Section 05: Solutions

1. Trickier Set Theory

Show that, for any set X, if $A \in \mathcal{P}(X)$, then there exists a set $B \in \mathcal{P}(X)$ such that $A \cap B = \emptyset$ and $A \cup B = X$.

(Note: this problem requires some thought.)

Solution:

This solution might look long, but most of it is explaining the intuition. The proof itself is fairly short!

We start by letting X and A be arbitrary sets and assume that $A \in \mathcal{P}(X)$. Now we think about our goal. We want to show there is some set B with the given properties. The way to do this is usually to construct B somehow, but there's nothing in the problem that tells us where B might come from!

When you get stuck like this, try to use all the information given in the problem to deduce as many things as we can. First we might notice that $A \in \mathcal{P}(X)$ means that $A \subseteq X$ and $B \in \mathcal{B}$ means $B \subseteq X$. So given some subset of X, we must construct some other subset.

Next, we consider what we know about B. The property that $A \cap B = \emptyset$ means that B and A share no elements in common. That is, B consists only of elements in X that are not in A. The property that $A \cup B = X$ is a little tricker. We might think of A as some collection of objects from X, $A \cup B$ throws in all the elements of B, and once we do that we have all the elements of X. In order for this to happen, we know B must contain all the elements of X that weren't in A.

At this point we've deduced that B contains only elements in X that are not in A, but also that it must contain all the elements of X that are not in A. This says that B is exactly the elements of X that are not in A. Does this sound familiar? It's exactly the set difference $X \setminus A$.

Now we can write out the proof. Let X be an arbitrary set and let A be an arbitrary element of $\mathcal{P}(X)$. Let $B = X \setminus A$. For any $x \in X \setminus A$, by definition we have $x \in X$ which shows that $B \subseteq X$ and by definition $B \in \mathcal{P}(X)$.

To show that $A \cap B = \emptyset$, we must show that there are no elements that are both in A and B. If x is in $X \setminus A$, then by definition x is not in A, so there's no element that can be in both. Thus, $A \cap B = \emptyset$. To prove $A \cup B = X$, we first suppose $x \in A \cup B$ which by definition means $x \in A$ or $x \in B$. If $x \in A$ then since $A \subseteq X$ we have $x \in A$. If $x \in B$ then $x \in X \setminus A$ which by definition means that $x \in X$. In either case $x \in X$. In the other direction suppose $x \in X$. We again consider two cases. If $x \in A$ then there's nothing to show because then $x \in A \cup B$ automatically. If $x \notin A$ then since x is an element of X not in A, by definition we have $x \in X \setminus A$ which is equal to B, so in this case we also have $x \in A \cup B$. In either case $x \in A \cup B$. Since we've shown $x \in A \cup B$ if and only if $x \in X$, we've shown $A \cup B = X$, which completes the proof.

2. Prime Checking

You wrote the following code, `isPrime(int n)` which you are confident returns `true` if and only if n is prime (we assume its input is always positive).

```
public boolean isPrime(int n) {
    int potentialDiv = 2;
    while (potentialDiv < n) {
        if (n % potenttialDiv == 0)
            return false;
        potentialDiv++;
    }
    return true;
}
```

Your friend suggests replacing `potentialDiv < n` with `potentialDiv <= Math.sqrt(n)`. In this problem, you'll argue the change is ok. That is, your method still produces the correct result if n is a positive integer.

We will use "nontrivial divisor" to mean a factor that isn't 1 or the number itself. Formally, a positive integer k being a "nontrivial divisor" of n means that $k|n$, $k \neq 1$ and $k \neq n$. Claim: when a positive integer n has a nontrivial divisor, it has a nontrivial divisor at most $\sqrt{n}$.

(a) Let's try to break down the claim and understand it through examples. Show an example (a specific n and k) of a nontrivial divisor, of a divisor that is not nontrivial, and of a number with only trivial divisors.
Solution:

Some examples of "trivial" divisors: (1 of 15), (3 of 3)
Some examples of nontrivial divisors: (3 of 15), (9 of 81)
A number with only trivial divisor is just a prime number: it has no factors.

(b) Prove the claim. Hint: you may want to divide into two cases!

Solution:

Let k be a nontrivial divisor of n. Since k is a divisor, $n = kc$ for some integer c. Observe that c is also nontrivial, since if c were 1 or n then k would have to be n or 1.

We now have two cases:

Case 1: $k \leq \sqrt{n}$
If $k \leq \sqrt{n}$, then we're done because k is the desired nontrivial divisor.

Case 2: $k > \sqrt{n}$
If $k > \sqrt{n}$, then multiplying both sides by c we get $ck > c\sqrt{n}$. But $ck = n$ so $n > c\sqrt{n}$. Finally, dividing both sides by $\sqrt{n}$ gives $\sqrt{n} > c$, so c is the desired nontrivial factor.

In both cases we find a nontrivial divisor at most $\sqrt{n}$, as required.

Alternate solution (proof by contradiction): Let k be a nontrivial divisor of n. Since k is a divisor, $n = kc$ for some integer c. Observe that c is also nontrivial, since if c were 1 or n then k would have to be n or 1.

Suppose, for contradiction, that $k > \sqrt{n}$ and $c > \sqrt{n}$. Then $kc > \sqrt{n}\sqrt{n} = n$. But by assumption we have $kc = n$, so this is a contradiction. It follows that either k or c is at most $\sqrt{n}$ meaning that n has a nontrivial divisor at most $\sqrt{n}$.

(c) Informally explain why the fact about integers proved in (b) lets you change the code safely.

Solution:

The new code makes a subset of "checks" that the old code makes, thus the only concern would be that a non-prime number we found in the later checks would "slip through" without the extra checks. However, if a number has any nontrivial divisor, it will have one that is $\leq \sqrt{n}$, so even if we exit the loop early after $\sqrt{n}$ instead of n checks, our method is still guaranteed to always work.

3. Modular Arithmetic

(a) Prove that if $a \mid b$ and $b \mid a$, where a and b are integers, then $a = b$ or $a = -b$.

Solution:

Suppose that $a \mid b$ and $b \mid a$, where a, b are integers. By the definition of divides, we have $a \neq 0$, $b \neq 0$ and $b = ka, a = jb$ for some integers k, j. Combining these equations, we see that $a = j(ka)$.

Then, dividing both sides by a, we get $1 = jk$. So, $\frac{1}{j} = k$. Note that j and k are integers, which is only possible if $j, k \in \{1, -1\}$. It follows that $b = -a$ or $b = a$.

(b) Prove that if $n \mid m$, where n and m are integers greater than 1, and if $a \equiv_m b$, where a and b are integers, then $a \equiv_n b$.

Solution:

Suppose $n \mid m$ with $n, m > 1$, and $a \equiv_m b$. By definition of divides, we have $m = kn$ for some $k \in \mathbb{Z}$. By definition of congruence, we have $m \mid a - b$, which means that $a - b = mj$ for some $j \in \mathbb{Z}$. Combining the two equations, we see that $a - b = (knj) = n(kj)$. By definition of congruence, we have $a \equiv_n b$, as required.

4. Euclid's Lemma[1]

Show that, if a prime p divides ab, where a and b are integers, then $p \mid a$ or $p \mid b$.

You can use the following fact: if an integer p divides ab and $\gcd(p, a) = 1$, then p divides b.

Solution:

Suppose that $p \mid ab$ for prime number p and integers a, b. There are two cases.

Case 1: $\gcd(p, a) = 1$
In this case, $p \mid b$ by the fact above.

Case 2: $\gcd(p, a) \neq 1$
In this case, p and a share a common positive factor greater than 1. But since p is prime, its only positive factors are 1 and p, meaning $\gcd(p, a) = p$. This says p is a factor of a, that is, $p \mid a$.

In both cases, we have shown that $p \mid a$ or $p \mid b$.

[1] This proof isn't much longer than what you've seen before, but it can be a little easier to get stuck — use these as a chance to practice how to get unstuck if you do!

5. Divisors and Primes

Write an English proof of the following claim about a positive integer n: if the sum of the divisors of n is $n + 1$, then n is prime.

Hint: note that $n \mid n$ is always true.

Solution:

Let the distinct divisors of n be $d_1, d_2, \ldots, d_k$, each of which is positive. Writing $n = 1 \cdot n$, we see that $1 \mid n$ and $n \mid n$, by the definition of "|", so these two numbers are in the list. Moving them around in the list, we can take $d_1 = n$ and $d_2 = 1$.

By assumption, we have $n + 1 = d_1 + d_2 + \cdots + d_k$. Substituting the values of d_1 and d_2, we have

$$n + 1 = n + 1 + d_3 + d_4 + \cdots + d_k.$$

Subtracting $n + 1$ from both sides, we see that

$$0 = d_3 + d_4 + \cdots + d_k.$$

Since each divisor in the list is positive, this is only possible if the right hand side is an empty list. That is, we must have $k = 2$, meaning the list of divisors is just 1 and n. By definition, this says that n is prime.

(This is an example of a proof that would be difficult to formalize. In particular, the formal system does not give us a way to name to all the divisors of n as we did above. It is possible to write a formal proof of this, but it would be much more complicated than the English proof.)

6. Have we derived yet?

Each of the following proofs has some mistake in its reasoning - identify that mistake.

(a) *Proof.* If it is sunny, then it is not raining. It is not sunny. Therefore it is raining. □

Solution:

Let p be the proposition that it is sunny and r be the proposition that it is not raining. We know $p \to \neg r$ and $\neg p$. Using this, the proof shows the inverse $\neg p \to r$. However, the inverse is not equivalent to the implication, so we cannot infer the inverse from the given statement.

(b) Prove that if $x + y$ is odd, either x or y is odd but not both.

Proof. Suppose without loss of generality that x is odd and y is even.

Then, $\exists k\ x = 2k + 1$ and $\exists m\ y = 2m$. Adding these together, we can see that $x + y = 2k + 1 + 2m = 2k + 2m + 1 = 2(k + m) + 1$. Since k and m are integers, we know that $k + m$ is also an integer. So, we can say that $x + y$ is odd. Hence, we have shown what is required. □

Solution:

Looking at this logically, let's let p be the proposition that $x + y$ is odd and r be the proposition that either x or y is odd but not both. This proof shows $r \to p$ instead of $p \to r$.

This proof is incorrect because we have assumed the conclusion. Remember, the converse is not equivalent to the implication.

(c) Prove that $2 = 1$. :)

Proof. Let a, b be two equal, non-zero integers. Then,

$$
\begin{aligned}
a &= b && \\
a^2 &= ab && \text{[Multiply both sides by a]} \\
a^2 - b^2 &= ab - b^2 && \text{[Subtract } b^2 \text{ from both sides]} \\
(a-b)(a+b) &= b(a-b) && \text{[Factor both sides]} \\
a + b &= b && \text{[Divide both sides by } a - b\text{]} \\
b + b &= b && \text{[Since } a = b\text{]} \\
2b &= b && \text{[Simplify]} \\
2 &= 1 && \text{[Divide both sides by b]}
\end{aligned}
$$

□

Solution:

In line 5, we divided by $a - b$. Since $a = b$, $b - a = 0$. Therefore, this was dividing by 0. Dividing by 0 is an undefined operation (!) so this was an invalid step in the proof.

(d) Prove that $\sqrt{3} + \sqrt{7} < \sqrt{20}$

Proof.

$$
\begin{aligned}
&\sqrt{3} + \sqrt{7} < \sqrt{20} \\
&(\sqrt{3} + \sqrt{7})^2 < 20 \\
&3 + 2\sqrt{21} + 7 < 20 \\
&19.165 < 20
\end{aligned}
$$

It is true that $19.165 < 20$, hence, we have shown that $\sqrt{3} + \sqrt{7} < \sqrt{20}$ □

Solution:

Like part (b), here too, we have assumed the conclusion was true. In this case, instead of showing that this statement is true, we have shown this statement $\rightarrow T$. Remember, this does not necessarily mean that p is true! If you think back to the truth table for the implication $p \rightarrow q$, the implication becomes a vacuous truth if q is true: we know nothing about the truth value of p.