Lifting the exponent

MOPSS

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 Lifting of the exponents

Theorem 1 (Lifting the exponent)
Let a, b be integers and p be a prime such that p divides $a-b$ and p does not divide ab. Let n be a positive integer.

(i) If $p \geq 3$, then

$$v_p(a^n - b^n) = v_p(a-b) + v_p(n).$$

(ii) If $p = 2$ and n is odd, then

$$v_2(a^n - b^n) = v_2(a-b).$$

(iii) If $p = 2$, n is even, and $v_2(a-b) \geq 2$, then

$$v_2(a^n - b^n) = v_2(a-b) + v_2(a+b) + v_2(n) - 1.$$

Exercise 1.1 (Hong Kong 2024 TST P3, AoPS)**.** Let n be a positive integer. Prove that there exists a positive integer $m > 1$ such that 7^n divides $3^m + 5^m - 1$.

Walkthrough —

(a)

Solution 1. Let $v_7(x)$ denote the highest power of 7 dividing the integer x. Consider the integer $m = 7^{n-1}$. Applying lifting-the-exponent lemma, we have

$$v_7(3^m + 4^m) = v_7(3^m - (-4)^m) = 1 + v_7(m) = n,$$

and similarly, we have

$$v_7(5^m + 2^m) = n.$$

This implies that

$$3^m + 5^m - 1 \equiv -(1 + 2^m + 4^m) \pmod{7^n} \equiv -\frac{8^m - 1}{2^m - 1}.$$

Applying lifting-the-exponent lemma again, we have

$$v_7(8^m - 1) = v_7(8-1) + v_7(m) = n.$$

Since the order of 2 modulo 7 is 3, and 3 does not divide m, it follows that 7 does not divide $2^m - 1$. This shows that $3^m + 5^m - 1$ is divisible by 7^n. ■

Example 1.2. Find the solutions of the equation

$$x^{2025} + y^{2025} = 5^z$$

in positive integers x, y, z.

Solution 2. Let x, y, z be positive integers satisfying

$$x^{2025} + y^{2025} = 5^z.$$

Write $x = 5^m a$ and $y = 5^n b$ where a, b are positive integers not divisible by 5, and m, n are non-negative integers. Note that $m = n$ holds. It follows that

$$a^{2025} + b^{2025} = 5^{z-2025m}.$$

Note that $z - 2025m$ is a positive integer. Since $a + b$ is greater than 1 and it divides a power of 5, it follows that $a + b$ is divisible by 5. Applying lifting-the-exponent lemma, we have

$$v_5(a^{2025} + b^{2025}) = v_5(a + b) + 2.$$

Hence, for some positive integer k, we have

$$a^{2025} + b^{2025} = 25 \cdot k \cdot (a + b).$$

Since $a^{2025}+b^{2025}$ is a power of 5, it follows that k is a power of 5, and moreover, k is equal to 1. This yields

$$a^{2025} + b^{2025} = 25(a + b).$$

This implies that at least one of a, b is equal to 1. If $a = 1$, then we have

$$b^{2025} = 24 + 25b < 2^5 + 2^5 b = 2^5(1 + b) < 2^6 b \leq b^7,$$

which is impossible. This shows that $a \neq 1$. Similarly, it follows that $b \neq 1$. This is a contradiction. This proves that there are no positive integers x, y, z satisfying the given equation. ■

References

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