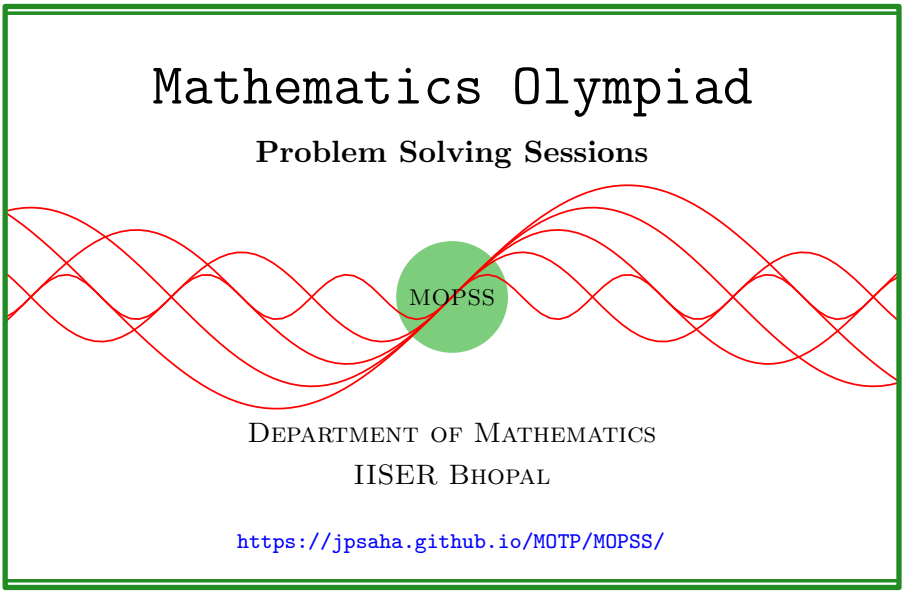
Gauss's lemma

MOPSS

3 June 2025



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 Gauss's lemma

Example 1.1 (ELMO 2009 P1, proposed by Evan O'Dorney)**.** Let a, b, c be positive integers such that $a^2 - bc$ is a square. Prove that $2a + b + c$ is not prime.

Solution 1. Consider the quadratic polynomial $p(x) = bx^2 + 2ax + c$ with integer coefficients. Since its discriminant is a perfect square, it follows that its roots are rational, that is, it can be factored over the rationals. By Gauss's lemma, $p(x)$ can be factored into linear polynomials with integer coefficients. Since the leading coefficient of $p(x)$ is positive, it follows that it can be factored into linear polynomials with integer coefficients and having positive leading coefficients. Note that the roots of $p(x)$ are negative rationals. This proves that $p(x)$ can be factored into linear polynomials with positive integer coefficients. Noting that $p(1) = 2a + b + c$, it follows that $2a + b + c$ is not a prime. ■

> **Remark.** Note that in the above, one may prove that $p(x)$ can be factored into linear polynomials with integer coefficients without using Gauss's lemma, possibly by establishing the lemma in this specific case. In fact, the above problem could serve as an introduction to Gauss's lemma.

The following is an argument from Mandar Kasulkar.

Solution 2. Let x be a nonnegative integer such that $a^2 - bc = x^2$. Note that

$$\begin{aligned}(2a + b + c)(2a - b - c) &= 4a^2 - (b + c)^2 \\ &= 4a^2 - 4bc + (b - c)^2 \\ &= 4x^2 - (b - c)^2 \\ &= (2x - b + c)(2x + b - c)\end{aligned}$$

holds. Also note that

$$\begin{aligned}-(2a + b + c) &< 2x - b + c \\ &< 2a - b + c \\ &< 2a + b + c, \\ -(2a + b + c) &< 2x + b - c \\ &< 2a + b - c \\ &< 2a + b + c.\end{aligned}$$

If $2a = b + c$, then $2a + b + c$ is not a prime. It remains to consider the case $2a \neq b + c$, which we assume from now on. It follows that the integers $2x - b + c, 2x + b - c$ are nonzero, and lies strictly between $-p$ and p. Since their product is a multiple of $2a + b + c$, we conclude that $2a + b + c$ is not a prime. ■

References

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