Math 347H: Fundamental Math (H) HOMEWORK 3 **Due date: Oct 5 (Thu)**

1. Let X be a set and recall that $\mathscr{P}(X)$ denotes its powerset. Recall the operation of symmetric difference $A \triangle B$ and realize that it is a *binary operation* on $\mathscr{P}(X)$, i.e. it is a function $\mathscr{P}(X) \times \mathscr{P}(X) \to \mathscr{P}(X)$ that takes a pair (A, B) of subsets of X to $A \triangle B$.

   (a) Verify that $\triangle$ (taken in place of $+$) satisfies the commutativity axiom (A3).

   REMARK: $\triangle$ also satisfies the associativity axiom (A2), but proving it is long and tedious, I'll spare you the hassle ;)

   (b) Show that (A4) also holds by finding a set $\mathbb{O} \in \mathscr{P}(X)$ that serves as the *identity* for the operation $\triangle$, i.e. is such that, for any set $A \in \mathscr{P}(X)$, $A \triangle \mathbb{O} = A = \mathbb{O} \triangle A$.

   (c) Show that even (A5) holds by finding, for each $A \in \mathscr{P}(X)$, a set $A' \in \mathscr{P}(X)$ such that $A \triangle A' = \mathbb{O} = A' \triangle A$.

2. Prove the following theorem.

   Shifted Strong Induction. *Let $P \subseteq \mathbb{Z}$ and let $n_0 \in \mathbb{Z}$. Suppose that for each $n \geq n_0$, if each integer $k \in [n_0, n)$ is in P, then n is also in P. Then, $P \supseteq \mathbb{Z}_{\geq n_0} := \{n \in \mathbb{Z} : n \geq n_0\}$.*

3. We say that integers $x, y \in \mathbb{Z}$ are *coprime* if their only common divisor is 1.

   (a) Prove: If $x, y \in \mathbb{N}$ are coprime and $x > y$, then $x - y$ and y are coprime.

   (b) Prove the following theorem.

   Bézout's Theorem. *If $x, y \in \mathbb{N}$ are coprime, then there are integers $a, b \in \mathbb{Z}$ such that $a \cdot x + b \cdot y = 1$.*

   HINT: Use strong induction on $\max\{x, y\}$; this means that you need to prove, by strong on n, the following statement:

   > For all $n \in \mathbb{N}$, for each pair $x, y \in \mathbb{N}$ with $x, y \leq n$, if x and y are coprime, then there are integers $a, b \in \mathbb{Z}$ such that $a \cdot x + b \cdot y = 1$.

   In the course of the proof, handle the case $x = y$ separately, then suppose, without loss of generality, that $x > y$ and consider the pair $x - y, y$.

4. Let $p \in \mathbb{N}$ be a prime number. Prove:

   (a) For any $x, y \in \mathbb{N}$, if p divides $x \cdot y$, then p divides x or p divides y.

   HINT: To prove this, suppose that p divides $x \cdot y$ but p doesn't divide x. Your task is to prove that it must divide y. Apply Bézout's theorem to p and x.

   (b) For any $\ell \in \mathbb{N}^+$ and any $x_1, x_2, \ldots, x_\ell \in \mathbb{N}$, if p divides $x_1 \cdot x_2 \cdot \ldots \cdot x_\ell$, then p divides x_i for some $i \in \{1, 2, \ldots, \ell\}$.

5. A *prime number decomposition* for any natural number $n \geq 2$ is a tuple of prime numbers $(p_1, p_2, \ldots, p_\ell)$ in the nondecreasing order, i.e. $p_1 \leq p_2 \leq \ldots \leq p_\ell$, such that $n = p_1 \cdot p_2 \cdot \ldots \cdot p_\ell$. In class, we proved the existence of such a decomposition. Prove that there is only one such decomposition, i.e. prove:

Prime Number Decomposition Theorem. *Every natural number $n \geq 2$ admits a unique prime number decomposition.*

Hint: Suppose there are two such decompositions:

$$p_1 \cdot p_2 \cdot \ldots \cdot p_\ell = q_1 \cdot q_2 \cdot \ldots \cdot q_m.$$

Cancel all common terms from both sides. If after this cancellation there is still a prime left on one of the sides, then it has to divide the other side, which leads to a contradiction!

6. Let X, Y be sets and $f : X \to Y$ be a function. Define the binary relation E_f on X as follows: for each $x_1, x_2 \in X$,

$$x_1 E_f x_2 \text{ if and only if } f(x_1) = f(x_2).$$

Prove that E_f is an *equivalence relation*, i.e. that it is reflexive, symmetric, and transitive.