Number Theory IMO Problems

Joshua Maglione

16 November 2024

Some IMO problems dealing with Number Theory

IMO 1994

Problem 4. Find all ordered pairs (m, n) where m and n are positive integers such that

$$\frac{n^3 + 1}{mn - 1}$$

is an integer.

IMO 2003

Problem 2. Determine all pairs of positive integers (a, b) such that

$$\frac{a^2}{2ab^2 - b^3 + 1}.$$

IMO 2006

Problem 5. Let $P(x)$ be a polynomial of degree $n > 1$ with integer coefficients, and let k be a positive integer. Consider the polynomial

$$Q(x) = P(P(\dots P(P(x))\dots)),$$

where P occurs k times. Prove that there are at most n integers t such that $Q(t) = t$.

IMO 2015

Problem 2. Determine all triples of positive integers (a, b, c) such that each of the numbers

$$ab - c, \qquad bc - a, \qquad ca - b$$

is a power of 2.

(A power of 2 is an integer of the form 2^n where n is a non-negative integer.)

IMO 2020

Problem 5. A deck of $n > 1$ cards is given. A positive integer is written on each card. The deck has the property that the arithmetic mean of the numbers on each pair of cards is also the geometric mean of the numbers on some collection of one or more cards.

For which n does it follow that the numbers on the cards are all equal?

USA Junior MO 2021

Problem 5. A finite set S of positive integers has the property that, for each $s \in S$, and each positive integer divisor d of s, there exists a unique element $t \in S$ satisfying $\gcd(s, t) = d$. (The elements s and t could be equal.)

Given this information, find all possible values for the number of elements of S.

What is Number Theory?

Number Theory broadly speaking is the study of whole numbers, or what we call **integers**. These are the numbers

$$\{\ldots, -2, -1, 0, 1, 2, \ldots\},$$

and this set is often denoted by $\mathbb{Z}$. (Here the Z is due to the German word for numbers: Zahlen.)

Number theory is one of the oldest disciplines in mathematics. Some of the major topics in the field are

1. the study of **prime numbers**, which are integers with exactly two divisors,
2. the study of integer solutions to equations.

Number theory is a field of **pure mathematics**, and thanks to centuries of research effort, it has applications in areas such as **cryptography**. We use number theory every time we encrypt data like passwords or other personal information. Every time you log into an account, passwords are encrypted and sent over the internet.

Integer solutions to equations

One area of number theory studies the integer solutions to equations. For example, are there positive integers (a, b, c) such that

$$a^2 + b^2 = c^2?$$

There are indeed solutions—for example $(3, 4, 5)$, $(5, 12, 13)$, and $(85, 132, 157)$. How many are there, and how do we find them all?

This style of problem is called a **Diophantine equation**, where one considers the integer solutions to a polynomial equation. One of the most famous Diophantine equations is the subject of **Fermat's Last Theorem**.

Fermat's Last Theorem (proved by Wiles 1994 and Taylor–Wiles 1995). There are no positive integer solutions for $n > 2$ to the equation

$$x^n + y^n = z^n.$$

There is a massive amount of history and breakthroughs leading to the proof. Pierre de Fermat claimed a proof around 1637. People that worked on this problem include

- Abu-Mahmud Khujandi (independently),
- Leonhard Euler,
- Sophie Germain,
- Carl Friedrich Gauss.

Primes and modular arithmetic

One of the oldest results on prime numbers is the fact that there are infinitely many primes. At the heart of studying prime numbers is the notion of divisibility.

Suppose a and b are integers. We say that a **divides** b if there is an integer c such that $b = ac$. We express this fact by writing $a \mid b$.

Along with division, we have **remainders** and the **modulus operator** is a way to keep track of remainders. For example, we know that 4 divides into 7 one time with a remainder of 3. We could keep track of this by writing

$$7 \equiv 3 \pmod 4.$$

Here, we express that 7 and 3 have the same number of remainders when dividing by 4. In symbols, we could write $7 = 3 + 4$. We also have

$$2 \equiv 6 \equiv 34 \equiv -102 \pmod 4.$$

In other words, each integer $2, 6, 34, -102$ has remainder 2 when we divide them by 4 as much as we can. In symbols, we can write

$$\begin{aligned} 6 &= 2 + 4, \\ 34 &= 2 + 32 = 2 + 4 \cdot 8, \\ -102 &= 2 - 104 = 2 + 4 \cdot (-26). \end{aligned}$$

The numbers $2, 6, 34, -102$ all diff by a **multiple of 4**.

In general, for integers a, b, and n, we write

$$a \equiv b \pmod n$$

if there is an integer k such that $a = b + nk$.

Try these problems.

1. What can we conclude about the integer a if

   $$a \equiv 0 \pmod n?$$

2. What kinds of integers b satisfy

   $$b \equiv 1 \pmod 2?$$

3. Suppose you leave from Dublin Airport at 11:00am and you fly to Rome (one hour ahead), which takes 3 hours. Using modular arithmetic, express when in the afternoon you land.

4. Let a, b, c, d, n be integers and assume that

   $$\begin{aligned} a &\equiv b \pmod n \\ c &\equiv d \pmod n. \end{aligned}$$

   Prove that

   $$\begin{aligned} a + c &\equiv b + d \pmod n \\ ac &\equiv bd \pmod n. \end{aligned}$$

5. Determine at least 3 integers for x that satisfy

   $$5x \equiv 6 \pmod 8.$$

6. Determine the last digit (i.e. one's digit) of 11^{2024}.

7. We write $n! = 1 \cdot 2 \cdots (n-1) \cdot n$. Find an x that solves the following equation:
$$1! + 2! + 3! + 4! + 5! + \cdots \equiv x \pmod 9.$$

8. Find a pair of integers x and y in $\{1, 2, \ldots, 13\}$ such that
$$xy \equiv 0 \pmod{14}.$$
Suppose N is a positive composite integer (i.e. not prime). Can you always find a pair of integers x and y in $\{1, 2, \ldots, N-1\}$ such that
$$xy \equiv 0 \pmod N?$$

9. Assume that p is a prime number. Show that there is no pair x and y in $\{1, 2, \ldots p-1\}$ such that
$$xy \equiv 0 \pmod p.$$

Fermat's Little Theorem. Let p be a prime and a an integer that is not divisible by p. Then
$$a^{p-1} \equiv 1 \pmod p.$$
As a consequence, we get
$$a^p \equiv a \pmod p.$$