JV: Modular Inverses

Gunmay Handa

1 Warm-up Questions

1. Find all values of x such that $37x \equiv 25 \pmod{39}$.
2. (Wilson's Theorem) Let p be a prime. Show that $(p-1)! \equiv -1 \pmod{p}$.
3. Determine the remainder when 2^{2015} is divided by 2017.

2 Problems

1. Find all the values of x such that $31x \equiv 1 \pmod{37}$.
2. Find all solutions x to the following equations (or state that none exist).
   (a) $7x \equiv 1 \pmod{24}$.
   (b) $6x \equiv 1 \pmod{22}$.
   (c) $18x \equiv 20 \pmod{45}$.
   (d) $48x \equiv 20 \pmod{247}$.
3. Compute all integer solutions (x, y) to $17x + 53y = 1$.
4. (CMIMC 2016) Determine the smallest positive prime p which satisfies the congruence
$$p + p^{-1} \equiv 25 \pmod{143}.$$
Here, p^{-1} as usual denotes multiplicative inverse.
5. Let n be the integer such that
$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{23} = \frac{n}{23!}$$
Compute the remainder when n is divided by 13.
6. Let p be an odd prime. Prove that $1^2 \cdot 3^2 \ldots \cdot (p-2)^2 \equiv 1 \pmod{p}$.
7. Let a, n be natural numbers such that $\gcd(a, n) = 1$. Prove that
$$\{a \,(\text{mod } n), 2a \,(\text{mod } n), 3a \,(\text{mod } n), \ldots, (n-1)a \,(\text{mod } n)\} = \{1, 2, \ldots, n-1\}$$

3 Challenge Problems

1. (IMO 1996) The positive integers a and b are such that the numbers $15a+16b$ and $16a-15b$ are both squares of positive integers. What is the least possible value that can be taken on by the smaller of these two squares?

2. (Wolstenholme's Theorem) Let $p > 5$ be a prime. Show that p^2 divides the numerator of the expression
$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1}.$$

Varsity: Chinese Remainder Theorem

David Altizio

4 Warm-up Questions

1. Here are a few questions to help you get re-acquainted with modular arithmetic.
   (a) Compute the remainder when $24^{50} - 15^{50}$ is divided by 13.
   (b) Let $N = \overline{a_0 a_1 a_2 \dots a_n}$ be an integer. Prove the divisibility rule for 9: N is divisible by 9 if and only if
   $$a_0 + a_1 + a_2 + \cdots + a_n$$
   is also divisible by 9.
   (c) Characterize all integer solutions (x, y) to the Diophantine equation $47x + 59y = 1$. Hence solve the equation $47x \equiv 1 \pmod{59}$.

2. (Concepts of Mathematics) Suppose m and n are relatively prime positive integers, and let a and b be arbitrary integers.
   (a) Let r and s be integers such that $mr \equiv 1 \pmod{n}$ and $ns \equiv 1 \pmod{m}$. Find an integer value of x in terms of a, b, m, n, r, s satisfying $x \equiv a \pmod{n}$ and $x \equiv b \pmod{n}$.
   (b) Suppose x and y are integers such that $x \equiv a \pmod{n}$ and $x \equiv b \pmod{m}$, and also $y \equiv a \pmod{n}$ and $y \equiv b \pmod{m}$. Show that $x \equiv y \pmod{mn}$.

5 Examples

1. Solve the system of equations
   $$x \equiv 2 \pmod{5} \qquad \text{and} \qquad x \equiv 8 \pmod{11}.$$

2. (AMC 10B 2011) What is the hundreds digit of 2011^{2011}?

3. (USAMO 2008) Prove that for each positive integer n, there are pairwise relatively prime integers $k_0, k_1, \dots, k_n$, all strictly greater than 1, such that $k_0 k_1 \dots k_n - 1$ is the product of two consecutive integers.

6 Problems

1. (Concepts of Mathematics) Determine the unknown digits a and b in the five-digit number $3a27b$ given that $3a27b \equiv 1 \pmod{9}$ and $3a27b \equiv 9 \pmod{11}$.

2. (Brilliant) What are the last two digits of 49^{19}?

3. (AMC 10B 2017) Let $N = 123456789101112 \dots 4344$ be the 79-digit number that is formed by writing the integers from 1 to 44 in order, one after the other. What is the remainder when N is divided by 45?

4. Let n be a positive integer. Determine the number of positive integers $x \in \{1, 2, \ldots, n\}$ such that $x^2 \equiv x \pmod{n}$.

5. (AIME II 2012) For a positive integer p, define the positive integer n to be p-safe if n differs in absolute value by more than 2 from all multiples of p. For example, the set of 10-safe numbers is $\{3, 4, 5, 6, 7, 13, 14, 15, 16, 17, 23, \ldots\}$. Find the number of positive integers less than or equal to $10,000$ which are simultaneously 7-safe, 11-safe, and 13-safe.

6. (CMIMC 2016, Andrew Kwon) Define a *tasty residue* of n to be an integer $1 \leq a \leq n$ such that there exists an integer $m > 1$ satisfying

$$a^m \equiv a \pmod{n}.$$

   Find the number of tasty residues of 2016.

7. (AoPS) The integer p is a 50 digit prime number. When its square is divided by 120, the remainder is not one. What is the remainder?

8. (Brilliant) Show that there exist 99 consecutive integers $a_1, a_2, \ldots, a_{99}$ such that each a_i is divisible by the cube of some integer greater than 1.

7 Challenge Problem

1. (Lemma used in CMIMC 2019) Let $p_1, p_2, \cdots, p_n$ be primes and $e_1, e_2, \cdots, e_n \in \{-1, 1\}$. Prove there exists a prime q with the property that $(\frac{p_i}{q}) = e_i$ for all $1 \leq i \leq n$. (Here $(\frac{p}{q})$ is the *Legendre symbol* which is 1 if p is a quadratic residue modulo q and -1 otherwise.)