Solutions to CS 70 Challenge Problems: Proof Techniques

Other worksheets and solutions at https://alextseng.net/teaching/cs70/

Alex Tseng

1 Proofs

Prove the following propositions using a direct proof, proof by contradiction, contraposition, or a proof by cases.

(a) $(\forall x, y \in \mathbb{Z})\ 6 \nmid xy \Rightarrow (6 \nmid x \wedge 6 \nmid y)$
In plain English: For all integers x and y, if xy is not divisible by 6, then neither x nor y are divisible by 6.
We use a proof by contraposition. Recall, proving $A \Rightarrow B$ is logically equivalent to proving $\neg B \Rightarrow \neg A$. In this case, we need to show $\neg(6 \nmid x \wedge 6 \nmid y) \Rightarrow 6 \mid xy$. We will to simplify the left-hand side. If you recall De Morgan's Law (or simply reason it out in plain English), then this proposition becomes $\neg(6 \nmid x \wedge 6 \nmid y) \equiv 6 \mid x \vee 6 \mid y$ (x is divisible by 6 or y is divisible by 6, or both). Without loss of generality, let us assume that x is divisible by 6. y may or may not be divisible by 6. It does not matter. Then x can be written as $6k$, where k is an integer. Then $xy = 6ky$, so xy is also divisible by 6. This concludes the proof.

(b) Every integer that is a perfect cube is either a multiple of 9, 1 more than a multiple of 9, or 1 less than a multiple of 9.
We use a proof by cases. The cases here are a little tricky. We shall prove this proposition for some integer n. We will use the fact that any integer is in one of three classes: a multiple of 3, 1 more than a multiple of 3, or 1 less than a multiple of 3. Note that any other classification can be rewritten as one of these (e.g. 2 more than a multiple of 3 is 1 less than a multiple of 3).
Case 1: $n = 3k$, where k is an integer. Then $n^3 = 9k^3$, which is a multiple of 9.
Case 2: $n = 3k+1$, where k is an integer. Then $n^3 = 27k^3 + 27k^2 + 9k + 1 = 9(3k^3 + 3k^2 + k) + 1$, which is 1 more than a multiple of 9.
Case 3: $n = 3k-1$, where k is an integer. Then $n^3 = 27k^3 - 27k^2 + 9k - 1 = 9(3k^3 - 3k^2 + k) - 1$, which is 1 less than a multiple of 9.
The hardest part of this proof for many is to come up with the cases of n in the first place. Sometimes multiple tries are necessary to get nice numbers in the end.

(c) The difference between a rational number and an irrational number is irrational.
Let x be rational and y be irrational. Assume for contradiction that $x - y$ is rational. Then $x - y = \frac{a}{b}$, where a, b are integers and $b \neq 0$. Then $b(x - y) = a$. We can rewrite this equality as $y = \frac{bx-a}{b}$. Since a and b are integers and x is rational, it must be that $\frac{bx-a}{b}$ is also rational. To see this, we can let $x = \frac{c}{d}$ where c, d are integers, and show that $y = \frac{bc-ad}{bd}$. Contradiction—we assumed that y would be irrational. Therefore the difference between a rational number and an irrational number is irrational.

(d) *Challenge* $\sqrt{2}$ is irrational.
Assume for contradiction that $\sqrt{2}$ is rational. Then let us write $\sqrt{2} = \frac{a}{b}$, where a, b are integers ($b \neq 0$), and $\frac{a}{b}$ *is in its simplest form*. Then $2 = \frac{a^2}{b^2}$, or $2b^2 = a^2$. Thus, a^2 is even. This implies that a is even, too (the square of an odd number is odd, so by contraposition, the square root of an even perfect square is even). Then we can write $a = 2k$, where k is an integer. Since $2b^2 = a^2 = 4k^2$, we conclude that b^2 is also even ($b^2 = 2k^2$), and therefore b is even, as well. Contradiction—since a and b are both even, the fraction $\frac{a}{b}$ is not in its simplest form. Therefore $\sqrt{2}$ is irrational.
It might be a little bothersome at first to view this as a complete proof by contradiction. After all, we disproved our assumption that $\frac{a}{b}$ is in its simplest form. How does that translate to the assumption that $\sqrt{2}$ being rational as incorrect? The answer is that our assumption that $\frac{a}{b}$ being in its simplest form *cannot be incorrect*. Any rational number can be simplified to its simplest form, and not any further.

One of our assumptions is wrong, but this assumption cannot be wrong. Then the incorrect assumption must have been the assumption that $\sqrt{2}$ can be written as $\frac{a}{b}$ in its simplest form in the first place.

2 Induction

(a) Assume that $P(x) \Rightarrow P(x+2)$. What would you need to show in order to prove that $P(x)\ \forall x \in \mathbb{N}$?
You would have to show that $P(0)$ and $P(1)$ are true. If you only showed $P(0)$, then you would have proven $P(x)$ for only even x. Similarly, only showing $P(1)$ would have proven $P(x)$ for only odd x. Showing both then proves $P(x)$ for all even and all odd x, and therefore all x in general.

(b) Is this proof correct? If not, explain why.
$\forall n \in \mathbb{N}\ (42^n = 1)$
Base Case: $n = 0$, $42^0 = 1$
Inductive Hypothesis: Assume that $42^k = 1$.
Inductive Step: $42^{k+1} = \frac{42^k \times 42^k}{42^{k-1}} = \frac{1 \times 1}{1} = 1$.
This proof is obviously incorrect, because the proposition is obviously wrong. The reason this proof is incorrect is actually similar to the reasoning for the question above. The Inductive Step for $k+1$ uses both k and $k-1$, but we only have 1 base case, and our Inductive Hypothesis only assumes the proposition is true for k. So our Inductive Step fails. More concretely, let's say we wish to prove that $42^1 = 1$. Then per our Inductive Hypothesis, we would need to use the fact that $42^0 = 1$ and $42^{-1} = 1$. The former is our base case. The latter, however, is still unproven (not to mention incorrect). In order to show that this proposition is correct, one would have to show that $42^0 = 1$, and that $42^{-1} = 1$ (or $42^1 = 1$). That is, as long as there are two consecutive base cases, the proposition holds for all subsequent values. Additionally, for rigor's sake, the Inductive Hypothesis would also have to assume $42^k = 1$ and $42^{k-1} = 1$.