USAMO 2006 Solution Notes

Evan Chen《陳誼廷》

21 January 2024

This is a compilation of solutions for the 2006 USAMO. Some of the solutions are my own work, but many are from the official solutions provided by the organizers (for which they hold any copyrights), and others were found by users on the Art of Problem Solving forums.

These notes will tend to be a bit more advanced and terse than the "official" solutions from the organizers. In particular, if a theorem or technique is not known to beginners but is still considered "standard", then I often prefer to use this theory anyways, rather than try to work around or conceal it. For example, in geometry problems I typically use directed angles without further comment, rather than awkwardly work around configuration issues. Similarly, sentences like "let $\mathbb{R}$ denote the set of real numbers" are typically omitted entirely.

Corrections and comments are welcome!

Contents

§0 Problems

1. Let p be a prime number and let s be an integer with $0 < s < p$. Prove that there exist integers m and n with $0 < m < n < p$ and
$$\left\{ \frac{sm}{p} \right\} < \left\{ \frac{sn}{p} \right\} < \frac{s}{p}$$
if and only if s is not a divisor of $p-1$.

2. Let $k > 0$ be a fixed integer. Compute the minimum integer N (in terms of k) for which there exists a set of $2k+1$ distinct positive integers that has sum greater than N, but for which every subset of size k has sum at most $N/2$.

3. For integral m, let $p(m)$ be the greatest prime divisor of m. By convention, we set $p(\pm 1) = 1$ and $p(0) = \infty$. Find all polynomials f with integer coefficients such that the sequence
$$\{p(f(n^2)) - 2n\}_{n \ge 0}$$
is bounded above. (In particular, this requires $f(n^2) \neq 0$ for $n \ge 0$.)

4. Find all positive integers n for which there exist an integer $k \ge 2$ and positive rational numbers $a_1, \dots, a_k$ satisfying $a_1 + a_2 + \dots + a_k = a_1 a_2 \dots a_k = n$.

5. A mathematical frog jumps along the number line. The frog starts at 1, and jumps according to the following rule: if the frog is at integer n, then it can jump either to $n+1$ or to $n + 2^{m_n+1}$ where 2^{m_n} is the largest power of 2 that is a factor of n. Show that if $k \ge 2$ is a positive integer and i is a nonnegative integer, then the minimum number of jumps needed to reach $2^i k$ is greater than the minimum number of jumps needed to reach 2^i.

6. Let $ABCD$ be a quadrilateral, and let E and F be points on sides AD and BC, respectively, such that $\frac{AE}{ED} = \frac{BF}{FC}$. Ray FE meets rays BA and CD at S and T, respectively. Prove that the circumcircles of triangles SAE, SBF, TCF, and TDE pass through a common point.

§1 Solutions to Day 1

§1.1 USAMO 2006/1, proposed by Kiran Kedlaya

Available online at https://aops.com/community/p490569.

Problem statement

Let p be a prime number and let s be an integer with $0 < s < p$. Prove that there exist integers m and n with $0 < m < n < p$ and

$$\left\{\frac{sm}{p}\right\} < \left\{\frac{sn}{p}\right\} < \frac{s}{p}$$

if and only if s is not a divisor of $p-1$.

It's equivalent to $ms \bmod p < ns \bmod p < s$, where $x \bmod p$ means the remainder when x is divided by p, by slight abuse of notation. We will assume $s \ge 2$ for simplicity, since the case $s = 1$ is clear.

For any $x \in \{1, 2, \dots, s-1\}$ we define $f(x)$ to be the unique number in $\{1, \dots, p-1\}$ such that $s \cdot f(x) \bmod p = x$. Then, m and n fail to exist exactly when

$$f(s-1) < f(s-2) < \cdots < f(1).$$

We give the following explicit description of f: choose $t \equiv -s^{-1} \pmod p$, $0 < t < p$. Then $f(x) = 1 + (s-x) \cdot t \bmod p$. So our displayed inequality is equivalent to

$$(1+t) \bmod p < (1+2t) \bmod p < (1+3t) \bmod p < \cdots < (1+(s-1)t) \bmod p.$$

This just means that the sequence $1 + kt$ never "wraps around" modulo p as we take $k = 1, 2, \dots, s-1$.

Since we assumed $s \neq 1$, we have $0 < 1 + t < p$. Now since $1 + kt$ never wraps around as $k = 1, 2, \dots, s-1$, and increases in increments of t, it follows that $1 + kt < p$ for all $k = 1, 2, \dots, s-1$. Finally, as $1 + st \equiv 0 \pmod p$ we get $1 + st = p$.

In summary, m, n fail to exist precisely when $1 + st = p$. That is of course equivalent to $s \mid p - 1$.

§1.2 USAMO 2006/2, proposed by Dick Gibbs

Available online at https://aops.com/community/p490581.

Problem statement

Let $k > 0$ be a fixed integer. Compute the minimum integer N (in terms of k) for which there exists a set of $2k + 1$ distinct positive integers that has sum greater than N, but for which every subset of size k has sum at most $N/2$.

The answer is $N = k(2k^2 + 3k + 3)$ given by

$$S = \left\{k^2 + 1, k^2 + 2, \dots, k^2 + 2k + 1\right\}.$$

To show this is best possible, let the set be $S = \{a_0 < a_1 < \dots < a_{2k}\}$ so that the hypothesis becomes

$$\begin{aligned} N + 1 &\le a_0 + a_1 + \dots + a_{2k} \\ N/2 &\ge a_{k+1} + \dots + a_{2k}. \end{aligned}$$

Subtracting twice the latter from the former gives

$$\begin{aligned} a_0 &\ge 1 + (a_{k+1} - a_1) + (a_{k+2} - a_2) + \dots + (a_{2k} - a_k) \\ &\ge 1 + \underbrace{k + k + \dots + k}_{k \text{ terms}} = 1 + k^2. \end{aligned}$$

Now, we have

$$\begin{aligned} N/2 &\ge a_{k+1} + \dots + a_{2k} \\ &\ge (a_0 + (k+1)) + (a_0 + (k+2)) + \dots + (a_0 + 2k) \\ &= k \cdot a_0 + ((k+1) + \dots + 2k) \\ &\ge k(k^2+1) + k \cdot \frac{3k+1}{2} \end{aligned}$$

so $N \ge k(2k^2 + 3k + 3)$.

Remark. The exact value of N is therefore very superficial. From playing with these concrete examples we find out we are essentially just trying to find an increasing set S obeying

$$a_0 + a_1 + \dots + a_k > a_{k+1} + \dots + a_{2k} \qquad (\star)$$

and indeed given a sequence satisfying these properties one simply sets $N = 2(a_{k+1} + \dots + a_{2k})$. Therefore we can focus almost entirely on a_i and not N.

Remark. It is relatively straightforward to figure out what is going on based on the small cases. For example, one can work out by hand that

- $\{2, 3, 4\}$ is optimal for $k = 1$
- $\{5, 6, 7, 8, 9\}$ is optimal for $k = 2$,
- $\{10, 11, 12, 13, 14, 15, 16\}$ is optimal for $k = 3$.

In all the examples, the a_i are an arithmetic progression of difference 1, so that $a_j - a_i \ge j - i$ is a sharp for all $i < j$, and thus this estimate may be used freely without loss of sharpness;

> applying it in $(\star)$ gives a lower bound on a_0 which is then good enough to get a lower bound on N matching the equality cases we found empirically.

§1.3 USAMO 2006/3, proposed by Titu Andreescu, Gabriel Dospinescu

Available online at https://aops.com/community/p490625.

Problem statement

For integral m, let $p(m)$ be the greatest prime divisor of m. By convention, we set $p(\pm 1) = 1$ and $p(0) = \infty$. Find all polynomials f with integer coefficients such that the sequence

$$\{p(f(n^2)) - 2n\}_{n \geq 0}$$

is bounded above. (In particular, this requires $f(n^2) \neq 0$ for $n \geq 0$.)

If f is the (possibly empty) product of linear factors of the form $4n - a^2$, then it satisfies the condition. We will prove no other polynomials work. In what follows, assume f is irreducible and nonconstant.

It suffices to show for every positive integer c, there exists a prime p and a nonnegative integer n such that $n \leq \frac{p-1}{2} - c$ and p divides $f(n^2)$.

Firstly, recall there are infinitely many odd primes p, with $p > c$, such that p divides some $f(n^2)$, by Schur's Theorem. Looking mod such a p we can find n between 0 and $\frac{p-1}{2}$ (since $n^2 \equiv (-n)^2 \pmod{p}$). We claim that only finitely many p from this set can fail now. For if a p fails, then its n must be between $\frac{p-1}{2} - c$ and $\frac{p-1}{2}$. That means for some $0 \leq k \leq c$ we have

$$0 \equiv f\left(\left(\frac{p-1}{2} - k\right)^2\right) \equiv f\left(\left(k + \frac{1}{2}\right)^2\right) \pmod{p}.$$

There are only finitely many p dividing

$$\prod_{k=1}^{c} f\left(\left(k + \frac{1}{2}\right)^2\right)$$

unless one of the terms in the product is zero; this means that $4n - (2k+1)^2$ divides $f(n)$. This establishes the claim and finishes the problem.

§2 Solutions to Day 2

§2.1 USAMO 2006/4, proposed by Ricky Liu

Available online at https://aops.com/community/p490647.

Problem statement

Find all positive integers n for which there exist an integer $k \geq 2$ and positive rational numbers $a_1, \ldots, a_k$ satisfying $a_1 + a_2 + \cdots + a_k = a_1 a_2 \ldots a_k = n$.

The answer is all n other than $1, 2, 3, 5$.

Claim — The only solution with $n \leq 5$ is $n = 4$.

Proof. The case $n = 4$ works since $2 + 2 = 2 \cdot 2 = 4$. So assume $n > 4$.

We now contend that $k > 2$. Indeed, if $a_1 + a_2 = a_1 a_2 = n$ then $(a_1 - a_2)^2 = (a_1 + a_2)^2 - 4a_1 a_2 = n^2 - 4n = (n-2)^2 - 4$ is a rational integer square, hence a perfect square. This happens only when $n = 4$.

Now by AM-GM,

$$\frac{n}{k} = \frac{a_1 + \cdots + a_k}{k} \geq \sqrt[k]{a_1 \ldots a_k} = n^{1/k}$$

and so $n \geq k^{\frac{1}{1-1/k}} = k^{\frac{k}{k-1}}$. This last quantity is always greater than 5, since

$$\begin{aligned} 3^{3/2} &= 3\sqrt{3} > 5 \\ 4^{4/3} &= 4\sqrt[3]{4} > 5 \\ k^{\frac{k}{k-1}} &> k \geq 5 \qquad \forall k \geq 5. \end{aligned}$$

This finishes the proof. □

Now, in general:

- If $n \geq 6$ is even, we may take $(a_1, \ldots, a_{n/2}) = (n/2, 2, 1, \ldots, 1)$.
- If $n \geq 9$ is odd, we may take $(a_1, \ldots, a_{(n-3)/2}) = (n/2, 1/2, 4, 1, \ldots, 1)$.
- A special case $n = 7$: one example is $(4/3, 7/6, 9/2)$. (Another is $(7/6, 4/3, 3/2, 3)$.)

Remark. The main hurdle in the problem is the $n = 7$ case. One good reason to believe a construction exists is that it seems quite difficult to prove that $n = 7$ fails.

§2.2 USAMO 2006/5, proposed by Zoran Sunik

Available online at https://aops.com/community/p490682.

Problem statement

A mathematical frog jumps along the number line. The frog starts at 1, and jumps according to the following rule: if the frog is at integer n, then it can jump either to $n+1$ or to $n+2^{m_n+1}$ where 2^{m_n} is the largest power of 2 that is a factor of n. Show that if $k \geq 2$ is a positive integer and i is a nonnegative integer, then the minimum number of jumps needed to reach $2^i k$ is greater than the minimum number of jumps needed to reach 2^i.

We will think about the problem in terms of finite sequences of jumps $(s_1, s_2, \dots, s_\ell)$, which we draw as

$$1 = x_0 \xrightarrow{s_1} x_1 \xrightarrow{s_2} x_2 \xrightarrow{s_3} \dots \xrightarrow{s_\ell} x_\ell$$

where $s_k = x_k - x_{k-1}$ is the length of some hop. We say the sequence is *valid* if it has the property required by the problem: for each k, either $s_k = 1$ or $s_k = 2^{m_{x_{k-1}}+1}$.

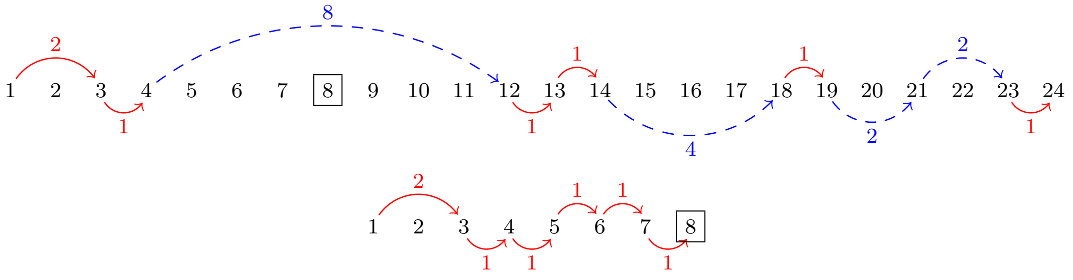
An example is shown below.

Lemma

Let $(s_1, \dots, s_\ell)$ be a sequence of jumps. Suppose we delete pick an index k and exponent $e > 0$, and delete any jumps after the kth one which are divisible by 2^e. The resulting sequence is still valid.

Proof. We only have to look after the kth jump. The launching points of the remaining jumps after the kth one are now shifted by multiples of 2^e due to the deletions; so given a jump $x \xrightarrow{s} x+s$ we end up with a jump $x' \xrightarrow{s} x'+s$ where $x - x'$ is a multiple of 2^e.

But since $s < 2^e$, we have $\nu_2(x') < e$ and hence $\nu_2(x) = \nu_2(x')$ so the jump is valid. □



Now let's consider a valid path to $2^i k$ with ℓ steps, say

$$1 = x_0 \xrightarrow{s_1} x_1 \xrightarrow{s_2} x_2 \xrightarrow{s_3} \dots \xrightarrow{s_\ell} x_\ell = 2^i \cdot k$$

where $s_i = x_i - x_{i-1}$ is the distance jumped.

We delete jumps in the following way: starting from the largest e and going downwards until $e = 0$, we delete all the jumps of length 2^e which end at a point exceeding the target 2^i.

By the lemma, at each stage, the path remains valid. We claim more:

Claim — Let $e \ge 0$. After the jumps of length greater than 2^e are deleted, the resulting end-point is at least 2^i, and divisible by $2^{\min(i,e)}$.

Proof. By downwards induction. Consider any step where *some* jump is deleted. Then, the end-point must be strictly greater than $x = 2^i - 2^e$ (i.e. we must be within 2^e of the target 2^i).

It is also divisible by $2^{\min(i,e)}$ by induction hypothesis, since we are changing the end-point by multiples of 2^e. And the smallest multiple of $2^{\min(i,e)}$ exceeding x is 2^i. $\square$

On the other hand by construction when the process ends the reduced path ends at a point at most 2^i, so it is 2^i as desired.

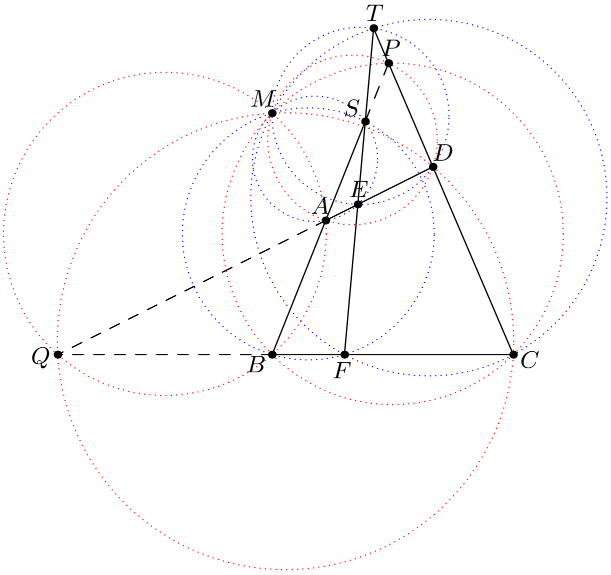
Therefore we have taken a path to $2^i k$ and reduced it to one to 2^i by deleting some jumps. This proves the result.

§2.3 USAMO 2006/6, proposed by Zuming Feng, Zhonghao Ye

Available online at https://aops.com/community/p490691.

Problem statement

Let $ABCD$ be a quadrilateral, and let E and F be points on sides AD and BC, respectively, such that $\frac{AE}{ED} = \frac{BF}{FC}$. Ray FE meets rays BA and CD at S and T, respectively. Prove that the circumcircles of triangles SAE, SBF, TCF, and TDE pass through a common point.



Let M be the Miquel point of $ABCD$. Then M is the center of a spiral similarity taking AD to BC. The condition guarantees that it also takes E to F. Hence, we see that M is the center of a spiral similarity taking $\overline{AB}$ to $\overline{EF}$, and consequently the circumcircles of QAB, QEF, SAE, SBF concur at point M.

In other words, the Miquel point of $ABCD$ is also the Miquel point of $ABFE$. Similarly, M is also the Miquel point of $EDCF$, so all four circles concur at M.