Homework 3

due Feb 13th

There are 13 problems on 2 pages of this homework assignment.

1. Fix an integer \( n \geq 2 \). Prove the following rules of modular arithmetic for all \( a, b, c, d \in \mathbb{Z} \).
   (a) If \( a \equiv b \pmod{n} \) and \( c \equiv d \pmod{n} \), then \( a + c \equiv b + d \pmod{n} \). \textit{Addition}
   (b) If \( a \equiv b \pmod{n} \) and \( c \equiv d \pmod{n} \), then \( a - c \equiv b - d \pmod{n} \). \textit{Subtraction}
   (c) If \( a \equiv b \pmod{n} \) and \( c \equiv d \pmod{n} \), then \( ac \equiv bd \pmod{n} \). \textit{Multiplication}

2. Fix an integer \( n \geq 2 \). Disprove: For all \( a, b, c \in \mathbb{Z} \), if \( ac \equiv bc \pmod{n} \), then \( a \equiv b \pmod{n} \).
   \textit{There is NO general division rule in modular arithmetic!}

3. Let \( n \in \mathbb{Z} \). Prove that \( a^2 \equiv (a - n)^2 \pmod{n} \) for all integers \( a \) using modular arithmetic.

4. (a) Let \( R \) be the relation defined on \( \mathbb{Z} \) by \( a R b \) if \( a + b \) is even. Show that \( R \) is an equivalence relation and determine the distinct equivalence classes.
   (b) Consider the relation \( S \) where “even” is replaced by “odd” above. Which properties of an equivalence relation does \( S \) possess?

5. Fix integers \( x, y, \) and \( n \geq 2 \). Let \( R \) be the relation on \( \mathbb{Z} \) defined by \( ax + by \equiv 0 \pmod{n} \).
   Give well-justified answers to the questions: under what conditions on \( x \) and \( y \) is \( R \)…
   (a) \ldots reflexive?
   (b) \ldots symmetric?
   (c) \ldots transitive?
   (d) \ldots an equivalence relation?
   \textit{Hint: see Problems 8.29, 8.30, 8.33, 8.34, 8.35 in the textbook.}

6. Let \( n \geq 2 \) be an integer. Define a relation \( R \) on \( \mathbb{Z} \) by \( a R b \) if and only if \( a^2 \equiv b^2 \pmod{n} \).
   (a) Prove that \( R \) is an equivalence relation when \( n = 5 \) and determine the distinct equivalence classes.
   (b) In general, under what conditions on \( n \) is \( R \) an equivalence relation? Prove that your answer is correct.
   (c) When \( R \) is an equivalence relation, what are the equivalence classes? Your answer should be in the form \( [a] = \{ b \in \mathbb{Z} \mid A \} \) where \( a \) is the representative element (as a function of \( n \)) and \( A \) is the criteria that \( b \) must satisfy to be in the set \( [a] \).

7. Find the smallest equivalence relation on the set \( \{a, b, c, d, e\} \) that contains the relation \( \{(a, b), (a, c), (d, e)\} \).
   What does “smallest” mean here?
8. Let $R$ be the relation on the set of ordered pairs of positive integers such that $((a, b), (c, d)) \in R$ if and only if $ad = bc$.

(a) Prove that $R$ is an equivalence relation.
(b) What is the equivalence class of $(1, 2)$ under this relation?
(c) Are there finitely many equivalence classes? Justify your answer.
(d) Give a description of each different equivalence class.

9. Let $R$ be a relation from a set $A$ to a set $B$. The inverse relation from $B$ to $A$, denoted by $R^{-1}$, is the set of ordered pairs $\{(b, a) \mid (a, b) \in R\}$.

(a) Prove that a relation $R$ on a set $A$ is symmetric if and only if $R = R^{-1}$.
(b) Prove that a relation $R$ on a set $A$ is antisymmetric if and only if $R \cap R^{-1}$ is a subset of the diagonal relation $\Delta = \{(a, a) \mid a \in A\}$.

10. Suppose that $R$ and $S$ are equivalence relations on the nonempty set $A$. Prove or disprove:

(a) $R \cup S$ is an equivalence relation.
(b) $R \cap S$ is an equivalence relation.

11. Let $R$, $S$, and $T$ be relations on $\mathbb{Z}$ defined as:

- $a R b$ if and only if $a \equiv b \pmod{2}$,
- $a S b$ if and only if $a \equiv b \pmod{3}$,
- and $a T b$ if and only if $a \equiv b \pmod{6}$

(a) List the equivalence classes for $R$, for $S$, and for $T$.
(b) If $R \cup S$ is an equivalence relation, find its equivalence classes.
(c) If $R \cap S$ is an equivalence relation, find its equivalence classes.

12. A partition $P_1$ is called a refinement of the partition $P_2$ if every set in $P_1$ is a subset of one of the sets in $P_2$. Show that the partition formed from the congruence classes modulo 6 is a refinement of the partition formed from the congruence classes modulo 3.

13. Prove that propositional equivalence is an equivalence relation on the set of all compound propositions. Hint: Let $C$ be the set of all compound propositions. For $p, q \in C$, define a relation $R$ on $C$ by $p R q$ if and only if $p \leftrightarrow q$ is a tautology.