Solutions for the AAC Competition Problems 2012

1. Let A be a square matrix of odd size. Prove that A is singular if and only if it can be carried to $-A$ by elementary operations of adding a multiple of one row to another row.

Solution: The indicated elementary operations preserve the determinant, so a nonsingular matrix A cannot be carried to $-A$ since $\det(-A) = (-1)^n \det(A) = -\det(A) \neq \det(A)$, where n is the size of A.

Now assume that A is singular. Then Gaussian elimination allows us to carry A to a matrix B that has a zero row at the bottom. Hence $B = E_s \cdots E_1 A$ where E_k, $k = 1, \ldots, s$, are elementary matrices corresponding to adding a multiple of one row to another row. It is easy to carry B to $-B$. Indeed, for each $i = 1, \ldots, n-1$, we can add row i to the last row, then subtract the double of the new last row from row i and finally add the new row i to the last row. Thus $-B = UB$ where U is the product of $3(n-1)$ elementary matrices. It remains to observe that $-A = E_1^{-1} \cdots E_s^{-1}(-B)$ and the matrices E_k^{-1} are also elementary. Hence

$$-A = E_1^{-1} \cdots E_s^{-1} U E_s \cdots E_1 A,$$

as required.

2. Let ξ be a primitive complex n-th root of unity, $n \geq 2$. Determine the n-th power of the following $n \times n$ matrix:

$$\begin{pmatrix}
1 & -1 & 0 & 0 & 0 & \ldots & 0 & 0 \\
0 & \xi & -1 & 0 & 0 & \ldots & 0 & 0 \\
0 & 0 & \xi^2 & -1 & 0 & \ldots & 0 & 0 \\
\ldots \\
0 & 0 & 0 & 0 & 0 & \ldots & \xi^{n-2} & -1 \\
-1 & 0 & 0 & 0 & 0 & \ldots & 0 & \xi^{n-1}
\end{pmatrix}.$$

Solution: Let us first compute the characteristic polynomial $\chi(t)$ of the given matrix A:

$$\chi(t) = \det(A - tI) = \begin{vmatrix}
1-t & -1 & 0 & 0 & 0 & \ldots & 0 & 0 \\
0 & \xi - t & -1 & 0 & 0 & \ldots & 0 & 0 \\
0 & 0 & \xi^2 - t & -1 & 0 & \ldots & 0 & 0 \\
\ldots \\
0 & 0 & 0 & 0 & 0 & \ldots & \xi^{n-2} - t & -1 \\
-1 & 0 & 0 & 0 & 0 & \ldots & 0 & \xi^{n-1} - t
\end{vmatrix}.$$

Using expansion down the last column, we obtain:

$$\chi(t) = \begin{vmatrix} 1-t & -1 & 0 & 0 & 0 & \dots & 0 \\ 0 & \xi - t & -1 & 0 & 0 & \dots & 0 \\ 0 & 0 & \xi^2 - t & -1 & 0 & \dots & 0 \\ \dots \\ 0 & 0 & 0 & 0 & 0 & \dots & -1 \\ -1 & 0 & 0 & 0 & 0 & \dots & 0 \end{vmatrix}$$

$$+ (\xi^{n-1} - t) \begin{vmatrix} 1-t & -1 & 0 & 0 & 0 & \dots & 0 \\ 0 & \xi - t & -1 & 0 & 0 & \dots & 0 \\ 0 & 0 & \xi^2 - t & -1 & 0 & \dots & 0 \\ \dots \\ 0 & 0 & 0 & 0 & 0 & \dots & -1 \\ 0 & 0 & 0 & 0 & 0 & \dots & \xi^{n-2} - t \end{vmatrix}$$

$$= (-1)^{n+1} \begin{vmatrix} -1 & 0 & 0 & 0 & \dots & 0 \\ \xi - t & -1 & 0 & 0 & \dots & 0 \\ 0 & \xi^2 - t & -1 & 0 & \dots & 0 \\ \dots \\ 0 & 0 & 0 & 0 & \dots & -1 \end{vmatrix}$$

$$+ (\xi^{n-1} - t)(1-t)(\xi - t) \cdots (\xi^{n-2} - t)$$

$$= (-1)^{n+1}(-1)^{n-2} + (-1)^n (t-1)(t-\xi) \cdots (t - \xi^{n-1}).$$

Since ξ is a primitive n-th root of unity, the numbers $1, \xi, \dots, \xi^{n-1}$ are precisely all the n-th roots of unity, so we have

$$\chi(t) = -1 + (-1)^n (t^n - 1) = \begin{cases} -t^n & \text{if } n \text{ is odd,} \\ t^n - 2 & \text{if } n \text{ is even.} \end{cases}$$

Now recall that, by Cayley–Hamilton Theorem, $\chi(A) = 0$, which immediately allows us to find A^n.

Answer: $A^n = 0$ if n is odd and $A^n = 2I$ if n is even.

Remark. An alternative solution is to observe that $A = X - Y$ where

$$X = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & \xi & 0 & \dots & 0 & 0 \\ 0 & 0 & \xi^2 & \dots & 0 & 0 \\ \dots \\ 0 & 0 & 0 & \dots & \xi^{n-2} & 0 \\ 0 & 0 & 0 & \dots & 0 & \xi^{n-1} \end{pmatrix} \text{ and } Y = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \dots \\ 0 & 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

One immediately verifies that $YX = \xi XY$, hence we can apply the Quantum Binomial Formula to compute:

$$A^n = (X - Y)^n = X^n + \sum_{k=1}^{n-1} \begin{bmatrix} n \\ k \end{bmatrix}_{\xi} (-1)^k X^{n-k} Y^k + (-1)^n Y^n$$

where $\begin{bmatrix} n \\ k \end{bmatrix}_\xi$ are the Gaussian binomial coefficients. Since ξ is a primitive n-th root of unity, all these coefficients vanish for $k = 1, \ldots, n-1$. It remains to observe that $X^n = Y^n = I$.

3. Harry Potter and Voldemort are playing a game by filling the squares of a chess board with integers as follows. First Voldemort fills the dark squares and then Harry must fill the light squares so that the resulting 8×8 matrix has rank r. For what values of r does Harry have a winning strategy?

Solution: It is easier to see what is going on if we permute the rows and columns of the chessboard so it looks like

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix},$$

where 0 stands for a light square and 1 for a dark square. Thus, during the game, Voldemort replaces the 1's by integers of his choice and Harry does the same with the 0's.

Now it is clear that, for $r < 4$, Harry does not have a winning strategy because Voldemort can create a nonzero minor of size 4. Let us show that, for any $r \geq 4$, Harry does have a winning strategy. For a given $r \geq 4$ and any 4×4 matrices A and B, Harry must find 4×4 matrices X and Y such that $\operatorname{rk} \begin{bmatrix} A & X \\ Y & B \end{bmatrix} = r$. One solution is $X = I$ and $Y = C + BA$ where C is any 4×4 matrix of rank $r - 4$. Indeed,

$$\begin{aligned} \operatorname{rk} \begin{bmatrix} A & I \\ C + BA & B \end{bmatrix} &= \operatorname{rk} \left(\begin{bmatrix} A & I \\ C + BA & B \end{bmatrix} \begin{bmatrix} I & 0 \\ -A & I \end{bmatrix} \right) = \operatorname{rk} \begin{bmatrix} 0 & I \\ C & B \end{bmatrix} \\ &= \operatorname{rk} \left(\begin{bmatrix} I & 0 \\ -B & I \end{bmatrix} \begin{bmatrix} 0 & I \\ C & B \end{bmatrix} \right) = \operatorname{rk} \begin{bmatrix} 0 & I \\ C & 0 \end{bmatrix} = 4 + \operatorname{rk} C \\ &= r. \end{aligned}$$

We have used the fact that multiplication by a nonsingular matrix on the left or on the right does not change the rank.

Answer: Harry has a winning strategy if and only if $4 \leq r \leq 8$.

4. Let $f(z)$ be a polynomial function with complex coefficients. Prove that if f maps the set of all complex roots of unity to itself, then f is a monomial.

Solution: Write $f(z) = \sum_k a_k z^k$. For any root of unity ξ, the value $f(\xi)$ is also a root of unity, so $f(\xi)\overline{f(\xi)} = 1$. We have $\overline{f(\xi)} = \bar{f}(\bar{\xi})$ where $\bar{f}(z) = \sum_k \bar{a}_k z^k$

is the conjugate polynomial. Also, $\bar{\xi} = \xi^{-1}$. Consider the Laurent polynomial $g(z) = f(z)\bar{f}(z^{-1}) - 1$. By the above argument, all complex roots of unity are roots of $g(z)$. It follows that $g(z)$ is identically zero. Hence $f(z)\bar{f}(z^{-1}) = 1$.

For a Laurent polynomial $h(z) = \sum_{k=s}^{t} c_k z^k$ with $c_s \neq 0$ and $c_t \neq 0$, let $\mathrm{HT}(h) = c_t z^t$ (highest term) and $\mathrm{LT}(h) = c_s z^s$ (lowest term). Then we have $\mathrm{HT}(h_1 h_2) = \mathrm{HT}(h_1)\mathrm{HT}(h_2)$ and $\mathrm{LT}(h_1 h_2) = \mathrm{LT}(h_1)\mathrm{LT}(h_2)$. Applying this to the equation $f(z)\bar{f}(z^{-1}) = 1$, we conclude that $\mathrm{HT}(f) = \mathrm{LT}(f)$, that is, $f(z)$ is a monomial.

5. Let p be a prime. For any integers $a_0, a_1, \ldots, a_p$, prove that

$$\sum a_{i_1} \cdots a_{i_p} \equiv a_1^p \pmod{p},$$

where the summation is over all $i_1, \ldots, i_p \geq 0$ such that $i_1 + \cdots + i_p = p$.

Solution: It will be convenient to work in the field $\mathbb{Z}_p$ of integers modulo p. Let t be an indeterminate and let $f = \sum_{k=0}^{p} a_k t^k \in \mathbb{Z}_p[t]$. Then the sum $\sum a_{i_1} \cdots a_{i_p}$ equals the coefficient of t^p in the polynomial f^p. But we have $(a+b)^p = a^p + b^p$ in characteristic p, hence, by induction, $f^p = \sum_{k=0}^{p} a_k^p t^{kp}$, so the coefficient of t^p equals a_1^p.

6. Let G be a finite simple group. Suppose G contains a subgroup of prime index p. Prove that p is the largest prime divisor of $|G|$ and, moreover, p^2 does not divide $|G|$.

Solution: Let $H \subset G$ be a subgroup of index p and let $X = G/H$ be the set of left cosets of G with respect to H. Then G acts on X by left translations. Since $|X| = p$, this action yields a homomorphism from G to S_p, the symmetric group on p symbols. Since the action of G on X is nontrivial (in fact, transitive), the kernel of the homomorphism $G \to S_p$ cannot be the entire G, hence it must be trivial by simplicity. Therefore, G is isomorphic to a subgroup of S_p. Hence $|G|$ is a divisor of $p!$. The result follows.