26^{th} TJIMO

Alexandria, Virginia

Round: **Practice Power Solutions**

1 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 $13 \equiv 1 \pmod{6}$.
   Solution. 6 divides $13 - 1 = 12$ evenly twice. Then $13 \equiv 1 \pmod{6}$.
   (b) Show $14 \equiv 2 \pmod{6}$.
   Solution. 6 divides $14 - 2 = 12$ evenly twice. Then $14 \equiv 2 \pmod{6}$.
   (c) Show $13 + 14 \equiv 1 + 2 \equiv 3 \pmod{6}$.
   Solution. 6 divides $(14 + 13) - (2 + 1) = 24$ evenly 4 times. Then $14 + 13 \equiv 2 + 1 \pmod{6}$.
   (d) Show $13 \times 14 \equiv 1 \times 2 \equiv 2 \pmod{6}$.
   Solution. 6 divides $(14 \times 13) - (2 \times 1) = 180$ evenly 30 times. Then $14 \times 13 \equiv 2 \times 1 \pmod{6}$.

2. Let a, b, c, d, m be integers such that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.

   (a) Show $a + c \equiv b + d \pmod{m}$.
   Solution. Since $a \equiv b \pmod{m}$, then a can be expressed as $b + s \cdot m$ for some integer s. Similarly, c can be expressed as $d + t \cdot m$ for some integer t.
   Then $a + c = b + d + m \cdot (s + t)$, so m evenly divides $(a + c) - (b + d)$ and $a + c \equiv b + d \pmod{m}$.
   (b) Show $a - c \equiv b - d \pmod{m}$.
   Solution. Since $a \equiv b \pmod{m}$, then a can be expressed as $b + s \cdot m$ for some integer s. Similarly, c can be expressed as $d + t \cdot m$ for some integer t.
   Then $a - c = b - d + m \cdot (s - t)$, so m evenly divides $(a - c) - (b - d)$ and $a + c \equiv b + d \pmod{m}$.
   (c) Show $a \times c \equiv b \times d \pmod{m}$.
   Solution. Since $a \equiv b \pmod{m}$, then a can be expressed as $b + s \cdot m$ for some integer s. Similarly, c can be expressed as $d + t \cdot m$ for some integer t.
   Then $a \times c = b \times d + m \cdot (ds + bt) + m^2 \cdot st$, so m evenly divides $(a \times c) - (b \times d)$ and $a \times c \equiv b \times d \pmod{m}$.

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

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

Solution. Since $mx \equiv nx \pmod{p}$, p divides $mx - nx = x \cdot (m - n)$. Since p does not divide x, p must divide $m - n$, so $m \equiv n \pmod{p}$.

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 $5 \equiv 2 \pmod{6}$?
   Solution. No. $5 \not\equiv 2 \pmod{6}$ since 6 does not divide $5 - 2 = 3$.

   (b) We know that $25 \equiv 55 \pmod{6}$. Can we divide both sides by 5? Is $5 \equiv 11 \pmod{6}$?
   Solution. Yes. $5 \equiv 11 \pmod{6}$ since 6 does divide $5 - 11 = -6$.

   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 $3x \equiv 1 \pmod{10}$.
   Solution. By multiplying the first 9 natural numbers by 3, we have the sequence

$$3, 6, 9, 12, 15, 18, 21, 24, 27.$$

   The only x satisfying $3x \equiv 1 \pmod{10}$ is $x = 7$.

   (b) Find positive $x < 10$ such that $7x \equiv 1 \pmod{10}$.
   Solution. By multiplying the first 9 natural numbers by 7, we have the sequence

$$7, 14, 21, 28, 35, 42, 49, 56, 63.$$

   The only x satisfying $7x \equiv 1 \pmod{10}$ is $x = 3$.

   (c) Find positive $x < 10$ such that $9x \equiv 1 \pmod{10}$.
   Solution. By multiplying the first 9 natural numbers by 9, we have the sequence

$$9, 18, 27, 36, 45, 54, 63, 72, 81.$$

   The only x satisfying $9x \equiv 1 \pmod{10}$ is $x = 9$.

   (d) Can we find x such that $2x \equiv 1 \pmod{10}$?
   Solution. No. If there exists such an x, then $2x - 1$ is divisible by 10 and thus divisible by 2. However, $2x$ is even so $2x - 1$ is odd, so 2 cannot divide $2x - 1$.

   (e) Can we find x such that $5x \equiv 1 \pmod{10}$?
   Solution. No. If there exists such an x, then $5x - 1$ is divisible by 10 and thus divisible by 5. However, $5x$ is divisible by 5 and -1 is not so $5x - 1$ is never divisibly by 5.

(f) For what values of a can we find x such that $ax \equiv 1 \pmod{10}$?

Solution. Any value a in $\{1, 3, 7, 9\}$ works. Parts (a), (b), and (c) showed 3, 7, 9, while $a = 1$ has a solution of $x = 1$.

Values of a divisible by 2 or 5 does not work, as $ax - 1$ is never divisible by 2 when a is divisible by 2 and is never divisible by 5 when a is divisble by 5.

Because multiplication is preserved in modular arithmetic, any a that can be expressed as one of $\{1 + 10n, 3 + 10n, 7 + 10n, 9 + 10n\}$ for some integer n is possible.