Du côté des élèves de Terminale

Questions proposées aux élèves de Terminale

1. ***a)*** Soit p un nombre premier. Démontrer que pour tout $n \in \mathbb{N}$,

$$\binom{n}{p} \equiv \left\lfloor \frac{n}{p} \right\rfloor \pmod{p},$$

où $\left\lfloor \frac{n}{p} \right\rfloor$ désigne la partie entière de $\frac{n}{p}$ (on convient que $\binom{n}{p} = 0$ si $n < p$).

b) Soit $r \in \mathbb{N}$ tel que p^r divise $\left\lfloor \frac{n}{p} \right\rfloor$. Montrer que p^r divise $\binom{n}{p}$.

2. Démontrer l'identité :

$$\forall n \in \mathbb{N}^*,\ \sum_{k=1}^{n} (-1)^{k+1} \frac{1}{k} \binom{n}{k} = \sum_{k=1}^{n} \frac{1}{k}.$$

3. Soit $A_1A_2A_3A_4$ un tétraèdre et O un point quelconque de l'espace tel que pour tout $i \in [\![1, 4]\!]$, la droite (OA_i) n'est pas parallèle au plan de la face opposée à A_i dans le tétraèdre $A_1A_2A_3A_4$; on note B_i le point d'intersection de (OA_i) avec le plan de la face opposée à A_i et on pose : $x_i = \dfrac{\overline{OA_i}}{\overline{OB_i}}$, la droite (OA_i) étant supposée orientée. Montrer que

$$x_1x_2x_3x_4 = 3 - 2\,(x_1 + x_2 + x_3 + x_4) + x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4.$$

4. On note $\mathcal{M}_n(\mathbb{R})$ l'ensemble des matrices carrées d'ordre $n \in \mathbb{N}^*$ à coefficients réels. Soient $\lambda \in \mathbb{R}$ et A, B, C trois matrices de $\mathcal{M}_n(\mathbb{R})$ telles que :
- C est la matrice dont tous les coefficients sont égaux à 1,
- A et B sont inversibles et $A + B = \lambda C$.

Pour $M \in \mathcal{M}_n(\mathbb{R})$, on note $\sigma(M)$ la somme de tous les coefficients de M. Montrer que

$$\lambda \cdot \sigma(A^{-1}) \cdot \sigma(B^{-1}) = \sigma(A^{-1}) + \sigma(B^{-1}).$$

Problème :

Olympiade internationale de mathématiques 2020 : corrigé des exercices 1 à 4

Les solutions des exercices 5 et 6 paraîtront dans le numéro suivant de la revue.

Solutions rédigées par Vincent Jugé, responsable de la délégation française à l'OIM.

Exercice 1. On considère un quadrilatère convexe $ABCD$. Un point P est situé à l'intérieur de $ABCD$. On suppose que les égalités de rapports ci-dessous sont vérifiées :

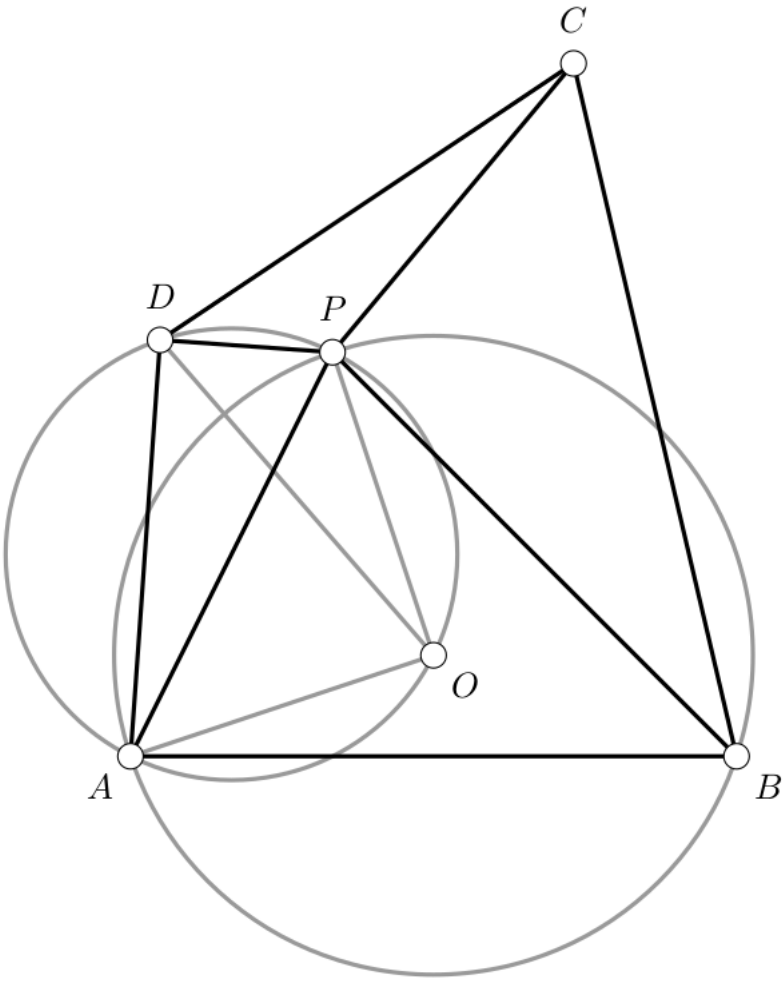
$$\widehat{PAD} : \widehat{PBA} : \widehat{DPA} = 1 : 2 : 3 = \widehat{CBP} : \widehat{BAP} : \widehat{BPC}.$$

Démontrer que les trois droites suivantes sont concourantes : la bissectrice intérieure de l'angle $\widehat{ADP}$, la bissectrice intérieure de l'angle $\widehat{PCB}$ et la médiatrice du segment $[AB]$.

Solution. Soit O le centre du cercle circonscrit à ABP. On pose $\alpha = \widehat{PAD}$ et $\beta = \widehat{PBO}$. En termes d'angles de droites, on vérifie que

$$(DP, DA) = (PD, PA) + (AP, AD) = 3\alpha + \alpha = 4\alpha = 2(BP, BA) = (OP, OA).$$

Cela signifie que les points A, D, P et O sont cocycliques.
En outre, on sait que $\widehat{PAD} + \widehat{DPA} = 4\alpha = 180^\circ - \widehat{ADP}$, donc que $2\alpha \leqslant 90^\circ$. Ainsi, l'angle $\widehat{PBA}$ est aigu, donc O et B sont du même côté de (AP). Or, P se trouve à l'intérieur du quadrilatère $ABCD$, donc B et D se trouvent de part et d'autre de (AP). On sait donc que $OA = OP$, que O et D se trouvent de part et d'autre de (AP) et que A, D, P et O sont cocycliques. Cela signifie que O est le pôle Sud issu de D dans le triangle APD, donc que O appartient à la bissectrice intérieure de l'angle $\widehat{ADP}$.
On démontre de même que O appartient à la bissectrice intérieure de l'angle $\widehat{PCB}$, et on conclut en remarquant que O appartient bien sûr à la médiatrice du segment $[AB]$.



Exercice 2. Soit a, b, c, d des nombres réels tels que $a \geqslant b \geqslant c \geqslant d > 0$ et $a+b+c+d = 1$. Démontrer que

$$(a + 2b + 3c + 4d)a^a b^b c^c d^d < 1.$$

Solution. Dans la suite, on pose $\mathbf{S} = (a+2b+3c+4d)a^a b^b c^c d^d$. Tout d'abord, si $a = b = c = d = 1/4$, on vérifie que $\mathbf{S} = 5/8 < 1$. On suppose donc désormais que les réels a, b, c et d ne sont pas tous égaux.
L'inégalité arithmético-géométrique pondérée, avec les poids a, b, c et d, indique alors que

$$a^a b^b c^c d^d < a^2 + b^2 + c^2 + d^2.$$

On en déduit que $\mathbf{S} < \mathbf{T}$, où l'on a posé $\mathbf{T} = (a + 2b + 3c + 4d)(a^2 + b^2 + c^2 + d^2)$.
On distingue enfin deux cas :

- si $0 \leqslant a \leqslant 1/2$, on vérifie que

$$\mathbf{T} \leqslant (a+3b+3c+3d)(a^2+ab+ac+ad) = (3-2a)a = 1-(a-1)(2a-1) \leqslant 1;$$

- si $1/2 \leqslant a \leqslant 1$, on vérifie également que

$$\begin{aligned} \mathbf{T} \leqslant (a+3b+3c+3d)(a^2+(b+c+d)^2) &= (3-2a)(a^2+(1-a)^2) \\ &= 1-2(a-1)^2(2a-1) \leqslant 1. \end{aligned}$$

On en conclut, dans chaque cas, que $\mathbf{S} < \mathbf{T} \leqslant 1$.

Exercice 3. On se donne $4n$ cailloux de poids $1, 2, 3, \ldots, 4n$. Chaque caillou est coloré en une couleur parmi n couleurs possibles, et il y a quatre cailloux de chaque couleur. Démontrer que l'on peut répartir les cailloux en deux tas de sorte que les deux conditions suivantes soient vérifiées :

- Les poids totaux des deux tas sont égaux.
- Chaque tas contient deux cailloux de chaque couleur.

Solution. On construit un graphe non orienté $\mathcal{G} = (V, E)$ comme suit :

- l'ensemble V des sommets se décomposent en l'ensemble V_1 des n couleurs utilisées et l'ensemble $V_2 = \{1, 2, \ldots, 4n\}$;
- tout sommet $v \in V_1$, que l'on identifie à une couleur, est relié aux poids des quatre cailloux de cette couleur ;
- en outre, pour tout entier $k \leqslant 2n$, les sommets k et $4n+1-k$ sont reliés l'un à l'autre.

Notons que chacun des n sommets $v \in V_1$ est de degré 4, tandis que chacun des $4n$ sommets $k \in V_2$ est de degré 2.
Chaque composante connexe $\mathcal{C}$ de $\mathcal{G}$ est donc un graphe formé de ℓ sommets $v \in V_1$ et de 4ℓ sommets $k \in V_2$, tous de degré pair, ainsi que de 6ℓ arêtes. D'après le théorème d'Euler, elle contient un cycle eulérien de longueur 6ℓ. Soit $v_0, v_1, \ldots, v_{6\ell-1}, v_0$ les sommets par lesquels passe un tel cycle, en partant d'un sommet $v_0 \in V_1$: on remarque que $v_i \in V_1$ si et seulement si 3 divise i.
Pour tout entier $u \in \{0, 1, \ldots, \ell-1\}$, on place alors dans le tas n°1 les cailloux de poids v_{6u+1} et v_{6u+2}, et dans le tas n°2 les cailloux de poids v_{6u+4} et v_{6u+5}. Ce faisant, puisque $v_{6u+1} + v_{6u+2} = v_{6u+4} + v_{6u+5} = 4n+1$, on vient d'augmenter de $(4n+1)\ell$ les poids totaux de chacun des tas.
En outre, chaque sommet $v \in V_1$ contenu dans $\mathcal{C}$ est égal à deux sommets v_{3i} et v_{3j}. Quitte à considérer les indices modulo 6ℓ, on a mis dans le tas n°1 exactement un des deux cailloux de poids v_{3i-1} et v_{3i+1}, et exactement un des deux cailloux de poids v_{3j-1} et v_{3j+1}. Or, il s'agit des quatre cailloux de couleur v. Chacun des deux tas contient donc exactement deux cailloux de couleur v, ce qui conclut.

Exercice 4. Soit $n \geqslant 2$ un entier. Il y a n^2 stations sur le versant d'une montagne, toutes à des altitudes différentes. Chacune des deux compagnies de téléphériques, A et B, gère k téléphériques ; chaque téléphérique permet de se déplacer d'une des stations vers une station plus élevée (sans arrêt intermédiaire). Les k téléphériques de A ont k points de départ différents et k points d'arrivée différents, et un téléphérique qui a un point de départ plus élevé a aussi un point d'arrivée plus élevé. Les mêmes conditions sont satisfaites pour B. On dit que deux stations sont *reliées* par une compagnie s'il est possible de partir de la station la plus basse et d'atteindre la plus élevée en utilisant un ou plusieurs téléphériques de cette compagnie (aucun autre mouvement entre les stations n'est autorisé).
Déterminer le plus petit entier strictement positif k qui garantisse qu'il existe deux stations reliées par chacune des deux compagnies.

Solution. Dans la suite, on trie nos stations par ordre croissant d'altitude, et on les identifie aux entiers de 1 à n^2, de sorte que la station $i+1$ soit plus haute que la station i.
On considère alors la situation où la compagnie A a mis en place un téléphérique entre chaque paire de stations (i, j) telle que $j = i + 1$ et $i \not\equiv 0 \pmod{n}$. De la sorte, elle possède $k = n^2 - n$ téléphériques, qui respectent bien les conditions de l'énoncé. De même, on suppose que la compagnie B a mis en place un téléphérique entre chaque paire de stations (i, j) telle que $j = i + n$ et $1 \leqslant i \leqslant n^2 - n$. Là aussi, elle possède $k = n^2 - n$ téléphériques, qui respectent bien les conditions de l'énoncé.
Enfin, s'il est possible de passer d'une station i à une station j en n'utilisant que des téléphériques gérés par la compagnie A, une récurrence immédiate indique que $\lfloor i/n \rfloor = \lfloor j/n \rfloor$. Au contraire, s'il est possible de passer de la station i à la station j en n'utilisant que des téléphériques gérés par la compagnie B, une récurrence immédiate indique que $\lfloor i/n \rfloor < \lfloor j/n \rfloor$.
Ainsi, lorsque $k = n^2 - n$, il est possible que nulle paire de stations ne puisse être reliée par les deux compagnies. En outre, pour tout $k \leqslant n^2 - n$, et en supprimant de manière arbitraire $n^2 - n - k$ lignes gérées par chacune des deux compagnies A et B, on constate toujours que nulle paire de stations n'est reliée par les deux compagnies, et que les conditions de l'énoncé sont bien respectées.
Réciproquement, soit $k = n^2 - n + 1$, et supposons que chacune des deux compagnies A et B gère k téléphériques. Puisque deux téléphériques gérés par A ont des stations de départ et d'arrivée différentes, il existe $n^2 - k = n - 1$ stations, que l'on notera $a_1 < a_2 < \ldots < a_{n-1}$, qui ne sont pas des stations d'arrivée de téléphérique.
Notons A_i l'ensemble des stations que l'on peut atteindre à partir de la station a_i en n'utilisant que des téléphériques gérés par la compagnie A. Une récurrence immédiate sur ℓ montre que toute station ℓ appartient à exactement un ensemble A_i, et que l'on peut aller d'une station ℓ à une station ℓ' si et seulement si $\ell' > \ell$ et si ℓ et ℓ' appartiennent à un même ensemble A_i.
On définit de même les stations $b_1 < b_2 < \ldots < b_{n-1}$ et les ensembles B_i, qui jouissent des mêmes propriétés.
Puisque toute station appartient à l'un des $n - 1$ ensembles A_i, et comme $(n-1)^2 < n^2$, l'un de ces ensembles, disons A_u, est de cardinal au moins n. Il existe donc un ensemble B_v qui contient au moins deux stations de A_u. Mais alors il est possible d'aller de la plus basse de ces stations à la plus haute, que ce soit en n'utilisant que des téléphériques gérés par la compagnie A ou des téléphériques gérés par la compagnie B.
Le plus petit entier recherché est donc $k = n^2 - n + 1$.

Solution des questions 2 et 4 proposées dans la RMS 130-2

Question 2. ***a)*** Vérifier que : $\forall n \in \mathbb{N}, \forall x \in \mathbb{R}, \mathrm{e}^x = \displaystyle\sum_{k=0}^{n} \frac{x^k}{k!} + \frac{\mathrm{e}^x}{n!} \int_0^x t^n \mathrm{e}^{-t} \mathrm{d}t.$

b) Montrer alors que pour tout $n \in \mathbb{N}^*$, $\displaystyle\sum_{k=0}^{n-1} \frac{n^k}{k!} \geqslant \mathrm{e}^{n-1}$, avec égalité si et seulement si $n = 1$.

Solution. ***a)*** Il s'agit d'une expression de la formule de Taylor avec reste intégral. Pour $n \in \mathbb{N}$, notons P_n la fonction polynôme $x \mapsto \displaystyle\sum_{k=0}^{n} \frac{x^k}{k!}$ et remarquons que : $\forall n \in \mathbb{N}^*$, $P_n' = P_{n-1}$.

Ainsi, pour tout $x \in \mathbb{R}$, $P_n(x) - P_n'(x) = P_n(x) - P_{n-1}(x) = \dfrac{x^n}{n!}$, ce qui reste vrai pour $n = 0$.

On a pour tout $n \in \mathbb{N}$ et pour tout $x \in \mathbb{R}$

$$\begin{aligned} \frac{\mathrm{d}}{\mathrm{d}x}\left(-\mathrm{e}^{-x} P_n(x)\right) &= \mathrm{e}^{-x} P_n(x) - \mathrm{e}^{-x} P_n'(x) = \mathrm{e}^{-x}\left(P_n(x) - P_n'(x)\right) \\ &= \mathrm{e}^{-x} \frac{x^n}{n!} \end{aligned}$$

et

$$\frac{\mathrm{d}}{\mathrm{d}x}\left(\frac{1}{n!}\int_0^x t^n \mathrm{e}^{-t} \mathrm{d}t\right) = \mathrm{e}^{-x}\frac{x^n}{n!}.$$

Il existe donc une constante $c \in \mathbb{R}$ telle que :

$\forall n \in \mathbb{N}, \forall x \in \mathbb{R},\ -\mathrm{e}^{-x} P_n(x) + c = \dfrac{1}{n!}\displaystyle\int_0^x t^n \mathrm{e}^{-t} \mathrm{d}t.$

Pour $x = 0$, on obtient : $c - 1 = 0$, donc $c = 1$.

Ainsi, $\forall n \in \mathbb{N}, \forall x \in \mathbb{R},\ 1 - \mathrm{e}^{-x} P_n(x) = \dfrac{1}{n!}\displaystyle\int_0^x t^n \mathrm{e}^{-t} \mathrm{d}t,$

d'où

$$\forall n \in \mathbb{N}, \forall x \in \mathbb{R}, \quad \mathrm{e}^x = P_n(x) + \frac{\mathrm{e}^x}{n!}\int_0^x t^n \mathrm{e}^{-t} \mathrm{d}t. \tag{1}$$

b) Soit $n \in \mathbb{N}^*$. Appliquons la formule (1) à l'ordre $n-1$ en posant $x = n$. On obtient :

$P_{n-1}(n) = \mathrm{e}^n - \dfrac{\mathrm{e}^n}{(n-1)!}\displaystyle\int_0^n \mathrm{e}^{-t} t^{n-1} \mathrm{d}t.$

L'inégalité à démontrer $P_{n-1}(n) \geqslant \mathrm{e}^{n-1}$ est alors équivalente à

$$\int_0^n \mathrm{e}^{-t} t^{n-1} \mathrm{d}t \leqslant (n-1)!\left(1 - \frac{1}{\mathrm{e}}\right) \tag{*}$$

Montrons par récurrence que l'inégalité $(*)$ est vraie pour tout $n \in \mathbb{N}^*$.

Si $n=1$, $\displaystyle\int_0^n \mathrm{e}^{-t}t^{n-1}\mathrm{d}t = \int_0^1 \mathrm{e}^{-t}\mathrm{d}t = \left[-\mathrm{e}^{-t}\right]_0^1 = 1-\frac{1}{\mathrm{e}}$ et
$(n-1)!\left(1-\dfrac{1}{\mathrm{e}}\right) = 1-\dfrac{1}{\mathrm{e}}$, ce qui vérifie $(*)$ pour $n=1$ (dans ce cas il y a égalité).

Supposons $(*)$ vraie pour un entier $n\in\mathbb{N}^*$. Calculons $\displaystyle\int_0^n \mathrm{e}^{-t}t^{n-1}\mathrm{d}t$ en intégrant par parties (on pose $u(t)=\mathrm{e}^{-t}$, $v'(t)=t^{n-1}$, d'où $u'(t)=-\mathrm{e}^{-t}$ et $v(t)=\dfrac{t^n}{n}$) :
$\displaystyle\int_0^n \mathrm{e}^{-t}t^{n-1}\mathrm{d}t = \left[\frac{t^n}{n}\mathrm{e}^{-t}\right]_0^n + \frac{1}{n}\int_0^n \mathrm{e}^{-t}t^n\mathrm{d}t = \frac{n^n\mathrm{e}^{-n}}{n} + \frac{1}{n}\int_0^n \mathrm{e}^{-t}t^n\mathrm{d}t.$
L'hypothèse de récurrence entraîne après multiplication des deux membres par n :

$$n^n\mathrm{e}^{-n} + \int_0^n \mathrm{e}^{-t}t^n\mathrm{d}t \leqslant n!\left(1-\frac{1}{\mathrm{e}}\right)\cdot \tag{2}$$

Or, $\displaystyle\int_0^{n+1} \mathrm{e}^{-t}t^n\mathrm{d}t = \int_0^n \mathrm{e}^{-t}t^n\mathrm{d}t + \int_n^{n+1} \mathrm{e}^{-t}t^n\mathrm{d}t.$
La fonction $t\mapsto \mathrm{e}^{-t}t^n$, ayant pour dérivée $t\mapsto \mathrm{e}^{-t}t^{n-1}\,(n-t)$, est strictement décroissante sur $[n,n+1]$, donc
$\displaystyle\int_n^{n+1} \mathrm{e}^{-t}t^n\mathrm{d}t \leqslant \int_n^{n+1} \mathrm{e}^{-n}n^n\mathrm{d}t = \mathrm{e}^{-n}n^n.$
Notons pour la suite que cette inégalité est stricte ; en effet, la fonction $t\mapsto \mathrm{e}^{-n}n^n - \mathrm{e}^{-t}t^n$ est continue, positive, non identiquement nulle puisque strictement croissante.
Ainsi, $\displaystyle\int_0^{n+1} \mathrm{e}^{-t}t^n\mathrm{d}t \leqslant \int_0^n \mathrm{e}^{-t}t^n\mathrm{d}t + \mathrm{e}^{-n}n^n$, donc d'après (2)

$$\int_0^{n+1} \mathrm{e}^{-t}t^n\mathrm{d}t \leqslant n!\left(1-\frac{1}{\mathrm{e}}\right),$$

ce qui prouve $(*)$ à l'ordre $n+1$. En conclusion $(*)$ est vraie pour tout $n\in\mathbb{N}^*$ et l'inégalité du texte est établie.
Ce qui précède montre que l'inégalité est stricte pour tout entier $n\geqslant 2$. Il y a donc égalité si et seulement si $n=1$.

Question 4. On note $\mathcal{M}_2(\mathbb{Z})$ l'ensemble des matrices 2×2 à coefficients dans $\mathbb{Z}$.
Soient $A=(a_{i,j})_{1\leqslant i,j\leqslant 2}$ et $B=(b_{i,j})_{1\leqslant i,j\leqslant 2}$ appartenant à $\mathcal{M}_2(\mathbb{Z})$ et $n\in\mathbb{N}\setminus\{0,1\}$. On écrit $A\equiv B \pmod n$ pour signifier que $\forall (i,j)\in\{1,2\}^2$, $a_{i,j}\equiv b_{i,j} \pmod n$. On pose $I_2=\begin{pmatrix}1&0\\0&1\end{pmatrix}$. Soient p un nombre premier et E l'ensemble des matrices $A=\begin{pmatrix}a&b\\c&d\end{pmatrix}$ telles que $(a,b,c,d)\in[\![0,p-1]\!]^4$ et il existe $A'\in\mathcal{M}_2(\mathbb{Z})$ vérifiant : $A\cdot A'\equiv I_2 \pmod p$.
Déterminer le cardinal de E.

Solution.
Remarque : Soit α un entier premier avec p. D'après le théorème de Bezout, il existe $\beta\in\mathbb{Z}$ tel que $\alpha\beta\equiv 1\ [p]$, autrement dit α est inversible modulo p.

Considérons deux entiers β, β' tels que $\alpha\beta \equiv 1\ [p]$ et $\alpha\beta' \equiv 1\ [p]$. Alors $\alpha\,(\beta - \beta') \equiv 0\ [p]$, donc $p \mid \alpha\,(\beta - \beta')$ et d'après le lemme de Gauss $p \mid \beta - \beta'$, i.e. $\beta \equiv \beta'\ [p]$. Il existe donc un unique élément de $[\![1, p-1]\!]$ que l'on note α_p^{-1} et nomme *l'inverse de α modulo p*, tel que $\alpha\alpha_p^{-1} \equiv 1\ [p]$.

Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$ et $A^* = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. On a : $AA^* = A^*A = \det A \cdot I_2$ où $\det A = ad - bc$, donc en réduisant modulo p, $AA^* = A^*A \equiv \det A \cdot I_2\ [p]$.
Montrons que A est inversible modulo p si et seulement si $\det A \not\equiv 0\ [p]$.
Si $\det A \not\equiv 0\ [p]$, soit $A' = (\det A)_p^{-1}\, A^*$. Alors,
$AA' = A'A = (\det A)_p^{-1} \det A \cdot I_2 \equiv I_2\ [p]$, donc A est inversible modulo p.
Si $\det A \equiv 0\ [p]$, on a $AA^* \equiv 0\ [p]$. Supposons A inversible modulo p, d'inverse A'. Alors $A'\,(AA^*) \equiv 0\ [p]$, d'où $(A'A)\,A^* \equiv 0\ [p]$, soit $A^* \equiv 0\ [p]$, donc $A \equiv 0\ [p]$. Le produit de A par toute matrice $B \in M_2(\mathbb{Z})$ étant nul modulo p, A n'est pas inversible modulo p, ce qui contredit l'hypothèse. Ainsi A n'est pas inversible modulo p. En prenant la contraposée, on obtient :
Si A est inversible modulo p, alors $\det A \not\equiv 0\ [p]$.

Il reste donc à déterminer le cardinal de l'ensemble E des quadruplets $(a, b, c, d) \in [\![0, p-1]\!]^4$ tels que $ad - bc \not\equiv 0\ [p]$.
Si $a \neq 0$, a est inversible modulo p. On peut choisir b et c arbitraires et d doit vérifier $d \not\equiv a_p^{-1}bc\ [p]$ pour que $ad - bc \not\equiv 0\ [p]$. Le nombre a étant donné, il y a p choix pour b, p choix pour c et $p-1$ choix pour d, donc $p^2(p-1)$ choix en tout. Le nombre d'éléments de E tels que $a \neq 0$ est donc $(p-1)p^2(p-1) = p^2(p-1)^2$.
Si $a = 0$, b et c doivent vérifier $bc \not\equiv 0\ [p]$ et d peut être choisi arbitrairement. Comme p est premier, la condition $bc \not\equiv 0\ [p]$ équivaut à $b \not\equiv 0\ [p]$ et $c \not\equiv 0\ [p]$, c'est-à-dire à $b \neq 0$ et $c \neq 0$, puisque $b, c \in [\![0, p-1]\!]$. Il y a donc $p-1$ choix pour b, $p-1$ choix pour c et p choix pour d. Le nombre d'éléments de E tels que $a = 0$ est donc $p(p-1)^2$.
Ainsi

$$\operatorname{card} E = p^2(p-1)^2 + p(p-1)^2 = (p-1)^2(p^2+p) = (p^2-1)(p^2-p).$$