Lesson - Proof by contradiction

Year: Year 13

In a proof by contradiction you assume that the statement you want to prove is **false**, then use correct algebra and logic to reach something impossible. This is a core A level technique, and the specification requires the proofs that $\sqrt{2}$ is irrational and that there are infinitely many primes.

Starter activity

Try to find two whole numbers a and b so that $a^2 = 2b^2$. Make a table for $b = 1, 2, 3, \ldots, 10$ and compare $2b^2$ with the nearest square. Do you ever get a perfect match? What does this suggest about $\sqrt{2}$? Why does a long table not prove it?

What is proof by contradiction?

Definition: proof by contradiction

A **proof by contradiction** (*reductio ad absurdum*) assumes the opposite of the statement, deduces something that cannot be true (an integer that is both odd and even, or a fraction both in and not in its lowest terms), and concludes that the original statement must be true, because every step was valid and so only the assumption can be wrong.

Method: structure of a proof by contradiction

1. **Assume the opposite**: "Assume, for contradiction, that ...".
2. **Work forwards** using definitions (even means $2k$, odd means $2k + 1$, rational means $\frac{a}{b}$).
3. **Reach a contradiction** and say exactly what is contradicted.
4. **Conclude**: "This is a contradiction, so the assumption is false and therefore ...".

Note: marks

Marks are awarded for each of the four stages, so never skip the assumption or the final sentence.

Negating statements

Rule: negations

- "n is even" becomes "n is odd"; "x is rational" becomes "x is irrational".

- "There are infinitely many primes" becomes "there are finitely many primes".
- "For all x, $P(x)$" becomes "there exists an x such that $P(x)$ is false".
- "$a \leq b$" becomes "$a > b$".

Watch out

Writing the wrong negation is the most common reason for losing marks. Do not assume what you want to prove: assume its opposite.

Useful facts

Key fact: results to quote

- If n^2 is even then n is even. (If n were odd, $n = 2k + 1$ and $n^2 = 4k^2 + 4k + 1$ would be odd.)
- The sum or product of integers is an integer; the product of an even integer and any integer is even.
- Every integer greater than 1 is prime or a product of primes, so it has a prime factor.
- If a prime p divides both N and $N - 1$, it divides their difference 1, which is impossible.

Proving $\sqrt{2}$ is irrational

Worked example 1

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

Assume $\sqrt{2}$ is rational. Then $\sqrt{2} = \frac{a}{b}$ where a, b are integers with no common factor (lowest terms) and $b \neq 0$. Squaring gives $a^2 = 2b^2$. Hence a^2 is even, so a is even and $a = 2k$. Then $4k^2 = 2b^2$, so $b^2 = 2k^2$, hence b^2 is even and b is even. Now both a and b are even, so they have a common factor 2. This contradicts the assumption that $\frac{a}{b}$ was in lowest terms. Therefore $\sqrt{2}$ is irrational. ■

Infinitely many primes

Worked example 2

Prove that there are infinitely many primes.

Assume there are finitely many primes $p_1, p_2, \ldots, p_k$. Let $N = p_1 p_2 \cdots p_k + 1$. Then $N > 1$, so N has a prime factor, which must be one of the p_i. That prime divides $p_1 p_2 \cdots p_k$ and also N, so it divides $N - p_1 \cdots p_k = 1$. No prime divides 1. This is a contradiction, so there are infinitely many primes. ■

Watch out

Do not claim N itself is prime: $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \times 509$. The argument only needs that N has a prime factor *not on the list*.

Other proofs by contradiction

Worked example 3

Prove that if x is rational and y is irrational then $x + y$ is irrational.

Assume $x + y$ is rational: $x + y = \frac{p}{q}$ and $x = \frac{r}{s}$ with integers p, q, r, s, $q, s \neq 0$. Then $y = \frac{p}{q} - \frac{r}{s} = \frac{ps - qr}{qs}$, a ratio of integers with $qs \neq 0$, so y is rational. This contradicts y being irrational. Hence $x + y$ is irrational. ■

Worked example 4

Prove that there are no integers m, n with $14m + 21n = 1$.

Assume there are. Then $7(2m + 3n) = 1$, so $2m + 3n = \frac{1}{7}$, but $2m + 3n$ is an integer. This is a contradiction. ■

Contradiction versus counterexample

Key fact: disproving and proving

To **disprove** a statement one counterexample is enough: for "$n^2 + n + 41$ is prime for all positive integers n", $n = 40$ gives 41^2, not prime. To **prove** a statement for all cases, examples are never enough: use algebra, deduction or contradiction.

Watch out

A calculator decimal never proves irrationality. In the $\sqrt{2}$ proof, forgetting "lowest terms" leaves no contradiction. Always finish with a conclusion in words.

Choosing a proof by contradiction

Note: when to use contradiction

Contradiction works best when the statement is a negative one ("there is no ...", "... is irrational", "... is not divisible by ...") or when a direct proof would have to deal with infinitely many cases. Assuming the opposite hands you an extra fact to work with: in the proof that $\sqrt{2}$ is irrational, you get the equation $\sqrt{2} = \frac{a}{b}$ that you can then square and manipulate. A direct proof would have nothing to start from. A good habit is to

ask: "if this were false, what would I be able to write down?"

Worked example 5: irrationality of the square root of 3

Prove that $\sqrt{3}$ is irrational.

Assume $\sqrt{3} = \frac{a}{b}$ with integers a, b in lowest terms, $b \neq 0$. Then $a^2 = 3b^2$, so $3 \mid a^2$. If $3 \nmid a$ then $a = 3k \pm 1$ and $a^2 = 9k^2 \pm 6k + 1$ leaves remainder 1 when divided by 3, a contradiction, so $3 \mid a$. Write $a = 3k$: $9k^2 = 3b^2$, so $b^2 = 3k^2$ and $3 \mid b$ by the same argument. So 3 divides both a and b, contradicting lowest terms. Hence $\sqrt{3}$ is irrational. ■

Worked example 6: there is no smallest positive rational

Prove that there is no smallest positive rational number.

Assume there is a smallest positive rational number r. Then $\frac{r}{2}$ is also rational and positive. But $\frac{r}{2} < r$ since $r > 0$. This contradicts r being the smallest. Hence there is no smallest positive rational number. ■ The same idea shows there is no largest integer: if n were the largest, $n + 1$ would be larger.

Worked example 7: a logarithm that is irrational

Prove that $\log_2 3$ is irrational.

Assume $\log_2 3 = \frac{p}{q}$ with positive integers p, q. Then $2^{p/q} = 3$, so $2^p = 3^q$. The left-hand side is even, since $p \geq 1$, and the right-hand side is odd, being a product of odd numbers. An integer cannot be both even and odd, so this is a contradiction. ■

Worked example 8: a cubic with no rational root

Prove that $x^3 + x + 1 = 0$ has no rational roots.

Assume the root is $\frac{p}{q}$ in lowest terms. Multiply by q^3: $p^3 + pq^2 + q^3 = 0$. At least one of p, q is odd. If both are odd, the three terms are odd, and their sum is odd. If p is even and q is odd, the terms are even, even, odd, so the sum is odd. If p is odd and q is even, the terms are odd, even, even, so the sum is odd. The sum is never 0, a contradiction. ■

Worked example 9: contradiction with an inequality

Prove that there are no real numbers x with $x^2 - 6x + 10$.

Assume there is such an x. Complete the square: $x^2 - 6x + 10 = (x - 3)^2 + 1$. Then $(x - 3)^2 + 1$ gives $(x - 3)^2$. But the square of a real number is never negative. This is

a contradiction. ■ In fact $x^2 - 6x + 10 \geq 1$ for all real x.

Worked example 10: a flaw spotted in a proof

A student argues: "Assume there is a largest prime P. Let $N = P + 1$. Then N is bigger than P, so N is not prime, so there is a contradiction." Explain what is wrong.

The student has not shown that N is composite or has a prime factor larger than P. For example, if $P = 2$ then $N = 3$ is prime. In Euclid's proof N is built as $p_1 p_2 \cdots p_k + 1$ so that it has remainder 1 on division by every listed prime, which forces a new prime factor. Always check that every step follows from the previous one.

Method: writing the proof out in full

1. Write the statement to be proved, then its negation, and begin with the words "Assume, for contradiction, that ...".
2. Introduce letters for the objects (such as integers a and b in lowest terms) and say what you know about them.
3. Take each logical step in a separate line, quoting any result you use, such as "if n^2 is even then n is even".
4. Arrive at a statement that clashes with an assumption or a known fact, and say exactly which one.
5. Conclude in words: "so the assumption is false, and therefore ...".

Examiners award marks for each of these stages, so keep them visible even in a short proof.

Watch out: marks lost in proofs by contradiction

- Not stating "lowest terms" when assuming $\sqrt{2} = \dfrac{a}{b}$: there is then no contradiction.
- Starting with the statement you want to prove instead of its negation.
- Using a decimal such as 1.414 as evidence: a finite decimal can never prove irrationality.
- Forgetting the concluding sentence: "this is a contradiction, so the assumption is false, and so ...".

Did you know?

The ancient Greek followers of Pythagoras believed that every length could be written as a ratio of whole numbers. Tradition says that a member of the group, Hippasus, found that the diagonal of a square could not be, and that this discovery was kept secret. The proof by contradiction you have just met is over two thousand years old, and Euclid's proof of the infinitude of primes is about 2300 years old. Both are still taught because they are perfect examples of mathematical reasoning.

Otto's tip

Before you start, write the first line "Assume, for contradiction, that ..." and the last line "This is a contradiction, so ...". Then fill in the middle.