26^{th} TJIMO

Alexandria, Virginia

Round: **Power**

1 Prime Mods

A *prime* p is defined as a number which has exactly two distinct divisors, 1 and p. Prime mods have many unique properties in modular arithmetic.

1. (a) Find $x < 5$ such that $2x \equiv 1 \pmod 5$.
   (b) Find $x < 5$ such that $3x \equiv 1 \pmod 5$.
   (c) Find $x < 5$ such that $4x \equiv 1 \pmod 5$.
   (d) For what a can we find an x such that $ax \equiv 1 \pmod 5$? For what a such that $0 \leq a < 5$ does no x exist such that $ax \equiv 1 \pmod 5$?

2. Let a be some nonzero number and p some prime. Let the sets A, B be defined as

$$A = \{1, 2, 3, \ldots, p-1\}$$
$$B = \{a, 2a, 3a, \ldots, (p-1)a\}.$$

   (a) Show that no two elements in B are equivalent modulo p. (Hint: Recall from the Practice Power that if a prime p evenly divides ab, then p must divide at least one of a or b.)
   (b) How many distinct elements are in B when taken modulo p?
   (c) Show that $A = B$ in modulo p. This means A and B, in modulo p contain the same elements.

3. For what a from $\{0, 1, 2, \ldots, p-1\}$ can we find an x such that $ax \equiv 1 \pmod p$ for some prime p? Also show that, if we can find such an x, the x is unique.

Problem 3 has shown that the integers modulo a prime constitute what is known as a *finite field*. Every nonzero value a in the field has a *multiplicative inverse*, or a number b such that $ab \equiv 1$.

4. (a) Find the smallest positive n such that $2^n \equiv 1 \pmod 3$.
   (b) i. Find the smallest positive n such that $2^n \equiv 1 \pmod 5$.
   ii. Find the smallest positive n such that $3^n \equiv 1 \pmod 5$.
   iii. Find the smallest positive n such that $4^n \equiv 1 \pmod 5$.
   iv. Find the smallest positive n such that $a^n \equiv 1 \pmod 5$ for all a not divisible by 5.
   (c) i. For every integer a in the set $\{1, 2, 3, 4, 5, 6\}$, find the smallest positive integer n such that $a^n \equiv 1 \pmod 7$.
   ii. Find the smallest positive n such that $a^n \equiv 1 \pmod{11}$ for all a not divisible by 11. Compare this with your result from part (b). What do you notice?

2 Fermat's Little Theorem

Fermat's Little Theorem states that $a^{p-1} \equiv 1 \pmod p$ for all primes p and all integers a not divisible by p. In this section you will put together the steps above to prove Fermat's Little Theorem.

5. Use problem 2 to show that $(p-1)! \equiv a^{p-1}(p-1)! \pmod{p}$.

6. (Fermat.) Show that $a^{p-1} \equiv 1 \pmod{p}$.

7. (a) Compute the remainder when 4^{45} is divided by 43.

   (b) Compute the remainder when 5^{1000} is divided by 7.

3 Wilson's Theorem

Wilson's Theorem states that $(n-1)! \equiv -1 \pmod{n}$ if and only if n is prime. In this section you will prove Wilson's Theorem from the steps above.

8. Verify Wilson's Theorem is true for $n = 5$ and $n = 6$.

9. First prove the only if direction: $(n-1)! \not\equiv -1 \pmod{n}$ if n is composite.

10. Now let's try the if direction: $(p-1)! \equiv -1 \pmod{p}$ for all primes p. First we'll split cases where p is odd and p is even. Prove Wilson's Theorem for all even primes p.

Recall from problem 3 we know every integer from $\{1, 2, \ldots, p-1\}$ has a unique multiplicative inverse modulo prime p. That means for a number a in $\{1, 2, \ldots, p-1\}$, there exists exactly one number b also in $\{1, 2, \ldots, p-1\}$ such that $ab \equiv 1 \pmod{p}$.

11. (a) Find the multiplicative inverses of 1 and $p-1$ modulo p.

    (b) Split the numbers $\{2, 3, 4, 5, 6, 7, 8, 9\}$ into four pairs, where each pair of numbers consists of multiplicative inverses modulo 11.

    (c) Show that the numbers from $\{2, 3, \ldots, p-2\}$ can be split into pairs where each pair consists of multiplicative inverses modulo p, where p is an odd prime.

12. Show that $(p-1)! \equiv -1 \pmod{p}$ for odd primes p.

Time limit: 45 minutes.