

IMO 2003 Solution Notes

COMPILED BY EVAN CHEN

April 15, 2019

This is an compilation of solutions for the 2003 IMO. 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 on the Art of Problem Solving forums.

Corrections and comments are welcome!

Contents

0 Problems	2
1 IMO 2003/1	3
2 IMO 2003/2	4
3 IMO 2003/3	5
4 IMO 2003/4	7
5 IMO 2003/5	8
6 IMO 2003/6	10

§0 Problems

1. Let A be a 101-element subset of $S = \{1, 2, \dots, 10^6\}$. Prove that there exist numbers t_1, t_2, \dots, t_{100} in S such that the sets

$$A_j = \{x + t_j \mid x \in A\}, \quad j = 1, 2, \dots, 100$$

are pairwise disjoint.

2. Determine all pairs of positive integers (a, b) such that

$$\frac{a^2}{2ab^2 - b^3 + 1}$$

is a positive integer.

3. Each pair of opposite sides of convex hexagon has the property that the distance between their midpoints is $\frac{\sqrt{3}}{2}$ times the sum of their lengths. Prove that the hexagon is equiangular.
4. Let $ABCD$ be a cyclic quadrilateral. Let P, Q and R be the feet of perpendiculars from D to lines \overline{BC} , \overline{CA} and \overline{AB} , respectively. Show that $PQ = QR$ if and only if the bisectors of angles ABC and ADC meet on segment \overline{AC} .
5. Let n be a positive integer and let $x_1 \leq x_2 \leq \dots \leq x_n$ be real numbers. Prove that

$$\left(\sum_{i=1}^n \sum_{j=1}^n |x_i - x_j| \right)^2 \leq \frac{2(n^2 - 1)}{3} \sum_{i=1}^n \sum_{j=1}^n (x_i - x_j)^2$$

with equality if and only if x_1, x_2, \dots, x_n form an arithmetic sequence.

6. Let p be a prime number. Prove that there exists a prime number q such that for every integer n , the number $n^p - p$ is not divisible by q .

§1 IMO 2003/1

Let A be a 101-element subset of $S = \{1, 2, \dots, 10^6\}$. Prove that there exist numbers t_1, t_2, \dots, t_{100} in S such that the sets

$$A_j = \{x + t_j \mid x \in A\}, \quad j = 1, 2, \dots, 100$$

are pairwise disjoint.

A greedy algorithm works: suppose we have picked

$$T = \{t_1, \dots, t_n\}$$

as large as possible, meaning it's impossible to add any more elements to T . That means, for each $t \in \{1, \dots, 10^6\}$ either $t \in T$ already or there exists two distinct elements $a, b \in A$ and $t_i \in T$ such that

$$t = t_i + b - a \quad (\star).$$

There are at most $|T| \cdot |A| \cdot (|A| - 1) = n \cdot 101 \cdot 100$ possible values for the right-hand side of (\star) . So we therefore must have

$$101 \cdot 100 \cdot n + n \geq 10^6$$

which implies $n > 99$, as desired.

§2 IMO 2003/2

Determine all pairs of positive integers (a, b) such that

$$\frac{a^2}{2ab^2 - b^3 + 1}$$

is a positive integer.

The answer is $(a, b) = (2\ell, 1)$, $(a, b) = (\ell, 2\ell)$ and $(a, b) = (8\ell^4 - \ell, \ell)$, for any ℓ . Check these work.

In the sequel, assume $b > 1$, and integers a, b, k obey $k = \frac{a^2}{2ab^2 - b^3 + 1}$. Expanding, we have the polynomial

$$X^2 - 2kb^2 \cdot X + k(b^3 - 1) = 0$$

has two integer roots, one of which is $X = a$. This means solutions to the original problem come in pairs (even with k fixed):

$$(a, b) \longleftrightarrow (2kb^2 - a, b) = \left(\frac{k(b^3 - 1)}{a}, b \right).$$

(Here, the first representation ensures $2kb^2 - a \in \mathbb{Z}$, while the latter representation and the hypothesis $b > 1$ ensures that $\frac{k(b^3 - 1)}{a} > 0$.)

On the other hand, we claim that:

Claim — For any solution (a, b) , either $2a = b$ or $a > b$.

Proof. Since the denominator is positive, $a \geq b/2$. Now,

$$a^2 \geq 2ab^2 - b^3 + 1 \iff a^2 \geq b^2(2a - b) + 1$$

and so if $2a - b > 0$ then $a^2 > b^2 \implies a > b$. □

Now assume we have pair (a_1, b) and (a_2, b) of solutions with $b \neq 2a_1, 2a_2$. Then assume $a_1 > a_2 > b$ and

$$\begin{aligned} a_1 + a_2 &= 2k \cdot b^2 \\ a_1 a_2 &= k(b^3 - 1) \end{aligned}$$

That's impossible, since then $a_1 \geq kb^2$ so $a_1 a_2 > kb^3$. Thus the only solutions are the ones we claimed at the beginning.

Remark. Important to notice that the problem is *positive divides*, not just divides. There is an implicit inequality built in to the problem statement and it is essentially impossible to solve without. I would be interested in a pair (a, b) for which $k < 0$, $k \in \mathbb{Z}$ yet $a, b > 0$.

§3 IMO 2003/3

Each pair of opposite sides of convex hexagon has the property that the distance between their midpoints is $\frac{\sqrt{3}}{2}$ times the sum of their lengths. Prove that the hexagon is equiangular.

Unsurprisingly, this is a geometric inequality. Denote the hexagon by $ABCDEF$. Then we have that

$$\left| \frac{\vec{D} + \vec{E}}{2} - \frac{\vec{A} + \vec{B}}{2} \right| = \sqrt{3} \cdot \frac{|\vec{B} - \vec{A}| + |\vec{E} - \vec{D}|}{2} \geq \sqrt{3} \cdot \left| \frac{(\vec{B} - \vec{A}) - (\vec{E} - \vec{D})}{2} \right|$$

and cyclic variations. Suppose we define the right-hand sides as variables

$$\vec{x} = (\vec{B} - \vec{A}) - (\vec{E} - \vec{D})$$

$$\vec{y} = (\vec{D} - \vec{C}) - (\vec{A} - \vec{F})$$

$$\vec{z} = (\vec{F} - \vec{E}) - (\vec{C} - \vec{B}).$$

Then we now have

$$|\vec{y} - \vec{z}| \geq \sqrt{3} |\vec{x}|$$

$$|\vec{z} - \vec{x}| \geq \sqrt{3} |\vec{y}|$$

$$|\vec{x} - \vec{y}| \geq \sqrt{3} |\vec{z}|.$$

We square all sides (using $|\vec{v}|^2 = \vec{v} \cdot \vec{v}$) and then sum to get

$$\sum_{\text{cyc}} (\vec{y} - \vec{z}) \cdot (\vec{y} - \vec{z}) \geq 3 \sum_{\text{cyc}} \vec{x} \cdot \vec{x}$$

which rearranges to

$$-|\vec{x} + \vec{y} + \vec{z}|^2 \geq 0.$$

This can only happen if $\vec{x} + \vec{y} + \vec{z} = 0$, and moreover all the inequalities above were actually equalities. That means that our triangle inequalities above were actually sharp (and already we have $\overline{AB} \parallel \overline{DE}$ and so on).

Working with just x and y now we have

$$\begin{aligned} 3(\vec{x} \cdot \vec{x}) &= (2\vec{y} - \vec{x}) \cdot (2\vec{y} - \vec{x}) \\ &= \vec{x} \cdot \vec{x} - 4\vec{y} \cdot \vec{x} + 4\vec{y} \cdot \vec{y} \\ \implies -\vec{x} \cdot \vec{x} + 2(\vec{y} \cdot \vec{y}) &= 2\vec{x} \cdot \vec{y} \\ 2(\vec{x} \cdot \vec{x}) - \vec{y} \cdot \vec{y} &= 2\vec{x} \cdot \vec{y}. \end{aligned}$$

which implies $\vec{x} \cdot \vec{x} = \vec{y} \cdot \vec{y}$, that is, \vec{x} and \vec{y} have the same magnitude. In this way we find \vec{x} , \vec{y} , \vec{z} all have the same magnitude, and since $\vec{x} + \vec{y} + \vec{z} = 0$ they are related by 120° rotations, as desired.

Remark. In fact one can show further that the equiangular hexagons which work are exactly those formed by taking an equilateral triangle and cutting off equally sized corners. This equality case helps motivate the solution.

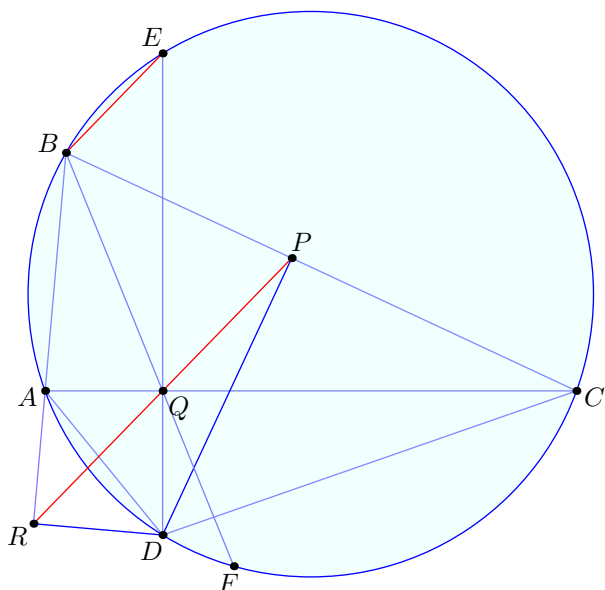
Remark. One can note this “must” be an inequality because the space of such hexagons is 2-dimensional, even though *a priori* the space of hexagons satisfying three given conditions should have dimension $9 - 3 = 6$.

§4 IMO 2003/4

Let $ABCD$ be a cyclic quadrilateral. Let P, Q and R be the feet of perpendiculars from D to lines BC, CA and AB , respectively. Show that $PQ = QR$ if and only if the bisectors of angles ABC and ADC meet on segment \overline{AC} .

Let γ denote the circumcircle of $ABCD$. The condition on bisectors is equivalent to $(AC; BD)_\gamma = -1$. Meanwhile if ∞ denotes the point at infinity along Simson line \overline{PQR} then $PQ = QR$ if and only if $(PR; Q\infty) = -1$.

Let rays BQ and DQ meet the circumcircle again at F and E .



Lemma (EGMO Proposition 4.1)

Then $\overline{BE} \parallel \overline{PQR}$.

Proof. Since $\angle DPR = \angle DAR = \angle DAB = \angle DEB$. □

Now we have

$$(PR; Q\infty) \stackrel{B}{=} (CA; FE)_\gamma \stackrel{Q}{=} (AC; BD)_\gamma$$

as desired.

§5 IMO 2003/5

Let n be a positive integer and let $x_1 \leq x_2 \leq \dots \leq x_n$ be real numbers. Prove that

$$\left(\sum_{i=1}^n \sum_{j=1}^n |x_i - x_j| \right)^2 \leq \frac{2(n^2 - 1)}{3} \sum_{i=1}^n \sum_{j=1}^n (x_i - x_j)^2$$

with equality if and only if x_1, x_2, \dots, x_n form an arithmetic sequence.

Let $d_1 = x_2 - x_1, \dots, d_{n-1} = x_n - x_{n-1}$. The inequality in question becomes:

$$\left(\sum_i i(n-i)d_i \right)^2 \leq \frac{n^2 - 1}{3} \cdot \left(\sum_i i(n-i)d_i^2 + 2 \sum_{i < j} i(n-j)d_i d_j \right).$$

Clearing the square on the right-hand side we want to show

$$\sum_{i < j} (3ij(n-i)(n-j) - (n^2 - 1)i(n-j)) \cdot 2d_i d_j \leq \sum_i (n^2 - 1 - 3i(n-i)) \cdot i(n-i)d_i^2.$$

We use AM-GM directly on $2d_i d_j \leq d_i^2 + d_j^2$: this actually solves the problem. The annoying part is to check that the coefficients actually match:

Claim (Big bash) — For an index $1 \leq k \leq n-1$, we have

$$\begin{aligned} & \sum_{i < k} (3ik(n-i)(n-k) - (n^2 - 1)i(n-k)) \\ & + \sum_{j > k} (3kj(n-k)(n-j) - (n^2 - 1)k(n-j)) \\ & = (n^2 - 1 - 3k(n-k)) \cdot k(n-k). \end{aligned}$$

Proof. Rewrite as:

$$\begin{aligned} 3k(n-k) \left(-k(n-k) + \sum_i i(n-i) \right) &= (n^2 - 1) \left((n-k) \sum_{i < k} i + k \sum_{j > k} (n-j) \right) \\ &\quad + (n^2 - 1 - 3k(n-k)) \cdot k(n-k) \\ \iff 3k(n-k) \sum_i i(n-i) &= (n^2 - 1) \left((n-k) \sum_{i < k} i + k \sum_{j > k} (n-j) \right) \\ &\quad + (n^2 - 1)k(n-k) - 3k^2(n-k)^2 \\ \iff 3k(n-k) \left(\sum_i i(n-i) \right) &= (n^2 - 1) \left((n-k) \sum_{i \leq k} i + k \sum_{i < n-k} i \right) \\ \iff 3k(n-k) \frac{(n-1)n(n+1)}{6} &= (n^2 - 1) \left((n-k) \frac{k(k+1)}{2} \right) \\ &\quad + (n^2 - 1) \left(k \frac{(n-k)(n-k-1)}{2} \right) \\ \iff 3k(n-k) \frac{(n-1)n(n+1)}{6} &= (n^2 - 1)k(n-k) \cdot \frac{n}{2} \end{aligned}$$

which is visibly true. □

Equality occurs only if all d_i are equal because the coefficient of $d_i d_j$ is nonzero for any $i \leq n/2$ and $j \geq n/2$.

§6 IMO 2003/6

Let p be a prime number. Prove that there exists a prime number q such that for every integer n , the number $n^p - p$ is not divisible by q .

By orders, we must have $q = pk + 1$ for this to be possible. So we just need $n^p \not\equiv p \pmod{q} \iff p^k \not\equiv 1 \pmod{q}$.

So we need a prime $q \equiv 1 \pmod{p}$ such that $p^k \not\equiv 1 \pmod{q}$. To do this, we first recall the following lemma.

Lemma

Let $\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$. For any integer a , if q is a prime divisor of $\Phi_p(a)$ other than p , then $a \pmod{q}$ has order p . (In particular, $q \equiv 1 \pmod{p}$.)

Proof. We have $a^p - 1 \equiv 0 \pmod{q}$, so either the order is 1 or p . If it is 1, then $a \equiv 1 \pmod{q}$, so $q \mid \Phi_p(1) = p$, hence $q = p$. \square

Now the idea is to extract a prime factor q from the cyclotomic polynomial

$$\Phi_p(p) = \frac{p^p - 1}{p - 1} \equiv 1 + p \pmod{p^2}$$

such that $q \not\equiv 1 \pmod{p^2}$; hence $k \not\equiv 0 \pmod{p}$, and as $p \pmod{q}$ has order p we have $p^k \not\equiv 1 \pmod{q}$.