Lecture Notes for International Mathematical Olympiad

LIFTING-THE-EXPONENT LEMMA

1. Statements and proofs

We first introduce a lemma before proving the main result. Denote $v_p(n)$ the exponent of prime divisor p of $n \in \mathbb{N}$ in its unique factorization.

Lemma 1. *Let $a, b \in \mathbb{Z}$, $l \in \mathbb{N}^*$, and p be a prime number. Then*

$$p^l \mid (a-b) \implies p^{l+1} \mid (a^p - b^p).$$

Proof. To show the idea of the proof we only do for $l = 1$, and the general case requires a similar argument only. Note that

$$\begin{aligned} a^p &= (a-b+b)^p \\ &= \underbrace{(a-b)^p + p(a-b)^{p-1}b + \frac{p(p-1)}{2}(a-b)^{p-2}b^2 + \cdots + p(a-b)b^{p-1}}_{\text{divided by } p^2} + b^p. \end{aligned}$$

Since $p \mid (a-b)$, we have $p^2 \mid (a^p - b^p)$. □

Theorem 2. *Let $a, b \in \mathbb{Z}$ and p be a prime number. For any $c \in \mathbb{N}$, we have*

$$v_p(a^c - b^c) \geqslant v_p(a-b) + v_p(c),$$

or alternatively,

$$v_p\left(\frac{a^c - b^c}{a-b}\right) \geqslant v_p(c).$$

Proof. Denote $k = v_p(c)$ and $l = v_p(a-b)$. It suffices to prove $p^{l+k} \mid (a^c - b^c)$. We have $p^l \mid a - b$. By the lemma, we have $p^{l+1} \mid a^p - b^p$. Apply the lemma iteratively, we have

$$p^l \mid a-b \implies p^{l+1} \mid a^p - b^p \implies p^{l+2} \mid a^{p^2} - b^{p^2} \implies p^{l+k} \mid a^{p^k} - b^{p^k}.$$

Since $p^k \mid c$, we have $(a^{p^k} - b^{p^k}) \mid (a^c - b^c)$. It follows that $p^{l+k} \mid (a^c - b^c)$, which is as desired. □

Problem 3. *Let $n \in \mathbb{N}^*$ and $a, b \in \mathbb{Z}$ be distinct integers. Assume $n \mid (a^n - b^n)$. Prove that n divides $(a^n - b^n)/(a-b)$.*

Proof. It suffices to show that for any prime divisor p of n, we have

$$v_p\left(\frac{a^n - b^n}{a-b}\right) \geqslant v_p(n).$$

If $p \mid (a-b)$, this is given by Theorem 2. Otherwise $(p, a-b) = 1$, and hence

$$v_p\left(\frac{a^n - b^n}{a-b}\right) = v_p(a^n - b^n) \geqslant v_p(n).$$

□

Date: August 30, 2022.

Theorem 4 (Lifting-the-exponent lemma for p odd)**.** *Let p be an odd prime and $a, b \in \mathbb{Z}$ coprime to p. Assume $p \mid (a-b)$. Then for each $n \in \mathbb{N}$ we have*

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

Proof. We first prove that if $m, n \in \mathbb{N}$ satisfy the LTE lemma then so also does mn. For this, we note that

$$\begin{aligned} v_p(a^{mn} - b^{mn}) &= v_p((a^m)^n - (b^m)^n) \\ &= v_p(a^m - b^m) + v_p(n) \\ &= v_p(a-b) + v_p(m) + v_p(n) \\ &= v_p(a-b) + v_p(mn). \end{aligned}$$

Then it suffices to replace n by any prime number q. Whenever $q \neq p$, it is enough to show that

$$\frac{a^q - b^q}{a-b} = a^{q-1} + a^{q-2}b + \cdots + b^{q-1}$$

is not divisible by p. By assumption we have $a \equiv b \bmod p$. And $p \nmid a$ implies $p \nmid qa$. Then

$$\frac{a^q - b^q}{a-b} \equiv qa^{q-1} \not\equiv 0 \bmod p.$$

In this case q satisfies the LTE lemma. We are remained to consider $q = p$. Let $a = b + p^k c$ with $(p, c) = 1$, that is, such that $v_p(a-b) = k$. Then

$$a^q - b^q = (b + p^k c)^p - b^p = pb^{p-1}p^k c + \binom{2}{p} b^{p-2}p^{2k}c^2 + \cdots + p^{kp}c^p.$$

Since $p > 2$, we have $v_p(\binom{2}{p} b^{p-2}p^{2k}c^2 + \cdots + p^{kp}c^p) > k+1$, and hence[1]

$$v_p(a^q - b^q) = v_p(pb^{p-1}p^k c) = k + 1 = v_p(a-b) + v_p(q)$$

with $q = p$, because of $(p, bc) = 1$. This completes the proof. □

Theorem 5 (Lifting-the-exponent lemma for $p = 2$)**.** *Let $x, y \in \mathbb{Z}$ be odd integers and $2 \mid n \in \mathbb{N}$. Then*

$$v_2(x^n - y^n) = v_2(x^2 - y^2) + v_2(n) - 1.$$

Proof. Denote $n = 2^k a$ for $k \in \mathbb{N}$ and a odd. Then

$$\begin{aligned} x^n - y^n &= (x^a)^{2^k} - (y^a)^{2^k} \\ &= (x^{2^{k-1}}a + y^{2^{k-1}}a)(x^{2^{k-2}}a + y^{2^{k-2}}a)\cdots(x^{2a} + y^{2a})(x^a + y^a)(x^a - y^a). \end{aligned}$$

Since x, y are odd, we have $x^2 + y^2 \equiv 2 \bmod 4$ and hence $v_2(x^2 + y^2) = 1$. Using the same identity, it follows that

$$\begin{aligned} v_2(x^n - y^n) &= v_2((x^{2^{k-1}}a + y^{2^{k-1}}a)(x^{2^{k-2}}a + y^{2^{k-2}}a)\cdots(x^{2a} + y^{2a})) + v_2(x^{2a} - y^{2a}) \\ &= k - 1 + v_2(x^{2a} - y^{2a}). \end{aligned}$$

Then

$$\frac{x^{2a} - y^{2a}}{x^2 - y^2} = x^{2(a-1)} + \cdots + y^{2(a-1)},$$

[1]In the context of algebraic number theory this is due to the strong triangle inequality of p-adic valuations.

which is the sum of a odd integers, where a is odd. Hence

$$v_2\left(\frac{x^{2a}-y^{2a}}{x^2-y^2}\right)=0,$$

and therefore $v_2(x^{2a}-y^{2a})=v_2(x^2-y^2)$. It follows that $v_2(x^n-y^n)=v_2(x^2-y^2)+v_2(n)-1$ as desired. □

Theorem 6. *Let x, y be odd integers and n is positive and odd. Then*

$$v_2(x^n-y^n)=v_2(x-y).$$

Proof. We compute that

$$\frac{x^n-y^n}{x-y}=x^{n-1}+\cdots+y^{n-1}\equiv 1 \bmod 2.$$

Then

$$v_2\left(\frac{x^n-y^n}{x-y}\right)=0 \implies v_2(x^n-y^n)=v_2(x-y).$$

□

2. Typical applications

Problem 7 (Chinese Girl's Mathematical Olympiad, 2017)**.** *Determine all possible positive integer n satisfying that for any positive odd integer a, we have $2^{2017} \mid a^n-1$.*

Solution. We are to satisfy $v_2(a^n-1)\geqslant 2017$. If we take $a=3$, then $3^n\equiv 1 \bmod 2^{2017}$, and hence $3^n\equiv 1 \bmod 4$. So $(-1)^n\equiv 1 \bmod 4$, which indicates that n is even. By Theorem 5, we have

$$v_2(3^n-1)=v_2(3^2-1)+v_2(n)-1=2+v_2(n).$$

This requires $v_2(n)\geqslant 2015$. Also,

$$2\nmid a \implies a^2\equiv 1 \bmod 8 \implies 8\mid a^2-1 \implies v_2(a^2-1)\geqslant 3.$$

On the other hand, we may check that

$$v_2(a^n-1)=v_2(a^2-1)+v_2(n)-1\geqslant 3+2015-1=2017.$$

To conclude, $n=2^{2015}m$ for $m\in\mathbb{N}$. □

Problem 8. *In a sequence of integers $\{a_n\}_{n\in\mathbb{N}}$, we assume $a_1=2018$ and $a_n=2018^{a_{n-1}}$ for $n\geqslant 2$. Find out $v_{2017}(a_{2018}-a_{2017})$.*

Proof. We obtain

$$a_{2018}-a_{2017}=2018^{a_{2017}}-2018^{a_{2016}}=2016^{a_{2016}}(2018^{a_{2017}-a_{2016}}-1).$$

Since $(2018^{a_{2016}}, 2017)=1$, we have by LTE lemma that

$$\begin{aligned}
v_{2017}(a_{2018}-a_{2017}) &= v_{2017}(2018^{a_{2017}-a_{2016}}-1)\\
&= v_{2017}(2018-1)+v_{2017}(a_{2017}-a_{2016})\\
&= 1+v_{2017}(a_{2017}-a_{2016})\\
&= 2+v_{2017}(a_{2016}-a_{2015})\\
&= \cdots\\
&= 2016+v_{2017}(a_2-a_1).
\end{aligned}$$

Using the LTE lemma again, the result turns out to be

$$\begin{aligned}2016 + v_{2017}(a_2 - a_1) &= 2016 + v_{2017}(2018^{2017} - 1)\\ &= 2016 + v_{2017}(2018 - 1) + v_{2017}(2017)\\ &= 2016 + 1 + 1 = 2018.\end{aligned}$$

□

Problem 9. *Determine all $n \in \mathbb{N}$ such that $n^2 \mid 2^n + 1$.*

Solution. It is clear that $n = 1$ is a solution. For $n > 1$, if p is the minimal prime divisor of n, then $p \mid 2^n + 1$ implies that p is an odd prime. By Fermat's little theorem, $p \mid 2^{p-1} - 1$. On the other hand, as $p \mid 2^n + 1$, we have $p \mid (2^n + 1)(2^n - 1) = 2^{2n} - 1$. From these, we see

$$p \mid (2^{p-1} - 1, 2^{2n} - 1) = 2^{(p-1,2n)} - 1 = 3$$

because $(p - 1, 2n) = 2$. Hence $p = 3$. By assumption,

$$n^2 \mid 2^n + 1 \implies 2v_3(n) \leqslant v_3(2^n + 1) = v_2(2 + 1) + v_3(n) = 1 + v_3(n) \implies v_3(n) \leqslant 1.$$

It is also clear that $v_3(n) \geqslant 1$, so $v_3(n) = 1$. Let $n = 3m$ for some $3 \nmid m$. We claim that $m = 1$. If $m > 1$ then there is a smallest prime divisor q of m say, such that $(q, 2) = 1$. Then $q \mid 2^n + 1 = 8^m + 1$, and hence $q \mid (8^m + 1)(8^m - 1) = 8^{2m} - 1$. Also, by Fermat's little theorem, $q \mid 8^{q-1} - 1$. Hence $q \mid 8^{(2m,q-1)} - 1 = 63$. It forces q to be 7, so $7 \mid 8^m + 1$. However, $8^m + 1 \equiv 1 + 1 = 2 \bmod 7$, which leads to a contradiction. This proves $m = 1$.

Therefore, $n = 1, 3$ are all the desired solutions. □

Problem 10 (Chinese Team Selection Test, 2009)**.** *Let $n \in N$ and $a > b > 1$ integers, such that b is odd and $b^n \mid a^n - 1$. Prove that*

$$a^b > \frac{3^n}{n}.$$

Proof. Take $p > 2$ to be any prime divisor of b. Then

$$b^n \mid a^n - 1 \implies p \mid a^n - 1 \implies p \nmid a^n \implies (a, p) = 1 \implies (a, b) = 1.$$

By Fermat's little theorem, we have $p \mid a^{p-1} - 1$. On the other hand, $a^n - 1 \mid (a^n)^{p-1} - 1 = (a^{p-1})^n - 1$. Then

$$n \leqslant v_p(b^n) \leqslant v_p(a^n - 1) \leqslant v_p((a^{p-1})^n - 1).$$

By LTE lemma, the RHS equals to

$$v_p((a^{p-1})^n - 1) = v_p(a^{p-1} - 1) + v_p(n).$$

Hence, by taking product on all prime divisors, we have

$$v_p(a^{p-1} - 1) \geqslant n - v_p(n) \implies a^{p-1} - 1 \geqslant p^{n - v_p(n)}.$$

Finally, one can complete the proof by noting

$$a^b > a^{p-1} > a^{p-1} - 1 \geqslant p^{n-v_p(n)} = \frac{p^n}{p^{v_p(n)}} \geqslant \frac{p^n}{n} \geqslant \frac{3^n}{n}.$$

□

School of Mathematical Sciences, Peking University, 100871, Beijing, China
Email address: daiwenhan@pku.edu.cn