Section 04: Solutions

1. Prime Checking

One possible way to check if an integer n that is greater than 1 is prime is to check whether it is divisible by any integer in the range $1 < i < n$ - if it is, n is not prime.

Your friend suggests that you don't need to check every integer in the above range, but that the range $1 < i \leq \sqrt{n}$ will suffice.

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 $k \mid n$, $k \neq 1$ 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 $\sqrt{n}$.

2. Proof by Contrapositive

Prove that if $n \nmid ab$, then $n \nmid a$ and $n \nmid b$ for any $a, b, n \in \mathbb{Z}$.

Solution:

We want to show for any $a, b, n \in \mathbb{Z}$ that $n \nmid ab \rightarrow n \nmid a \wedge n \nmid b$.

We know the contrapositive of this is $\neg(n \nmid a \wedge n \nmid b) \rightarrow \neg(n \nmid ab)$, which can be rewritten as $n \mid a \vee n \mid b \rightarrow n \mid ab$.

That is, we want to prove that if n is divisible by a or n is divisible by b, then n is divisible by ab.

Let's split this into two cases.

Case 1: Suppose $n \mid a$. Then, $\exists k\ a = kn$. So, $ab = knb = (kb)n$. Therefore, $n \mid ab$.

Case 2: Suppose $n \mid b$. Then, $\exists k\ b = kn$. So, $ab = akn = (ak)n$. Therefore, $n \mid ab$.

Therefore, we have shown by contrapositive that if $n \nmid ab$, then $n \nmid a$ and $n \nmid b$ for any $a, b, n \in \mathbb{Z}$.

3. Which Do You Proofer?

For each of the following, if it is true, prove it; if it is not true, find a counterexample.

(a) $\forall x \in \mathbb{R}\ (x+1)^2 = x^2 + 1$ **Solution:**

This statement is not true. Consider $x = 1$. In this case, the LHS evaluates to 4 and the RHS evaluates to 2. $4 \neq 2$, hence we have shown that the statement does not hold.

(b) If n^2 is even, n is even. **Solution:**

Let us show this by showing the contrapositive: if n is odd then n^2 is odd.

Suppose n is odd. Then, there is an integer k such that $n = 2k + 1$. We can express n^2 as $(2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Therefore, n^2 is odd.

Hence, we have shown by contrapositive that if n^2 is even, n is even.

(c) $\sqrt{2}$ is irrational. Hint: you may need to use the above result :) **Solution:**

Let us prove this statement by contradiction.

Suppose $\sqrt{2}$ is rational. Then there are integers p, q such that $\sqrt{2} = \frac{p}{q}$ where p and q have no factors in common other than 1 (if they had factors in common, we could simplify the fraction to get p and q in the form we want). Squaring both sides, we get $2 = \frac{p^2}{q^2}$ or $2q^2 = p^2$. We know $2q^2$ is even. Since they are equal, p^2 must also be even. Then, p must also be even from (b).

Let $p = 2k$ for some integer k. Now, we have $2q^2 = (2k)^2$ or $2q^2 = 4k^2$, which is $q^2 = 2k^2$. We know $2k^2$ is even. Since they are equal, q^2 must also be even. Then, q must also be even from (b).

So p and q are even, and share a common factor of 2. However, we assumed p and q had no common factors. This is a contradiction. Therefore, $\sqrt{2}$ is irrational.

4. How Many Elements?

For each of these, how many elements are in the set? If the set has infinitely many elements, say ∞.

(a) $A = \{1, 2, 3, 2\}$

Solution:

3

(b) $B = \{\{\},\ \{\{\}\},\ \{\{\},\{\}\},\ \{\{\},\{\},\{\}\},\ \ldots\}$

Solution:

$$\begin{aligned} B &= \{\{\},\ \{\{\}\},\ \{\{\},\{\}\},\ \{\{\},\{\},\{\}\},\ \ldots\} \\ &= \{\{\},\ \{\{\}\},\ \{\{\}\},\ \{\{\}\},\ \ldots\} \\ &= \{\varnothing, \{\varnothing\}\} \end{aligned}$$

So, there are two elements in B.

(c) $C = A \times (B \cup \{7\})$

Solution:

$C = \{1,2,3\} \times \{\varnothing, \{\varnothing\}, 7\} = \{(a,b) \mid a \in \{1,2,3\}, b \in \{\varnothing, \{\varnothing\}, 7\}\}$. It follows that there are $3 \times 3 = 9$ elements in C.

(d) $D = \varnothing$

Solution:

0.

(e) $E = \{\varnothing\}$

Solution:

1.

(f) $F = \mathcal{P}(\{\varnothing\})$

Solution:

$2^1 = 2$. The elements are $F = \{\varnothing, \{\varnothing\}\}$.

5. Set = Set

Prove the following set identities.

(a) Let the universal set be $\mathcal{U}$. Prove $A \cap \overline{B} \subseteq A \backslash B$ for any sets A, B.

Solution:

Suppose $A \cap \overline{B}$ is nonempty (if it is empty, the proof is done; we need this line in order to assert that there is an element x in the next sentence). Let x be an arbitrary element in $A \cap \overline{B}$.

$$\begin{aligned} x \in A \cap \overline{B} \quad &\text{implies that} \quad x \in A \wedge x \in \overline{B} && \text{[Definition of } \cap\text{]} \\ &\text{which implies that} \quad x \in A \wedge x \notin B && \text{[Definition of } \overline{B}\text{]} \\ &\text{which implies that} \quad x \in A \setminus B && \text{[Definition of } \setminus\text{]} \end{aligned}$$

The above logic shows that $x \in A \cap \overline{B} \to x \in A \setminus B$. So by the definition of subset, we have $A \cap \overline{B} \subseteq A \setminus B$.

Solution:

Observe that the following equalities hold.

$$\begin{array}{rcll} A \cap \overline{B} & = & \{x : x \in A \wedge x \in \overline{B}\} & \text{[Definition of } \cap\text{]} \\ & = & \{x : x \in A \wedge x \notin B\} & \text{[Definition of } \overline{B}\text{]} \\ & = & \{x : x \in A \setminus B\} & \text{[Definition of } \setminus\text{]} \\ & = & A \setminus B & \text{[Definition of set comprehension]} \end{array}$$

Thus, the two sets $A \cap \overline{B}$ and $A \setminus B$ are in fact equal, so each is a subset of the other.

Solution:

Let x be arbitrary.

$$\begin{array}{rcll} x \in A \cap \overline{B} & \to & x \in A \wedge x \in \overline{B} & \text{[Definition of } \cap\text{]} \\ & \to & x \in A \wedge x \notin B & \text{[Definition of } \overline{B}\text{]} \\ & \to & x \in A \setminus B & \text{[Definition of } \setminus\text{]} \end{array}$$

Thus, since $x \in A \cap \overline{B} \to x \in A \setminus B$, it follows that $A \cap \overline{B} \subseteq A \setminus B$, by definition of subset.

(b) Prove that $(A \cap B) \times C \subseteq A \times (C \cup D)$ for any sets A, B, C, D.

Solution:

Let x be an arbitrary element of $(A \cap B) \times C$. Then, by definition of Cartesian product, x must be of the form (y, z) where $y \in A \cap B$ and $z \in C$. Since $y \in A \cap B$ by definition of $\cap$, $y \in A$ and $y \in B$; in particular, all we care about is that $y \in A$. Since $z \in C$, by definition of $\cup$, we also have $z \in C \cup D$. Therefore since $y \in A$ and $z \in C \cup D$, by definition of Cartesian product we have $x = (y, z) \in A \times (C \cup D)$.

Since x was an arbitrary element of $(A \cap B) \times C$ we have proved that $(A \cap B) \times C \subseteq A \times (C \cup D)$ as required.

6. 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 $a \equiv b \pmod{m}$, where a and b are integers, then $a \equiv b \pmod{n}$.

Solution:

Suppose $n \mid m$ with $n, m > 1$, and $a \equiv b \pmod{m}$. 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 $a \equiv b \pmod{n}$, as required.

7. Trickier Set Theory

Note, this problem requires a little more thinking. The solution will cover both the answer as well as the intuition used to arrive at it.

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

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.