Math 311 - Introduction to Proof and Abstract Mathematics
Group Assignment # 18 **Name:**_____
Due: At the end of class on Tuesday, April 9th

Congruences:

1. The following activity is designed to introduce you to the concept of **congruence modulo** n in a natural way.

   (a) What day of the week will it be 4 days from now? How about 11 days from now? 18 days from now?

   (b) Find 6 other integers k for which the answer to the question "What day will it be k days from now?" is the same as in part (a) above. Make sure that two of them are negative (do negative values make sense?).

   (c) Pick any two numbers that you found in either part (a) or (b) and subtract them. Do this several times. What pattern (if any) do you notice? Why do you think this happens?

Definition 6.4.1: Let $a, b \in \mathbb{Z}$, and let $m \in \mathbb{Z}^+$. The integers a and b are **congruent modulo** m, written $a \equiv b \bmod m$ if $m \mid (a - b)$.

Examples:

- $25 \equiv 3 \pmod{11}$ since $25 - 3 = 22$, and $11 \mid 22$.
- $39 \equiv 5 \pmod{17}$ since $39 - 5 = 34$, and $17 \mid 34$.
- $-8 \equiv 7 \pmod{5}$ since $-8 - 7 = -15$, and $5 \mid -15$.

2. Find (or describe) all correct values of k in each of the following expressions. Briefly justify your answers.

   (a) $123 \equiv k \pmod 7$

   (b) $57 \equiv 7 \pmod k$

   (c) $k \equiv 1 \pmod{12}$

Recall: Theorem 6.1.1 (The Division Algorithm). Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r$, where $0 \leq r < b$.

Proposition 6.4.3: Let $a, b \in \mathbb{Z}$. Then $a \equiv b \bmod m \Leftrightarrow (\exists q \in \mathbb{Z})[a = mq + b]$.

3. Prove Proposition 6.4.3.

Theorem 6.4.4:

- For all $a \in \mathbb{Z}$, $a \equiv a \bmod m$ (that is, congruence modulo m is reflexive).
- For all $a, b \in \mathbb{Z}$, if $a \equiv b \bmod m$, then $b \equiv a \bmod m$ (that is, congruence modulo m is symmetric).
- For all $a, b, c \in \mathbb{Z}$, if $a \equiv b \bmod m$, and $b \equiv c \bmod m$ then $a \equiv c \bmod m$ (that is, congruence modulo m is transitive).

Proof:

Let $a \in \mathbb{Z}$. Notice that $a - a = 0 \cdot m$. Thus $m \mid (a - a)$. Hence, by definition 6.4.1, $a \equiv a \bmod m$ (therefore congruence modulo m is reflexive).

Let $a, b \in \mathbb{Z}$ and suppose that $a \equiv b \bmod m$. Then, by definition 6.4.1, $m \mid (a-b)$. That is, for some $k \in \mathbb{Z}$, $(a-b) = km$. Therefore, $(b-a) = -km$. Moreover, since $k \in \mathbb{Z}$, $-k \in \mathbb{Z}$. Hence $m \mid (b-a)$. Thus $b \equiv a \bmod m$ (therefore, congruence modulo m is symmetric).

Let $a, b, c \in \mathbb{Z}$ and suppose that $a \equiv b \bmod m$ and $b \equiv c \bmod m$. Then, by definition 6.4.1, $m \mid (a - b)$ and $m \mid (b - c)$. That is, there exist $k, \ell \in \mathbb{Z}$ such that $(a - b) = km$ and $(b - c) = \ell m$. Therefore, $(a - b) + (b - c) = km + \ell m$. That is, $(a - c) = (k + \ell)m$. Moreover, since $k, \ell \in \mathbb{Z}$, $k + \ell \in \mathbb{Z}$. Hence $m \mid (a - c)$. Thus $a \equiv c \bmod m$ (therefore, congruence modulo m is transitive). $\square$.

Theorem 6.4.5: Let $a, b \in \mathbb{Z}$.

- There is a unique $r \in \mathbb{Z}$ such that $0 \leq r < m$ and $a \equiv r \bmod m$.
- The congruence $a \equiv b \bmod m$ holds if and only if there exists $r \in \mathbb{Z}$ with $0 \leq r < m$ such that $a \equiv r \bmod m$ and $b \equiv r \bmod m$ (that is, a and b have the same non-negative remainder $r < m$ when divided by m).

Proof: This first part is a direct consequence of the Division Algorithm. The second part is proved is your textbook on page 146.

Theorem 6.4.6 Let $a_1, a_2, b_1, b_2, c \in \mathbb{Z}$. and assume that $a_1 \equiv a_2 \bmod m$ and $b_1 \equiv b_2 \bmod m$. Then:

- $a_1 + b_1 \equiv a_2 + b_2 \bmod m$
- $a_1 - b_1 \equiv a_2 - b_2 \bmod m$
- $a_1 + c \equiv a_2 + c \bmod m$
- $a_1 b_1 \equiv a_2 b_2 \bmod m$
- $a_1 c \equiv a_2 c \bmod m$

Proof: The first three parts of this Theorem are presentation eligible problems. The fourth statement if proved in your book on page 147. I will prove the final part:

Suppose that $a_1, a_2, c \in \mathbb{Z}$ and that $a_1 \equiv a_2 \bmod m$. Then $m \mid a_1 - a_2$. That is, there exists $k \in \mathbb{Z}$ such that $a_1 - a_2 = km$. Then $c(a_1 - a_2) = c(km)$, or, using the distributive property, the commutative property of multiplication, and the associative property of multiplication, $c(a_1 - a_2) = ca_1 - ca_2 = a_1c - a_2c = c(km) = (ck)m$. That is, $a_1c - a_2c = (ck)m$. Therefore, $m \mid a_1c - a_2c$. Hence $a_1c \equiv a_2c \bmod m$. $\square$.

4. Prove that if $a \equiv b \pmod{n}$ and $m \in \mathbb{N}$, then $a^m \equiv b^m \pmod{n}$. [Hint: What does the previous Theorem say in the special case when $a_1 = b_1$ and $a_2 = b_2$?]

5. Prove or Disprove: If $a^2 \equiv b^2 \bmod m$, then $a \equiv b \bmod m$.