JV: Modular Arithmetic

Zichao Dong

1 Warm-Up Problems

1. 11 girls and n boys picked $n^2 + 9n - 2$ mushrooms, and each kid picked equally many mushrooms. Are there more girls or boys?
2. Prove that congruence is an *equivalence relation*, that is for any integers a, b, c and $n > 1$,
   - $a \equiv a \pmod{n}$;
   - If $a \equiv b \pmod{n}$, then $b \pmod{a} \pmod{n}$;
   - If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.
3. Find the last digit of 7^{100}.

2 Problems

1. How many lattice points are on the line segment with endpoints $(0, 3)$ and $(100, 2019)$.
2. (PUMaC 2015) Find the remainder when
$$\sum_{n=0}^{100} 10^n$$
is divided by 9.
3. Find the remainder when $1! + 2! + \cdots + 100!$ is divided by 16.
4. (PUMaC 2018) Find the number of positive integers $n < 2018$ such that $25^n + 9^n$ is divisible by 13.
5. Suppose that a, b are digits in $\{1, 2, 3, 4, 5\}$ and the 7-digit number $30a0b03$ is divisible by 13. Compute the ordered pair (a, b).
6. (PUMaC 2014) What is the last digit of $17^{17^{17^{17}}}$?
7. Find the number of perfect squares in the sequence
$$4, 44, 444, 4444, \cdots$$
8. A sequence $\{x_n\}$ is given by $1, 3, 5, 11, \cdots$ such that $x_{n+1} = x_n + 2x_{n-1}$ for every $n \geqslant 2$. A sequence $\{y_n\}$ is given by $7, 17, 55, 161, \cdots$ such that $y_{n+1} = 2y_n + 3y_{n-1}$ for every $n \geqslant 2$. Find the number of common terms among $\{x_n\}$ and $\{y_n\}$.
9. Suppose that x, y, z are integers such that
$$(x - y)(y - z)(z - x) = x + y + z.$$
Prove that $27 \mid x + y + z$.

10. Let a and b be distinct 7-digit numbers, each of which uses the digits $1, 2, 3, 4, 5, 6, 7$ exactly once apiece. Is it possible that $a \mid b$?

3 Challenge Problem

1. (ARML 2018 TB-1) The increasing infinite arithmetic sequence $x_1, x_2, x_3, \cdots$ contains the terms 17! and 18!. Compute the greatest integer X for which $X!$ must also appears in the sequence.

4 Definitions/Review

- Given integers a, b, c where $b \neq 0$, we write $a \equiv c \pmod{b}$ if b divides $(a - c)$.

Varsity: Euclidean Algorithm and Modular Inverses

Ariel Uy

5 Definitions/Review

Definition 1. Given integers a, b, c where $b \neq 0$, we write $a \equiv c \pmod{b}$ if b divides $(a - c)$.

Definition 2 (Mod inverse)**.** If $ax \equiv 1 \pmod{b}$, then we say x is a multiplicative modular inverse (mod b) of a.

Definition 3 (The Euclidean Algorithm)**.** Given integers a, b, the series of divisors $q_1, q_2, \ldots$ such that $a = bq_1 + q_2, b = q_2q_3 + q_4, q_2 = q_4q_5 + q_6, \ldots$ (see example). The final value (when the other is 0) gives $\gcd(a, b)$, i.e. the greatest common divisor of a and b.

Example 4. Find $\gcd(126, 224)$.

Solution.

$$\begin{aligned} \gcd(126, 224) &= \gcd(126, 224 - 126) & 224 &= 1 \times 126 + 98 \\ \gcd(126, 98) &= \gcd(98, 126 - 98) & 126 &= 1 \times 98 + 28 \\ \gcd(98, 28) &= \gcd(28, 98 - 3 \cdot 28) & 98 &= 3 \times 28 + 14 \\ \gcd(28, 14) &= \gcd(14, 28 - 2 \cdot 14) & 28 &= 2 \times 14 + 0 \\ &= \gcd(14, 0) \end{aligned}$$

Thus, $\gcd(126, 224) = \boxed{14}$.

Theorem 5 (Bezout's Lemma)**.** Given nonzero integers a, b and their greatest common divisor d, there exist integers x, y such that $ax + by = d$.

6 Warm-Up Problems

1. Find x that satisfies each of the following equations:
   $5x \equiv 1 \pmod{8}$
   $5x \equiv 2 \pmod{8}$
   $5x \equiv 3 \pmod{8}$
   $5x \equiv 6 \pmod{8}$

2. Is it possible to find x such that $6x \equiv 1 \pmod{8}$? If yes, give an example. If not, explain why.

3. Find the last digit of 7^{100}.

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 - $pp^{-1} \equiv 1 \pmod{143}$.

5. Let $a \geq b$. Prove that $\gcd(a, b) = \gcd(a - b, b)$. Now prove that $\gcd(a, b) = \gcd(a \mod b, b)$.

7 Problems

1. Find $\gcd(221, 299)$ and $\gcd(2520, 399)$ using the Euclidean algorithm.
2. Find a pair of integers (x, y) such that $102x + 38y = 2$.
3. (IMO 1959) Prove that the fraction $\frac{21n+4}{14n+3}$ is irreducible for every natural number n.
4. $56a = 65b$, where a, b are positive integers. Prove that $a + b$ is composite.
5. (AIME 1985) The numbers in the sequence 101, 104, 109, 116,... are of the form $a_n = 100+n^2$, where $n = 1, 2, 3, \ldots$ For each n, let d_n be the greatest common divisor of a_n and a_{n+1}. Find the maximum value of d_n as n ranges through the positive integers.
6. Compute $gcd(F_{100}, F_{99})$ and $gcd(F_{100}, F_{96})$, where F_i is the ith Fibonacci number. (Don't try to compute F_{100}, F_{99}, or F_{96}).
7. (ARML 2018 TB-1) The increasing infinite arithmetic sequence $x_1, x_2, x_3, \cdots$ contains the terms 17! and 18!. Compute the greatest integer X for which $X!$ must also appears in the sequence.
8. Assume prime $p \geq 5$. If $1 + \frac{1}{2} + \cdots + \frac{1}{p-1} = \frac{m}{n}$ where m, n are coprime. Show that $p^2 \mid m$.
9. For positive integers m, n, find $\gcd(2^m - 1, 2^n - 1)$.
10. (AMC 2007) How many pairs of positive integers (a, b) are there such that $\gcd(a, b) = 1$ and
$$\frac{a}{b} + \frac{14b}{9a}$$
is an integer?

8 Challenge Problems

1. Prove Bezout's Lemma as stated prior.
2. (2018 USAJMO) Let p be a prime, and let $a_1, \ldots, a_p$ be integers. Show that there exists an integer k such that the numbers
$$a_1 + k, a_2 + 2k, \ldots, a_p + pk$$
produce at least $\frac{1}{2}p$ distinct remainders upon division by p.
3. (2013 AIME) Ms. Math's kindergarten class has 16 registered students. The classroom has a very large number, N, of play blocks which satisfies the conditions:
   (a) If 16, 15, or 14 students are present in the class, then in each case all the blocks can be distributed in equal numbers to each student, and
   (b) There are three integers $0 < x < y < z < 14$ such that when x, y, or z students are present and the blocks are distributed in equal numbers to each student, there are exactly three blocks left over.

   Find the sum of the distinct prime divisors of the least possible value of N satisfying the above conditions.