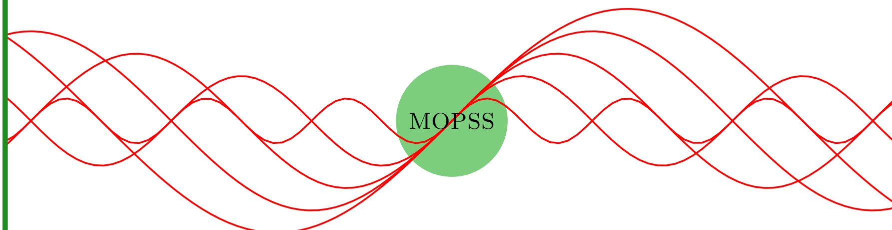
MOPSS

31 July 2025

Mathematics Olympiad

Problem Solving Sessions



DEPARTMENT OF MATHEMATICS
IISER BHOPAL

https://jpsaha.github.io/MOTP/MOPSS/

Suggested readings

- Evan Chen's advice On reading solutions, available at https://blog.evanchen.cc/2017/03/06/on-reading-solutions/.
- Evan Chen's Advice for writing proofs/Remarks on English, available at https://web.evanchen.cc/handouts/english/english.pdf.
- Notes on proofs by Evan Chen from OTIS Excerpts [Che25, Chapter 1].
- Tips for writing up solutions by Edward Barbeau, available at https://www.math.utoronto.ca/barbeau/writingup.pdf.
- Evan Chen discusses why math olympiads are a valuable experience for high schoolers in the post on Lessons from math olympiads, available at https://blog.evanchen.cc/2018/01/05/lessons-from-math-olympiads/.

List of problems and examples

§1 Part A

Exercise 1.1. Determine if the product of some four consecutive integers can be equal to the product of a few consecutive primes.

> **Walkthrough** — The product of any four consecutive positive integers is a multiple of 4.

Exercise 1.2. Suppose we are given a positive integer, and any of its digits is equal to 0 or 6. Show that the given integer is not a perfect square.

> **Walkthrough** —
>
> **(a)** Show that the last two digits of a square cannot be 06 or 66.
>
> **(b)** Conclude that the last two digits are equal to 00.

(c) Use this argument repeatedly.

Example 1.3 (Bay Area MO 1999 P1)**.** Prove that among any 12 consecutive positive integers, there is at least one which is smaller than the sum of its proper divisors. (The proper divisors of a positive integer n are all positive integers other than 1 and n which divide n. For example, the proper divisors of 14 are 2 and 7.)

Walkthrough — $3, 4, \ldots$!

Solution 1. Among any twelve consecutive integers, there is a multiple of 12. For any positive integer n, note that

$$3n, 4n, 6n$$

are proper divisors of $12n$, and

$$12n < 3n + 4n + 6n$$

holds. This completes the proof. ■

Remark. Note that

$$\begin{aligned} 2^2 &= 4, \\ 2^6 &= 64, \\ 2^5 &= 32, \\ 2^{25} &= 33554432 \end{aligned}$$

holds. This shows that there are distinct powers of 2 whose last digits are equal, and that there are distinct powers of 2 whose blocks of last two digits are the same. This leads to the following questions.

Exercise 1.4. Are there two powers of 2 such that the blocks of their last three digits are the same?

Walkthrough — Apply the pigeonhole principle to all powers of 2, considering their last three digits.

Exercise 1.5. Are there two powers of 2 such that the blocks of their last 2025 digits are the same?

Remark. Observe that both of the integers $3457, 7453$ leave a remainder of 1 when divided by 9. Note that

(i) 3000 differs from 3 by a multiple of 9,

(ii) 400 differs from 4 by a multiple of 9,

(iii) 50 differs from 5 by a multiple of 9,

(iv) 7 differs from 7 by a multiple of 9,

and hence 3457 differs from the sum $3 + 4 + 5 + 7$ by a multiple of 9.

Exercise 1.6. Suppose we are given a positive integer. We interchange its digits to form another integer. Show that these two integers leave the same remainder when divided by 9.

Walkthrough — Does the above remark help?

Remark. One may move towards discussing criteria for divisibility by $3, 9$, $2, 4, 8, 16$, 11 etc.

Exercise 1.7. Note that $3, 5, 7$ are three consecutive odd integers and all of them are primes. How many such examples of three consecutive odd integers are there such that all of them are primes?

Remark. Examples of three consecutive odd integers include

- $11, 13, 15$,
- $25, 27, 29$,
- $37, 39, 41$.

Example 1.8. [**FGI96**, Problem 83, p. 72] Prove that if a prime number is divided by 30, the remainder is a prime or 1.

Solution 2. Let p be a prime number. If p is less than 5, then we are done. Henceforth, let us assume that $p \geq 5$. It follows that p is of the form $6k \pm 1$ for some positive integer k. If $k \equiv 1 \pmod 5$, then p is equivalent to one of $5, 7$ modulo 30. If $k \equiv 2 \pmod 5$, then p is equivalent to one of $1, 3$ modulo 30. If $k \equiv 3 \pmod 5$, then p is equivalent to 2 modulo 30. If $k \equiv 4 \pmod 5$, then p is equivalent to one of $3, 5$ modulo 30. This completes the proof. ■

Example 1.9 (Infinitude of primes)**.** [**Sai06**] Let $a_1, a_2, a_3, a_4, a_5, \ldots$ be a sequence of integers such that

$$a_1 = 2,$$

$$\begin{aligned} a_2 &= a_1(a_1+1), \\ a_3 &= a_2(a_2+1), \\ a_4 &= a_3(a_3+1), \\ a_5 &= a_4(a_4+1), \\ a_6 &= a_5(a_5+1) \end{aligned}$$

etc. holds, that is, for any positive integer n,

$$a_{n+1} = a_n(a_n+1)$$

holds. Show that a_n has at least n distinct prime factors for any positive integer n.

> **Walkthrough** — Check it for first few values to n. Expect that **the pattern will continue!** Try to figure out what more to do to see/get convinced/prove/establish that the pattern **does continue**.
>
> This is important since the statement that EVERY POSITIVE INTEGER n IS SMALLER THAN 1000 is true for first few values of n! However, "the pattern" does **not** continue in this case. The **upshot** is that observing a pattern does **not** guarantee its validity all throughout.

> **Walkthrough** —
>
> **(a)** Show that $a_n \geq 2$ for any integer $n \geq 1$.
>
> **(b)** Note that the integers $a_n, a_n + 1$ have no common prime factor.
>
> **(c)** Conclude using induction.

> **Remark.** This shows that the list of primes does not stop anywhere.

Exercise 1.10. Show that for any odd prime number p, the numerator of the rational number

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{p-1}$$

is divisible by p.

> **Walkthrough** — Let S denote the above sum. Consider $2S$ and arrange the summands suitably.

Example 1.11. Among any four consecutive positive integers, one of them is coprime to (that is, no common factor with) the remaining three.

> **Walkthrough** — Show that among any four consecutive positive integers, at least one of the odd integers is not divisible by 3. Consider the case when this odd integer is equal to 1, and the case when it it greater than one. In the second case, find a suitable prime divisor of this odd integer.

Proof. Note that among any four consecutive positive integers, at least one of the odd integers is not divisible by 3, and hence, either it is equal to 1, in which case it is coprime to the remaining ones, or it is greater than one, and its smallest prime factor is at least 5, and hence, it is coprime to the remaining ones. □

Exercise 1.12 (Tournament of Towns, Spring 2019, Junior, O Level, P4 by Boris Frenkin)**.** The product of two positive integers m and n is divisible by their sum. Prove that $m + n \leq n^2$.

> **Walkthrough** — Note that if $m + n$ divides mn, then $m + n$ divides $n(m + n) - mn$.

Exercise 1.13. Show that a perfect square leaves 0 or 1 as the remainder upon division by 4.

> **Walkthrough** — Consider the squares of $2n$ and $2n + 1$.

Exercise 1.14. If an integer leaves a remainder of 3 upon division by 4, then it cannot be expressed as a sum of two squares.

> **Walkthrough** — Use the above Exercise.

Exercise 1.15. Is 2025^{2025} divisible by 23? If not, what would be the remainder when it is divided by 23?

> **Walkthrough** — Check that $2025 \equiv 1 \pmod{23}$.

Exercise 1.16. Determine the remainder to be obtained when 133^{133} is divided by 13.

Exercise 1.17. No integer that leaves a remainder of 7 upon division by 8 can be expressed as a sum of three squares.

Walkthrough — Try to read the squares modulo 8.

Exercise 1.18 (Tournament of Towns, Fall 2019, Junior, O Level, P4 by Boris Frenkin)**.** There are given 1000 integers $a_1, \dots, a_{1000}$. Their squares $a_1^2, \dots, a_{1000}^2$ are written along the circumference of a circle. It so happened that the sum of any 41 consecutive numbers on this circle is a multiple of 41^2. Is it necessarily true that every integer $a_1, \dots, a_{1000}$ is a multiple of 41?

Remark. Replace 1000 by 10 and 41 by 7, and try to work on the problem.

Solution 3. For any integer m, let $\overline{m}$ denote the integer lying between 1 and 1000, which is congruent to m modulo 1000. Note that

$$a_i^2 \equiv a_j^2 \bmod 41^2$$

holds for any integers i, j lying between 1 and 1000, and satisfying $i \equiv j \bmod 41$. It follows that

$$a_1^2 \equiv a_{\overline{41k+1}}^2 \bmod 41^2$$

for any integer k. Since the integers $41, 1000$ are relatively prime, it follows that the integers

$$41, 41 \cdot 2, 41 \cdot 3, \dots, 41 \cdot 1000$$

are pairwise distinct modulo 1000, that is, these integers are congruent to $1, 2, \dots, 1000$ modulo 1000 in some order. This shows that a_1^2 is congruent to a_i^2 modulo 41^2 for any integer $1 \leq i \leq 1000$. It follows that

$$41a_1^2 \equiv a_1^2 + a_2^2 + \dots + a_{41}^2 \bmod 41^2$$

Since the sum $a_1^2 + a_2^2 + \dots + a_{41}^2$ is divisible by 41^2, this shows that 41 divides a_1. For any integer $1 \leq i \leq 1000$, 41^2 divides $a_1^2 - a_i^2$, and using that 41 divides a_1, we obtain 41 divides a_i.

This proves that it is necessary that every integer $a_1, \dots, a_{1000}$ is a multiple of 41. ■

Exercise 1.19 (India RMO 2017a P2)**.** Show that the sum of the cubes of any seven consecutive integers cannot be expressed as the sum of the fourth powers of two consecutive integers.

Walkthrough — Read it modulo ___!

Solution 4. Note that the fourth powers of the integers $0, 1, 2, 3, 4, 5, 6$ are congruent to $0, 1, 2, 4, 4, 2, 1$ modulo 7 respectively. The shows that the sum of the fourth powers of two consecutive integers is congruent to one of

$$0 + 1, 1 + 2, 2 + 4, 4 + 2, 2 + 1, 1 + 0$$

modulo 7. Hence, the sum of the fourth powers of two consecutive integers is not divisible by 7. Also note the cubes of seven consecutive integers is congruent to

$$0^3 + 1^3 + 2^3 + 3^3 + 4^3 + 5^3 + 6^3$$

modulo 7, which is congruent to

$$1^3 + 2^3 + 3^3 + (-3)^3 + (-2) + (-1)^3 = 0$$

modulo 7. This shows that the sum of the cubes of seven consecutive integers is not equal to the sum of the fourth powers of two consecutive integers. This completes the proof. ■

§2 Congruences

Consider the integers $0, 1, 2, 3, \ldots$. Dividing them by 2 yields

$$0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, \ldots$$

as the respective remainders. Also note that dividing $0, 1, 2, 3, \ldots$ by 3 yields

$$0, 1, 2, 0, 1, 2, 0, 1, 2, 0, 1, 2, 0, 1, 2, \ldots$$

as the respective remainders. Observe that dividing $0, 1, 2, 3, \ldots$ by 3 yields

$$0, 1, 2, 3, 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, 2, 3, \ldots$$

as the respective remainders.

The integers $0, 2, 4, 6, \ldots$ leave the same remainder when divided by 2, and the integers $1, 3, 5, 7, \ldots$ leave the same remainder when divided by 2.

Note that the integers $0, 3, 6, 9, \ldots$ leave the same remainder when divided by 3, the integers $1, 4, 7, \ldots$ leave the same remainder when divided by 3, and the integers $2, 5, 8, \ldots$ leave the same remainder when divided by 3.

From now on, let us call the integers $0, 2, 4, 6, \ldots$ the same with respect to 2, or **congruent modulo** 2, and also call the integers $1, 3, 5, 7, \ldots$ **congruent modulo** 2.

Definition 1. Let n be a positive integer. Two integers a, b are said to be **congruent modulo** n if

$$n \text{ divides } a - b.$$

If a, b are congruent modulo n, we write

$$a \equiv b \pmod{n}.$$

Remark. Note that if a, b, n are integers with $n \geq 1$, then

$$a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n},$$
$$a \equiv b \pmod{n} \Leftarrow b \equiv a \pmod{n}.$$

These are often combinded and written as

$$a \equiv b \pmod{n} \iff b \equiv a \pmod{n}.$$

Lemma 2

Let a, b, c, d, k, n be integers with $n \geq 1$ and $k \neq 0$.

1. The congruence $a \equiv a \pmod{n}$ holds.
2. If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.
3. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then
$$a \equiv c \pmod{n}.$$
4. If $a \equiv b \pmod{n}$, then
$$ka \equiv kb \pmod{kn}$$
and
$$ka \equiv kb \pmod{n}$$
holds.
5. If $ac \equiv bc \pmod{n}$ and $\gcd(c, n) = 1$, then
$$a \equiv b \pmod{n}.$$
6. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then
$$a + c \equiv b + d \pmod{n},$$
$$ac \equiv bd \pmod{n}$$
holds.
7. If $a \equiv b \pmod{n}$, then
$$a^m \equiv b^m \pmod{n}$$
holds for any positive integer m.

Example 2.1 (China TST 1995 Day 1 P1)**.** Find the smallest prime number p that cannot be represented in the form $|3^a - 2^b|$, where a and b are non-negative integers.

Walkthrough —

(a) Any prime smaller than 41 can be expressed as the absolute value of the difference of a nonnegative power of 3 and a nonnegative power of 2.

(b) If $41 = 2^b - 3^a$, then $b \geq 3$ and hence $3^a \equiv -1 \bmod 8$, which is impossible.

(c) Assume that $41 = 3^a - 2^b$. Considering congruence modulo 3, show that b is an even positive integer. Reduce modulo 4 to show that a is even.

(d) Write $a = 2x, b = 2y$, and factorize 41.

(e) Conclude by obtaining a contradiction.

Solution 5. Note that any prime smaller than 41 can be expressed as the absolute value of the difference of a nonnegative power of 3 and a nonnegative power of 2, as shown below.

$$\begin{aligned} 2 &= 3 - 1, \\ 3 &= 4 - 1, \\ 5 &= 9 - 4, \\ 7 &= 8 - 1, \\ 11 &= 27 - 16, \\ 13 &= 16 - 3, \\ 17 &= 81 - 64, \\ 19 &= 27 - 8, \\ 23 &= 32 - 9, \\ 29 &= 32 - 3, \\ 31 &= 32 - 1, \\ 37 &= 64 - 27. \end{aligned}$$

Let us prove the following claim.

Claim — The prime number 41 cannot be expressed as the absolute value of the difference of a nonnegative power of 3 and a nonnegative power of 2.

Proof of the Claim. On the contrary, let us assume that

$$41 = |3^a - 2^b|$$

holds for some nonnegative integers a, b.

First, let us consider the case that $41 = 2^b - 3^a$. Note that $b \geq 3$ holds, and reducing the above modulo 8, it follows that $3^a \equiv -1 \pmod 8$, which is impossible.

Now, let us consider the case that $41 = 3^a - 2^b$. Reducing modulo 3, it follows that $2^b \equiv 1 \pmod 3$, which shows that b is even. Note that b is nonzero. Next, reducing modulo 4, we obtain $3^a \equiv 1 \pmod 4$, which implies that a is even. Writing $a = 2x, b = 2y$ for some positive integers x, y, we obtain

$$41 = 3^{2x} - 2^{2y} = (3^x - 2^y)(3^x + 2^y)$$

with $1 \leq 3^x - 2^y < 3^x + 2^y$, which yields

$$3^x - 2^y = 1, 3^x + 2^y = 41,$$

which is impossible.

Considering the above cases, the claim follows. □

This proves that 41 is smallest prime that cannot be expressed in the given form. ■

Example 2.2 (India RMO 1998 P2)**.** Let n be a positive integer and $p_1, p_2, \ldots, p_n$ be n prime numbers all larger than 5 such that 6 divides $p_1^2 + p_2^2 + \cdots + p_n^2$. Prove that 6 divides n.

> **Walkthrough** — Observe that any prime larger than 5 is congruent to ± 1 modulo 6.

Solution 6. Note that any prime number larger than 5 is of the form $6k \pm 1$. This yields

$$p_1^2 + p_2^2 + \cdots + p_n^2 \equiv (\pm 1)^2 + (\pm 1)^2 + \cdots + (\pm 1)^2 \bmod 6 \equiv n \bmod 6.$$

Since 6 divides $p_1^2 + p_2^2 + \cdots + p_n^2$, it follows that 6 divides n. ■

Example 2.3 (India RMO 2023a P2)**.** Given a prime number p such that $2p$ is equal to the sum of the squares of some four consecutive positive integers. Prove that $p - 7$ is divisible by 36.

> **Walkthrough** — Show that the sum of four consecutive squares is congruent to 6 modulo 8, and conclude that $p \equiv 3 \bmod 4$. Considering congruence conditions modulo 3, prove that the smallest of the four consecutive numbers is a multiple of 3. Deduce that the sum of the four consecutive squares is 5 modulo 9.

Solution 7. Let p be a prime satisfying the given condition. Write

$$2p = x^2 + (x+1)^2 + (x+2)^2 + (x+3)^2$$

where x is a positive integer. Note that

$$\begin{aligned} x^2 + (x+1)^2 + (x+2)^2 + (x+3)^2 &= 4x^2 + 12x + 14 \\ &\equiv 4x(x+1) + 6 \bmod 8 \\ &\equiv 6 \bmod 8 \end{aligned}$$

holds. It follows that $2p$ is congruent to 6 modulo 8, which shows that p is congruent to 3 modulo 4.

Note that if $x \equiv \pm 1 \bmod 3$, then

$$\begin{aligned} x^2 + (x+1)^2 + (x+2)^2 + (x+3)^2 &= 4x^2 + 12x + 14 \\ &\equiv x^2 + 2 \bmod 3 \\ &\equiv 0 \bmod 3 \end{aligned}$$

holds, which shows that 3 divides $2p$, and hence $p = 3$. However, 6 cannot be expressed as the sum of four consecutive positive integers since $3^2 > 6$. This shows that x is divisible by 3. It follows that

$$\begin{aligned} x^2 + (x+1)^2 + (x+2)^2 + (x+3)^2 &= 4x^2 + 12x + 14 \\ &\equiv 14 \bmod 9. \end{aligned}$$

So, $2p - 14$ is a multiple of 9, and hence, it is an even multiple of 9, implying that $p - 7$ is a multiple of 9. Since $p \equiv 3 \bmod 4$, we obtain $p \equiv 7 \bmod 36$. ■

Example 2.4 (India RMO 2023b P1)**.** Let $\mathbb{N}$ be the set of all positive integers and

$$S = \left\{(a, b, c, d) \in \mathbb{N}^4 : a^2 + b^2 + c^2 = d^2\right\}.$$

Find the largest positive integer m such that m divides $abcd$ for all $(a, b, c, d) \in S$.

Walkthrough —

(a) Show that $(1, 2, 2, 3)$ lies in S, and deduce that m divides 12.

(b) Let (a, b, c, d) be an element of S. Show that at least one of a, b, c, d is divisible by 3, and at least one of them is even.

(c) Prove that if d is even, then at least one of a, b, c is even, and that if d is odd, then at least two of a, b, c are even.

(d) Conclude that m is divisible by $2 \cdot 2 \cdot 3$.

Solution 8. Let m denote the largest positive integer such that it divides $abcd$ for all (a, b, c, d) in S. Note that $1^2 + 2^2 + 2^2 = 3^2$ holds, which shows that $(1, 2, 2, 3)$ lies in S. This shows that m divides 12.

Let (a, b, c, d) be an element of S. Note that at least one of a, b, c, d is divisible by 3 since

$$(\pm 1)^2 + (\pm 1)^2 + (\pm 1)^2 \not\equiv (\pm 1)^2 \bmod 3.$$

Also note that if all of a, b, c, d are odd, then we obtain

$$(\pm 1)^2 + (\pm 1)^2 + (\pm 1)^2 \equiv (\pm 1)^2 \bmod 4,$$

which is impossible. It follows that at least one of a, b, c, d is even.

If d is even, then at least one of a, b, c is even because the sum of squares of three odd integers is congruent to 3 modulo 4. If d is odd, then at least one of a, b, c is even. Note that $0 + (\pm 1)^2 + (\pm 1)^2 \not\equiv (\pm 1)^2 \bmod 4$, which shows that if d is odd, then at least two of a, b, c are even. This implies that at least two of a, b, c, d are even. Hence, m is divisible by $2 \cdot 2 \cdot 3 = 12$.

This proves that $m = 12$. ■

References

[**Che25**] EVAN CHEN. *The OTIS Excerpts*. Available at https://web.evanchen.cc/excerpts.html. 2025, pp. vi+289 (cited p. 1)

[**FGI96**] DMITRI FOMIN, SERGEY GENKIN, and ILIA ITENBERG. *Mathematical circles (Russian experience)*. Vol. 7. Mathematical World. Translated from the Russian and with a foreword by Mark Saul. American Mathematical Society, Providence, RI, 1996, pp. xii+272. ISBN: 0-8218-0430-8 (cited p. 4)

[**Sai06**] FILIP SAIDAK. A new proof of Euclid's theorem. In: *Amer. Math. Monthly*, **113**:10 (2006), pp. 937–938. ISSN: 0002-9890. DOI: 10.2307/27642094. URL: http://dx.doi.org/10.2307/27642094 (cited p. 4)