

Problem Set Week 7 Solutions

ETHZ Math Olympiad Club

7 April 2025

Problem A-2 (IMC 1999)

Does there exist a bijective map $\pi: \mathbb{N}_{>0} \rightarrow \mathbb{N}_{>0}$ such that

$$\sum_{n=1}^{\infty} \frac{\pi(n)}{n^2} < \infty?$$

Solutions:

Solution 1.

No. For a very quick and clever solution, if we let π be a permutation of $\mathbb{N}_{>0}$ and let $N \in \mathbb{N}$, we shall argue that

$$\sum_{n=N+1}^{3N} \frac{\pi(n)}{n^2} > \frac{1}{9}.$$

In fact, of the $2N$ numbers $\pi[\llbracket N+1; 3N \rrbracket] = \{\pi(N+1), \dots, \pi(3N)\}$, only N can be smaller than or equal to N , so at least N of them must be strictly bigger than N . Hence,

$$\sum_{n=N+1}^{3N} \frac{\pi(n)}{n^2} \geq \frac{1}{(3N)^2} \sum_{n=N+1}^{3N} \pi(n) \geq \frac{1}{9N^2} \cdot N \cdot N = \frac{1}{9}.$$

The result follows directly because we have the infinite decomposition $\mathbb{N}_{>0} = \bigsqcup_{N \in 3\mathbb{N}} \llbracket N+1; 3N \rrbracket$.

Alternative solutions. There are two more solutions, both of which use the following fact:

Let π be a permutation of \mathbb{N}^* . Fix $N \in \mathbb{N}^*$: the set of numbers $\pi[\llbracket 1; N \rrbracket] = \{\pi(1), \dots, \pi(N)\}$ is of size N , i.e., the numbers are distinct positive integers. Thus, it is easy to prove¹ by

¹For the case $N = 1$, take $\iota_1 = \text{id}_{\llbracket 1; 1 \rrbracket}$. The condition holds vacuously as $\llbracket 1; N-1 \rrbracket = \emptyset$.

Now assume the result holds for $N \geq 1$. We prove it for $N+1$. By the inductive hypothesis, there exists a permutation $\iota_N: \llbracket 1; N \rrbracket \hookrightarrow \llbracket 1; N \rrbracket$ such that $\pi(\iota_N(i+1)) > \pi(\iota_N(i))$ for all $i \in \llbracket 1; N-1 \rrbracket$. If $\pi(N+1) > \pi(\iota_N(N))$, define $\iota_{N+1} = \iota_N \cup \{(N+1, N+1)\}$. This extends ι_N to $\llbracket 1; N+1 \rrbracket$ while preserving the order, so the result holds. Else, by injectivity, equality is impossible, so $\pi(N+1) < \pi(\iota_N(N))$, and hence we can take k to be the smallest index in $\llbracket 1; N \rrbracket$ such that $\pi(N+1) < \pi(\iota_N(k))$. Define:

$$\iota_{N+1} = \iota_N|_{\llbracket 1; k-1 \rrbracket} \cup \{(k, N+1)\} \cup \{(t+1, \iota_N(t)) \mid t \in \llbracket k; N \rrbracket\}.$$

This changes the value at k to $N+1$ and shifts the rest to take the preceding value. Clearly, ι_N is a bijection, and $\iota_{N+1}|_{\llbracket 1; k-1 \rrbracket}$ preserves the order. By choice of k , $\pi(\iota_{N+1}(k)) = \pi(N+1) < \pi(\iota_N(k)) = \pi(\iota_{N+1}(k+1))$. Now if $k > 1$, then by minimality (and again by injectivity), we have $\pi(\iota_{N+1}(k)) = \pi(N+1) > \pi(\iota_N(k-1)) = \pi(\iota_{N+1}(k-1))$. In all cases, $\iota_{N+1}|_{\llbracket 1; k+1 \rrbracket}$ preserves the order. For $N \geq i > k$, we have $\pi(\iota_{N+1}(i+1)) = \pi(\iota_N(i)) > \pi(\iota_N(i-1)) = \pi(\iota_{N+1}(i))$ by the inductive hypothesis. In total, ι_{N+1} satisfies the required ordering. This concludes the induction step and hence the induction.

induction over \mathbb{N}^* that there exists a permutation $\iota_N: \llbracket 1; N \rrbracket \hookrightarrow \llbracket 1; N \rrbracket$ such that:

$$\forall i \in \llbracket 1; N-1 \rrbracket, \quad \pi(\iota_N(i+1)) > \pi(\iota_N(i)).$$

Solution 2.

Fix $N \geq 1$. From our proposition above, it follows that there is a permutation of $\llbracket 1; N \rrbracket$ such that for all $t \in \llbracket 1; N-1 \rrbracket$, $\pi(\iota_N(t+1)) > \pi(\iota_N(t))$. In particular, since $\pi(\iota_N(1)) \geq 1$, we get trivially by induction that for all $t \in \llbracket 1; N \rrbracket$, $\pi(\iota_N(t)) \geq t$, so that:

$$\sum_{i=1}^N \pi(i) = \sum_{i=1}^N \pi(\iota_N(i)) \geq \sum_{i=1}^N i = \frac{N(N+1)}{2},$$

and this holds for all $N \in \mathbb{N}^*$. Now we perform the very useful-to-know **Abel transformation** on the finite sequences $\pi|_{\llbracket 1; N \rrbracket}$ and $\left(\frac{1}{n^2}\right)_{1 \leq n \leq N}$ to obtain:

$$\begin{aligned} \sum_{n=1}^N \frac{\pi(n)}{n^2} &= \frac{1}{N^2} \left(\sum_{n=1}^N \pi(n) \right) + \sum_{n=1}^{N-1} \left(\sum_{j=1}^n \pi(j) \right) \left(\frac{1}{n^2} - \frac{1}{(n+1)^2} \right) \\ &\geq \sum_{n=1}^{N-1} \left(\frac{n(n+1)}{2} \right) \left(\frac{1}{n^2} - \frac{1}{(n+1)^2} \right) = \sum_{n=1}^{N-1} \frac{2n+1}{2n(n+1)} \geq \sum_{n=1}^{N-1} \frac{1}{n+1} = \sum_{n=2}^N \frac{1}{n}. \end{aligned}$$

Thus,

$$\liminf_{N \rightarrow +\infty} \sum_{n=1}^N \frac{\pi(n)}{n^2} \geq \liminf_{N \rightarrow +\infty} \sum_{n=2}^N \frac{1}{n} = +\infty.$$

Solution 3.

Fix $N \geq 1$. Again, from our proposition, there is a permutation of $\llbracket 1; N \rrbracket$ such that for all $t \in \llbracket 1; N-1 \rrbracket$, $\pi(\iota_N(t+1)) > \pi(\iota_N(t))$. We are in the following situation:

$$\begin{aligned} \frac{1}{N^2} &\leq \dots \leq \frac{1}{1^2} \\ \pi(\iota_N(1)) &\leq \dots \leq \pi(\iota_N(N)) \end{aligned}$$

By the very useful-to-know **rearrangement inequality**, we obtain:

$$\sum_{n=1}^N \frac{\pi(n)}{n^2} \geq \sum_{n=1}^N \frac{\pi(\iota_N(n))}{n^2}.$$

Since $\pi(\iota_N(1)) \geq 1$, we get trivially by induction that $\pi(\iota_N(t)) \geq t$, so that:

$$\sum_{n=1}^N \frac{\pi(\iota_N(n))}{n^2} \geq \sum_{n=1}^N \frac{n}{n^2} = \sum_{n=1}^N \frac{1}{n}.$$

Thus,

$$\sum_{n=1}^N \frac{\pi(n)}{n^2} \geq \sum_{n=1}^N \frac{1}{n}.$$

In particular, as N was arbitrary, we get:

$$\liminf_{N \rightarrow +\infty} \sum_{n=1}^N \frac{\pi(n)}{n^2} \geq \liminf_{N \rightarrow +\infty} \sum_{n=2}^N \frac{1}{n} = +\infty.$$

Problem 2 (IMC 1994)

Let $f \in C^1(]a, b[, \mathbb{R})$ with $\lim_{x \rightarrow a^+} f(x) = +\infty$, $\lim_{x \rightarrow b^-} f(x) = -\infty$, and $f'(x) + f^2(x) \geq -1$ for all $x \in]a, b[$. Prove that $b - a \geq \pi$ and give an example where $b - a = \pi$.

Solution:

From the inequality, we obtain:

$$\frac{d}{dx} (\arctan(f(x)) + x) = \frac{f'(x)}{1 + f^2(x)} + 1 \geq 0$$

for all $x \in]a, b[$. Therefore, the function $\arctan(f(x)) + x$ is non-decreasing on $]a, b[$. Taking limits as x approaches the endpoints, we get:

$$\lim_{\substack{x \rightarrow a \\ >}} (\arctan(f(x)) + x) = \frac{\pi}{2} + a, \quad \lim_{\substack{x \rightarrow b \\ <}} (\arctan(f(x)) + x) = -\frac{\pi}{2} + b.$$

Hence,

$$\frac{\pi}{2} + a \leq -\frac{\pi}{2} + b,$$

which implies $b - a \geq \pi$.

Equality is achieved when:

$$f(x) = \cot(x) = \frac{\cos(x)}{\sin(x)}, \quad a = 0, \quad b = \pi,$$

since for any $x \in]0, \pi[$, we have:

$$f'(x) + f^2(x) = -\frac{1}{\sin^2(x)} + \frac{\cos^2(x)}{\sin^2(x)} = -\frac{\sin^2(x)}{\sin^2(x)} = -1,$$

and the boundary conditions are satisfied:

$$\lim_{\substack{x \rightarrow 0^+ \\ >}} \cot(x) = +\infty, \quad \lim_{\substack{x \rightarrow \pi^- \\ <}} \cot(x) = -\infty.$$

Problem B-3 (IMC 2005)

In the linear space of all real $n \times n$ matrices, find the maximum possible \mathbb{R} -dimension of an \mathbb{R} -linear subspace V such that

$$\forall X, Y \in V, \quad \text{tr}(XY) = 0.$$

(The trace of a matrix is the sum of its diagonal entries.)

Solution:

For $\{\mathbf{0}_{n \times n}\}$, we have

$$\text{tr}(\mathbf{0}_{n \times n} \cdot \mathbf{0}_{n \times n}) = \text{tr}(\mathbf{0}_{n \times n}) = 0,$$

so it is clear that an \mathbb{R} -subspace satisfying the condition exists. Denote by V such a subspace with the maximum possible \mathbb{R} -dimension (necessarily less than n^2).

Now, if A is a symmetric matrix, then:

$$\text{tr}(A^2) = \text{tr}(A^T A) = \sum_{i=0}^{n-1} (A^T A)_{ii} = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} (A^T)_{ij} A_{ji} = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} (A_{ji})^2 = \|A\|_F^2,$$

which is the sum of the squared entries of A (the Frobenius norm squared), and is strictly positive as long as $A \neq \mathbf{0}_{n \times n}$. Therefore, V cannot contain any symmetric matrix except $\mathbf{0}_{n \times n}$.

Denote by S the \mathbb{R} -linear space of all real $n \times n$ symmetric matrices; its \mathbb{R} -dimension is clearly $\frac{n(n+1)}{2}$. Since $V \cap S = \{\mathbf{0}_{n \times n}\}$, we have

$$\dim_{\mathbb{R}}(V) + \dim_{\mathbb{R}}(S) \leq n^2,$$

which gives

$$\dim_{\mathbb{R}}(V) \leq n^2 - \frac{n(n+1)}{2} = \frac{n(n-1)}{2}.$$

Thus, the maximum \mathbb{R} -dimension is bounded above by $\frac{n(n-1)}{2}$. This bound is tight: the space of strictly upper triangular matrices clearly has \mathbb{R} -dimension $\frac{n(n-1)}{2}$ and satisfies the given condition.

Therefore, the maximum \mathbb{R} -dimension of subspaces V satisfying the given condition is $\frac{n(n-1)}{2}$.

Problem 4 (Bernoulli Competition 2024)

Let $n, m \in \mathbb{N}_{>0}$ be positive integers, with $m \geq 3$, and let $A \in \mathbb{Z}^{n \times n}$. Suppose A has finite order ($\exists k \in \mathbb{N}^*$, $A^k = I_n$) and satisfies

$$A \equiv I_n \pmod{m}^2.$$

Prove that $A = I_n$, and find counterexamples when $m = 2$.

Solutions:

Solution 1.

Since $A \equiv I_n \pmod{m}$, there exists $B \in \mathbb{Z}^{n \times n}$ such that $A = I_n + mB$. Then we have the following equality of characteristic polynomials:

$$P_{\text{char},A}(X) = \det_{\mathbb{Q}(X)}(XI_n - A) = \det_{\mathbb{Q}(X)}((X - 1)I_n - mB) = P_{\text{char},mB}(X - 1).$$

Therefore, $\alpha \in \mathbb{C}$ is an eigenvalue of A if and only if $\alpha - 1$ is an eigenvalue of mB ; that is, if and only if $\frac{\alpha - 1}{m}$ is an eigenvalue of B .

Since $\exists k \in \mathbb{N}_{>0}$ with $A^k = I_n$, any eigenvalue $\alpha \in \mathbb{C}$ of A satisfies $\alpha^k = 1$; thus, they are k -th roots of unity and lie on the unit circle \mathbb{S}^1 , i.e., $|\alpha| = 1$. Any eigenvalue $\beta \in \mathbb{C}$ of B then satisfies (here $m \geq 3$ is crucial):

$$|\beta| = \left| \frac{\alpha - 1}{m} \right| \leq \frac{|\alpha| + 1}{m} = \frac{2}{m} < 1.$$

Now we prove that 0 is the only eigenvalue of B

From this point, there are multiple ways to proceed; we present two approaches here.

Intermediate step using Vieta's formula.

Since \mathbb{Z} is a unique factorisation domain (UFD), so is $\mathbb{Z}[X]$, and we can factor the characteristic polynomial of B (which is of degree $n \geq 1$), $P_{\text{char},B}(X) := \det_{\mathbb{Q}(X)}(XI_n - B) \in \mathbb{Z}[X]$, as a product of $l \in \mathbb{N}^*$ unique irreducible polynomials (up to invertible element here these are ± 1). Since $P_{\text{char},B}(X)$ is monic, the irreducible polynomials must have leading coefficients in $\mathbb{Z}^\times = \{\pm 1\}$. Therefore, they must have degree at least one and cannot be irreducible elements of $\mathbb{Z} \subset \mathbb{Z}[X]$ —namely, the primes up to sign. Hence, we may assume them to be monic (by multiplying, *ubi opus est*, by -1). That is,

$$\exists \{P_i(X) \mid \forall i \in l, P_i(X) \text{ is irreducible and monic}\} \subset \mathbb{Z}_{\text{irr}}[X] \setminus \mathbb{Z}$$

such that

$$P_{\text{char},B}(X) = \prod_{i \in l} P_i(X).$$

Now, let β be an eigenvalue of B , i.e., $\beta \in \text{Root}_{P_{\text{char},B}(X)}(\mathbb{C})$. Hence, there exists $j \in l$ such that $\beta \in \text{Root}_{P_j(X)}(\mathbb{C})$. For a certain $s_j \in \mathbb{N}_{>0}$ and distinct complex numbers $\{j\beta_i \mid i \in s_j\} \subset \mathbb{C}$, we have

$$\text{Root}_{P_j(X)}(\mathbb{C}) = \{j\beta_i \mid i \in s_j\}.$$

²For an integer $u \in \mathbb{Z}$, $\equiv \pmod{u}$ is the equivalence relation on the set of integer matrices $\bigcup_{r,l \in \mathbb{N}^*} \mathbb{Z}^{r \times l}$, where for $C, D \in \mathbb{Z}^{r \times l}$, $C \equiv D \pmod{u} \Leftrightarrow \forall (i, j) \in r \times l, u \mid (C - D)(i, j)$.

As we have seen above,

$$\text{Root}_{P_{\text{char},B}(X)}(\mathbb{C}) \subset \mathbb{D},$$

so $\{j\beta_i \mid i \in s_j\} \subset \mathbb{D}$. However, since these are the roots of $P_j(X)$, we must have, by Vieta's formula, that their product equals (up to a sign) the constant term of $P_j(X)$:

$$\prod_{i \in s_j} j\beta_i = \pm P_j(0).$$

Then

$$|P_j(0)| = \left| \prod_{i \in s_j} j\beta_i \right| = \prod_{i \in s_j} |j\beta_i| < 1.$$

Since $P_j(X) \in \mathbb{Z}[X]$, we must have $P_j(0) \in \mathbb{Z}$, and because $|P_j(0)| < 1$ we must have $P_j(0) = 0$. Therefore, 0 is a root of P_j , and thus X divides $P_j(X)$ in $\mathbb{Z}[X]$. Since $P_j(X)$ has degree at least 1 and is irreducible in $\mathbb{Z}[X]$, this cannot happen unless $P_j(X)$ has degree 1. So $P_j(X) = kX$ for a certain $k \in \mathbb{Z} \setminus \{0\}$. Since $P_j(X)$ is monic, $k = 1$, and we conclude $P_j(X) = X$. Hence $\beta = 0$, since it is a root of $P_j(X)$ by choice of j . As $\beta \in \sigma(B)$ was arbitrary we conclude $\sigma(B) = \{0\}$ as desired.

Alternative proof of intermediate step using Newton's identities.

Fix $m \in \mathbb{N}_{>0}$. For $k \in \mathbb{N}$, let the k -th power sum polynomials in m variables

$$p_k(\mathbf{X}) := \sum_{i \in m} X_i^k \in \mathbb{Z}[\mathbf{X}],$$

and the k -th elementary symmetric polynomials in m

$$e_k(\mathbf{X}) := \sum_{\substack{A \in \mathcal{P}(m) \\ |A|=k}} \prod_{a \in A} X_a \in \mathbb{Z}[\mathbf{X}]^3.$$

The **Newton's identities** relate these polynomials by the identity (valid for $m \geq k \geq 1$):

$$k e_k(\mathbf{X}) = \sum_{i=1}^k (-1)^{i-1} e_{k-i}(\mathbf{X}) p_i(\mathbf{X}).$$

For a short combinatorial proof of these identities, see the Appendix [A.1]. As shown earlier, all eigenvalues of B lie inside the unit disc: $\text{Root}_{P_{\text{char},B}(X)}(\mathbb{C}) \subset \mathbb{D}$. Let $\beta \in \mathbb{D}^n$ be the vector of eigenvalues of B , counted with multiplicity, so that $\sigma(B) = \text{Root}_{P_{\text{char},B}(X)}(\mathbb{C}) = \{\beta_i \mid i \in n\}$. In our case, where the number of variables is $n \geq 1$, we define, for all $k \geq 0$, the k -th power sum and the k -th elementary symmetric polynomial in the eigenvalues of B , respectively:

$$p_k := p_k(\beta) = \sum_{i \in n} \beta_i^k, \quad e_k := e_k(\beta) = \sum_{\substack{A \in \mathcal{P}(n) \\ |A|=k}} \prod_{a \in A} \beta_a.$$

Note that $p_k = \text{tr}(B^k)$, and $e_k = c_{n-k}(P_{\text{char},B}(X))$. Since $B \in \mathbb{Z}^{n \times n}$, we have $p_k \in \mathbb{Z}$ and $e_k \in \mathbb{Z}$.

³That is:

$$e_0(\mathbf{X}) = 1, \quad e_1(\mathbf{X}) = \sum_{i \in m} X_i, \quad e_2(\mathbf{X}) = \sum_{0 \leq i < j < m} X_i X_j, \quad \dots, \quad e_n(\mathbf{X}) = \prod_{i \in m} X_i,$$

and $e_k(\mathbf{X}) = 0$ for $k > m$.

Let $\gamma \in \sigma(B)$ be an eigenvalue of B . Since $|\gamma| < 1$, we have $\gamma^N \xrightarrow{N \rightarrow +\infty} 0$. Therefore, each term in the finite sum (comprising n summands) p_N tends to zero as $N \rightarrow +\infty$; that is,

$$p_N \xrightarrow{N \rightarrow +\infty} 0.$$

However, as mentioned earlier, for all $N \in \mathbb{N}$, $p_N \in \mathbb{Z}$, so there exists $M \geq 0$ such that for all $N \geq M$, $p_N = 0$. We now show that this condition implies, surprisingly, that $\beta = \mathbf{0}_n$. For this, we denote by $\beta^M := (\beta_i^M)_{i \in n}$ the eigenvalues of B^M , and we define, for all $k \geq 0$,

$$\tilde{p}_k := p_k(\beta^M) = \sum_{i \in n} (\beta_i^M)^k = p_{Mk}, \quad \tilde{e}_k := e_k(\beta^M) = \sum_{\substack{A \in \mathcal{P}(n) \\ |A|=k}} \prod_{a \in A} \beta_a^M.$$

Notice that $\tilde{e}_k = c_{n-k}(P_{\text{char}, B^M}(X))$. We prove by induction that for $k \geq 1$, we have $\tilde{e}_k = 0$.

- For $k = 1$, $\tilde{e}_1 = \tilde{p}_1 = p_M = 0$.
- Let $k \geq 1$ and assume that for all j with $1 \leq j \leq k-1$, we have $\tilde{e}_j = 0$. Then Newton's identities give

$$k\tilde{e}_k = (-1)^{k-1}\tilde{e}_0\tilde{p}_k = (-1)^{k-1}\tilde{p}_k = (-1)^{k-1}p_{Mk}.$$

As $Mk \geq M$, we have $p_{Mk} = 0$, so $k\tilde{e}_k = 0$, and since $k \neq 0$, it follows that $\tilde{e}_k = 0$.

This implies that the characteristic polynomial of B^M is X^n , meaning all eigenvalues of B^M are zero; that is, $\beta^M = \mathbf{0}_n$, and hence $\beta = \mathbf{0}_n$ ⁴.

This concludes the two different approaches to show that $\sigma(B) = \{0\}$. We can now quickly finish the problem. All the eigenvalues of B are 0; this is clearly equivalent to $P_{\text{char}, B}(X) = X^n$. According to the Cayley-Hamilton theorem, $B^n = \mathbf{0}_{n \times n}$, so B is nilpotent and thus mB is nilpotent. Now, use the following

Lemma. *Let K be a field of characteristic $\text{char}(K) = 0$, $l \in \mathbb{N}_{>0}$, and $N \in K^{l \times l}$ be a nilpotent matrix. If $I_l + N$ has finite order, then $N = \mathbf{0}_{l \times l}$.*

The proof can be found in Appendix [A.2].

Apply this result to the field \mathbb{Q} with $n \geq 1$; since $mB \in \mathbb{Q}^{n \times n}$ is nilpotent and $A = I_n + mB$ has finite order, we conclude that $mB = \mathbf{0}_{n \times n}$, and so $B = \mathbf{0}_{n \times n}$ (as $m \in \mathbb{Q}^\times$). Hence, $A = I_n$, and this concludes the proof.

⁴In fact, we have just proved a curious result: if we have $\lambda \in \mathbb{C}^n$ such that there exists some $M \in \mathbb{N}$ for which, for all $N \geq M$, we have $p_N(\lambda) = 0$, then it follows that $\lambda = \mathbf{0}_n$. Indeed, one may either take the **companion matrix** of the monic polynomial $\prod_{i \in n} (X - \lambda_i)$ —that is, the matrix whose characteristic polynomial is this one—and proceed as we have just done, or, without speaking of matrices at all, define for all $k \geq 0$ the elements $\hat{e}_k := e_k(\lambda^M)$, and prove by induction, as above, that each of them (starting from 1) is zero. Then perform a descending induction: $0 = \hat{e}_n = \prod_{i \in n} \lambda_i^M$, hence there is an $i_0 \in n$ with $\lambda_{i_0} = 0$. Now remove λ_{i_0} from the set $\{\lambda_i \mid i \in n\}$, obtaining a smaller set of size n' . If it is empty ($n' = 0$) then $\lambda = \mathbf{0}_n$, else we consider the vector $\lambda' \in \mathbb{C}^{n'}$ consisting of the remaining elements. Again, it is clear that for all $N \geq M$, each $p_N(\lambda') = 0$ (where the N -th power sum polynomials are in n' variables); their k -th elementary symmetric sums in $(\lambda')^M$ must again vanish (starting from $k = 1$ and applying the same induction), so $e_{n'}((\lambda')^M) = 0$ and there is $i_1 \in n$ such that $\lambda_{i_1} \in \{\lambda_i \mid i \in n\} \setminus \{\lambda_{i_0}\}$ is 0. Continue this process until the entire set is exhausted. The advantage of the latter procedure is that we can, in fact, apply it to any integral ring R of characteristic 0, since it then canonically contains $\mathbb{Z} \hookrightarrow R$, and thus the Newton identities hold on R .

Solution 2.

Assume for contradiction that $A \neq I_n$. Since $m \geq 3$, m must be divisible by some prime power greater than 2, that is, there exists $p \in \mathbb{P}$ a prime number and $c \geq 1$ such that $p^c \mid m$ and $p^c > 2$ (if $p = 2$, then $c \geq 2$ necessarily). In particular, from $A \equiv I_n \pmod{m}$, we must have $A \equiv I_n \pmod{p^c}$.

Since $A \neq I_n$, there is $(i, j) \in n \times n$ such that $(A - I_n)(i, j) \neq 0$, and so

$$c \leq v_p((A - I_n)(i, j)) \neq +\infty,$$

where $v_p: \mathbb{Q} \rightarrow \mathbb{Z} \cup \{+\infty\}$ denotes the p -adic valuation. We can thus let

$$c' := \min \{v_p((A - I_n)(i, j)) \mid (i, j) \in n \times n\} \geq c.$$

Then $c' \in \mathbb{N}_{\geq c}$ is (by construction) the largest integer such that $A \equiv I_n \pmod{p^{c'}}$. Consequently, we define

$$B := \frac{1}{p^{c'}}(A - I_n),$$

for which (by definition of c'), $B \in \mathbb{Z}^{n \times n}$ and $B \not\equiv \mathbf{0}_{n \times n} \pmod{p}$.

Since A has finite order, there exists $k \in \mathbb{N}^*$ with $A^k = I_n$; furthermore, $k \geq 2$ because $A \neq I_n$. We want to expand:

$$I_n = A^k = (I_n + p^{c'}B)^k.$$

This can be done (happily) by the binomial theorem since I_n and $p^{c'}B$ commute, and we obtain:

$$I_n = \sum_{i=0}^k \binom{k}{i} p^{ic'} B^i.$$

This implies:

$$\sum_{i=1}^k \binom{k}{i} p^{ic'} B^i = \mathbf{0}_{n \times n},$$

or equivalently (since $k \geq 2$), we obtain the equation:

$$\sum_{i=2}^k \binom{k}{i} p^{ic'} B^i = -kp^{c'}B.$$

We shall show that this leads to a contradiction. Let $c'' := v_p(k) \geq 0$. We prove:

$$-kp^{c'}B \not\equiv \mathbf{0}_{n \times n} \pmod{p^{c'+c''+1}}, \quad (1)$$

whilst

$$\sum_{i=2}^k \binom{k}{i} p^{ic'} B^i \equiv \mathbf{0}_{n \times n} \pmod{p^{c'+c''+1}}, \quad (2)$$

which is impossible by the derived equation above.

For (1): because $v_p(kp^{c'}) = c' + c''$ and $B \not\equiv \mathbf{0}_{n \times n} \pmod{p}$, we have $-kp^{c'}B \not\equiv \mathbf{0}_{n \times n} \pmod{p^{c'+c''+1}}$ (but obviously $kp^{c'}B \equiv \mathbf{0}_{n \times n} \pmod{p^{c'+c''}}$).

For (2): let $2 \leq i \leq k$, note that $i! \binom{k}{i} = \frac{k!}{(k-i)!}$ is divisible by k , hence by $p^{c''}$, whilst the largest power of p dividing $i!$ is classically bounded above by the famous **Legendre's formula**:

$$v_p(i!) = {}^5 \sum_{j=1}^{+\infty} \left\lfloor \frac{i}{p^j} \right\rfloor < \sum_{j=1}^{+\infty} \frac{i}{p^j} = \frac{i}{p-1}.$$

We claim that $v_p(i!) \leq \left\lfloor \frac{i-1}{p-1} \right\rfloor$. Assume for the sake of contradiction that $\left\lfloor \frac{i-1}{p-1} \right\rfloor < v_p(i!)$. Since both are integers, $\left\lfloor \frac{i-1}{p-1} \right\rfloor + 1 \leq v_p(i!)$. As $v_p(i!) < \frac{i}{p-1}$ and $i \geq 2 \Rightarrow \left\lfloor \frac{i-1}{p-1} \right\rfloor + 1 \geq 1$, we obtain:

$$\left\lfloor \frac{i-1}{p-1} \right\rfloor + 1 < \frac{i}{p-1} \Rightarrow (p-1) \left(\left\lfloor \frac{i-1}{p-1} \right\rfloor + 1 \right) < i.$$

Again, since $i, (p-1) \left(\left\lfloor \frac{i-1}{p-1} \right\rfloor + 1 \right)$ are integers, we have:

$$(p-1) \left(\left\lfloor \frac{i-1}{p-1} \right\rfloor + 1 \right) + 1 \leq i.$$

However, by definition of the floor function:

$$\frac{i-1}{p-1} < \left\lfloor \frac{i-1}{p-1} \right\rfloor + 1 \Rightarrow i < (p-1) \left(\left\lfloor \frac{i-1}{p-1} \right\rfloor + 1 \right) + 1.$$

Combining:

$$i < (p-1) \left(\left\lfloor \frac{i-1}{p-1} \right\rfloor + 1 \right) + 1 \leq i,$$

that is, $i < i$, a contradiction. Thus, $v_p(i!) \leq \left\lfloor \frac{i-1}{p-1} \right\rfloor$. So:

$$v_p \left(\binom{k}{i} p^{ic'} \right) = v_p \left(\frac{i! \binom{k}{i}}{i!} p^{ic'} \right) = v_p(p^{ic'}) + v_p \left(i! \binom{k}{i} \right) - v_p(i!) \geq ic' + c'' - \left\lfloor \frac{i-1}{p-1} \right\rfloor.$$

If $p = 2$, then $c' \geq c \geq 2$ and $\frac{i-1}{p-1} = i-1$, so:

$$\begin{aligned} ic' + c'' - \left\lfloor \frac{i-1}{p-1} \right\rfloor &= i(c'-1) + c'' + 1 \\ &\geq 2(c'-1) + c'' + 1 = c' + c'' + (c'-2) + 1 \geq c' + c'' + 1. \end{aligned}$$

If $p \geq 3$, then $\frac{i-1}{p-1} \leq \frac{i-1}{2}$, so that $\left\lfloor \frac{i-1}{p-1} \right\rfloor \leq \left\lfloor \frac{i-1}{2} \right\rfloor$, and thus:

$$\begin{aligned} ic' + c'' - \left\lfloor \frac{i-1}{p-1} \right\rfloor &\geq ic' + c'' - \left\lfloor \frac{i-1}{2} \right\rfloor \\ &= c' + c'' + (i-1)c' - \left\lfloor \frac{i-1}{2} \right\rfloor \geq c' + c'' + (i-1) - \left\lfloor \frac{i-1}{2} \right\rfloor \end{aligned}$$

⁵A quick proof of this formula for $p \in \mathbb{P}$ and $i \geq 1$ proceeds as follows: define $M := \max \{v_p(t) \mid 1 \leq t \leq i\}$, then: $v_p(i!) = \sum_{t=1}^i v_p(t) = \sum_{t=1}^i \left(\sum_{\substack{j=1 \\ p^j |_Z t}}^M 1 \right) = \sum_{(t,j) \in \llbracket 1, i \rrbracket \times \llbracket 1, M \rrbracket} 1 = \sum_{j=1}^M \left(\sum_{\substack{t=1 \\ p^j |_Z t}}^i 1 \right) = \sum_{j=1}^M |\{t \in \llbracket 1, i \rrbracket \mid p^j |_Z t\}| = \sum_{j=1}^M |\{p^j s \leq i \mid s \in \mathbb{N}_{>0}\}| = \sum_{j=1}^M |\{s \in \mathbb{N}_{>0} \mid p^j s \leq i\}| = \sum_{j=1}^M \left\lfloor \frac{i}{p^j} \right\rfloor = \sum_{j=1}^{+\infty} \left\lfloor \frac{i}{p^j} \right\rfloor$. Here, we use the total multiplicativity of v_p for the first equality; the interchange of sums is justified by their finiteness. The final equality follows from the definition of M , since if $j \in \mathbb{N}$ is such that $j > M$, then $j > v_p(i)$, hence $\frac{i}{p^j} < 1$, and thus $\left\lfloor \frac{i}{p^j} \right\rfloor = 0$. The remaining equalities follow from elementary counting.

$$= c' + c'' + \left\lceil \frac{i-1}{2} \right\rceil \geq c' + c'' + 1,$$

where we used the fact that for an integer $r \in \mathbb{Z}$, we have $r - \lfloor \frac{r}{2} \rfloor = \lceil \frac{r}{2} \rceil$ (for this equality, break r into two cases based on its parity: $2t$ or $2t+1$) and that $i-1 > 0$.

In all cases for p :

$$v_p \left(\binom{k}{i} p^{ic'} \right) \geq c' + c'' + 1,$$

and so $p^{c'+c''+1}$ divides $\binom{k}{i} p^{ic'}$. As $2 \leq i \leq k$ was arbitrary, we get that:

$$\sum_{i=2}^k \binom{k}{i} p^{ic'} B^i \equiv \mathbf{0}_{n \times n} \pmod{p^{c'+c''+1}}.$$

This shows our desired contradiction. Thus, our initial assumption must be false and $A = I_n$. This concludes the proof.

Counterexamples for general $n \geq 1$ is easy to find for example $-I_n$. If we want to find one that is not a diagonal matrix, we split the case between even and odd dimension. When $n = 2k > 0$ we place k copies of a 2×2 counterexamples block (which satisfies the condition) along the diagonal, when $n = 2k+1 > 0$ we place k copies of the same 2×2 block and a final ± 1 on the diagonal

$$\begin{pmatrix} 1 & 2 & 0 & \cdots & 0 & 0 & 0 \\ 0 & -1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & \cdots & 0 & 0 \\ 0 & 0 & 0 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 2 \\ & & & & & 0 & -1 \end{pmatrix} \in \mathbb{Z}^{2k \times 2k},$$

$$\begin{pmatrix} 1 & 2 & 0 & \cdots & 0 & 0 & 0 \\ 0 & -1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & \cdots & 0 & 0 \\ 0 & 0 & 0 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 2 \\ 0 & 0 & 0 & 0 & \cdots & 0 & -1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & \pm 1 \end{pmatrix} \in \mathbb{Z}^{(2k+1) \times (2k+1)}.$$

A

A.1

Theorem 1 (Newton's Identities). *For positive integers $m \geq k \geq 1$, the following identity holds over the ring $\mathbb{Z}[X_0, \dots, X_{m-1}] = \mathbb{Z}[\mathbf{X}]$:*

$$k \left(\sum_{\substack{A \in \mathcal{P}(m) \\ |A|=k}} \prod_{a \in A} X_a \right) - \sum_{i=1}^k (-1)^{i-1} \left(\sum_{\substack{A \in \mathcal{P}(m) \\ |A|=k-i}} \prod_{a \in A} X_a \right) \left(\sum_{j \in m} X_j^i \right) = 0.$$

The following short combinatorial proof is due to Doron Zeilberger (1983).

Proof. Alternatively, the identity can be rewritten as:

$$\begin{aligned} 0 &= k \left(\sum_{\substack{A \in \mathcal{P}(m) \\ |A|=k}} \prod_{a \in A} X_a \right) + \sum_{i=1}^k (-1)^i \left(\sum_{\substack{A \in \mathcal{P}(m) \\ |A|=k-i}} \prod_{a \in A} X_a \right) \left(\sum_{j \in m} X_j^i \right) \\ &= \left(\sum_{\substack{A \in \mathcal{P}(m) \\ |A|=k}} \sum_{j \in A} (-1)^0 \left(\prod_{a \in A} X_a \right) X_j^0 \right) + \left(\sum_{i=1}^k \sum_{\substack{A \in \mathcal{P}(m) \\ |A|=k-i}} \sum_{j \in m} (-1)^i \left(\prod_{a \in A} X_a \right) X_j^i \right). \quad (*) \end{aligned}$$

We establish the identity by defining a sign-reversing involution on a combinatorial structure.

Define the set of 3-tuples:

$$\mathcal{A}(n, k) := \left\{ \langle A, i, j \rangle \mid \begin{array}{l} A \in \mathcal{P}(m), |A| \leq k, j \in m, i = k - |A|, \\ \text{and if } i = 0 \text{ then } j \in A \end{array} \right\}.$$

The *weight* of $\langle A, j, i \rangle$ is defined as:

$$w(\langle A, j, i \rangle) := (-1)^i \left(\prod_{a \in A} X_a \right) X_j^i \in \mathbb{Z}[\mathbf{X}].$$

The sum of the weights of all elements in $\mathcal{A}(n, k)$ is readily seen to be equal to (*). To show this sum is zero, define the function $T : \mathcal{A}(n, k) \rightarrow \mathcal{A}(n, k)$ as:

$$T(\langle A, j, i \rangle) = \begin{cases} \langle A \setminus \{j\}, j, i+1 \rangle, & \text{if } j \in A, \\ \langle A \cup \{j\}, j, i-1 \rangle, & \text{if } j \notin A. \end{cases}$$

With a mental exercise, we see that T is well defined and satisfies:

- $w(T(\langle A, j, i \rangle)) = -w(\langle A, j, i \rangle)$,
- $T \circ T = \text{id}_{\mathcal{A}(n, k)}$.

Thus, every element $\langle A, j, i \rangle$ uniquely pairs with its image under T (since it is an involution), and their weights cancel. Hence, the total sum is zero. \square

A.2

Lemma. *Let $l \in \mathbb{N}_{>0}$ and R be a commutative unital ring together with the canonical morphism $\text{can}_R : \mathbb{Z} \rightarrow R$. Let $N \in R^{l \times l}$ be a nilpotent matrix. If $I_l + N$ has finite order $r \in \mathbb{Z}_{>0}$ (where I_l is the identity matrix in $R^{l \times l}$) such that $\text{can}_R(r) \stackrel{\text{not.}}{=} r_R \in R^\times$ is invertible, then $N = \mathbf{0}_{R^{l \times l}}$.*

Proof. Let $r := \text{ord}_{R^{l \times l}}(I_l + N) \in \mathbb{Z}_{>0}$ be the order of $I_l + N$. Then, by the binomial theorem (noting that I_l and N commute),

$$I_l = (I_l + N)^r = \sum_{j=0}^r \binom{r}{j}_R N^j = I_l + \sum_{j=1}^r \binom{r}{j}_R N^j,$$

where the binomial coefficient is interpreted through the canonical morphism $\text{can}_R : \mathbb{Z} \rightarrow R$. It follows that

$$\mathbf{0}_{R^{l \times l}} = \sum_{j=1}^r \binom{r}{j}_R N^j,$$

and because R is commutative, we can factor N to obtain:

$$\mathbf{0}_{R^{l \times l}} = N \left(\sum_{j=1}^r \binom{r}{j}_R N^{j-1} \right) = N \left(r_R I_l + \sum_{j=2}^r \binom{r}{j}_R N^{j-1} \right).$$

Let $S := r_R I_l + \sum_{j=2}^r \binom{r}{j}_R N^{j-1} \in R^{l \times l}$ be the right-hand factor in this product, and define $E := \sum_{j=2}^r \binom{r}{j}_R N^{j-1} \in R^{l \times l}$ (the sum is possibly empty if $r = 1$, in which case it is the empty sum and $E = \mathbf{0}_{l \times l}$). So $S = r_R I_l + E$, and we claim that S is invertible.

Indeed, N is nilpotent, and so are all of its powers. Since R is commutative, any scalar multiple λN^k with $\lambda \in R$ and $k \in \mathbb{N}_{>0}$ is nilpotent. Moreover, for any (possibly non-commutative) unital ring A (here $R^{l \times l}$), the set of nilpotent elements $\text{Nil}(A)$ is closed⁶ under finite sums and products, provided that the terms commute pairwise. Because R is commutative, we get that for any $\lambda, \lambda' \in R$ and $k, k' \in \mathbb{N}_{>0}$, the elements λN^k and $\lambda' N^{k'}$ commute. Hence $E \in \text{Nil}(R^{l \times l})$.

Now $r_R \in R^\times$, so we must have $r_R I_l \in (R^{l \times l})^\times$. As E is nilpotent and E commutes with $r_R I_l$ (since R is commutative), the element $S := r_R I_l + E$, being the sum of an invertible element of $R^{l \times l}$ and a nilpotent one, must be invertible⁷.

Thus, multiplying by S^{-1} on both sides of the equation $\mathbf{0}_{R^{l \times l}} = NS$ yields $N = \mathbf{0}_{R^{l \times l}}$. \square

⁶For the finite product, the index of nilpotency is bounded above by the minimum of the respective indices of nilpotency (use the commutativity of the factors). For the finite sum, the index of nilpotency is bounded above by 1 plus the sum of the nilpotency indices minus the number of summands. To see this, use the multinomial theorem (which is valid since the summands commute) and use the pigeon hole principle.

⁷This is a general fact about any (possibly non-commutative) unital ring A : if $a \in A^\times$, $b \in \text{Nil}(A)$, and $ab = ba$, then $a + b \in A^\times$. Indeed, let $v \in \mathbb{N}_{>0}$ be the index of nilpotency of b . Then, since a and b commute, so do a^{-1} and b , and we have $(ba^{-1})^v = b^v a^{-v} = 0_A$. A simple computation (using the fact that $\pm 1_A$ commutes with every element, and that a , b , and a^{-1} commute with one another, as do their powers) shows that the element

$$a^{-1} \left(\sum_{k=0}^{v-1} (-1_A)^k (ba^{-1})^k \right) \in A,$$

is both a left and right inverse of $a + b = a(1_A + a^{-1}b) = (1_A + ba^{-1})a$, and so $a + b \in A^\times$