Lecture Notes for International Mathematical Olympiad

ON MINIMAL PRIME DIVISORS

1. Introduction

We introduce two tricks on divisor analysis:

- Assume $n \geqslant 2$. It will be convenient to let p be the minimal prime divisor of n, which is particularly useful while considering the condition $n \mid (a^n - b^n)$. (c.f. Lifting-the-exponent lemma.)
- Suppose n is a compositum number. Then we can take p to be the minimal prime divisor of n, and write $n = pm$ for $2 \leqslant p \leqslant m$.

2. Basic examples

Problem 1. *Suppose $n \in \mathbb{Z}$ and $n > 1$. Show that $n \nmid 2^n - 1$.*

Proof. Let p be the minimal prime divisor of $n > 1$. Assume $p \mid n \mid 2^n - 1$ for the sake of contradiction. Since $2^n - 1$ is odd we have $2 \nmid p$, and by Fermat's little theorem,

$$2^{p-1} \equiv 1 \bmod p.$$

Then we have

$$p \mid (2^n - 1, 2^{p-1} - 1) = 2^{(n,p-1)} - 1.$$[1]

But p is the minimal divisor of n, which forces $(n, p-1) = 1$. This leads to a contradiction because $p \mid 2^1 - 1 = 1$. □

Problem 2. *Determine all positive odd integers, say n's, such that $n \mid 3^n + 1$.*

Solution. It is clear that $n = 1$ is a solution. When $n > 1$ we take $2 \nmid p$ to be the minimal prime divisor of n. Note that $3 \nmid 3^n + 1$, and hence $(3, p) = 1$. By Fermat's little theorem $p \mid 3^{p-1} - 1$. On the other hand,

$$p \mid 3^n + 1 \implies p \mid (3^n + 1)(3^n - 1) = 3^{2n} - 1.$$

Combining these we get

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

But $p - 1$ does not contain any divisor of n and $p - 1 \neq 2$. We get $(2n, p-1) = 1$, and therefore $p \mid 2$, which leads to a contradiction. To conclude, $n = 1$ is the only solution. □

Problem 3. *Determine all pairs (n, a), such that $n \in \mathbb{N}^*$, $a \in \mathbb{Z}$, and $n \mid (a+1)^n - a^n$.*

Date: August 28, 2022.

[1]Recall that for $a, b, m, n \in \mathbb{N}^*$ with $(a, b) = 1$, we have

$$(a^m - b^m, a^n - b^n) = a^{(m,n)} - b^{(m,n)}.$$

Solution. Note that $n = 1$ satisfies the condition for all $a \in \mathbb{Z}$. Assume $n > 1$ with p its minimal prime divisor. Then $p \mid (a+1)^n - a^n$. It follows that $p \nmid a$ and $p \nmid a+1$. By Fermat's little theorem,

$$a^{p-1} \equiv 1 \bmod p, \quad (a+1)^{p-1} \equiv 1 \bmod p,$$

and hence

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

Combining this with the given condition we see

$$p \mid ((a+1)^{p-1} - a^{p-1}, (a+1)^n - a^n) = (a+1)^{(p-1,n)} - a^{(p-1,n)}.$$

However, we have $(p-1, n) = 1$ as before, and hence the contradiction arises when we deduce $p \mid 1$. So the only solution is $n = 1$ with $a \in \mathbb{Z}$. □

3. Advanced problems

Problem 4 (IMO, 2020)**.** *We are given a deck of $n > 1$ cards in which each card is assigned with a positive integer. This deck of cards obtains the following property. The arithmetic mean of numbers on any two distinct cards equals a geometric mean of numbers on some collection of one or more cards.*

Determine those n such that this property implies that all cards are assigned with the same positive integer.

Solution. Suppose the n cards are assigned with positive integers $a_1, \ldots, a_n$ and satisfy the given property. We prove firstly that $a_1/d, \ldots, a_n/d$ also satisfy the given property, where $d = \gcd(a_1, \ldots, a_n)$. Denote $a_i = db_i$ with $\gcd(b_1, \ldots, b_n) = 1$. Then

$$\frac{a_1 + a_2}{2} = \sqrt[k]{a_{i_1} \cdots a_{i_k}} \iff \frac{d(b_1 + b_2)}{2} = \sqrt[k]{d^k b_{i_1} \cdots b_{i_k}} = d\sqrt[k]{b_{i_1} \cdots b_{i_k}}$$
$$\iff \frac{b_1 + b_2}{2} = \sqrt[k]{b_{i_1} \cdots b_{i_k}}.$$

May assume $b_1 \geqslant b_2 \geqslant \cdots \geqslant b_n$. Our goal is to show that they are all equal to 1. Assume $b_1 \geqslant 2$ with p its minimal prime divisor. Then, as $(b_1, \ldots, b_n) = 1$ by assumption, there exists a minimal index $m \in \{2, 3, \ldots, n\}$ such that $p \nmid b_m$. Again, by the given property,

$$\frac{b_1 + b_m}{2} = \sqrt[k]{b_{i_1} \cdots b_{i_k}}$$

for some $i_1, \ldots, i_k$. Note that in the above equality,

$$\frac{b_1 + b_m}{2} \in \mathbb{Q}, \quad \sqrt[k]{b_{i_1} \cdots b_{i_k}} \in \mathbb{N} \text{ or } \mathbb{R} \backslash \mathbb{Q}.$$

Consequently, the LHS and RHS are both the same positive integer. However,

$$b_1 > b_m \implies \frac{b_1 + b_m}{2} > b_m \implies \sqrt[k]{b_{i_1} \cdots b_{i_k}} > b_m,$$

and therefore, there is some $1 \leqslant r \leqslant k$ such that $b_{i_r} > b_m$. Recall that m is the minimal index such that $p \nmid b_m$. So, as $\sqrt[k]{b_{i_1} \cdots b_{i_k}} \in \mathbb{N}$,

$$p \mid b_{i_1}, \ldots, b_{i_r} \implies p \mid \sqrt[k]{b_{i_1} \cdots b_{i_k}} \implies p \mid \frac{b_1 + b_m}{2}.$$

On the other hand, we have $p \mid b_1$ and $p \nmid b_m$ by assumption, which leads to a contradiction because $p \nmid b_1 + b_m$. Therefore, we have proved that $b_1 = 1$, and hence $b_1 = \cdots = b_n = 1$.

To conclude, for any integer $n \geqslant 2$, the property implies that all numbers on all cards are the same. □

Problem 5. *Let p be a prime and r the remainder of p modulo 210. Suppose r is not a prime and has the form $a^2 + b^2$ for some $a, b \in \mathbb{N}^*$. Determine r.*

Solution. Write $p = 210n + r$ with $0 < r < 210$. Let q be the minimal prime divisor of r and hence $r = qm$ for $q \leqslant m \in \mathbb{N}^*$. Then we have

$$210 > r = qm \geqslant q^2 \implies q \leqslant 13.$$

On the other hand, r cannot be divisible by either of $2, 3, 5, 7$, which are prime divisors of 210; otherwise p must be a compositum number. This forces q to be either 11 or 13.

Let $r = a^2 + b^2$. If $q = 11$ then $11 \mid (a^2 + b^2)$. Note that for any $t \in \mathbb{N}$ we have $t^2 \equiv 0, 1, 4, 9, 5, 3 \bmod 11$. It follows that $11 \mid a$ and $11 \mid b$. Then $r \geqslant 121 + 121 > 210$, which is impossible.

Now we have $q = 13$. Consequently,

$$m \leqslant \left[\frac{210}{13}\right] = 16.$$

If $m \in \{16, 15, 14\}$ then p is a multiple of $2, 3, 7$ and $p > 2, 3, 7$, respectively. This implies that p is not prime, which is also impossible.

To conclude, $m = 13$ with $r = 169 = 5^2 + 12^2$ and $p = 379$, $n = 1$. □

In the upcoming context we call d a *proper divisor* of $n \in \mathbb{N}^*$ if $d \mid n$ and $1 < d < n$.

Problem 6. *Let n be a composite number. For any proper divisor d of n, write on the blackboard the number $d + 1$. Find out all such integers n so that all the numbers on the blackboard are exactly all proper divisors of some other positive integer m.*

Proof. Let p be the minimal prime divisor of n. Then $p + 1$ must be the minimal prime divisor of m, and hence $p = 2$ and $3 \mid m$. It follows that m is odd and all proper divisors of m are odd. Hence all proper divisors of n are even, and hence n obtains no odd prime divisors.

Write $n = 2^k$ for $k \geqslant 2$. Then the maximal proper divisor of n is 2^{k-1}.

- If $k \geqslant 4$ otherwise, then $2, 4, 8$ are all proper divisors of n, and hence $3, 5, 9$ are all proper divisors of m. Then $15 \mid m$ properly. It follows that $14 \mid n$ properly, which is impossible.
- If $k = 2$, then $n = 4$ and $m = 9$ satisfy the condition.
- If $k = 3$, then $n = 8$ and $m = 15$ is also a valid solution.

To sum up, we have $n = 4$ or 8. □

Problem 7. *Determine all positive integers n to satisfy the following conditions:*

(1) *n has at least 4 positive divisors, and*
(2) *for any pair of proper divisors a, b of n, we have $(b - a) \mid n$.*

Proof. We first note that if $2 \nmid n$ then $2 \nmid a, b$ and hence $2 \mid (b-a) \mid n$, which is a contradiction. Hence $2 \mid n$. Take $a = 2$ and $b = n/2$ to obtain

$$\left(\frac{n}{2} - 2\right) \mid n,\ (\frac{n}{2} - 2) \mid (n-4) \left(\frac{n}{2} - 2\right) \mid 4.$$

Then $n \in \{6, 8, 12\}$. It is easy to check that all these numbers are valid solutions. □

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