CPSC 418/MATH 318 Practice Problems

Modular Arithmetic

Fix a positive integer m (the *modulus*).

Let $a, b \in \mathbb{Z}$ (the set of integers). Recall that *a is congruent to b modulo m*, written as $a \equiv b \pmod{m}$, if $a - b$ is an integer multiple of m; in other words, $a = b + km$ for some integer k.

This means that in order to prove that an integer a is congruent modulo m to some other integer b, it suffices to show that their difference $a - b$ is divisible by m. Alternatively, you can exhibit an explicit integer k such that $a = b + km$.

The *congruence class* of a modulo m is the set of all integers that are congruent to a modulo m.

1. True of False?
   (a) $8 \equiv 2 \pmod{5}$.
   (b) $3 \equiv 1000002 \pmod{3}$.
   (c) $7 \equiv -364 \pmod{7}$.
   (d) $a \equiv a + 2 \pmod{4}$ for all integers a.
   (e) $a \equiv a + 2 \pmod{4}$ for no integer a.
   (f) $5 \equiv 0 \pmod{1}$.

2. Write down 3 positive integers and 3 negative integers that belong to the congruence class of 2 modulo 7.

3. Which of the following elements belong to the congruence class of -1 modulo 13?
   (a) 14.
   (b) -1379.

4. Describe (mathematically or in words) the elements in the congruence class of 0 modulo 5.

5. Describe in words the congruence class of
   (a) 0 modulo 2.
   (b) 1 modulo 2.

6. Let m be a fixed positive integer and $a, b, c \in \mathbb{Z}$. Formally prove the following properties of congruences:
   (a) (Reflexivity) $a \equiv a \pmod{m}$.
   (b) (Symmetry) If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.
   (c) (Transitivity) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

7. Let m be a fixed positive integer.
   (a) Prove that no two among the integers $0, 1, 2, \ldots, m - 1$ are congruent to each other modulo m.
   (b) Prove that every integer is congruent modulo m to one of $0, 1, 2, \ldots, m - 1$.

8. Let m be a fixed positive integer and $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. Formally prove the following properties of congruences:
   (a) If $a_1 \equiv a_2 \pmod{m}$ and $b_1 \equiv b_2 \pmod{m}$, then $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$.
   (b) If $a_1 \equiv a_2 \pmod{m}$, then $ca_1 \equiv ca_2 \pmod{m}$ for all $c \in \mathbb{Z}$.
   (c) If $a_1 \equiv a_2 \pmod{m}$ and $b_1 \equiv b_2 \pmod{m}$, then $a_1 b_1 \equiv a_2 b_2 \pmod{m}$.

9. Use the decimal representation of integers and properties (a) and (c) in Problem 8 to prove the following:
   (a) An integer is divisible by 3 if and only if the sum of its decimal digits is divisible by 3.
   (b) An integer is divisible by 9 if and only if the sum of its decimal digits is divisible by 9.
   (c) An integer is divisible by 11 if and only if the alternating sum of its decimal digits is divisible by 11. Here, if an integer has decimal digits $a_0, a_1, \ldots, a_n$, i.e. its decimal representation is $a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n$, then its *alternating sum* of its digits is $a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n$.