Lesson - Proof by induction

Year: Further Maths

Mathematical induction proves that a statement $P(n)$ is true for **every** integer $n \geq n_0$, usually $n \geq 1$. It works like a line of dominoes: if the first falls, and each one knocks over the next, then all of them fall.

Starter activity

Line up a row of dominoes on a table. What do you need to be sure of in order to know that every domino will fall, however long the row is? Most people quickly agree on two things: the first domino must be pushed, and each domino must be close enough to knock over the next one. Now think about the statement "$1 + 3 + 5 + \cdots + (2n - 1) = n^2$". Check it for the first few values of n. Checking cannot cover every case, so how could the two domino conditions be turned into a proof?

The structure of a proof

Definition: proof by induction

A proof by **mathematical induction** shows that $P(n_0)$ is true (the basis) and that, whenever $P(k)$ is true, $P(k+1)$ is also true (the inductive step). Then $P(n)$ is true for all $n \geq n_0$.

Method: the four steps

1. **Basis:** show $P(n_0)$ is true by substituting $n = n_0$ into both sides.
2. **Assumption:** assume $P(k)$ is true for some integer $k \geq n_0$.
3. **Inductive step:** using the assumption, show that $P(k+1)$ is true.
4. **Conclusion:** "If true for $n = k$ then true for $n = k + 1$. True for $n = 1$, so by mathematical induction true for all positive integers n."

Watch out

- Never write "assume true for all k"; that is what has to be proved. Say "for some integer $k \geq 1$".
- Do not forget the basis, or check it for the wrong n.
- The conclusion sentence carries a mark.

Summation of series

Rule: adding one more term

$\sum_{r=1}^{k+1} f(r) = \sum_{r=1}^{k} f(r) + f(k+1)$. Replace the first part using the assumption, then manipulate until you reach the formula with n replaced by $k+1$. Write the target first and factorise rather than expand.

Example 1

Prove that $\sum_{r=1}^{n} r^2 = \frac{1}{6}n(n+1)(2n+1)$.

Basis $n = 1$: LHS $= 1$, RHS $= \frac{1}{6} \cdot 1 \cdot 2 \cdot 3 = 1$. True.

Assume true for $n = k$: $\sum_{r=1}^{k} r^2 = \frac{1}{6}k(k+1)(2k+1)$.

Then $\sum_{r=1}^{k+1} r^2 = \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 = \frac{1}{6}(k+1)\left[k(2k+1) + 6(k+1)\right] = \frac{1}{6}(k+1)(2k^2+7k+6) = \frac{1}{6}(k+1)(k+2)(2k+3)$, which is the formula with $n = k+1$. So true for $n = k+1$; with the basis, true for all $n \geq 1$.

Divisibility

Method: divisibility proofs

1. Let $f(n)$ be the expression and check $f(n_0)$ is a multiple of the divisor.
2. Assume $f(k) = md$ for an integer m (where d is the divisor).
3. Compute $f(k+1) - af(k)$ for a suitable constant a, usually the base of the power.
4. Show the result is a multiple of d, so $f(k+1)$ is too.

Example 2

Prove that $f(n) = 7^n + 5$ is divisible by 6 for $n \geq 1$.

$f(1) = 12 = 6 \times 2$. Assume $f(k) = 6m$. Then $f(k+1) - f(k) = 7^{k+1} - 7^k = 6 \cdot 7^k$, so $f(k+1) = 6m + 6 \cdot 7^k = 6(m + 7^k)$, which is divisible by 6. Hence true for all $n \geq 1$.

Matrix powers

Method: matrix powers

1. Calculate $\mathbf{M}^1, \mathbf{M}^2$ and conjecture the pattern for $\mathbf{M}^n$.
2. Check the basis case.
3. Assume the formula for $\mathbf{M}^k$ and write $\mathbf{M}^{k+1} = \mathbf{M}^k\mathbf{M}$.
4. Multiply out, showing every entry, and match the formula for $k+1$.

Example 3

Prove that $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix}$.

Basis $n = 1$ is immediate. If true for k, then $\begin{pmatrix} 1 & 2k \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2+2k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2(k+1) \\ 0 & 1 \end{pmatrix}$. Done.

Recurrence relations, inequalities and derivatives

Key fact: variations

- For $u_{n+1} = g(u_n)$, assume the closed form for u_k and substitute into g.
- For $u_{n+2} = au_{n+1} + bu_n$ you need *two* base cases and the assumption for $n = k$ and $n = k+1$ (two-step induction).
- For inequalities, keep track of the direction when you multiply or add; the basis may start at $n_0 > 1$.
- For nth derivatives, assume the pattern for $\dfrac{d^k y}{dx^k}$ and differentiate once more.

Example 4: recurrence

Given $u_1 = 4$ **and** $u_{n+1} = 2u_n - 3$**, prove that** $u_n = 2^{n-1} + 3$**.**

Basis: $2^0 + 3 = 4$. Assume $u_k = 2^{k-1} + 3$. Then $u_{k+1} = 2(2^{k-1} + 3) - 3 = 2^k + 3$, the formula with $n = k+1$. The conjecture came from calculating $u_2 = 5,\ u_3 = 7,\ u_4 = 11$: the differences from 3 are $1, 2, 4, 8$, a doubling pattern.

Example 5: inequality

Prove that $2^n \geq n + 1$ **for** $n \geq 1$**.**

Basis $n = 1$: $2 \geq 2$. Assume $2^k \geq k + 1$. Then $2^{k+1} = 2 \times 2^k \geq 2(k+1) = 2k + 2 \geq k + 2$ since $k \geq 0$. So true for $n = k + 1$.

Note: marks

Marks are usually 1 for the basis, 1 for the assumption, 2 or 3 for the algebra and 1 for the conclusion. For divisibility say clearly "where m is an integer".

More methods and worked examples

Method: writing a complete induction proof

1. **Basis.** Show clearly that the statement is true for the first value, usually $n = 1$, by working out both sides separately.

2. **Assumption.** Write "Assume the statement is true for $n = k$" and copy the statement with k in place of n.
3. **Inductive step.** Use the assumption to show that the statement is true for $n = k + 1$. Write down what you are aiming for, so that you can see when you have reached it.
4. **Conclusion.** State that the result is true for the first value, that truth for $n = k$ implies truth for $n = k + 1$, and hence that it is true for all the required values of n.

Worked example 6: the sum of odd numbers

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

For $n = 1$ the left side is 1 and the right side is $1^2 = 1$, so the statement is true. Assume that $\sum_{r=1}^{k}(2r-1) = k^2$. Adding the next term, which is $2(k+1) - 1 = 2k + 1$, gives $\sum_{r=1}^{k+1}(2r-1) = k^2 + 2k + 1 = (k+1)^2$. This is the statement with $n = k + 1$. Since the statement is true for $n = 1$, and if it is true for $n = k$ then it is true for $n = k + 1$, it is true for all positive integers by induction. A picture explains the result: each odd number is an L-shaped border that turns a square of side k into a square of side $k + 1$.

Worked example 7: divisibility using a difference

Prove that $8^n - 3^n$ is divisible by 5 for all positive integers n.

Let $f(n) = 8^n - 3^n$. Then $f(1) = 5$, which is divisible by 5. Assume that $f(k) = 5m$ for some integer m. Then $f(k+1) = 8 \cdot 8^k - 3 \cdot 3^k = 8(8^k - 3^k) + 8 \cdot 3^k - 3 \cdot 3^k = 8f(k) + 5 \cdot 3^k$. Both terms are multiples of 5, so $f(k+1)$ is divisible by 5. The key idea is to split off a multiple of $f(k)$ and check that what remains is a multiple of the divisor. Another way is to work out $f(k+1) - 8f(k)$ directly, which gives the same result.

Worked example 8: a sequence defined by a recurrence

Given that $u_1 = 1$ and $u_{n+1} = u_n + 2n + 1$, prove that $u_n = n^2$.

For $n = 1$ the formula gives $1^2 = 1 = u_1$. Assume that $u_k = k^2$. Then $u_{k+1} = k^2 + 2k + 1 = (k+1)^2$, so the formula is true for $n = k + 1$. By induction, $u_n = n^2$ for all positive integers n. Notice that the recurrence relation provides the link between consecutive terms, so the inductive step is often just one line of algebra. The work is in guessing the formula, which can be done by calculating the first few terms.

Watch out: common errors in induction proofs

Do not assume what you are trying to prove. In the inductive step you may use the statement for $n = k$, but not for $n = k + 1$. Do not stop after showing a few cases: checking $n = 1, 2, 3$ is evidence, not a proof. Write a full conclusion, because

examiners usually reserve a mark for it, and it must refer to both the basis and the inductive step. In divisibility proofs, the expression you finish with must be shown to be a multiple of the divisor, for example $5(6m-4)$, rather than simply described as divisible. Finally, take care with the first value: an inequality such as $n! > 2^n$ needs a basis of $n = 4$, because it is false for smaller values.

Why induction is a valid method

Induction rests on a basic property of the positive integers: every non-empty set of positive integers has a smallest element. Suppose a statement satisfied both the basis and the inductive step, but failed for some values. Then there would be a smallest value m for which it failed. Since the basis holds, m is greater than 1, so the statement is true for $m-1$. The inductive step then makes it true for m, which is a contradiction. So the statement cannot fail anywhere. This argument shows that induction is a form of proof by contradiction, and it explains why both parts of the proof are essential.

Strong induction and other variations

Sometimes the step from k to $k+1$ needs more than the previous case. For a sequence such as the Fibonacci numbers, where each term depends on the two before it, we check two basis cases and assume the result for both $n = k-1$ and $n = k$. In other problems the statement starts at a different value, such as $n = 2$ or $n = 5$, or covers only even numbers, in which case the inductive step goes from k to $k+2$. The structure is always the same: a starting point, and a rule that carries the truth from one case to the next case that you need.

Did you know?

The first clear use of mathematical induction is often credited to the French mathematician Blaise Pascal, who used it in 1654 to prove properties of the number triangle that now carries his name, although earlier scholars, including al-Karaji in Baghdad around the year 1000, used similar arguments. The name induction was given by Augustus De Morgan in 1838. Induction is now used every day by computer scientists to prove that programs and loops always give the right answer, however many times they run.

Otto's tip

Before expanding anything, write the target expression for $n = k+1$ at the side of the page. Then you know exactly what to factorise towards.