Les problèmes de l'APMEP

Les propositions de problèmes, solutions ou commentaires, sont à envoyer à
Max HOCHART
13, rue des Garennes
63 800 Cournon d'Auvergne
ou
hochartmax@yahoo.fr

Énoncés des nouveaux problèmes

Problème 502–1 (Gauthier Gidel, Alexandre Benchaouine, Benoît Joly)

Soit $n \in \mathbb{N}^*$, $x_1, \ldots, x_n$ des réels strictement positifs et $p_1, \ldots, p_n$ des réels strictement positifs de somme 1. Pour tous les réels S et t vérifiant, pour tout $i \in [[1, n]]$,

$$\mathrm{S} \leq \sqrt{x_i} \leq \mathrm{S} + t,$$

montrer que

$$\frac{1}{\sum_{i=1}^{n} \frac{p_i}{x_i}} \leq \sum_{i=1}^{n} p_i x_i \leq \frac{1}{\sum_{i=1}^{n} \frac{p_i}{x_i}} + t^2.$$

Problème 502–2 (Michel Lafond (Dijon))

Soit p et q deux entiers premiers entre eux et impairs. Un damier rectangulaire $p \times q$ a ses cases colorées alternativement en noir et blanc, les quatre coins étant noirs. Une diagonale Δ est tracée. Une partie de Δ est noire, l'autre est blanche. Démontrer que la proportion de noir le long de Δ est égale à $\frac{1}{2}\left(1 + \frac{1}{pq}\right)$.

Problème 502–3 (Jean-Claude Blanchard (Brunoy))

Pour $n \in \mathbb{N}$, calculer le pgcd de $2^n + 3^n$ et de 5^n.

Problème 502–4 (G.L. Kocher, Ravières)

On suppose que le trinôme $ax^2 + bx + c$ possède deux racines réelles distinctes. En déduire les solutions de l'équation

$$a\left(ax^2 + (b+1)x + c\right)^2 + b\left(ax^2 + (b+1)x + c\right) + c - x = 0.$$

Solutions des problèmes antérieurs

Problème 493–2 (Question de Jean-Pierre Friedelmeyer)

Dans le plan euclidien, soit Γ un cercle de centre O, et soit U et V deux points distincts, alignés avec le centre O. À partir d'un point A du cercle Γ, on trace la droite (AU) qui recoupe Γ en un point B ; on trace la droite (BL) perpendiculaire à (UV) qui recoupe Γ en un point C ; on trace la droite (CV) qui recoupe Γ en un point A_1. Puis l'on recommence : on trace la droite (A_1U) qui recoupe Γ en un point B_1 ; on trace (B_1L_1) perpendiculaire à (UV) qui recoupe Γ en un point C_1 ; on trace (C_1V), etc. Est-il possible que la ligne polygonale $ABCA_1B_1C_1A_2B_2C_2$… se referme en un point A_n pour un entier naturel $_n$? Autrement dit, existe t-il $n \in \mathbb{N}$ tel que A_n soit confondu avec A?

Solutions de Jean-Pierre Friedelmeyer (Strasbourg), Georges Lion (Wallis), Pierre Renfer (Saint Georges d'Orques)

Les trois réponses reçues sont très proches et utilisent les homographies du plan projectif. Suivons par exemple **Georges Lion**. On peut supposer que le cercle Γ est le cercle trigonométrique. L'application définie par $A \mapsto A_1$ et donc toutes ses itérées $A \mapsto A_n$ sont des homographies du cercle Γ. On en connaît deux points fixes aux extrémités du diamètre porté par (UV). S'il existait un troisième point fixe, cette homographie serait l'identité. C'est cette situation que l'on va maintenant étudier.

La transformation projective définie par

$$x = \frac{1-X}{Y}, y = \frac{1+X}{Y}$$

envoie le cercle Γ d'équation $X^2 + Y^2 = 1$ sur l'hyperbole h d'équation $xy = 1$.

Les points P et Q, extrémités du diamètre de Γ contenant U et V, deviennent p et q à l'infini sur les asymptotes de h, d'équations $x = 0$ et $y = 0$, tandis que U et V ont pour images u et v à l'infini également.

Si a, b, c, a_1 sont les images de A, B, C, A_1, m le milieu de $[ab]$, ω le centre de h, alors les droites (ωm) et (ab) ont des coefficients directeurs opposés. Ainsi il existe $\alpha \neq 0$ tel que l'application $\overrightarrow{\omega a} \mapsto \overrightarrow{\omega b}$ ait une matrice du type

$$\begin{pmatrix} 0 & \frac{1}{\alpha} \\ \alpha & 0 \end{pmatrix}$$

De même, l'application $\overrightarrow{\omega c} \mapsto \overrightarrow{\omega a_1}$ a pour matrice (où $\beta \neq 0$)

$$\begin{pmatrix} 0 & \frac{1}{\beta} \\ \beta & 0 \end{pmatrix}.$$

Enfin à la symétrie orthogonale d'axe (PQ) correspond la symétrie de centre ω.

L'application $\overrightarrow{\omega a} \mapsto \overrightarrow{\omega a_1}$ possède alors pour matrice

$$\begin{pmatrix} -\dfrac{\alpha}{\beta} & 0 \\ 0 & -\dfrac{\beta}{\alpha} \end{pmatrix}.$$

Cette application est donc l'identité si et seulement si $\beta = -\alpha$, c'est-à-dire si et seulement si (au) et (cv) ont des directions conjuguées par rapport aux asymptotes, ou encore si et seulement si $[\mathrm{P}, \mathrm{Q}, \mathrm{U}, \mathrm{V}\,] = [p, q, u, v] = -1$.

Soit n entier > 1. L'application $\overrightarrow{\omega a} \mapsto \overrightarrow{\omega a_n}$ a pour matrice

$$\begin{pmatrix} \left(-\dfrac{\alpha}{\beta}\right)^n & 0 \\ 0 & \left(-\dfrac{\beta}{\alpha}\right)^n \end{pmatrix}$$

et vaut I si et seulement si $\alpha = -\beta$.

En conclusion, la ligne polygonale $\mathrm{A}\ldots\mathrm{A}_1\ldots\mathrm{A}_n$ est fermée si et seulement si $\mathrm{A} = \mathrm{A}_1$ et cela se produit seulement lorsque U et V sont conjugués par rapport à Γ.

Jean-Pierre Friedelmeyer apporte quelques précisions sur cet énoncé. Il écrit : « le problème m'a été inspiré comme cas particulier du problème de Castillon(1) dont je rappelle l'énoncé : on donne un cercle (O) et trois points U, V, W de son plan ; construire un triangle ABC inscrit au cercle, dont les côtés respectifs passent par les trois points.

Le problème a en général au maximum deux solutions, sauf lorsque les trois points donnés définissent un triangle autopolaire, auquel cas il y a une infinité de solutions obtenues en partant d'un point quelconque (par exemple A) du cercle.

Il s'en déduit un problème de fermeture : on donne un cercle (O) et trois points U, V, W de son plan. À partir d'un point A quelconque du cercle, on trace (AU) qui recoupe le cercle en B ; on trace (BV) qui recoupe le cercle en C ; on trace (CW) qui recoupe le cercle en A_1, etc. La ligne polygonale $\mathrm{ABCA}_1\mathrm{B}_1\mathrm{C}_1\mathrm{A}_2\ldots$ se ferme t-elle en un point A_n pour un certain entier naturel non nul n ?

Le problème proposé en est un cas particulier, où U et V sont alignés avec le centre et W est le point à l'infini, pôle du diamètre passant par U et V.

(1) Castillon, de son vrai nom Francesco Melchiore Salvemini (1704-1791) a publié ce problème et sa solution dans les Nouveaux Mémoires de l'Académie Royale des Sciences et Belles Lettres de Berlin, en 1776 sous le titre : « Sur un problème de géométrie plane qu'on regarde comme fort difficile. » Voir par exemple le livre de Marcel Berger, Géométrie, II, 16.3.10.3., Nathan, 1990.

Le problème de Castillon a été généralisé au début du 19e siècle de trois manières : en remplaçant le cercle par une conique quelconque, en demandant d'inscrire un polygone d'un nombre N de côtés passant par N points donnés, en posant le problème dual, c'est-à-dire : circonscrire un polygone de N côtés à une conique, dont les sommets soient situés sur N droites données. Ce qui fait que ce problème est alors représentatif des méthodes de la géométrie projective naissante. Sa solution moderne repose sur la détermination des points fixes d'une homographie. »

Problème 496–2

Pour $n \in \mathbb{N}$ et $k \in [[0, n]]$, on note $\binom{n}{k}$ le coefficient binomial $\frac{n!}{k!(n-k)!}$. Pour tout nombre premier p, établir les relations suivantes :

1. $\binom{p-1}{k} \equiv (-1)^k \mod p$ pour tout entier $k \in [\![0, p-1]\!]$;
2. $\binom{p+1}{k} \equiv 0 \mod p$ pour tout entier $k \in [\![2, p-1]\!]$;
3. $\binom{2p}{p} \equiv 2 \mod p$;
4. $\binom{pa}{pb} \equiv \binom{a}{b} \mod p$ pour $a, b \in \mathbb{N}$ avec $a \geq b$.

Solutions de Jean-Claude Carréga (Strasbourg), Bernard Collignon (Coursan), François Couloigner (Tarbes), Paul Péchoux, Pierre Renfer (Saint Georges d'Orques)

Pour aborder cet énoncé (tiré d'un problème Putnam posé en 1977), **Jean-Claude Carréga**, **Bernard Collignon**, **Paul Péchoux** et **Pierre Renfer** utilisent des relations classiques sur les coefficients binomiaux, et des factorisations astucieuses (dans la question 4 en particulier). **François Couloigner** dessine un très joli triangle de Pascal où les coefficients binomiaux apparaîssent modulo p et en déduit des résultats. **Bernard Collignon** travaille aussi dans l'anneau des polynômes à coefficients dans le corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ pour quelques questions. On verra que cette méthode apporte toutes les réponses.

Commençons par l'approche purement arithmétique. Le premier point peut être établi par récurrence sur k. Le résultat étant clair pour $k = 0$, on suppose que la relation

$$\binom{p-1}{k} \equiv (-1)^k \mod p$$

est vraie pour un certain k entre 0 et $p - 2$. Alors

$$\binom{p-1}{k+1} = \binom{p}{k+1} - \binom{p-1}{k}.$$

Classiquement, p divise $\binom{p}{k+1}$, par le lemme de Gauss appliqué à la relation

$$(k+1)\binom{p}{k+1} = p\binom{p-1}{k},$$

puisque $k+1$ est premier à p. Donc

$$\binom{p-1}{k+1} \equiv -\binom{p-1}{k} \equiv (-1)^{k+1} \mod p,$$

ce qui termine la récurrence. Mais nul besoin de récurrence, puisque le lemme de Gauss donne aussitôt le résultat. Soit $k \in [[0, p-1]]$. Par définition,

$$\binom{p-1}{k} = \frac{(p-1)(p-2)\ldots(p-k)}{k!},$$

soit encore

$$k!\binom{p-1}{k} = (p-1)(p-2)\ldots(p-k).$$

On réduit modulo p :

$$k!\binom{p-1}{k} \equiv (-1)^k k! \mod p.$$

Comme k appartient à $[[0, p-1]]$, $k!$ admet un inverse modulo p, et ainsi

$$\binom{p-1}{k} \equiv (-1)^k \mod p.$$

Le second point s'obtient de la même façon : pour $k \in [[2, p-1]]$,

$$k!\binom{p+1}{k} = (p+1)p\ldots(p-k+2) \equiv 0 \mod p,$$

et l'on conclut par le lemme de Gauss.
Pour le troisième point,

$$(p-1)!\binom{2p}{p} = 2(2p-1)\ldots(p+1),$$

donc

$$(p-1)!\binom{2p}{p} \equiv 2(-1)(-2)\ldots(-p+1) \equiv 2(-1)^{p-1}(p-1)! \mod p,$$

et l'on peut simplifier par $(p-1)!$ qui est premier à p (ou invoquer le théorème de Wilson : $(p-1)! \equiv -1 \mod p$).

Pour le dernier point, on peut écrire

$$(pa)! = \prod_{i=1}^{a}\left(pi\prod_{j-1}^{p-1}(pi-j)\right) = p^a a!\prod_{i=1}^{a}\mathrm{P}_i \text{ avec } \mathrm{P}_i = \prod_{j-1}^{p-1}(pi-j),$$

Ainsi,

$$\binom{pa}{pb} = \frac{p^a a!\prod_{i=1}^{a}\mathrm{P}_i}{p^{a-b}(a-b)!\prod_{i=1}^{a-b}\mathrm{P}_i \times p^b b!\prod_{i=1}^{b}\mathrm{P}_i} = \binom{a}{b}\frac{\prod_{i=b+1}^{a}\mathrm{P}_i}{\prod_{i=1}^{a-b}\mathrm{P}_i}.$$

Ainsi,

$$\left(\prod_{i=1}^{a-b}\mathrm{P}_i\right)\binom{pa}{pb} = \left(\prod_{i=b+1}^{a}\mathrm{P}_i\right)\binom{a}{b}.$$

Or, par définition,

$$\mathrm{P}_i = \prod_{j-1}^{p-1}(pi-j) \equiv (-1)^{p-1}(p-1)! \equiv (p-1!) \quad \text{mod } p.$$

Ainsi,

$$\left((p-1)!\right)^{a-b}\binom{pa}{pb} \equiv \left((p-1)!\right)^{a-b}\binom{a}{b} \quad \text{mod } p,$$

et l'on peut simplifier par $((p-1)!)^{a-b}$.

Voici maintenant l'approche consistant à travailler dans $\mathbb{F}_p[\mathrm{X}]$. La relation

$$(\mathrm{X}+1)^p = \mathrm{X}^p + \sum_{j=1}^{p-1}\binom{p}{j}\mathrm{X}^j + 1 \quad \text{dans } \mathbb{Z}[\mathrm{X}]$$

donne alors, puisque p divise $\binom{p}{j}$ pour $1 \leq j \leq p-1$,

$$(\mathrm{X}+1)^p = \mathrm{X}^p + 1 \quad \text{dans } \mathbb{F}_p[\mathrm{X}]. \tag{1}$$

On revient sur la première question. On peut écarter le cas $p = 2$, qui se traite à la main. On suppose donc $p \geq 3$ et, en particulier, p est impair. Alors, dans $\mathbb{F}_p[\mathrm{X}]$,

$$(\mathrm{X}+1)^p = \mathrm{X}^p + 1 = \mathrm{X}^p - (-1)^p = (\mathrm{X}+1)\left(\sum_{j=0}^{p-1}(-1)^{p-j-1}\mathrm{X}^j\right).$$

Puisque $p-1$ est pair, $(-1)^{p-1-j} = (-1)^j$. Par simplification par $\mathrm{X}+1$, on obtient

$$\sum_{k=0}^{p-1}\binom{p-1}{k}\mathrm{X}^k = \sum_{j=0}^{p-1}(-1)^j\mathrm{X}^j \quad \text{dans } \mathbb{F}_p[\mathrm{X}].$$

Par identification des coefficients,

$$\binom{p-1}{k} = (-1)^k \quad \text{dans } \mathbb{F}_p,$$

c'est-à-dire que

$$\binom{p-1}{k} \equiv (-1)^k \mod p.$$

On en vient au second point. On multiple l'égalité (1) par X + 1 :

$$\sum_{k=0}^{p+1} \binom{p+1}{k} \mathrm{X}^k = (\mathrm{X}+1)^{p+1} = (\mathrm{X}+1)(\mathrm{X}^p+1) = \mathrm{X}^{p+1} + \mathrm{X}^p + \mathrm{X} + 1.$$

De nouveau, par identification des coefficients, on obtient, pour $k \in [[2, p-1]]$,

$$\binom{p+1}{k} \equiv 0 \mod p.$$

Le troisième point n'est qu'un cas particulier du dernier point, en prenant $a = 2$ et $b = 1$. On montre donc directement ce dernier point. Par la formule du binôme, on a, dans $\mathbb{F}_p[\mathrm{X}]$,

$$\sum_{k=0}^{pa} \binom{pa}{k} \mathrm{X}^k = (\mathrm{X}+1)^{ap} = \left((\mathrm{X}+1)^p\right)^a = (\mathrm{X}^p+1)^a = \sum_{j=0}^{a} \binom{a}{j} \mathrm{X}^{pj}.$$

On fixe maintenant $k \in [[0, ap]]$. Si p ne divise pas k, $\binom{pa}{k} \equiv 0 \mod p$. Sinon, p divise k et l'on écrit $k = pb$. Alors

$$\binom{pa}{pb} \equiv \binom{a}{b} \mod p.$$

Bernard Collignon signale que la dernière congruence est une simple conséquence du théorème de Lucas : en désignant toujours par p un nombre premier et par n, k des entiers tels que $0 \le k \le n$ dont les écritures en base p sont

$$n = \sum_{j=0}^{r} n_j p^j$$

et

$$k = \sum_{j=0}^{r} k_j p^j,$$

alors

$$\binom{n}{k} = \binom{n_r}{k_r}\binom{n_{r-1}}{k-1}\cdots\binom{n_0}{k_0} \mod p.$$

Ce théorème peut être établi en travaillant de nouveau dans $\mathbb{F}_p[\mathrm{X}]$:

$$\sum_{k=0}^{n}\binom{n}{k}X^k=(X+1)^n=(X+1)^{\sum_{j=0}^{r}n_jp^j}=\prod_{j=0}^{r}\left((X+1)^{p^j}\right)^{n_j}.$$

Or une application successive de la relation

$$(X+1)^p=X^p+1$$

donne

$$(X+1)^{p^2}=\left((X+1)^p\right)^p=\left(X^p+1\right)^p=X^{p^2}+1$$

et plus généralement, pour tout $\alpha\in\mathbb{N}$,

$$(X+1)^{p^\alpha}=X^{p^\alpha}+1$$

Ainsi,

$$\sum_{k=0}^{n}\binom{n}{k}X^k=\prod_{j=0}^{r}\left(X^{p^j}+1\right)^{n_j}=\prod_{j=0}^{r}\left(\sum_{s=0}^{n_j}\binom{n_j}{s}X^{sp^j}\right).$$

Maintenant, par identification des coefficients dans $\mathbb{F}_p$, l'unicité de la décomposition d'un entier en base p donne aussitôt, pour

$$k=\sum_{s=0}^{r}k_sp^s,$$

l'égalité

$$\binom{n}{k}=\prod_{s=0}^{r}\binom{n_s}{k_s}\quad\operatorname{mod}p,$$

comme annoncé.

On retrouve alors la dernière congruence de l'énoncé ainsi : pour deux entiers naturels $a\geq b\geq 0$, donnés en base p par

$$a=\sum_{s=0}^{r}a_sp^s\quad\text{et}\quad b=\sum_{s=0}^{r}b_sp^s,$$

alors

$$ap=\sum_{s=0}^{r}a_sp^{s+1}\quad\text{et}\quad bp=\sum_{s=0}^{r}b_sp^{s+1},$$

donc

$$\binom{ap}{bp}=\prod_{s=0}^{r}\binom{a_s}{b_s}\times\binom{0}{0}\equiv\binom{a}{b}\quad\operatorname{mod}p.$$