NUMBER & ALGEBRA

Chapter 3

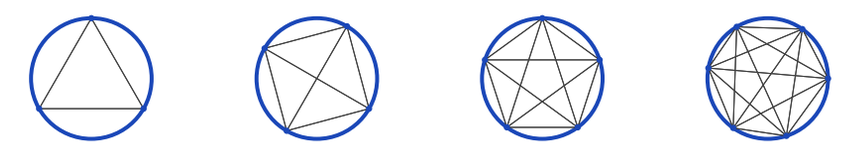
Proofs

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, and no three chords meet at one point.

Five cases followed the doubling rule and the sixth did not. The first five gave no sign of it, and no number of agreeing cases could have shown the rule 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 fail, however many points you take.

By the end of this chapter you will be able to prove a statement directly from definitions, disprove one with a single counterexample, argue by contradiction, and prove a result about every positive integer by induction. Checking a rule on a few cases shows only that it has not failed yet. A proof shows that it cannot fail.

© 2026 Hasan Khan 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.

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 worked in the opposite direction. It used a few particular cases 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 cannot.

The two directions differ in certainty. Deduction goes from a rule about every case to one particular case. Induction in the everyday sense goes from a few cases to a rule about all of them, and only deduction is certain. 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, and it is the last method this chapter builds.

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.

DEF An **equation** is a statement that two expressions are equal for *some particular* values of the variable. An **identity** is a statement that they are equal 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 $\equiv$ marks which of the two is meant: where it appears, the claim is "for all x", not "find x".

You already know one important identity from trigonometry:

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

This is true for every angle x, not for some particular angles, which is why it is written with $\equiv$. 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 the LHS, change it one line at a time, and finish with the RHS. Write the labels LHS and RHS in your working, so the direction of the argument is clear to the marker.

CAUTION Do not start by assuming the identity is true and then manipulate both sides until you reach something obvious like $0 = 0$. That assumes what you are trying to prove. Transform *one* side into the other instead.

Worked through. To prove that $(a+b)^2 - (a-b)^2 \equiv 4ab$, the difficulty is avoiding a common error: doing the same thing to both sides. Start from the LHS instead 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:

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

Nothing but expansion was used, and the LHS turned into the RHS. The two sides were never assumed to be equal. That they are equal is the result, not the starting point.

A quick **check** takes about five seconds, and many errors show up in it. At $a = 3$, $b = 2$ the left side is $25 - 1 = 24$ and the right side is $4(3)(2) = 24$. A check is not a proof. But if a check fails, something is certainly wrong.

TIP Check your results by substituting a number where you can. An algebra error will usually show up at one well-chosen value.

EXAMPLE 3.1

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

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

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 $m^2 + m = 12$.

For the general statement, start from the left side and factor 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.

Once the general case is written in symbols, the rest is ordinary algebra.

Worked through. A single example such as $3+5=8$ confirms nothing about *all* odd numbers. To prove that the sum of any two odd numbers is even, let the two odd numbers be $2a+1$ and $2b+1$, where a and b are integers. Their sum is

$$(2a+1)+(2b+1) = 2a+2b+2 = 2(a+b+1).$$

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

EXAMPLE 3.2

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

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, prove divisibility by each factor separately. The factors must be **coprime**, sharing no factor larger than 1: a number divisible by 2 and by 4 need not be divisible by 8, as 12 shows.

EXAMPLE 3.3

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

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 the forms $3k$, $3k+1$ or $3k+2$, where k is an integer. If $n = 3k$, then the first factor is a multiple of 3. If $n = 3k+1$, then $2n+1 = 6k+3 = 3(2k+1)$. If $n = 3k+2$, then $n+1 = 3k+3 = 3(k+1)$. 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. Since 2 and 3 are coprime, these are separate factors, and the product is divisible by $2 \times 3 = 6$. ■

CAUTION One example can never prove a statement that begins "for all." It can only *disprove* one, which is the subject of the next section. The proofs above work because the algebra stands for every case at once.

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 $n^2 + (n+1)^2 + \big(n(n+1)\big)^2 \equiv (n^2+n+1)^2$, 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.

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

The logic is exact. "Every n has property P" is false as soon as one value of n does not have property P. 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.

Worked through. The formula $n^2 + n + 41$ is famous because it produces a prime number for $n = 0, 1, 2, \ldots, 39$, forty primes in a row. To decide whether it produces a prime for *every* non-negative integer n, test the claim at the first value the pattern does not cover. At $n = 40$:

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

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. One case was enough to make it false. Examples can make a claim look true. They can never make it certain.

EXAMPLE 3.4

Disprove the claim: "every multiple of 3 is odd."

The number 6 is a multiple of 3, and 6 is even. That single case is a counterexample, so the claim is false. ■

EXAMPLE 3.5

Show that this statement is not always true: "there are no positive integer solutions to the equation $x^2 + y^2 = 10$."

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. ■

Notice what the answer contains: the values, the substitution, and the conclusion. Giving only "$x = 1$, $y = 3$" would not earn full marks.

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 $9 > 1$ while $-3 < 1$, because squaring removes the sign. The second is "the product of two irrational numbers is irrational". Take $\sqrt{2} \times \sqrt{2} = 2$, which is rational.

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.

CAUTION A counterexample only *disproves* a claim. Finding no counterexample after many attempts is not a proof. The circle problem at the start of this chapter shows why: five cases agreed, and the sixth did not.

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.

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. The claim disproves itself.

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.

DEF In **proof by contradiction**, you assume the negation of what you want to prove, then derive a logical contradiction. The contradiction forces the assumption to be false, which establishes the original claim.

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. A direct proof that no fraction equals $\sqrt{2}$ would mean checking infinitely many fractions. 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. 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.

Worked through. To prove that $\sqrt{2}$ is irrational, a classical result alluded to by Aristotle in the 4th century BCE, assume the opposite: that $\sqrt{2}$ *is* rational. Then we can write

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

where p and q are integers **sharing no common factor**, so the fraction is fully cancelled. The contradiction at the end of the proof depends on this condition, so state it explicitly. Squaring both sides gives $2 = \dfrac{p^2}{q^2}$, hence

$$p^2 = 2q^2.$$

So p^2 is even, which forces p itself to be even (the square of an odd number is odd). Write $p = 2m$. Then $p^2 = 4m^2$, and substituting,

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

so q^2 is even, and therefore q is even too. But now p and q are both even, sharing the factor 2, contradicting our choice of a fully cancelled fraction. The assumption that $\sqrt{2}$ is rational is impossible, so $\sqrt{2}$ is irrational. ∎

Tradition links this result to the end of the Pythagorean belief that every ratio of lengths is a ratio of whole numbers. The diagonal of a unit square has length $\sqrt{2}$, and the proof above says no fraction gives it.

Worked through. To prove that there are infinitely many prime numbers, a result from Euclid's *Elements* (c. 300 BCE), assume the opposite: that there are only finitely many primes, and list them all as $p_1, p_2, \ldots, p_n$. Build the number

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

the product of every prime, plus one. Dividing N by any prime on the list leaves remainder 1, so N is divisible by none of them. Yet every integer greater than 1 has at least one prime factor. That factor cannot be on our list, so our list was not complete, a contradiction. No

finite list can hold all the primes, so there are infinitely many. ■

Notice what the proof does not do: it never produces a new prime, only shows that the list was incomplete. N itself need not be prime. With $2, 3, 5, 7, 11, 13$ the number $N = 30031 = 59 \times 509$, and both factors are primes missing from the list.

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. A small result proved on the way to a larger one is called a **lemma**. With the matching lemma in place of the fact about even numbers, the $\sqrt{2}$ proof works for $\sqrt{5}$ step by step. The next example proves that fact directly, by checking every case; it is not itself a proof by contradiction.

EXAMPLE 3.6

Prove that if n^2 is a multiple of 5, then n is a multiple of 5.
Nothing is assumed here; every possible case is checked. Every integer lies within 2 of a multiple of 5, so n is $5k$, $5k \pm 1$ or $5k \pm 2$ for some integer k. Square each form:

$$(5k)^2 = 5(5k^2), \qquad (5k \pm 1)^2 = 5(5k^2 \pm 2k) + 1, \qquad (5k \pm 2)^2 = 5(5k^2 \pm 4k) + 4.$$

Only the first of these 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, assume $\sqrt{5} = \frac{p}{q}$ in lowest terms, deduce that 5 divides p and then that 5 divides q, and reach the same contradiction.

Rational numbers have **closure**: adding, subtracting or multiplying two rational numbers, or dividing one by a non-zero rational, gives a rational number. 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.

EXAMPLE 3.7

Prove that $(1 + \sqrt{2})^2$ is irrational. You may use the theorem that $\sqrt{2}$ is irrational.
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. ■

Both middle steps use closure. Subtracting 3 and dividing by 2 each move from one rational number to another, so neither could have carried a rational number to an irrational one.

The contradiction here is with a result already established, not with anything internal to $(1+\sqrt{2})^2$. Expanding made the argument possible, because it wrote the expression in terms of $\sqrt{2}$: identify the known irrational first, then rearrange to make it 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) The sum of a rational number and an irrational number 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.

Mathematical induction is exactly this idea, used to prove a statement P_n for every integer n from some starting value onward. The subscript in P_n matters: it marks the n-th claim in an infinite list $P_1, P_2, P_3, \ldots$, not a function being evaluated. You verify the first claim, then prove that each claim forces the one after it.

KEY **Principle of mathematical induction.** To prove that P_n holds for all integers $n \geq 1$:

1. Show that P_1 is true.
2. Assume that P_k is true for **some** $k \geq 1$ (the *inductive hypothesis*).
3. Show that P_k implies P_{k+1}.
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_0, begin at P_{n_0} instead of P_1.)

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.

Step 3 is written $P_k \Rightarrow P_{k+1}$, read "P_k implies P_{k+1}". In logic, an implication $A \Rightarrow B$ is false in exactly one case: when A is true and B is false.

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

So step 3 does not claim that P_k is true. It claims only that P_k cannot be true while P_{k+1} is false, which is why the hypothesis may be assumed without being proved. For the same reason step 1 cannot be skipped. If P_n is "$n(n+1)$ is odd", then $(k+1)(k+2) = k(k+1) + 2(k+1)$, so $P_k \Rightarrow P_{k+1}$ holds, yet every P_n is false: $n(n+1)$ is a product of consecutive integers and is always even. The implications form a chain, but the chain proves nothing until one case is known to be true.

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 withhold the reasoning marks for it. The hypothesis is one domino falling, not the whole line.

3.4.1 Why induction works

The domino image can be made precise. Suppose steps 1 and 3 are done, and pick any n you like, say $n = 1000$. Then P_1 is true; P_1 forces P_2; P_2 forces P_3; and after 999 applications of the inductive step, 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 ever proved.

There is a second way to see it, and it connects induction to the previous section. Suppose the two steps are done, but P_n failed for some values of n. Among the failures there would be a *smallest* one, say P_m. Now $m \neq 1$, because step 1 checked P_1. So $m - 1 \geq 1$, and

P_{m-1} is true, since m was the smallest failure. But step 3 says that P_{m-1} forces P_m, which contradicts the failure of P_m. So the principle of induction can itself be justified by contradiction, and the two techniques of this chapter are closely connected.

Induction is not only for sums. It also proves divisibility statements and inequalities below, De Moivre's theorem in Ch. 17, and formulas for n-th derivatives in Ch. 13. 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

How to approach it. Here P_n says that a sum equals a formula. Add the next term of the sum to both sides of the assumption P_k. Then rearrange the right-hand side until it becomes the original formula with $k+1$ written wherever n appeared. Write that target expression down before you begin, so you know what you are aiming at.

Worked through. To prove that $3 + 7 + 11 + \cdots + (4n-1) = n(2n+1)$ for all integers $n \geq 1$, let P_n be the statement $3 + 7 + \cdots + (4n-1) = n(2n+1)$.

Step 1 (P_1): the left side is 3; the right side is $1(2(1)+1) = 3$. They agree, so P_1 is true.

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

$$3 + 7 + \cdots + (4k-1) = k(2k+1).$$

Step 3: add the next term, $4(k+1) - 1 = 4k + 3$, to both sides:

$$3 + 7 + \cdots + (4k-1) + (4k+3) = k(2k+1) + 4k + 3.$$

Expand the right side and factorise it:

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

This is exactly P_{k+1}, the original formula with n replaced by $k+1$. So $P_k \Rightarrow P_{k+1}$.

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 $n \geq 1$. ■

3.4.3 Induction for divisibility

The same four steps prove divisibility statements.

How to approach it. 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 $d \times (\text{integer})$.

Worked through. To prove that $8^n - 1$ is divisible by 7 for all integers $n \geq 1$, 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: consider the next case:

$$8^{k+1} - 1 = 8 \cdot 8^k - 1 = 8(8^k - 1) + 8 - 1 = 8(7m) + 7 = 7(8m + 1).$$

Since $8m + 1$ is an integer, $8^{k+1} - 1$ is divisible by 7, which is P_{k+1}. So $P_k \Rightarrow P_{k+1}$.

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 hypothesis was used: rewriting $8^k - 1$ as $7m$ is the only reason the final line factors cleanly.

EXAMPLE 3.8

In $8^n - 1$ the previous expression appeared as soon as a factor was taken out at the front. Prove that $n^5 + 4n$ is divisible by 5 for all integers $n \geq 1$, where it has to be extracted from an expansion instead.

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: expand the next case and collect $k^5 + 4k$ out of it:

$$(k+1)^5+4(k+1) = k^5+5k^4+10k^3+10k^2+5k+1+4k+4 = (k^5+4k)+5k^4+10k^3+10k^2+5k+5.$$

The hypothesis replaces the bracket by $5m$, and every remaining term has a factor 5:

$$= 5m + 5(k^4 + 2k^3 + 2k^2 + k + 1) = 5(m + k^4 + 2k^3 + 2k^2 + k + 1).$$

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 $P_k \Rightarrow P_{k+1}$.

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 $n \geq 1$. ■

Expand fully first, then look for the previous expression inside the result. If what is left over after removing it does not carry the required factor, the grouping is wrong, not the statement.

3.4.4 Induction for an inequality

How to approach it. Here P_n says that $A_n > B_n$. Inequalities are proved by chaining: 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 link. Now prove separately that this new quantity is at least B_{k+1}, which gives the second link. The two

links join into a single chain from A_{k+1} down to B_{k+1}.

Worked through. To prove that $2^n > n^2$ for all integers $n \geq 5$, let P_n be the statement $2^n > n^2$. The base case is not $n = 1$ here, and that matters: the inequality is false for $n = 2, 3, 4$.

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: then

$$2^{k+1} = 2 \cdot 2^k > 2k^2.$$

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 certainly holds, since $k^2 - 2k - 1 = (k-1)^2 - 2 \geq 16 - 2 > 0$. Therefore

$$2^{k+1} > 2k^2 \geq (k+1)^2,$$

which is P_{k+1}. So $P_k \Rightarrow P_{k+1}$.

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

How to approach it. Here the sequence is given by a rule linking each term to the one before, with no formula in n to prove. Compute the first few terms, conjecture a **closed form** for u_n, and let P_n be that closed form. In the inductive step the hypothesis is substituted into the recurrence rather than added to a sum: 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.

Worked through. A sequence is defined by $u_1 = 1$ and $u_{n+1} = \dfrac{u_n}{1 + 2u_n}$ for $n \geq 1$. To find a formula for u_n and prove it, 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 $u_n = \dfrac{1}{2n-1}$. 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: substitute the hypothesis into the recurrence:

$$u_{k+1} = \frac{u_k}{1 + 2u_k} = \frac{1/(2k-1)}{1 + 2/(2k-1)}.$$

Multiply numerator and denominator by $2k-1$:

$$= \frac{1}{(2k-1)+2} = \frac{1}{2k+1} = \frac{1}{2(k+1)-1},$$

which is the formula with n replaced by $k+1$, so $P_k \Rightarrow P_{k+1}$.

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 $n \geq 1$. ■

The four terms produced the conjecture and established nothing; the induction established it. A question of this shape marks the two jobs separately, so give the terms, state the conjecture, and then prove it.

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 hypothesis. If you never used P_k, you have not built a chain, only restated the problem.

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

(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 for which the inequality holds.

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

Recurrences

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 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 $n \geq 1$.

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 those starting points, the axioms, are assumed rather than proved. In 1931 Kurt Gödel showed that any consistent system (one that never proves a contradiction) rich enough to describe arithmetic contains true statements 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 contradicted that belief: the diagonal of a unit square has length $\sqrt{2}$, and no such ratio gives it. Nobody knows how the discovery was made. The classical argument, which Aristotle alludes to, is the one used in §3.3, and it is a proof by contradiction: assume $\sqrt{2} = p/q$ in lowest terms, and an impossibility follows. The discovery is credited to Hippasus in the fifth century BCE, and later writers report that his school received it badly. The result stood regardless, 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 exactly. 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 not been proved hard.

EXT The four-colour theorem says any map can be coloured with four colours so that no two neighbouring regions match. In 1976 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?

A gallery of conjectures

Many theorems began as conjectures. The seven below are a small selection, chosen because each is about whole numbers and can be stated with nothing beyond the arithmetic of this course. Those marked open have been neither proved nor disproved; the remaining two show what settling a conjecture looks like, in opposite directions. None is examinable, and far more exist than are listed here, so you are invited to search out others of your own.

Goldbach conjecture (1742): open. Every even number greater than 2 is the sum of two primes: $28 = 5 + 23$, $100 = 3 + 97$. Checked for every even number up to 4×10^{18}, and still unproved.

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 2013 Yitang Zhang proved there are infinitely many prime pairs at most 70 million apart. Later work brought that down to 246. Closer, but 246 is not 2.

Collatz conjecture: open. Take any positive integer. Halve it if even; triple it and add 1 if odd. Repeat. Does every starting number reach 1? Try 27 on your GDC: it takes 111 steps and climbs to 9232 on the way. Checked for a vast number of starting values, proved for none.

Odd perfect numbers: open for ∼2300 years. A number is perfect if it equals the sum of its proper divisors, such as $6 = 1 + 2 + 3$ and $28 = 1 + 2 + 4 + 7 + 14$. Every perfect number ever found is even. Whether an odd one exists is among the oldest unsolved problems in mathematics. Any example must be larger than 10^{1500}.

Legendre's conjecture: open. Between any two consecutive squares n^2 and $(n + 1)^2$ there is always at least one prime. It is true in every case ever checked, and still unproved.

Fermat's Last Theorem (1637): proved, 1995. No positive integers satisfy $x^n + y^n = z^n$ for $n \geq 3$. Fermat wrote in a book's margin that he had a proof, but that the margin was too small to hold it. The first accepted proof came 358 years later, from Andrew Wiles, and it uses mathematics far beyond anything Fermat could have known. Conjectures can be settled, and this one was.

Pólya's conjecture (1919): disproved. For every $N > 1$, at least half of the numbers up to N have an odd number of prime factors, counted with repetition. Checked for millions of cases and believed for nearly forty years, it was disproved by Haselgrove in 1958; the smallest counterexample, $N = 906{,}150{,}257$, was found by Tanaka in 1980. This is the circle problem from the start of the chapter on a larger scale: millions of cases agreed, one did not, and the claim is false.

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. 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]

4. 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]

5.

(a) Prove that $a^2 + b^2 \geq 2ab$ for all real numbers a and b. [2]
(b) Hence prove that $x + \dfrac{1}{x} \geq 2$ 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]

6. 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]

7. Prove by contradiction that $x^2 - 6x + 10 = 0$ has no real solution, without using the discriminant. [3]

8. 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 $\dfrac{\sqrt{2}}{5}$ is rational or irrational. [2]

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

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

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

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

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

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

15.

(a) Show that the inequality $2^n > n^2$ is true for $n = 1$ but false for $n = 2$, 3 and 4. [2]
(b) Prove by induction that $2^n > n^2$ for all integers $n \geq 5$. [5]

16. Prove that $1 + 3 + 5 + \cdots + (2n - 1) = n^2$ in two ways:

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

17.

(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]

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

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

20. 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]

21.

(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]

22.

(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]

23. 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]

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.

24. 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]

25. 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]

26. 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]

27. 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]

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

$$\frac{d^n}{dx^n}(xe^x) = (x+n)e^x$$

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

29. 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]

30. 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

31. 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]

32. 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. [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) Euler also 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]

33. 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 (Q12), 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]

34. 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 $n \geq 1$.

(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]

35. 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]