Section 05: Number Theory

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.)

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.

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

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

3. Modular Arithmetic

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

(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 $a \equiv_n b$.

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.

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.

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. □

(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. □

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

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

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

□

(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 $\sqrt{3} + \sqrt{7} < \sqrt{20}$ □

[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!