

Some notes on constructing proofs

1. In a string of relations, the main news value should appear at the ends of the string and all of the intermediate steps should be easily verifiable.

If $r > 2$, then $r^2 + r - 6 = (r + 3)(r - 2) > 0$ ($r \in \mathbf{R}$). The point being made is that if r is greater than 2, then $r^2 + r - 6$ is positive. The equality $r^2 + r - 6 = (r + 3)(r - 2)$ is verified by multiplying out the right hand side; the inequality $(r + 3)(r - 2) > 0$ follows from the fact that both factors are positive under the assumption $r > 2$.

$(2 + 3)^2 = 5^2 = 25 \neq 13 = 4 + 9 = 2^2 + 3^2$. This says that $(2 + 3)^2 \neq 2^2 + 3^2$.

$\frac{1}{2} + \frac{2}{3} - \frac{1}{4} = \frac{6}{12} + \frac{8}{12} - \frac{3}{12} = \frac{11}{12} \notin \mathbf{Z}$. This says that $\frac{1}{2} + \frac{2}{3} - \frac{1}{4}$ is not an integer. It is confusing to the reader if this point is made by writing $\frac{11}{12} = \frac{6}{12} + \frac{8}{12} - \frac{3}{12} = \frac{1}{2} + \frac{2}{3} - \frac{1}{4} \notin \mathbf{Z}$. In working from left to right, he can easily check each step except for the last, $\frac{1}{2} + \frac{2}{3} - \frac{1}{4} \notin \mathbf{Z}$. For this, he has to work backwards to see that $\frac{1}{2} + \frac{2}{3} - \frac{1}{4}$ equals $\frac{11}{12}$ which is not an integer.

2. To prove a statement of the form “If P , then Q ” (which is the same as “ P implies Q ”), assume that P is true and show that Q is true.

If $a < b$ and $c < 0$ for $a, b, c \in \mathbf{R}$, then $ca > cb$. Proof: Assume that $a < b$ and $c < 0$ ($a, b, c \in \mathbf{R}$). Since $a < b$, we have $a - b < 0$. Therefore, $ca - cb = c(a - b) > 0$. Hence, $ca > cb$, as desired. \square

3. A statement of the form “ P if and only if Q ” is a combination of the two statements “If P , then Q ” and “If Q , then P ,” so it is often written with a double implication symbol: “ $P \iff Q$.” To prove it, take each implication separately and proceed as in (2).

$r^2 - 2r = -1$ if and only if $r = 1$ ($r \in \mathbf{R}$). Proof: (\implies) Assume $r^2 - 2r = -1$. Then $(r - 1)^2 = r^2 - 2r + 1 = 0$, which implies $r - 1 = 0$. Hence, $r = 1$. (\impliedby) Assume $r = 1$. Then $r^2 - 2r = 1^2 - 2(1) = -1$. \square

It is common to use (\implies) and (\impliedby) as above to introduce the particular implication being proved. Incidentally, you should convince yourself that (\impliedby) corresponds to the statement “ P if Q ” while (\implies) corresponds to the statement “ P only if Q .”

4. To show that a statement is false, provide a single, explicit counterexample.

For every positive real number r , we have $r^3 > r^2$. This statement is false, for if $r = \frac{1}{2}$, then $r^3 = \frac{1}{8} \not> \frac{1}{4} = r^2$. (I could also have said that the statement is false, for if r is any real number less than 1, then $r^3 - r^2 = r^2(r - 1) < 0$, whence $r^3 < r^2$. However, the explicit counterexample above is preferable to this argument in that it is easier to understand and it says just what needs to be said.)

5. To prove a statement involving “there exists,” just exhibit a single such object and show that it satisfies the stated property.

There exists an $r \in \mathbb{R}$ satisfying $r^2 + r - 12 = 0$. Proof: Let $r = 3$. Then, $r^2 + r - 12 = 3^2 + 3 - 12 = 0$. \square

Notice that I did not tell the reader how I came up with an r that works. There is no obligation to reveal the thought processes that lead to the insight. In fact, to do so risks confusing the reader since he is not expecting it. Also, I did not include that $r = -4$ also works since to demonstrate the truth of the statement requires only that I show the existence of at least one such r .

6. To prove a statement involving “for every,” start with an arbitrary such object and show that it satisfies the given property.

For every $r \in \mathbb{R}$ with $r \geq 3$, we have $r^2 - 2r + 1 \geq 4$. Proof: Let $r \in \mathbb{R}$ with $r \geq 3$. Then $r^2 - 2r + 1 = (r - 1)^2 \geq (3 - 1)^2 = 4$. \square

The first sentence of the proof means “Let r denote an arbitrary (i.e., any old) real number greater than or equal to 3.”

7. There is a method for proving a statement called “Proof by contradiction” which is sometimes useful. To use this method, one assumes that the given statement is false and then proceeds to derive a contradiction. The contradiction signals the presence somewhere of an invalid step. Therefore, provided all other steps are valid, one can conclude that the initial assumption was not correct, which is to say that the given statement is in fact true.

There are infinitely many prime numbers. (A prime number is an integer greater than 1 that is evenly divisible by no positive integers except 1 and itself (e.g., 2, 3, 5, 7, 11, ...).) Proof: Suppose the statement is false. In other words, suppose there are only finitely many primes. We may enumerate them: p_1, p_2, \dots, p_n . Consider the number $s := p_1 p_2 \cdots p_n + 1$. Now s is an integer greater than 1, so it must be divisible by some prime, say p_i . This means that $s = p_i m$ for some integer m . But then, $1 = s - p_1 p_2 \cdots p_n = p_i(m - p_1 p_2 \cdots \hat{p}_i \cdots p_n)$ where the symbol \hat{p}_i means “delete p_i .” The expression in the parentheses is just some integer and, since it is not possible to multiply the prime p_i by another integer and get 1, this is an obvious contradiction. Hence, our original assumption is wrong, that is, there are infinitely many prime numbers. \square

(This is essentially Euclid’s famous proof of the infinitude of primes.)

8. A statement of the form “If P , then Q ” is logically equivalent to the statement “If not Q , then not P ” meaning that one is true if and only if the other is true (you should be able to convince yourself that this is the case). This second statement is called the *contrapositive* of the first. Sometimes, proving the contrapositive of a statement is easier than proving the statement itself.

If $r \neq s$, then $2r + 3 \neq 2s + 3$ ($r, s \in \mathbb{R}$). Proof: We prove the contrapositive: If $2r + 3 = 2s + 3$, then $r = s$. Assume $2r + 3 = 2s + 3$. Subtracting 3 from both sides and dividing through by 2 gives $r = s$, as desired. \square

Occasionally, people give a proof by contradiction (see (7)) of a statement that can be established more directly by proving its contrapositive. For example, to prove the above statement by contradiction, we would start off assuming

that there exist $r, s \in \mathbb{R}$ such that $r \neq s$ and $2r + 3 = 2s + 3$. Then, as above, we would obtain $r = s$, contradicting that $r \neq s$. This proof is valid, but it is not as direct as the first proof. When a proof by contradiction ends up contradicting one of the initial assumptions, as in this case, it can usually be recast using the contrapositive. (Notice that this was not the case in the example worked for (7).)

9. In order to formulate the contrapositives of statements or to give proofs by contradiction, one needs to be able to negate statements. Usually, this is easy; for instance, the negative of $a = b$ is $a \neq b$. However, more complicated statements require some thought. Logicians have formal rules that can be used to accurately negate extremely complex statements, but since most statements occurring in mathematics have very simple logical structures, mathematicians tend not to use the formulas relying instead on their own reasoning. Statements involving “for every” sometimes cause problems, so here is an example.

$ab = ba$ for every $a, b \in G$. The negative is “There exist $a, b \in G$ such that $ab \neq ba$ ” (not “ $ab \neq ba$ for every $a, b \in G$ ”).