26^{th} TJIMO

ALEXANDRIA, VIRGINIA

Round: **Power Solutions**

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 $2x \equiv 1 \pmod 5$.
   Solution. $x = 3$, as $2 \cdot 3 - 1$ is divisible by 5.

   (b) Find $x < 5$ such that $3x \equiv 1 \pmod 5$.
   Solution. $x = 2$, as $3 \cdot 2 - 1$ is divisible by 5.

   (c) Find $x < 5$ such that $4x \equiv 1 \pmod 5$.
   Solution. $x = 4$, as $4 \cdot 4 - 1$ is divisible by 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 $ax \equiv 1 \pmod 5$?
   Solution. We can find a corresponding x for $a = 2, 3, 4$ as shown in parts (a), (b), and (c). For $a = 1$, the corresponding $x = 1$ as $1 \cdot 1 - 1$ is divisible by 5. However, there does not exist an x for $a = 0$, as $0 \cdot x = 0$ and -1 is not divisible by 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.)
   Solution. Suppose two elements in B were equivalent modulo p. Then we can write

$$a \cdot i \equiv a \cdot j \pmod p$$

   for some $i > j$. However, this means that

$$a \cdot (i - j) \equiv 0 \pmod p.$$

   However, p does not divide either a or $(i - j)$, so this is not possible.

   (b) How many distinct elements are in B when taken modulo p?
   Solution. Since no two elements in B are equivalent modulo p, there exist $p - 1$ distinct elements.

   (c) Show that $A = B$ in modulo p. This means A and B, in modulo p contain the same elements.
   Solution. Since both A and B are equivalent to exactly the $p - 1$ nonzero residues (that is, numbers) modulo p, $A = B$.

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.

   Solution. For any a from $\{1, 2, \ldots, p-1\}$ we can find an x such that $ax \equiv 1 \pmod{p}$, as from problem 2 the set $\{a, 2a, \ldots, (p-1)\cdot a\}$ is equivalent to the set $\{1, 2, \ldots p-1\}$.

   Note that this x is unique since all elements in the set $a, 2a, \ldots, (p-1)\cdot a$ are unique modulo p.

   For $a = 0$, no such x exists as for any x, $ax - 1 = -1$ is not divisible by p.

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 $2^n \equiv 1 \pmod{3}$.
   Solution. By listing the powers of 2 modulo 3, we have

   $$2 \equiv 2, 4 \equiv 1, \ldots$$

   so $n = 2$.

   (b) i. Find the smallest positive n such that $2^n \equiv 1 \pmod{5}$.
   Solution. By listing the powers of 2 modulo 5, we have

   $$2 \equiv 2, 4 \equiv 4, 8 \equiv 3, 16 \equiv 1 \ldots$$

   so $n = 4$.

   ii. Find the smallest positive n such that $3^n \equiv 1 \pmod{5}$.
   Solution. By listing the powers of 3 modulo 5, we have

   $$3 \equiv 3, 9 \equiv 4, 27 \equiv 2, 81 \equiv 1 \ldots$$

   so $n = 4$.

   iii. Find the smallest positive n such that $4^n \equiv 1 \pmod{5}$.
   Solution. By listing the powers of 3 modulo 5, we have

   $$3 \equiv 3, 9 \equiv 4, 27 \equiv 2, 81 \equiv 1 \ldots$$

   so $n = 4$.

   iv. Find the smallest positive n such that $a^n \equiv 1 \pmod{5}$ for all a not divisible by 5.
   Solution. From previous parts, $n = 4$ satisfies $a = 2, 3, 4$. For $a = 1$, we see $1^4 \equiv 1 \pmod{5}$. Because multiplication is preserved under modular arithmetic, this result can be extended to 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 $a^n \equiv 1 \pmod{7}$.
   Solution. By listing powers of numbers from $\{1, 2, 3, 4, 5, 6\}$, we see $n = 6$ satisfies

   $$1^6 \equiv 2^6 \equiv 3^6 \equiv 4^6 \equiv 5^6 \equiv 6^6 \equiv 1 \pmod{7}.$$

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?
Solution. By listing powers of numbers from $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, we see $n = 10$ satisfies
$$1^{10} \equiv 2^{10} \equiv 3^{10} \equiv \ldots \equiv 10^{10} \equiv 1 \pmod{11}.$$
In both cases, $n = p - 1$.

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 $(p-1)! \equiv a^{p-1}(p-1)! \pmod{p}$.

   Solution. We multiply all the numbers in each set together. However, we know the two sets are equivalent modulo p. Therefore the products must be equivalent modulo p as well. Thus
   $$(p-1)! \equiv a^{p-1}(p-1)! \pmod{p}.$$

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

   Solution. By rearranging the previous part, we have
   $$\begin{aligned} a^{p-1}(p-1)! - (p-1)! &\equiv 0 \pmod{p} \\ (a^{p-1} - 1)(p-1)! &\equiv 0 \pmod{p}. \end{aligned}$$
   Since p does not divide $(p-1)!$, we have p must divide $a^{p-1} - 1$. Therefore
   $$a^{p-1} \equiv 1 \pmod{p}.$$

7. (a) Compute the remainder when 4^{45} is divided by 43.
   Solution. By Fermat,
   $$\begin{aligned} 4^{45} &\equiv 4^{43} \cdot 4^2 \\ &\equiv 1 \cdot 4^2 \\ &\equiv 16 \pmod{43}. \end{aligned}$$

   (b) Compute the remainder when 5^{1000} is divided by 7.
   Solution. By Fermat,
   $$\begin{aligned} 5^{1000} &\equiv 5^{996} \cdot 5^4 \\ &\equiv (5^6)^{166} \cdot 5^4 \\ &\equiv 1^{166} \cdot 5^4 \\ &\equiv 625 \equiv 2 \pmod{7}. \end{aligned}$$

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 $n = 6$.

   Solution. For $n = 5$, $4! \equiv 24 \equiv -1 \pmod{5}$, which confirms Wilson's Theorem as 5 is prime.

   For $n = 6$, $5! \equiv 120 \not\equiv -1 \pmod{6}$, which confirms Wilson's Theorem as 6 is composite.

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

   Solution. If n is composite, it is either a square of a prime or can be expressed as $a \cdot b$ for $a < b \leq n-1$. In the latter case, it is easy to see that $(n-1) \equiv 0 \not\equiv 1 \pmod{n}$.

   In the former case, Let $n = q^2$ for some prime q. $(q^2-1)!$ is divisible by q exactly $q-1$ times. If $q = 2$, then $(4-1)! \equiv 2 \pmod{4}$. Otherwise, $(q^2-1)!$ is again divisible by q^2, and $(n-1)! \equiv 0 \pmod{n}$.

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.

    Solution. The only even prime is $p = 2$. Then we need only confirm Wilson's Theorem for $p = 2$, which follows since $1 \equiv -1 \pmod{2}$.

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.
    Solution. The multiplicative inverse of $1 \pmod{p}$ is 1.
    The multiplicative inverse of $p-1 \pmod{p}$ is $p-1$, since $(p-1)^2 \equiv p^2 - 2p + 1 \equiv 1 \pmod{p}$.

    (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.
    Solution. The following pairing of the numbers works:

    $$(2, 6), (3, 4), (5, 9), (7, 8).$$

    (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.
    Solution. Every number from the set has a unique multiplicative inverse. Furthermore, this multiplicative inverse is not the number itself, as otherwise we have

    $$\begin{aligned} a^2 &\equiv 1 \pmod{p} \\ a^2 - 1 &\equiv 0 \pmod{p} \\ (a-1)(a+1) &\equiv 0 \pmod{p} \end{aligned}$$

so p must divide either $a-1$ or $a+1$, but since $2 \leq a \leq p-2$ it cannot be either. Thus we can pair all the numbers together.

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

    Solution. Since we can pair all numbers from $\{2, 3, \ldots, p-2\}$ together, we have

$$\begin{aligned}(p-1)! &\equiv 1 \cdot (1 \cdot 1 \cdot \cdots \cdot 1) \cdot (p-1) \\ &\equiv p-1 \\ &\equiv -1 \pmod{p}.\end{aligned}$$