# On the principal minors of the powers of a matrix

Darij Grinberg*

April 7, 2026

**Abstract.** We show that if $A$ is an $n \times n$-matrix, then the diagonal entries of each power $A^m$ are uniquely determined by the principal minors of $A$, and can be written as universal (integral) polynomials in the latter. Furthermore, if the latter all equal 1, then so do the former. These results are inspired by Problem B5 on the Putnam contest 2021, and shed a new light on the behavior of minors under matrix multiplication.

**Keywords:** principal minors, determinantal identities, determinants, matrices, determinantal ideals, Putnam contest.

**MSC2020 classes:** 11C20, 14M12, 15A15.

## 1. Introduction

Let $R$ be a commutative ring. Let $A$ be an $n \times n$-matrix over $R$, where $n$ is a nonnegative integer.

A *principal submatrix* of $A$ means a matrix obtained from $A$ by removing some rows and the corresponding columns (i.e., removing the $i_1$-th, $i_2$-th, ..., $i_k$-th rows and the $i_1$-th, $i_2$-th, ..., $i_k$-th columns for some choice of $k$ integers $i_1, i_2, \ldots, i_k$ satisfying $1 \leq i_1 < i_2 < \cdots < i_k \leq n$). In particular, $A$ itself is a principal submatrix of $A$ (obtained for $k = 0$).

A *principal minor* of $A$ means the determinant of a principal submatrix of $A$. In particular, each diagonal entry of $A$ is a principal minor of $A$ (being the determinant of a principal submatrix of size $1 \times 1$). In total, $A$ has $2^n$ principal minors, including its own determinant $\det A$ as well as the trivial principal minor 1 (obtained as the determinant of a $0 \times 0$ matrix, which is what remains when all rows and columns are removed).

Problem B5 on the Putnam contest 2021 asked for a proof of the following:

*Drexel University, Korman Center, 15 S 33rd Street, Philadelphia PA, 19104, USA

**Theorem 1.1.** Assume that $R = \mathbb{Z}$. Assume that each principal minor of $A$ is odd. Then, each principal minor of $A^m$ is odd whenever $m$ is a nonnegative integer.

Without giving the solution away, it shall be noticed that essentially only one proof is known (see [1] or [3] for it), and it is not as algebraic as the statement of Theorem 1.1 might suggest. In particular, it is unclear if the theorem remains valid if "odd" is replaced by "congruent to 1 modulo 4", or if $R$ is replaced by another ring; the official solution (most of which originates in a result by Dobrinskaya [2, Lemma 3.3]) certainly does not apply to such extensions. An approach that is definitely doomed is to try expressing the principal minors of a power $A^m$ in terms of those of $A$. The following example shows that the latter do not uniquely determine the former:

**Example 1.2.** Set

$$C := \begin{pmatrix} a & b & 1 & 1 \\ c & d & 1 & 1 \\ 1 & 1 & p & q \\ 1 & 1 & r & s \end{pmatrix} \qquad \text{and} \qquad D := \begin{pmatrix} a & b & 1 & 1 \\ c & d & 1 & 1 \\ 1 & 1 & p & r \\ 1 & 1 & q & s \end{pmatrix}$$

for some $a, b, c, d, p, q, r, s \in R$. Then, the matrices $C$ and $D$ have the same principal minors, but their squares $C^2$ and $D^2$ differ in their $\{2, 3\}$-principal minor (i.e., their principal minor obtained by removing the 1-st and 4-th rows and columns) unless $(q - r)(b - c) = 0$. Thus, the principal minors of the square of a matrix are not uniquely determined by the principal minors of the matrix itself.

This example is inspired by [4, Example 3], where further related discussion of matrices with equal principal minors can be found.

## 2. Nevertheless...

However, not all is lost. Among the principal minors of $A^m$, the simplest ones (besides 1) are those of size $1 \times 1$, that is, the diagonal entries of $A^m$. It turns out that these diagonal entries are indeed uniquely determined by the principal minors of $A$, and even better, they can be written as universal polynomials[1] in the latter. That is, we have the following:[2]

**Theorem 2.1.** Let $n$ and $m$ be nonnegative integers, and let $i \in \{1, 2, \ldots, n\}$. Then, there exists an integer polynomial $P_{n,i,m}$ in $2^n$ indeterminates that is independent of $R$ and $A$, and that has the following property: If $A$ is any $n \times n$-matrix over

[1] A "universal polynomial" means a polynomial with integer coefficients that depends neither on $A$ nor on $R$ (but can depend on $m$ as well as on the location of the diagonal entry).

[2] An *integer polynomial* means a polynomial with integer coefficients.

any commutative ring $R$, then the $i$-th diagonal entry of $A^m$ can be obtained by substituting the principal minors of $A$ into $P_{n,i,m}$. In particular, the principal minors of $A$ uniquely determine this entry.

Let us verify this for $m = 2$: If we denote the $(i, j)$-th entry of a matrix $B$ by $B_{i,j}$, then each diagonal entry of $A^2$ has the form

$$\left(A^2\right)_{i,i} = \sum_{j=1}^{n} A_{i,j}A_{j,i} = A_{i,i}^2 + \sum_{j \neq i} \underbrace{A_{i,j}A_{j,i}}_{=A_{i,i}A_{j,j} - \det \begin{pmatrix} A_{i,i} & A_{i,j} \\ A_{j,i} & A_{j,j} \end{pmatrix}}$$
$$= A_{i,i}^2 + \sum_{j \neq i} \left( A_{i,i}A_{j,j} - \det \begin{pmatrix} A_{i,i} & A_{i,j} \\ A_{j,i} & A_{j,j} \end{pmatrix} \right),$$

which is visibly an integer polynomial in the principal minors of $A$ (since all the $A_{i,i}$ and $A_{j,j}$ and $\det \begin{pmatrix} A_{i,i} & A_{i,j} \\ A_{j,i} & A_{j,j} \end{pmatrix}$ are principal minors of $A$). This verifies Theorem 2.1 for $m = 2$. Such explicit computations remain technically possible for higher values of $m$, but become longer and more cumbersome as $m$ increases.

The goal of this note is to prove Theorem 2.1. We will first show the following theorem, which looks weaker but is essentially equivalent:

**Theorem 2.2.** Let $n$ and $m$ be nonnegative integers. Let $R$ be a commutative ring. Let $A$ be an $n \times n$-matrix over $R$. Let $\mathcal{P}$ be the subring of $R$ generated by all principal minors of $A$. Then, all diagonal entries of $A^m$ belong to $\mathcal{P}$.

Before we prove this, let us explain how Theorem 2.1 can be easily derived from Theorem 2.2:

*Proof of Theorem 2.1 using Theorem 2.2.* The notation $B_{i,j}$ shall denote the $(i, j)$-th entry of any matrix $B$.

Let $\mathbf{R}$ be the polynomial ring $\mathbb{Z}\left[x_{i,j} \mid 1 \leq i \leq n \text{ and } 1 \leq j \leq n\right]$ in $n^2$ independent indeterminates $x_{i,j}$ over $\mathbb{Z}$. (For instance, if $n = 2$, then $\mathbf{R} = \mathbb{Z}\left[x_{1,1}, x_{1,2}, x_{2,1}, x_{2,2}\right]$.) Let $\mathbf{A}$ be the $n \times n$-matrix over $\mathbf{R}$ whose $(i, j)$-th entry is $x_{i,j}$ for each $(i, j) \in \{1, 2, \ldots, n\}^2$. This matrix $\mathbf{A}$ is known as "the general $n \times n$-matrix", since any matrix $A$ over any commutative ring can be obtained from it by substituting appropriate elements (viz., the entries of $A$) for the variables $x_{i,j}$. This very property will be crucial to the argument that follows.

Let $\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_{2^n}$ be the $2^n$ principal minors of $\mathbf{A}$ (numbered in some order). Let $\mathcal{P}$ denote the subring of $\mathbf{R}$ generated by all these principal minors of $\mathbf{A}$. Theorem 2.2 (applied to $\mathbf{R}$ and $\mathbf{A}$ instead of $R$ and $A$) shows that all diagonal entries of $\mathbf{A}^m$ belong to $\mathcal{P}$. In other words, for each $i \in \{1, 2, \ldots, n\}$, we have $\left(\mathbf{A}^m\right)_{i,i} \in \mathcal{P}$.

Fix $i \in \{1, 2, \ldots, n\}$. As we just showed, we have $(\mathbf{A}^m)_{i,i} \in \mathcal{P}$. In other words, there exists an integer polynomial $P_{n,i,m}$ in $2^n$ indeterminates such that $(\mathbf{A}^m)_{i,i} = P_{n,i,m}(\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_{2^n})$ (since $\mathcal{P}$ is the subring of $\mathbf{R}$ generated by $\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_{2^n}$). Consider this polynomial $P_{n,i,m}$; note that it is independent of $R$ and $A$ (by its very construction).

Now, consider a commutative ring $R$ and an $n \times n$-matrix $A$ over $R$. Let $p_1, p_2, \ldots, p_{2^n}$ be the $2^n$ principal minors of $A$ (numbered in the same order as $\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_{2^n}$). Let $f : \mathbf{R} \to R$ be the $\mathbb{Z}$-algebra homomorphism that sends each indeterminate $x_{i,j}$ to the $(i,j)$-th entry $A_{i,j}$ of $A$. This homomorphism $f$ therefore sends each entry of the matrix $\mathbf{A}$ to the corresponding entry of $A$, and thus also sends each principal minor of $\mathbf{A}$ to the corresponding principal minor of $A$ (since a principal minor is a certain signed sum of products of entries of the matrix). In other words,

$$f(\mathbf{p}_j) = p_j \qquad \text{for each } j \in \{1, 2, \ldots, 2^n\}. \tag{1}$$

However, $P_{n,i,m}$ is an integer polynomial, and thus "commutes" with any $\mathbb{Z}$-algebra homomorphism – i.e., if $a_1, a_2, \ldots, a_{2^n}$ are any $2^n$ elements of a commutative ring, and if $g$ is any $\mathbb{Z}$-algebra homomorphism out of that ring, then

$$g(P_{n,i,m}(a_1, a_2, \ldots, a_{2^n})) = P_{n,i,m}(g(a_1), g(a_2), \ldots, g(a_{2^n})).$$

Applying this to $a_i = \mathbf{p}_i$ and $g = f$, we obtain

$$\begin{aligned} f(P_{n,i,m}(\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_{2^n})) &= P_{n,i,m}(f(\mathbf{p}_1), f(\mathbf{p}_2), \ldots, f(\mathbf{p}_{2^n})) \\ &= P_{n,i,m}(p_1, p_2, \ldots, p_{2^n}) \qquad (\text{by (1)}). \end{aligned}$$

In view of $(\mathbf{A}^m)_{i,i} = P_{n,i,m}(\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_{2^n})$, we can rewrite this as

$$f\left((\mathbf{A}^m)_{i,i}\right) = P_{n,i,m}(p_1, p_2, \ldots, p_{2^n}). \tag{2}$$

However, the $\mathbb{Z}$-algebra homomorphism $f$ sends each entry of the matrix $\mathbf{A}$ to the corresponding entry of $A$, and therefore also sends each entry of the matrix $\mathbf{A}^m$ to the corresponding entry of $A^m$ (since the entries of $\mathbf{A}^m$ are certain sums of products of entries of $\mathbf{A}$, whereas the entries of $A^m$ are the same sums of products of entries of $A$). In other words, $f\left((\mathbf{A}^m)_{u,v}\right) = (A^m)_{u,v}$ for any $u, v \in \{1, 2, \ldots, n\}$. Thus, in particular, $f\left((\mathbf{A}^m)_{i,i}\right) = (A^m)_{i,i}$. Comparing this with (2), we obtain $(A^m)_{i,i} = P_{n,i,m}(p_1, p_2, \ldots, p_{2^n})$. In other words, the $i$-th diagonal entry of $A^m$ can be obtained by substituting the principal minors of $A$ into $P_{n,i,m}$ (since $p_1, p_2, \ldots, p_{2^n}$ are these principal minors of $A$). This proves Theorem 2.1. □

# 3. Notations

In order to prove Theorem 2.2, we will need some more notations regarding matrices and their minors:

- If $m \in \mathbb{Z}$, then $[m]$ shall denote the set $\{1, 2, \ldots, m\}$.
- If $B$ is a $u \times v$-matrix and if $i \in [u]$ and $j \in [v]$, then $B_{i,j}$ shall denote the $(i, j)$-th entry of $B$.
- If $u$ and $v$ are two nonnegative integers, and if $a_{i,j}$ is an element of a ring for each $i \in [u]$ and $j \in [v]$, then the notation $\left(a_{i,j}\right)_{1 \leq i \leq u,\ 1 \leq j \leq v}$ means the $u \times v$-matrix whose $(i, j)$-th entry is $a_{i,j}$ for all $i \in [u]$ and $j \in [v]$.
- If $B$ is a $u \times v$-matrix, and if $\left(i_1, i_2, \ldots, i_p\right) \in [u]^p$ and $\left(j_1, j_2, \ldots, j_q\right) \in [v]^q$ are two sequences of integers, then $\operatorname{sub}_{i_1, i_2, \ldots, i_p}^{j_1, j_2, \ldots, j_q} B$ shall denote the $p \times q$-matrix $\left(B_{i_x, j_y}\right)_{1 \leq x \leq p,\ 1 \leq y \leq q}$. If $i_1 < i_2 < \cdots < i_p$ and $j_1 < j_2 < \cdots < j_q$, then this matrix is a submatrix of $B$.
- If $B$ is a $u \times v$-matrix, and if $I$ is a subset of $[u]$, and if $J$ is a subset of $[v]$, then $\operatorname{sub}_I^J B$ shall denote the submatrix $\operatorname{sub}_{i_1, i_2, \ldots, i_p}^{j_1, j_2, \ldots, j_q} B$ of $B$, where $i_1, i_2, \ldots, i_p$ are the elements of $I$ in increasing order, and where $j_1, j_2, \ldots, j_q$ are the elements of $J$ in increasing order.

  Thus, in particular, if $B$ is an $n \times n$-matrix, and if $I$ is a subset of $[n]$, then $\operatorname{sub}_I^I B$ is a principal submatrix of $B$, so that $\det\left(\operatorname{sub}_I^I B\right)$ is a principal minor of $B$.
- If $B$ is an $n \times n$-matrix, and if $i, j \in [n]$, then $B_{\sim i, \sim j}$ shall denote the submatrix of $B$ obtained by removing the $i$-th row and the $j$-th column from $B$. In other words, $B_{\sim i, \sim j}$ denotes the matrix $\operatorname{sub}_{[n] \setminus \{i\}}^{[n] \setminus \{j\}} B$.
- If $B$ is an $n \times n$-matrix, then $\operatorname{adj} B$ shall mean the *adjugate matrix* of $B$. This is defined as the $n \times n$-matrix $\left((-1)^{i+j} \det\left(B_{\sim j, \sim i}\right)\right)_{1 \leq i \leq n,\ 1 \leq j \leq n}$.
- If $m$ is a nonnegative integer, then $I_m$ denotes the $m \times m$ identity matrix.

We will need the following properties of determinants:

- For any $n \times n$-matrix $B$, we have
  $$B \cdot (\operatorname{adj} B) = (\operatorname{adj} B) \cdot B = (\det B) \cdot I_n. \tag{3}$$
  (This is the main property of adjugates; see, e.g., [5, Theorem 6.100] for a proof.)
- For any commutative ring $S$, any $m \times m$-matrix $B$ and any element $x \in S$, we have
  $$\det\left(B + x I_m\right) = \sum_{P \subseteq [m]} \det\left(\operatorname{sub}_P^P B\right) \cdot x^{m - |P|}. \tag{4}$$

(This is a folklore result – essentially the explicit formula for the characteristic polynomial of a matrix in terms of its principal minors. The proof is straightforward: Expand the left hand side into a sum of products, and combine products according to "which factors come from $B$ and which factors come from $xI_m$". See [7, Proposition 6.4.29] or [5, Corollary 6.164] for detailed proofs.)

For any ring $S$, we consider the univariate polynomial ring $S[t]$ as well as the ring $S[[t]]$ of formal power series. Of course, $S[t]$ is a subring of $S[[t]]$. Note that the ring $S$ need not be commutative for $S[t]$ and $S[[t]]$ to be defined.

# 4. Proof of Theorem 2.2

We now finally step to the proof of Theorem 2.2.

*Proof of Theorem 2.2.* We must prove that all diagonal entries of $A^m$ belong to $\mathcal{P}$. In other words, we must prove that $(A^m)_{i,i} \in \mathcal{P}$ for each $i \in [n]$.

It is well-known that a polynomial over a matrix ring is "essentially the same as" a matrix with polynomial entries. In other words, we can identify the ring $R^{n\times n}[t]$ with the ring $(R[t])^{n\times n}$ using a straightforward ring isomorphism (which sends each $\sum_{i\geq 0} C_i t^i \in R^{n\times n}[t]$ to $\sum_{i\geq 0} C_i t^i \in (R[t])^{n\times n}$). In the same way, we identify the ring $R^{n\times n}[[t]]$ with the ring $(R[[t]])^{n\times n}$.

Let $B$ be the matrix $I_n - tA$ in the power series ring $R^{n\times n}[[t]]$. This matrix $B = I_n - tA$ is invertible, and its inverse is

$$B^{-1} = I_n + tA + t^2A^2 + t^3A^3 + \cdots . \tag{5}$$

(This can be proved by directly verifying that $I_n + tA + t^2A^2 + t^3A^3 + \cdots$ is inverse to $I_n - tA$. Indeed, both products $\left(I_n + tA + t^2A^2 + t^3A^3 + \cdots\right)\cdot(I_n - tA)$ and $(I_n - tA)\cdot\left(I_n + tA + t^2A^2 + t^3A^3 + \cdots\right)$ turn, upon expanding, into sums that telescope to $I_n$.)

Since the matrix $B$ is invertible, its determinant $\det B$ is invertible as well (since $(\det B)\cdot\left(\det\left(B^{-1}\right)\right) = \det\left(\underbrace{BB^{-1}}_{=I_n}\right) = \det(I_n) = 1$).

Now, recall that we must prove that $(A^m)_{i,i} \in \mathcal{P}$ for each $i \in [n]$. So let us fix $i \in [n]$. Then, (5) yields

$$\begin{aligned}\left(B^{-1}\right)_{i,i} &= \left(I_n + tA + t^2A^2 + t^3A^3 + \cdots\right)_{i,i} \\ &= (I_n)_{i,i} + tA_{i,i} + t^2\left(A^2\right)_{i,i} + t^3\left(A^3\right)_{i,i} + \cdots .\end{aligned}$$

Hence, the $t^m$-coefficient of the power series $\left(B^{-1}\right)_{i,i} \in R[[t]]$ is $(A^m)_{i,i}$. Thus, in order to prove that $(A^m)_{i,i} \in \mathcal{P}$ (which is our goal), it suffices to show that all coefficients of the power series $\left(B^{-1}\right)_{i,i}$ belong to $\mathcal{P}$. In other words, it suffices to show that $\left(B^{-1}\right)_{i,i} \in \mathcal{P}\left[\left[t\right]\right]$. This is what we shall now show.

From (3), we obtain $B \cdot (\operatorname{adj} B) = (\operatorname{adj} B) \cdot B = (\det B) \cdot I_n$, so that

$$B^{-1} = \frac{1}{\det B} \cdot \operatorname{adj} B.$$

Hence,

$$\left(B^{-1}\right)_{i,i} = \frac{1}{\det B} \cdot (\operatorname{adj} B)_{i,i}. \tag{6}$$

Our next goal is to show that both factors $\dfrac{1}{\det B}$ and $(\operatorname{adj} B)_{i,i}$ on the right hand side of this equality belong to $\mathcal{P}\left[\left[t\right]\right]$. This will then entail that $\left(B^{-1}\right)_{i,i} \in \mathcal{P}\left[\left[t\right]\right]$ as well, and we will be done.

From $B = I_n - tA = -tA + 1I_n$, we obtain

$$\begin{aligned}
\det B = \det\left(-tA + 1I_n\right) &= \sum_{P \subseteq [n]} \det\left(\underbrace{\operatorname{sub}_P^P(-tA)}_{=-t\operatorname{sub}_P^P A}\right) \cdot \underbrace{1^{n-|P|}}_{=1} \\
&\qquad \left(\begin{array}{c}\text{by (4), applied to } n,\ R\left[\left[t\right]\right],\ -tA \text{ and } 1 \\ \text{instead of } m,\ S,\ B \text{ and } x\end{array}\right) \\
&= \sum_{P \subseteq [n]} \underbrace{\det\left(-t\operatorname{sub}_P^P A\right)}_{=(-t)^{|P|}\det\left(\operatorname{sub}_P^P A\right)} \\
&= \sum_{P \subseteq [n]} (-t)^{|P|} \underbrace{\det\left(\operatorname{sub}_P^P A\right)}_{\substack{\in \mathcal{P} \\ \text{(since } \det\left(\operatorname{sub}_P^P A\right) \text{ is} \\ \text{a principal minor of } A\text{)}}} \qquad (7) \\
&\in \mathcal{P}\left[t\right] \subseteq \mathcal{P}\left[\left[t\right]\right].
\end{aligned}$$

Thus, $\det B$ is a formal power series over $\mathcal{P}$. Moreover, (7) shows that this power series has constant term 1 (since the only addend in the sum in (7) that contributes to the constant term is the addend for $P = \varnothing$, but this addend is $\underbrace{(-t)^{|\varnothing|}}_{=1} \underbrace{\det\left(\operatorname{sub}_\varnothing^\varnothing A\right)}_{\substack{=1 \\ \text{(since the } 0\times 0\text{-matrix} \\ \text{has determinant 1)}}} = 1$). Thus, this power series is invertible in $\mathcal{P}\left[\left[t\right]\right]$. Therefore,

$$\frac{1}{\det B} \in \mathcal{P}\left[\left[t\right]\right]. \tag{8}$$

Now, recall the definition of an adjugate matrix. This definition yields

$$\begin{aligned}
(\operatorname{adj} B)_{i,i} &= \underbrace{(-1)^{i+i}}_{=1} \det\left(B_{\sim i,\sim i}\right) = \det\left(B_{\sim i,\sim i}\right) \\
&= \det\left(\left(-tA + 1I_n\right)_{\sim i,\sim i}\right) \qquad \left(\text{since } B = -tA + 1I_n\right) \\
&= \det\left(-tA_{\sim i,\sim i} + 1I_{n-1}\right) \qquad \left(\text{since } \left(-tA + 1I_n\right)_{\sim i,\sim i} = -tA_{\sim i,\sim i} + 1I_{n-1}\right) \\
&= \sum_{P \subseteq [n-1]} \det\left(\underbrace{\operatorname{sub}_P^P\left(-tA_{\sim i,\sim i}\right)}_{=-t\operatorname{sub}_P^P\left(A_{\sim i,\sim i}\right)}\right) \cdot \underbrace{1^{n-1-|P|}}_{=1} \\
&\qquad \left(\begin{array}{c}\text{by (4), applied to } n-1,\ R[[t]],\ -tA_{\sim i,\sim i} \text{ and } 1 \\ \text{instead of } m,\ S,\ B \text{ and } x\end{array}\right) \\
&= \sum_{P \subseteq [n-1]} \underbrace{\det\left(-t\operatorname{sub}_P^P\left(A_{\sim i,\sim i}\right)\right)}_{=(-t)^{|P|}\det\left(\operatorname{sub}_P^P\left(A_{\sim i,\sim i}\right)\right)} \\
&= \sum_{P \subseteq [n-1]} (-t)^{|P|} \det\left(\operatorname{sub}_P^P\left(A_{\sim i,\sim i}\right)\right). \qquad (9)
\end{aligned}$$

Now, let $P$ be an arbitrary subset of $[n-1]$. Write this subset $P$ in the form $P = \{p_1, p_2, \ldots, p_r\}$, where $p_1 < p_2 < \cdots < p_r$. Furthermore, let $g \in \{0, 1, \ldots, r\}$ be the element that satisfies

$$p_1 < p_2 < \cdots < p_g < i \leq p_{g+1} < p_{g+2} < \cdots < p_r.$$

(Here, $g$ will be 0 if all elements of $P$ are $\geq i$, and $g$ will be $r$ if all elements of $P$ are $< i$.) Then, due to the combinatorial nature of removing rows and columns, we have

$$\operatorname{sub}_P^P\left(A_{\sim i,\sim i}\right) = \operatorname{sub}_{P'}^{P'} A,$$

where $P'$ is the subset $\left\{p_1, p_2, \ldots, p_g\right\} \cup \left\{p_{g+1}+1, p_{g+2}+1, \ldots, p_r+1\right\}$ of $[n]$. Hence, $\operatorname{sub}_P^P\left(A_{\sim i,\sim i}\right)$ is a principal submatrix of $A$. Therefore, its determinant $\det\left(\operatorname{sub}_P^P\left(A_{\sim i,\sim i}\right)\right)$ is a principal minor of $A$, thus belongs to $\mathcal{P}$.

Forget that we fixed $P$. We thus have shown that $\det\left(\operatorname{sub}_P^P\left(A_{\sim i,\sim i}\right)\right) \in \mathcal{P}$ for each $P \subseteq [n-1]$. Therefore, (9) becomes

$$(\operatorname{adj} B)_{i,i} = \sum_{P \subseteq [n-1]} (-t)^{|P|} \underbrace{\det\left(\operatorname{sub}_P^P\left(A_{\sim i,\sim i}\right)\right)}_{\in \mathcal{P}} \in \mathcal{P}[t] \subseteq \mathcal{P}[[t]]. \qquad (10)$$

Now, (6) becomes

$$\left(B^{-1}\right)_{i,i} = \frac{1}{\underbrace{\det B}_{\substack{\in \mathcal{P}[[t]] \\ \text{(by (8))}}}} \cdot \underbrace{(\operatorname{adj} B)_{i,i}}_{\substack{\in \mathcal{P}[[t]] \\ \text{(by (10))}}} \in \mathcal{P}[[t]] \cdot \mathcal{P}[[t]] \subseteq \mathcal{P}[[t]].$$

As explained above, this completes our proof of Theorem 2.2. □

Somewhat regrettably, the above proof is the slickest I am aware of. A more-or-less equivalent proof can be given avoiding the use of power series (using [6, Proposition 3.9 and Lemma 3.11] instead). A more pedestrian (but harder to formalize) proof uses the Cayley–Hamilton theorem and a variant of the inclusion/exclusion principle.

# 5. Variants

A counterpart of Theorem 2.2 for the off-diagonal entries of $A^m$ exists as well:

**Theorem 5.1.** Let $n$, $m$, $R$, $A$ and $\mathcal{P}$ be as in Theorem 2.2.

Let $i$ and $j$ be two distinct elements of $[n]$. An $(i,j)$-*quasiprincipal minor* of $A$ shall mean a determinant of the form $\det\left(\operatorname{sub}_I^J A\right)$, where $I$ and $J$ are two subsets of $[n]$ satisfying

$$i \in I \text{ and } j \in J \text{ and } |I| = |J| \text{ and } J = (I \setminus \{i\}) \cup \{j\}.$$

(For instance, if $n \geq 7$, then $\det\left(\operatorname{sub}_{\{1,2,7\}}^{\{2,5,7\}} A\right)$ is a $(1,5)$-quasiprincipal minor of $A$.)

Let $\mathcal{K}_{i,j}$ be the $\mathbb{Z}$-submodule of $R$ spanned by all $(i,j)$-quasiprincipal minors of $A$. Then,

$$(A^m)_{i,j} \in \mathcal{P} \cdot \mathcal{K}_{i,j}.$$

*Proof outline.* This is similar to our above proof of Theorem 2.2, but some changes are needed. Most importantly, instead of proving that $(\operatorname{adj} B)_{i,i} \in \mathcal{P}[[t]]$, we now need to show that $(\operatorname{adj} B)_{i,j} \in \mathcal{K}_{i,j}[[t]]$ (that is, that all coefficients of the power series $(\operatorname{adj} B)_{i,j}$ belong to $\mathcal{K}_{i,j}$). To do so, we apply the definition of the adjugate matrix to see that

$$(\operatorname{adj} B)_{i,j} = (-1)^{j+i} \det\left(B_{\sim j,\sim i}\right). \tag{11}$$

We can simplify $B_{\sim j,\sim i}$ further to $-tA_{\sim j,\sim i} + (I_n)_{\sim j,\sim i}$ (since $B = I_n - tA = -tA + I_n$), but unfortunately this is not the same as $-tA_{\sim j,\sim i} + 1I_{n-1}$, and thus we can no longer apply (4). Instead, we use a trick:

- We define $A'$ to be the matrix obtained from $-tA$ by replacing the $j$-th row by $(0,0,\ldots,0,1,0,0,\ldots,0)$, where the only entry equal to 1 is in the $i$-th position.
- We define $I_n'$ to be the matrix obtained from $I_n$ by replacing the 1 in the $j$-th row by a 0.
- We define $B'$ to be the matrix obtained from $B$ by replacing the $j$-th row by $(0,0,\ldots,0,1,0,0,\ldots,0)$, where the only entry equal to 1 is in the $i$-th position.

Laplace expansion along the $j$-th row shows that

$$\det\left(B'\right) = (-1)^{j+i} \det\left(\left(B'\right)_{\sim j,\sim i}\right) = (-1)^{j+i} \det\left(B_{\sim j,\sim i}\right)$$

(since the matrix $B'$ differs from $B$ only in the $j$-th row, and thus we have $\left(B'\right)_{\sim j,\sim i} = B_{\sim j,\sim i}$). Comparing this with (11), we find

$$\left(\operatorname{adj} B\right)_{i,j} = \det\left(B'\right). \tag{12}$$

Furthermore, recall that $B = I_n - tA = -tA + I_n$. Thus, $B' = A' + I'_n$ (based on how $A'$, $I'_n$ and $B'$ were constructed).

On the other hand, the definition of $I'_n$ shows that $I'_n$ is a diagonal $n \times n$-matrix with diagonal entries $1, 1, \ldots, 1, 0, 1, 1, \ldots, 1$, where the only diagonal entry equal to 0 is in the $j$-th position. However, another classical fact about determinants ([7, Theorem 6.4.26], [5, Corollary 6.162]) shows that if $C$ is any $n \times n$-matrix, and if $D$ is a diagonal $n \times n$-matrix with diagonal entries $d_1, d_2, \ldots, d_n$, then

$$\det\left(C + D\right) = \sum_{P \subseteq [n]} \det\left(\operatorname{sub}_P^P C\right) \cdot \prod_{k \in [n] \setminus P} d_k.$$

We can apply this to $C = A'$ and $D = I'_n$ and $\left(d_1, d_2, \ldots, d_n\right) = \underbrace{\left(1, 1, \ldots, 1, 0, 1, 1, \ldots, 1\right)}_{\text{the 0 is in the } j\text{-th position}}$, and thus obtain

$$\begin{aligned}
&\det\left(A'+I'_n\right)\\
&=\sum_{P\subseteq[n]}\det\left(\operatorname{sub}_P^P\left(A'\right)\right)\cdot\prod_{k\in[n]\setminus P}\begin{cases}1, & \text{if } k\neq j;\\ 0, & \text{if } k=j\end{cases}\\
&\qquad\qquad\left(\text{since the } k\text{-th diagonal entry of } I'_n \text{ is } \begin{cases}1, & \text{if } k\neq j;\\ 0, & \text{if } k=j\end{cases}\right)\\
&=\sum_{P\subseteq[n]}\det\left(\operatorname{sub}_P^P\left(A'\right)\right)\cdot\begin{cases}1, & \text{if } j\notin[n]\setminus P;\\ 0, & \text{if } j\in[n]\setminus P\end{cases}\\
&=\sum_{\substack{P\subseteq[n];\\ j\notin[n]\setminus P}}\det\left(\operatorname{sub}_P^P\left(A'\right)\right)=\sum_{\substack{P\subseteq[n];\\ j\in P}}\det\left(\operatorname{sub}_P^P\left(A'\right)\right)\\
&=\sum_{\substack{P\subseteq[n];\\ j\in P \text{ and } i\in P}}\det\left(\operatorname{sub}_P^P\left(A'\right)\right)+\sum_{\substack{P\subseteq[n];\\ j\in P \text{ and } i\notin P}}\underbrace{\det\left(\operatorname{sub}_P^P\left(A'\right)\right)}_{\substack{=0\\ \text{(since all entries in the } j\text{-th row of } A'\\ \text{are 0 except for the } i\text{-th entry, and thus}\\ \text{the matrix } \operatorname{sub}_P^P(A') \text{ has a zero row)}}}\\
&=\sum_{\substack{P\subseteq[n];\\ j\in P \text{ and } i\in P}}\underbrace{\det\left(\operatorname{sub}_P^P\left(A'\right)\right)}_{\substack{=\pm\det\left(\operatorname{sub}_{P\setminus\{j\}}^{P\setminus\{i\}}(-tA)\right)\\ \text{(by Laplace expansion along the row}\\ \text{that was the } j\text{-th row of } A')}}=\sum_{\substack{P\subseteq[n];\\ j\in P \text{ and } i\in P}}\pm\underbrace{\det\left(\operatorname{sub}_{P\setminus\{j\}}^{P\setminus\{i\}}\left(-tA\right)\right)}_{=\pm t^{|P|-1}\det\left(\operatorname{sub}_{P\setminus\{j\}}^{P\setminus\{i\}}A\right)}\\
&=\sum_{\substack{P\subseteq[n];\\ j\in P \text{ and } i\in P}}\pm t^{|P|-1}\underbrace{\det\left(\operatorname{sub}_{P\setminus\{j\}}^{P\setminus\{i\}}A\right)}_{\substack{\in\mathcal{K}_{i,j}\\ \text{(since } \det\left(\operatorname{sub}_{P\setminus\{j\}}^{P\setminus\{i\}}A\right) \text{ is}\\ \text{an } (i,j)\text{-quasiprincipal minor of } A)}}\in\sum_{\substack{P\subseteq[n];\\ j\in P \text{ and } i\in P}}\pm t^{|P|-1}\mathcal{K}_{i,j}\subseteq\mathcal{K}_{i,j}\left[[t]\right].
\end{aligned}$$

In view of $B'=A'+I'_n$, this rewrites as $\det\left(B'\right)\in\mathcal{K}_{i,j}\left[[t]\right]$. Hence, (12) becomes $\left(\operatorname{adj}B\right)_{i,j}=\det\left(B'\right)\in\mathcal{K}_{i,j}\left[[t]\right]$. Having showed this, we can finish the proof as we did for Theorem 2.2. □

Another variant of Theorem 2.2 is the following:

**Theorem 5.2.** Let $n$ and $m$ be nonnegative integers. Let $R$ be a commutative ring. Let $A$ be an $n\times n$-matrix over $R$. Assume that all principal minors of $A$ equal 1. Then, all diagonal entries of $A^m$ equal 1.

*Proof.* Follow the above proof of Theorem 2.2. From (7), we obtain

$$\det B=\sum_{P\subseteq[n]}(-t)^{|P|}\underbrace{\det\left(\operatorname{sub}_P^P A\right)}_{\substack{=1\\ \text{(by assumption, since } \det\left(\operatorname{sub}_P^P A\right)\\ \text{is a principal minor of } A)}}=\sum_{P\subseteq[n]}(-t)^{|P|}=(1-t)^n$$

(since the binomial formula yields $(1-t)^n = \sum_{k=0}^{n} \binom{n}{k} (-t)^k = \sum_{P \subseteq [n]} (-t)^{|P|}$). Let $i \in \{1, 2, \ldots, n\}$. From (9), we obtain

$$(\operatorname{adj} B)_{i,i} = \sum_{P \subseteq [n-1]} (-t)^{|P|} \underbrace{\det\left(\operatorname{sub}_P^P (A_{\sim i, \sim i})\right)}_{\substack{=1 \\ \text{(by assumption,} \\ \text{since } \det(\operatorname{sub}_P^P(A_{\sim i,\sim i})) \\ \text{is a principal minor of } A)}} = \sum_{P \subseteq [n-1]} (-t)^{|P|} = (1-t)^{n-1}$$

(again by the binomial formula). Now, (6) becomes

$$\left(B^{-1}\right)_{i,i} = \frac{1}{\det B} \cdot (\operatorname{adj} B)_{i,i} = \underbrace{(\operatorname{adj} B)_{i,i}}_{=(1-t)^{n-1}} \diagup \underbrace{(\det B)}_{=(1-t)^n} = (1-t)^{n-1} \diagup (1-t)^n$$
$$= \frac{1}{1-t} = 1 + t + t^2 + t^3 + \cdots .$$

Thus, the $t^m$-coefficient of the power series $\left(B^{-1}\right)_{i,i} \in R[[t]]$ is 1. However, we have already seen that this coefficient is $(A^m)_{i,i}$. Thus, we conclude that $(A^m)_{i,i} = 1$. This shows that all diagonal entries of $A^m$ equal 1, so that Theorem 5.2 is proved. □

# 6. Back to Putnam 2021

As already mentioned, we do not know whether Theorem 1.1 can be generalized by replacing "odd" by "congruent to 1 modulo 4". More generally, we are tempted to ask the following:

**Question 6.1.** Fix a commutative ring $R$. Let $A$ be an $n \times n$-matrix over $R$. Let $m$ be a nonnegative integer. Assume that each principal minor of $A$ is 1. Is it true that each principal minor of $A^m$ is 1 as well?

For $R = \mathbb{Z}/2$, this would yield Theorem 1.1; the "congruent to 1 modulo 4" variant would follow for $R = \mathbb{Z}/4$. Theorem 5.2 corresponds to the case when the principal minor of $A^m$ is a diagonal entry. The argument from [2, Lemma 3.3] shows that Question 6.1 has a positive answer whenever $R$ is an integral domain; thus, the answer is also positive when $R$ is a product of integral domains. On the other hand, if $R$ can be arbitrary, then the answer to Question 6.1 is negative, but the only counterexample we know is when $R$ is a certain quotient ring of a polynomial ring[3] (and $n = 4$ and $m = 2$). The smallest ring $R$ for which the question remains open is $\mathbb{Z}/4$.

[3] Here are the details: Let $R$ be the quotient ring

$$\mathbb{Q}[x, y] \diagup \left(x^3 + y^3, xy, x^4, x^3y, x^2y^2, xy^3, y^4\right),$$

# References

[1] Kiran Kedlaya, *The Putnam Archive*, https://kskedlaya.org/putnam-archive/ .

[2] Mikiya Masuda, Taras Panov, *Semifree circle actions, Bott towers, and quasitoric manifolds*, Sbornik Math. **199** (2008), no. 7-8, 1201-1223, arXiv:math/0607094v2.

[3] MAA, *Putnam Competition*, official website, https://www.maa.org/math-competitions/putnam-competition .

[4] D. J. Hartfiel and R. Loewy, *On matrices having equal corresponding principal minors*, Linear Algebra and its Applications **56** (1984), pp. 147–167.

[5] Darij Grinberg, *Notes on the combinatorial fundamentals of algebra*, 15 September 2022, arXiv:2008.09862v3.

[6] Darij Grinberg, *The trace Cayley-Hamilton theorem*, arXiv:2510.20689v1.
https://www.cip.ifi.lmu.de/~grinberg/algebra/trach.pdf

[7] Darij Grinberg, *An Introduction to Algebraic Combinatorics [Math 701, Spring 2021 lecture notes]*, 30 January 2022.
https://www.cip.ifi.lmu.de/~grinberg/t/21s/lecs.pdf

and let $A := \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & y & x \\ x & 0 & 1 & y \\ y & 0 & x & 1 \end{pmatrix} \in R^{4\times 4}$. Then, all principal minors of $A$ are 1, but the principal minor $\det\left(\operatorname{sub}_{\{2,3\}}^{\{2,3\}}\left(A^2\right)\right) = 1 - x^3 - xy$ is not 1 since $x^3 \neq 0$ in $R$. Actually, we can replace $\mathbb{Q}$ by any field here (even by $\mathbb{Z}/2$); then, $R$ becomes a finite ring. (But we cannot turn $R$ into $\mathbb{Z}/n$ without changing the construction of $A$.)