Second stage of Israeli students competition, 2020 - Solutions.

Remark. Problem 1 that was given was not the intended problem. We present both the problem 1 that was given (which is called here problem 1) and the intended problem, problem 1` which might be more interesting.

1. Let A be the number of ways to present 5780 as a sum of a finite sequence of non-decreasing positive integers, such that the 5^{th} integer is 5. Let B be the number of ways to present 5755 as a sum of a sequence of length at most 9 of non-decreasing positive integers. Which of the two numbers is greater: A or $126 \cdot B$?

Answer: *A* is greater.

Solution. We will construct a lot of presentations of 5780 that will give a bound on A, then we will give a naïve bound on B, showing that A is much bigger.

We need to construct many examples of $x_1 + x_2 + ... + x_n = 5780$, so that x_i are non-decreasing and $x_5 = 5$. We choose $x_1 = x_2 = ... = x_5 = 5$, so we now need $x_6 + x_7 + ... + x_n = 5755$ with x_i non-decreasing and each one at least 5**,** write $y_i = x_{i+5} - 5$ and $m = n - 5$, now we need $y_1 + y_2 + ... + y_m = 5755 - 5m$ with y_i non-decreasing and non-negative.

Choose $S \subset \{1,2,...,100\}$, and set $m = 101$, $y_i = i \cdot 1_{i \in S}$ (in other words it is i if $i \in S$ and 0 otherwise) for $1 \le i \le 100$ and $y_{101} = 5755 - 5m - \sum_{i \in S} i$.

notice that since $\sum_{i=1}^{100} i = \frac{100 \cdot 101}{2} = 5050 = 5755 - 5 \cdot 101 - 250$ we will have $y_{101} \ge 250$. The only problem with this example is that the series could decrease, we fix this by reordering the y_i in ascending order. This gives 2^{100} examples, and they are all different since the numbers between 1 and 100 appearing in the series is exactly S. Therefore $A \ge 2^{100}$.

For B we have to bound the number of $x_1 + x_2 ... + x_9 = 5755$ with x_i non-decreasing. Notice that $5755 \le 2^{13}$, and that $x_i \le \frac{2^{13}}{10-i}$ since otherwise the sum would be too big, since x_9 is determined by $x_1, x_2, ..., x_8$ we get that $B \le \frac{2^{13}}{9} \cdot \frac{2^{13}}{8} \cdot ... \cdot \frac{2^{13}}{2} = \frac{2^{13 \cdot 8}}{9!} = \frac{2^{104}}{9!}$, now a simple calculation would show that

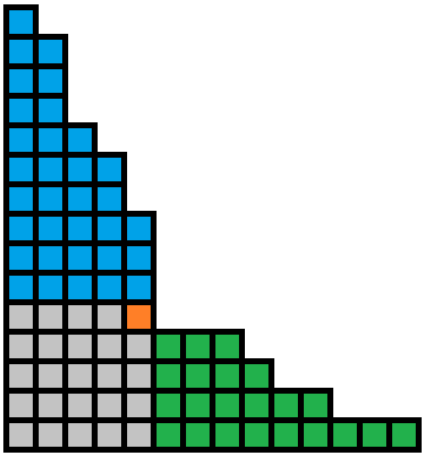
$$9! = 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 = 2 \cdot 4 \cdot (3 \cdot 6) \cdot (5 \cdot 7) \cdot 8 \cdot 9 > 2 \cdot 4 \cdot 2^4 \cdot 2^5 \cdot 2^3 \cdot 2^3 =$$
$$= 2^{3+4+5+3+3} = 2^{18}$$

so $B \le 2^{86}$, since $126 \le 2^7 < 2^{12}$ we are done.

1'. Let A be the number of ways to present 5780 as a sum of a finite sequence of non-increasing positive integers, such that the 5^{th} integer is 5. Let B be the number of ways to present 5755 as a sum of a sequence of length at most 9 of non-increasing positive integers. Which of the two numbers is greater: A or $126 \cdot B$?

Answer. $126 \cdot B$ is greater.

Solution. For brevity, we shall call "the number of ways to present number as a sum of …" a *partition*. It is useful to think of partitions as Young diagrams: several rows of cells, in organized in decreasing order from bottom to top, one above another, starting at the same place on the left.



If we have a partition of 5780 such that the 5^{th} largest number is 5, and if we take out the 5×5 cells in the corner (gray and orange), we get that all the other 5755 cells are either in 5 lowest rows or 4 leftmost columns.

So from a partition of 5780 of a prescribed kind (which are enumerated by the number A in the problem) we get a partition of 5755 into 9 summands.

It is possible to reconstruct the original partition given sum additional data. Let us assume we have a partition $5755 = b_1 + b_2 + ... + b_9$ where $b_1 \geq b_2 \geq ... \geq b_9 \geq 0$, which is the same as the prescribed type of a partitions enumerated by B in the problem; additionally we assume that we have a separation of $\{1,2,3,4,5,6,7,8,9\}$ into a disjoint union of $\{i_1, i_2, i_3, i_4\}$ and $\{j_1, j_2, j_3, j_4, j_5\}$. Given such partition + separation, we may define the partition of the first kind (such as enumerated by A): we start by making a 5×5 square, we add $b_{i_1}, b_{i_2}, b_{i_3}, b_{i_4}$ cells to the first 4 rows, and add $b_{j_1}, b_{j_2}, b_{j_3}, b_{j_4}, b_{j_5}$ cells to the first 5 columns; we get 5755 + 25 cells in total which is 5780.

So we have defined a function from a set of $\binom{9}{4} \cdot B$ elements (separation and a partition of 5755 of the second kind) to a set of A elements (partition of 5780 of the first kind). This function is surjective, but it is not injective. It might happen that $b_{i_k} = b_{j_m}$ and in that case flipping the two indices i_k and j_m, meaning moving each of them to the other section, doesn't really change the result.

So, $\binom{9}{4} \cdot B > A$.

It remains to compute that $\binom{9}{4} = \frac{9 \cdot 8 \cdot 7 \cdot 6}{4 \cdot 3 \cdot 2 \cdot 1} = 9 \cdot 7 \cdot 2 = 63 \cdot 2 = 126$.

2. Find the greatest real α for which the sequence $a_n = n^\alpha \int_0^\infty \left(\frac{\sin x}{x} \right)^n dx$ will converge, and compute $\lim a_n$ for that value of α.

Answer. $\alpha = \frac{1}{2}$ and in that case $\lim a_n = \sqrt{\frac{3\pi}{2}}$.

Solution. Denote $f(x) = \frac{\sin x}{x}$.

Let us discuss behavior of f. Since $|\sin x| \le |x|$, we have $|f(x)| < 1$ for $x > 0$ but $f(x) \underset{x \to 0}{\to} 1$.

It is reasonable to divide the integral into the following intervals:

$$I_0 = [0, \varepsilon],\ I_1 = [\varepsilon, \pi],\ I_2 = [\pi, 2\pi],\ I_3 = [2\pi, 3\pi], \ldots$$

where ε is some fixed small positive number, say $\frac{1}{100}$.

For $k \ge 2$, we have $|f(x)| \le \frac{1}{(k-1)\pi}$ and $\left| \int_{I_k} (f(x))^n dx \right| \le \frac{\pi}{(k-1)^n \pi^n}$.

Notice that $\sum_{k=2}^{\infty} \frac{1}{(k-1)^n} < C$ for some constant C and for any α we have $\frac{n^\alpha}{\pi^n} \underset{n \to \infty}{\to} 0$. From here it follows easily that we may disregard $x > \pi$ (since exponent is stronger than polynomial).

For similar reasons, we may disregard I_1. Indeed, take $r = f(\varepsilon) < 1$.

It is easy to verify that f is monotonically decreasing on $[0, \pi]$.

Then $\left| n^\alpha \int_{I_1} (f(x))^n dx \right| \le n^\alpha \cdot \pi \cdot r^n \to 0$

So it is enough to discuss the interval $[0, \varepsilon]$.

Notice that $\sin x = x - \frac{x^3}{3!} + o(x^4)$, so $f(x) = 1 - \frac{x^2}{6} + o(x^3)$.

In other words for any $\delta > 0$ (say $\delta = 0.01$) we may assume we have chosen ε so that $1-\left(\frac{1}{6}+\delta\right)x^2 \le f(x) \le 1-\left(\frac{1}{6}-\delta\right)x^2$.

We shall write $X = L(Y)$ to say $|X| \le |Y|$. (Remark: we want to emphasize the difference with a common notation $O(N), \Theta(N)$ - in our notation no constant is hidden.)

So the previous formula may be shortened to $f(x) = 1-\left(\frac{1}{6}+L[\delta]\right)x^2$.

Notice that $\left(1-\frac{u}{n}\right)^n > e^{-au} > \left(1-\frac{u}{n}\right)^{n+1}$, so $\left(1-\frac{u}{n}\right)^n = e^{-u}\cdot\left(1-L\left(\frac{u}{n}\right)\right)$

Consider an example $\alpha = \frac{1}{2}$.

$$a_n = \sqrt{n}\cdot\int_0^{\varepsilon}\left(f(x)\right)^n dx = \frac{1}{2}\sqrt{n}\cdot\int_{-\varepsilon}^{\varepsilon}\left(f(x)\right)^n dx = \frac{1}{2}\cdot\int_{-\varepsilon\sqrt{n}}^{\varepsilon\sqrt{n}}\left(f\left(\frac{y}{\sqrt{n}}\right)\right)^n dy =$$

$$= \frac{1}{2}\cdot\int_{-\varepsilon\sqrt{n}}^{\varepsilon\sqrt{n}}\left(1-\left(\frac{1}{6}+L(\delta)\right)\frac{y^2}{n}\right)^n dy = \frac{1}{2}\cdot\int_{-\varepsilon\sqrt{n}}^{\varepsilon\sqrt{n}} e^{-y^2\left(\frac{1}{6}+L(\delta)\right)}\left(1-L\left(\frac{1}{5}\cdot\frac{y^2}{n}\right)\right)dy =$$

$$= \frac{1}{2}\cdot\int_{-\varepsilon\sqrt{n}}^{\varepsilon\sqrt{n}} e^{-y^2\left(\frac{1}{6}+L(\delta)\right)}\left(1-L\left(\frac{\varepsilon^2}{5}\right)\right)dy$$

For ε, δ sufficiently small, the expression will be as close as you require to $\frac{1}{2}\cdot\int_{-\varepsilon\sqrt{n}}^{\varepsilon\sqrt{n}} e^{-\frac{y^2}{6}}dy$. The error of this approximation is independent on n, as the integrand is rapidly decaying and the integral over all the reals converges.

When $n\to\infty$ it tends to $\frac{1}{2}\cdot\int_{-\infty}^{\infty} e^{-\frac{y^2}{6}}dy = \frac{1}{2}\sqrt{6\pi}$. So, for $\alpha = \frac{1}{2}$ we have $a_n \to \sqrt{\frac{3}{2}\pi}$.

From here it follows, that for any higher α the sequence will diverge, and for any lower α it will converge to 0.

3. A equilateral triangle with sides of length 100 is contained in the N-dimensional closed unit cube $[0,1]^N$. What is the minimal possible N?

Answer. 15000.

Solution. In the 15000-dimensional unit cube, introduce coordinates:

$$0 \le x_1, x_2, ..., x_{5000}, y_1, y_2, ..., y_{5000}, z_1, z_2, ..., z_{5000} \le 1.$$

Now, define 3 vertices:

Point A: $x_i = 0, \quad y_i = 1, \quad z_i = 1,$ for all i.

Point B: $x_i = 1, \quad y_i = 0, \quad z_i = 1,$ for all i.

Point C: $x_i = 1, \quad y_i = 1, \quad z_i = 0,$ for all i.

Notice that distances AB, AC, BC are precisely 100.

Now to prove minimality on 15000 , we shall need the lemma:

Lemma. If $0 \le x_1, x_2, x_3 \le 1$ then $(x_1 - x_2)^2 + (x_1 - x_3)^2 + (x_2 - x_3)^2 \le 2$.

We shall prove it a bit later, now we shall finish the solution using the lemma. Assume you have points: point A with coordinates $a_1, ..., a_N$, point B with coordinates $b_1, ..., b_N$, and point C with coordinates $c_1, ..., c_N$. Then by the lemma

$$3 \cdot 10000 = \sum_{i=1}^{N} (a_i - b_i)^2 + \sum_{i=1}^{N} (a_i - c_i)^2 + \sum_{i=1}^{N} (b_i - c_i)^2 =$$

$$= \sum_{i=1}^{N} \left((a_i - b_i)^2 + (a_i - c_i)^2 + (b_i - c_i)^2 \right) \le 2N$$

Hence $15000 \le N$. It remains to prove the lemma.

Proof of the lemma. We may assume WLOG that $x_1 \le x_2 \le x_3$. Then the expression becomes greater if x_1 is reduced, and also if x_3 is increased. Therefore WLOG we take $x_1 = 0$ and $x_3 = 1$. We get a convex function in x_2. It is maximal at one of the endpoints. At both ends, the value is 2.

4. Is it possible to find a bounded family of real numbers $a_{m,n}$ for $m,n \in \mathbb{N}$ such that $\lim\limits_{n\to\infty} a_{m,n}$ is defined for any m, $\lim\limits_{m\to\infty} a_{m,n}$ is defined for any n, but for any bijection $\sigma:\mathbb{N}\to\mathbb{N}$ the sequence $a_{k,\sigma(k)}$ diverges?

Answer. Yes.

First solution. Take $$a_{m,n} = \begin{cases} 1, & \text{if } m < n \\ (-1)^n, & \text{if } m = n \\ -1, & \text{if } m > n \end{cases}$$

Obviously, if m is fixed $a_{m,n} \underset{n\to\infty}{\to} 1$; if n is fixed $a_{m,n} \underset{m\to\infty}{\to} -1$.

Now consider the permutations. If among the pairs $(m,n) = (k,\sigma(k))$ there is an infinite amount of such pairs that $m < n$ and also an infinite amount of such pairs $m > n$ then the sequence diverges. If there is a finite amount of both types, then for all k except finitely many we get $\sigma(k) = k$, and then the sequence diverges as well.

So we need to consider only the case when one of two types (meaning $m > n$ or $m < n$) appears infinitely many times in the sequence, and another type appears finitely many times. We shall prove that one of those cases is impossible, the proof that another case is impossible is similar (just replace σ by its inverse).

Assume there is a bijection $\sigma:\mathbb{N}\to\mathbb{N}$ such that for $\sigma(k) < k$ infinitely many times, and $\sigma(k) > k$ finitely many times.

So the sequence $d_k = \sigma(k) - k$ is a sequence of integers which contains only finitely many positive numbers and infinitely many negative numbers. However, $\sum\limits_{k=1}^{N} d_k \geq 0$ for any N; indeed, by the definitions of d_k it is a sum of N distinct positive integers minus the least possible sum of N distinct positive integers. However, if M is the sum of all positive numbers of the sequence d_k and N is chosen large enough so that

among $a_1, a_2, ..., a_N$ there are more than N negative numbers, then $\sum_{k=1}^{N} d_k < 0$.

Second solution. Take $a_{m,n} = (-1)^n \frac{m}{m+n}$.

Obviously, if m is fixed $a_{m,n} \underset{n\to\infty}{\to} 0$; if n is fixed $a_{m,n} \underset{m\to\infty}{\to} (-1)^n$.

In the sequence $a_{k,\sigma(k)}$ there is an infinite amount of both positive and negative elements (odd are negative, even are positive). Therefore, if that sequence would converge, it should converge to 0.

Notice that $|a_{m,n}| = \frac{m}{m+n}$, so in that case also $|a_{k,\sigma(k)}|$ would converge to 0. However, for infinitely many values of j we get $k > \frac{\sigma(k)}{10}$. Indeed, if we would have that for less than N values, than for $k \in \{1,2,...,10N\}$ we would get that for at least $9N$ of them $\sigma(k) \le N$, so we'd get an injective function from a set of $9N$ elements to the set of N elements which is not possible.

So for infinitely many values of k we get $10 > \frac{\sigma(k)}{k}$ and hence

$$|a_{k,\sigma(k)}| = \frac{k}{k+\sigma(k)} = \frac{1}{1+\frac{\sigma(k)}{k}} \ge \frac{1}{11}.$$

So it can't converge to 0.

5. Consider $n \times n$ matrices with real entries, given $n > 1$. A matrix N will be called **nilpotent** if N^n is a zero matrix. Let $\mathbf{S}$ the linear space of all $n \times n$ matrixes which can be presented as a sum of nilpotent matrices, i. e. as $N_1 + N_2 + ... + N_k$ where all N_i are nilpotent.

(a) Find $\dim \mathbf{S}$.

(b) Find the minimal k such that any $M \in \mathbf{S}$ can be presented as $N_1 + N_2 + ... + N_k$ where all N_i are nilpotent.

Answers. (*a*) $n^2 - 1$. (*b*) 2.

Solution. (*a*) It is easy to see that nilpotent matrix has zero trace. Indeed, it each eigenvalue is zero (otherwise its eigenvector wouldn't be killed by any power of the nilpotent matrix) and the trace equals the sum of eigenvalues. Sum of zero-trace matrices is also has zero trace.

We claim that $\mathbf{S}$ is consists of all matrices with trace zero. It will follow that $\dim \mathbf{S} = n^2 - 1$.

To do that we have to represent any zero-trace matrix as a sum of nilpotent matrices. Notice that the following types of matrices are nilpotent:

- Upper triangular with zeroes on the diagonal.
- Lower triangular with zeroes on the diagonal.
- Matrices with zero trace, such that all the entries in the same row are equal to each other, for instance $\begin{pmatrix} 1 & 1 & 1 \\ -3 & -3 & -3 \\ 2 & 2 & 2 \end{pmatrix}$.

Using the last type, we may make any diagonal any entries we want under the restriction of zero trace. Adding one upper triangular matrix and one lower-triangular matrix with zeroes on diagonals, we may obtain any number on the diagonal.

(*b*) We have shown that $k = 3$ is big enough.

It is easy to see that $k = 1$ is not big enough. Indeed, the matrix $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ is invertible, so all its powers are nonzero. Also for higher n, we may add

zero columns to the right and zero rows below, and we get matrices which are not nilpotent for any n.

So, the most interesting part of the question is whether each matrix with zero trace is a sum of two nilpotent matrices. The answer is yes.

In other to prove that, we shall try to bring the matrix to the form such that all diagonal entries are 0. Moreover, we shall do it using an orthogonal matrix. In other words, we claim that for any square matrix M satisfying $\operatorname{tr} M = 0$ there is an ortonormal basis $\{b_i\}$ such that $b_i^t M b_i = 0$. We prove it by induction. Assume we have an ortonormal basis $\{b_i\}$ such that $b_i^t M b_i = 0$ for $i \le k$. Notice that $\sum_{i=1}^{n} b_i^t M b_i = 0$. So if one of the summands is non-zero, there is also another summand with the opposite sign. So, if we are not finished, there is $r, s > k$ such that $b_s^t M b_s < 0 < b_r^t M b_r$. Consider a unit vector $b = \cos\alpha \cdot b_r + \sin\alpha \cdot b_s$. The value of $b^t \cdot M \cdot b$ is positive when $\alpha = 0$ and negative when $\alpha = \frac{\pi}{2}$, so it is zero in between. The set of vectors $\{b_1, b_2, ..., b_k, b\}$ is ortonormal; it might be completed to an ortonormal basis, which completes the step of induction.

6. Is there a polynomial of two variables $p(x,y)$ with real coefficients of degree 2, such that for any integer n there exists exactly one pair of integers x, y such that $p(x,y)=n$?

Answer. No.

Solution. Assume such a polynomial exists. It is easy to show the coefficients are rational. For instance, if

$$p(x,y)=a\cdot x^2+b\cdot xy+c\cdot y^2+d\cdot x+e\cdot y+f$$

is a polynomial that receives integer values at integer points, then

$$a=\frac{1}{2}\big(p(2,0)-2\cdot p(1,0)+p(0,0)\big)$$

$$b=\frac{1}{2}\big(p(1,1)-p(1,0)-p(0,1)+p(0,0)\big)$$

$$c=\frac{1}{2}\big(p(0,2)-2\cdot p(0,1)+p(0,0)\big)$$

$$f=p(0,0)$$

And having the linear polynomial $\ell(x,y)=p(x,y)-ax^2-bxy-cy^2-f$ we easily find $d=p(1,0)-p(0,0)$ and $e=p(0,1)-p(0,0)$.

We may perform a linear change of coordinates with rational coefficients to bring the polynomial to one of the following forms:

- $A\tilde{x}^2+B\tilde{y}^2+C$ where $A\cdot B>0$ (elliptic case)
- $A\big(\tilde{x}^2-B\tilde{y}^2\big)+C$, where B is not an integer square (hyperbolic case)
- $A\cdot\tilde{x}\cdot\tilde{y}+C$ (the second hyperbolic case)
- $A\cdot\tilde{x}^2+\tilde{y}$ (generic parabolic case)
- $A\cdot\tilde{x}^2+C$ (degenerate parabolic case)
- $\tilde{x}$ (linear case)

We may multiply the polynomial by -1: if it achieves all integer values on some rational lattice, it will do that still; and assume that $A>0$.

In elliptic and in the degenerate parabolic case we won't get integer values which are too low.

We can also disregard the linear case. Indeed, if a linear polynomial accepts all integer values precisely once on some rational lattice spanned by vectors u and v then $p(X+u)=p(x)+m$ and $p(X+v)=p(X)+n$ for some integer m and n, and hence $p(X+n\cdot u+m\cdot v)=p(X)$ so in that lattice each value of p appears many times.

So we remain with the generic parabolic case and two hyperbolic cases. In all those cases we shall prove that the function is not injective, but we shall start with some general remark about lattices. After a rational change of coordinates, the lattice of integer becomes some shifted twisted lattice. However, we may consider its sub-lattice of certain simple type. If we prove that the polynomial is not injective on the sub-lattice, it will be enough. Let u,v be the vectors generating the lattice (meaning that all points of the lattice are $z+nv+mu$, where z is any fixed point of a lattice, and n,m run over all integer numbers). In our case, u,v are rational vectors, but multiplying them by some integers (common denomator of the coordinates of each vector) we may assume they are integer vectors for a certain sub-lattice. We may take a vector w_1 to be an integer linear combination of u and v, so that it will be horizontal, but nonzero. Similarly, we may take an integer linear combination w_2 which is vertical. Then w_1 and w_2 generate a sub-lattice. Also $|w_2|\cdot w_1$ and $|w_1|\cdot w_2$ generate a sub-lattice of type $N\cdot\mathbb{Z}^2$. So, each rational lattice is a has a rational translation of $N\cdot\mathbb{Z}^2$ as a sub-lattice. From now on a lattice will be replaced by that such-lattice.

Now back to the case checking:

Generic parabolic case $p(x,y)=A\cdot x^2+y$:

When we substitute for $N+1$ different (relevant) values of x with some relevant value of y, we get different integer numbers two of which are equal modulo N. So, in one of the cases we may change y by a correct multiple of N so that we get the same value of p.

Yet another general remark: we may also apply a homothety $(x,y)\mapsto(kx,ky)$ for some integer k, so the lattice will consist of integer points. Of course, it might influence the coefficients. So we can use a sub-lattice of $\mathbb{Z}^2$ so that $(x,y)=(x_0,y_0)\bmod N$.

First hyperbolic case: $p(x,y)=A\left(x^2-By^2\right)+C=0$, where B is not an integer square. The homothety might influence A and C, but not B.

We know there is a solution of Pell equation. That means there are integer x_1,y_1 so that $x_1^2-d\cdot y_1^2=1$. There is a linear transformation defined by a formula $\begin{pmatrix}x\\y\end{pmatrix}\mapsto\begin{pmatrix}x_1 & d\cdot y_1\\ y_1 & x_1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}$, which for integer x,y is the same as the formula $L: x+\sqrt{d}\cdot y\mapsto\left(x_1+\sqrt{d}\cdot y_1\right)\left(x+\sqrt{d}\cdot y\right)$. This linear transformation is invertible in integer matrices, so it gives a bijective mapping of $\mathbb{Z}^2$ to itself, and it sends the level sets of $p(x,y)$ to themselves. Therefore, it also defines a bijective mapping from $\left(\mathbb{Z}/N\right)^2$ to itself.

The group of invertible linear transformation on $\left(\mathbb{Z}/N\right)^2$ is a finite group, with M elements. So L^M defines an identity mapping from $\left(\mathbb{Z}/N\right)^2$ to itself, and L^M sends each integer point to another integer point which is the same modulo N (no point except $(0,0)$ remains in its place, since 1 is not an eigenvalue).

Now, take an integer point P within our sub-lattice. The transformation L^M takes it to a different point Q which is on the same sub-lattice. So we have two different points in the sub-lattice such that $p(\mathrm{P})=p(\mathrm{Q})$, so p is not injective.

Second hyperbolic case: $p(x,y) = A \cdot x \cdot y + C$. We need to find two pairs of integers (x,y) such that $x = x_0 \pmod N$ and $y = y_0 \pmod N$ so that p will get the same value at both points.

We shall assume that A and C are integer; if they are just rational, we shall multiply the polynomial by their common denominator; it will not help or hinder the polynomial to become injective on the sub-lattice.

We can try an arbitrary point (x,y) on the sub-lattice. If $x = 0$ is allowed, the value doesn't depend on y_0 and we see that p is not injective on the sub-lattice. But let us assume x_0 is not divisible by n and y_0 is not divisible by N as well. So, for some arbitrary point (x_1, y_1) on the sub-lattice we get $Ax_1y_1 + C = D$ where D is an integer.

Consider a large composite number E such that $E = D - C \pmod{Ax_1}$ and E is divisible by $q = NAx_1 + 1$, so q is coprime to Ax_1; it follows from Chinese remainder theorem that such E exists. Then there exists y such that $Ax_1y = E$. Since Ax_1 is coprime to q, we know that y is divisible by q. So if we define $x_2 = x_1 \cdot q$ and $y_2 = \frac{y}{q}$, we get another pair x_2, y_2 of integers which satisfies $Ax_2y_2 = E$. Notice that since $q = 1 \pmod N$, we conclude that $x_1 = x_2 \pmod N$ and $y = y_2 \pmod N$.

Therefore $x_1y = x_2y_2$ and both points (x_1, y) and (x_2, y_2) belong to the sub-lattice. Hence there are two distinct points on the sublattice with the same value of p.