Problem Set Week 6 Solutions

Math Olympiad Club Zurich

Spring 2025

Problem B-1 (IMC 2023)

Ivan writes the matrix

$$A = \begin{bmatrix} 2 & 2 \\ 3 & 4 \end{bmatrix}$$

on the board. Then he performs the following operation on the matrix several times:

- He chooses a row or a column of the matrix, and
- He multiplies or divides the chosen row or column entry-wise by the other row or column, respectively.

Can Ivan end up with the matrix

$$B = \begin{bmatrix} 2 & 2 \\ 4 & 3 \end{bmatrix}$$

after finitely many steps?

Solution:

We show that starting from $A = \begin{bmatrix} 2 & 2 \\ 3 & 4 \end{bmatrix}$, Ivan cannot reach the matrix $B = \begin{bmatrix} 2 & 2 \\ 4 & 3 \end{bmatrix}$.

Notice first that the allowed operations preserve the positivity of entries; all matrices Ivan can reach have only positive entries. The key insight is to recognize that the operations resemble standard row/column addition/subtraction operations (which preserve determinants), but here addition/subtraction is replaced by multiplication/division. This suggests the need for a group morphism. Hence, we define boldly for any matrix $X = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} \in \mathbb{R}_{>0}^{2\times 2}$ with positive entries, the following auxiliary logarithmic transformation matrix:

$$L(X) = \begin{bmatrix} \log_2(x_{11}) & \log_2(x_{12}) \\ \log_2(x_{21}) & \log_2(x_{22}) \end{bmatrix}.$$

By taking logarithms of the entries, which transform multiplication to addition (as it is a group morphism from $(\mathbb{R}_{>0}, \cdot)$ to $(\mathbb{R}, +)$), Ivan's operations on $L(X)$ translate to adding or subtracting a row or column of $L(X)$ to itself. Such standard row and column operations are well known to preserve the determinant. Hence, if Ivan performs one operation on matrix X_0 to obtain X_1, then:

$$\det_{\mathbb{R}}(L(X_0)) = \det_{\mathbb{R}}(L(X_1)).$$

By a trivial induction, for any finite sequence of operations of length $n \geq 0$, applied recursively starting from X_0, we obtain the sequence of matrices $X_0, \ldots, X_n$ for which we have:

$$\det_{\mathbb{R}} (L(X_0)) = \det_{\mathbb{R}} (L(X_n)) .$$

Thus, a necessary condition to reach B from A with a finite sequence of operations on A is that the corresponding logarithmic matrix satisfies:

$$\det_{\mathbb{R}} (L(A)) = \det_{\mathbb{R}} (L(B)) .$$

However,

$$\det_{\mathbb{R}} (L(A)) = \log_2 (2) \cdot \log_2 (4) - \log_2 (2) \cdot \log_2 (3) = \log_2 \left(\frac{4}{3}\right) > \log_2 (1) = 0,$$

and

$$\det_{\mathbb{R}} (L(B)) = \log_2 (2) \cdot \log_2 (3) - \log_2 (2) \cdot \log_2 (4) = \log_2 \left(\frac{3}{4}\right) < \log_2 (1) = 0.$$

That is $\det_{\mathbb{R}} (L(B)) < 0 < \det_{\mathbb{R}} (L(A))$ and the two quantities cannot be equal. This proves that Ivan cannot transform A into B.

Vieta Jumping Problems

0.1 Problem 6 (IMO 1988)

Let a and b be positive integers such that $ab+1$ divides a^2+b^2. Show that

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

is the square of an integer.

Solution:

Define

$$S := \left\{(a,b) \in \mathbb{N}^* \times \mathbb{N}^* \mid ab+1 \mid a^2+b^2\right\}.$$

For each $k \in \mathbb{N}^*$, define

$$S_k := \left\{(a,b) \in \mathbb{N}^* \times \mathbb{N}^* \mid a^2+b^2 = k(ab+1)\right\}.$$

Clearly, S is decomposed into the sets S_k:

$$S = \bigcup_{k\in\mathbb{N}^*} S_k,$$

and for any $k \in \mathbb{N}^*$ we have:

$$(a,b) \in S_k \Leftrightarrow (b,a) \in S_k.$$

To show the statement of the problem, we therefore need to show that for a fixed $k > 0$ with $S_k \neq \varnothing$, we have $k \in \square_{\mathbb{N}} := \{n^2 \mid n \in \mathbb{N}\}$.

For a fixed $k > 0$ with $S_k \neq \varnothing$, we can define the following minimum:

$$b' := \min\left\{\min\{a,b\} \mid (a,b) \in S_k\right\}.$$

By construction, there exists $(a,b) \in S_k$ such that $b' = \min\{a,b\}$. Label

$$a' = \max\{a,b\}.$$

Then $(a',b') \in S_k$ and we have the equation:

$$a'^2 - ka'b' + b'^2 - k = 0,$$

which is quadratic in a'. Let $c' \in \mathbb{C}$ be the other root of the polynomial $X^2 - kb'X + b'^2 - k$ (this is the famous *root jumping*). We show that $c' = 0$, leading to the factorization

$$X^2 - kb'X + b'^2 - k = X(X-a'),$$

and will imply that $k = b'^2$, which will conclude $k \in \square_{\mathbb{N}}$.

By Vieta's formulas for the coefficient of degree 1 and the constant coefficient, we obtain respectively:

$$c' = kb' - a' \in \mathbb{Z},$$

and

$$a'c' = b'^2 - k < b'^2,$$

where we used the fact $k \geq 1$. In particular, c' is subject to the order $<$ of $\mathbb{Z}$. Suppose to obtain a contradiction that $c' > 0$; then:

$$b'c' \leq a'c' < b'^2 \implies c' < b',$$

where we used $0 < b' \leq a'$ and $0 < c'$.

By choice of c', we have $c'^2 - kb'c' + b'^2 - k = 0$, i.e.,

$$c'^2 + b'^2 = k(c'b' + 1),$$

this implies that $(c', b') \in S_k$. As $c' < b'$, we have a contradiction to the minimality of b'. Thus $c' \leq 0$.

Additionally,

$$(a'+1)(c'+1) = a'c' + a' + c' + 1 = b'^2 - k + b'k + 1 = b'^2 + (b'-1)k + 1 \geq 1,$$

where we used $b' \geq 1$ and $k > 0$. As $a' + 1 > 1$, we must have $c' + 1 > 0$, i.e., $c' > -1$, so we conclude that $c' = 0$ as desiblack. Since $k > 0$ with $S_k \neq \varnothing$ was arbitrary, we are done.

0.2 Problem (Kevin Buzzard & Edward Crane)

Let a and b be positive integers. Show that if $4ab - 1$ divides $\left(4a^2 - 1\right)^2$, then $a = b$.

Solution:

Standard manipulations[1] of $4ab - 1 \mid \left(4a^2 - 1\right)^2$ show that this implies $4ab - 1 \mid (a-b)^2$.

So it suffices to show the statement that if $4ab - 1 \mid_{\mathbb{Z}} (a-b)^2$ then $a = b$. Assume for the sake of contradiction that there exist positive integers a and b with $a \neq b$ such that $4ab - 1 \mid (a-b)^2$. Define:

$$k = \frac{(a-b)^2}{4ab - 1} > 0.$$

Consider the set

$$S_k := \left\{(a', b') \in \mathbb{N}^* \times \mathbb{N}^* \mid (a' - b')^2 = k(4a'b' - 1)\right\}.$$

Notice that S_k cannot contain a pair on the diagonal of $\mathbb{N}^*$ as $4a'b' - 1 \geq 3$ and $k > 0$ and, in addition, $(a', b') \in S_k \Leftrightarrow (b', a') \in S_k$.

Since $S_k \neq \varnothing$, there exists a pair $(A, B) \in S_k$ that minimizes $A + B$. As said above, we necessarily have $A \neq B$ and by the symmetry above we can without loss of generality assume $A > B$. Consider the quadratic polynomial arising from the condition of $(A, B) \in S_k$:

$$X^2 - (2B + 4kB)X + B^2 + k = 0.$$

[1] Let $m = 4ab - 1$. Since $\gcd(b, m) = 1$, b is invertible modulo m. Note that

$$4a^2b \;=\; a\,(4ab) \;\equiv\; a \pmod{m} \quad\implies\quad 4a^2 \equiv a\,b^{-1} \pmod{m}.$$

Hence $b\,(4a^2 - 1) \equiv b\,(ab^{-1} - 1) \equiv a - b \pmod{m} \quad\implies\quad b^2\,(4a^2-1)^2 \equiv (a-b)^2 \pmod{m}$. By hypothesis $m \mid (4a^2-1)^2$, so $m \mid b^2(4a^2-1)^2$. Therefore, $4ab - 1 \mid (a-b)^2$, as claimed.

This polynomial has roots $x_1 := A > 0$ by construction. By Vieta's formulas for the coefficient of degree 1 and the constant coefficient, we obtain respectively that:

$$x_2 := 2B + 4kB - A \in \mathbb{Z}$$

is also a root (this is the famous *root jumping*) and an integer, satisfying:

$$x_2 = \frac{B^2 + k}{A} > 0.$$

Since x_2 is a positive integer, we have $(x_2, B) \in S_k$. By the minimality of $A+B$: $A+B \leq x_2+B$ from which it follows $x_2 \geq A$, i.e.,

$$\frac{B^2 + k}{A} \geq A.$$

Thus, we obtain (as $A > 0$)

$$k \geq A^2 - B^2 = (A - B)(A + B) > 0.$$

From $k \geq (A - B)(A + B) > 0$ and $4AB - 1 \geq 3$ we get in order:

$$(A - B)^2 = k(4AB - 1) \geq \left(A^2 - B^2\right) 3.$$

Since $A - B > 0$ we can divide the inequality on both sides without changing the inequality direction to obtain:

$$A + B \geq A - B \geq 3(A + B) \geq 3(A + B),$$

Again dividing by $A + B > 0$ the inequality is preserved and we obtain $1 \geq 3$. This is a contradiction. Thus, our assumption must be false, and the statement is proven.

Problem A-3 (IMC 2015)

Let $F(0) = 0$, $F(1) = \frac{3}{2}$, and

$$F(n) = \frac{5}{2}F(n-1) - F(n-2) \quad \text{for } n \geq 2.$$

Determine whether or not

$$\sum_{n=0}^{\infty} \frac{1}{F(2^n)}$$

is a rational number.

Solution:

The characteristic polynomial of the linear recurrence is:

$$X^2 - \frac{5}{2}X + 1,$$

which has roots $\{2, \frac{1}{2}\}$. Thus, the general form of $F(n)$ is given by:

$$F(n) = a \cdot 2^n + b \cdot \left(\frac{1}{2}\right)^n$$

for some constants a and b. Using the initial conditions $F(0) = 0$ and $F(1) = \frac{3}{2}$, we obtain the system:

$$a + b = 0,$$
$$2a + \frac{b}{2} = \frac{3}{2}.$$

Solving for a and b, we get $a = 1$, $b = -1$. Therefore,

$$F(n) = 2^n - 2^{-n}$$

which is strictly greater than 0 as long as $n \geq 1$. Now, we can rewrite the summand:

$$\frac{1}{F(2^n)} = \frac{1}{2^{2^n} - 2^{-2^n}} = \frac{2^{2^n}}{(2^{2^n})^2 - 1} = \frac{1}{2^{2^n} - 1} - \frac{1}{2^{2^{n+1}} - 1},$$

where we use in the last equality the fact that for $a \in \mathbb{R} \setminus \{\pm 1\}$ we have:

$$\frac{a}{a^2 - 1} = \frac{a}{a+1}\frac{1}{a-1} = \left(1 - \frac{1}{a+1}\right)\frac{1}{a-1} = \frac{1}{a-1} - \frac{1}{a^2 - 1}.$$

We obtain clearly a telescoping sum:

$$\sum_{n=0}^{\infty} \frac{1}{F(2^n)} = \sum_{n=0}^{\infty} \left(\frac{1}{2^{2^n} - 1} - \frac{1}{2^{2^{n+1}} - 1}\right) = \frac{1}{2^{2^0} - 1} = 1.$$

Since 1 is rational, the sum is rational.