Section 04: English Proofs, Sets

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 $1 < i \le \sqrt{n}$ 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 $k \mid n$, $k \ne 1$ and $k \ne n$.

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!

2. Proof by Contrapositive

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

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

(b) If n^2 is even, n is even.

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

4. How Many Elements?

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

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

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

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

(d) $D = \varnothing$

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

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

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.

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

6. Modular Arithmetic

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

(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 $a \equiv b \pmod{n}$.

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 $A \cup B = X$.