SECTION 1.6 Introduction to Proofs

This introduction applies jointly to this section and the next (1.7).

Learning to construct good mathematical proofs takes years. There is no algorithm for constructing the proof of a true proposition (there is actually a deep theorem in mathematical logic that says this). Instead, the construction of a valid proof is an art, honed after much practice. There are two problems for the beginning student—figuring out the key ideas in a problem (what is it that really makes the proposition true?) and writing down the proof in acceptable mathematical language.

Here are some general things to keep in mind in constructing proofs. First, of course, you need to find out exactly what is going on—why the proposition is true. This can take anywhere from ten seconds (for a really simple proposition) to a lifetime (some mathematicians have spent their entire careers trying to prove certain conjectures). For a typical student at this level, tackling a typical problem, the median might be somewhere around 15 minutes. This time should be spent looking at examples, making tentative assumptions, breaking the problem down into cases, perhaps looking at analogous but simpler problems, and in general bringing all of your mathematical intuition and training to bear.

It is often easiest to give a proof by contradiction, since you get to assume the most (all the hypotheses as well as the negation of the conclusion), and all you have to do is to derive a contradiction. Another thing to try early in attacking a problem is to separate the proposition into several cases; proof by cases is a valid technique, if you make sure to include all the possibilities. In proving propositions, all the rules of inference are at your disposal, as well as axioms and previously proved results. Ask yourself what definitions, axioms, or other theorems might be relevant to the problem at hand. The importance of constantly returning to the definitions cannot be overstated!

Once you think you see what is involved, you need to write down the proof. In doing so, pay attention both to content (does each statement follow logically? are you making any fallacious arguments? are you leaving out any cases or using hidden assumptions?) and to style. There are certain conventions in mathematical proofs, and you need to follow them. For example, you must use complete sentences and say exactly what you mean. (An equation is a complete sentence, with "equals" as the verb; however, a good proof will usually have more English words than mathematical symbols in it.) The point of a proof is to convince the reader that your line of argument is sound, and that therefore the proposition under discussion is true; put yourself in the reader's shoes, and ask yourself whether you are convinced.

Most of the proofs called for in this exercise set are not extremely difficult. Nevertheless, expect to have a fairly rough time constructing proofs that look like those presented in this solutions manual, the textbook, or other mathematics textbooks. The more proofs you write, utilizing the different methods discussed in this section, the better you will become at it. As a bonus, your ability to construct and respond to nonmathematical arguments (politics, religion, or whatever) will be enhanced. Good luck!

1. We must show that whenever we have two odd integers, their sum is even. Suppose that a and b are two odd integers. Then there exist integers s and t such that $a = 2s + 1$ and $b = 2t + 1$. Adding, we obtain $a + b = (2s + 1) + (2t + 1) = 2(s + t + 1)$. Since this represents $a + b$ as 2 times the integer $s + t + 1$, we conclude that $a + b$ is even, as desired.

3. We need to prove the following assertion for an arbitrary integer n: "If n is even, then n^2 is even." Suppose that n is even. Then $n = 2k$ for some integer k. Therefore $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$. Since we have written n^2 as 2 times an integer, we conclude that n^2 is even.

5. We can give a direct proof. Suppose that $m + n$ is even. Then $m + n = 2s$ for some integer s. Suppose that $n + p$ is even. Then $n + p = 2t$ for some integer t. If we add these [this step is inspired by the fact that we want to look at $m + p$], we get $m + p + 2n = 2s + 2t$. Subtracting $2n$ from both sides and factoring, we have

$m + p = 2s + 2t - 2n = 2(s + t - n)$. Since we have written $m + p$ as 2 times an integer, we conclude that $m + p$ is even, as desired.

7. The difference of two squares can be factored: $a^2 - b^2 = (a + b)(a - b)$. If we can arrange for our given odd integer to equal $a + b$ and for $a - b$ to equal 1, then we will be done. But we can do this by letting a and b be the integers that straddle $n/2$. For example, if $n = 11$, then we take $a = 6$ and $b = 5$. Specifically, if $n = 2k+1$, then we let $a = k+1$ and $b = k$. Here, then, is our proof. Since n is odd, we can write $n = 2k+1$ for some integer k. Then $(k + 1)^2 - k^2 = k^2 + 2k + 1 - k^2 = 2k + 1 = n$. This expresses n as the difference of two squares.

9. The proposition to be proved here is as follows: If r is a rational number and i is an irrational number, then $s = r + i$ is an irrational number. So suppose that r is rational, i is irrational, and s is rational. Then by Example 7 the sum of the rational numbers s and $-r$ must be rational. (Indeed, if $s = a/b$ and $r = c/d$, where a, b, c, and d are integers, with $b \neq 0$ and $d \neq 0$, then by algebra we see that $s+(-r) = (ad-bc)/(bd)$, so that patently $s + (-r)$ is a rational number.) But $s + (-r) = r + i - r = i$, forcing us to the conclusion that i is rational. This contradicts our hypothesis that i is irrational. Therefore the assumption that s was rational was incorrect, and we conclude, as desired, that s is irrational.

11. To disprove this proposition it is enough to find a counterexample, since the proposition has an implied universal quantification. We know from Example 10 that $\sqrt{2}$ is irrational. If we take the product of the irrational number $\sqrt{2}$ and the irrational number $\sqrt{2}$, then we obtain the rational number 2. This counterexample refutes the proposition.

13. We give an proof by contraposition. The contrapositive of this statement is "If $1/x$ is rational, then x is rational" so we give a direct proof of this contrapositive. Note that since $1/x$ exists, we know that $x \neq 0$. If $1/x$ is rational, then by definition $1/x = p/q$ for some integers p and q with $q \neq 0$. Since $1/x$ cannot be 0 (if it were, then we'd have the contradiction $1 = x \cdot 0$ by multiplying both sides by x), we know that $p \neq 0$. Now $x = 1/(1/x) = 1/(p/q) = q/p$ by the usual rules of algebra and arithmetic. Hence x can be written as the qnotient of two integers with the denominator nonzero. Thus by definition, x is rational.

15. We will prove the contrapositive (that if it is not true that $x \geq 1$ or $y \geq 1$, then it is not true that $x+y \geq 2$), using a direct argument. Assume that it is not true that $x \geq 1$ or $y \geq 1$. Then (by De Morgan's law) $x < 1$ and $y < 1$. Adding these two inequalities, we obtain $x + y < 2$. This is the negation of $x + y \geq 2$, and our proof is complete.

17. **a)** We must prove the contrapositive: If n is odd, then $n^3 + 5$ is even. Assume that n is odd. Then we can write $n = 2k+1$ for some integer k. Then $n^3+5 = (2k+1)^3+5 = 8k^3+12k^2+6k+6 = 2(4k^3+6k^2+3k+3)$. Thus $n^3 + 5$ is two times some integer, so it is even.
b) Suppose that $n^3 + 5$ is odd and that n is odd. Since n is odd, and the product of odd numbers is odd, in two steps we see that n^3 is odd. But then subtracting we conclude that 5, being the difference of the two odd numbers $n^3 + 5$ and n^3, is even. This is not true. Therefore our supposition was wrong, and the proof by contradiction is complete.

19. The proposition we are trying to prove is "If 0 is a positive integer greater than 1, then $0^2 > 0$." Our proof is a vacuons one, exactly as in Example 5. Since the hypothesis is false, the conditional statement is automatically true.

21. The proposition we are trying to prove is "If a and b are positive real numbers, then $(a+b)^1 \geq a^1 + b^1$." Our proof is a direct one. By the definition of exponentiation, any real number to the power 1 is itself. Hence $(a+b)^1 = a+b = a^1 + b^1$. Finally, by the addition rule, we can conclude from $(a+b)^1 = a^1 + b^1$ that $(a+b)^1 \geq a^1 + b^1$ (the latter being the disjunction of $(a+b)^1 = a^1 + b^1$ and $(a+b)^1 > a^1 + b^1$). One might also say that this is a trivial proof, since we did not use the hypothesis that a and b are positive (although of course we used the hypothesis that they are numbers).

23. We give a proof by contradiction. If there were nine or fewer days on each day of the week, this would account for at most $9 \cdot 7 = 63$ days. But we chose 64 days. This contradiction shows that at least ten of the days must be on the same day of the week.

25. One way to prove this is to use the rational root test from high school algebra: Every rational number that satisfies a polynomial with integer coefficients is of the form p/q, where p is a factor of the constant term of the polynomial, and q is a factor of the coefficient of the leading term. In this case, both the constant and the leading coefficient are 1, so the only possible values for p and q are ± 1. Therefore the only possible rational roots are $\pm 1/(\pm 1)$, which means that 1 and -1 are the only possible rational roots. Clearly neither of them is a root, so there are no rational roots.

Alternatively, we can follow the hint. Suppose by way of contradiction that a/b is a rational root, where a and b are integers and this fraction is in lowest terms (that is, a and b have no common divisor greater than 1). Plug this proposed root into the equation to obtain $a^3/b^3 + a/b + 1 = 0$. Multiply through by b^3 to obtain $a^3 + ab^2 + b^3 = 0$. If a and b are both odd, then the left-hand side is the sum of three odd numbers and therefore must be odd. If a is odd and b is even, then the left-hand side is odd + even + even, which is again odd. Similarly, if a is even and b is odd, then the left-hand side is even + even + odd, which is again odd. Because the fraction a/b is in simplest terms, it cannot happen that both a and b are even. Thus in all cases, the left-hand side is odd, and therefore cannot equal 0. This contradiction shows that no such root exists.

27. We must prove two conditional statements. First, we assume that n is odd and show that $5n+6$ is odd (this is a direct proof). By assumption, $n = 2k+1$ for some integer k. Then $5n+6 = 5(2k+1)+6 = 10k+11 = 2(5k+5)+1$. Since we have written $5n+6$ as 2 times an integer plus 1, we have showed that $5n+6$ is odd, as desired. Now we give an proof by contraposition of the converse. Suppose that n is not odd—in other words, that n is even. Then $n = 2k$ for some integer k. Then $5n+6 = 10k+6 = 2(5k+3)$. Since we have written $5n+6$ as 2 times an integer, we have showed that $5n+6$ is even. This completes the proof by contraposition of this conditional statement.

29. This proposition is true. We give a proof by contradiction. Suppose that m is neither 1 nor -1. Then mn has a factor (namely $|m|$) larger than 1. On the other hand, $mn = 1$, and 1 clearly has no such factor. Therefore we conclude that $m = 1$ or $m = -1$. It is then immediate that $n = 1$ in the first case and $n = -1$ in the second case, since $mn = 1$ implies that $n = 1/m$.

31. Perhaps the best way to do this is to prove that all of them are equivalent to x being even, which one can discover easily enough by trying a few small values of x. If x is even, then $x = 2k$ for some integer k. Therefore $3x+2 = 3 \cdot 2k + 2 = 6k+2 = 2(3k+1)$, which is even, since it has been written in the form $2t$, where $t = 3k+1$. Similarly, $x+5 = 2k+5 = 2k+4+1 = 2(k+2)+1$, so $x+5$ is odd; and $x^2 = (2k)^2 = 2(2k^2)$, so x^2 is even. For the converses, we will use a proof by contraposition. So assume that x is not even; thus x is odd and we can write $x = 2k+1$ for some integer k. Then $3x+2 = 3(2k+1)+2 = 6k+5 = 2(3k+2)+1$, which is odd (i.e., not even), since it has been written in the form $2t+1$, where $t = 3k+2$. Similarly, $x+5 = 2k+1+5 = 2(k+3)$, so $x+5$ is even (i.e., not odd). That x^2 is odd was already proved in Example 1. This completes the proof.

33. It is easiest to give proofs by contraposition of $(i) \rightarrow (ii)$, $(ii) \rightarrow (i)$, $(i) \rightarrow (iii)$, and $(iii) \rightarrow (i)$. For the first of these, suppose that $3x + 2$ is rational, namely equal to p/q for some integers p and q with $q \neq 0$. Then we can write $x = ((p/q) - 2)/3 = (p - 2q)/(3q)$, where $3q \neq 0$. This shows that x is rational. For the second conditional statement, suppose that x is rational, namely equal to p/q for some iutegers p and q with $q \neq 0$. Then we can write $3x + 2 = (3p + 2q)/q$, where $q \neq 0$. This shows that $3x + 2$ is rational. For the third conditional statement, suppose that $x/2$ is rational, namely equal to p/q for some integers p and q with $q \neq 0$. Then we can write $x = 2p/q$, where $q \neq 0$. This shows that x is rational. And for the fourth conditional statement, suppose that x is rational, namely equal to p/q for some integers p and q with $q \neq 0$. Then we can write $x/2 = p/(2q)$, where $2q \neq 0$. This shows that $x/2$ is rational.

35. The steps are valid for obtaining possible solutions to the equations. *If* the given equation is true, then we can conclude that $x = 1$ or $x = 6$, since the truth of each equation implies the truth of the next equation. However, the steps are not all reversible; in particular, the squaring step is not reversible. Therefore the possible answers must be checked in the original equation. We know that no other solutions are possible, but we do not know that these two numbers are in fact solutions. If we plug in $x = 1$ we get the true statement $2 = 2$; but if we plug in $x = 6$ we get the false statement $3 = -3$. Therefore $x = 1$ is the one and only solution of $\sqrt{x+3} = 3 - x$.

37. Suppose that we have proved $p_1 \rightarrow p_4 \rightarrow p_2 \rightarrow p_5 \rightarrow p_3 \rightarrow p_1$. Imagine these conditional statements arranged around a circle. Then to prove that each one of these propositions (say p_i) implies each of the others (say p_j), we just have to follow the circle, starting at p_i, until we come to p_j, using hypothetical syllogism repeatedly.

39. We can give a very satisfying proof by contradiction here. Suppose instead that all of the numbers a_1, a_2, $\ldots$, a_n are less than their average, which we can denote by A. In symbols, we have $a_i < A$ for all i. If we add these n inequalities, we see that

$$a_1 + a_2 + \cdots + a_n < nA .$$

By definition,

$$A = \frac{a_1 + a_2 + \cdots + a_n}{n} .$$

The two displayed formulae clearly contradict each other, however: they imply that $nA < nA$. Thus our assumption must have been incorrect, and we conclude that at least one of the numbers a_i is greater than or equal to their average.

41. We can prove that these four statements are equivalent in a circular way: $(i) \rightarrow (ii) \rightarrow (iii) \rightarrow (iv) \rightarrow (i)$. For the first, we want to show that if n is even, then $n + 1$ is odd. Assume that n is even. Then $n = 2k$ for some integer k. Thus $n + 1 = 2k + 1$, so by definition $n + 1$ is odd. This completes the first proof. Next we give a direct proof of $(ii) \rightarrow (iii)$. Suppose that $n + 1$ is odd, say $n + 1 = 2k + 1$. Then $3n + 1 = 2n + (n + 1) = 2n + 2k + 1 = 2(n + k) + 1$. Since this shows that $3n + 1$ is 2 times an integer plus 1, we conclude that $3n+1$ is odd, as desired. For the next proof, suppose that $3n+1$ is odd, say $3n+1 = 2k+1$. Then $3n = (3n + 1) - 1 = (2k + 1) - 1 = 2k$. Therefore by definition $3n$ is even. Finally, we must prove that if $3n$ is even, then n is even. We will do this using a proof by contraposition. Suppose that n is not even. Then n is odd, so we can write $n = 2k + 1$ for some integer k. Then $3n = 3(2k + 1) = 6k + 3 = 2(3k + 1) + 1$. This exhibits $3n$ as 2 times an integer plus 1, so $3n$ is odd, completing the proof by contraposition.