PROBLEM-SOLVING AND PROOFS: ASSIGNMENT 1
DUE FRIDAY, MARCH 3, 4PM.

Warm-up problems. These are completely optional.

(1) Let $a < b < c < d$ be real numbers. Express $[a, b] \cup [c, d]$ as a difference of sets.

(2) For what conditions on sets A and B does $A - B = B - A$.

(3) Suppose you play the coin game repeatedly, starting with a single pile of 5 coins. What happens? What if you start with a single pile of 6 coins?

Problems to be handed in. Solve three of the following four problems. One of the three must be Problem (4).

(1) **Prove that $\sqrt{11} \notin \mathbb{Q}$. You may use the fact that every integer can be uniquely decomposed as a product of primes.**

Suppose, for the sake of contradiction, that $11 \in \mathbb{Q}$. This means that we can write

$$\sqrt{11} = \frac{a}{b} \tag{1}$$

where a and b are integers with no common factor. More explicitly, we may write a and b uniquely as a product of primes:

$$a = p_1 \dots p_k \tag{2}$$
$$b = q_1 \dots q_m \tag{3}$$

where each p_i and q_i are prime numbers. The statement that a and b have no common factors then says that $p_i \neq q_j$ for any i, j. Squaring the first equation, and using our prime factorisation of a and b, we get

$$11 = \frac{p_1^2 \dots p_k^2}{q_1^2 \dots q_m^2} \tag{4}$$

and rearranging gives us

$$p_1^2 \dots p_k^2 = 11\, q_1^2 \dots q_m^2. \tag{5}$$

The RHS of this equation is divisible by 11, so the LHS must also be divisible by 11. This means that 11 divides $p_i^2 = p_i p_i$, for some i, and therefore divides p_i. Since p_i is prime, if 11 divides it we must have $p_i = 11$, for some i. If we now substitute this value of p_i into (5), we get

$$p_1^2 \dots 11^2 \dots p_k^2 = 11 q_1^2 \dots q_m^2. \tag{6}$$

After dividing by 11, we obtain

$$p_1^2 \dots 11 \dots p_k^2 = q_1^2 \dots q_m^2. \tag{7}$$

Since 11 divides the LHS, it must also divide the RHS, and the same argument as before tells us that we must have $q_j = 11$ for some j. This is a contradiction, since we assumed that $p_i \neq q_j$ for any i, j. It follows that $\sqrt{11} \notin \mathbb{Q}$.

(2) **Let S denote the set of all prime numbers of the form $4k+3$ with $k \in \mathbb{N}$. (So $3 \in S$, $7 \in S$, but $5 \notin S$.) Prove that S is infinite.**

Before beginning the proof of this problem, let us note that we will make free use of the fact that every odd number is either of the form $4k+1$ or $4k+3$, but not both.

Suppose, for the sake of contradiction, that S has only finitely many elements. This means we can write S as a (finite) list:

$$S = \{p_1, p_2, \ldots, p_n\}.$$

Now consider the integer

$$N := 4p_1p_2 \ldots p_n - 1.$$

We make two easy observations about N. First, none of the p_i's can be a factor of N. Second, N is of the form $4k+3$ for some integer k. Indeed, we can take $k = 4(p_1p_2 \ldots p_n - 1)$.

Now we will show that N must have at least one prime factor q of the form $4k+3$. Since, by the first observation above, q is not equal to any of the p_i, q will be a prime of the form $4k+3$ not contained in S. This gives a contradiction (since we supposed S to contain all such primes), and thus will finish the proof.

To see that N contains a prime factor of the form $4k+3$, suppose, on the contrary, that all prime factors were of the form $4k+1$. Then N would have the form

$$N = (4k_1 + 1)(4k_2 + 1) \ldots (4k_m + 1) = 4k + 1 \tag{8}$$

for some integer k. But since we already saw that N is form $4k+3$, this is impossible. Thus, N has a prime factor of the form $4k+3$, and the proof is complete.

(3) **Let $f : S \to T$ be a function, and let A and B be subsets of S. Prove that $f(A \cap B) \subseteq f(A) \cap f(B)$. Give an example to show that the reverse inclusion need not hold.**

To show that $f(A \cap B) \subseteq f(A) \cap f(B)$, we take an arbitrary element in $f(A \cap B)$, and show that it must be contained in $f(A) \cap f(B)$. To that end, let $y \in f(A \cap B)$. This means that $y = f(x)$, for some $x \in A \cap B$.

Now $x \in A \cap B$ means that $x \in A$ and $x \in B$. But $x \in A$ implies $f(x) \in f(A)$, and $x \in B$ implies $f(x) \in f(B)$. It follows that $f(x)$ is in both $f(A)$ and $f(B)$, that is, $f(x) \in f(A) \cap f(B)$. Since $y = f(x)$, we have $y \in f(A) \cap f(B)$ as desired.

An example which shows that the reverse inclusion doesn't hold: Consider the function

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^2. \end{aligned}$$

(In this example, the sets S and T are both are $\mathbb{R}$.) If we look at the subsets $A \subseteq S$ and $B \subseteq S$ given by

$$\begin{aligned} A &= \{-2\} \\ B &= \{2\} \end{aligned}$$

Then $f(A) = \{4\}$ and $f(B) = \{4\}$, so $f(A) \cap f(B) = \{4\}$. On the other side, we have $A \cap B = \emptyset$, so $f(A \cap B) = f(\emptyset) = \emptyset$. Thus, in this example, $f(A) \cap f(B) \not\subseteq f(A \cap B)$.

(4) **Let f and g denote functions from $\mathbb{R}$ to $\mathbb{R}$. Recall that such a function is *bounded* if there exists a real number M such that $|f(x)| < M$ for all $x \in \mathbb{R}$. Determine whether each of the following statements is true. If true, provide a proof. If false, provide a counterexample.**
- **If f and g are bounded, then $f + g$ is bounded.**
- **If f and g are bounded, then fg is bounded.**
- **If $f + g$ is bounded, then f and g are bounded.**
- **If fg is bounded, then f and g are bounded.**
- **If $f + g$ and fg are bounded, then f and g are bounded.**

You may use the *triangle inequality* which states that for all $x, y \in \mathbb{R}$,

$$|x + y| \leq |x| + |y|.$$

True: If f and g are bounded, then there exist real numbers M and N such that $|f(x)| < M$ and $|g(x)| < N$ for all $x \in \mathbb{R}$. Then, for each $x \in \mathbb{R}$, we have (using the triangle inequality):

$$|f(x) + g(x)| \leq |f(x)| + |g(x)| < M + N$$

This inequality shows that $f + g$ satisfies the definition of a bounded function (using $M + N$ as the bound).

True: We use the same notation as above, and simply compute:

$$|f(x)g(x)| = |f(x)|\,|g(x)| < MN$$

That is, fg is bounded (using MN as the bound).

False: Consider the functions $f(x) = x$ and $g(x) = -x$. Then $f(x) + g(x) = 0$ is certainly bounded, even though neither f nor g is.

False: Consider the functions $f(x) = e^x$ and $g(x) = e^{-x}$. Then $f(x)g(x) = 1$ is certainly bounded, even though neither f nor g is.

True: Suppose that $f + g$ and fg are both bounded. Then there exist real numbers M and N such that

$$\begin{aligned} |f(x) + g(x)| &< M \\ |f(x)g(x)| &< N. \end{aligned}$$

We then compute[1]

$$\begin{aligned}
|f(x)|^2 &= |f(x)^2| \\
&\le |f(x)^2 + g(x)^2| \\
&= \left|(f(x)+g(x))^2 - 2f(x)g(x)\right| \\
&\le |\,(f(x)+g(x))^2\,| + |2f(x)g(x)| \\
&= |f(x)+g(x)|^2 + 2|f(x)g(x)| \\
&< M^2 + 2N
\end{aligned}$$

It follows that $|f(x)| < \sqrt{M^2 + 2N}$ for all $x \in \mathbb{R}$, and therefore that f is bounded. The same argument with f and g swapped shows that g is also bounded.

[1] Make sure you understand the reasoning behind each of these steps!