26^{th} TJIMO

ALEXANDRIA, VIRGINIA

Round: **Practice Power**

1 Introduction

You are all familiar with taking the remainder of a number when divided by another number. Modular arithmetic is an extension of this study, analyzing properties of numbers when remainders are taken.

For example, 11 leaves a remainder of 3 when divided by 4. However, 11 is not the only number with this property: 7, 15, 19, etc. on also have this property, as well as the negative numbers -1, -5, etc. We call these numbers *congruent modulo 4*, which we will define more rigorously below.

2 Modulo Arithmetic

Let a, b, m be integers. a and b are said to be *congruent modulo* m if m evenly divides $a - b$. We write this as

$$a \equiv b \pmod{m}.$$

For example, $1 \equiv 1 \pmod 5$ since $1 - 1 = 0$ is divisible by 5. Similarly, $1 \equiv 6 \pmod 5$.

1. (a) Show $13 \equiv 1 \pmod 6$.
   (b) Show $14 \equiv 2 \pmod 6$.
   (c) Show $13 + 14 \equiv 1 + 2 \equiv 3 \pmod 6$.
   (d) Show $13 \times 14 \equiv 1 \times 2 \equiv 2 \pmod 6$.

2. Let a, b, c, d, m be integers such that $a \equiv b \pmod m$ and $c \equiv d \pmod m$.
   (a) Show $a + c \equiv b + d \pmod m$.
   (b) Show $a - c \equiv b - d \pmod m$.
   (c) Show $a \times c \equiv b \times d \pmod m$.

So far we have seen that addition, subtraction, and multiplication are preserved under modulo arithmetic. *The same is not necessarily true for division.*

3. We know that if a prime p evenly divides ab, then p must divide at least one of a or b. (Convince yourself of this!) Use this fact to prove that if

   $$mx \equiv nx \pmod p$$

   for x not divisible by p, then

   $$m \equiv n \pmod p.$$

4. What if the modulo is not prime?
   (a) We know that $10 \equiv 4 \pmod 6$. Can we divide both sides by 2? Is $5 \equiv 2 \pmod 6$?
   (b) We know that $25 \equiv 55 \pmod 6$. Can we divide both sides by 5? Is $5 \equiv 11 \pmod 6$?

Time limit: 30 minutes.

What makes (a) any different from (b)? It turns out we can divide when the greatest common divisor of the number to be divided and the mod m is 1. For instance,

$$5a \equiv 5b \pmod 6$$

implies

$$a \equiv b \pmod 6$$

since $\gcd(a, b) = 1$.

5. (a) Find positive $x < 10$ such that $3x \equiv 1 \pmod{10}$.
   (b) Find positive $x < 10$ such that $7x \equiv 1 \pmod{10}$.
   (c) Find positive $x < 10$ such that $9x \equiv 1 \pmod{10}$.
   (d) Can we find x such that $2x \equiv 1 \pmod{10}$?
   (e) Can we find x such that $5x \equiv 1 \pmod{10}$?
   (f) For what values of a can we find x such that $ax \equiv 1 \pmod{10}$?

Time limit: 30 minutes.