# Rubrique des problèmes de l'A.P.M.

Cette rubrique est pour le plaisir, celui qui nous fait choisir les mathématiques à vingt ans, et non directement pour notre enseignement.

Le niveau ne doit pas excéder celui des classes préparatoires ou des deux premières années de faculté. Un certain caractère d'originalité dans l'énoncé est souhaité, ce qui exclut, en particulier, les applications immédiates de théorèmes classiques, ou les problèmes déjà parus dans d'autres revues.

Si l'auteur d'un énoncé n'est pas en mesure d'en donner la solution, il doit accompagner son envoi du maximum d'informations concernant le problème, afin d'aider les responsables de la rubrique. Un astérisque signale un problème dont la solution n'est pas connue de ceux-ci. Le bulletin publie les meilleures solutions.

Enoncés et solutions sur feuilles séparées et tapées à la machine S.V.P. N'oubliez pas de signer. Toute correspondance concernant la rubrique est à adresser à :

Gérard LETAC
Rubrique des problèmes
I.U.T. de Clermont
B.P. 29
63 — Aubière

Les solutions des problèmes suivants doivent nous parvenir avant le 1.3.1973.

*Enoncé n° 22* (J. LAGRANGE, Faculté des Sciences de Reims)

Soient n et s deux entiers strictement positifs, $r_s(n)$ le nombre de solutions dans $Z^s$ de l'équation

$$x_1^2 + x_2^2 + \dots + x_s^2 = n\ ;$$

autrement dit, $r_s(n)$ est le nombre de décompositions de n en somme de s carrés. Montrer que si n est premier à s, $r_s(n)$ est divisible par 2s.

Exemple : $r_3(1) = 6$ car

$$1 = 1^2 + 0 + 0 = (-1)^2 + 0 + 0 = 0 + 1^2 + 0 = \dots$$

*Enoncé n° 23* (M. BOURDEAU — Etudiant à Sherbrooke — Québec)

Soit n un entier $\geqslant 6$. Si $a$ , $a_1$ , ..., $a_n$ sont des entiers $\geqslant 0$, on pose

$$P(X) = \sum_{k=0}^{n} X^{a_k}$$

Si P(X) est identique à $\sum_{k=0}^{n} a_k \ X^k$, alors :

$$P(X) = (n-3) + 2X + X^2 + X^{n-3}.$$

*Enoncé n° 24* (Communiqué par M. VIDIANI, Lycée Berthollet, Annecy)

Un sultant décide qu'après sa mort, les f femmes de son harem seront à partager entre ses m ministres de la façon suivante :

Le premier ministre choisira d'abord la plus belle femme puis le (1/k)ième de ce qui restera ensuite. Dans ce qui restera ensuite une fois que toutes les femmes du premier ministre auront été désignées, le deuxième ministre choisira les deux plus belles femmes puis prendra le (1/k)ième de ce qui restera ensuite. De même le troisième ministre choisira dans celles qui resteront les trois plus belles femmes puis prendra le (1/k)ième de ce qui restera, et ainsi de suite jusqu'au dernier ministre.

Quels sont les triplets (f, m, k) possibles ?

*Enoncé n° 25* ( A. BLANCHARD — Faculté des Sciences de Marseille)

Il n'est pas possible de répartir les entiers positifs en un nombre fini de progressions arithmétiques dont l'une soit de raison strictement supérieure aux raisons de toutes les autres.

*Enoncé n° 12* (L. COMTET, Faculté des Sciences d'Orsay)

Soit S(p, k) le nombre de partitions en k classes d'un ensemble à p éléments (ou nombre de Stirling de 2ème espèce : voir l'article de M. Glaymann, A.P.M., Janvier-Février 1971 — Page 87). Si p est premier, montrer que p divise les S(p, k), si $2 \leqslant k \leqslant p-1$.

*Solution de J. CHONÉ* (L.E.M. Thiers)

Raisonnons par récurrence sur k.

1°) Etude du cas où k = 2.

En dénombrant de deux façons les applications surjectives d'un ensemble contenant p éléments dans l'ensemble $\{0, 1\}$ on obtient la formule :

$$2.S(p, 2) = 2^p - 2$$

Le théorème de Fermat permet de dire que p divise $2^p - 2$.

Donc, p étant un nombre premier strictement supérieur à 2, p divise S(p, 2).

2°) Supposons que la proposition soit vraie pour tout k' compris entre 2 et $(k-1)$. Montrons qu'elle est vraie pour k , $(3 \leqslant k \leqslant p-1)$ ; posons $n = p + k$.

Il y a $n^p$ applications d'un ensemble $E_p$ ayant p éléments dans un ensemble $E_n$ ayant n éléments. Mais on peut aussi dénombrer ces applications suivant le nombre i d'éléments de $E_n$ ayant au moins un antécédent; il y a $S(p, i)$ façons de grouper en i parties non vides les éléments de $E_n$ et il y a

$$n(n-1) \dots (n-i+1) = (n)_i$$

façons d'envoyer ces i parties sur i éléments de $E_n$.

D'où :

$$n^p = \sum_{i=1}^{p} S(p, i)\ (n)_i$$

A partir de $i = k + 1$, $(n)_i$ contient un facteur p ; donc, dans Z/pZ, la classe de $n^p$ est égale à celle de $\sum_{i=1}^{k} S(p, i)\ (n)_i$ :

$$\overline{n^p} = \sum_{i=1}^{k} \overline{S(p, i)\ (n)_i} \quad \text{dans } Z/pZ.$$

L'hypothèse de récurrence montre que :

$$\overline{n^p} = \overline{S(p, 1).n} + \overline{S(p, k)\ (n)_k} \text{ dans } Z/pZ.$$

Le fait que $S(p, 1) = 1$ et le théorème de Fermat montrent que :

$$\overline{S(p, k)}\ \overline{(p+k)\ (p+k-1) \dots (p+1)} = \overline{0} \text{ dans } Z/pZ.$$

p étant premier et $k \leqslant p - 1$, on obtient enfin

$$\overline{S(p, k)} = \overline{0} \quad \text{dans } Z/pZ$$

c'est-à-dire que p divise $S(p, k)$.

*Solution de P. BELLIVIER* (Lorgues)

D'après la formule

$$S_{p,k} = \frac{1}{k!} \sum_{j=1}^{k} (-1)^{k-j} C_k^j\, j^p,$$

on voit que :

$$S_{p,k} = \frac{1}{k!} \sum_{j=1}^{k} (-1)^{k-j} C_k^j\, j$$

car, p étant premier, un théorème de Fermat nous permet de dire que

quel que soit j, $j^p \equiv j \pmod p$

$$\text{Or } \sum_{j=1}^{k} (-1)^{k-j} C_k^j \times j = \left\{\text{Dérivée de } (1+x)^k\right\}_{x=-1} = \left\{k(1+x)^{k-1}\right\}_{x=-1} = 0$$

Donc $S_{p,k} \equiv 0 \pmod p$.

*Autres solutions de :* R. Cuculière (CPR, Paris — Nord), J. Legrand (Bordeaux), Mme M. Malléus (I.U.T. Avenue de Versailles, Paris), G. Vilhosc (Nice) et l'auteur.

Quelques solutions erronées par suite d'une faute d'impression dans l'article de M. Glaymann. La solution de G. Vilhosc utilise des nombres de Stirling de 1ère espèce, dont la matrice est inverse de celle de ceux de 2ème espèce.

*Enoncé n° 14* (Gérard LETAC — I.U.T. de Clermont)

Soit f une fonction continue sur les réels positifs. Le célèbre lemme de Croft affirme que si pour tout x la suite $(f(nx))_{n\geq 1}$ possède une limite si $n\to\infty$, il en est de même pour f(x) si $x \to \infty$. Peut-on dire que si pour tout x la suite $(f(nx))_{n\geq 1}$ est monotone (ou bien bornée supérieurement), alors la fonction f(x) est monotone (ou bien bornée supérieurement) sur les réels positifs ?

*Solution par Georges VILHOSC* (Nice)

La première propriété est immédiate. Du fait que f est continue et que les rationnels positifs sont denses dans $[0, \infty]$, il suffit de voir que si $(f(nx))_{n=1}^{\infty}$ est une suite non décroissante pour tout x et si $\frac{p}{q}$ et $\frac{p'}{q'}$ sont deux nombres rationnels tels que $\frac{p}{q} \leqslant \frac{p'}{q'}$ alors

$f(\frac{p}{q}) = f(\frac{pq'}{qq'}) \leqslant f(\frac{p'q}{qq'}) = f(\frac{p'}{q'})$. La seconde propriété est plus profonde :

*Théorème :* f étant continue sur $[0, +\infty]$ on suppose que pour tout x la suite $(f(nx))_{n=1}^{\infty}$ est bornée supérieurement. Alors f(x) est bornée supérieurement.

*Démonstration :* Soit N un entier, on pose :

$$F_N = \{x \,;\, f(nx) \leqslant N \text{ pour tout } n = 1, 2 \dots\}$$

Par hypothèse $\bigcup_{N=1}^{\infty} F_N = [0,\infty]$. Comme f est continue, $F_N$ est fermé, et d'après le théorème de Baire, il existe $N_0$ tel que $F_{N_0}$ contienne un intervalle, disons (a, b). Or il est évident que pour tous entiers n et N, on a $n F_N \subset F_N$, ce qui entraîne :

$$\bigcup_{n=1}^{\infty} (na, nb) \subset F_{N_0}$$

Un petit calcul montre que $(\frac{ab}{b-a}, \infty) \subset \bigcup_{n=1}^{\infty} (na, nb)$. Donc $f(x) \leqslant N_0$ si $x > ab/(b-a)$, ce qui achève la démonstration.

Autres solutions de Pierre MAMEL (étudiant à Poitiers), Christiane LECCIA (C.P.R. Paris) et l'auteur.

*Enoncé n° 15* (J. LEGRAND — Faculté des Sciences de Bordeaux)

Soit $n = a^p + (a+1)^p$ où a est un entier positif et p un nombre premier impair. Montrer que si $n \neq 9$, n possède au moins un diviseur premier q tel que $q \equiv 1 \pmod{2p}$. En déduire qu'il existe une infinité de nombres premiers de la forme $2pk + 1$ (avec k entier).

*Solution de André WARUSFEL* (Paris)

1) Soit q un diviseur de n, et $\alpha = \frac{1-n}{a}$ qui est un entier. On a $a\alpha \equiv 1$ [q] , $(1+\alpha)^p \equiv (a+1)^p \alpha^p \equiv -a^p \alpha^p \equiv -1$ [q] .

$1+\alpha$ est un élément de $(Z/qZ)^*$, son ordre ne divise pas p, mais divise 2p car $(1+\alpha)^{2p} \equiv 1$ [q] . C'est donc 2 ou 2 p. S'il est égal à 2p — ce qui est notamment le cas pour p = 2 —, alors 2p divise le cardinal $q-1$ de $F_q^*$, d'où $q = 2lp + 1$.

2) Supposons donc que cet ordre soit égal à 2 pour tous les diviseurs premiers de n. p est alors impair. On a :

$(1+\alpha)^2 \equiv 1$ [q] , $(a+1)^2 \equiv (1+\alpha)^2 a^2 \equiv a^2$ [q] , $2a+1 \equiv 0$ [q] .

Tout diviseur premier de n divise 2a + 1.

3) 2a + 1 divise n, car :

$$\frac{n}{2a+1} = \sum_{k=0}^{p-1} (a+1)^k (-a)^{p-k-1}$$

On a facilement les congruences :

$$(a+1)^k - (-a)^k \equiv (-a)^{p-k-1} - (a+1)^{p-k-1} \equiv 0 \qquad [2a+1]$$

d'où :

$$\frac{n}{2a+1} \equiv p(-a)^{p-1} \equiv p(a+1)^{p-1} \qquad [2a+1]$$

4) Notons que $n = a^p + (a+1)^p > a + (a+1)$. Tout diviseur premier q de $\frac{n}{2a+1}$ — il en existe — divise n, donc 2a + 1, donc également $pa^{p-1}$ et $p(a+1)^{p-1}$ ; q est nécessairement égal à p, d'où $n = (2a+1)p^h$ ($h \geqslant 1$). L'entier p, divisant n, divise donc aussi 2a+1 d'où $a \geqslant \frac{p-1}{2}$ . Posons $2a+1 = \lambda p$ :

$(\lambda p-1)^p + (\lambda p+1)^p = (2a)^p + (2a+2)^p = 2^p n = \lambda 2^p p^{h+1}$ .

$\lambda p^{h+1}$ divise dont l'entier :

$$(\lambda p-1)^p + (\lambda p+1)^p = 2\lambda p^2 + 2 \sum_{s=0}^{\frac{p-3}{2}} \binom{p}{2s} \lambda^{p-2s} p^{p-2s} \equiv 2p^2 \ [\lambda p^3]$$

Par suite $h + 1 \leqslant 2$, et $h = 1$.

5) La relation $n = (2a + 1)p$ est impossible pour $n \neq 9$. En effet, pour $a \geqslant 2$ on a :

$n = a^p + (a+1)^p > a^p + (a^p + pa) \geqslant 2(2^{p-1})\,a + pa > 3pa > (2a+1)p$

Pour $a = 1$, ce qui donne $1 \geqslant \frac{p-1}{2}$ ou $p = 3$, on a $n = 9$.

D'où le résultat.

*Conséquence :* Pour tout nombre entier p, il existe une infinité de nombres premiers q de la forme $2kp + 1$.

Considérons en effet le produit a des nombres de ce type, s'il n'en existe qu'un nombre fini. Le cas $p = 3$ et $a = 1$ est exclu, puisque $7 \equiv 1\ [6]$. La démonstration précédente prouve l'existence d'un diviseur premier $q = 2kp + 1$ de n. Par hypothèse, q divise également a, d'où une contradiction ($n \equiv 1\ [a]$).

Remarque : Le paragraphe 1 et la démonstration du corollaire prouvent donc, de manière très courte, l'existence d'une infinité de nombres premiers de la forme $4K + 1$ (ici $\alpha = -2a - 2$).

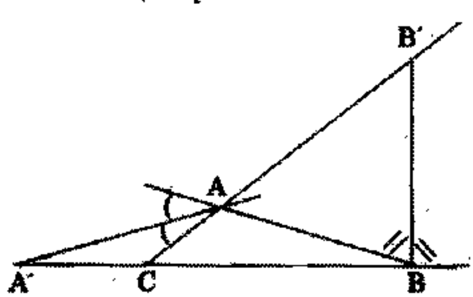
*Autres solutions* de Charles AUQUES (Mathématiques, Université de Clermont), Gilbert BLANCHARD (Marseille), Roger CUCULIERE (C.P.R. Paris-Nord), Christian RADOUX (Libramont, Belgique) et l'auteur.

A. WARUSFEL remarque que si on vise seulement la dernière partie, il est plus simple de considérer $n = (a + 1)^p - a^p$ dont *tous* les diviseurs premiers q sont de la forme $2kp + 1$. En effet $n \equiv 0 \mod q$ entraîne l'existence d'un entier c tel que $c^p \equiv 1 \mod q$ ce qui entraîne que p divise l'ordre du groupe multiplicatif $(Z/qZ)^*$.

*Enoncé n° 16* (J. LAGRANGE, Faculté des Sciences de Reims).

"En utilisant seulement le premier livre d'Euclide, montrez l'existence d'un triangle non isocèle ayant deux bissectrices extérieures égales".

*Solution de R. MAILLARD,* Inspecteur Général Honoraire.



La question posée admet une infinité de solutions. En voici une qui me paraît simple. Les mesures des angles du triangle ABC choisi sont respectivement : $\widehat{A} = 132^o, \widehat{B} = 12^o, \widehat{C} = 36^o$.
(j'écris $\widehat{A}$ pour mesure en degrés de l'angle $\widehat{BAC}$ , etc...)

La bissectrice extérieure AA' coupe la droite BC en A' (C entre B et A' parce que $\widehat{CAA'} < \widehat{ACB}$) et l'on a :

$\widehat{CAA'} = 24^o$, $\widehat{ACA'} = 144^o$ donc $\widehat{AA'C} = 12^o$. Par suite AA' = AB

La bissectrice extérieure BB' coupe la droite AC en B' (A entre B' et C parce que $\widehat{ABB'} < \widehat{BAC}$) et l'on a :

$\widehat{BAB'} = 48^o$, $\widehat{ABB'} = 84^o$ donc $\widehat{AB'B} = 48^o$. Par suite BB' = AB

On en conclut AA' = BB'.

Compléments :

D'une manière générale, on pourrait traiter la question par le calcul. BC = a, AC = b, AB = c

$$AA'^2 = bc\,\frac{a^2 - (b-c)^2}{(b-c)^2}\ , \qquad BB'^2 = ca\,\frac{b^2 - (a-c)^2}{(a-c)^2}$$

En écrivant $AA'^2 = BB'^2$ , on trouve bien sûr a = b et une autre relation que l'on transforme aisément en posant :

$ab = x, \quad a + b = c + 2y$

et l'on trouve $\quad xy + c^2 y - cx = 0$

On démontre alors les relations :

$$\sin\frac{C}{2} = \frac{y}{c} \text{ et } \sin\frac{2C}{2} = \sin\frac{A}{2}\,\sin\frac{B}{2}$$

Ceci permet d'établir qu'entre les distances IA, IB, IC du centre du cercle inscrit aux sommets A, B, C il existe la relation

$IC^2 = IA.IB$

et que l'angle C est inférieur à $60^o$ (si $C = 60^o$ , ABC est équilatéral).

Je ne crois pas utile de donner les démonstrations car elles sont faciles.

Exemples :

$1^o)\ \sin\frac{C}{2} = \frac{1}{4}\ , \quad y = \frac{c}{4}\ , \quad x = \frac{c^2}{3}$

$$ab = \frac{c^2}{3}\ , \quad a + b = \frac{3c}{2}$$

a et b sont racines de l'équation $X^2 - \frac{3c}{2}X + \frac{c^2}{3} = 0$.

2°) $\sin \frac{C}{2} = \frac{\sqrt{5}-1}{4}$

On trouve facilement $\cos 2C = \sin \frac{C}{2}$ d'où $C = 36°$ et l'on retrouve ke cas simple traité élémentairement.

*Autres solutions* de A. MARCADRÉ (I.U.T. de Reims) et de l'auteur.

*Enoncé n° 18* (G. LETAC, I.U.T. de Clermont)

Si S est un ensemble d'entiers relatifs, on note $S_k$ l'ensemble des entiers de la forme $s_1 + s_2 + \dots + s_k$, avec $s_i \in S$ pour tout $i = 1,2 \dots k$. Montrer que S a au moins 2n éléments lorsque

$0 \notin \bigcup_{1 \leqslant k < np} S_k$ et $S \subset S_{q+1}$, q et n étant des entiers positifs.

*Solution de R. LAFRAMBOISE* (Collège de Watawata, Québec).

*Lemme 1 :* Soit $A \subset S$ et $f : A \to A$
telle que $s - f(s) \in S_q$ pour tout s de A.
Alors $f^{(p)}(s_o) = s_o$ entraîne $p \geqslant n$ ; ($f^{(p)}$ = $p^{\text{ième}}$ itérée de f).

*Démonstration :*

$0 = s_o - f^{(p)}(s_o) = (s_o - f(s_o)) + (f(s_o) - f^{(2)}(s_o)) + \dots + (f^{(p-1)}(s_o) - f^{(p)}(s_o)) \in S_{pq}$

Donc $pq \geqslant nq$ et $p \geqslant n$.

*Lemme 2 :* Soit G un semi-groupe de Z tel que $A = S \setminus G$ soit non vide. Alors il existe $f : A \to A$ tel que $s - f(s) \in S_q$, pour tout s de A, et $|A| \geqslant n$.

*Démonstration :* Comme $S \setminus G \subset S_{q+1}$, tout s de $S \setminus G$ s'écrit :
$s = s_1 + \dots + s_{q+1}$: Si $s_i \in G$ pour tout i, s aussi. C'est impossible, donc il existe i tel que $s_i \in S \setminus G$, et on pose $f(s) = s_i$. Le fait que $|A| \geqslant n$ découle alors du lemme 1.

Appliquons le lemme 2 à G = N. S possède des éléments négatifs car $S \subset S_{q+1}$. Donc S comporte au moins n éléments négatifs. On procède de même avec G = — N, et S comprend au moins n éléments positifs.

Concluons en remarquant que cette borne est la meilleure ; posons :

$A = \{1, (q+1), (q+1)^2, \dots, (q+1)^{n-1}\}$ et

$S = A \cup [A - (q+1)^n + 1]$ ; on établit facilement que S a les propriétés requises.

Autre solution de l'auteur.