

Number Theory & IMO Problems

Joshua Maglione

8 November 2025

- Some IMO problems dealing with Number Theory
 - IMO 1994
 - IMO 2003
 - Indonesia MO 2005
 - IMO 2006
 - IMO 2015
 - IMO 2020
 - USA Junior MO 2021
- What is Number Theory?
- Integer solutions to equations
 - A brief introduction to elliptic curves
- Primes and modular arithmetic
- Solutions
 - IMO 1994 P4
 - IMO 2015 P2

Download the PDF if you want



<https://tinyurl.com/SME25-NT>

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

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

Indonesia MO 2005

Problem 2. For an arbitrary positive integer n , define $p(n)$ as the product of the digits of n (in decimal). Find all positive integers n such that

$$11p(n) = n^2 - 2005.$$

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

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

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

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

and this set is often denoted by $\mathbb{Z}$. (Here the $\mathbb{Z}$ 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.

The proof of Wiles and Taylor & Wiles actually proves a much stronger statement about **elliptic curves**.

A brief introduction to elliptic curves

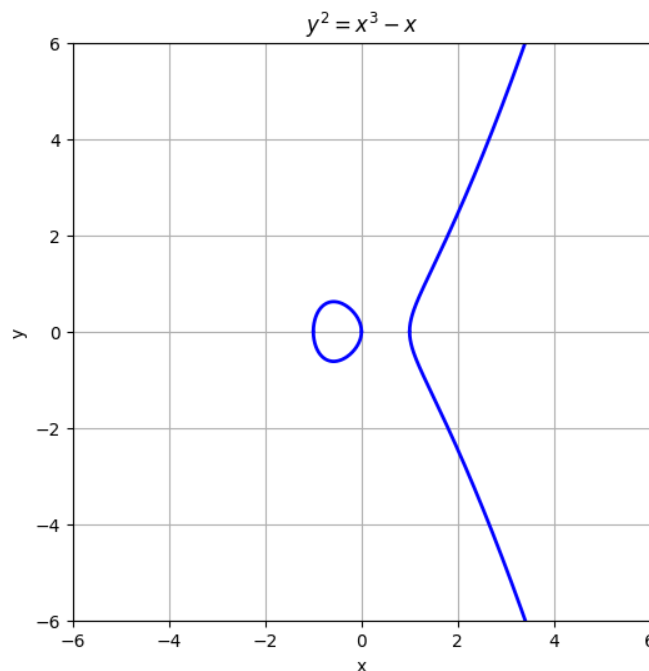
Let a and b be rational numbers with

$$4a^3 + 27b^2 \neq 0.$$

An **elliptic curve** is the set of points (x, y) that satisfy

$$y^2 = x^3 + ax + b.$$

Here is a plot of an elliptic curve with $(a, b) = (-1, 0)$:



You can follow this link to see a Desmos plot of $y^2 = x^3 + ax + b$ where you can play around with values for a and b :

<https://www.desmos.com/calculator/qtikf2suwm>

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 $\{1, 2, \dots, 13\}$ 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 $\{1, 2, \dots, N-1\}$ 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 $\{1, 2, \dots, p-1\}$ 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

$$a^p \equiv a \pmod{p}.$$

Solutions

These solutions purposefully contain gaps. See if you can fill them yourself. Otherwise, feel free to email me: joshua.maglione@universityofgalway.ie.

IMO 1994 P4

We want to determine all of the positive integers m and n such that

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

is an integer. So let's assume $\ell = (n^3 + 1)/(mn - 1)$ is an integer. Therefore,

$$n^3 + 1 = (mn - 1)\ell. \tag{1}$$

We take both sides of Equation (1) modulo n , and we find that $1 \equiv -\ell \pmod{n}$. In other words, $\ell \equiv -1 \pmod{n}$. This means that there exists a positive integer a such that $\ell = an - 1$.

Now consider the quadratic polynomial in the variable x :

$$x^2 - amx + a + m = 0.$$

Claim: Show that n is a root of this quadratic polynomial. Show that the other root, call it b , is also a positive integer.

From the claim, it follows that

$$bn = a + m, \tag{2}$$

$$b + n = am. \tag{3}$$

Let's consider the case where all four integers a, b, m, n are greater than 1. We see that $(a, b, m, n) = (2, 2, 2, 2)$ works in Equations (2) and (3). Indeed,

$$\frac{2^3 + 1}{2 \cdot 2 - 1} = 3,$$

so $(m, n) = (2, 2)$ is one solution. Still assuming that a, b, m, n are greater than 1, we furthermore assume $(a, b, m, n) \neq (2, 2, 2, 2)$. Now $bn > b + n$ and $am > a + m$. **Claim:** This leads to a contradiction, so $(2, 2, 2, 2)$ is the only solution when all four integers are greater than 1. Therefore at least one of a, b, m, n is 1.

Claim: There are eight more solutions, for a total of nine solutions including $(m, n) = (2, 2)$.

IMO 2015 P2

We need to determine all triples of positive integers (a, b, c) such that $ab - c, bc - a, ca - b$ are powers of 2. Observe that if we change the order of (a, b, c) , we do not change the values of $ab - c, bc - a, ca - b$.

Therefore, we can assume we rearrange the integers so that $a \leq b \leq c$. Let m, n, ℓ be non-negative integers such that

$$ab - c = 2^m, \quad ca - b = 2^n, \quad bc - a = 2^\ell.$$

Since $a \leq b \leq c$, we have $m \leq n \leq \ell$.

Claim: Show that $a > 1$, and use this to show that $n \geq 1$.

Case 1: $a = 2$.

Therefore,

$$2b - c = 2^m, \quad 2c - b = 2^n, \quad bc - 2 = 2^\ell.$$

Since $n \geq 1$, the second equation implies that b is even. If $\ell = 1$, then the third equation is $bc = 4$. This means that $b = c = 2$. This is our first solution: $(a, b, c) = (2, 2, 2)$. Now we assume $\ell > 1$.

Claim: Conclude that c is odd, so that $m = 0$.

Therefore,

$$2^n + 2 = 2^n + 2 \cdot 2^m = 2c - b + 2(2b - c) = 3b, \quad (4)$$

so $n \geq 2$. Similarly,

$$2 \cdot 2^n + 1 = 2 \cdot 2^n + 2^m = 2(2c - b) + (2b - c) = 3c. \quad (5)$$

Putting both Equations (4) and (5) together (and dividing by 2) yields

$$(2^{n-1} + 1)(2^{n+1} + 1) = \frac{9}{2}bc = 9(2^{\ell-1} + 1).$$

Since $n \leq \ell$,

$$1 \equiv (2^{n-1} + 1)(2^{n+1} + 1) = 9(2^{\ell-1} + 1) \equiv 9,$$

where all equivalences are modulo 2^{n-1} . Hence, $n \leq 4$, so $2 \leq n \leq 4$. From either Equations (4) or (5), we see that $n = 3$ is impossible. **Claim:** We get exactly two more solutions in this case. [One in each case.]

Case 2: $a \geq 3$.

First, we establish that $a \neq b$. Suppose that $a = b$; we will show that this leads to a contradiction. It follows that

$$2^n = ca - b = a(c - 1),$$

so both a and $c - 1$ are powers of 2. Moreover,

$$2^m = ab - c = a^2 - c.$$

Claim: $c + 1$ is a power of two, so we conclude that $c = 3$. Thus, $a = b = c = 3$, but this is impossible since a is a power of 2. Hence, $a < b$.

Since $b \leq c$, we have

$$(a - 1)c = ac - c \leq ac - b = 2^n,$$

Since $a \geq 3$, it follows that $c \leq 2^{n-1}$. Since $3 \leq a < b$,

$$a + b < 2c \leq \frac{2^{n+1}}{a - 1} \leq 2^n.$$

Additionally, $b < a + c$, so $b - a < c \leq 2^{n-1}$. Putting this together, we have shown that

$$b - a < 2^{n-1} \quad b + a < \frac{2^{n+1}}{a - 1} \leq 2^n.$$

We will use these to relate them to sums and differences of 2^n and 2^ℓ :

$$\begin{aligned} 2^\ell - 2^n &= bc - a - ca + b = (c + 1)(b - a), \\ 2^\ell + 2^n &= bc - a + ca - b = (c - 1)(b + a). \end{aligned}$$

Since $a < b$, we have $n < \ell$. Moreover, $2^\ell - 2^n$ and $2^\ell + 2^n$ are divisible by 2^n . Since $b - a < 2^{n-1}$, it follows that $b - a$ is divisible by at most 2^{n-2} , so $c + 1$ is divisible by 4. Hence, $c - 1$ is not divisible by 4 but by 2. This implies that $b + a$ is divisible by 2^{n-1} . Since $b + a < 2^n$ and $b + a$ is a multiple of 2^{n-1} , it follows that $b + a = 2^{n-1}$. Therefore,

$$2^{n-1} = b + a < \frac{2^{n+1}}{a-1},$$

so $a - 1 < 4$. In other words, a is either 3 or 4.

Assume $a = 3$, so

$$3b - c = 2^m, \quad 3c - b = 2^n, \quad b + 3 = 2^{n-1}.$$

Thus, $b = 2^{n-1} - 3$ and $c = 2^{n-1} - 1$, so

$$bc - a = 2^{2n-2} - 2^{n+1} = 2^{n+1}(2^{n-3} - 1).$$

Since $bc - a$ is a power of 2, we have $n = 4$. Hence, $(a, b, c) = (3, 5, 7)$ is a solution.

Assume $a = 4$. **Claim:** There are no additional solutions.