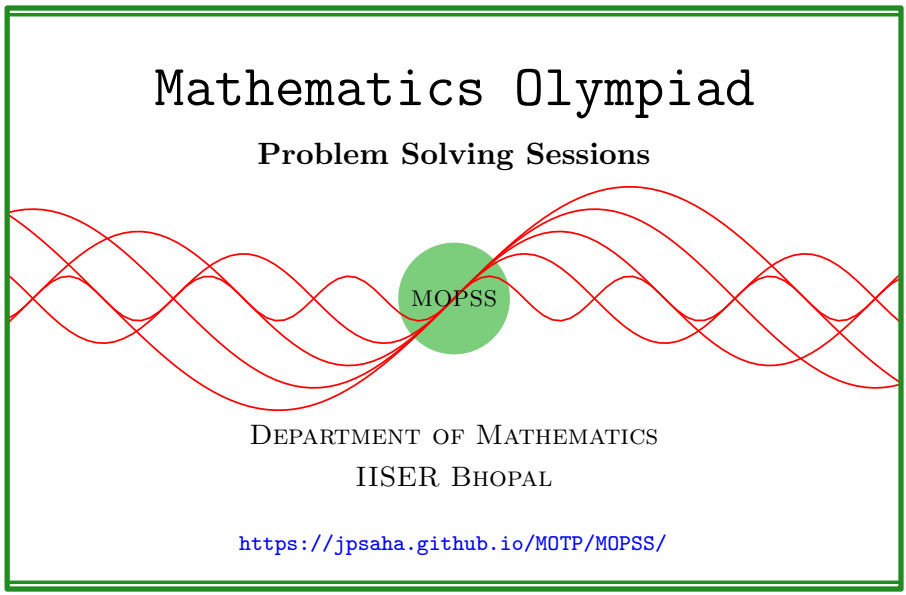
Lifting the exponent

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. ■

Exercise 1.2 (Kürschák Competition 2020 P2, AoPS)**.** Find all functions $f\colon \mathbb{Q} \to \mathbb{R}_{\geq 0}$ such that for any two rational numbers x and y, the conditions

$$f(x + y) \leq f(x) + f(y), f(xy) = f(x)f(y)$$

hold, and $f(2) = \frac{1}{2}$.

Walkthrough — Let $f\colon \mathbb{Q} \to \mathbb{R}_{\geq 0}$ be a function satisfying the given conditions.

(a) Show that $f(0) = 0$ and $f(1) = f(-1) = 1$.

(b) Show that for any integer n, $f(n)$ is nonzero.

(c) Using the fact that any positive integer can be written as a sum of distinct powers of 2, show that for any positive integer n, the inequality $f(n) \leq 2$ holds.

(d) Prove that for any positive integer n, the inequality $f(n) \leq 1$ holds.

(e) For any odd positive integer n and for any positive integer m, show that the inequality $1 - f(n)^{2^m} \leq f(n^{2^m} - 1)$ holds, and using divisibility properties by powers of 2, prove that $1 - f(n)^{2^m} \leq \frac{1}{2^m}$ holds.

(f) Deduce that for any odd positive integer n, $f(n) = 1$ holds.

(g) Prove that for any rational number r,

$$f(r) = \begin{cases} 0 & \text{if } r = 0, \\ 2^{-v_2(r)} & \text{if } r \neq 0. \end{cases}$$

Let $f\colon \mathbb{Q} \to \mathbb{R}_{\geq 0}$ be the function defined above. Show that f satisfies the given conditions.

Solution 2. Let $f : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ be a function satisfying the given conditions. Note that

$$f(2) = f(2)f(1) = f(-2)f(-1)$$

holds. Since $f(2)$ is nonzero, it follows that $f(1), f(-1)$ are nonzero. Also note that

$$f(1) = f(1)f(1) = f(-1)f(-1)$$

holds. Using that $f(1), f(-1)$ are nonzero, we obtain $f(1) = 1$ and $f(-1) = 1$. Further, note that

$$f(0) = f(0)f(2) = \frac{1}{2}f(0),$$

which implies $f(0) = 0$. For any integer n, using

$$f(n)f\left(\frac{1}{n}\right) = f(1) = 1,$$

it follows that $f(n)$ is nonzero.

For any positive integer n, writing n as a sum of distinct powers of 2, we obtain

$$f(n) \leq \sum_{k=0}^{\infty} f(2^k) = \sum_{k=0}^{\infty} f(2)^k = \sum_{k=0}^{\infty} \frac{1}{2^k} = 2.$$

It follows that for any positive integer n,

$$f(n)^m = f(n^m) \leq 2$$

holds for any positive integer m. Thus, $f(n) \leq 1$ holds for any positive integer n. Indeed, if $f(n) > 1$ holds for some positive integer n, then we obtain that

$$2 \geq 1 + m(f(1) - 1)$$

holds for any positive integer m, which is a contradiction.

Let n be an odd positive integer, and let m be a positive integer. Note that

$$1 - f(n)^{2^m} = f(1) - f(n)^{2^m} \leq f(1 - n^{2^m}) = f(-1)f(n^{2^m} - 1) = f(n^{2^m} - 1)$$

holds. Using induction, it follows that the integer $n^{2^m} - 1$ is divisible by 2^m, and consequently,

$$f(n^{2^m} - 1) \leq f\left(\frac{n^{2^m} - 1}{2^m}\right) f(2^m) = \frac{1}{2^m} f\left(\frac{n^{2^m} - 1}{2^m}\right) \leq \frac{1}{2^m}$$

holds. This shows that

$$f(n)^{2^m} + \frac{1}{2^m} \geq 1$$

holds. If $f(n) < 1$, then using the above and that $f(n)$ is nonzero, we obtain that

$$\frac{1}{2} \leq 1 - \frac{1}{2^m} \leq f(n)^{2^m} < \frac{1}{1 + 2^m(f(n)^{-1} - 1)}$$

holds for any positive integer m, which is a contradiction. Therefore, for any odd positive integer n, it follows that $f(n) = 1$.

This proves that for any $r \in \mathbb{Q}$,

$$f(r) = \begin{cases} 0 & \text{if } r = 0, \\ \frac{1}{2^k} & \text{if } r = \frac{2^k a}{b} \text{ for some odd integers } a, b \text{ and for some integer } k \geq 0. \end{cases}$$

Note that for any nonzero rational number r, there exists a unique integer k such that $r = \frac{2^k a}{b}$ holds for some odd integers a, b. The integer k is called the

2-adic valuation of r, and is denoted by $v_2(r)$. Therefore, the function f can be expressed as

$$f(r) = 2^{-v_2(r)}$$

for any nonzero rational number r, and $f(0) = 0$.

If $f\colon \mathbb{Q} \to \mathbb{R}_{\geq 0}$ satisfies this property, that is,

$$f(r) = \begin{cases} 0 & \text{if } r = 0, \\ 2^{-v_2(r)} & \text{if } r \neq 0, \end{cases}$$

for any rational number r, then f also satisfies the given conditions. Indeed, $f(2) = \frac{1}{2}$ holds, and for any nonzero rational numbers x, y, we have

$$f(xy) = 2^{-v_2(xy)} = 2^{-v_2(x)-v_2(y)} = 2^{-v_2(x)}2^{-v_2(y)} = f(x)f(y).$$

If x, y are rational numbers and at least one of them is zero, then the condition $f(xy) = f(x)f(y)$ is immediate.

Let x, y be rational numbers. If $x = 0$ or $y = 0$ or $x + y = 0$, then the condition

$$f(x + y) \leq f(x) + f(y)$$

holds. Using the multiplicative property of f, it suffices to consider the case that x, y are integers. Indeed, if

$$f(kx + ky) \leq f(kx) + f(ky)$$

holds for some positive integer k, then we have

$$f(x + y) = \frac{1}{f(k)} f(kx + ky) \leq \frac{1}{f(k)}(f(kx) + f(ky)) = f(x) + f(y).$$

Thus, it suffices to consider the case that x, y are integers. If one of $x, y, x + y$ is zero, then the inequality $f(x + y) \leq f(x) + f(y)$ holds.

Suppose that $x, y, x + y$ are nonzero. Note that

$$v_2(x + y) \geq \min\{v_2(x), v_2(y)\}$$

holds, which implies that

$$f(x + y) = 2^{-v_2(x+y)} \leq 2^{-\min\{v_2(x),v_2(y)\}} = \max\{f(x), f(y)\} \leq f(x) + f(y)$$

holds. Therefore, the function f satisfies the given conditions.

Hence, the only function $f\colon \mathbb{Q} \to \mathbb{R}_{\geq 0}$ satisfying the given conditions is given by

$$f(r) = \begin{cases} 0 & \text{if } r = 0, \\ 2^{-v_2(r)} & \text{if } r \neq 0, \end{cases}$$

for any rational number r. ■

Example 1.3. Find the solutions of the equation

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

in positive integers x, y, z.

Solution 3. 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)