Specialist Mathematics Units 1 & 2

Chapter 1 — Proof and number

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

Attribution: Classbasics Pty Ltd, vwx.au

Aboriginal and Torres Strait Islander content has been excluded as accuracy cannot be guaranteed, and it is better to be respectful than cover the entire curriculum inaccurately.

Significant effort has been made to ensure this content is legal. Please send any areas of concern to admin@vwx.au with appropriate document/legal references so errors can be verified and changes be made.

Contents

Theory

Specialist Mathematics is a course about *why* results are true, not merely how to compute them. Before any proof can be written, the objects a proof talks about must be named precisely. This first section fixes that language: the **sets** that mathematics collects its objects into, and the tower of **number systems** $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ that the whole subject is built on. The ideas are elementary, but the precision is not optional — every later argument leans on it.

Sets, elements and membership.

A **set** is a collection of distinct objects, considered as a whole. The objects in a set are its **elements** (or **members**). If an object x is an element of a set A we write $x \in A$; if it is not, we write $x \notin A$. A set is completely determined by *which* objects belong to it — nothing else. In particular the elements of a set are **distinct** (each is listed once) and **unordered** (listing order carries no meaning), so $\{3,5,8\}$, $\{8,3,5\}$ and $\{3,3,5,8\}$ all denote the same set.

A set may be described by **listing** (roster) its elements inside braces, as in $A = \{2,4,6,8\}$, or by **set-builder notation**, which states a defining property:

$$A = \{x : x \text{ has the property } P\},$$

read "the set of all x such that P". For example $\{x \in \mathbb{Z} : 1 \le x \le 4\}$ is the set $\{1,2,3,4\}$. The number of elements of a finite set A is its **cardinality**, written $|A|$; here $|A| = 4$.

The **empty set**, written $\varnothing$ (or $\{\}$), is the unique set with no elements at all, so $|\varnothing| = 0$. It is not "nothing"; it is a perfectly good set that happens to contain nothing.

Subsets.

A set A is a **subset** of a set B, written $A \subseteq B$, when *every* element of A is also an element of B:

$$A \subseteq B \text{ means } x \in A \Rightarrow x \in B.$$

If in addition $A \neq B$ — that is, B contains at least one element not in A — then A is a **proper subset** of B, written $A \subset B$. Two sets are **equal** exactly when each is a subset of the other: $A = B$ precisely when $A \subseteq B$ and $B \subseteq A$. Two conventions hold for every set A: the empty set is a subset of it, $\varnothing \subseteq A$, and A is a subset of itself, $A \subseteq A$.

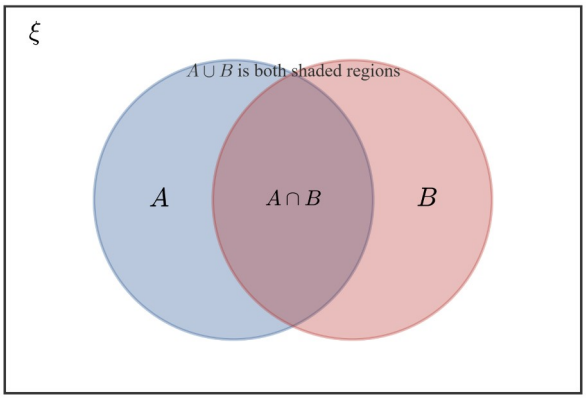
It is essential to keep **membership** ($\in$) and **subset** ($\subseteq$) apart. For $S = \{3,5,8\}$ the object 5 is an *element*, so $5 \in S$; the one-element set $\{5\}$ is a *subset*, so $\{5\} \subseteq S$; but $5 \subseteq S$ is meaningless nonsense (a number is not a set of elements of S).

Set operations.

Fix a **universal set** ξ (also written U) — the set of all objects currently under discussion. For sets $A, B \subseteq \xi$:

- the **union** $A \cup B = \{x : x \in A \text{ or } x \in B\}$ collects the elements in *either* set (the "or" is inclusive);
- the **intersection** $A \cap B = \{x : x \in A \text{ and } x \in B\}$ collects the elements in *both* sets;
- the **complement** $A^c = \{x \in \xi : x \notin A\}$ collects the elements of the universal set *not* in A;
- the **set difference** $A \setminus B = \{x : x \in A \text{ and } x \notin B\}$ collects the elements of A that are not in B, so that $A^c = \xi \setminus A$.

Two sets with no common element, $A \cap B = \varnothing$, are said to be **disjoint**. These operations are pictured with a **Venn diagram**, in which the universal set is a rectangle and each set a region inside it.



The two operations of union and complement obey **De Morgan's laws**,

$$(A \cup B)^c = A^c \cap B^c, (A \cap B)^c = A^c \cup B^c,$$

which say that the complement of a union is the intersection of the complements, and vice versa; both are read directly off the diagram and verified again in the questions.

The power set.

Gathering *all* the subsets of a set into a single new set gives the **power set**. For any set A,

$$P(A) = \{S : S \subseteq A\},$$

the set whose elements are exactly the subsets of A. Every power set contains at least and A itself. For example, if $A = \{4, 7\}$ then

$$P(A) = \{\quad, \{4\}, \{7\}, \{4, 7\}\},$$

which has 4 elements. In general, building a subset means deciding *independently* for each element whether to include it — two choices per element — so a set with n elements has exactly

$$|P(A)| = 2^n$$

subsets. (Of these, $2^n - 1$ are proper subsets, all except A itself.) The elements of $P(A)$ are *sets*, not the original objects: for $A = \{4, 7\}$ we have $4 \in A$ but $\{4\} \in P(A)$.

The number systems.

Counting begins with the **natural numbers**

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\},$$

the positive whole numbers used for counting. (Some authors include 0; in this course $\mathbb{N}$ denotes the positive integers.) Allowing zero and the negatives gives the **integers**

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

Permitting division produces the **rational numbers** — the numbers expressible as a ratio of two integers:

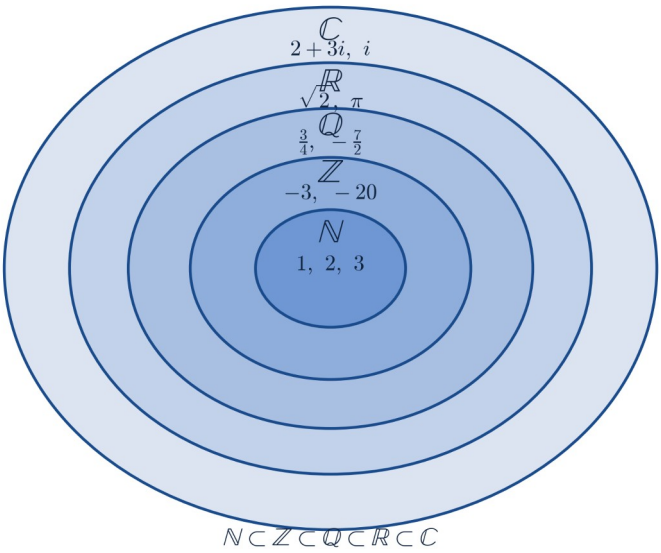
$$\mathbb{Q} = \{p/q : p, q \in \mathbb{Z}, q \neq 0\}.$$

Not every length is rational: the diagonal of a unit square has length $\sqrt{2}$, which is not a ratio of integers (a fact proved in a later section). Filling in every point of the number line — every rational together with every **irrational** such as $\sqrt{2}$ and π — gives the **real numbers** $\mathbb{R}$. The irrationals are precisely those reals not in $\mathbb{Q}$, that is $\mathbb{R} \setminus \mathbb{Q}$. Finally, adjoining a number i with $i^2 = -1$ (developed in Chapter 11) gives the **complex numbers**

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}.$$

Each system sits inside the next as a *proper* subset, since each new stage introduces numbers the previous one lacked:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$



To classify a given number, name the **smallest** system in this chain that contains it: $6 \in \mathbb{N}$, $-6 \in \mathbb{Z}$, $3/4 \in \mathbb{Q}$, $\sqrt{5} \in \mathbb{R}$, and $2+3i \in \mathbb{C}$.

Closure and structure.

What distinguishes these systems is not only *which* numbers they hold but *how they behave* under arithmetic. A set S is **closed** under a binary operation $*$ if performing that operation on members of S never leaves S:

$$S \text{ is closed under } * \text{ means } a, b \in S \Rightarrow a * b \in S.$$

The natural numbers are closed under addition and multiplication (a sum or product of positive integers is again a positive integer) but **not** under subtraction — for instance $3-8=-5 \notin \mathbb{N}$ — nor under division. Extending to $\mathbb{Z}$ restores closure under subtraction, yet $\mathbb{Z}$ is still not closed under division, since $7 \div 2 = 7/2 \notin \mathbb{Z}$. The rationals $\mathbb{Q}$ close this last gap: they are closed under addition, subtraction, multiplication and division by any *non-zero* rational, because

$$\frac{p}{q} \div \frac{r}{s} = \frac{ps}{qr} \in \mathbb{Q} \left(r \neq 0\right).$$

A single counterexample is enough to show a set is *not* closed under an operation, whereas closure itself is a claim about *every* pair of members. Each of $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ is closed under all four operations (excluding division by zero) and, with the usual commutative, associative and distributive laws, forms what is later called a **field**; the natural numbers and integers do not.

Rationals as decimals: terminating and recurring.

Because a rational is a ratio p/q, its decimal form comes from the division $p \div q$. At each step the remainder is one of the finitely many values $0, 1, \ldots, q-1$; if a remainder 0 occurs the process stops and the decimal **terminates**, and if not, some remainder must eventually repeat, from which point the digits **recur** in a fixed block. This gives a clean characterisation:

> A real number is **rational** if and only if its decimal expansion either **terminates** or is eventually **recurring**.

A recurring block is marked with an overbar: $0.\overline{4} = 0.444\ldots$ and $0.2\overline{3} = 0.2333\ldots$ Whether a rational terminates can be decided *without dividing*, by inspecting the denominator in lowest terms. A terminating decimal is a fraction over a power of ten, and $10^k = 2^k \times 5^k$ has only 2 and 5 as prime factors, so:

Written in lowest terms, p/q has a **terminating** decimal exactly when the only prime factors of q are 2 and/or 5; otherwise the decimal **recurs**.

Thus $9/40 = 9/2^3 \times 5$ terminates ($=0.225$), while $7/30 = 7/2 \times 3 \times 5$ recurs ($=0.2\overline{3}$) because of the factor 3. The lowest-terms proviso matters: $21/56$ *looks* as though the 7 in 56 forces recurrence, but $21/56 = 3/8$ terminates.

Converting a recurring decimal to a fraction.

The characterisation above guarantees every recurring decimal *is* rational; the fraction is recovered by a subtraction that cancels the infinite tail. Multiply the number by the power of ten that shifts one full recurring block to the left of the point, then subtract the original so the identical tails cancel. For $x = 0.\overline{72}$ the block has two digits, so multiply by 100:

$$100x = 72.\overline{72}, \quad 100x - x = 72.\overline{72} - 0.\overline{72} = 72,$$

hence $99x = 72$ and $x = 72/99 = 8/11$. When some digits *precede* the recurring block, first shift past the non-recurring digits as well; this technique is carried out in full in the worked examples.

Worked examples

Example 1 — scaffolded

Let $\xi = \{n \in \mathbb{Z} : 20 \le n \le 30\}$, with $A = \{21, 23, 24, 29\}$ and $B = \{20, 24, 26, 29, 30\}$. Find (a) whether $24 \in A$ and whether $25 \in A$, and state $|B|$; (b) $A \cup B$; (c) $A \cap B$; (d) A^c; and (e) $B \setminus A$.

Working	Comment
$\xi = \{20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30\}$.	List the universal set from the set-builder rule.
$24 \in A$ is **true**; $25 \in A$ is **false**; $\lvert B \rvert = 5$.	Check membership element by element; B has five listed members.
$A \cup B = \{20, 21, 23, 24, 26, 29, 30\}$.	Union: everything in A **or** B, each element once.
$A \cap B = \{24, 29\}$.	Intersection: only the elements in **both** A and B.
$A^c = \xi \setminus A = \{20, 22, 25, 26, 27, 28, 30\}$.	Complement: the members of ξ **not** in A.
$B \setminus A = \{20, 26, 30\}$.	In B but not in A: remove 24 and 29 from B.

Example 2 — scaffolded

(a) Name the smallest of $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ to which each of 12, -8, $7/16$, $\sqrt{5}$ and $4 - 3i$ belongs. (b) State, with a counterexample if false, whether $\mathbb{N}$ is closed under subtraction. (c) State, with reasoning, whether $\mathbb{Q}$ is closed under division by a non-zero rational.

Working	Comment
$12 \in \mathbb{N}$; $-8 \in \mathbb{Z}$.	12 is a counting number; -8 is a negative integer, not natural.
$7/16 \in \mathbb{Q}$; $\sqrt{5} \in \mathbb{R}$.	$7/16$ is a ratio of integers; $\sqrt{5}$ is irrational, so real but not rational.
$4 - 3i \in \mathbb{C}$.	Its imaginary part is non-zero, so it is complex but not real.
(b) **Not** closed: $5, 12 \in \mathbb{N}$ but $5 - 12 = -7 \notin \mathbb{N}$.	One counterexample settles a closure claim as false.
(c) Closed: $\dfrac{p}{q} \div \dfrac{r}{s} = \dfrac{ps}{qr} \in \mathbb{Q}$ for $r \neq 0$.	The quotient is again a ratio of integers with non-zero denominator.

Example 3 — unscaffolded

Let $S = \{7, 9, 11\}$. Write down the power set $P(S)$, state $|P(S)|$ and confirm it equals 2^n, and give the number of proper subsets of S. Explain why $\{9\} \subseteq S$ is true but $9 \subseteq S$ is not.

A subset is formed by choosing, for each of the three elements, whether to include it. The eight resulting subsets are

$$P(S)=\{\quad,\{7\},\{9\},\{11\},\{7,9\},\{7,11\},\{9,11\},\{7,9,11\}\}.$$

Thus $|P(S)|=8$, and since S has $n=3$ elements this agrees with $2^n=2^3=8$. All of these except $S=\{7,9,11\}$ itself are proper subsets, so there are $2^3-1=7$ proper subsets. Finally, 9 is an *element* of S so $9\in S$, and the one-element *set* $\{9\}$ is a subset, so $\{9\}\subseteq S$; but "$9\subseteq S$" would treat the number 9 as a set of elements of S, which it is not.

$\therefore P(S)$ has $2^3=8$ members, of which 7 are proper subsets, and $9\in S$ while $\{9\}\subseteq S$.

Example 4 — unscaffolded

(a) Convert $13/25$ and $5/6$ to decimals, in each case using the denominator to say whether the decimal terminates or recurs. (b) Express the recurring decimal $0.\overline{54}$ as a fraction in lowest terms.

For (a), factorise each denominator in lowest terms. Since $25=5^2$ has only the prime 5, the fraction $13/25$ terminates, and dividing gives $13/25=0.52$. Since $6=2\times3$ contains the prime 3, the fraction $5/6$ recurs, and dividing gives $5/6=0.8333\ldots=0.8\overline{3}$.

For (b), let $x=0.\overline{54}$. The recurring block has two digits, so multiplying by 100 shifts exactly one block past the point:

$$100x=54.\overline{54},\ 100x-x=54.\overline{54}-0.\overline{54}=54,$$

so $99x=54$ and $x=\dfrac{54}{99}=\dfrac{6}{11}$ after dividing numerator and denominator by 9.

$\therefore 13/25=0.52$ (terminating), $5/6=0.8\overline{3}$ (recurring), and $0.\overline{54}=6/11$.

Practice questions

Scaffolded

Q1. Let $\xi=\{n\in\mathbb{Z}:11\le n\le20\}$, $A=\{12,15,16,19\}$ and $B=\{11,15,17,19,20\}$. (a) State whether $15\in A$ and whether $17\in A$, and write down $|B|$. (b) Find $A\cup B$. (c) Find $A\cap B$. (d) Find A^c. (e) Find $B\setminus A$.

Q2. With universal set $\xi=\{1,2,3,\ldots,10\}$, let $C=\{x\in\xi:x\text{ is even}\}$ and $D=\{x\in\xi:x\le5\}$. (a) List the elements of C and of D. (b) Find $C\cap D$. (c) Find $C\cup D$. (d) State whether $D\subseteq\xi$, whether $C\subseteq D$, and whether $\{2,4\}\subset C$. (e) Find $C\setminus D$ and state $|C\setminus D|$.

Q3. Let $S=\{2,6,13\}$. (a) Write down all the subsets of S. (b) State $|P(S)|$ and confirm it equals 2^n for the appropriate n. (c) How many proper subsets does S have? (d) State whether $\quad\in P(S)$, whether $\{6\}\subseteq S$, and whether $6\subseteq S$.

Q4. Consider the numbers -15, $9/4$, $\sqrt{7}$ and 6. (a) For each, name the smallest of $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R}$ to which it belongs. (b) State whether $\mathbb{Z}$ is closed under multiplication, and whether it is closed under division, giving a counterexample for whichever fails. (c) Write down one rational number and one irrational number, each lying between 3 and 4.

Q5. For each fraction, give its decimal form and state, with a reason based on the denominator, whether it terminates or recurs. (a) $7/16$. (b) $11/20$. (c) $5/12$. (d) $4/9$.

Q6. Convert the recurring decimal $0.\overline{81}$ to a fraction in lowest terms. (a) Let $x=0.\overline{81}$ and write down $100x$. (b) Subtract x from $100x$ to remove the recurring tail. (c) Solve the resulting equation for x. (d) Simplify your answer to lowest terms.

Unscaffolded

Q7. With $\xi=\{1,2,3,\ldots,12\}$, let $G=\{1,2,3,4,5,6\}$, $H=\{4,5,6,7,8\}$ and $K=\{2,4,6,8,10\}$. Find $G\cap H\cap K$, $G\cup H\cup K$ and $(G\cap H)^c$.

Q8. With $\xi=\{1,2,3,\ldots,20\}$, let $M=\{x\in\xi : x \text{ is a multiple of } 3\}$ and $W=\{x\in\xi : x \text{ is a multiple of } 4\}$. Find $M\cap W$ and $M\cup W$, and describe $M\cap W$ in words.

Q9. A set $T=\{2,4,6,8,10\}$ has five elements. (a) How many subsets does T have? (b) How many of these are proper subsets? (c) How many subsets of T contain the element 2? (d) How many subsets of T have exactly two elements?

Q10. A finite set A has power set of size $|P(A)|=64$. (a) Find $|A|$. (b) State the number of proper subsets of A. (c) How many subsets of A have the same number of elements as A itself?

Q11. Classify each of $\sqrt{49}$, $\sqrt{50}$, $0.\overline{6}$, π, $-22/7$ and $\sqrt[3]{27}$ as rational or irrational, and name the smallest of $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R}$ to which each belongs.

Q12. For each set and operation, state whether the set is closed under the operation; if not, give a counterexample. (a) The odd integers, under addition. (b) The irrational numbers, under multiplication. (c) The integers, under subtraction.

Q13. Without performing the division, state (with a reason from the denominator in lowest terms) whether each decimal terminates or recurs. (a) $17/80$. (b) $9/14$. (c) $13/125$. (d) $45/60$.

Q14. Express the recurring decimal $0.\overline{135}$ as a fraction in lowest terms.

Q15. Express the recurring decimal $0.4\overline{6}$ as a fraction in lowest terms.

Q16. (a) Express $2.\overline{45}$ as a fraction in lowest terms. (b) Hence, or by the same method, show that $0.\overline{9}=1$.

Q17. With $\xi=\{1,2,3,\ldots,9\}$, let $A=\{1,2,3,4,5\}$ and $B=\{4,5,6,7\}$. By computing both sides, verify De Morgan's law $(A\cup B)^c=A^c\cap B^c$.

Q18. Let $A=\{x\in\mathbb{Z} : x^2<20\}$. (a) List the elements of A and state $|A|$. (b) State $|P(A)|$. (c) Express $0.\overline{27}$ as a fraction in lowest terms and name the smallest number system to which it belongs.

Answers

Q1. (a) $15 \in A$ true, $17 \in A$ false, $|B| = 5$; (b) $\{11, 12, 15, 16, 17, 19, 20\}$; (c) $\{15, 19\}$; (d) $\{11, 13, 14, 17, 18, 20\}$; (e) $\{11, 17, 20\}$. **Q2.** (a) $C = \{2, 4, 6, 8, 10\}$, $D = \{1, 2, 3, 4, 5\}$; (b) $\{2, 4\}$; (c) $\{1, 2, 3, 4, 5, 6, 8, 10\}$; (d) $D \subseteq \xi$ true, $C \subseteq D$ false, $\{2, 4\} \subset C$ true; (e) $C \setminus D = \{6, 8, 10\}$, $|C \setminus D| = 3$. **Q3.** (a) $\varnothing, \{2\}, \{6\}, \{13\}, \{2, 6\}, \{2, 13\}, \{6, 13\}, \{2, 6, 13\}$; (b) $|P(S)| = 8 = 2^3$; (c) 7; (d) $\varnothing \in P(S)$ true, $\{6\} \subseteq S$ true, $6 \subseteq S$ false. **Q4.** (a) $-15 \in \mathbb{Z}$, $9/4 \in \mathbb{Q}$, $\sqrt{7} \in \mathbb{R}$, $6 \in \mathbb{N}$; (b) closed under multiplication; not under division, e.g. $5 \div 2 = 5/2 \notin \mathbb{Z}$; (c) e.g. rational $7/2$, irrational $\sqrt{10}$. **Q5.** (a) 0.4375, terminates; (b) 0.55, terminates; (c) $0.41\overline{6}$, recurs; (d) $0.\overline{4}$, recurs. **Q6.** $x = 81/99 = 9/11$. **Q7.** $G \cap H \cap K = \{4, 6\}$; $G \cup H \cup K = \{1, 2, 3, 4, 5, 6, 7, 8, 10\}$; $(G \cap H)^c = \{1, 2, 3, 7, 8, 9, 10, 11, 12\}$. **Q8.** $M \cap W = \{12\}$; $M \cup W = \{3, 4, 6, 8, 9, 12, 15, 16, 18, 20\}$; $M \cap W$ is the multiples of 12 in ξ. **Q9.** (a) 32; (b) 31; (c) 16; (d) 10. **Q10.** (a) $|A| = 6$; (b) 63; (c) 1. **Q11.** $\sqrt{49} = 7$ rational, $\mathbb{N}$; $\sqrt{50}$ irrational, $\mathbb{R}$; $0.\overline{6} = 2/3$ rational, $\mathbb{Q}$; π irrational, $\mathbb{R}$; $-22/7$ rational, $\mathbb{Q}$; $\sqrt[3]{27} = 3$ rational, $\mathbb{N}$. **Q12.** (a) not closed, e.g. $3 + 5 = 8$ is even; (b) not closed, e.g. $\sqrt{2} \times \sqrt{2} = 2$ is rational; (c) closed. **Q13.** (a) terminates ($80 = 2^4 \times 5$); (b) recurs ($14 = 2 \times 7$); (c) terminates ($125 = 5^3$); (d) terminates ($45/60 = 3/4$, $4 = 2^2$). **Q14.** $0.\overline{135} = 135/999 = 5/37$. **Q15.** $0.4\overline{6} = 42/90 = 7/15$. **Q16.** (a) $2.\overline{45} = 243/99 = 27/11$; (b) $0.\overline{9} = 9/9 = 1$. **Q17.** $(A \cup B)^c = \{8, 9\}$ and $A^c \cap B^c = \{8, 9\}$, which are equal. **Q18.** (a) $A = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$, $|A| = 9$; (b) $|P(A)| = 2^9 = 512$; (c) $0.\overline{27} = 27/99 = 3/11 \in \mathbb{Q}$.

Fully-worked solutions

Q1. The universal set is $\xi = \{11, 12, 13, 14, 15, 16, 17, 18, 19, 20\}$. (a) 15 is listed in A, so $15 \in A$ is true; 17 is not listed, so $17 \in A$ is false; B has the five members $11, 15, 17, 19, 20$, so $|B| = 5$. (b) Collecting every element in A or B, $A \cup B = \{11, 12, 15, 16, 17, 19, 20\}$. (c) The elements in both are $A \cap B = \{15, 19\}$. (d) Removing the members of A from ξ, $A^c = \{11, 13, 14, 17, 18, 20\}$. (e) Removing from B those elements also in A (namely 15 and 19), $B \setminus A = \{11, 17, 20\}$.

Q2. (a) The even members of $\{1, \ldots, 10\}$ are $C = \{2, 4, 6, 8, 10\}$, and those at most 5 are $D = \{1, 2, 3, 4, 5\}$. (b) The common elements are $C \cap D = \{2, 4\}$. (c) Their union is $C \cup D = \{1, 2, 3, 4, 5, 6, 8, 10\}$. (d) Every element of D lies in ξ, so $D \subseteq \xi$ is true; $6 \in C$ but $6 \notin D$, so $C \subseteq D$ is false; both 2 and 4 lie in C and $\{2, 4\} \neq C$, so $\{2, 4\} \subset C$ is true. (e) The members of C not in D are $C \setminus D = \{6, 8, 10\}$, so $|C \setminus D| = 3$.

Q3. (a) Choosing independently whether to include each of $2, 6, 13$ gives the eight subsets

$$\varnothing, \{2\}, \{6\}, \{13\}, \{2, 6\}, \{2, 13\}, \{6, 13\}, \{2, 6, 13\}.$$

(b) Hence $|P(S)| = 8$, and as S has $n = 3$ elements this matches $2^n = 2^3 = 8$. (c) Every subset except S itself is proper, giving $8 - 1 = 7$ proper subsets. (d) $\varnothing$ is a subset of every set, so $\varnothing \in P(S)$ is true; $\{6\}$ is a one-element subset, so $\{6\} \subseteq S$ is true; but 6 is a number, not a set of elements of S, so $6 \subseteq S$ is false (the correct statement is $6 \in S$).

Q4. (a) -15 is a negative integer, so its smallest system is $\mathbb{Z}$; $9/4$ is a non-integer ratio, so $\mathbb{Q}$; $\sqrt{7}$ is irrational, so $\mathbb{R}$; and 6 is a counting number, so $\mathbb{N}$. (b) A product of two integers is an integer, so $\mathbb{Z}$ is closed under multiplication; but $5 \div 2 = 5/2 \notin \mathbb{Z}$, so it is not closed under division. (c) For example $7/2 = 3.5$ is rational and lies between 3 and 4, while $\sqrt{10} \approx 3.162$ is irrational and lies between 3 and 4 (since $9 < 10 < 16$).

Q5. (a) $16 = 2^4$ has only the prime 2, so $7/16$ terminates; $7/16 = 0.4375$. (b) $20 = 2^2 \times 5$ has only 2 and 5, so $11/20$ terminates; $11/20 = 0.55$. (c) $12 = 2^2 \times 3$ contains the prime 3, so $5/12$ recurs; $5/12 = 0.41666\ldots = 0.41\overline{6}$. (d) $9 = 3^2$ contains the prime 3, so $4/9$ recurs; $4/9 = 0.4444\ldots = 0.\overline{4}$.

Q6. (a) With $x = 0.\overline{81}$ the block has two digits, so $100x = 81.\overline{81}$. (b) Subtracting, $100x - x = 81.\overline{81} - 0.\overline{81} = 81$, that is $99x = 81$. (c) Solving, $x = 81/99$. (d) Dividing numerator and denominator by 9, $x = 9/11$.

Q7. First $G \cap H = \{4,5,6\}$, and intersecting with $K = \{2,4,6,8,10\}$ leaves $G \cap H \cap K = \{4,6\}$. The union of all three is $G \cup H \cup K = \{1,2,3,4,5,6,7,8,10\}$ (only $9, 11, 12$ of ξ are missing). Finally $G \cap H = \{4,5,6\}$, so its complement in ξ is $(G \cap H)^c = \{1,2,3,7,8,9,10,11,12\}$.

Q8. The multiples of 3 up to 20 are $M = \{3,6,9,12,15,18\}$ and the multiples of 4 are $W = \{4,8,12,16,20\}$. Their intersection is $M \cap W = \{12\}$, and their union is $M \cup W = \{3,4,6,8,9,12,15,16,18,20\}$. A number lies in $M \cap W$ exactly when it is a multiple of both 3 and 4, that is a multiple of 12; the only one in ξ is 12.

Q9. (a) A five-element set has $2^5 = 32$ subsets. (b) All but the whole set are proper, giving $32 - 1 = 31$. (c) Fixing 2 as included, the other four elements are each free to be in or out, giving $2^4 = 16$ subsets that contain 2. (d) The number of two-element subsets is the number of ways to choose 2 of the 5 elements, $\binom{5}{2} = 10$.

Q10. (a) Since $|P(A)| = 2^{|A|} = 64 = 2^6$, we have $|A| = 6$. (b) All but A itself are proper subsets, so there are $64 - 1 = 63$. (c) The only subset of A with as many elements as A is A itself, so there is exactly 1.

Q11. $\sqrt{49} = 7$ is rational, smallest system $\mathbb{N}$. $\sqrt{50} = 5\sqrt{2}$ is irrational (as 50 is not a perfect square), smallest system $\mathbb{R}$. $0.\overline{6} = 2/3$ is a recurring decimal, hence rational, smallest system $\mathbb{Q}$. π is irrational, smallest system $\mathbb{R}$. $-22/7$ is a ratio of integers, hence rational, smallest system $\mathbb{Q}$ (note it only approximates π; it is not equal to it). $\sqrt[3]{27} = 3$ is rational, smallest system $\mathbb{N}$.

Q12. (a) Not closed: 3 and 5 are odd but $3 + 5 = 8$ is even, so a sum of two odd integers need not be odd. (b) Not closed: $\sqrt{2}$ is irrational but $\sqrt{2} \times \sqrt{2} = 2$ is rational. (c) Closed: the difference of two integers is always an integer.

Q13. Reduce each to lowest terms and factorise the denominator. (a) $80 = 2^4 \times 5$ uses only 2 and 5, so $17/80$ terminates. (b) $14 = 2 \times 7$ contains the prime 7, so $9/14$ recurs. (c) $125 = 5^3$ uses only 5, so $13/125$ terminates. (d) $45/60$ is not in lowest terms; cancelling 15 gives $45/60 = 3/4$ with $4 = 2^2$, so it terminates (the apparent factor 3 disappears).

Q14. Let $x = 0.\overline{135}$. The recurring block has three digits, so $1000x = 135.\overline{135}$. Subtracting, $1000x - x = 135$, that is $999x = 135$, so

$$x = \frac{135}{999} = \frac{5}{37}$$

after dividing numerator and denominator by 27.

Q15. Here one digit precedes the recurring block, so let $x = 0.4\overline{6}$. Then $10x = 4.\overline{6}$ and $100x = 46.\overline{6}$. Subtracting the first from the second cancels the tail: $100x - 10x = 46.\overline{6} - 4.\overline{6} = 42$, so $90x = 42$ and

$$x = \frac{42}{90} = \frac{7}{15}.$$

Q16. (a) Let $x = 2.\overline{45}$. The block has two digits, so $100x = 245.\overline{45}$, and $100x - x = 245.\overline{45} - 2.\overline{45} = 243$, that is $99x = 243$. Hence $x = 243/99 = 27/11$ (dividing by 9). (b) Let $y = 0.\overline{9}$. Then $10y = 9.\overline{9}$ and $10y - y = 9.\overline{9} - 0.\overline{9} = 9$, so $9y = 9$ and $y = 1$. Thus the recurring decimal $0.\overline{9}$ is exactly equal to 1.

Q17. The union is $A \cup B = \{1,2,3,4,5,6,7\}$, so its complement in $\xi = \{1,\ldots,9\}$ is $(A \cup B)^c = \{8,9\}$. Separately, $A^c = \{6,7,8,9\}$ and $B^c = \{1,2,3,8,9\}$, so $A^c \cap B^c = \{8,9\}$. The two results are equal, confirming $(A \cup B)^c = A^c \cap B^c$ for these sets.

Q18. (a) The integers with $x^2 < 20$ satisfy $-\sqrt{20} < x < \sqrt{20}$, and since $4^2 = 16 < 20 < 25 = 5^2$ the largest is 4; thus $A = \{-4,-3,-2,-1,0,1,2,3,4\}$ and $|A| = 9$. (b) A nine-element set has $|P(A)| = 2^9 = 512$ subsets. (c) Let $x = 0.\overline{27}$; then $100x = 27.\overline{27}$ and $99x = 27$, so $x = 27/99 = 3/11$, a ratio of integers, whose smallest number system is $\mathbb{Q}$.

Chapter 1 Proof and number — 1B Direct proof, cases, contradiction and contrapositive

Theory

Mathematics advances by **proof**: a proof is a chain of logically valid steps that establishes a statement beyond doubt, each step justified by a definition or by a result already proved. This section develops the standard machinery of proof — the language of statements and quantifiers, and the four workhorse methods (direct proof, proof by cases, proof by contradiction, and proof using the contrapositive) — applied to simple results about parity, divisibility and number.

Statements and propositions.

A **statement** (or **proposition**) is a sentence that is either true or false, but never both. "17 is prime" is a true statement and "21 is prime" is a false one. An open sentence such as "n is a multiple of 4" is not itself a statement, because its truth depends on n; it becomes a statement only once n is fixed, or once it is placed under a quantifier. Writing $\neg P$ for the **negation** of a statement P ("not P"), exactly one of P and $\neg P$ is true.

Quantifiers.

Two **quantifiers** turn an open sentence into a statement. The **universal quantifier** $\forall$ (read "for all") asserts that a property holds in every case: $\forall n \in \mathbb{Z}, n^2 \geq 0$ says that the square of every integer is non-negative. The **existential quantifier** $\exists$ (read "there exists") asserts that a property holds in at least one case: $\exists n \in \mathbb{Z}, n^2 = 49$ says that some integer squares to 49. Negating a quantified statement swaps the quantifier and negates the inside:

$$\neg\big(\forall n, P(n)\big) \equiv \exists n, \neg P(n), \quad \neg\big(\exists n, P(n)\big) \equiv \forall n, \neg P(n).$$

So the negation of "every integer has property P" is "some integer fails P", and the negation of "some integer has property P" is "no integer has property P".

Implications, converse and contrapositive.

Most theorems are **implications** $P \Rightarrow Q$, read "if P then Q". Here P is the **hypothesis** and Q the **conclusion**; the implication claims only that whenever P holds, Q holds too, and says nothing when P is false. Three related statements are named:

- the **converse** $Q \Rightarrow P$ (hypothesis and conclusion swapped);
- the **contrapositive** $\neg Q \Rightarrow \neg P$ (both negated and swapped);
- the **negation** of the implication, which asserts that P is true while Q is false.

A statement and its **contrapositive** are **logically equivalent** — one is true exactly when the other is — while a statement and its converse are not. This equivalence is the foundation of proof by contrapositive. Note that the negation of $\forall n, \big(P(n) \Rightarrow Q(n)\big)$ is $\exists n, \big(P(n) \text{ true and } Q(n) \text{ false}\big)$: a single instance where the hypothesis holds but the conclusion fails destroys a universal implication.

Definitions used throughout.

Proof depends on stating definitions precisely. For integers a, b and n:

- n is **even** if $n = 2k$ for some integer k, and **odd** if $n = 2k+1$ for some integer k; every integer is exactly one of the two.
- a **divides** b, written $a \mid b$, if $b = ak$ for some integer k; we then call a a **factor** of b and b a multiple of a.
- a real number is **rational** if it equals $\dfrac{p}{q}$ for integers p, q with $q \neq 0$, and **irrational** otherwise.

A useful refinement of parity is division with remainder: every integer n can be written $n = 3k$, $n = 3k+1$ or $n = 3k+2$ according to its **remainder** (or **residue**) on division by 3, and similarly for any other divisor. These residue forms are what make proof by cases work.

Direct proof.

A **direct proof** of $P \Rightarrow Q$ assumes P and reaches Q by a chain of valid steps

$$P \Rightarrow R_1 \Rightarrow R_2 \Rightarrow \cdots \Rightarrow Q,$$

each link justified by a definition, an algebraic manipulation or an earlier result. To prove a parity or divisibility result directly, one typically substitutes the defining form ($2k$, $2k+1$, ak, and so on), manipulates algebraically, and recognises the target form at the end.

Proof by cases.

When no single argument covers every possibility, split the situation into a finite list of **cases** that together **exhaust** all possibilities, and prove the conclusion in each. A common split is by parity (n even or odd), and a finer one is by residue modulo 3, 4 or 5. Because the cases leave nothing out, establishing the conclusion in every case establishes it in general. The cases must genuinely cover all possibilities, or the proof has a gap.

Proof by contradiction.

To prove a statement S by **contradiction**, assume instead that S is *false* and reason until two conclusions collide — some statement is forced to be both true and false, or an established fact is violated. Since correct reasoning cannot produce an impossibility, the assumption must have been wrong, so S is true. Contradiction is the natural tool for proving that something *cannot* happen — that a number is irrational, or that no integer solution exists.

Proof using the contrapositive.

Because $P \Rightarrow Q$ and its contrapositive $\neg Q \Rightarrow \neg P$ are logically equivalent, either may be proved in place of the other. The contrapositive is the better target whenever negating the conclusion gives a more concrete starting point than the hypothesis. For instance "if n^2 is a multiple of 5 then n is a multiple of 5" is awkward head-on, but its contrapositive "if n is not a multiple of 5 then n^2 is not a multiple of 5" yields to a short check of residues.

Counterexamples.

To **disprove** a universal statement $\forall n, P(n)$ it is enough to produce a single **counterexample** — one value of n for which $P(n)$ is false — because that single instance verifies the negation $\exists n, \neg P(n)$. Consider the claim "every odd integer greater than 1 is prime". The value $n = 9$ is odd and greater than 1, yet $9 = 3 \times 3$ is not prime, so $n = 9$ is a counterexample and the claim is false. One counterexample settles the matter; no amount of confirming cases can rescue a false universal. By contrast, an existential statement $\exists n, P(n)$ is *proved* by exhibiting one value that works.

Choosing a technique.

Attempt a direct proof first. If the hypothesis is hard to use but the negated conclusion is concrete, switch to the contrapositive. If assuming the statement false gives a firm foothold — a fraction in lowest terms, or a supposed integer solution — use contradiction. If the integers behave differently according to their parity or residue, split into cases. To disprove a universal claim, hunt for a counterexample. Whichever route is taken, every proof should close with a sentence stating that the required result has been reached.

Worked examples

Example 1 — scaffolded

Prove that for every integer n, the sum of the squares of two consecutive integers, $n^2 + (n+1)^2$, is odd.

Working	Comment
Let n be any integer; the next consecutive integer is $n+1$.	A direct proof: work with a general integer n.
$n^2 + (n+1)^2 = n^2 + n^2 + 2n + 1 = 2n^2 + 2n + 1.$	Expand $(n+1)^2$ and collect like terms.

Working	Comment
$=2(n^2+n)+1.$	Factor 2 from the first two terms to expose the form $2(\text{integer})+1.$
Since n^2+n is an integer, $2(n^2+n)+1$ is odd.	This matches the definition of an odd number.
Hence $n^2+(n+1)^2$ is odd, as required.	Concluding sentence.

Example 2 — scaffolded

Prove that for every integer n, the number n^2+2 is not divisible by 4.

Working	Comment
Every integer is even or odd, so $n=2k$ or $n=2k+1$ for some integer k.	The two parity cases exhaust all integers.
Case $n=2k$: $n^2+2=4k^2+2=4(k^2)+2.$	Substitute; this is 2 more than a multiple of 4, so the remainder is 2.
Case $n=2k+1$: $n^2+2=4k^2+4k+1+2=4(k^2+k)+3.$	Expand and regroup; this is 3 more than a multiple of 4, remainder 3.
In both cases the remainder on division by 4 is 2 or 3, never 0.	Neither case produces a multiple of 4.
Since the two cases cover every integer, 4 does not divide n^2+2, as required.	The cases are exhaustive; concluding sentence.

Example 3 — unscaffolded

Prove that there are no integers x and y satisfying $x^2-y^2=10$.

Suppose, for the sake of contradiction, that there are integers x and y with $x^2-y^2=10$. Factorising the left-hand side,

$$(x-y)(x+y)=10.$$

The two factors have the same parity, because their difference $(x+y)-(x-y)=2y$ is even; so either both are odd or both are even, and there is no third possibility. If both factors are odd, then their product is odd, yet 10 is even — impossible. If both factors are even, write $x-y=2a$ and $x+y=2b$ for some integers a and b; then $10=2a\times 2b=4ab$, so 10 would be a multiple of 4, and it is not. Both cases are impossible, so the assumption was false. Therefore no integers x and y satisfy $x^2-y^2=10$, as required.

Example 4 — unscaffolded

Prove that for every integer n, if n^2-6n+5 is even then n is odd.

We prove the logically equivalent contrapositive: if n is even, then n^2-6n+5 is odd. Assume n is even, so $n=2k$ for some integer k. Then

$$n^2-6n+5=4k^2-12k+5=2(2k^2-6k+2)+1,$$

which has the form $2(\text{integer})+1$ and so is odd. This proves the contrapositive; since a statement and its contrapositive are logically equivalent, the original statement follows: if n^2-6n+5 is even, then n is odd, as required.

Practice questions

Scaffolded

Q1. Prove that if m is an odd integer and n is an even integer, then $m+n$ is odd. (a) Using the definitions, write $m=2s+1$ and $n=2t$. (b) Add and simplify $m+n$. (c) Exhibit the form $2(\text{integer})+1$ and state the conclusion.

Q2. Let a, b, c be integers. Prove that if $a \mid b$ and $a \mid c$, then $a \mid (5b-2c)$. (a) Use the definition of "divides" to write $b=as$ and $c=at$. (b) Form $5b-2c$ and factor out a. (c) State why $a \mid (5b-2c)$.

Q3. Prove that for every integer n, exactly one of the three integers n, $n+2$, $n+4$ is divisible by 3. (a) Write n in the residue form $3k$, $3k+1$ or $3k+2$. (b) In each case determine which of n, $n+2$, $n+4$ is a multiple of 3, and check the other two are not. (c) Conclude that exactly one is divisible by 3.

Q4. Prove that for every integer n, the number n^2+n+1 is odd. (a) Split into the cases n even and n odd. (b) In each case substitute and factor out 2. (c) Conclude that n^2+n+1 is odd in both cases.

Q5. Prove that there is no smallest positive rational number. (a) Assume for contradiction that r is the smallest positive rational number. (b) Consider $\frac{r}{2}$ and explain why it is also a positive rational number. (c) Compare $\frac{r}{2}$ with r, state the contradiction, and conclude.

Q6. Prove that for every integer n, if $3n+2$ is even then n is even. (a) State the contrapositive of the implication. (b) Prove the contrapositive by a direct argument. (c) Conclude the original statement.

Unscaffolded

Q7. Prove that the sum of any three consecutive integers is divisible by 3.

Q8. Prove that the product of two consecutive even integers is divisible by 8.

Q9. Let a and b be integers. Prove that if $a \mid b$, then $a \mid (b^3+4b)$.

Q10. Consider the statement "every prime number is odd". (a) Write the statement using a quantifier. (b) Write its negation using a quantifier. (c) Decide whether the statement is true or false, proving your answer.

Q11. Disprove the statement: "for every positive integer n, the number n^2-n+11 is prime."

Q12. Disprove the statement: "for every prime number p, the number 2^p-1 is prime."

Q13. Prove that for all integers m and n, the number $mn(m+n)$ is even.

Q14. Prove that for every integer n, the number n^2+n+1 is never divisible by 5.

Q15. Prove that for every integer n, if n^3-1 is even then n is odd.

Q16. Prove that for every integer n, if n^2 is divisible by 7 then n is divisible by 7.

Q17. Prove that there are no integers x and y satisfying $4x+6y=2025$.

Q18. Prove that $\log_3 7$ is irrational.

Answers

Q1. Proof — $m+n=2(s+t)+1$, which is odd. See solutions. **Q2.** Proof — $5b-2c=a(5s-2t)$. See solutions. **Q3.** Proof by cases (residues mod 3) — exactly one of n, $n+2$, $n+4$ is a multiple of 3. See solutions. **Q4.** Proof by cases — even: $n^2+n+1=2(2k^2+k)+1$; odd: $=2(2k^2+3k+1)+1$. See solutions. **Q5.** Proof by contradiction — $\frac{r}{2}$ is a positive rational smaller than r. See solutions. **Q6.** Contrapositive "if n is odd then $3n+2$ is odd". See solutions. **Q7.** Proof — sum $=3(n+1)$. See solutions. **Q8.** Proof — product $=4k(k+1)=8j$, since $k(k+1)$ is even. See solutions. **Q9.** Proof — $b^3+4b=a(a^2s^3+4s)$. See solutions. **Q10.** (a) $\forall n(n \text{ prime} \Rightarrow n \text{ odd})$; (b) $\exists n(n \text{ prime and } n \text{ even})$; (c) false — counterexample $n=2$ (prime and even). See solutions. **Q11.** False; counterexample $n=11$: $11^2-11+11=121=11^2$, not prime. See solutions. **Q12.** False; counterexample $p=11$: $2^{11}-1=2047=23\times 89$, not prime. See solutions. **Q13.** Proof by cases (parity) — if m or n is even the product is even; if both are odd then $m+n$ is even. See solutions. **Q14.** Proof by cases (residues mod 5) — n^2+n+1 has residue $1, 3, 2, 3$ or 1, never 0. See solutions. **Q15.** Contrapositive "if n is even then n^3-1 is odd". See solutions. **Q16.** Contrapositive "if 7 does not divide n then 7 does not divide n^2". See solutions. **Q17.** Proof by contradiction — $4x+6y$ is even, but 2025 is odd. See solutions. **Q18.** Proof by contradiction — $3^p=7^q$ forces $7 \mid 3^p$, which is impossible. See solutions.

Fully-worked solutions

Q1. Assume m is odd and n is even. By definition $m=2s+1$ and $n=2t$ for some integers s, t. Adding,

$$m+n=(2s+1)+2t=2(s+t)+1.$$

Since $s+t$ is an integer, $m+n$ has the form $2(\text{integer})+1$ and so is odd, as required.

Q2. Assume $a \mid b$ and $a \mid c$. By the definition of "divides", $b=as$ and $c=at$ for some integers s, t. Then

$$5b-2c=5as-2at=a(5s-2t),$$

and $5s-2t$ is an integer, so $a \mid (5b-2c)$, as required.

Q3. Every integer is $n=3k$, $n=3k+1$ or $n=3k+2$ for some integer k.

- $n=3k$: here $n=3k$ is a multiple of 3; $n+2=3k+2$ and $n+4=3(k+1)+1$ leave remainders 2 and 1, so neither is.
- $n=3k+1$: here $n+2=3(k+1)$ is a multiple of 3; $n=3k+1$ and $n+4=3(k+1)+2$ leave remainders 1 and 2, so neither is.
- $n=3k+2$: here $n+4=3(k+2)$ is a multiple of 3; $n=3k+2$ and $n+2=3(k+1)+1$ leave remainders 2 and 1, so neither is.

In every case exactly one of n, $n+2$, $n+4$ is divisible by 3. Since the three cases exhaust all integers, the result holds for every integer n. This completes the proof.

Q4. Split by parity. Case n even, $n=2k$: $n^2+n+1=4k^2+2k+1=2(2k^2+k)+1$, which is odd. Case n odd, $n=2k+1$: $n^2+n+1=(4k^2+4k+1)+(2k+1)+1=4k^2+6k+3=2(2k^2+3k+1)+1$, which is odd. In both cases n^2+n+1 has the form $2(\text{integer})+1$, so it is odd for every integer n. This completes the proof.

Q5. Suppose, for contradiction, that there is a smallest positive rational number r. Consider $\frac{r}{2}$. Writing $r=\frac{p}{q}$ with integers p, q and $q \neq 0$, we have $\frac{r}{2}=\frac{p}{2q}$, again a ratio of integers with non-zero denominator, so $\frac{r}{2}$ is rational. Since $r>0$, also $\frac{r}{2}>0$, and

$$\frac{r}{2} < r.$$

Thus $\frac{r}{2}$ is a positive rational number strictly smaller than r, contradicting the assumption that r was the smallest. Therefore there is no smallest positive rational number, as required.

Q6. The contrapositive of "if $3n+2$ is even then n is even" is "if n is odd then $3n+2$ is odd". Assume n is odd, so $n = 2k+1$ for some integer k. Then

$$3n+2 = 3(2k+1)+2 = 6k+5 = 2(3k+2)+1,$$

which is odd. This proves the contrapositive, so the original statement holds: if $3n+2$ is even then n is even. Hence the result holds.

Q7. Let the three consecutive integers be n, $n+1$ and $n+2$. Their sum is

$$n+(n+1)+(n+2) = 3n+3 = 3(n+1),$$

and $n+1$ is an integer, so the sum is divisible by 3, as required.

Q8. Two consecutive even integers may be written $2k$ and $2k+2$ for some integer k. Their product is

$$2k(2k+2) = 4k(k+1).$$

Among the consecutive integers k and $k+1$ one is even, so their product $k(k+1)$ is even; write $k(k+1) = 2j$ for some integer j. Then the product is $4 \times 2j = 8j$, so it is divisible by 8, as required.

Q9. Assume $a \mid b$, so $b = as$ for some integer s. Then

$$b^3 + 4b = (as)^3 + 4(as) = a^3 s^3 + 4as = a(a^2 s^3 + 4s),$$

and $a^2 s^3 + 4s$ is an integer, so $a \mid (b^3 + 4b)$, as required.

Q10. (a) In symbols the statement is $\forall n(n \text{ is prime} \Rightarrow n \text{ is odd})$. (b) Its negation is $\exists n(n \text{ is prime and } n \text{ is even})$. (c) The statement is **false**. The integer $n = 2$ is prime, since its only positive factors are 1 and 2, yet $2 = 2 \times 1$ is even. Thus $n = 2$ satisfies the negation in part (b), and a single counterexample disproves the universal statement. Hence not every prime is odd, as required.

Q11. The statement is false; one counterexample is enough. Take $n = 11$:

$$n^2 - n + 11 = 11^2 - 11 + 11 = 121 = 11 \times 11,$$

which is not prime. (The expression does happen to be prime for $n = 1, 2, \ldots, 10$, which is why the claim looks plausible, but $n = 11$ breaks it.) Therefore the statement is false, as required.

Q12. The statement is false; one counterexample suffices. The number $p = 11$ is prime, yet

$$2^{11} - 1 = 2047 = 23 \times 89$$

is a product of two integers each greater than 1, so it is not prime. Therefore the statement is false, as required.

Q13. Let m and n be integers, and split into cases according to their parities.

- m even, say $m = 2s$: then $mn(m+n) = 2sn(m+n) = 2(sn(m+n))$.
- n even, say $n = 2t$: then $mn(m+n) = 2mt(m+n) = 2(mt(m+n))$.
- m and n both odd, say $m = 2s+1$ and $n = 2t+1$: then $m+n = 2s+2t+2 = 2(s+t+1)$, so $mn(m+n) = 2(mn(s+t+1))$.

In each case $mn(m+n)$ has the form $2\times(\text{integer})$ and so is even. Every pair of integers m, n falls into at least one of the three cases — if neither m nor n is even, both are odd — so $mn(m+n)$ is even for all integers m and n. This completes the proof.

Q14. Write $n=5k+r$, where $r\in\{0,1,2,3,4\}$ is the remainder of n on division by 5. Expanding, $n^2+n+1=25k^2+10kr+r^2+5k+r+1$, and every term except r^2+r+1 is a multiple of 5; hence n^2+n+1 and r^2+r+1 leave the same remainder on division by 5. Evaluating r^2+r+1 for the five residues gives

$$1,3,7,13,21,$$

with remainders $1, 3, 2, 3, 1$ on division by 5 — none equal to 0. Since the five residues exhaust all integers, n^2+n+1 is never divisible by 5. This completes the proof.

Q15. We prove the contrapositive: if n is even then n^3-1 is odd. Assume n is even, so $n=2k$ for some integer k. Then

$$n^3-1=8k^3-1=2(4k^3-1)+1,$$

which has the form $2(\text{integer})+1$ and so is odd. This proves the contrapositive, so the original statement holds: if n^3-1 is even then n is odd. Hence the result holds.

Q16. We prove the contrapositive: if 7 does not divide n, then 7 does not divide n^2. Assume 7 does not divide n; then n leaves remainder $1, 2, 3, 4, 5$ or 6 on division by 7, so $n=7k+r$ with $r\in\{1,2,3,4,5,6\}$. Since $n^2=49k^2+14kr+r^2$ has the same remainder as r^2 on division by 7, and the six values $r^2=1,4,9,16,25,36$ leave remainders $1, 4, 2, 2, 4, 1$ — none zero — the number n^2 is not divisible by 7. This proves the contrapositive, so the original statement holds: if $7\mid n^2$ then $7\mid n$. Hence the result holds.

Q17. Suppose, for contradiction, that there are integers x and y with $4x+6y=2025$. The left-hand side factors as

$$4x+6y=2(2x+3y),$$

which is even, being twice the integer $2x+3y$. But 2025 is odd. An even number cannot equal an odd number, a contradiction. Therefore no such integers x and y exist, as required.

Q18. Suppose, for contradiction, that $\log_3 7$ is rational. Since $\log_3 7>0$, we may write $\log_3 7=\dfrac{p}{q}$ with p,q positive integers. Then $3^{p/q}=7$, and raising both sides to the power q,

$$3^p=7^q.$$

The right-hand side is divisible by 7, because $q\geq 1$. Hence $7\nmid 3^p$. But 7 is prime and does not divide 3, so 7 cannot divide any power of 3 — the only prime factor of 3^p is 3. This contradiction shows $\log_3 7$ cannot be rational, so $\log_3 7$ is irrational, as required.

Theory

Many results in mathematics are claims about **every** positive integer at once: a formula for the sum of the first n terms of a series, a statement that some fixed number divides an expression for all n, or an inequality that is supposed to hold from a certain point onward. Testing such a claim at $n=1,2,3,\ldots$ can make it *look* certain, yet no finite amount of checking can settle a statement about infinitely many integers — the very next case might be the one that fails. **Proof by mathematical induction** is the method that converts this kind of evidence into a genuine proof.

The ladder picture.

Picture an infinitely tall ladder. Suppose you know two facts: that you can reach the **bottom rung**, and that **from any rung you can always climb to the next one up**. Then, without testing each rung separately, you can be sure that **every** rung is reachable — the bottom rung gets you started, and the climbing rule carries you upward forever. Induction is exactly this argument made precise. Reaching the bottom rung is the **base case**; the rule "from any rung to the next" is an implication that passes the truth of one case on to the case immediately after it.

The principle of mathematical induction.

Let $P(n)$ be a statement depending on an integer n, and let n_0 be a fixed starting value (most often $n_0=1$). If

1. **(Base case)** $P(n_0)$ is true, and
2. **(Inductive step)** for every integer $k\geq n_0$, the truth of $P(k)$ forces the truth of $P(k+1)$ — that is, $P(k)\Rightarrow P(k+1)$,

then $P(n)$ is true for **all** integers $n\geq n_0$. The assumption "$P(k)$ is true", made at the start of the inductive step, is called the **inductive hypothesis**. It is a temporary supposition about a *single unspecified* value k, not a claim that has already been proved; its whole purpose is to be used in deriving $P(k+1)$.

The shape of every induction proof.

A well-set-out proof by induction has four clearly separated parts, and it is worth writing each of them explicitly.

- **Name the statement.** Begin "Let $P(n)$ be the statement …", so that $P(1)$, $P(k)$ and $P(k+1)$ each have a definite meaning.
- **Base case.** Substitute the smallest value $n=n_0$ into *both* sides and confirm the statement holds there. This must not be skipped: the inductive step on its own proves nothing at all.
- **Inductive step.** *Assume* $P(k)$ for some integer $k\geq n_0$, then *deduce* $P(k+1)$. The entire argument lives in getting from the hypothesis to $P(k+1)$, and it is good practice to mark the exact line at which the hypothesis is used.
- **Conclusion.** State that, since $P(n_0)$ holds and $P(k)\Rightarrow P(k+1)$, the principle of mathematical induction gives $P(n)$ for all integers $n\geq n_0$.

Application 1 — closed forms for a finite series.

Suppose $P(n)$ asserts that a partial sum $S_n=t_1+t_2+\ldots+t_n$ equals some closed expression in n. The single algebraic fact that drives every such proof is that the sum to $k+1$ terms is the sum to k terms with one extra term attached:

$$S_{k+1}=S_k+t_{k+1}.$$

In the inductive step you replace S_k by the formula (this is where the hypothesis is used), add the $(k+1)$-th term, and then **factorise and tidy the algebra until the result is exactly the formula with n replaced by $k+1$.** The standard sum of the first n positive integers,

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

is the model case; the sums $\sum r^2$ and $\sum r^3$ have closed forms proved the same way. A **geometric series** is handled identically: for a common ratio $q \neq 1$,

$$\sum_{r=1}^{n} a\,q^{r-1} = a\,\frac{q^n - 1}{q - 1}.$$

Throughout, the dummy index r counts the terms of the sum, while k is reserved for the integer fixed in the inductive step.

Application 2 — divisibility.

To prove that a fixed integer d divides an expression $f(n)$ for all $n \geq 1$ — written $d \mid f(n)$ — take $P(n)$ to be that divisibility statement. The base case checks that $f(n_0)$ is a multiple of d. For the step, assume $f(k)$ is divisible by d, and record this as $f(k) = d\,m$ for some **integer** m; it is usually convenient to rearrange this as an expression for the highest power in $f(k)$. The goal is then to show $f(k+1)$ is also a multiple of d, typically by writing

$$f(k+1) = (\text{a multiple of } d) + (\text{a multiple of } f(k)),$$

so that the hypothesis makes the whole thing divisible by d. Because m need only be an integer, keep it as a letter and never pin it to a particular value.

Application 3 — inequalities.

Induction also proves inequalities such as $2^n > 2n+1$ or $n! > 3^n$. Two features recur. First, the starting value n_0 is frequently **larger than** 1, because a small case may fail; the base case must be taken at the first value where the inequality genuinely holds. Second, the inductive step usually needs an **auxiliary inequality**: from $P(k)$ you reach some intermediate expression, and you must then argue separately that this intermediate expression is itself at least (or greater than) the target for $P(k+1)$. Chaining the two comparisons together completes the step. When the terms themselves are positive, the same idea bounds a running sum from above or below.

Worked examples

Example 1 — scaffolded

Use mathematical induction to prove that

$$\sum_{r=1}^{n} (4r - 3) = n(2n-1) \text{ for all integers } n \geq 1.$$

Let $P(n)$ be this statement and write $S_n = 1 + 5 + 9 + \ldots + (4n-3)$, so that $P(n)$ claims $S_n = n(2n-1)$.

Working	Comment
Base case $n=1$: $S_1 = 4(1) - 3 = 1$ and $1(2(1)-1) = 1$.	Substitute $n=1$ into both sides; they agree, so $P(1)$ is true.
Assume $S_k = k(2k-1)$ for some integer $k \geq 1$.	This is the inductive hypothesis — assume $P(k)$.
The $(k+1)$-th term is $4(k+1) - 3 = 4k+1$.	Put $r = k+1$ into $4r-3$.
$S_{k+1} = S_k + (4k+1) = k(2k-1) + (4k+1)$.	Add the next term; replace S_k using the hypothesis.
$= 2k^2 - k + 4k + 1 = 2k^2 + 3k + 1$.	Expand and collect like terms.
$= (k+1)(2k+1) = (k+1)(2(k+1)-1)$.	This is the formula with n replaced by $k+1$, namely $P(k+1)$.

Working	Comment
Hence $P(k)\Rightarrow P(k+1)$.	The inductive step is complete.

Since $P(1)$ is true and $P(k)\Rightarrow P(k+1)$ for every integer $k\geq 1$, by the principle of mathematical induction $S_n=n(2n-1)$ for all integers $n\geq 1$, as required.

Example 2 — scaffolded

Use mathematical induction to prove that 4^n+2 is divisible by 6 for all integers $n\geq 1$; that is, $6\mid 4^n+2$.

Let $P(n)$ be this statement and write $f(n)=4^n+2$.

Working	Comment
Base case $n=1$: $f(1)=4+2=6=6\times 1$.	A multiple of 6, so $P(1)$ is true.
Assume $f(k)=4^k+2=6m$ for some integer m, $k\geq 1$.	The inductive hypothesis; rearranged, $4^k=6m-2$.
$f(k+1)=4^{k+1}+2=4\cdot 4^k+2$.	Use $4^{k+1}=4\cdot 4^k$.
$=4(6m-2)+2=24m-6$.	Substitute $4^k=6m-2$ from the hypothesis.
$=6(4m-1)$.	Factor out 6; here $4m-1$ is an integer.
So $f(k+1)$ is a multiple of 6, i.e. $P(k)\Rightarrow P(k+1)$.	$P(k+1)$ holds.

Since $P(1)$ is true and $P(k)\Rightarrow P(k+1)$ for every integer $k\geq 1$, by the principle of mathematical induction $6\mid 4^n+2$ for all integers $n\geq 1$, as required.

Example 3 — unscaffolded

Use mathematical induction to prove that

$$\sum_{r=1}^{n} 3^{r-1}=\frac{3^n-1}{2} \text{ for all integers } n\geq 1.$$

Let $P(n)$ be this statement and write $S_n=1+3+9+\ldots+3^{n-1}$, the geometric series with first term 1 and common ratio 3; then $P(n)$ claims $S_n=\frac{3^n-1}{2}$.

Base case. For $n=1$, $S_1=3^0=1$ and $\frac{3^1-1}{2}=\frac{2}{2}=1$. The two sides agree, so $P(1)$ is true.

Inductive step. Assume $S_k=\frac{3^k-1}{2}$ for some integer $k\geq 1$. The $(k+1)$-th term is $3^{(k+1)-1}=3^k$, so

$$S_{k+1}=S_k+3^k=\frac{3^k-1}{2}+3^k=\frac{3^k-1+2\cdot 3^k}{2}=\frac{3\cdot 3^k-1}{2}=\frac{3^{k+1}-1}{2},$$

which is exactly the formula with n replaced by $k+1$, namely $P(k+1)$. Hence $P(k)\Rightarrow P(k+1)$.

Since $P(1)$ is true and $P(k)\Rightarrow P(k+1)$ for every integer $k\geq 1$, by the principle of mathematical induction $S_n=\frac{3^n-1}{2}$ for all integers $n\geq 1$, as required.

Example 4 — unscaffolded

Use mathematical induction to prove that

$$\sum_{r=1}^{n}\frac{1}{r^2}\le 2-\frac{1}{n}\text{ for all integers }n\ge 1.$$

Let $P(n)$ be this statement and write $S_n=1+\frac{1}{2^2}+\frac{1}{3^2}+\ldots+\frac{1}{n^2}$.

Base case. For $n=1$, $S_1=1$ and $2-\frac{1}{1}=1$, so $S_1\le 1$ (in fact equality). Thus $P(1)$ is true.

Inductive step. Assume $S_k\le 2-\frac{1}{k}$ for some integer $k\ge 1$. The $(k+1)$-th term is $\frac{1}{(k+1)^2}$, so adding it to both sides,

$$S_{k+1}=S_k+\frac{1}{(k+1)^2}\le 2-\frac{1}{k}+\frac{1}{(k+1)^2}.$$

It remains to show the right-hand side is at most $2-\frac{1}{k+1}$. Since

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

this amounts to checking $\frac{1}{(k+1)^2}\le\frac{1}{k(k+1)}$. Because $k+1>k>0$ we have $(k+1)^2>k(k+1)$, and taking reciprocals reverses the inequality to give exactly $\frac{1}{(k+1)^2}\le\frac{1}{k(k+1)}$. Therefore

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

which is $P(k+1)$. Hence $P(k)\Rightarrow P(k+1)$.

Since $P(1)$ is true and $P(k)\Rightarrow P(k+1)$ for every integer $k\ge 1$, by the principle of mathematical induction $S_n\le 2-\frac{1}{n}$ for all integers $n\ge 1$, as required.

Practice questions

Scaffolded

Q1. Use mathematical induction to prove that

$$\sum_{r=1}^{n}(6r-5)=n(3n-2)\text{ for all integers }n\ge 1.$$

(a) Verify the base case $P(1)$. (b) Write down the inductive hypothesis $P(k)$. (c) Assuming $P(k)$, add the $(k+1)$-th term and simplify to reach the formula at $n=k+1$. (d) State the conclusion.

Q2. Use mathematical induction to prove that

$$\sum_{r=1}^{n}r(r+3)=\frac{n(n+1)(n+5)}{3}\text{ for all integers }n\ge 1.$$

(a) Verify $P(1)$. (b) State the inductive hypothesis. (c) Add the term $(k+1)(k+4)$ and factorise to the formula at $n=k+1$. (d) Conclude.

Q3. Use mathematical induction to prove that

$$\sum_{r=1}^{n} 4^{r-1} = \frac{4^n - 1}{3} \text{ for all integers } n \geq 1.$$

(a) Verify $P(1)$. (b) State the inductive hypothesis. (c) Add the $(k+1)$-th term 4^k and simplify to $\frac{4^{k+1}-1}{3}$. (d) Conclude.

Q4. Use mathematical induction to prove that $9 \mid n^3 + (n+1)^3 + (n+2)^3$ for all integers $n \geq 1$. (a) Verify the base case. (b) State the inductive hypothesis in the form $f(k) = 9m$. (c) Show that $f(k+1) = f(k) + (k+3)^3 - k^3$, and hence that $f(k+1)$ is $9m$ plus a multiple of 9. (d) Conclude.

Q5. Use mathematical induction to prove that $6 \mid 11^n - 5^n$ for all integers $n \geq 1$. (a) Verify the base case. (b) State the inductive hypothesis $f(k) = 11^k - 5^k = 6m$. (c) Writing $11^{k+1} - 5^{k+1} = 11(11^k - 5^k) + 6 \cdot 5^k$, deduce $P(k+1)$. (d) Conclude.

Q6. Use mathematical induction to prove that $2^n \geq n+1$ for all integers $n \geq 1$. (a) Verify the base case. (b) State the inductive hypothesis. (c) From $2^{k+1} = 2 \cdot 2^k$ and the hypothesis, show $2^{k+1} \geq (k+1)+1$. (d) Conclude.

Unscaffolded

Q7. Use mathematical induction to prove that

$$\sum_{r=1}^{n} (2r+1) = n(n+2) \text{ for all integers } n \geq 1.$$

Q8. Use mathematical induction to prove that

$$\sum_{r=1}^{n} r(3r+1) = n(n+1)^2 \text{ for all integers } n \geq 1.$$

Q9. Use mathematical induction to prove that

$$\sum_{r=1}^{n} r(2r-1) = \frac{n(n+1)(4n-1)}{6} \text{ for all integers } n \geq 1.$$

Q10. Use mathematical induction to prove that

$$\sum_{r=1}^{n} 6^r = \frac{6^{n+1} - 6}{5} \text{ for all integers } n \geq 1.$$

Q11. Use mathematical induction to prove that

$$\sum_{r=1}^{n} \frac{1}{2^r} = 1 - \frac{1}{2^n} \text{ for all integers } n \geq 1.$$

Q12. Use mathematical induction to prove that

$$\sum_{r=1}^{n} r\,3^{r-1} = \frac{(2n-1)3^n + 1}{4} \text{ for all integers } n \geq 1.$$

Q13. Use mathematical induction to prove that $9 \mid 10^n - 1$ for all integers $n \geq 1$.

Q14. Use mathematical induction to prove that $6 \mid n^3 + 11n$ for all integers $n \geq 1$.

Q15. Use mathematical induction to prove that $5 \mid 2^{4n} - 1$ for all integers $n \geq 1$.

Q16. Use mathematical induction to prove that $3^n > 2n+1$ for all integers $n \geq 2$.

Q17. Use mathematical induction to prove that $n! > 3^n$ for all integers $n \geq 7$.

Q18. Use mathematical induction to prove that

$$\sum_{r=1}^{n} \frac{1}{\sqrt{r}} \geq \sqrt{n} \text{ for all integers } n \geq 1.$$

Answers

Q1. Proof by induction; base $P(1)$: $1=1$; step reaches $(k+1)(3k+1)=(k+1)\big(3(k+1)-2\big)$. **Q2.** Proof by induction; base $P(1)$: $4=4$; step reaches $\dfrac{(k+1)(k+2)(k+6)}{3}$. **Q3.** Proof by induction; base $P(1)$: $1=1$; step reaches $\dfrac{4^{k+1}-1}{3}$. **Q4.** Proof by induction; base $f(1)=36$; step: $f(k+1)=9m+9(k^2+3k+3)$. **Q5.** Proof by induction; base $f(1)=6$; step: $f(k+1)=6\big(11m+5^k\big)$. **Q6.** Proof by induction; base $2^1=2\geq 2$; step uses $2\cdot 2^k\geq 2(k+1)\geq k+2$. **Q7.** Proof by induction; base $P(1)$: $3=3$; step reaches $(k+1)(k+3)$. **Q8.** Proof by induction; base $P(1)$: $4=4$; step reaches $(k+1)(k+2)^2$. **Q9.** Proof by induction; base $P(1)$: $1=1$; step reaches $\dfrac{(k+1)(k+2)(4k+3)}{6}$. **Q10.** Proof by induction; base $P(1)$: $6=6$; step reaches $\dfrac{6^{k+2}-6}{5}$. **Q11.** Proof by induction; base $P(1)$: $1/2=1/2$; step reaches $1-\dfrac{1}{2^{k+1}}$. **Q12.** Proof by induction; base $P(1)$: $1=1$; step reaches $\dfrac{(2k+1)3^{k+1}+1}{4}$. **Q13.** Proof by induction; base $f(1)=9$; step: $f(k+1)=9(10m+1)$. **Q14.** Proof by induction; base $f(1)=12$; step: $f(k+1)=6m+3k(k+1)+12$. **Q15.** Proof by induction; base $f(1)=15$; step: $f(k+1)=5(16m+3)$. **Q16.** Proof by induction; base $3^2=9>5$; step: $3^{k+1}>3(2k+1)\geq 2(k+1)+1$. **Q17.** Proof by induction; base $7!=5040>2187=3^7$; step uses $k+1\geq 8>3$. **Q18.** Proof by induction; base $1\geq 1$; step uses $\dfrac{1}{\sqrt{k+1}}\geq\sqrt{k+1}-\sqrt{k}$.

Fully-worked solutions

Q1. Let $P(n)$ be the statement $S_n=n(3n-2)$, where $S_n=1+7+\ldots+(6n-5)$. *Base case* $n=1$: $S_1=6(1)-5=1$ and $1\big(3(1)-2\big)=1$, so $P(1)$ holds. *Inductive step*: assume $S_k=k(3k-2)$ for some integer $k\geq 1$. The $(k+1)$-th term is $6(k+1)-5=6k+1$, so

$$S_{k+1}=k(3k-2)+(6k+1)=3k^2-2k+6k+1=3k^2+4k+1=(k+1)(3k+1).$$

Since $3k+1=3(k+1)-2$, this is $(k+1)\big(3(k+1)-2\big)$, which is $P(k+1)$. By the principle of mathematical induction the formula holds for all integers $n\geq 1$, as required.

Q2. Let $P(n)$ be $S_n=\dfrac{n(n+1)(n+5)}{3}$, where S_n sums $r(r+3)$ from $r=1$ to n. *Base case* $n=1$: $S_1=1\cdot 4=4$ and $\dfrac{1\cdot 2\cdot 6}{3}=4$, so $P(1)$ holds. *Inductive step*: assume $S_k=\dfrac{k(k+1)(k+5)}{3}$. The $(k+1)$-th term is $(k+1)(k+4)$, so

$$S_{k+1}=\frac{k(k+1)(k+5)}{3}+(k+1)(k+4)=\frac{k+1}{3}\big[k(k+5)+3(k+4)\big]=\frac{k+1}{3}\big[k^2+8k+12\big].$$

Since $k^2+8k+12=(k+2)(k+6)$,

$$S_{k+1}=\frac{(k+1)(k+2)(k+6)}{3}=\frac{(k+1)\big((k+1)+1\big)\big((k+1)+5\big)}{3},$$

which is $P(k+1)$. By induction the formula holds for all integers $n\geq 1$, as required.

Q3. Let $P(n)$ be $S_n=\dfrac{4^n-1}{3}$, where $S_n=1+4+\ldots+4^{n-1}$. *Base case* $n=1$: $S_1=4^0=1$ and $\dfrac{4^1-1}{3}=1$, so $P(1)$ holds.

Inductive step: assume $S_k=\dfrac{4^k-1}{3}$. The $(k+1)$-th term is 4^k, so

$$S_{k+1}=\frac{4^k-1}{3}+4^k=\frac{4^k-1+3\cdot 4^k}{3}=\frac{4\cdot 4^k-1}{3}=\frac{4^{k+1}-1}{3},$$

which is $P(k+1)$. By induction the formula holds for all integers $n\geq 1$, as required.

Q4. Let $P(n)$ be $9\,/\,f(n)$, where $f(n)=n^3+(n+1)^3+(n+2)^3$. *Base case* $n=1$: $f(1)=1+8+27=36=9\times 4$, so $P(1)$ holds. *Inductive step*: assume $f(k)=k^3+(k+1)^3+(k+2)^3=9m$ for some integer m. Passing from k to $k+1$ drops the term k^3 and gains the term $(k+3)^3$, so

$$f(k+1)=(k+1)^3+(k+2)^3+(k+3)^3=f(k)+(k+3)^3-k^3.$$

Since $(k+3)^3-k^3=\left(k^3+9k^2+27k+27\right)-k^3=9\left(k^2+3k+3\right)$,

$$f(k+1)=9m+9\left(k^2+3k+3\right)=9\left(m+k^2+3k+3\right),$$

a multiple of 9, which is $P(k+1)$. By induction $9\,/\,n^3+(n+1)^3+(n+2)^3$ for all integers $n\geq 1$, as required.

Q5. Let $P(n)$ be $6\,/\,f(n)$, where $f(n)=11^n-5^n$. *Base case* $n=1$: $f(1)=11-5=6=6\times 1$, so $P(1)$ holds. *Inductive step*: assume $f(k)=11^k-5^k=6m$ for some integer m. Then

$$f(k+1)=11^{k+1}-5^{k+1}=11\cdot 11^k-5\cdot 5^k=11\left(11^k-5^k\right)+11\cdot 5^k-5\cdot 5^k=11\left(11^k-5^k\right)+6\cdot 5^k.$$

So $f(k+1)=11\cdot 6m+6\cdot 5^k=6\left(11m+5^k\right)$, a multiple of 6, which is $P(k+1)$. By induction $6\,/\,11^n-5^n$ for all integers $n\geq 1$, as required.

Q6. Let $P(n)$ be the statement $2^n\geq n+1$. *Base case* $n=1$: $2^1=2$ and $1+1=2$, so $2^1\geq 2$ and $P(1)$ holds. *Inductive step*: assume $2^k\geq k+1$ for some integer $k\geq 1$. Then

$$2^{k+1}=2\cdot 2^k\geq 2(k+1)=2k+2.$$

Since $k\geq 1>0$, we have $2k+2\geq k+2=(k+1)+1$, so $2^{k+1}\geq (k+1)+1$, which is $P(k+1)$. By induction $2^n\geq n+1$ for all integers $n\geq 1$, as required.

Q7. Let $P(n)$ be $S_n=n(n+2)$, where $S_n=3+5+\ldots+(2n+1)$. *Base case* $n=1$: $S_1=2(1)+1=3$ and $1\cdot 3=3$, so $P(1)$ holds. *Inductive step*: assume $S_k=k(k+2)$. The $(k+1)$-th term is $2(k+1)+1=2k+3$, so

$$S_{k+1}=k(k+2)+(2k+3)=k^2+2k+2k+3=k^2+4k+3=(k+1)(k+3),$$

which is $(k+1)\big((k+1)+2\big)=P(k+1)$. By induction the formula holds for all integers $n\geq 1$, as required.

Q8. Let $P(n)$ be $S_n=n(n+1)^2$, where S_n sums $r(3r+1)$ from $r=1$ to n. *Base case* $n=1$: $S_1=1\cdot 4=4$ and $1\cdot 2^2=4$, so $P(1)$ holds. *Inductive step*: assume $S_k=k(k+1)^2$. The $(k+1)$-th term is $(k+1)\big(3(k+1)+1\big)=(k+1)(3k+4)$, so

$$S_{k+1}=k(k+1)^2+(k+1)(3k+4)=(k+1)\left[k(k+1)+3k+4\right]=(k+1)\left[k^2+4k+4\right].$$

Since $k^2+4k+4=(k+2)^2$,

$$S_{k+1}=(k+1)(k+2)^2=(k+1)\big((k+1)+1\big)^2,$$

which is $P(k+1)$. By induction the formula holds for all integers $n \geq 1$, as required.

Q9. Let $P(n)$ be $S_n = \frac{n(n+1)(4n-1)}{6}$, where S_n sums $r(2r-1)$ from $r=1$ to n. *Base case* $n=1$: $S_1 = 1 \cdot 1 = 1$ and $\frac{1 \cdot 2 \cdot 3}{6} = 1$, so $P(1)$ holds. *Inductive step*: assume $S_k = \frac{k(k+1)(4k-1)}{6}$. The $(k+1)$-th term is $(k+1)(2(k+1)-1) = (k+1)(2k+1)$, so

$$S_{k+1} = \frac{k(k+1)(4k-1)}{6} + (k+1)(2k+1) = \frac{k+1}{6}\left[k(4k-1) + 6(2k+1)\right] = \frac{k+1}{6}\left[4k^2 + 11k + 6\right].$$

Since $4k^2 + 11k + 6 = (k+2)(4k+3)$,

$$S_{k+1} = \frac{(k+1)(k+2)(4k+3)}{6} = \frac{(k+1)\big((k+1)+1\big)\big(4(k+1)-1\big)}{6},$$

which is $P(k+1)$. By induction the formula holds for all integers $n \geq 1$, as required.

Q10. Let $P(n)$ be $S_n = \frac{6^{n+1}-6}{5}$, where $S_n = 6 + 36 + \ldots + 6^n$. *Base case* $n=1$: $S_1 = 6^1 = 6$ and $\frac{6^2-6}{5} = \frac{30}{5} = 6$, so $P(1)$ holds. *Inductive step*: assume $S_k = \frac{6^{k+1}-6}{5}$. The $(k+1)$-th term is 6^{k+1}, so

$$S_{k+1} = \frac{6^{k+1}-6}{5} + 6^{k+1} = \frac{6^{k+1} - 6 + 5 \cdot 6^{k+1}}{5} = \frac{6 \cdot 6^{k+1} - 6}{5} = \frac{6^{k+2}-6}{5},$$

which is $P(k+1)$. By induction the formula holds for all integers $n \geq 1$, as required.

Q11. Let $P(n)$ be $S_n = 1 - \frac{1}{2^n}$, where $S_n = \frac{1}{2} + \frac{1}{4} + \ldots + \frac{1}{2^n}$. *Base case* $n=1$: $S_1 = \frac{1}{2}$ and $1 - \frac{1}{2} = \frac{1}{2}$, so $P(1)$ holds. *Inductive step*: assume $S_k = 1 - \frac{1}{2^k}$. The $(k+1)$-th term is $\frac{1}{2^{k+1}}$, so

$$S_{k+1} = 1 - \frac{1}{2^k} + \frac{1}{2^{k+1}} = 1 - \frac{2}{2^{k+1}} + \frac{1}{2^{k+1}} = 1 - \frac{1}{2^{k+1}},$$

which is $P(k+1)$. By induction the formula holds for all integers $n \geq 1$, as required.

Q12. Let $P(n)$ be $S_n = \frac{(2n-1)3^n + 1}{4}$, where S_n sums $r\,3^{r-1}$ from $r=1$ to n. *Base case* $n=1$: $S_1 = 1 \cdot 3^0 = 1$ and $\frac{(1)3^1+1}{4} = \frac{4}{4} = 1$, so $P(1)$ holds. *Inductive step*: assume $S_k = \frac{(2k-1)3^k + 1}{4}$. The $(k+1)$-th term is $(k+1)3^k$, so

$$S_{k+1} = \frac{(2k-1)3^k + 1}{4} + (k+1)3^k = \frac{(2k-1)3^k + 1 + 4(k+1)3^k}{4} = \frac{(6k+3)3^k + 1}{4}.$$

Since $(6k+3)3^k = 3(2k+1)3^k = (2k+1)3^{k+1}$,

$$S_{k+1} = \frac{(2k+1)3^{k+1} + 1}{4} = \frac{\big(2(k+1)-1\big)3^{k+1} + 1}{4},$$

which is $P(k+1)$. By induction the formula holds for all integers $n \geq 1$, as required.

Q13. Let $P(n)$ be $9 \mid f(n)$, where $f(n) = 10^n - 1$. *Base case* $n=1$: $f(1) = 10 - 1 = 9 = 9 \times 1$, so $P(1)$ holds. *Inductive step*: assume $f(k) = 10^k - 1 = 9m$ for some integer m; so $10^k = 9m + 1$. Then

$$f(k+1)=10^{k+1}-1=10\cdot 10^{k}-1=10(9m+1)-1=90m+9=9(10m+1),$$

a multiple of 9, which is $P(k+1)$. By induction $9\mid 10^{n}-1$ for all integers $n\geq 1$, as required.

Q14. Let $P(n)$ be $6\mid f(n)$, where $f(n)=n^{3}+11n$. *Base case* $n=1$: $f(1)=1+11=12=6\times 2$, so $P(1)$ holds. *Inductive step*: assume $f(k)=k^{3}+11k=6m$ for some integer m. Then

$$f(k+1)=(k+1)^{3}+11(k+1)=k^{3}+3k^{2}+3k+1+11k+11=(k^{3}+11k)+3k^{2}+3k+12.$$

So $f(k+1)=6m+3k(k+1)+12$. Now $k(k+1)$ is a product of two consecutive integers and so is even, say $k(k+1)=2t$; then $3k(k+1)=6t$ and

$$f(k+1)=6m+6t+12=6(m+t+2),$$

a multiple of 6, which is $P(k+1)$. By induction $6\mid n^{3}+11n$ for all integers $n\geq 1$, as required.

Q15. Let $P(n)$ be $5\mid f(n)$, where $f(n)=2^{4n}-1$. Writing $2^{4n}=(2^{4})^{n}=16^{n}$, this is $5\mid 16^{n}-1$. *Base case* $n=1$: $f(1)=16-1=15=5\times 3$, so $P(1)$ holds. *Inductive step*: assume $f(k)=16^{k}-1=5m$ for some integer m; so $16^{k}=5m+1$. Then

$$f(k+1)=16^{k+1}-1=16\cdot 16^{k}-1=16(5m+1)-1=80m+15=5(16m+3),$$

a multiple of 5, which is $P(k+1)$. By induction $5\mid 2^{4n}-1$ for all integers $n\geq 1$, as required.

Q16. Let $P(n)$ be the statement $3^{n}>2n+1$. *Base case* $n=2$: $3^{2}=9$ and $2(2)+1=5$, and $9>5$, so $P(2)$ holds. (The starting value is 2 because at $n=1$ both sides equal 3, so the strict inequality fails there.) *Inductive step*: assume $3^{k}>2k+1$ for some integer $k\geq 2$. Multiplying by 3,

$$3^{k+1}=3\cdot 3^{k}>3(2k+1)=6k+3.$$

Since $6k+3\geq 2k+3=2(k+1)+1$ for $k\geq 0$, combining gives $3^{k+1}>2(k+1)+1$, which is $P(k+1)$. By induction $3^{n}>2n+1$ for all integers $n\geq 2$, as required.

Q17. Let $P(n)$ be the statement $n!>3^{n}$. *Base case* $n=7$: $7!=5040$ and $3^{7}=2187$, and $5040>2187$, so $P(7)$ holds. (For $n\leq 6$ the inequality fails, e.g. $6!=720<729=3^{6}$, so the starting value is 7.) *Inductive step*: assume $k!>3^{k}$ for some integer $k\geq 7$. Then

$$(k+1)!=(k+1)\cdot k!>(k+1)\cdot 3^{k}.$$

Since $k\geq 7$, we have $k+1\geq 8>3$, so $(k+1)\cdot 3^{k}>3\cdot 3^{k}=3^{k+1}$. Hence $(k+1)!>3^{k+1}$, which is $P(k+1)$. By induction $n!>3^{n}$ for all integers $n\geq 7$, as required.

Q18. Let $P(n)$ be the statement $S_{n}\geq\sqrt{n}$, where $S_{n}=\frac{1}{\sqrt{1}}+\frac{1}{\sqrt{2}}+\ldots+\frac{1}{\sqrt{n}}$. *Base case* $n=1$: $S_{1}=1$ and $\sqrt{1}=1$, so $S_{1}\geq 1$ and $P(1)$ holds. *Inductive step*: assume $S_{k}\geq\sqrt{k}$ for some integer $k\geq 1$. Adding the $(k+1)$-th term,

$$S_{k+1}=S_{k}+\frac{1}{\sqrt{k+1}}\geq\sqrt{k}+\frac{1}{\sqrt{k+1}}.$$

It suffices to show $\sqrt{k}+\frac{1}{\sqrt{k+1}}\geq\sqrt{k+1}$, i.e. $\frac{1}{\sqrt{k+1}}\geq\sqrt{k+1}-\sqrt{k}$. Rationalising,

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

and since $\sqrt{k+1}+\sqrt{k}>\sqrt{k+1}>0$ we have $\frac{1}{\sqrt{k+1}+\sqrt{k}}<\frac{1}{\sqrt{k+1}}$. Therefore $S_{k+1}\geq\sqrt{k+1}$, which is $P(k+1)$. By induction $S_n\geq\sqrt{n}$ for all integers $n\geq 1$, as required.

Chapter 1 Proof and number — 1D Primes and the fundamental theorem of arithmetic

Theory

The integers greater than 1 are built from a set of indivisible pieces — the prime numbers — in essentially one way. This section makes that idea precise. It states the **fundamental theorem of arithmetic**, proves that every integer above 1 really does break into primes and in only one way, uses the prime factorisation as a practical tool for greatest common divisors, least common multiples and counting factors, and closes with Euclid's proof that the supply of primes never runs out.

Divisibility.

For integers a and b, we say a **divides** b, written $a \mid b$, if $b = a\,k$ for some integer k; a is then a **factor** (or **divisor**) of b, and b is a **multiple** of a. When no such integer k exists we write $a \nmid b$. Two facts used constantly below follow straight from the definition: if $d \mid a$ and $d \mid b$ then d divides every combination $a\,x + b\,y$ (for integers x, y), and the only positive integer dividing 1 is 1 itself.

Primes and composites.

A **prime number** is an integer $p > 1$ whose only positive divisors are 1 and p. An integer $n > 1$ that is not prime is **composite**; it can be written $n = a\,b$ with $1 < a < n$ and $1 < b < n$. The integer 1 is deliberately counted as *neither* prime nor composite — it is a **unit**, the only positive integer with a multiplicative inverse among the integers. Excluding 1 from the primes is not a whim: it is exactly what makes factorisation into primes **unique**, as the theorem below requires. The first few primes are

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots,$$

and 2 is the only even prime, since every other even number has 2 as a proper factor.

Testing for primality by trial division.

To decide whether a given $n > 1$ is prime, it is enough to test for a prime factor up to $\sqrt{n}$. For if $n = a\,b$ is composite with $1 < a \le b$, then $a^2 \le a\,b = n$, so $a \le \sqrt{n}$; thus a composite number always has a factor (and hence a *prime* factor) not exceeding its square root. If no prime $p \le \sqrt{n}$ divides n, then n is prime. For example, to test 211 we need only check the primes up to $\sqrt{211} \approx 14.5$, namely $2, 3, 5, 7, 11, 13$; none divides 211, so 211 is prime. Removing all multiples of each prime in turn from a list of integers is the ancient **sieve of Eratosthenes**, which produces every prime up to a chosen bound.

Every integer above 1 has a prime factor.

Before stating the main theorem we record the building block on which it rests.

> **Lemma.** Every integer $n > 1$ has at least one prime factor.

Proof. Suppose not, and let n be the **smallest** integer greater than 1 with no prime factor (such a smallest one exists because any non-empty set of positive integers has a least member — the **well-ordering principle**). Now n cannot be prime, since a prime is its own prime factor; so n is composite, say $n = a\,b$ with $1 < a < n$. By the choice of n as *smallest*, the smaller integer a does have a prime factor p. But $p \mid a$ and $a \mid n$, so $p \mid n$, giving n a prime factor after all — a contradiction. Hence every integer $n > 1$ has a prime factor, as required.

The fundamental theorem of arithmetic.

> **Fundamental theorem of arithmetic.** Every integer $n > 1$ can be written as a product of primes, and this factorisation is **unique** apart from the order in which the primes are written.

The theorem has two halves — *existence* (a factorisation exists) and *uniqueness* (there is only one) — and each needs proof.

Existence. Suppose some integer greater than 1 cannot be written as a product of primes, and let m be the smallest such integer. Then m is not prime, for a prime is already a product of primes (of one factor). So m is composite, $m = a\,b$ with $1 < a < m$ and $1 < b < m$. By the minimality of m, each of the smaller integers a and b *is* a product of primes; writing the two factorisations side by side expresses $m = a\,b$ as a product of primes, contradicting the choice of m. Hence every integer $n > 1$ is a product of primes.

Uniqueness. This half relies on a result about primes and products.

> **Euclid's lemma.** If a prime p divides a product $a\,b$ of integers, then $p \mid a$ or $p \mid b$. More generally, if p divides a product $a_1 a_2 \cdots a_r$, then p divides at least one factor a_i.

Euclid's lemma is what singles primes out from composite numbers: $6 \mid 4 \times 9$ yet 6 divides neither 4 nor 9, whereas a **prime** factor of a product must land inside one of the factors. (The lemma follows from the theory of the greatest common divisor; we take it as established.) Granting it, suppose some integer greater than 1 had *two* different prime factorisations, and let n be the smallest such integer, with

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s .$$

Since $p_1 \mid n = q_1 q_2 \cdots q_s$, Euclid's lemma gives $p_1 \mid q_j$ for some j; but q_j is prime and $p_1 > 1$, so $p_1 = q_j$. Cancelling this common prime from both sides leaves a smaller integer, n / p_1, with two prime factorisations. By the minimality of n those must agree, and restoring the cancelled prime shows the two factorisations of n agree as well. This contradiction proves the factorisation unique.

Canonical (index) form.

Collecting repeated primes and listing them in increasing order writes each integer $n > 1$ uniquely in **canonical form**

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},\ p_1 < p_2 < \cdots < p_k,\ a_i \geq 1 ,$$

where the p_i are the distinct primes dividing n and each exponent a_i is the number of times that prime occurs. For instance $450 = 2 \times 3^2 \times 5^2$ and $726 = 2 \times 3 \times 11^2$. The uniqueness in the theorem is exactly what lets us speak of *the* prime factorisation of a number and read information off it.

Greatest common divisor and least common multiple.

Write two integers over the *same* list of primes, allowing an exponent to be 0 when a prime is absent:

$$a = p_1^{a_1} \cdots p_k^{a_k},\ b = p_1^{b_1} \cdots p_k^{b_k} .$$

An integer divides a exactly when, prime by prime, its exponent does not exceed the corresponding a_i. So the **greatest common divisor** $gcd(a,b)$ — the largest integer dividing both — takes the *smaller* exponent on each prime, and the **least common multiple** $lcm(a,b)$ — the smallest positive integer that both divide — takes the *larger*:

$$gcd(a,b) = p_1^{min(a_1,b_1)} \cdots p_k^{min(a_k,b_k)},\ lcm(a,b) = p_1^{max(a_1,b_1)} \cdots p_k^{max(a_k,b_k)} .$$

Because $min(a_i,b_i) + max(a_i,b_i) = a_i + b_i$ for every i, multiplying these two results adds the exponents back to $a_i + b_i$, giving the identity

$$gcd(a,b) \times lcm(a,b) = a\,b .$$

Counting divisors.

A positive divisor of $n = p_1^{a_1} \cdots p_k^{a_k}$ is precisely a number $p_1^{e_1} \cdots p_k^{e_k}$ with $0 \leq e_i \leq a_i$ for each i — a consequence of unique factorisation. There are $a_i + 1$ independent choices for each exponent e_i (namely $0, 1, \ldots, a_i$), so the number of positive divisors of n is the product

$$\tau(n) = (a_1 + 1)(a_2 + 1) \cdots (a_k + 1) .$$

For example $200 = 2^3 \times 5^2$ has $(3+1)(2+1) = 12$ positive divisors.

Infinitely many primes.

Finally, the primes never run out. This is one of the oldest theorems in mathematics, and Euclid's proof by contradiction is a model of the method.

Theorem (Euclid). There are infinitely many primes.

Proof. Suppose, for contradiction, that there are only finitely many primes, so that they can be listed in full as $p_1, p_2, \ldots, p_n$. Consider the integer formed by multiplying them all together and adding 1:

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

Since $N > 1$, the lemma above gives N a prime factor q, and as our list is supposed to contain *every* prime, q must be one of $p_1, \ldots, p_n$. But dividing N by any p_i leaves remainder 1: for $p_i \mid p_1 p_2 \cdots p_n$, so if $p_i \mid N$ as well then p_i would divide the difference $N - p_1 p_2 \cdots p_n = 1$, which is impossible. Hence no p_i divides N, so its prime factor q lies outside the list — contradicting that the list was complete. Therefore no finite list can contain all the primes; there are infinitely many, as required.

Two remarks sharpen the argument. First, the number N need not itself be prime — the proof only needs it to *have* a prime factor beyond the list. With the first four primes, $2 \times 3 \times 5 \times 7 + 1 = 211$, which happens to be prime; but with the first six, $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509$, which is composite, its prime factors 59 and 509 both lying beyond 13. Second, the same construction, applied to any finite collection of primes, always manufactures a fresh one, which is the real content of the theorem.

Worked examples

Example 1 — scaffolded

(a) Classify each of 51, 61, 91 and 133 as prime or composite. Find the prime factorisation, in index form, of (b) 792 and (c) 4116.

Working	Comment
$51 = 3 \times 17$, so 51 is composite. Testing 61 against $2, 3, 5, 7$ (all primes $\le \sqrt{61} \approx 7.8$) finds no factor, so 61 is prime.	A single proper factor settles "composite"; trial division up to $\sqrt{n}$ settles "prime".
$91 = 7 \times 13$ and $133 = 7 \times 19$, so both are composite.	91 and 133 are not divisible by $2, 3, 5$, but are by 7.
$792 = 2 \times 396 = 2 \times 2 \times 198 = 2 \times 2 \times 2 \times 99.$	Divide out the smallest prime, 2, repeatedly.
$= 2^3 \times 9 \times 11 = 2^3 \times 3^2 \times 11.$	Then $99 = 9 \times 11 = 3^2 \times 11$; collect equal primes as powers.
$4116 = 2^2 \times 1029 = 2^2 \times 3 \times 343 = 2^2 \times 3 \times 7^3.$	$4116 = 4 \times 1029$, $1029 = 3 \times 343$, and $343 = 7^3$.

Example 2 — scaffolded

The integers 504 and 588 have prime factorisations $504 = 2^3 \times 3^2 \times 7$ and $588 = 2^2 \times 3 \times 7^2$. Use these to find (a) $gcd(504, 588)$, (b) $lcm(504, 588)$, (c) the number of positive divisors of each, and (d) a check that $gcd \times lcm = 504 \times 588$.

Working	Comment
$504 = 2^3 \times 3^2 \times 7^1$, $588 = 2^2 \times 3^1 \times 7^2$.	Write both over the same primes $2, 3, 7$ with explicit exponents.
$gcd = 2^{min(3,2)} 3^{min(2,1)} 7^{min(1,2)} = 2^2 \times 3 \times 7 = 84.$	The gcd takes the **smaller** exponent on each prime.
$lcm = 2^{max(3,2)} 3^{max(2,1)} 7^{max(1,2)} = 2^3 \times 3^2 \times 7^2 = 3528.$	The lcm takes the **larger** exponent on each prime.
$\tau(504) = (3+1)(2+1)(1+1) = 24,$	Add 1 to each exponent and multiply.

Working	Comment
$\tau(588)=(2+1)(1+1)(2+1)=18.$	
$gcd\times lcm=84\times 3528=296\,352=504\times 588.$	Confirms $gcd(a,b)\,lcm(a,b)=a\,b.$

Example 3 — unscaffolded

The integer $N=2016$ has prime factorisation $2016=2^5\times 3^2\times 7$. Find the number of positive divisors of N, and determine how many of them are even.

Applying the divisor-counting formula to $N=2^5\times 3^2\times 7^1$,

$$\tau(N)=(5+1)(2+1)(1+1)=6\times 3\times 2=36.$$

A divisor is **odd** exactly when it contains no factor of 2, that is, when the exponent of 2 is 0; the odd divisors are therefore the divisors of $3^2\times 7=63$, of which there are $(2+1)(1+1)=6$. The remaining divisors are even, so the number of even divisors is $36-6=30$.

$\therefore N$ has 36 positive divisors, of which 30 are even.

Example 4 — unscaffolded

Prove that a positive integer $n>1$ is a perfect square **if and only if** every exponent in its prime factorisation is even.

Write the canonical factorisation $n=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$; the claim is a biconditional, so we prove each direction in turn.

Backward (even exponents $\Rightarrow$ perfect square). Suppose every a_i is even, say $a_i=2b_i$ for integers $b_i\geq 1$. Setting $m=p_1^{b_1}p_2^{b_2}\cdots p_k^{b_k}$, an integer, gives

$$m^2=p_1^{2b_1}p_2^{2b_2}\cdots p_k^{2b_k}=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}=n,$$

so n is a perfect square.

Forward (perfect square $\Rightarrow$ even exponents). Suppose $n=m^2$ for some integer $m>1$, and let $m=p_1^{c_1}p_2^{c_2}\cdots p_k^{c_k}$ be the canonical factorisation of m. Squaring, $n=m^2=p_1^{2c_1}p_2^{2c_2}\cdots p_k^{2c_k}$. By the **uniqueness** in the fundamental theorem of arithmetic, this is *the* prime factorisation of n, so its exponents are exactly $a_i=2c_i$ — each an even number.

Both directions hold, so n is a perfect square if and only if every exponent in its prime factorisation is even. As a check, $600=2^3\times 3\times 5^2$ has odd exponents and is not a square, whereas $600^2=2^6\times 3^2\times 5^4$ has all exponents even, as required.

Practice questions

Scaffolded

Q1. Consider the integers 77, 83, 111 and 119. (a) Classify each as prime or composite, giving a factor for any composite number. (b) Explain why testing primes up to $\sqrt{83}$ suffices to confirm 83 is prime. (c) Find the prime factorisation of 630 in index form.

Q2. Find the prime factorisation, in index form, of each integer. (a) 924. (b) 1188. (c) State the distinct primes dividing 1188 and the exponent of each.

Q3. Let $168=2^3\times 3\times 7$ and $180=2^2\times 3^2\times 5$. (a) Write both numbers over the primes $2,3,5,7$ with explicit exponents. (b) Find $gcd(168,180)$. (c) Find $lcm(168,180)$. (d) Verify that $gcd\times lcm=168\times 180$.

Q4. Let $N=2200=2^3\times 5^2\times 11$. (a) State the exponents of 2, 5 and 11. (b) Use the divisor-counting formula to find the number of positive divisors of N. (c) How many of those divisors are odd?

Q5. Take the five primes $2,3,5,7,11$ and form $N = 2\times3\times5\times7\times11+1$. (a) Evaluate N. (b) Show that none of $2,3,5,7,11$ divides N. (c) Explain what part (b), together with the fact that $N>1$, tells you about the primes.

Q6. Let $M = 1500 = 2^2\times3\times5^3$. (a) Is M a perfect square? Justify your answer using the exponents. (b) Find the smallest positive integer t such that Mt is a perfect square. (c) State Mt and its square root.

Unscaffolded

Q7. Find the prime factorisation of 6300 in index form.

Q8. Given $240 = 2^4\times3\times5$ and $350 = 2\times5^2\times7$, find $gcd(240,350)$ and $lcm(240,350)$.

Q9. Find $gcd(84,126,210)$ and $lcm(84,126,210)$, using prime factorisations.

Q10. The integer 5292 has prime factorisation $2^2\times3^3\times7^2$. Find the number of positive divisors of 5292 and how many of them are odd.

Q11. Find the smallest positive integer with exactly 15 positive divisors, and justify that it is the smallest.

Q12. A positive integer has the form $N = 2^a\times3^2\times5$ and has exactly 24 positive divisors. Find a and hence N.

Q13. Prove that if p is a prime and $p\mid n^2$ for an integer n, then $p\mid n$.

Q14. Prove, using prime factorisations, that $gcd(a,b)\times lcm(a,b) = ab$ for all positive integers a and b.

Q15. Prove that a positive integer $n>1$ is a perfect cube if and only if every exponent in its prime factorisation is a multiple of 3.

Q16. Prove that a positive integer has an **odd** number of positive divisors if and only if it is a perfect square.

Q17. Prove that there are infinitely many primes of the form $6k-1$ (equivalently, primes that leave remainder 5 on division by 6).

Q18. Prove that there are arbitrarily long runs of consecutive composite integers; specifically, show that for every integer $n\geq2$ the $n-1$ integers $n!+2, n!+3, \ldots, n!+n$ are all composite.

Answers

Q1. (a) $77 = 7 \times 11$ composite, 83 prime, $111 = 3 \times 37$ composite, $119 = 7 \times 17$ composite; (b) any composite n has a prime factor $\le \sqrt{n}$; (c) $630 = 2 \times 3^2 \times 5 \times 7$. **Q2.** (a) $924 = 2^2 \times 3 \times 7 \times 11$; (b) $1188 = 2^2 \times 3^3 \times 11$; (c) primes 2 (exp 2), 3 (exp 3), 11 (exp 1). **Q3.** (a) $168 = 2^3 \times 3^1 \times 5^0 \times 7^1$, $180 = 2^2 \times 3^2 \times 5^1 \times 7^0$; (b) $gcd = 2^2 \times 3 = 12$; (c) $lcm = 2^3 \times 3^2 \times 5 \times 7 = 2520$; (d) $12 \times 2520 = 30\,240 = 168 \times 180$. **Q4.** (a) $3, 2, 1$; (b) $(3+1)(2+1)(1+1) = 24$; (c) odd divisors $= (2+1)(1+1) = 6$. **Q5.** (a) $N = 2311$; (b) each leaves remainder 1; (c) 2311 has a prime factor outside $\{2, 3, 5, 7, 11\}$ (indeed 2311 is itself prime), so no finite list of primes is complete. **Q6.** (a) no — the exponents $2, 1, 3$ of $2, 3, 5$ are not all even; (b) $t = 3 \times 5 = 15$; (c) $Mt = 22\,500 = 150^2$. **Q7.** $6300 = 2^2 \times 3^2 \times 5^2 \times 7$. **Q8.** $gcd = 2 \times 5 = 10$, $lcm = 2^4 \times 3 \times 5^2 \times 7 = 8400$. **Q9.** $gcd = 2 \times 3 \times 7 = 42$, $lcm = 2^2 \times 3^2 \times 5 \times 7 = 1260$. **Q10.** $\tau(5292) = (2+1)(3+1)(2+1) = 36$; odd divisors $= (3+1)(2+1) = 12$. **Q11.** $144 = 2^4 \times 3^2$. **Q12.** $a = 3$, so $N = 2^3 \times 3^2 \times 5 = 360$. **Q13.** Proof — a prime in n^2 must be a prime of n; see solutions. **Q14.** Proof — $min(a_i, b_i) + max(a_i, b_i) = a_i + b_i$; see solutions. **Q15.** Proof — biconditional via unique factorisation; see solutions. **Q16.** Proof — $\tau(n)$ is odd iff every $(a_i + 1)$ is odd iff every a_i is even; see solutions. **Q17.** Proof by contradiction — Euclid-style, $N = 6q_1q_2 \cdots q_m - 1$; see solutions. **Q18.** Proof — $j \mid n! + j$ for $2 \le j \le n$, giving a proper factor; see solutions.

Fully-worked solutions

Q1. (a) $77 = 7 \times 11$, $111 = 3 \times 37$ and $119 = 7 \times 17$ are composite, each shown by exhibiting a proper factor. For 83, the primes up to $\sqrt{83} \approx 9.1$ are $2, 3, 5, 7$; none divides 83, so 83 is prime. (b) If 83 were composite it would factor as $83 = ab$ with $1 < a \le b$, and then $a^2 \le ab = 83$, so $a \le \sqrt{83}$; hence a prime factor would appear at or below $\sqrt{83}$, and finding none proves primality. (c) Dividing out primes, $630 = 2 \times 315 = 2 \times 3 \times 105 = 2 \times 3 \times 3 \times 35 = 2 \times 3^2 \times 5 \times 7$.

Q2. (a) $924 = 2 \times 462 = 2^2 \times 231 = 2^2 \times 3 \times 77 = 2^2 \times 3 \times 7 \times 11$. (b) $1188 = 2 \times 594 = 2^2 \times 297 = 2^2 \times 3^3 \times 11$, since $297 = 27 \times 11$. (c) The distinct primes dividing 1188 are $2, 3, 11$, with exponents $2, 3, 1$ respectively.

Q3. (a) Over $2, 3, 5, 7$: $168 = 2^3 \times 3^1 \times 5^0 \times 7^1$ and $180 = 2^2 \times 3^2 \times 5^1 \times 7^0$. (b) The gcd takes the smaller exponent on each prime: $gcd = 2^2 \times 3^1 \times 5^0 \times 7^0 = 12$. (c) The lcm takes the larger: $lcm = 2^3 \times 3^2 \times 5^1 \times 7^1 = 8 \times 9 \times 5 \times 7 = 2520$. (d) $gcd \times lcm = 12 \times 2520 = 30\,240$, and $168 \times 180 = 30\,240$; the two agree, as the identity $gcd(a, b)\,lcm(a, b) = ab$ predicts.

Q4. (a) In $N = 2^3 \times 5^2 \times 11^1$ the exponents of $2, 5, 11$ are $3, 2, 1$. (b) $\tau(N) = (3+1)(2+1)(1+1) = 4 \times 3 \times 2 = 24$. (c) An odd divisor contains no factor 2, so it is a divisor of $5^2 \times 11 = 275$; there are $(2+1)(1+1) = 6$ of them.

Q5. (a) $N = 2 \times 3 \times 5 \times 7 \times 11 + 1 = 2310 + 1 = 2311$. (b) Each of $2, 3, 5, 7, 11$ divides the product 2310, so dividing $N = 2310 + 1$ by any of them leaves remainder 1; none is a factor of N. (c) Since $N > 1$, it has a prime factor, and by (b) that factor is none of $2, 3, 5, 7, 11$ (in fact 2311 is itself prime). So there is a prime beyond the chosen list; no finite list of primes can be complete, which is the heart of Euclid's argument.

Q6. (a) $M = 2^2 \times 3^1 \times 5^3$. The exponents $2, 1, 3$ are not all even (those of 3 and 5 are odd), so by the perfect-square criterion M is **not** a perfect square. (b) Multiplying M by a positive integer t makes it a perfect square exactly when every exponent becomes even; the smallest such t raises each odd exponent by 1, so $t = 3^1 \times 5^1 = 15$. (c) Then $Mt = 2^2 \times 3^2 \times 5^4 = 22\,500$, with $\sqrt{22\,500} = 2 \times 3 \times 5^2 = 150$.

Q7. $6300 = 2^2 \times 1575 = 2^2 \times 3 \times 525 = 2^2 \times 3^2 \times 175 = 2^2 \times 3^2 \times 5^2 \times 7$.

Q8. Over $2, 3, 5, 7$: $240 = 2^4 \times 3^1 \times 5^1 \times 7^0$ and $350 = 2^1 \times 3^0 \times 5^2 \times 7^1$. Taking the smaller exponent on each prime, $gcd = 2^1 \times 5^1 = 10$; taking the larger, $lcm = 2^4 \times 3^1 \times 5^2 \times 7^1 = 16 \times 3 \times 25 \times 7 = 8400$. (Check: $10 \times 8400 = 84\,000 = 240 \times 350$.)

Q9. Factorise: $84=2^2\times3\times7$, $126=2\times3^2\times7$, $210=2\times3\times5\times7$. The gcd takes the smallest exponent of each prime across all three: $2^{min(2,1,1)}3^{min(1,2,1)}5^{min(0,0,1)}7^{min(1,1,1)}=2\times3\times7=42$. The lcm takes the largest: $2^{max(2,1,1)}3^{max(1,2,1)}5^{max(0,0,1)}7^{max(1,1,1)}=2^2\times3^2\times5\times7=1260$.

Q10. With $5292=2^2\times3^3\times7^2$, the number of positive divisors is $\tau(5292)=(2+1)(3+1)(2+1)=3\times4\times3=36$. The odd divisors are those with no factor 2, i.e. the divisors of $3^3\times7^2$, of which there are $(3+1)(2+1)=12$.

Q11. If $n=p_1^{a_1}\cdots p_k^{a_k}$ then $\tau(n)=(a_1+1)\cdots(a_k+1)=15$. Factor 15 as a product of integers each ≥2: either 15 (one factor) or 3×5. These give exponent patterns $\{14\}$ or $\{4,2\}$ (in some order). To minimise n, assign the larger exponent to the smaller prime: $\{14\}$ gives $2^{14}=16\,384$; $\{4,2\}$ gives $2^4\times3^2=144$ (smaller than $2^2\times3^4=324$). The least value is therefore $n=144=2^4\times3^2$, and no smaller integer has exactly 15 divisors because every admissible exponent pattern has been tested.

Q12. From $N=2^a\times3^2\times5^1$, the divisor count is $\tau(N)=(a+1)(2+1)(1+1)=6(a+1)$. Setting this equal to 24 gives $6(a+1)=24$, so $a+1=4$ and $a=3$. Hence $N=2^3\times3^2\times5=8\times9\times5=360$.

Q13. Assume p is prime and $p\mid n^2$. If $n=0$ or $n=\pm1$ the statement is immediate ($p\mid0$, and $p\nmid1$ with $p\nmid n^2=1$), so take $|n|>1$ and let $n=q_1q_2\cdots q_r$ be a prime factorisation of $|n|$. Then $n^2=q_1q_1q_2q_2\cdots q_rq_r$ is a product of primes, and $p\mid n^2$ means, by Euclid's lemma, that p equals one of these prime factors q_i. But every q_i divides n, so $p=q_i$ divides n. Hence $p\mid n$, as required.

Q14. Write a and b over a common list of primes, $a=p_1^{a_1}\cdots p_k^{a_k}$ and $b=p_1^{b_1}\cdots p_k^{b_k}$ (with zero exponents where a prime is absent). Then

$$gcd(a,b)=p_1^{min(a_1,b_1)}\cdots p_k^{min(a_k,b_k)},\ lcm(a,b)=p_1^{max(a_1,b_1)}\cdots p_k^{max(a_k,b_k)}.$$

Multiplying, the exponent of p_i in the product $gcd(a,b)\,lcm(a,b)$ is $min(a_i,b_i)+max(a_i,b_i)$. For any two numbers the smaller plus the larger equals their sum, so $min(a_i,b_i)+max(a_i,b_i)=a_i+b_i$. Hence each prime p_i carries exponent a_i+b_i, which is exactly its exponent in ab. Therefore $gcd(a,b)\times lcm(a,b)=ab$, as required.

Q15. Let $n=p_1^{a_1}\cdots p_k^{a_k}$ be the canonical factorisation. *Backward:* if every $a_i=3b_i$ for integers b_i, put $m=p_1^{b_1}\cdots p_k^{b_k}$; then $m^3=p_1^{3b_1}\cdots p_k^{3b_k}=n$, so n is a perfect cube. *Forward:* if $n=m^3$ with $m=p_1^{c_1}\cdots p_k^{c_k}$, then $n=m^3=p_1^{3c_1}\cdots p_k^{3c_k}$, and by the uniqueness of prime factorisation the exponents of n are $a_i=3c_i$, each a multiple of 3. Both directions hold, so n is a perfect cube if and only if every exponent in its prime factorisation is a multiple of 3, as required.

Q16. Write $n=p_1^{a_1}\cdots p_k^{a_k}$, so $\tau(n)=(a_1+1)\cdots(a_k+1)$. A product of integers is odd if and only if every factor is odd, so $\tau(n)$ is odd exactly when each a_i+1 is odd, that is, when each a_i is even. By the perfect-square criterion (Example 4) this happens precisely when n is a perfect square. Therefore n has an odd number of positive divisors if and only if n is a perfect square, as required. (Geometrically, divisors pair up as d and n/d, leaving an unpaired middle divisor $\sqrt{n}$ exactly when n is a square.)

Q17. First note that every prime other than 2 and 3 leaves remainder 1 or 5 on division by 6 (remainders $0,2,4$ give a factor of 2, and 3 gives a factor of 3). Also 5 itself is a prime of the form $6k-1$. Suppose, for contradiction, that there are only finitely many primes of the form $6k-1$, and list them as $q_1,q_2,\ldots,q_m$ (so $q_1=5$). Consider

$$N=6q_1q_2\cdots q_m-1.$$

Writing $N=6(q_1q_2\cdots q_m-1)+5$ shows that $N>1$ and that N leaves remainder 5 on division by 6. In particular N is odd (as $6q_1\cdots q_m$ is even) and is not a multiple of 3 (as $6q_1\cdots q_m$ is), so by the opening remark every prime factor of N leaves remainder 1 or 5 on division by 6. Now a product of two numbers of the form $6a+1$ is again of that form, since

$$(6a+1)(6b+1)=36ab+6a+6b+1=6(6ab+a+b)+1,$$

and applying this one factor at a time shows that a product of *any* number of factors of the form $6a+1$ also leaves remainder 1 on division by 6. So if every prime factor of N were of the form $6a+1$, then N itself would leave remainder 1 on division by 6, contradicting the remainder 5 found above. Hence N has at least one prime factor p leaving remainder 5 on division by 6, that is, of the form $6k-1$. This p cannot be any q_i: if $p=q_i$ then $p \mid 6q_1\cdots q_m$ and $p \mid N$, so p would divide their difference $6q_1\cdots q_m - N = 1$, which is impossible. So p is a prime of the form $6k-1$ outside the list, contradicting completeness. Therefore there are infinitely many primes of the form $6k-1$, as required.

Q18. Fix an integer $n \geq 2$ and consider the $n-1$ consecutive integers $n!+2, n!+3, \ldots, n!+n$. Take any one of them, $n!+j$ with $2 \leq j \leq n$. Since $j \leq n$, the factorial $n! = 1\times 2\times \cdots \times n$ includes j as one of its factors, so $j \mid n!$; and clearly $j \mid j$. Hence $j \mid (n!+j)$. Because $2 \leq j \leq n < n!+j$, this j is a factor strictly between 1 and $n!+j$, so $n!+j$ is composite. As j ranges over $2, 3, \ldots, n$ this gives $n-1$ consecutive composite integers. Since n can be taken as large as we please, runs of consecutive composites can be made arbitrarily long, as required.

Theory

This section develops two families of "simple proof" that recur throughout Specialist Mathematics: proofs of **inequalities** between real numbers, and proofs that certain numbers are **irrational**. The two look very different, yet each turns on a single sharp idea — the first on the fact that a square is never negative, the second on the method of **proof by contradiction**. A proof is a sequence of logically valid steps, each justified by a definition or a result already established, and every proof below closes with a sentence stating that the required result has been reached.

Squares are never negative.

The foundation of every inequality in this section is one fact about the real numbers: for every real number t,

$$t^2 \geq 0,$$

with **equality if and only if** $t = 0$. This is immediate — a positive number and a negative number both square to something positive, and only 0 squares to 0. Trivial as it looks, it is the engine of the whole topic, because any expression that can be written as a square (or a sum of squares) is thereby known to be non-negative without any further calculation.

Proving an inequality by "considering a square".

To prove that one expression is greater than or equal to another, the standard strategy is to form their difference, recognise it as a square, and invoke $t^2 \geq 0$. The archetype is the inequality

$$a^2 + b^2 \geq 2ab,$$

true for **all** real numbers a and b. To prove it, *consider* the square $(a-b)^2$. Since it is a square it is non-negative:

$$(a-b)^2 \geq 0.$$

Expanding the left-hand side gives $a^2 - 2ab + b^2 \geq 0$, and adding $2ab$ to both sides rearranges this into $a^2 + b^2 \geq 2ab$. Because $(a-b)^2 = 0$ only when $a = b$, **equality holds precisely when** $a = b$.

The logic here runs in one direction only, and the direction matters. A valid proof *begins* from a statement already known to be true — here $(a-b)^2 \geq 0$ — and deduces the target by reversible algebra. It is **not** correct to start by assuming the very inequality to be proved and manipulate it until something true appears; that argues the wrong way round. The discipline "start from a square, expand, rearrange" keeps the logic flowing from the known to the required.

The arithmetic mean–geometric mean inequality.

For two non-negative numbers a and b, the **arithmetic mean** is $\frac{a+b}{2}$ and the **geometric mean** is $\sqrt{ab}$. The **AM–GM inequality** states that for all $a, b \geq 0$,

$$\frac{a+b}{2} \geq \sqrt{ab},$$

with equality if and only if $a = b$. It is proved by the same device, applied to a different square. Because $a, b \geq 0$, the numbers $\sqrt{a}$ and $\sqrt{b}$ are real, so $\left(\sqrt{a} - \sqrt{b}\right)^2 \geq 0$. Expanding, and using $\left(\sqrt{a}\right)^2 = a$, $\left(\sqrt{b}\right)^2 = b$ and $\sqrt{a}\sqrt{b} = \sqrt{ab}$,

$$a - 2\sqrt{ab} + b \geq 0 \Rightarrow a + b \geq 2\sqrt{ab},$$

and dividing by the positive number 2 gives $\frac{a+b}{2} \geq \sqrt{ab}$. Equality requires $\sqrt{a} = \sqrt{b}$, that is $a = b$. In words: **the average of two non-negative numbers is never smaller than their geometric mean.**

Related inequalities.

Many further inequalities are just $a^2+b^2\geq 2ab$ or AM–GM in disguise. For example, dividing $a^2+b^2\geq 2ab$ by the positive quantity ab (for $a,b>0$) gives

$$\frac{a}{b}+\frac{b}{a}\geq 2,$$

and setting $a=x$, $b=1$ in this (with $x>0$) gives the useful

$$x+\frac{1}{x}\geq 2,$$

each with equality when the two numbers involved are equal. The recurring move is always the same: locate a square that must be non-negative, then expand and rearrange.

Rational and irrational numbers.

A real number is **rational** if it can be written as a fraction $\frac{p}{q}$ with p and q integers and $q\neq 0$; the set of rationals is written $\mathbb{Q}$. A real number that is **not** rational is **irrational**. Every rational number can be written in **lowest terms**, meaning p and q are chosen with no common factor greater than 1 (any shared factor is cancelled first). This "lowest terms" assumption is the lever used in almost every irrationality proof.

Proving irrationality by contradiction.

To prove that a number is irrational one cannot check every possible fraction, so a direct approach is hopeless. Instead we argue by **contradiction**: *suppose* the number were rational, write it as a fraction in lowest terms, and reason until an impossibility appears. Since correct reasoning cannot produce an impossibility, the supposition must be false — and so the number is irrational.

The classic example is $\sqrt{2}$. Before giving it, note one small lemma that the argument needs: **if** 2 **divides** n^2 **then** 2 **divides** n (equivalently, the square of an odd number is odd, since $(2k+1)^2=2(2k^2+2k)+1$). With this in hand:

Suppose, for the sake of contradiction, that $\sqrt{2}$ is rational. Then $\sqrt{2}=\frac{p}{q}$ for some integers p,q with $q\neq 0$, and we may take the fraction in lowest terms, so p and q have no common factor greater than 1. Squaring gives $2=\frac{p^2}{q^2}$, hence

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

Thus p^2 is even, so by the lemma p is even; write $p=2m$. Substituting, $4m^2=2q^2$, so $q^2=2m^2$, which makes q^2 even and therefore q even as well. But then 2 divides both p and q, contradicting the choice of lowest terms. The supposition is false, so $\sqrt{2}$ **is irrational.**

The same template, and two variations.

The argument adapts unchanged to $\sqrt{3}$, $\sqrt{5}$, $\sqrt{6}$ and many more; only the supporting divisibility fact changes. For a prime r, the needed lemma is "**if** r **divides** n^2 **then** r **divides** n", which is checked by examining the possible remainders of n on division by r. Two variations are worth meeting:

- **Logarithms.** To show $\log_2 5$ is irrational, suppose it equals $\frac{p}{q}$ with p,q positive integers. Then $2^{p/q}=5$, so $2^p=5^q$; but 2^p is even while 5^q is odd, an impossibility. The clash is one of parity rather than of common factors.
- **A rational plus an irrational.** The sum of a rational number and an irrational number is always irrational. For if r is rational and x is irrational, and $r+x$ were rational, then $x=(r+x)-r$ would be a difference of two rationals and hence rational — contradicting that x is irrational.

In every case the shape of the argument is identical: assume rationality, extract a fraction in lowest terms (or a whole-number equation), and drive it to a contradiction.

Worked examples

Example 1 — scaffolded

Prove that $a^2+b^2\geq 2ab$ for all real numbers a and b, and state when equality holds.

Working	Comment
Let a and b be any real numbers. A square is never negative, so $(a-b)^2\geq 0$.	Begin from a square, which cannot be negative — the standard opening.
Expanding, $a^2-2ab+b^2\geq 0$.	Expand $(a-b)^2=a^2-2ab+b^2$.
Adding $2ab$ to both sides, $a^2+b^2\geq 2ab$.	Rearranging preserves the inequality; this is the target.
Equality holds exactly when $(a-b)^2=0$, that is when $a=b$.	A square equals 0 only when its base is 0.
Hence $a^2+b^2\geq 2ab$ for all real a,b, with equality if and only if $a=b$, as required.	Concluding statement.

Example 2 — scaffolded

Prove the AM–GM inequality for two numbers: for all $a,b\geq 0$, $\dfrac{a+b}{2}\geq\sqrt{ab}$, and state when equality holds.

Working	Comment
Since $a,b\geq 0$, the numbers $\sqrt{a}$ and $\sqrt{b}$ are real, so $(\sqrt{a}-\sqrt{b})^2\geq 0$.	The square is defined precisely because a and b are non-negative.
Expanding, $a-2\sqrt{ab}+b\geq 0$.	Use $(\sqrt{a})^2=a$, $(\sqrt{b})^2=b$ and $\sqrt{a}\sqrt{b}=\sqrt{ab}$.
So $a+b\geq 2\sqrt{ab}$.	Add $2\sqrt{ab}$ to both sides.
Dividing by 2, $\dfrac{a+b}{2}\geq\sqrt{ab}$.	Dividing by the positive number 2 preserves the inequality.
Equality holds when $\sqrt{a}=\sqrt{b}$, that is when $a=b$.	The square is zero only when its base $\sqrt{a}-\sqrt{b}$ is zero.
Thus the arithmetic mean is at least the geometric mean, with equality if and only if $a=b$, as required.	Name the result and conclude.

Example 3 — unscaffolded

Prove that $\sqrt{5}$ is irrational.

Suppose, for the sake of contradiction, that $\sqrt{5}$ is rational. Then it can be written as $\sqrt{5}=\dfrac{m}{n}$ for integers m,n with $n\neq 0$, and we may take the fraction in lowest terms, so m and n have no common factor greater than 1. Squaring both sides gives $5=\dfrac{m^2}{n^2}$, and therefore

$$m^2=5n^2.$$

Hence 5 divides m^2. Now 5 is prime, and if 5 did **not** divide m then m would leave one of the remainders $1,2,3,4$ on division by 5, whose squares leave remainders $1,4,4,1$ respectively — never 0. So $5\mid m^2$ forces $5\mid m$; write $m=5k$ for some integer k. Substituting, $25k^2=5n^2$, so

$$n^2=5k^2,$$

which shows $5 \mid n^2$ and hence, by the same reasoning, $5 \mid n$. But then 5 divides both m and n, contradicting the assumption that the fraction was in lowest terms. This contradiction shows the supposition was false, so $\sqrt{5}$ is irrational, as required.

Example 4 — unscaffolded

Prove that $\log_2 5$ is irrational.

Suppose, for the sake of contradiction, that $\log_2 5$ is rational. Since $5 > 1$ we have $\log_2 5 > 0$, so it may be written as $\log_2 5 = \dfrac{p}{q}$ with p and q positive integers. By the definition of a logarithm this means $2^{p/q} = 5$, and raising both sides to the power q gives

$$2^p = 5^q.$$

The left-hand side 2^p is even, because $p \geq 1$. The right-hand side 5^q is a product of the odd number 5 with itself and so is odd. An even number cannot equal an odd number, so we have reached a contradiction. The supposition is therefore false, and $\log_2 5$ is irrational, as required.

Practice questions

Scaffolded

Q1. Prove that $x^2 + 25 \geq 10x$ for every real number x, and state when equality holds. (a) Write down a square involving x and 5 that must be non-negative. (b) Expand that square. (c) Rearrange to obtain $x^2 + 25 \geq 10x$. (d) State the value of x for which equality holds.

Q2. Prove that $2(a^2 + b^2) \geq (a + b)^2$ for all real numbers a and b. (a) Start from $(a - b)^2 \geq 0$ and expand it. (b) Expand $(a + b)^2$. (c) Show that $2(a^2 + b^2) - (a + b)^2$ equals $(a - b)^2$. (d) Conclude, and state when equality holds.

Q3. Prove that $\dfrac{a}{b} + \dfrac{b}{a} \geq 2$ for all $a, b > 0$. (a) Write $\dfrac{a}{b} + \dfrac{b}{a}$ as a single fraction. (b) Identify the numerator and apply the inequality $a^2 + b^2 \geq 2ab$. (c) Simplify the resulting fraction. (d) State when equality holds.

Q4. Prove that $\sqrt{3}$ is irrational. (a) Assume $\sqrt{3} = \dfrac{p}{q}$ in lowest terms and square both sides. (b) Show that $p^2 = 3q^2$ and deduce that $3 \mid p$. (c) Write $p = 3m$ and deduce that $3 \mid q$. (d) Explain the contradiction and state the conclusion.

Q5. Given that $\sqrt{2}$ is irrational, prove that $4 + \sqrt{2}$ is irrational. (a) Suppose, for contradiction, that $4 + \sqrt{2}$ is rational. (b) Make $\sqrt{2}$ the subject. (c) Explain why the right-hand side would then be rational. (d) State the contradiction and the conclusion.

Q6. Prove that $x + \dfrac{9}{x} \geq 6$ for all $x > 0$, and state when equality holds. (a) Explain why $\left(\sqrt{x} - \dfrac{3}{\sqrt{x}}\right)^2 \geq 0$. (b) Expand this square. (c) Rearrange to obtain $x + \dfrac{9}{x} \geq 6$. (d) State the value of x for which equality holds.

Unscaffolded

Q7. Prove that $x^2 + 49 \geq 14x$ for every real number x.

Q8. Prove that $a^2 + b^2 \geq 2ab$ for all real a, b, and hence prove that $a^4 + b^4 \geq 2a^2b^2$.

Q9. Prove that $(a + b)\left(\dfrac{1}{a} + \dfrac{1}{b}\right) \geq 4$ for all $a, b > 0$.

Q10. Prove that $x+\frac{1}{x}\geq 2$ for all $x>0$, and state when equality holds.

Q11. Prove that $a+b\geq 2\sqrt{ab}$ for all $a,b\geq 0$.

Q12. Prove that $\frac{a^2}{b}+b\geq 2a$ for all $a,b>0$, and hence prove that $\frac{a^2}{b}+\frac{b^2}{a}\geq a+b$.

Q13. Prove that $\sqrt{7}$ is irrational.

Q14. Prove that $\sqrt{6}$ is irrational.

Q15. Prove that $\log_2 7$ is irrational.

Q16. Prove that the sum of a rational number and an irrational number is irrational.

Q17. Given that $\sqrt{6}$ is irrational, prove that $\sqrt{2}+\sqrt{3}$ is irrational.

Q18. Prove that $(a+b)^2\geq 4ab$ for all real a,b, and hence show that if two positive numbers a and b satisfy $a+b=10$ then $ab\leq 25$. State when equality holds.

Answers

Q1. Proof — from $(x-5)^2 \geq 0$; equality at $x=5$. See solutions. **Q2.** Proof — $2(a^2+b^2)-(a+b)^2=(a-b)^2 \geq 0$; equality when $a=b$. See solutions. **Q3.** Proof — $\frac{a}{b}+\frac{b}{a}=\frac{a^2+b^2}{ab} \geq \frac{2ab}{ab}=2$; equality when $a=b$. See solutions. **Q4.** Proof by contradiction — $p^2=3q^2$ forces $3 \mid p$ and $3 \mid q$, contradicting lowest terms. See solutions. **Q5.** Proof by contradiction — $\sqrt{2}=(4+\sqrt{2})-4$ would be rational. See solutions. **Q6.** Proof — from $(\sqrt{x}-3/\sqrt{x})^2 \geq 0$; equality at $x=3$. See solutions. **Q7.** Proof — from $(x-7)^2 \geq 0$. See solutions. **Q8.** Proof — from $(a-b)^2 \geq 0$; then apply $a^2+b^2 \geq 2ab$ with a^2, b^2 in place of a, b. See solutions. **Q9.** Proof — expands to $2+\frac{a}{b}+\frac{b}{a} \geq 4$. See solutions. **Q10.** Proof — from $(\sqrt{x}-1/\sqrt{x})^2 \geq 0$; equality at $x=1$. See solutions. **Q11.** Proof — from $(\sqrt{a}-\sqrt{b})^2 \geq 0$. See solutions. **Q12.** Proof — $\frac{a^2}{b}+b-2a=\frac{(a-b)^2}{b} \geq 0$; sum the two versions. See solutions. **Q13.** Proof by contradiction — $p^2=7q^2$ forces $7 \mid p$ and $7 \mid q$. See solutions. **Q14.** Proof by contradiction — $p^2=6q^2$ forces $2 \mid p$ and $2 \mid q$. See solutions. **Q15.** Proof by contradiction — $2^p=7^q$ makes an even number equal an odd number. See solutions. **Q16.** Proof by contradiction — $x=(r+x)-r$ would be rational. See solutions. **Q17.** Proof by contradiction — $(\sqrt{2}+\sqrt{3})^2=5+2\sqrt{6}$ would make $\sqrt{6}$ rational. See solutions. **Q18.** Proof — $(a+b)^2-4ab=(a-b)^2 \geq 0$; with $a+b=10$, $ab \leq 25$, equality at $a=b=5$. See solutions.

Fully-worked solutions

Q1. A square is never negative, so $(x-5)^2 \geq 0$. Expanding, $x^2-10x+25 \geq 0$, and adding $10x$ to both sides gives $x^2+25 \geq 10x$. This holds for every real x, and equality occurs exactly when $(x-5)^2=0$, that is when $x=5$, as required.

Q2. Since a square is never negative, $(a-b)^2 \geq 0$, so $a^2-2ab+b^2 \geq 0$. Also $(a+b)^2=a^2+2ab+b^2$. Subtracting,

$$2(a^2+b^2)-(a+b)^2=2a^2+2b^2-a^2-2ab-b^2=a^2-2ab+b^2=(a-b)^2 \geq 0.$$

Hence $2(a^2+b^2) \geq (a+b)^2$ for all real a, b, with equality when $a=b$, as required.

Q3. For $a, b>0$, combine over a common denominator:

$$\frac{a}{b}+\frac{b}{a}=\frac{a^2+b^2}{ab}.$$

By the inequality $a^2+b^2 \geq 2ab$ and since $ab>0$,

$$\frac{a^2+b^2}{ab} \geq \frac{2ab}{ab}=2.$$

Therefore $\frac{a}{b}+\frac{b}{a} \geq 2$, with equality when $a^2+b^2=2ab$, that is when $a=b$, as required.

Q4. Suppose, for contradiction, that $\sqrt{3}$ is rational, say $\sqrt{3}=\frac{p}{q}$ in lowest terms, so p and q have no common factor greater than 1. Squaring, $3=\frac{p^2}{q^2}$, hence $p^2=3q^2$, so $3 \mid p^2$. If 3 did not divide p, then p would leave remainder 1 or 2 on division by 3, and p^2 would leave remainder 1 — not 0. So $3 \mid p^2$ forces $3 \mid p$; write $p=3m$. Then $9m^2=3q^2$, so $q^2=3m^2$ and hence $3 \mid q$ by the same reasoning. But then 3 divides both p and q, contradicting lowest terms. Therefore $\sqrt{3}$ is irrational, as required.

Q5. Suppose, for contradiction, that $4+\sqrt{2}$ is rational, say $4+\sqrt{2}=r$ with r rational. Making $\sqrt{2}$ the subject, $\sqrt{2}=r-4$. The right-hand side is a difference of two rational numbers and so is rational. Thus $\sqrt{2}$ would be rational, contradicting the given fact that $\sqrt{2}$ is irrational. Therefore $4+\sqrt{2}$ is irrational, as required.

Q6. Since $x>0$, the number $\sqrt{x}$ is real and positive, so $\left(\sqrt{x}-\frac{3}{\sqrt{x}}\right)^2\geq 0$. Expanding,

$$\left(\sqrt{x}-\frac{3}{\sqrt{x}}\right)^2=x-2\cdot\sqrt{x}\cdot\frac{3}{\sqrt{x}}+\frac{9}{x}=x-6+\frac{9}{x}\geq 0.$$

Adding 6 to both sides gives $x+\frac{9}{x}\geq 6$. Equality holds when $\sqrt{x}=\frac{3}{\sqrt{x}}$, that is $x=3$, as required.

Q7. A square is never negative, so $(x-7)^2\geq 0$, giving $x^2-14x+49\geq 0$. Adding $14x$ to both sides, $x^2+49\geq 14x$ for every real x, as required.

Q8. From $(a-b)^2\geq 0$ we get $a^2-2ab+b^2\geq 0$, so $a^2+b^2\geq 2ab$ for all real a,b. Now apply this with a^2 and b^2 in place of a and b (both are real): $(a^2)^2+(b^2)^2\geq 2(a^2)(b^2)$, that is

$$a^4+b^4\geq 2a^2b^2,$$

as required. (Equivalently, $a^4+b^4-2a^2b^2=(a^2-b^2)^2\geq 0$.)

Q9. Expanding the product for $a,b>0$,

$$(a+b)\left(\frac{1}{a}+\frac{1}{b}\right)=1+\frac{a}{b}+\frac{b}{a}+1=2+\frac{a}{b}+\frac{b}{a}.$$

By the result of Q3, $\frac{a}{b}+\frac{b}{a}\geq 2$, so the expression is at least $2+2=4$. Therefore $(a+b)\left(\frac{1}{a}+\frac{1}{b}\right)\geq 4$, with equality when $a=b$, as required.

Q10. Since $x>0$, we have $\left(\sqrt{x}-\frac{1}{\sqrt{x}}\right)^2\geq 0$. Expanding,

$$x-2+\frac{1}{x}\geq 0,$$

so $x+\frac{1}{x}\geq 2$. Equality holds when $\sqrt{x}=\frac{1}{\sqrt{x}}$, that is $x=1$, as required.

Q11. Since $a,b\geq 0$, the numbers $\sqrt{a}$ and $\sqrt{b}$ are real, so $\left(\sqrt{a}-\sqrt{b}\right)^2\geq 0$. Expanding, $a-2\sqrt{ab}+b\geq 0$, and adding $2\sqrt{ab}$ to both sides gives $a+b\geq 2\sqrt{ab}$, with equality when $a=b$, as required.

Q12. For $a,b>0$, consider

$$\frac{a^2}{b}+b-2a=\frac{a^2+b^2-2ab}{b}=\frac{(a-b)^2}{b}\geq 0,$$

since $(a-b)^2\geq 0$ and $b>0$. Hence $\frac{a^2}{b}+b\geq 2a$. By symmetry (swap a and b), $\frac{b^2}{a}+a\geq 2b$. Adding the two inequalities,

$$\frac{a^2}{b}+\frac{b^2}{a}+(a+b)\geq 2a+2b,$$

and subtracting $a+b$ from both sides gives $\frac{a^2}{b}+\frac{b^2}{a}\geq a+b$, as required.

Q13. Suppose, for contradiction, that $\sqrt{7}$ is rational, say $\sqrt{7}=\frac{p}{q}$ in lowest terms. Squaring, $p^2=7q^2$, so $7\mid p^2$. Since 7 is prime, if 7 did not divide p then p would leave one of the remainders $1,2,3,4,5,6$ on division by 7, whose squares leave remainders $1,4,2,2,4,1$ respectively — none equal to 0. So $7\mid p^2$ forces $7\mid p$; write $p=7m$. Then $49m^2=7q^2$, so $q^2=7m^2$ and hence $7\mid q$. But then 7 divides both p and q, contradicting lowest terms. Therefore $\sqrt{7}$ is irrational, as required.

Q14. Suppose, for contradiction, that $\sqrt{6}$ is rational, say $\sqrt{6}=\frac{p}{q}$ in lowest terms. Squaring, $p^2=6q^2=2(3q^2)$, so p^2 is even and hence p is even; write $p=2m$. Then $4m^2=6q^2$, so $2m^2=3q^2$. The left side is even, so $3q^2$ is even; as 3 is odd this forces q^2 to be even, and hence q is even. But then 2 divides both p and q, contradicting lowest terms. Therefore $\sqrt{6}$ is irrational, as required.

Q15. Suppose, for contradiction, that $\log_2 7$ is rational. Since $7>1$, $\log_2 7>0$, so we may write $\log_2 7=\frac{p}{q}$ with p,q positive integers. Then $2^{p/q}=7$, and raising both sides to the power q gives $2^p=7^q$. The left side 2^p is even (as $p\geq 1$), while the right side 7^q is a product of odd numbers and so is odd. An even number cannot equal an odd number, a contradiction. Therefore $\log_2 7$ is irrational, as required.

Q16. Let r be a rational number and x an irrational number, and suppose, for contradiction, that $s=r+x$ is rational. Then $x=s-r$. If $s=\frac{a}{b}$ and $r=\frac{c}{d}$ with $b,d\neq 0$, then

$$x=s-r=\frac{ad-bc}{bd},$$

a ratio of integers with non-zero denominator, hence rational. This contradicts the assumption that x is irrational. Therefore $r+x$ is irrational, as required.

Q17. Suppose, for contradiction, that $\sqrt{2}+\sqrt{3}$ is rational, say $\sqrt{2}+\sqrt{3}=r$ with r rational. Squaring both sides,

$$r^2=(\sqrt{2}+\sqrt{3})^2=2+2\sqrt{6}+3=5+2\sqrt{6}.$$

Making $\sqrt{6}$ the subject, $\sqrt{6}=\frac{r^2-5}{2}$. Since r is rational, so are r^2 and $\frac{r^2-5}{2}$, which would make $\sqrt{6}$ rational — contradicting the given fact that $\sqrt{6}$ is irrational. Therefore $\sqrt{2}+\sqrt{3}$ is irrational, as required.

Q18. A square is never negative, so $(a-b)^2\geq 0$, giving $a^2-2ab+b^2\geq 0$. Adding $4ab$ to both sides,

$$a^2+2ab+b^2\geq 4ab, \text{ that is } (a+b)^2\geq 4ab.$$

Now suppose $a,b>0$ with $a+b=10$. Then $(a+b)^2=100$, so $100\geq 4ab$ and hence $ab\leq 25$. Equality holds when $a=b$, which with $a+b=10$ gives $a=b=5$, as required.