single form works, split into cases that cover every integer, such as n even or odd, or $n = 3k$, $3k+1$, $3k+2$, and prove the claim in each case. Every integer must fall in exactly one case. This is called **proof by cases**.

A **direct proof** starts from what is given and reaches the claim through algebra. Most direct proofs follow four steps:

1. **State** the assumptions in words.
2. **Write** them in algebra, using the forms in the table.
3. **Simplify** until the required form appears.
4. **Explain** in words why the result proves the claim.

EXAMPLE 3.3

Prove that the sum of any two odd numbers is even.

SOLUTION

Let the two odd numbers be $2a+1$ and $2b+1$, where a and b are integers. Their sum is

$$\begin{aligned}(2a+1)+(2b+1) &= 2a+2b+2 && \text{collect the terms}\\ &= 2(a+b+1) && \text{take out the factor } 2.\end{aligned}$$

Since $a+b+1$ is an integer, the sum is $2 \times (\text{integer})$, which is by definition even. ■

EXAMPLE 3.4

Prove that the product of two consecutive integers is always even.

SOLUTION

Take the consecutive integers n and $n+1$. One of any two consecutive integers is even. If n is even, the product $n(n+1)$ has an even factor. If n is odd, then $n+1$ is even, and the product has an even factor again. Either way $n(n+1)$ is a multiple of 2, so it is even. ■

To prove divisibility by a **composite** number (a whole number greater than 1 that is not prime), write it as a product of **coprime** factors (factors sharing no factor larger than 1), such as $12 = 4 \times 3$, and prove divisibility by each factor. The factors must be coprime: a number divisible by 2 and by 4 need not be divisible by 8, as 12 shows. The general result for coprime factors is not proved in this course, but a particular case can be checked directly, as the next example shows for 2 and 3.

EXAMPLE 3.5

Prove that $n(n+1)(2n+1)$ is divisible by 6 for every integer n.

SOLUTION

Since $6 = 2 \times 3$, find a factor 2 and a factor 3 separately.

A factor of 2. One of any two consecutive integers is even, so one of n and $n+1$ is even, and the product is divisible by 2.

A factor of 3. Every integer leaves remainder 0, 1 or 2 on division by 3, so n has one of three forms, where k is an integer:

$$\begin{aligned} n = 3k: &\quad n \text{ itself is a multiple of } 3; \\ n = 3k+1: &\quad 2n+1 = 6k+3 = 3(2k+1); \\ n = 3k+2: &\quad n+1 = 3k+3 = 3(k+1). \end{aligned}$$

The three cases cover every integer, and in each one of the three factors is a multiple of 3, so the product is divisible by 3.

The product is divisible by 2 and by 3. To combine the two facts, write the product as $3m$, where m is an integer. If m were odd, $3m$ would be odd $\times$ odd, which is odd. But the product is even, so m is even, say $m = 2j$. Then the product is $3(2j) = 6j$, a multiple of 6. ■

CAUTION One example cannot prove a statement about infinitely many cases, such as one that begins "for all integers n". It can only *disprove* one, which is the subject of the next section.

YOUR TURN 3.1 Deductive Proof

Equation or identity

1. State whether each of the following is an equation or an identity.

(a) $3x = 12$

(b) $(x+2)^2 = x^2 + 4x + 4$

Proving an identity

2. Prove each identity. Start from one side and label LHS and RHS in your working.

(a) $(a+b)^2 \equiv a^2 + 2ab + b^2$

(b) $(a-b)^2 \equiv a^2 - 2ab + b^2$

(c) $\dfrac{1}{x} - \dfrac{1}{x+1} \equiv \dfrac{1}{x(x+1)}$, for $x \neq 0, -1$

(d) $(x+3)(x-3) \equiv x^2 - 9$

(e) $\dfrac{1}{x-1} - \dfrac{1}{x+1} \equiv \dfrac{2}{x^2-1}$, for $x \neq \pm 1$

3. Prove that $(x-3)^2 + 5 \equiv x^2 - 6x + 14$. Check your result at $x = 1$.

Verify, then generalise

4. This question checks one case, then proves the general result.

(a) Verify that $3^2 + 4^2 + 12^2 = 13^2$.

(b) Prove that $n^2 + (n+1)^2 + (n(n+1))^2 \equiv (n^2+n+1)^2$, and state the value of n that gives part (a).

5. Two examples of a pattern are $7 \times 9 = 8^2 - 1$ and $11 \times 13 = 12^2 - 1$.

(a) Verify both examples.

(b) Prove that the product of two consecutive odd numbers is always one less than the square of the even number between them.

Odd, even and divisibility

6. Prove each statement about odd and even integers.

(a) The sum of any two even integers is even.

(b) The sum of an even integer and an odd integer is odd.

(c) The product of any two odd integers is odd.

7. Prove each statement for every integer n.

(a) $(2n+1)^2$ is odd.

(b) $n^2 + 3n$ is even.

(c) $(2n+1)^2 - 1$ is divisible by 4.

(d) $n^3 - n$ is divisible by 6.

Proof by cases

8. Prove that $n^2 + n + 1$ is odd for every integer n, by considering the cases n even and n odd.

9. Prove that, for every integer n, the remainder when n^2 is divided by 3 is either 0 or 1. Consider the three cases $n = 3k$, $n = 3k + 1$ and $n = 3k + 2$, where k is an integer.

Concept check

10. A student sets out to prove that the sum of any two odd integers is even, and writes the two odd integers as $2n + 1$ and $2n + 3$, where n is an integer. Explain why this does not prove the claim, and give a correct proof.

3.2 Disproof by Counterexample HL

A universal statement claims something about every member of a collection. To show that such a claim is false, you do not need to discuss the whole collection. You need one member for which the claim fails.

DEFINITION 3.2 **Counterexample**

A **counterexample** is one specific case for which a general statement fails. A single counterexample is enough to prove that the statement is false.

This is what happened with the circle problem. The claim "the number of regions doubles each time" was a universal statement, and $n = 6$ was a counterexample to it.

EXAMPLE 3.6

The expression $n^2 + n + 41$ gives a prime number for $n = 0, 1, 2, \ldots, 39$, forty primes in a row. Show that the statement "$n^2 + n + 41$ is prime for every non-negative integer n" is false.

SOLUTION

Look for a value of n that makes every term a multiple of 41. At $n = 40$, $n^2 + n = 40 \times 41$, so

$$40^2 + 40 + 41 = 1600 + 40 + 41 = 1681 = 41^2.$$

This is 41×41, not prime. So $n = 40$ is a counterexample, and the statement "$n^2 + n + 41$ is always prime" is false. ■

Forty cases agreed with the claim, and one case was enough to make it false. Examples can make a claim look true, but for a claim about infinitely many cases they cannot make it certain. A claim about a *finite* set is different: checking every member is a proof, called **proof by exhaustion**. What does not work is checking some cases and assuming the rest.

EXAMPLE 3.7

Show that this statement is false: "there are no positive integer solutions to the equation $x^2 + y^2 = 10$."

SOLUTION

Take $x = 1$ and $y = 3$. Both are positive integers, and

$$1^2 + 3^2 = 1 + 9 = 10.$$

So a positive integer solution does exist, and the statement is false. ■

TIP A counterexample must be *explained*, not just named. State the case, substitute it into the claim, show the calculation, and say in words why this makes the claim false. The IB is explicit that stating the counterexample alone is not enough.

Two more claims are disproved by counterexamples. The first is "if $a^2 > b^2$ then $a > b$". Take $a = -3$ and $b = 1$. Then $a^2 = 9 > 1 = b^2$, but $a = -3 < 1 = b$, so the claim fails: squaring removes the sign. The second is "the product of two irrational numbers is irrational". Take $a = b = \sqrt{2}$, which is irrational proved in §3.3. Then $ab = 2$, which is rational, so the claim fails.

RW In 1640 Fermat studied the numbers $F_n = 2^{2^n} + 1$ and found that $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ and $F_4 = 65\,537$ are all prime. He conjectured that every F_n is prime. Almost a century later, in 1732, Euler tested the next one:

$$F_5 = 2^{32} + 1 = 4\,294\,967\,297 = 641 \times 6\,700\,417.$$

One counterexample was enough to disprove the conjecture. No larger Fermat prime has ever been found.

YOUR TURN 3.2 Disproof by Counterexample HL

Counterexamples with integers

11. Disprove each claim by giving a counterexample. Show the substitution, and say why it makes the claim false.

(a) $n^2 + n + 1$ is prime for every positive integer n.

(b) Every prime number is odd.
(c) If n is divisible by 4 then n is divisible by 8.
(d) The sum of two prime numbers is always even.
(e) $2^n + 1$ is prime for every positive integer n.
(f) If $a > b$ then $a^2 > b^2$.

Counterexamples with algebra

12. Disprove each claim by giving a counterexample. Show the substitution, and say why it makes the claim false.

(a) $n^2 \geq 2n$ for all integers n.
(b) $x^2 > x$ for all real x.
(c) If n^2 is even then n is odd.
(d) $\sqrt{a+b} = \sqrt{a} + \sqrt{b}$ for all $a, b \geq 0$.
(e) If p is prime then $2^p - 1$ is prime.

13. Disprove each claim by giving a counterexample.

(a) If ab is rational, then a and b are both rational.
(b) $\sqrt{x^2} = x$ for every real number x.

Showing that a statement is not always true

14. Show that each statement is not always true.

(a) There is no integer n for which $n^2 + 1$ is divisible by 5.
(b) There are no positive integers x and y with $x^2 - y^2 = 15$.

Concept check

15. A student checks $n^2 - n + 41$ for $n = 1, 2, \ldots, 10$, finds a prime every time, and concludes that $n^2 - n + 41$ is prime for every positive integer n.

(a) Explain why the checks do not prove the claim.
(b) By taking $n = 41$, show that the claim is false.
(c) Prove by exhaustion that every even number from 4 to 30 is the sum of two primes. Explain why checking cases is a proof here, although it was not in part (a).

3.3 Proof by Contradiction HL

Suppose a friend tells you they have written down the largest whole number that exists. You do not need to see it to know they are wrong. Whatever the number is, add 1 to it. The result is a whole number, and it is larger. So the claim is false.

You have just proved something without ever finding the answer. You did not search for the largest whole number. You assumed it existed and showed that the assumption leads to an impossible situation.

This is the idea of **proof by contradiction**. Assume the statement you want to prove is *false*. Reason correctly from that assumption until you reach something impossible. Correct reasoning cannot turn a true assumption into an impossible result, so the assumption must have been false. The original statement is therefore true.

DEFINITION 3.3 **Proof by contradiction**

In **proof by contradiction**, you assume the **negation** (the opposite) of what you want to prove, then derive a logical contradiction. The contradiction shows that the assumption is false, so the original claim is true.

The method has a Latin name, *reductio ad absurdum*, meaning "reduction to the absurd". The method is useful because the assumption itself is a starting point. Checking fractions one by one could never prove that no fraction equals $\sqrt{2}$, because there are infinitely many of them. Assuming that such a fraction exists produces an equation instead, and an equation can be worked on. To prove a number irrational, assume it equals $\frac{p}{q}$, where p and q are integers with $q \neq 0$ that share no common factor other than 1. The contradiction usually comes from showing that they do share one. Two classic results, each more than two thousand years old, show the method at work: $\sqrt{2}$ is irrational, and there are infinitely many primes.

The first step is always to write down the negation of the claim, which is what you assume. Four patterns cover most cases.

Claim	Its opposite: what you assume
every x has property P	some x does not have P
there is an x with property P	no x has P
x is irrational	x is rational
if A, then B	A is true **and** B is false

A proof by contradiction is written in four stages:

1. **Assumption.** State the negation of the claim.
2. **Consequences.** Reason correctly from the assumption.
3. **Contradiction.** Reach a statement that cannot be true, and say what it contradicts.
4. **Conclusion.** Say that the assumption is false, so the claim is true.

The proof for $\sqrt{2}$ uses a smaller result, proved first: if p^2 is even, then p is even. A small result proved on the way to a larger one is called a **lemma**. If p were odd, say $p = 2k + 1$,

then $p^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ would be odd. So when p^2 is even, p cannot be odd.

EXAMPLE 3.8

Prove that $\sqrt{2}$ is irrational.

SOLUTION

Aristotle mentions this result in the 4th century BCE.

Assumption. Suppose $\sqrt{2}$ *is* rational, so that

$$\sqrt{2} = \frac{p}{q},$$

where p and q are integers, $q \neq 0$, with **no common factor other than** 1. Any fraction can be cancelled until this is true, so the assumption is allowed. The contradiction at the end depends on this condition, so state it explicitly.

Consequences. Squaring both sides gives $2 = \frac{p^2}{q^2}$, hence $p^2 = 2q^2$. So p^2 is even, and by the lemma p is even. Write $p = 2m$, where m is an integer. Then $p^2 = 4m^2$, and substituting,

$$4m^2 = 2q^2 \implies q^2 = 2m^2,$$

so q^2 is even, and by the same lemma q is even.

Contradiction. Now p and q are both even, so they share the factor 2. That contradicts the choice of a fully cancelled fraction.

Conclusion. The assumption is impossible, so $\sqrt{2}$ is irrational. ■

The next proof also rests on a lemma. **Lemma: every integer greater than 1 has at least one prime factor.** Take the integer's smallest factor greater than 1; call it d. If d were not prime, it would have a factor between 1 and d, and that factor would also divide the integer, so d would not be the smallest. Hence d is prime. For example, the smallest factor of 91 greater than 1 is 7, which is prime.

EXAMPLE 3.9

Prove that there are infinitely many prime numbers.

SOLUTION

This result is from Euclid's *Elements* (c. 300 BCE).

Assumption. Suppose there are only finitely many primes. Then you can list every one of them:

$$p_1,\ p_2,\ \cdots,\ p_n.$$

Consequences. Multiply all the primes on the list together and add 1:

$$N = p_1 \times p_2 \times \cdots \times p_n + 1.$$

- N is greater than 1, because the product is at least 2, so by the lemma N has a prime factor; call it p.
- Take any prime p_i on the list. It divides the product $p_1 \times p_2 \times \cdots \times p_n$ exactly, so dividing N by p_i leaves remainder 1. Hence no prime on the list divides N.
- So p, which does divide N, is not on the list.

Contradiction. p is a prime that is missing from the list, yet the list was assumed to contain every prime.

Conclusion. The assumption is impossible: no finite list can hold all the primes, so there are infinitely many. ■

Notice what the proof does not do: it does not say which prime is missing, only that the list was incomplete. N itself need not be prime, but every prime factor of N is absent from the list. With $2, 3, 5, 7, 11, 13$ the number $N = 30031 = 59 \times 509$, and both factors are primes missing from the list. The table shows the first six cases.

primes on the list	N	prime?
2	3	yes
$2, 3$	7	yes
$2, 3, 5$	31	yes
$2, \ldots, 7$	211	yes
$2, \ldots, 11$	2311	yes
$2, \ldots, 13$	$30031 = 59 \times 509$	**no**

The $\sqrt{2}$ proof used one fact about even numbers: if p^2 is even, then p is even. To prove that $\sqrt{5}$ is irrational in the same way, you need the matching fact about multiples of 5. The next example proves that fact directly, by checking every case; it is not itself a proof by contradiction.

EXAMPLE 3.10

Prove that if n^2 is a multiple of 5, then n is a multiple of 5.

SOLUTION

Every integer lies within 2 of a multiple of 5, so for some integer k, n has one of five forms. Square each one:

n	n^2	remainder on division by 5
$5k$	$5(5k^2)$	0
$5k+1$	$5(5k^2+2k)+1$	1
$5k-1$	$5(5k^2-2k)+1$	1
$5k+2$	$5(5k^2+4k)+4$	4
$5k-2$	$5(5k^2-4k)+4$	4

Only the first is a multiple of 5; the others leave remainder 1 or 4. So n^2 can be a multiple of 5 only when n has the form $5k$, which is to say only when n is a multiple of 5. ■

With this lemma in place of the fact about even numbers, the proof for $\sqrt{5}$ follows the same stages. Assume $\sqrt{5} = \frac{p}{q}$ in lowest terms. Deduce that 5 divides p, then that 5 divides q. This contradicts the lowest terms.

Many statements have the form "if A then B". Such a statement is an **implication**, written $A \Rightarrow B$ and read "A implies B". The statement A is the **premise** and B is the **conclusion**. The table gives the truth of the implication in each of the four cases.

premise A	conclusion B	$A \Rightarrow B$
true	true	true
true	false	**false**
false	true	true
false	false	true

Think of a promise: "If you score a 7, I will buy you a pizza." The promise is broken in one case only: you score a 7 and no pizza arrives. If you do not score a 7, the promise is kept whether or not there is pizza.

So the statement "if A then B" is false in one case only: A is true and B is false. To prove it by contradiction, assume *both* that A is true and that B is false, and show that the two cannot hold together. Do not assume that A is false: the statement makes no claim about that case, so no contradiction can come from it.

EXAMPLE 3.11

Prove by contradiction that, for an integer n, if $3n+2$ is odd then n is odd.

SOLUTION

Assume the opposite: that $3n+2$ is odd *and* n is even. Then $n = 2k$ for some integer k, and

$$3n + 2 = 6k + 2 = 2(3k + 1).$$

Since $3k+1$ is an integer, $3n+2$ is even. That contradicts the assumption that $3n+2$ is odd. So the assumption fails, and if $3n+2$ is odd then n is odd. ■

The method used for $\sqrt{2}$ also works for a cube root. Suppose $\sqrt[3]{2} = \frac{p}{q}$ in lowest terms. Cubing gives $p^3 = 2q^3$, so p^3 is even. The cube of an odd number is odd, $(2k+1)^3 = 2(4k^3 + 6k^2 + 3k) + 1$, so p is even. Write $p = 2m$. Then $8m^3 = 2q^3$, so $q^3 = 4m^3 = 2(2m^3)$ is even, and q is even too. Both are even, which contradicts the lowest terms. The same steps prove that $\sqrt{3}$ and $\sqrt[3]{5}$ are irrational; each needs its own lemma.

Adding, subtracting or multiplying two rational numbers, or dividing one by a non-zero rational, always gives a rational number: the result of these operations is always rational. This property is called **closure**. For a sum, $\frac{p}{q} + \frac{r}{s} = \frac{ps+qr}{qs}$, which is a ratio of two integers with $qs \neq 0$, and the other three operations are checked in the same way. So to show that an expression built from a known irrational is irrational, assume it is rational and use only these operations to make the known irrational the subject. The known irrational is then rational, a contradiction. This works only if you never divide by zero: $0 \times \sqrt{2} = 0$ is rational, so a claim such as "$a\sqrt{2}$ is irrational for rational a" needs $a \neq 0$.

EXAMPLE 3.12

Prove that the sum of a rational number and an irrational number is irrational.

SOLUTION

Let a be rational and b be irrational, and assume the opposite: that $a+b$ is rational. Call it c. Then

$$b = c - a,$$

the difference of two rational numbers, which is rational by closure. That contradicts the fact that b is irrational. So $a+b$ is irrational. ■

EXAMPLE 3.13

Prove that $(1+\sqrt{2})^2$ is irrational. You may use the theorem $(\text{a statement that has been proved})$ that $\sqrt{2}$ is irrational.

SOLUTION

Expand first, so that the known irrational stands alone in a single term:

$$(1+\sqrt{2})^2 = 1 + 2\sqrt{2} + 2 = 3 + 2\sqrt{2}.$$

Assume the opposite: that this number is rational. Then

$$3 + 2\sqrt{2} = \frac{p}{q},$$

where p and q are integers with $q \neq 0$. Isolate $\sqrt{2}$ by subtracting 3 and halving:

$$\sqrt{2} = \frac{1}{2}\left(\frac{p}{q} - 3\right) = \frac{p - 3q}{2q}.$$

Now $p - 3q$ and $2q$ are integers and $2q \neq 0$, so the right-hand side is a ratio of two integers, and $\sqrt{2}$ is rational. That contradicts the theorem that $\sqrt{2}$ is irrational, so the assumption fails and $(1 + \sqrt{2})^2$ is irrational. ■

Here the contradiction is with a result proved earlier, that $\sqrt{2}$ is irrational, not with an assumption made inside this proof. Expanding first wrote the number as $3 + 2\sqrt{2}$, with $\sqrt{2}$ in a single term, and that is what allowed $\sqrt{2}$ to be made the subject.

CAUTION State your assumption clearly at the start ("assume …is rational") and name the contradiction when you reach it. A proof by contradiction with no clearly identified contradiction proves nothing.

YOUR TURN 3.3 Proof by Contradiction HL

No largest or smallest

16. Prove each statement by contradiction.

(a) There is no smallest positive rational number.

(b) There is no smallest positive real number.

Statements about integers

17. Let n be an integer. Prove each statement by contradiction.

(a) If n^2 is odd then n is odd.

(b) If n^2 is even then n is even.

18. Prove each statement by contradiction.

(a) There are no integers x and y with $2x + 4y = 5$.

(b) There are no integers x and y with $6x + 9y = 10$.

Irrational numbers

19. Prove each statement by contradiction.

(a) If x^2 is irrational, then x is irrational.

(b) $\sqrt{3}$ is irrational.

(c) If x is irrational and $x \neq 0$, then $\dfrac{1}{x}$ is irrational.

20. Prove each statement by contradiction. You may use the facts that $\sqrt{2}$ and $\sqrt{3}$ are irrational.

(a) $5 - \sqrt{2}$ is irrational.

(b) $(2 + \sqrt{3})^2$ is irrational.

Infinitely many primes

21. Suppose there were only finitely many primes, $p_1, p_2, \ldots, p_n$. Let $N = p_1 p_2 \cdots p_n - 1$. By considering the remainder when N is divided by each p_i, prove by contradiction that there are infinitely many primes.

Concept check

22. To prove "*if n^2 is even then n is even*" by contradiction, a student begins: "*Assume that n^2 is odd.*" Explain the error, and state the correct assumption.

3.4 Proof by Induction HL

Picture an endless line of dominoes. You cannot knock over infinitely many by hand. But suppose you can show two things: that the first domino falls, and that *whenever* a domino falls it topples the next. Then every domino in the line must fall, however long the line.

Many statements depend on a whole number n. For example,

$$1 + 2 + 3 + \cdots + n = \tfrac{1}{2}n(n+1)$$

is a different statement for each value of n. Label it P_n. Then $P_1, P_2, P_3, \ldots$ is an infinite list of statements, one for each n, and you can write down P_n for any n. For instance, P_3 says $1 + 2 + 3 = \frac{1}{2}(3)(4)$, which is true. The subscript is a label for the nth statement in the list, not a function being evaluated. Checking the statements one at a time can never cover every n.

Mathematical induction covers them all, using the domino idea. You show that the first statement is true, then show that whenever one statement is true, the next one is true too.

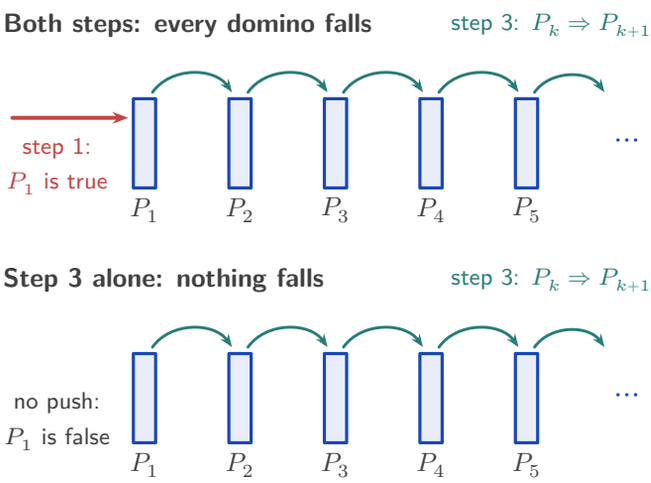


Figure 3.2 Induction needs both steps: the first domino must fall, and each must knock over the next.

KEY 3.1 **Principle of mathematical induction**

Start by labelling the statement to be proved as P_n. Then, to prove that P_n holds for all integers $n \geq 1$:

1. Show that P_1 is true (the *base case*).
2. Assume that P_k is true for **some** $k \geq 1$ (the *inductive hypothesis*).
3. Show that P_{k+1} is true, using the assumption P_k. Write down P_{k+1} first, so that you know the target. This proves $P_k \Rightarrow P_{k+1}$ (read "P_k implies P_{k+1}") (the *inductive step*).
4. Conclude: *since P_1 is true, and P_k true implies P_{k+1} true, by the principle of mathematical induction P_n is true for all integers $n \geq 1$.*

(If the statement starts later, at $n = n_0$, prove P_{n_0} in step 1, assume P_k for some $k \geq n_0$ in step 2, and conclude for all integers $n \geq n_0$.)

An induction proof in this course follows these four steps, and the sentence in step 4 should be written out in full. It is not decoration. It is the step that turns the two facts you proved into a conclusion about every n, and markschemes usually award a mark for it.

In step 2, k is an **arbitrary** (any one value, not chosen in advance) but fixed integer in the stated range: apart from P_k itself, nothing is assumed about it except $k \geq 1$.

In the proofs below, the words in blue are the standard wording of an induction proof; the algebra between them changes from question to question. Here is a complete proof.

EXAMPLE 3.14

Prove that $1 + 3 + 5 + \cdots + (2n - 1) = n^2$ for all integers $n \geq 1$.

SOLUTION

Let P_n be the statement $1 + 3 + 5 + \cdots + (2n - 1) = n^2$.

Step 1 (P_1): the left side is 1; the right side is $1^2 = 1$. They agree, so P_1 is true.

Step 2: assume P_k is true for some $k \geq 1$, that is,

$$1 + 3 + 5 + \cdots + (2k-1) = k^2.$$

Step 3: we now show that P_{k+1} is true, that is, with n replaced by $k+1$ (its last term is $2(k+1)-1 = 2k+1$):

$$P_{k+1}: \quad 1 + 3 + 5 + \cdots + (2k-1) + (2k+1) = (k+1)^2.$$

Start from the left-hand side. Its first k terms are the left-hand side of P_k, so the assumption replaces them by k^2:

$$\begin{aligned} \text{LHS} &= \big[1 + 3 + 5 + \cdots + (2k-1)\big] + (2k+1) \\ &= k^2 + (2k+1) && \text{by the assumption} \\ &= (k+1)^2 = \text{RHS}. \end{aligned}$$

The left-hand side has become the right-hand side, so P_{k+1} is true. So if P_k is true, then P_{k+1} is true.

Step 4: since P_1 is true, and P_k true implies P_{k+1} true, by the principle of mathematical induction P_n is true for all integers $n \geq 1$. ■

3.4.1 Why induction works

- Step 3 asks an "if … then" question, not an "is" question, and it is often misread. **It does not claim that the k-th domino has fallen**. It proves only that *if* domino k falls, domino $k+1$ falls with it. That is why step 2 may assume P_k: you are not claiming that P_k is true, only working out what would follow if it were.

  Recall from §3.3 that an implication $A \Rightarrow B$ is false only when the premise is true and the conclusion is false.

  In step 3 the premise is P_k and the conclusion is P_{k+1}. So step 3 rules out one situation only: P_k true while P_{k+1} is false. It says nothing about whether P_k itself is true. That job belongs to step 1, which is why step 1 can never be skipped.

  Without step 1, the inductive step can hold for a statement that is false for every n. Let P_n be "$n(n+1)$ is odd".

  - *Step 3 works.* Suppose P_k is true, so $k(k+1)$ is odd. Then

    $$(k+1)(k+2) = \underbrace{k(k+1)}_{\text{assumed odd}} + \underbrace{2(k+1)}_{\text{always even}} = \text{odd} + \text{even} = \text{odd}.$$

    Hence P_{k+1} is true whenever P_k is true: the implication $P_k \Rightarrow P_{k+1}$ holds.
  - *Step 1 fails.* P_1 says that $1 \times 2 = 2$ is odd, which is false.

- *Every P_n is false.* $n(n+1)$ is a product of two consecutive integers, one of which is even, so it is always even.

The implication in step 3 is true only because its premise is never true. Every case is the last row of the truth table in §3.3: premise false, conclusion false, implication true. Every domino would knock over the next, but none is ever pushed.

With both steps in place, the domino picture becomes precise. Pick any n, say $n = 1000$. Step 1 shows that P_1 is true. Step 3 with $k = 1$ then shows that P_2 is true, step 3 with $k = 2$ shows that P_3 is true, and after 999 uses of step 3, P_{1000} is true. The same finite chain reaches any n, so no value of n is left out, even though only two things were proved.

The same fact can be seen by contradiction, which connects induction to §3.3. Suppose both steps are done, but P_n is false for some values of n. Any collection of positive integers that is not empty has a smallest member, so there is a smallest failure, say P_m. Now $m \neq 1$, because step 1 showed that P_1 is true. So $m - 1 \geq 1$, and P_{m-1} is true, because m is the smallest failure. Step 3 with $k = m - 1$ then shows that P_m is true. This contradicts the failure of P_m, so there are no failures: P_n is true for every $n \geq 1$.

CAUTION In step 2, assume P_k for **some** k, never for *all* k. Assuming it for all k assumes the very thing you are proving, and examiners do not award the reasoning marks for it. The hypothesis is one domino falling, not the whole line.

Induction is not only for sums. It also proves divisibility statements, inequalities, formulas for recurrences and formulas for nth derivatives below, and De Moivre's theorem in Ch. 17. When a claim is about every integer $n \geq n_0$ and each case builds on the one before, induction is a natural method to try.

3.4.2 Induction for a sum

The proof of $1 + 3 + 5 + \cdots + (2n - 1) = n^2$ above is of this kind. Here P_n says that a sum equals a formula. Write down P_{k+1} first, so you know the target. Start from its left-hand side. Its first k terms are the left-hand side of P_k, so the assumption replaces them by the right-hand side of P_k. Then simplify until you reach the right-hand side of P_{k+1}: the original formula with $k + 1$ written wherever n appeared.

The sum is often given in sigma notation instead, for example

$$\sum_{r=1}^{n} (2r - 1) = n^2.$$

If the terms are not obvious, expand the sigma: substitute $r = 1, 2, 3$ and $r = n$ to write the sum out as $1 + 3 + 5 + \cdots + (2n - 1)$. The next term, needed in step 3, is the $r = k + 1$ term, $2(k + 1) - 1$.

3.4.3 Induction for divisibility

Here P_n says that an expression E_n is divisible by a fixed number d. Turn the assumption into an equation: divisible by d means $E_k = dm$ for some integer m. Then rewrite E_{k+1} so that E_k appears inside it, replace that part by dm, and take d outside as a common factor. The aim is to reach the form $d \times (\text{integer})$.

EXAMPLE 3.15

Prove that $8^n - 1$ is divisible by 7 for all integers $n \geq 1$.

SOLUTION

Let P_n be the statement "$8^n - 1$ is divisible by 7."
Step 1 (P_1): $8^1 - 1 = 7$, which is divisible by 7, so P_1 is true.
Step 2: assume P_k is true for some $k \geq 1$, so $8^k - 1 = 7m$ for some integer m.
Step 3: we now show that P_{k+1} is true, that is, P_{k+1}: $8^{k+1} - 1 = 7 \times (\text{an integer})$.
Start from the expression $8^{k+1} - 1$ and use the assumption:

$$\begin{aligned} 8^{k+1} - 1 &= 8 \cdot 8^k - 1 = 8(8^k - 1) + 8 - 1 \\ &= 8(7m) + 7 && \text{by the assumption, } 8^k - 1 = 7m \\ &= 7(8m + 1). \end{aligned}$$

Since $8m + 1$ is an integer, $8^{k+1} - 1$ is divisible by 7, which is P_{k+1}. So if P_k is true, then P_{k+1} is true.
Step 4: since P_1 is true, and P_k true implies P_{k+1} true, by the principle of mathematical induction P_n is true for all integers $n \geq 1$. ■

Notice where the assumption was used: replacing $8^k - 1$ by $7m$ is what makes both terms of the last line multiples of 7.

Sometimes E_k does not appear after taking out a factor. Then expand E_{k+1} fully and look for E_k inside the expansion. If what is left after removing E_k is not a multiple of d, check the expansion and the grouping before you doubt the statement.

EXAMPLE 3.16

Prove that $n^5 + 4n$ is divisible by 5 for all integers $n \geq 1$.

SOLUTION

Let P_n be the statement "$n^5 + 4n$ is divisible by 5."
Step 1 (P_1): $1^5 + 4(1) = 5$, which is divisible by 5, so P_1 is true.
Step 2: assume P_k is true for some $k \geq 1$, so $k^5 + 4k = 5m$ for some integer m.
Step 3: we now show that P_{k+1} is true, that is, P_{k+1}:
$(k+1)^5 + 4(k+1) = 5 \times (\text{an integer})$. Start from the expression $(k+1)^5 + 4(k+1)$

and use the assumption:

$$\begin{aligned}(k+1)^5+4(k+1) &= k^5+5k^4+10k^3+10k^2+5k+1+4k+4 && \text{expand §2.9}\\ &= (k^5+4k)+5k^4+10k^3+10k^2+5k+5 && \text{collect } k^5+4k\\ &= 5m+5k^4+10k^3+10k^2+5k+5 && \text{by the assumption}\\ &= 5(m+k^4+2k^3+2k^2+k+1) && \text{take out } 5.\end{aligned}$$

Since $m+k^4+2k^3+2k^2+k+1$ is an integer, $(k+1)^5+4(k+1)$ is divisible by 5, which is P_{k+1}. So if P_k is true, then P_{k+1} is true.

Step 4: since P_1 is true, and P_k true implies P_{k+1} true, by the principle of mathematical induction P_n is true for all integers $n \geq 1$. ■

3.4.4 Induction for an inequality

Here P_n says that $A_n > B_n$. Inequalities are proved by a 'chain' of inequalities, each one leading to the next: if $a > b$ and $b \geq c$, then $a > c$. Start from A_{k+1} and rewrite it so that A_k appears, then use the assumption to replace A_k by something smaller. That gives the first inequality. Now prove separately that this new quantity is at least B_{k+1}, which gives the second. Together they give $A_{k+1} > B_{k+1}$:

$$A_{k+1} \underbrace{>}_{\text{by } P_k} (\text{new quantity}) \underbrace{\geqslant}_{\text{separate check}} B_{k+1}.$$

EXAMPLE 3.17

Prove that $2^n > n^2$ for all integers $n \geq 5$.

SOLUTION

Let P_n be the statement $2^n > n^2$. The inequality is true for $n = 1$ but false for $n = 2$, 3 and 4, so the induction cannot start at $n = 1$. It starts at $n = 5$, the first value from which every later case is true.

Step 1 (P_5): $2^5 = 32$ and $5^2 = 25$, and $32 > 25$, so P_5 is true.

Step 2: assume P_k is true for some $k \geq 5$, that is, $2^k > k^2$.

Step 3: we now show that P_{k+1} is true, that is, P_{k+1}: $2^{k+1} > (k+1)^2$. Start from the left-hand side and use the assumption:

$$\text{LHS} = 2^{k+1} = 2 \cdot 2^k > 2k^2 \qquad \text{by the assumption.}$$

It is now enough to show $2k^2 \geq (k+1)^2$. Expanding, this asks whether $2k^2 \geq k^2+2k+1$, that is, $k^2-2k-1 \geq 0$. For $k \geq 5$ this holds, since $k^2-2k-1 = (k-1)^2-2 \geq 16-2 > 0$. Therefore

$$\text{LHS} = 2^{k+1} > 2k^2 \geq (k+1)^2 = \text{RHS},$$

so P_{k+1} is true. So if P_k is true, then P_{k+1} is true.

Step 4: since P_5 is true, and P_k true implies P_{k+1} true for $k \geq 5$, by the principle of mathematical induction $2^n > n^2$ for all integers $n \geq 5$. ■

3.4.5 Induction for a recurrence

Here the sequence is given by a rule that links each term to the one before, and no formula for u_n is given. Compute the first few terms, conjecture a closed form for u_n, and let P_n be that closed form. In the inductive step, substitute the assumed u_k into the rule for u_{k+1}. Then simplify until the closed form with $k+1$ in place of n appears.

EXAMPLE 3.18

A sequence is defined by $u_1 = 1$ and $u_{n+1} = \dfrac{u_n}{1+2u_n}$ for $n \geq 1$. Find a formula for u_n, and prove it by induction.

SOLUTION

First compute u_2, u_3 and u_4, each from the one before:

$$u_2 = \frac{1}{1+2} = \frac{1}{3}, \qquad u_3 = \frac{1/3}{1+2/3} = \frac{1/3}{5/3} = \frac{1}{5}, \qquad u_4 = \frac{1/5}{1+2/5} = \frac{1/5}{7/5} = \frac{1}{7}.$$

The terms so far are $1, \frac{1}{3}, \frac{1}{5}, \frac{1}{7}$, which suggests the conjecture $\boxed{u_n = \dfrac{1}{2n-1}}$

Let P_n be that statement.

Step 1 (P_1): the definition gives $u_1 = 1$, and the formula gives $\dfrac{1}{2(1)-1} = 1$. They agree, so P_1 is true.

Step 2: assume P_k is true for some $k \geq 1$, that is, $u_k = \dfrac{1}{2k-1}$.

Step 3: we now show that P_{k+1} is true, that is, P_{k+1}: $u_{k+1} = \dfrac{1}{2(k+1)-1}$. Start from the left-hand side, u_{k+1}: apply the recurrence, then substitute the assumption:

$$\begin{aligned} \text{LHS} = u_{k+1} &= \frac{u_k}{1+2u_k} = \frac{1/(2k-1)}{1+2/(2k-1)} && \text{by the assumption} \\ &= \frac{1}{(2k-1)+2} && \text{multiply top and bottom by } 2k-1 \\ &= \frac{1}{2k+1} = \frac{1}{2(k+1)-1} = \text{RHS}, \end{aligned}$$

so P_{k+1} is true. So if P_k is true, then P_{k+1} is true.

Step 4: since P_1 is true, and P_k true implies P_{k+1} true, by the principle of mathematical induction $u_n = \dfrac{1}{2n-1}$ for all integers $n \geq 1$. ■

Four terms are evidence for a formula, not a proof of it; the induction proves it for every n. Markschemes for a question of this kind give marks for the conjecture and for the proof separately, so give the terms, state the conjecture, and then prove it.

3.4.6 Induction for a derivative formula

Here P_n gives a formula for the nth derivative of a function. The step from k to $k+1$ is one more differentiation: start from the $(k+1)$th derivative, write it as the derivative of the kth derivative, and replace the kth derivative by the formula that P_k gives. The example uses the product rule, which is met in Ch. 13, §13.6, and the fact that e^x is its own derivative.

EXAMPLE 3.19

Prove that $\dfrac{d^n}{dx^n}(xe^x) = (x+n)e^x$ for all integers $n \geq 1$.

SOLUTION

Let P_n be the statement $\dfrac{d^n}{dx^n}(xe^x) = (x+n)e^x$.

Step 1 (P_1): by the product rule, $\dfrac{d}{dx}(xe^x) = 1 \cdot e^x + xe^x = (x+1)e^x$, so P_1 is true.

Step 2: assume P_k is true for some $k \geq 1$, that is, $\dfrac{d^k}{dx^k}(xe^x) = (x+k)e^x$.

Step 3: we now show that P_{k+1} is true, that is, P_{k+1}: $\dfrac{d^{k+1}}{dx^{k+1}}(xe^x) = (x+k+1)e^x$.
Start from the left-hand side and use the assumption:

$$\begin{aligned} \text{LHS} = \frac{d}{dx}\left(\frac{d^k}{dx^k}(xe^x)\right) &= \frac{d}{dx}((x+k)e^x) && \text{by the assumption} \\ &= 1 \cdot e^x + (x+k)e^x && \text{product rule} \\ &= (x+k+1)e^x = \text{RHS}, \end{aligned}$$

so P_{k+1} is true. So if P_k is true, then P_{k+1} is true.

Step 4: since P_1 is true, and P_k true implies P_{k+1} true, by the principle of mathematical induction P_n is true for all integers $n \geq 1$. ■

CAUTION Two failures are common. One is forgetting the base case, so the dominoes can topple each other yet never start. The other is proving the inductive step *without using* the assumption. Show clearly where P_k is used. If you never used it, look for a gap in the step: either the step is incomplete, or the result did not need induction at all.

The four methods of this chapter do different jobs. Read the claim first, then use the table to choose a method.

	What you do	Use it when
Direct proof	start from what is given and derive the claim; for an identity, change one side into the other	the claim follows by algebra from a general form
Counterexample	give one case in which the claim fails	you want to *disprove* a claim about every case
Contradiction	assume the claim is false and derive an impossibility	the claim says something does not exist or is irrational, or a direct start is hard to find
Induction	prove a base case and the step from k to $k+1$	the claim is about every integer $n \geq n_0$

YOUR TURN 3.4 Proof by Induction HL

Sums

23. Prove each result by induction, for all $n \geq 1$.

(a) $1+2+3+\cdots+n=\dfrac{n(n+1)}{2}$

(b) $2+4+6+\cdots+2n=n(n+1)$

(c) $1^2+2^2+\cdots+n^2=\dfrac{n(n+1)(2n+1)}{6}$

(d) $1^3+2^3+\cdots+n^3=\dfrac{n^2(n+1)^2}{4}$

24. Prove each result by induction, for all $n \geq 1$.

(a) $1+4+7+\cdots+(3n-2)=\dfrac{n(3n-1)}{2}$

(b) $1+2+4+\cdots+2^{n-1}=2^n-1$

(c) $1\cdot 2+2\cdot 3+\cdots+n(n+1)=\dfrac{n(n+1)(n+2)}{3}$

(d) $\dfrac{1}{1\cdot 2}+\dfrac{1}{2\cdot 3}+\cdots+\dfrac{1}{n(n+1)}=\dfrac{n}{n+1}$

Divisibility

25. Prove each divisibility result by induction, for all $n \geq 1$.

(a) $3^n - 1$ is divisible by 2.
(b) $7^n - 3^n$ is divisible by 4.
(c) $n^3 + 2n$ is divisible by 3.
(d) $2n^3 + 3n^2 + n$ is divisible by 6.

Inequalities

26.

(a) Prove by induction that $2^n \geq n + 1$ for all $n \geq 0$.
(b) Explain why the base case here is $n = 0$ rather than $n = 1$.

27. Prove each inequality by induction. Check that the base case is the first value from which the inequality holds for all larger n.

(a) $n! > 2^n$ for all integers $n \geq 4$
(b) $3^n > n^3$ for all integers $n \geq 4$

Recurrences and derivative formulas

28. A sequence is defined by $u_1 = 2$ and $u_{n+1} = 2u_n - 1$ for $n \geq 1$.

(a) Find u_2, u_3 and u_4, and conjecture a formula for u_n.
(b) Prove your conjecture by induction.

29.

(a) A sequence is defined by $u_1 = 1$ and $u_{n+1} = 2u_n + n$ for $n \geq 1$. Prove by induction that $u_n = 3 \cdot 2^{n-1} - n - 1$ for all $n \geq 1$.
(b) You may assume that $\frac{d}{dx}(e^x) = e^x$ and the product rule. Prove by induction that $\frac{d^n}{dx^n}((2x+1)e^x) = (2x + 2n + 1)e^x$ for all $n \geq 1$.

Concept check

30. A student claims that $n^2 + n + 1$ is even for every integer $n \geq 1$. The student shows that, if $k^2 + k + 1$ is even, then $(k+1)^2 + (k+1) + 1$ is even.

(a) Show that the student's inductive step is correct.
(b) Explain why the claim is nonetheless false, and state which part of an induction proof the student left out.

31. In an induction proof, a student writes: "*Assume that the result is true for all positive integers* n." Explain the error, and write the correct assumption.

Chapter 3 · Proofs

Reflections

TOK A proof reduces a claim to things already accepted. But the starting points of a proof are assumed rather than proved. They are called **axioms**. In the 1930s Kurt Gödel proved a result about systems of axioms. Take any consistent system (one that never proves a contradiction) whose axioms can be listed by a fixed procedure and which can describe arithmetic. Then the system contains true statements that it cannot prove. Mathematical certainty is real, then, but not absolute. It is certainty *relative* to a chosen foundation. Does that make mathematics discovered, or invented?

IM The Pythagoreans believed that any two lengths share a common unit, so that every ratio of lengths is a ratio of whole numbers. Their own theorem showed that the belief was false: the diagonal of a unit square has length $\sqrt{2}$, and no such ratio gives it. Nobody knows exactly how the discovery was made. The classical argument, which Aristotle mentions, is the one in §3.3, a proof by contradiction: assume $\sqrt{2} = p/q$ in lowest terms, and an impossibility follows. Legend credits the discovery to Hippasus, and later writers report that the other Pythagoreans reacted with anger. The result remained true, and Greek mathematics had to widen its idea of number.

RW Proof is not confined to pure mathematics. In software engineering, *formal verification* proves that a program meets its specification (the exact description of what it must do) exactly, under the stated assumptions. Whether the specification asks for the right thing is a separate question. No amount of testing can give that guarantee, so the method is used where failure would be very dangerous: aircraft control, medical devices, spacecraft. Cryptography uses proved properties of prime numbers. Its security also depends on problems, such as factorising very large numbers, that are believed to be hard but have never been proved hard.

EXT The four-colour theorem says that any map drawn on a plane can be coloured with four colours so that no two regions sharing a border have the same colour. Regions that meet at a single point do not count as sharing a border. In the 1970s it became one of the first major theorems whose proof needed a computer. The machine checked nearly two thousand cases, far more than a person could. That raised a new question. If a proof is too long for anyone to read, but every step has been checked by machine, is it still a proof? What is a proof *for*: certainty, or understanding?

TOK Can you prove you are not dreaming? Which of the four methods here would you try?

A gallery of conjectures

Every theorem in this chapter was once a guess that someone had to prove. Here are seven guesses about whole numbers. Each one can be stated, and tested, with the arithmetic you already know. Five are still OPEN: nobody has proved them or found a counterexample, although many strong mathematicians have tried. One was PROVED after more than 350 years. One was DISPROVED by a number far too large to find by hand. None is examinable. Most entries end with something to try.

Odd perfect numbers: OPEN. A number is perfect if it equals the sum of its proper divisors (its divisors smaller than itself): $6 = 1 + 2 + 3$ and $28 = 1 + 2 + 4 + 7 + 14$. Over two thousand years ago Euclid showed how to build even perfect numbers. Nobody has ever found an odd one, and nobody has proved that none exists. If one does exist, it is larger than 10^{1500}. *Try it:* show that 496 is perfect.

Goldbach conjecture: OPEN. Every even number greater than 2 is the sum of two primes: $28 = 5 + 23$, $100 = 3 + 97$. Christian Goldbach suggested it to Euler in a letter in the 1700s. Larger even numbers tend to have more such pairs, but a trend is not a proof. Every even number up to 4×10^{18} has been checked. *Try it:* find all the ways of writing 98 as a sum of two primes.

Twin prime conjecture: OPEN. There are infinitely many primes p for which $p + 2$ is also prime, such as $11, 13$ and $101, 103$. In the 2010s Yitang Zhang, then a little-known university lecturer, proved that there are infinitely many pairs of primes at most 70 million apart. Within a year, a collaboration of mathematicians working together online reduced 70 million to 246. Closer, but 246 is not 2. *Try it:* list the twin prime pairs below 100.

Legendre's conjecture: OPEN. For every positive integer n, between the consecutive squares n^2 and $(n + 1)^2$ there is at least one prime: between 25 and 36 lie 29 and 31. It holds for every n up to about 10^9, and is still unproved. *Try it:* count the primes between 100 and 121.

Collatz conjecture: OPEN. Take any positive integer. Halve it if it is even; triple it and add 1 if it is odd. Repeat. Starting from 6 gives $6, 3, 10, 5, 16, 8, 4, 2, 1$. Does every starting number reach 1? Every start up to at least 2^{68}, about 3×10^{20}, does. Paul Erdős said of it that mathematics may not be ready for such problems. *Try it:* start from 27 with a spreadsheet or a few lines of code. It takes 111 steps to reach 1, and its largest value on the way is 9232.

Fermat's Last Theorem: PROVED. No positive integers x, y, z satisfy $x^n + y^n = z^n$ for any integer $n \geq 3$. For $n = 2$ there are many solutions, such as $3^2 + 4^2 = 5^2$. In the 1600s Fermat wrote in the margin of a book that he had a proof, but that the margin was too small to contain it. For more than 350 years it was called a theorem while it was only a conjecture. The accepted proof, by Andrew Wiles, came in the 1990s and uses mathematics developed long after Fermat. Fermat appears twice in this chapter:

his conjecture that every $2^{2^n}+1$ is prime (§3.2) was disproved by a single counterexample.

Pólya's conjecture: DISPROVED**.** For every $N>1$, at least half of the numbers from 1 to N have an odd number of prime factors, counted with repetition. It holds for every N below $906\,150\,257$, and it was believed for nearly forty years. In the 1950s Haselgrove proved that it must fail somewhere, without finding where. Decades later Tanaka found the smallest counterexample, $N=906\,150\,257$. This is the circle problem from the start of the chapter on a larger scale: nearly a billion cases agreed, then one did not. *Try it:* check that the conjecture holds for $N=10$. (The number 1 has no prime factors, and zero is even.)

Choose one of the open problems and test it for a few more cases. Notice how convincing the evidence starts to feel. Then remember Pólya.

End-of-Chapter Problems
Chapter 3: Proofs

1. Prove that the difference between the squares of any two consecutive odd integers is a multiple of 8. [3]

2. Consider the cube of a binomial.

(a) Prove the identity $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$. [3]
(b) Hence prove that $(n+1)^3 - n^3 = 3n^2 + 3n + 1$ for every integer n. [3]

3.

(a) Prove that $a^2 + b^2 \geq 2ab$ for all real numbers a and b. [2]
(b) Hence prove that $x + \frac{1}{x} \geq 2$ for every positive real number x, and state the value of x for which equality holds. [3]
(c) Prove that $a^2 + b^2 + c^2 \geq ab + bc + ca$ for all real numbers a, b and c. [3]

4. Disprove each claim by giving a counterexample.

(a) For every real number x, if $x^2 > 4$ then $x > 2$. [2]
(b) $3^n + 2$ is prime for every positive integer n. [2]

5. A student claims that $n^2 - n + 11$ is prime for every positive integer n.

(a) Verify the claim for $n = 1$ and $n = 2$. [2]
(b) Disprove the claim with a counterexample. [3]

6. Prove by contradiction that $x^2 - 6x + 10 = 0$ has no real solution, without using the discriminant. *(Hint: complete the square; see §4.4)* [3]

7. Let a be a non-zero rational number and b an irrational number.

(a) Prove by contradiction that ab is irrational. [4]
(b) Hence state, with a reason, whether $\frac{\sqrt{2}}{5}$ is rational or irrational. [2]

8. Prove by contradiction that there are no integers x and y such that $x^2 - y^2 = 10$. [5]

9. Prove that $\sqrt{2} + \sqrt{3}$ is irrational. You may assume that $\sqrt{6}$ is irrational. [5]

10. Prove by contradiction that $\sqrt[3]{5}$ is irrational. [6]

11. Prove that $\log_2 3$ is irrational. [5]

12. Prove that $3 + 8 + 13 + \cdots + (5n - 2) = \dfrac{n(5n+1)}{2}$ in two ways:

(a) directly, using the sum of an arithmetic sequence; [3]

(b) by induction. [3]

13.

(a) Prove by induction that $\displaystyle\sum_{r=1}^{n} \frac{1}{(2r-1)(2r+1)} = \frac{n}{2n+1}$ for all $n \geq 1$. [5]

(b) Hence find the least value of n for which the sum exceeds 0.49. [2]

(c) Write down the value that the sum approaches as n increases. [1]

14. Prove by induction that $\displaystyle\sum_{r=1}^{n} r \cdot r! = (n+1)! - 1$ for all $n \geq 1$. [6]

15. Prove by induction that $6^n + 4$ is divisible by 5 for all $n \geq 1$. [5]

16. Prove by induction that $5^{2n} - 1$ is divisible by 24 for all $n \geq 1$. [5]

17. Prove by induction that $3^{2n+2} - 8n - 9$ is divisible by 64 for all $n \geq 1$. [6]

18.

(a) Show that the inequality $2^n > n^2 + n$ is false for $n = 1$, 2, 3 and 4 but true for $n = 5$. [2]

(b) Prove by induction that $2^n > n^2 + n$ for all integers $n \geq 5$. [5]

19. Mira claims that $n > \log_2 n$ for every $n \in \mathbb{Z}^+$.

(a) Show that $1 + \log_2 n \geq \log_2(n+1)$ for $n \in \mathbb{Z}^+$. [2]

(b) Use mathematical induction and the result of part (a) to prove that Mira's claim is true. [5]

(c) Hence show that $2^n > n$ for every $n \in \mathbb{Z}^+$. [1]

20. Let n be an integer.

(a) By considering the cases n even and n odd, prove that n^2 leaves remainder 0 or 1 when divided by 4. [3]

(b) Hence prove by contradiction that no integer of the form $4m + 3$, where m is an integer, is the sum of the squares of two integers. [3]

21.

(a) Prove that if n^2 is a multiple of 3, then n is a multiple of 3. [3]

(b) Hence prove by contradiction that $\sqrt{3}$ is irrational. [5]

(c) Explain precisely where the argument in part (b) breaks down if you attempt to use it to prove that $\sqrt{9}$ is irrational. [3]

(d) A student writes: *"$\sqrt{3}$ is irrational, so $\sqrt{3} \times \sqrt{3}$ must be irrational too."* Explain the error, and state what it shows about products of irrational numbers. [3]

22.

(a) Prove by induction that $\sum_{r=1}^{n} r = \frac{n(n+1)}{2}$ for all $n \geq 1$. [5]

(b) You may assume that $\sum_{r=1}^{n} r^2 = \frac{n(n+1)(2n+1)}{6}$. Find $\sum_{r=1}^{n} r(r-1)$, giving your answer in fully factorised form. [4]

(c) Hence evaluate $\sum_{r=1}^{20} r(r-1)$. [3]

(d) Show that $\sum_{r=1}^{n} r(r-1) = 2\,{}^{n+1}C_3$, and explain why this means the sum is always even. [3]

23. This question proves *Bernoulli's inequality*.

(a) Prove by induction that $(1+x)^n \geq 1+nx$ for every integer $n \geq 1$ and every real number $x \geq -1$. [5]

(b) Hence show that $1.01^{100} \geq 2$. [2]

(c) By taking $n = 3$ and $x = -4$, show that the inequality can fail when $x < -1$, and identify the step of your proof in part (a) that needs $x \geq -1$. [3]

24. A sequence is defined by $u_1 = 1$ and $u_{n+1} = \frac{u_n}{1+u_n}$ for $n \geq 1$.

(a) Find u_2, u_3 and u_4. [3]

(b) Write down a conjecture for u_n in terms of n. [1]

(c) Prove your conjecture by induction. [5]

(d) A student's whole proof reads: *"Assume the statement is true for $n = k$. Then it is true for $n = k+1$. Hence it is true for all n."* State what is missing, and explain why the argument establishes nothing without it. [3]

(e) Give a statement P_n for which $P_k \Rightarrow P_{k+1}$ is true for every k, but P_n is false for every n. Justify both claims. [3]

25. Let n and r be integers with $1 \leq r \leq n$. Starting from ${}^{n}C_r = \frac{n!}{r!\,(n-r)!}$, prove Pascal's identity

$$ {}^{n}C_r + {}^{n}C_{r-1} = {}^{n+1}C_r. $$

[5]

26. Using Pascal's identity, prove by induction that for every integer $n \geq 1$,

$$(a+b)^n = \sum_{r=0}^{n} {}^nC_r a^{n-r} b^r.$$

[7]

27. A student claims that $\sqrt{x^2-2x+1} = x-1$ for every real number x. To prove it, the student squares both sides, obtains $x^2-2x+1=(x-1)^2$, notes that this is true for every x, and concludes that the claim is an identity.

(a) Disprove the claim with a counterexample. [2]
(b) Explain which step of the student's argument is not valid. [1]
(c) Find the set of real values of x for which $\sqrt{x^2-2x+1} = x-1$, justifying your answer. [3]

28. Let a and b be rational numbers. You may use the fact that $\sqrt{2}$ is irrational.

(a) Prove by contradiction that if $b \neq 0$, then $a+b\sqrt{2}$ is irrational. [4]
(b) State, with a reason, whether the result of part (a) remains true when $b=0$. [1]
(c) Hence find all rational numbers p and q such that $(p+q\sqrt{2})^2 = 3+2\sqrt{2}$. [5]

29. Let n be an integer.

(a) Prove by contradiction that if n^2+2n is odd, then n is odd. [3]
(b) A student begins a proof of part (a) with "*Assume that n^2+2n is even.*" Explain why this cannot lead to a proof. [1]
(c) Prove or disprove: if n is odd, then n^2+2n is odd. [2]

The remaining questions use the proof techniques of this chapter on material introduced later in the book. They appear in the order those topics are covered, so return to them as you go.

30. You may assume the compound-angle formulae for $\cos(A+B)$ and $\sin(A+B)$. Prove by induction that

$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta$$

for every integer $n \geq 1$. [6]

31. You may assume that $\dfrac{d}{dx}(x) = 1$ and the product rule. Prove by induction that

$$\frac{d}{dx}(x^n) = nx^{n-1}$$

for every integer $n \geq 1$. [6]

32. You may assume that $\dfrac{d}{dx}(e^x) = e^x$ and the product rule. Prove by induction that

$$\frac{d^n}{dx^n}(x^2 e^x) = (x^2 + 2nx + n(n-1))e^x$$

for every integer $n \geq 1$. [5]

33. You may assume $\lim\limits_{h \to 0} \dfrac{\sin h}{h} = 1$ and $\lim\limits_{h \to 0} \dfrac{\cos h - 1}{h} = 0$. Working from the definition

$$f'(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h},$$

prove that the derivative of $\sin x$ is $\cos x$. [6]

34. Let $I_n = \displaystyle\int_0^{\pi/2} \sin^n x \, dx$ for integers $n \geq 0$.

(a) Use integration by parts to prove that $I_n = \dfrac{n-1}{n} I_{n-2}$ for every integer $n \geq 2$. [5]
(b) Write down I_0 and I_1, and hence find I_4 and I_5. [4]

Challenge Questions

C1. Counting the regions of a circle. This investigation completes the problem from the start of the chapter. Throughout, n points are placed on a circle so that no three chords meet at a single interior point.

(a) By drawing, verify that $n = 1, 2, 3, 4, 5$ give $1, 2, 4, 8, 16$ regions. [2]
(b) Explain why each interior intersection point corresponds to exactly one choice of 4 of the n points, and deduce that there are ${}^nC_4$ interior points. [3]
(c) The chords and arcs form a network. Show that it has $V = n + {}^nC_4$ vertices and $E = n + {}^nC_2 + 2\,{}^nC_4$ edges. *(Hint: each interior point adds one extra segment to each of the two chords through it)* [4]
(d) Euler's formula for a connected planar network states $V - E + F = 2$, where F counts all faces including the region outside the circle. Use it to prove that the number of regions inside the circle is ${}^nC_4 + {}^nC_2 + 1$. [4]
(e) Hence find the number of regions for $n = 6$ and $n = 10$. [2]
(f) If the n points are equally spaced, the count for $n = 6$ is 30 rather than 31. Explain what changes. [3]

(g) Suggest two ways in which this investigation could be extended, for example by changing where the points are placed or by moving to three dimensions. For one of them, state a conjecture and describe how you would test it. [3]

C2. A proof that names no example. Consider the number $\sqrt{2}^{\sqrt{2}}$.

(a) Suppose $\sqrt{2}^{\sqrt{2}}$ is rational. Explain why this immediately produces an irrational number raised to an irrational power that is rational. [2]

(b) Suppose instead $\sqrt{2}^{\sqrt{2}}$ is irrational. Show that $\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = 2$, and explain why this also produces such a pair. [4]

(c) Conclude that there exist irrational a and b with a^b rational. [2]

(d) Given that $\log_2 3$ is irrational (Q11), show that $2\log_2 3$ is irrational and that $\sqrt{2}^{\,2\log_2 3} = 3$. Explain why this gives a second proof of the result in part (c). [3]

(e) The argument in parts (a) to (c) proves that such a pair exists without telling you which case is the true one. Compare it with the proof in part (d), and comment on what each proof gives you. [3]

(f) Investigate which positive rational numbers r can be written as a^b with a and b both irrational and $a > 0$. Justify your answer for at least one value of r that needs a different method from part (d), and suggest how the question could be taken further. [3]

C3. Fermat's conjecture. In 1640 Fermat studied the numbers $F_n = 2^{2^n} + 1$, for integers $n \geq 0$, and conjectured that all of them are prime.

(a) Show that F_0, F_1, F_2, F_3 and F_4 are prime. For $F_4 = 65\,537$ you may use a calculator or a short program to test divisors. [3]

(b) Let m be a positive integer, and suppose m has an odd factor $d > 1$, so $m = de$. Using the factorisation

$$x^d + 1 = (x+1)\left(x^{d-1} - x^{d-2} + \cdots - x + 1\right) \quad (d \text{ odd}),$$

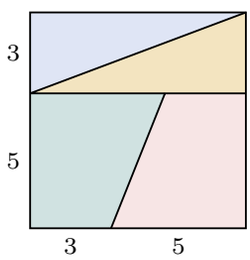
with $x = 2^e$, prove that $2^m + 1$ is not prime. [5]

(c) Let m be a positive integer. Deduce that if $2^m + 1$ is prime, then m must be a power of 2. [2]

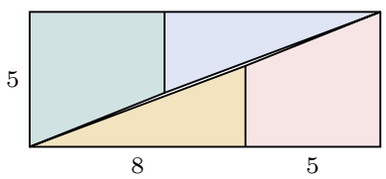
(d) Euler found in 1732 that 641 divides $F_5 = 2^{32} + 1$. This part proves it without dividing. Let $x = 5 \cdot 2^7$, and note that $641 = x + 1 = 5^4 + 2^4$. Show that 641 divides $x^4 - 1$, and that $5^4 \cdot 2^{28} + 2^{32} = 641 \cdot 2^{28}$. Deduce that 641 divides $2^{32} + 1$, and state what this shows about Fermat's conjecture. [5]

(e) Lucas later proved that, for $n \geq 2$, every prime factor of F_n has the form $k \cdot 2^{n+2} + 1$ for some positive integer k. Check this for the factor 641 of F_5, and explain how the result shortens a search for a factor of F_6. Suggest a direction in which Fermat numbers could be investigated further. [3]

C4. Cassini's identity and a missing square. The Fibonacci numbers are defined by $f_1 = f_2 = 1$ and $f_{n+2} = f_{n+1} + f_n$ for $n \geq 1$. The diagram shows the dissection used in part (c).



8×8 square, area 64



5×13 rectangle, area 65

(a) Compute $f_{n-1}f_{n+1} - f_n^2$ for $n = 2, 3, \ldots, 8$, and make a conjecture. [2]

(b) Prove by induction that $f_{n-1}f_{n+1} - f_n^2 = (-1)^n$ for all integers $n \geq 2$. [5]

(c) An 8×8 square is cut into four pieces: two right-angled triangles with perpendicular sides 3 and 8, and two right-angled trapezia with parallel sides 3 and 5 and perpendicular height 5. The pieces are rearranged to appear to fill a 5×13 rectangle. Use part (b) to explain why the two areas differ by exactly 1, and state the general version of the puzzle for an $f_n \times f_n$ square, saying when the rectangle appears larger and when smaller. [3]

(d) In the rectangle the long edges of the pieces should lie along a diagonal. Find the gradient of the hypotenuse of a triangle, the gradient of the slanted edge of a trapezium, and the gradient of the diagonal of the rectangle. Hence explain where the extra unit of area is. [4]

(e) The same puzzle made from a 21×21 square uses pieces whose slanted edges have gradients $\frac{8}{21}$ and $\frac{5}{13}$. Find the difference between these gradients, compare it with part (d), and explain why this version is harder to detect by eye. [2]

(f) Cassini's identity is the case $r = 1$ of Catalan's identity, $f_n^2 - f_{n-r}f_{n+r} = (-1)^{n-r}f_r^2$ for $1 \leq r < n$. Verify Catalan's identity for $n = 7$, $r = 3$, and suggest a direction in which this investigation could be extended. [3]

C5. When does 2^n overtake n^3? Exponential growth eventually beats any power, but "eventually" can take a while. This investigation finds exactly when, and proves it.

(a) Tabulate 2^n and n^3 for $n = 1, 2, \ldots, 12$. State the values of n in this range for which $2^n > n^3$, and conjecture the least integer N such that $2^n > n^3$ for all $n \geq N$. [2]

(b) Show that $\left(1 + \frac{1}{k}\right)^3 < 2$ for every integer $k \geq 4$. [2]

(c) Prove by induction that $2^n > n^3$ for all integers $n \geq 10$. [5]

(d) The inductive step in part (c) is valid for every $k \geq 4$, and $2^1 > 1^3$ is true. Explain why neither fact allows the induction to start before $n = 10$. [2]

(e) Find the least integer N such that $2^n > n^4$ for all $n \geq N$, and prove your answer. [4]

(f) Let $N(k)$ be the least integer such that $2^n > n^k$ for all $n \geq N(k)$. Using your results and the notes' $N(2) = 5$, find $N(k)$ for $k = 5, 6, 7$ by calculation, and conjecture how $N(k)$ grows with k. Suggest how the conjecture could be tested or explained. [3]