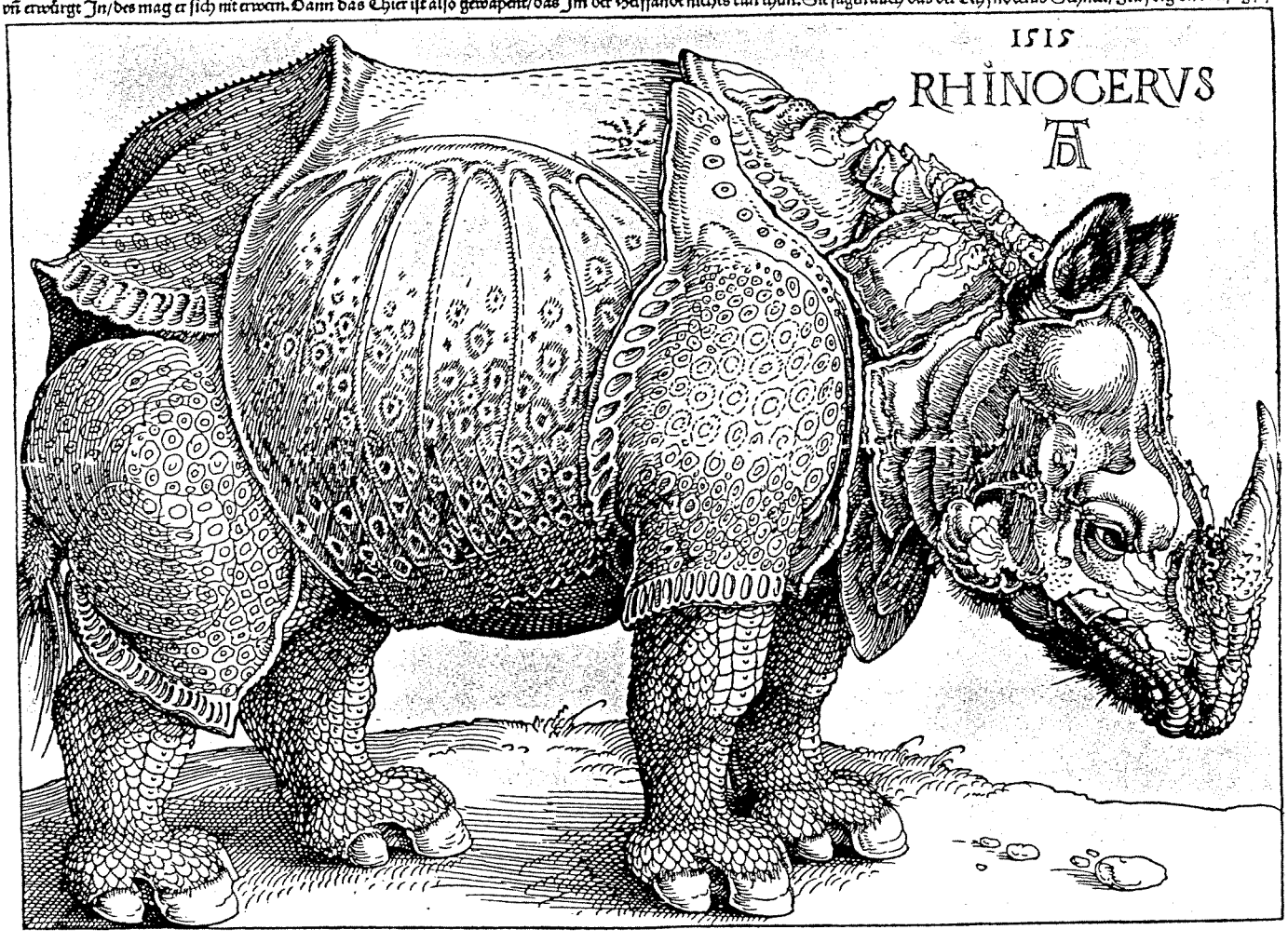
# L'OUVERT

JOURNAL DE L'A.P.M.E.P. D'ALSACE ET DE L'I.R.E.M. DE STRASBOURG
n° 57 – DÉCEMBRE 1989 I.S.S.N. 0290 - 0068

Nach Christus geburt. 1513. Jar. Adi. 1. May. Hat man dem großmechtigen Kunig von Portugall Emanuell gen Lysabona pracht auß India/ein sollich lebendig Thier. Das nennen sie Rhinocerus. Das ist hye mit aller seiner gestalt Abcondarfet. Es hat ein farb wie ein gesprickelte Schildcrot. Und ist vō dicken Schalen vberlegt fast fest. Und ist in der größ als der Helfande Aber ny dertrechtiger von paynen/vnd fast weehaffig. Es hat ein scharff starck Horn vom auff der nasen/Das begyndt es albeg zu wetzen wo es bey staynen ist. Das dosig Thier ist des Helfs fantz todt feynde. Der Helffandt furcht es fast vbel/dann wo es In ankumbt/so laufft Im das Thier mit dem kopff zwischen dye forderen payn/vnd reyst den Helffandt vnden am pauch auff vñ erwürgt In/des mag er sich mit erwern. Dann das Thier ist also gewapent/das Im der Helffande nichts kan thün. Sie sagen auch das der Rhynocerus Schnell/Fraydig vnd Listig sey.



NOTRE COUVERTURE : RHINOCERUS - par A. DÜRER - 1515

On dit qu'un petit dessin vaut mieux qu'un long discours. Mais ici DÜRER illustre par un grand dessin un texte assez court.

C'est en effet à partir de la seule description donnée au-dessus de la gravure et qu'il avait reçue par courrier d'une relation à Lisbonne que DÜRER a réalisé cette représentation du Rhinocéros dont, pour la première fois en Europe, un exemplaire venait d'être offert au Roi Emmanuel du Portugal.

Voici la traduction de ce texte à la fois précis et mythique :
"*Le 1er mai de l'an* 1513 *après J.-C. on a apporté à Lisbonne au tout-puissant roi Emmanuel du Portugal, en provenance des Indes, un animal vivant semblable à celui-ci. On l'appelle Rhinocéros. Il est représenté sur ce tableau. Il a la couleur d'une tortue mouchetée. Il est couvert d'épaisses écailles assez dures. Il a la taille d'un éléphant, mais plus court sur pattes, et il est très fort. Sur le nez il porte une forte corne pointue. Il se met à aiguiser celle-ci dès qu'il se trouve devant des rochers. Ce même animal est l'ennemi mortel de l'éléphant qui le craint avant tout, parce que lorsqu'il l'attaque en passant entre ses pattes antérieures, il lui déchire le ventre et l'étrangle de façon qu'il ne puisse pas s'en défendre. Car l'animal est armé de telle façon que l'éléphant ne peut rien lui faire. On dit aussi que le rhinocéros est rapide, agressif et rusé.*"

Etre capable de passer d'un texte à la représentation graphique, n'est-ce pas une connaissance nécessaire à l'étudiant en mathématiques ?

# CE N'EST PAS POUR LES FEMMES ...

Les filles ne vont pas en C. Il paraît qu'il faut modifier cet état de fait. Les filles ne vont pas en $F_1$ ou $F_3$, on parle beaucoup moins de modifier cet état de fait là. Il faut, paraît-il former encore plus de scientifiques et les filles semblent former un bon réservoir où il suffit de puiser. Pas si simple! Une anecdote illustrera mon propos.

Fabienne est une très bonne élève de terminale C. Elle est admise en math-sup. Après réflexion, elle renonce à cette option et choisit une autre voie. Un de ses professeurs l'a questionnée sur l'attitude de ses parents. Il en ressort que ces derniers la laissent libre de choisir l'orientation qu'elle veut. Fort bien. Voilà des parents admirables qui ont compris le sens de l'éducation, l'importance du développement harmonieux de la personnalité bien avant l'accumulation de connaissances ... Seulement voilà, quand ce même professeur pose à Fabienne la question de savoir quelle aurait été l'attitude de ses parents si elle avait été un garçon, elle répond sans hésiter, "mon père m'aurait obligée à faire math-sup!"

Liberté pour les unes, contraintes pour les autres. L'école et le lycée n'ont finalement qu'un pouvoir marginal. Et si vous êtes de ces professeurs qui voulez privilégier l'éducation sur l'enseignement, quel rôle devez-vous jouer vis à vis de vos élèves filles ou garçons? A trop pousser des élèves vers les mathématiques malgré leur réussite modeste ne renforce-t-on pas l'opinion dominante sur le rôle des mathématiques qui finissent par apparaître comme un mal nécessaire.

On touche ici toute l'ambiguïté d'un service qui s'intitule éducatif et qui fournit de l'enseignement car ce dernier est plus facilement quantifiable.

J. LEFORT.

# SOMMAIRE

N° 57 – 1989




L'OUVERT

ISSN 0290 – 0068

◇ *Responsable de la publication* : Jean LEFORT

◇ *Correspondance à adresser à :*
Université Louis Pasteur
Bibliothèque de l'I.R.E.M.
10, rue du Général Zimmer
67084 STRASBOURG CEDEX
Tél. : 88-41-64-40

◇ *Abonnement (pour 4 numéros annuels)*
50 F (95 F/2 ans) pour les membres A.P.M. d'Alsace
90 F (170 F/2 ans) pour l'Alsace
120 F (220 F/2 ans) pour la France ou l'Étranger.

◇ Chèque à l'ordre de Monsieur l'Agent Comptable de l'U.L.P. (IREM)

◇ *Prix du numéro* : 25.– F

# EQUATIONS DIOPHANTIENNES (*)

Jean-François BOUTOT

L'étude des équations diophantiennes est l'un des plus anciens problèmes des mathématiques : on s'y intéressait bien avant DIOPHANTE d'Alexandrie qui leur laissa son nom au 3$^{e}$ siècle de notre ère. On appelle équation diophantienne une équation algébrique à coefficients dans $\mathbb{Z}$ dont on cherche les solutions dans $\mathbb{Z}$ comme par exemple $x^2 - 3y^2 = 2z^3$.

On généralise cette notion au cas de la recherche des solutions rationnelles d'une équation algébrique à coefficients entiers ou rationnels (on peut toujours se ramener au cas des coefficients entiers en multipliant par le dénominateur commun de tous les coefficients). L'ensemble $\mathbb{Q}$ des rationnels formant un corps, la résolution de ce type d'équations en est facilité. On peut d'ailleurs associer aux solutions rationnelles d'une équation diophantienne les solutions entières d'une autre équation diophantienne. Par exemple :

$$\begin{array}{lll} x^2 + y^2 = 1 & \text{et} & X^2 + Y^2 = T^2 \\ (x, y) \in \mathbb{Q}^2 & & (X, Y, T) \in \mathbb{Z}^3 \end{array}$$

puisque si $(x, y)$ est solution rationnelle de la première on peut écrire $x = X/T$ et $y = Y/T$ ce qui conduit au deuxième système (dit homogène).

Dans ce qui suit nous nous intéresserons aux équations diophantiennes rationnelles à deux inconnues : $f(x, y) = 0$. Résoudre $f(x, y) = 0$ s'interprète comme la recherche sur une courbe algébrique du plan $\mathbb{R}^2$ des points à coordonnées rationnelles (ou points rationnels). Pour une bonne approche du problème on commence par voir ce qui se passe pour $f$ de degré petit.

## Le DEGRÉ 1 : Cas des droites

C'est un problème classique d'arithmétique. On sait qu'il y a une infinité de solutions et que quand on en connaît une $(x_0, y_0)$ alors en posant $f(x, y) = ax + by + c = 0$; $(a, b, c, ) \in \mathbb{Z}^3$ on a : $f(x, y) - f(x_0, y_0) = a(x - x_0) + b(y - y_0) = 0$ donc toutes les autres sont de la forme

$$\begin{aligned} x &= x_0 + tb \\ y &= y_0 - ta \end{aligned}$$

où $t \in \mathbb{Q}$.

---

(*) Rédaction d'après les notes de Jean LEFORT, d'une conférence APM - IREM, donnée le 15 mars 1989

## Le DEGRÉ 2 : Cas des coniques

Le problème se complique puisqu'il y a des cas où il n'y a pas de solution comme cela est manifeste, par exemple, pour l'équation $x^2 + y^2 + 1 = 0$ qui n'a pas de solutions réelles donc a fortiori de solutions rationnelles.

Il est facile de voir que si il y a une solution rationnelle alors il y en a une infinité. Pour comprendre pourquoi cela a lieu, prenons l'exemple du cercle $x^2 + y^2 = 1$ qui admet le point rationnel $p_0(-1, 0)$. On fait passer par $p_0$ une droite de pente $t$ rationnelle. Il est clair que le deuxième point d'intersection de cette droite avec le cercle a des coordonnées rationnelles qui valent

$$x = \frac{1 - t^2}{1 + t^2}$$
$$y = \frac{2t}{1 + t^2} \qquad t \in \mathbb{Q}$$

Dans le cas présent, comme il a été signalé initialement, il aurait été équivalent de chercher les solutions entières de l'équation homogène associée : $X^2 + Y^2 = Z^2$, ce qui revient à résoudre le problème des triplets de nombre pythagoriciens (nombres entiers pouvant être les côtés d'un triangle rectangle). Alors le même raisonnement conduit à :

$$X = a^2 - b^2$$
$$Y = 2ab$$
$$Z = a^2 + b^2$$

avec $a$ et $b$ entiers et premiers entre eux.

Le raisonnement que nous venons de faire pour le cercle s'applique tel quel à n'importe quelle conique. Ou bien elle n'a pas de points rationnels, ou bien elle en a un $p_0$, et une droite de pente $t$ ($\in \mathbb{Q}$) passant par $p_0$ recoupe la conique en un point rationnel P(t). Toute la question est de savoir si il y a ou non au moins un point rationnel sur la conique. Ce problème a été résolu par LEGENDRE. On se ramène par changement de repère à l'équation homogène

$$AX^2 + BY^2 + CZ^2 = 0 \qquad (A, B, C) \in \mathbb{Z}^3.$$

Pour que l'équation ait une solution rationnelle il faut

1) qu'il existe une solution réelle
2) qu'il existe une solution modulo $A$
une solution modulo $B$
et une solution modulo $C$
3) qu'il existe une solution modulo 8

Il est facile de voir qu'il n'y a qu'un nombre fini de triplets $(X, Y, Z)$ à tester. Cette règle est un cas particulier du principe de HASSE.

## Le DEGRÉ 3 : Cas des cubiques

Nous distinguerons deux cas selon qu'il s'agit d'une cubique singulière (c'est-à-dire présentant un point double ou un point de rebroussement) ou non.

### 1. Cas des cubiques singulières

Considérons l'exemple de la strophoïde d'équation

$$x(x^2+y^2) = x^2 - y^2$$

qui admet un point double ordinaire (c'est-à-dire à tangentes distinctes) à l'origine. Rappelons que les tangentes à l'origine sont données par les termes de plus bas degré, ici $x^2 - y^2$ soit $(x-y)(x+y) = 0$.

Coupons la strophoïde par une droite de pente rationnelle passant par le point double. Nous obtenons alors le paramétrage

$$x = \frac{1-t^2}{1+t^2}$$
$$y = \frac{t(1-t^2)}{1+t^2}$$

qui donne ainsi une infinité de points rationnels.

Une étude analogue pour la cissoïde d'équation $x(x^2+y^2) = y^2$ qui admet un point de rebroussement à l'origine conduit au paramétrage

$$x = \frac{t^2}{1+t^2}$$
$$y = \frac{t^3}{1+t^2}.$$

D'une façon générale une cubique n'admet qu'au plus un point singulier et on démontre que si le point singulier existe c'est un point à coordonnées rationnelles (toujours dans le cas où les coefficients de l'équation sont rationnels).

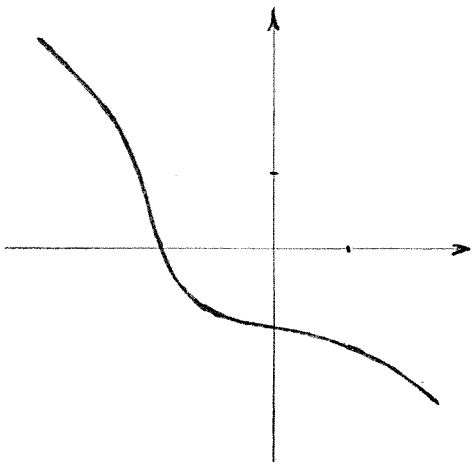
### 2. Cas des cubiques non singulières

Une cubique a toujours des points réels mais pas toujours des points rationnels. SELMER a donné en 1951 l'exemple de

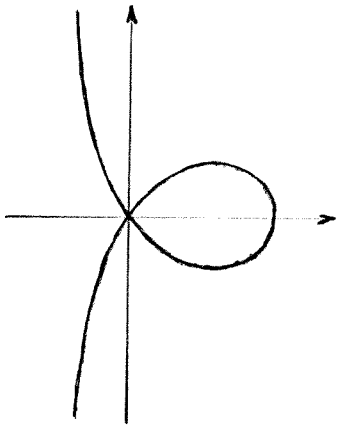
$$3X^3 + 4Y^3 + 5Z^3 = 0 \quad \text{(équation homogène associée)}$$

qui malgré l'existence de solution modulo $n$ pour tout $n$ n'admet pas de solution entière. Il n'y a donc pas de points rationnels sur la cubique

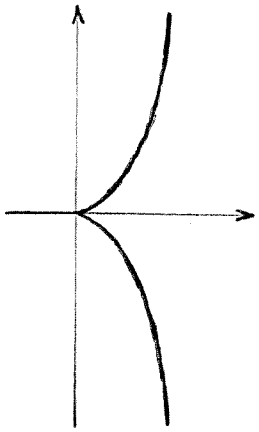
$$3x^3 + 4y^3 + 5 = 0$$



Cubique de Selmer



Strophoïde droite



Cissoïde droite

*Figure 1*

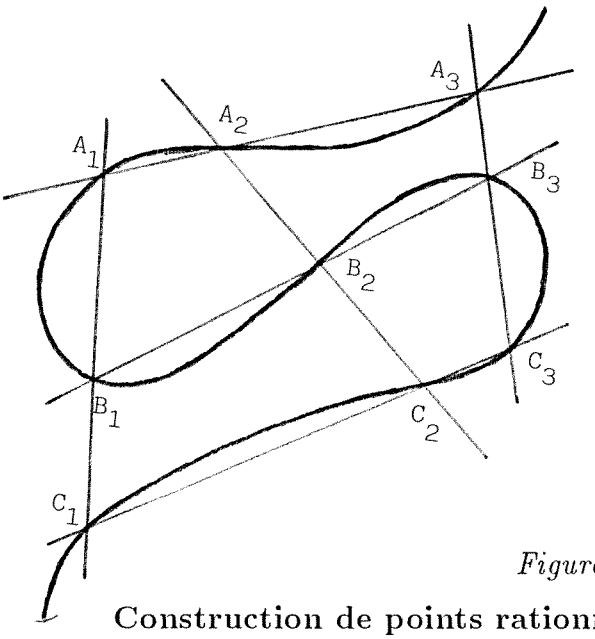
Pour aller plus loin, nous avons besoin de quelques résultats.

**Théorème de Lamé.** Soit $C$ une cubique. Soient $A_1, A_2, A_3, B_1, B_2, B_3, C_1, C_2, C_3$ neuf points tels que

$A_1A_2A_3$ soient alignés
$B_1B_2B_3$ soient alignés
$C_1C_2C_3$ soient alignés
$A_1B_1C_1$ soient alignés
$A_2B_2C_2$ soient alignés.

Alors les points $A_3B_3$ et $C_3$ sont aussi alignés (fig. 2 ci-dessous).

**Loi de groupe sur une cubique.** En se plaçant dans l'espace projectif complexe on démontre qu'une cubique admet neuf points d'inflexions. On en choisit un comme origine $\Omega$ et on associe à deux points $P$ et $Q$ de la cubique le point $R$ tel que si la droite $(PQ)$ recoupe en $T$ la cubique, alors $T\Omega$ recoupe en $R$ la cubique. Une autre façon de voir est de dire que trois points alignés ont une somme nulle (égale à $\Omega$). On définit ainsi une loi interne sur l'ensemble des points de la cubique $(P+Q=R)$. Cette loi est commutative, admet $\Omega$ comme élément neutre, l'opposé de $P$ étant le point $P'$ tel que $(PP')$ passe par $\Omega$. Le théorème de LAMÉ traduit l'associativité de cette loi qui est donc une loi de groupe.




En effet, prenons $B_2 = \Omega$ comme origine (fig. ci-contre). Alors

$$\begin{aligned}(A_2 + A_1) + B_1 &= -A_3 + B_1 \\ &= -A_3 - B_3 = C_3 \\ A_2 + (A_1 + B_1) &= A_2 - C_1 \\ &= -C_2 - C_1 = C_3\end{aligned}$$

*Figure 2*

**Construction de points rationnels à partir de l'un d'eux :**

Soit $P$ un point rationnel. On peut définir $2P, 3P \ldots nP$ de la façon suivante : la tangente en $P$ recoupe la cubique en $-2P$. $2P$ est le point aligné avec $\Omega$ (point d'inflexion choisi comme origine) et $-2P$ (voir fig. 3). Puis avec $P+2P$ on construit $3P$ etc...

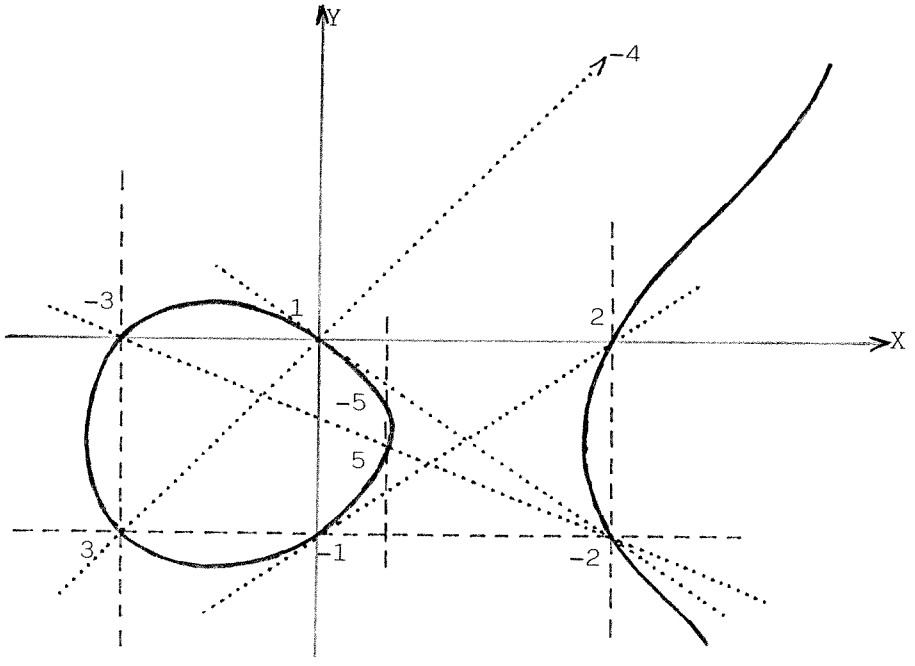



*Figure 3*

Cubique $y^2 = x^3 + px + q$.

On choisit comme origine le point d'inflexion à l'infini dans la direction de $Oy$.

On démontre que $nP$ est rationnel ce qui permet d'affirmer que l'ensemble des points rationnels forme un sous-groupe abelien : $C(\mathbb{Q})$. En 1922 MORDELL

démontra :

**Théorème de Mordell** : Le groupe des points rationnels d'une cubique est de type fini, ce qui veut dire qu'il existe $n$ points $P_1, P_2 \dots P_n$ de $C(\mathbb{Q})$ tels que pour tout $P$ de $C(\mathbb{Q})$ il existe des $m_i$ dans $\mathbb{Z}$ avec :

$$P = m_1 P_1 + m_2 P_2 + \cdots m_n P_n.$$

Le groupe $C(\mathbb{Q})$ est de la forme $\mathbb{Z}^r \oplus$ groupe abelien fini. $\mathbb{Z}^r$ correspond aux points $P_i$ d'ordre infini tandis que le groupe fini, dit groupe de torsion, correspond aux points $P_i$ d'ordre fini (c'est-à-dire pour lesquels il existe $n$ tel que $nP_i = \Omega$).

Ce n'est qu'en 1976 que MAZUR donna la forme du groupe de torsion. Il n'y a que 15 possibilités :

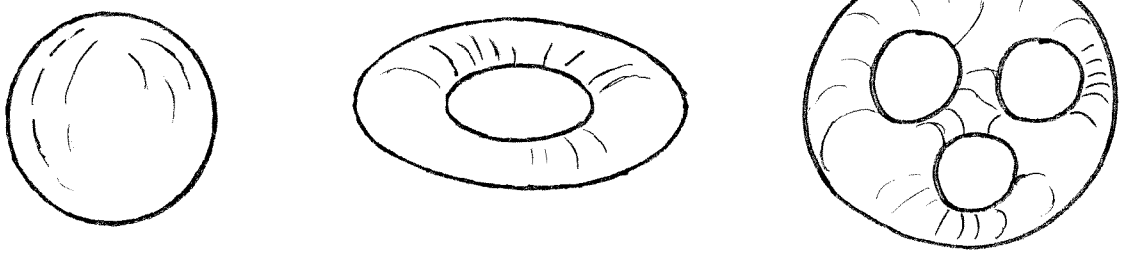
$$\mathbb{Z}/m\mathbb{Z} \text{ avec } m \leq 10 \text{ ou } m = 12$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \text{ avec } n \leq 4.$$

Quand au rang $r$, on a fait beaucoup de conjectures en étudiant les solutions modulo un nombre premier $p$. Les exemples suivants montrent la grande variété des possibilités :

* FERMAT : $X^3 + Y^3 = Z^3$ alors $C(\mathbb{Q}) = \{(1,-1,0),(1,0,1),(0,1,1)\}$
$= \mathbb{Z}/3\mathbb{Z}$.
* EULER : $X^3 + Y^3 = 3Z^3$ alors $C(\mathbb{Q}) = \{(1,-1,0)\}$
$X^3 + Y^3 = 2Z^3$ alors $C(\mathbb{Q}) = \{(1,-1,0),(1,1,1)\}$.
* TATE : $y^2 + y = x^3 - x$ alors $C(\mathbb{Q}) = \mathbb{Z}$ engendré par $(0,0)$.
Il n'y a pas de torsion.

## Approche du cas général

• Il ressort de l'étude précédente que le degré n'est pas l'invariant fondamental. Il faut aussi tenir compte des singularités. L'invariant qui en tient compte est le **genre**. Pour définir le genre d'une courbe plane, il faut la considérer comme une surface réelle plongée dans un espace de dimension 4. A cet effet on considère le plan projectif complexe $\mathbb{P}^2_{\mathbb{C}}$ qui est de dimension 2 sur $\mathbb{C}$ mais 4 sur $\mathbb{R}$. La courbe $C$ est alors une surface dans cet espace et on s'intéresse à son genre (c'est-à-dire schématiquement au nombre de trous analogues à celui d'un tore qui est de genre 1).



sphère : genre 0 — tore : genre 1 — surface de genre 3

*Figure 4*

• Reprenons l'exemple de la droite. Dans $\mathbb{P}^2_{\mathbb{C}}$ elle correspond à un plan auquel on a adjoint un point à l'infini ce qui en fait l'analogue d'une sphère de genre 0.

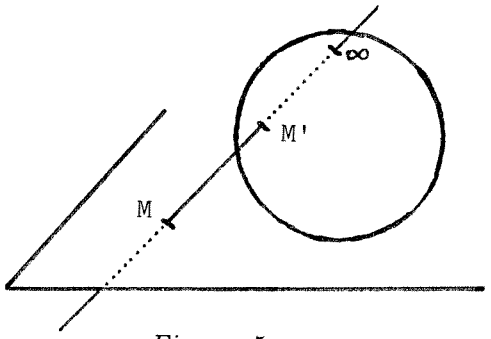



*Figure 5*

Bijection entre les points $M$ d'un plan
et les points $M^0$ d'une sphère tangente à ce plan.

Mais ce sera également le cas quand on peut établir une "*bijection*" entre une droite et la courbe $C$ comme cela a été fait pour les coniques et les cubiques singulières.

Dans le cas des cubiques singulières on n'avait pas réellement une bijection (et c'est la raison de la présence des guillemets). Mais il existe une méthode : l'éclatement, qui permet de construire une "*vraie*" bijection.

• Nous allons maintenant démontrer que le genre d'une cubique non singulière est 1. Pour cela considérons une fonction $f$ méromorphe et doublement périodique sur $\mathbb{C}$ (soient 1 et $\tau$ ses périodes). On sait que ce sont des fonctions elliptiques telles que la fonction $\wp(z)$ de WEIERSTRASS définie par :

$$\wp(z) = \frac{1}{z^2} + \Sigma_{w \in \bigwedge^*} [\frac{1}{(z-w)^2} - \frac{1}{w^2}]$$

où $\bigwedge = \mathbb{Z}_1 \oplus \mathbb{Z}_\tau$ est l'ensemble des nœuds du quadrillage engendré par 1 et $\tau$, et $\bigwedge^*$ cet ensemble privé de $(0,0)$.

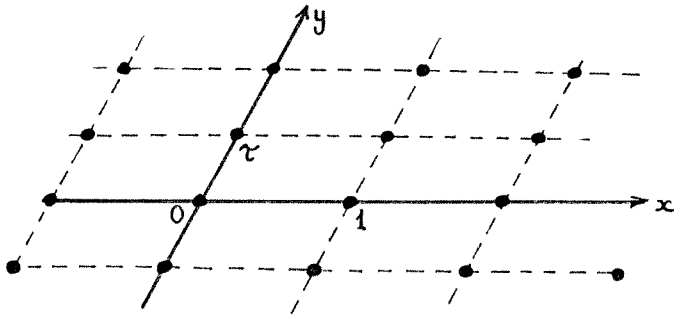



*Figure 6*

éléments de $\bigwedge$

Par dérivation on a : $\wp'(z) = \Sigma_{w \in \bigwedge} \frac{-2}{(z-w)^3}$ et on peut voir que $\wp(z)$ satisfait l'équation différentielle :

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3$$

où

$$g_2 = 60\Sigma_{w\in\bigwedge^*}\frac{1}{w^4}$$

et

$$g_3 = 140\Sigma_{w\in\bigwedge^*}\frac{1}{w^6}.$$

En posant $\wp' = y$ et $\wp = x$ on trouve une cubique. On sait que toutes les fonctions elliptiques sont engendrées par $\wp$ et $\wp'$ et forment ainsi un corps. La procédure précédente permet de mettre en bijection l'ensemble $\mathbb{C}/\bigwedge$ et la courbe $C_{\mathbb{C}}$ d'équation $y^2 = 4x^3 - g_2 - g_3$. Or $\mathbb{C}/\bigwedge$ s'identifie sans problème à un tore (de genre 1) en "*recollant*" les côtés opposés du parallélogramme construit sur 1 et $\tau$.


*Figure 7*

La loi de groupe qui a été mise en évidence sur la cubique n'est rien d'autre que l'addition dans $\mathbb{C}$.

• En genre supérieur ou égal à 2, MORDELL, en 1922, à partir de nombreux exemples, conjecture qu'il n'y a qu'un nombre fini de points rationnels. Ce n'est qu'en 1983 que G. FALTINGS démontre cette conjecture. Il n'est pas question dans le cadre de cet exposé de présenter la démonstration de FALTINGS, démonstration qui fait appel à toutes les ressources de la géométrie algébrique telle que l'a reformulée GROTHENDIECK.

Donnons toutefois quelques renseignements sur la façon de calculer le genre d'une courbe :
Si $f(x, y) = 0$ définit une courbe $C$ non singulière de degré $d$ alors son genre $g$ est :

$$g = \frac{(d-1)(d-2)}{2}.$$

Si la courbe $C$ possède $n$ points singuliers ordinaires (point double à tangentes distinctes ou points de rebroussement) alors le genre vaut

$$g = \frac{(d-1)(d-2)}{2} - n.$$

On fera cependant attention que le décompte doit se faire dans le plan projectif complexe. C'est ainsi que l'**astroïde** d'équation :

$$(x^2 + y^2 - 1)^3 + 27x^2y^2 = 0$$

possède :

4 points singuliers réels (points de rebroussement);
4 points doubles complexes $((\pm i, \pm i))$;
2 points doubles à l'infini.

ce qui conduit pour cette courbe de degré 6 à un genre égal à 0. On aurait pu s'en douter autrement quand on connaît la représentation paramétrique de l'astroïde :

$$x = \cos^3 \theta$$
$$y = \sin^3 \theta$$

qui met en évidence la "*bijection*" avec la droite par l'intermédiaire de $\theta$ (et d'un cercle).

• Et FERMAT dans tout ça? On sait que FERMAT avait annoncé en marge de son exemplaire de l'arithmétique de DIOPHANTE, avoir trouvé une démonstration simple de l'inexistence de solutions entières non triviales de l'équation

$$x^n + y^n = z^n$$

pour $n \geq 3$ (les solutions triviales sont du type $(0, a, a)$). Or pour $n \geq 4$, le genre de $X^n + Y^n = Z^n$ vaut $\big((n-1)(n-2)\big)/2$ qui est supérieur ou égal à 3. Le théorème de FALTINGS assure que cette équation n'a qu'un nombre fini de solutions entières avec $X, Y$ et $Z$ premiers entre eux. Ceci ne résoud pas tout à fait la question mais laisse de sérieux espoirs.

On sait qu'on a l'habitude de décomposer le problème de FERMAT en deux cas :
— le 1er cas qui dit que l'équation $x^p + y^p = z^p$ n'a pas de solution en entiers non divisibles par $p$,
— le 2ème cas qui dit que l'équation n'a pas de solution en entiers dont l'un au moins est divisible par $p$.

On conjecture que le 1er cas est vrai car si il y avait une solution $(\alpha, \beta, \gamma)$ avec $\alpha^p + \beta^p = \gamma^p$ la cubique $y^2 = x(x - \alpha^p)(x - \beta^p)$ pourrait ne pas exister.

En fait le problème de FERMAT a donné lieu à de très nombreuses recherches dans toutes les directions et on peut signaler que c'est grâce à lui que KUMMER a construit ses "nombres idéaux" qui ont conduit plus tard à la notion d'idéal d'anneaux.

On a montré récemment qu'il existait une infinité de nombres premiers pour lesquels le 1er cas est vrai, ce qui ne veut pas dire qu'il est vrai pour tout $p$ même si on sait qu'il est vrai pour $p \leq 253\ 747\ 889$.

UNE NOUVELLE PARUTION :

## LE PETIT LIVRE DE TEX

Raymond SEROUL

InterEditions – 1989 – ISBN 2 7296 0233 X

TEX, le traitement de texte spécialement conçu par Donald KNUTH pour la saisie et la mise en page de textes scientifiques, est le standard mondial en la matière. Longtemps confiné aux gros systèmes, il fonctionne maintenant sur les micro-ordinateurs IBM et Macintosh.

Cet ouvrage est le fruit d'une expérience quotidienne de TEX pendant plusieurs années. Le but que s'est fixé l'auteur est de vous initier sans douleur à ce traitement de texte si attachant. Le livre se compose de deux parties :

• La première présente les mécanismes de base et vous gruide pas à pas vers la maîtrise du logiciel. Elle contient de nombreux exemples et exercices, que vous pouvez reproduire et adapter à votre guise.

• La deuxième partie est un Dictionnaire-Index très complet des commandes de TEX, qui vous permet de les retrouver facilement lors de votre pratique quotidienne, avec là encore de très nombreux exemples.

Que vous soyez étudiant, professeur, chercheur, secrétaire dans un laboratoire, auteur d'ouvrages scientifiques, vous serez amené un jour ou l'autre à utiliser TEX. Ce livre sera alors le compagnon qui vous permettra de réussir votre auto-formation, puis la référence constante lors de votre pratique au jour le jour, et enfin le pied à l'étrier qui vous rendra plus aisé l'usage du TEXbook, le manuel de référence en anglais développé par Donald KNUTH.

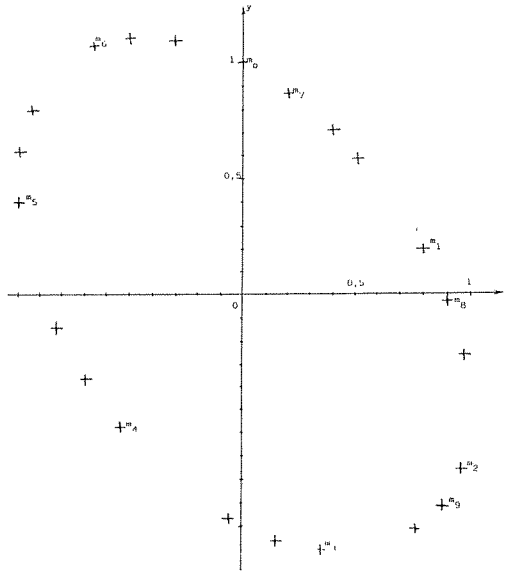
*L'auteur (*) , Maître de Conférences en informatique et mathématiques à l'Université Louis Pasteur de Strasbourg, est responsable de la composition en TEX du Bulletin de la Société Mathématique de France, dans le cadre du Laboratoire de Typographie informatique.*

---

(*) C'est grâce à ses précieux conseils que notre bibliothécaire à l'IREM de Strasbourg, Evelyne LE GUYADER, après avoir suivi des cours d'initiation à TEX au Laboratoire de Typographie informatique a pu se perfectionner pour la saisie des articles destinés à *'L'Ouvert'* . Nous tenons ici à le remercier chaleureusement pour sa disponibilité, sa gentillesse à toute épreuve et son savoir-faire de Grand Sorcier.

# DES POINTS SUR UN GRAPHIQUE

Jacques LUBCZANSKI



ÉNONCÉ

L'objet de ce problème est d'étudier une suite de points $(m_n)_{n\in\mathbb{N}}$ du plan euclidien, dont les coordonnées $x_n$ et $y_n$ dans un repère orthonormé vérifient :

$$\begin{cases} x_0 &= 0 \\ y_0 &= 1 \end{cases}$$

et $\forall n \in \mathbb{N}$ :

$$\begin{cases} x_{n+1} = & x_n + 0,8y_n \\ y_{n+1} = & -x_n + 0,2y_n \end{cases}.$$

## A.— TOUS LES POINTS $m_n$ SONT SUR UNE COURBE $\Gamma$ :

1.- Calculer les coordonnées des points $m_1, m_2$ et $m_3$.
Calculer des valeurs approchées, à $10^{-3}$ près, des coordonnées de $m_4, m_5 \ldots m_{19}$ et $m_{20}$.
Tracer, dans un repère où une unité vaut 8 cm, tous les points $m_n$ calculés.

2.- Calculez les nombres $A, B, C$ et $D$ de façon que les points $m_0, m_1$ et $m_2$ appartiennent à la courbe $\Gamma$ d'équation $Ax^2 + By^2 + Cxy + D = 0$.

3.- Démontrer, par récurrence, que $\forall n \in \mathbb{N}$, $m_n \in \Gamma$.

## B.— INSCRIPTION DE LA COURBE $\Gamma$ DANS UN PARALLÉLOGRAMME

1.– On coupe $\Gamma$ par une droite "verticale" d'équation $x = m$ où $m \in \mathbb{R}$.
Discuter selon les valeurs de $m$ le nombre de points d'intersection.

2.– Lorsqu'il y a deux points d'intersection $M_1$ et $M_2$, on note $I$ le milieu de $[M_1M_2]$.
Etablir une relation entre les coordonnées $x_I$ et $y_I$ de $I$, où $m$ n'intervient pas.
Quel est l'ensemble des points $I$, lorsque $m$ varie?

3.– On note $E$ et $F$ les positions extrêmes de $I$, et on coupe $\Gamma$ par une droite $D$ parallèle à $[EF]$. Montrer que l'ensemble des milieux $J$ des points d'intersection ainsi obtenus, lorsque $D$ varie, est le segment $[A, B]$ où $A\binom{0}{-1}$ et $B\binom{0}{1}$.

4.– Quelles sont les tangentes à $\Gamma$ aux points $A, B, E$ et $F$?

## C.— TRANSFORMATION DE $\Gamma$ EN UN CERCLE

Dans cette partie, on va transformer, par une application affine, $\Gamma$ en un cercle : l'étude de la suite des points $m_n$ se ramènera alors à l'étude, plus facile, de la suite des points $M_n$ correspondants sur le cercle.

1.– Soit $C\binom{-1}{0}$, $D\binom{1}{0}$ et $\mathcal{C}$ le cercle d'équation $x^2+y^2=1$.
On cherche les applications affines qui transforment l'ensemble des deux *diamètres* $[A,B]$ et $[E,F]$ de $\Gamma$ en l'ensemble des deux diamètres $[A,B]$ et $[C,D]$ du cercle $\mathcal{C}$.
Si $f$ est une telle application, montrer que $f(0)=0$ et que $f(A)$ est un des quatre points $A,B,C,D$. Quelles sont alors les images possibles pour $E$?
Combien d'applications affines répondent à la question?

2.– Montrer que deux des applications trouvées sont des symétries axiales.
On note $\sigma$ celle qui est une symétrie axiale de direction $\vec{j}$, et $\Delta$ son axe.
Etablir les formules analytiques de $\sigma$ et vérifier que $\sigma(\Gamma)=\mathcal{C}$.
Tracer, dans un repère d'unité 8 cm, $\Delta$, $\mathcal{C}$ et $\Gamma$.

3.– On pose : $\forall n \in \mathbb{N}\ M_n = \sigma(m_n)$. Si $X_n$ et $Y_n$ sont les coordonnées de $M_n$, établir les formules de récurrence liant $X_{n+1}, Y_{n+1}$ et $X_n, Y_n$.
Par quelle transformation géométrique passe-t-on de $M_n$ à $M_{n+1}$?
En déduire une construction géométrique de $m_{n+1}$ à partir de $m_n$.

4.– Comment évolue la distance $m_n m_{n+1}$ quand $n$ tend vers l'infini?
Les suites $(x_n)_{n\in\mathbb{N}}$ sont-elles convergentes?

5.– Soit $\alpha$ tel que $\sin\alpha = 0,8$ et $\cos\alpha = 0,6$; en admettant que, pour $p$ et $q$ premiers entre eux, $(p>1, q>2) \Rightarrow (\sin\frac{p}{q}\pi$ irrationnel), montrer que $\forall n \in \mathbb{N}^*, n\alpha \neq 2K\pi, k \in \mathbb{Z}$.
La suite $(m_n)$ est-elle périodique?

ÉLÉMENTS DE SOLUTION

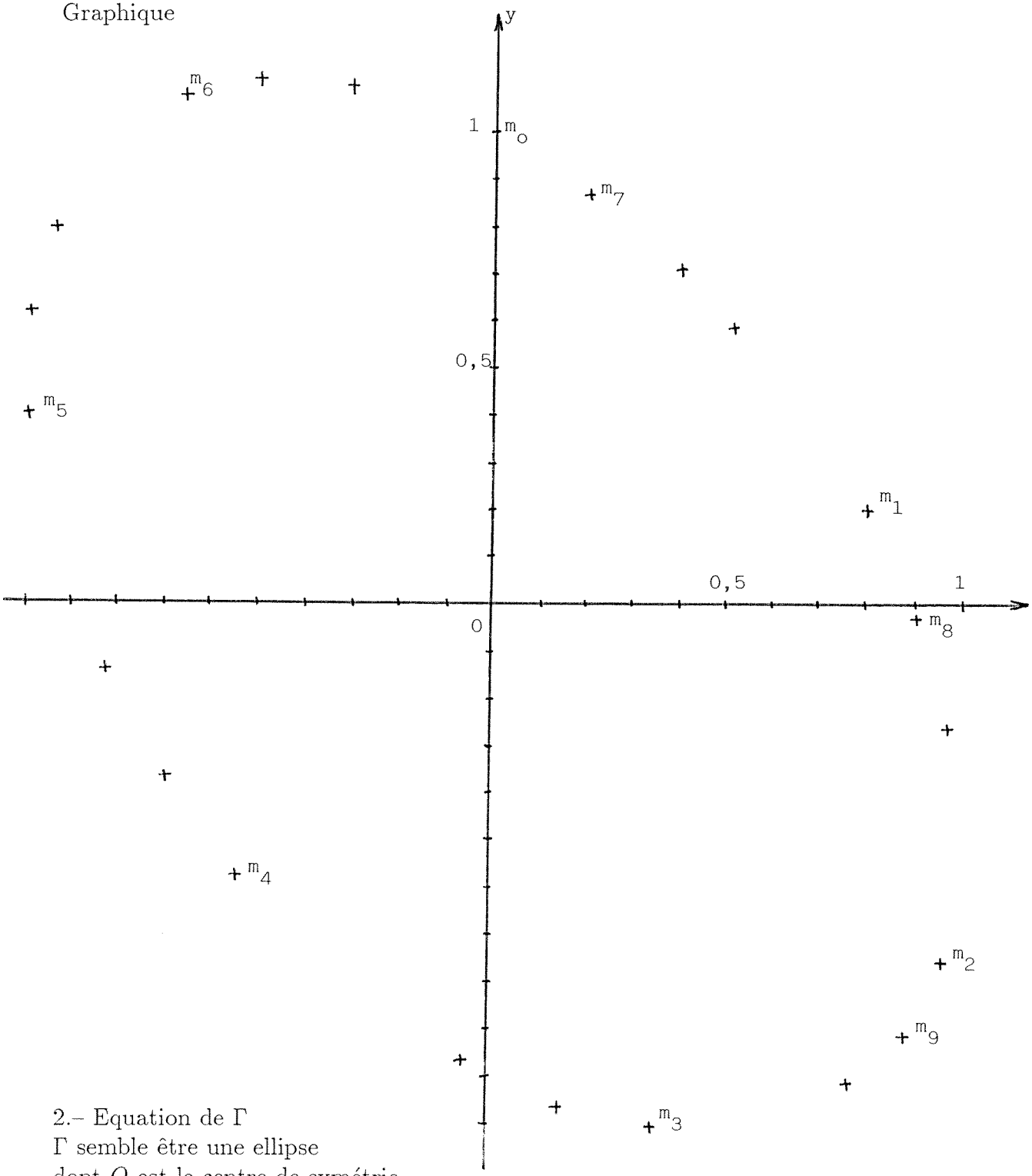
## A.— TOUS LES POINTS $m_n$ SONT SUR UNE COURBE $\Gamma$

1.– Coordonnées des points $m_n$ ($\times$ 1000)

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|
| 800 | 960 | 352 | −538 | −997 | −659 | 206 | 907 | 882 | 151 |
| 200 | −760 | −1112 | −575 | 423 | 1082 | 875 | −31 | −913 | −1064 |

| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
|---|---|---|---|---|---|---|---|---|---|---|
| −700 | −991 | −490 | 404 | 974 | 765 | −56 | −832 | −943 | −299 | 584 |
| −364 | 627 | 1117 | 713 | −261 | −1026 | −970 | −138 | 805 | 1104 | 520 |

Graphique




2.– Equation de $\Gamma$

$\Gamma$ semble être une ellipse
dont $O$ est le centre de symétrie.
Son équation serait alors de la forme

$$Ax^2 + By^2 + Cxy + D = 0.$$

Cherchons $A, B, C$ et $D$ pour que les trois premiers points $m_0, m_1$ et $m_2$ soient sur $\Gamma$ :

$m_0\binom{0}{1}$ ; $m_1\binom{0,8}{0,2}$ ; $m_2\binom{0,96}{-0,76}$ $\rightarrow m_0 \in \Gamma \Leftrightarrow \quad B+D=0 \quad (1)$

$m_1 \in \Gamma \Leftrightarrow \quad 64A+4B+16C+100D=0 \quad (2)$

$m_2 \in \Gamma \Leftrightarrow 9216A+5776B-7296C+10000D=0 \quad (3)$

D'où le système, après simplification de (2) par 4 et de (3) par 16 :

$B+D=0 \quad \Leftrightarrow D=-B$ qu'on reporte : 16A-24B+4C+25D=0 (4)

$16A+B+4C+25D=0$ 576A-264B-456C=0 (5)

$576A+361B-456C+625D=0.$

Soit après simplification de (4) par 4 et de (5) par 8 $\begin{cases} 4A-6B+C=0 \\ 72A-33B-57C=0 \end{cases}$

Supposons $C$ connu et résolvons en inconnues $A$ et $B$ le système de CRAMER :

$$\begin{cases} 4A-6B=-C \\ 72A-33B=57C \end{cases} \quad D=\begin{vmatrix} 4 & -6 \\ 72 & -33 \end{vmatrix}=300 \quad A=\frac{\begin{vmatrix} -C & -6 \\ 57C & -33 \end{vmatrix}}{300}=\frac{375}{300}C=1,25C$$

$$B=\frac{\begin{vmatrix} 4 & -C \\ 72 & 57C \end{vmatrix}}{300}=\frac{300}{300}C=C.$$

On obtient donc $A=1,25C$; $B=C$; $D=-C$.

Si on choisit $C=1$, l'équation de $\Gamma$ peut s'écrire : $\boxed{1,25x^2+y^2+xy-1=0.}$

3.– Tous les points $m_n$ sont sur $\Gamma$ :

Par récurrence :
— initialisation : $m_0 \in \Gamma$ d'après le calcul précédent
— incrémentation : $m_n \in \Gamma \Longleftrightarrow 1,25x_n^2+y_n^2+x_ny_n-1=0$
Calculons alors $1,25x_{n+1}^2+y_{n+1}^2+x_{n+1}y_{n+1}-1$. Cela donne :
$1,25(x_n+0,8y_n)^2+(-x_n+0,2y_n)^2+(x_n+0,8y_n)(-x_n+0,2y_n)-1$
$=\ldots$
$=1,25x_n^2+y_n^2+x_ny_n-1=0$ d'après l'hypothèse : $m_{n+1} \in \Gamma$.
Conclusion : d'après le principe de récurrence, $\forall n, m_n \in \Gamma$.

## B.— INSCRIPTION DE LA COURBE $\Gamma$ DANS UN PARALLÉLOGRAMME

1.– Intersection de $\Gamma$ avec des droites "verticales" :

Les coordonnées des points d'intersection sont solution du système

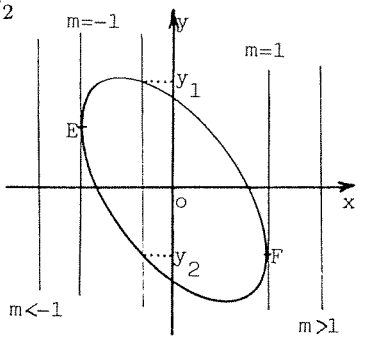
$$\begin{cases} 1,25x^2+y^2+xy-1=0 \\ x=m \end{cases}.$$

En particulier les ordonnées $y$ sont racines de l'équation :

$$y^2 + my + 1,25m^2 - 1 = 0$$
$$\Longleftrightarrow (y + 0,5m)^2 - 0,25m^2 + 1,25m^2 - 1 = 0 \Longleftrightarrow (y + 0,5m)^2 = 1 - m^2$$

Donc si

$1 - m^2 < 0 \Longleftrightarrow m < -1$ ou $m > 1$ : pas de solution
$1 - m^2 = 0 \Longleftrightarrow m = \pm 1$ : une racine double : la droite est tangente à $\Gamma$
$1 - m^2 > 0 \Longleftrightarrow -1 < m < 1$ : deux racines $y_1$ et $y_2$

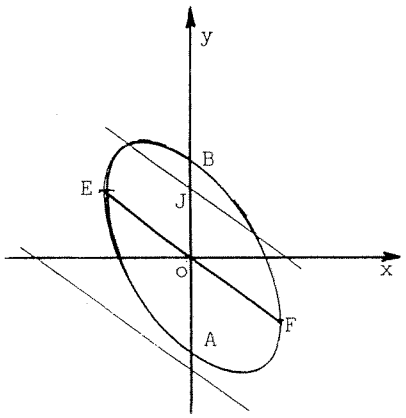



2.– Ensemble des milieux des points d'intersection :

L'ordonnée du milieu est $1/2(y_1 + y_2)$. Or $y_1 + y_2$, somme des racines de l'équation, vaut $-m$ : donc l'ordonnée du milieu vaut $-m/2$. Or son abscisse vaut $m$ : Le milieu appartient donc à la droite $y = (-1/2)x$.

L'ensemble des points $I$, lorsque $m$ varie entre $-1$ et 1 est donc le **segment de droite** $[E, F]$ où $E$ a pour coordonnées $\binom{-1}{0.5}$ et $F\binom{1}{-0,5}$.

3.– Intersection avec des droites parallèles à $[E, F]$

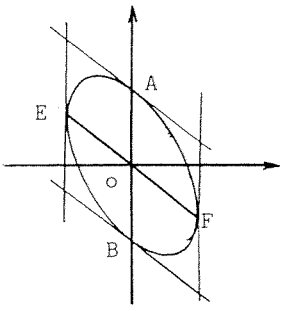



On doit résoudre :

$$\begin{cases} 1,25x^2 + y^2 + xy - 1 = 0 \\ y = (-1/2)x + m \end{cases}$$

D'où $1,25x^2 + (-0,5x + m)^2 + (-0,5x + m)x - 1 = 0$
$\Longleftrightarrow x^2 = 1 - m^2$ :
si $m < -1$ ou $m > 1$ : pas d'intersection
si $m = 1$ : une racine double : tangence
si $-1 < m < 1$ : deux racines $x_1$ et $x_2$.
Alors $x_J = 1/2(x_1 + x_2) = 0$ : $J$ **est sur le segment vertical** $[AB]$.

4.– Tangentes à $\Gamma$ aux points $A, B, E$ et $F$ :




La situation de tangence est caractérisée par la racine double dans l'équation du second degré :
les tangentes en $A$ et $B$ sont parallèles à $[EF]$
les tangentes en $E$ et $F$ sont parallèles à $[AB]$.

## C.— TRANSFORMATION DE $\Gamma$ EN UN CERCLE

1.– Applications affines transformant $[A, B] \cup [E, F]$ en $[A, B] \cup [C, D]$

• On aura $f([A, B] \cap [E, F]) = f([A, B] \cap [C, D])$ c'est-à-dire $f(0) = 0$.

• En outre, $f$ conservant les barycentres, tout point intérieur à l'un des diamètres aura pour image un point intérieur à l'un ou l'autre des deux diamètres : en effet

$$\begin{aligned} M \in ]A,B[ &\Longleftrightarrow \exists \alpha > O \text{ et } B > 0 \text{ tels que } M \text{ soit barycentre de } (A,\alpha) \text{ et } (B,\beta) \\ &\Longleftrightarrow f(M) \text{ barycentre de } (f(A),\alpha) \text{ et } (f(B),\beta) \text{ avec } \alpha > 0 \text{ et } \beta > 0 \\ &\Longleftrightarrow f(M) \in ]f(A),f(B)[. \end{aligned}$$

Par conséquent, l'image d'une extrémité sera aussi une extrémité de segment.
• $A$ a donc quatre images possibles : $A, B, C$ ou $D$.
Discutons alors selon les images de $O, A$ et $E$, qui détermine complètement $f$ :

| si $[A,B] \mapsto [A,B]$ et $[E,F] \mapsto [C,D]$ | | si $[A,B] \mapsto [C,D]$ et $[E,F] \mapsto [A,B]$ | |
|---|---|---|---|
| $A \mapsto A$ | $A \mapsto B$ | $A \mapsto C$ | $A \mapsto D$ |
| $E \mapsto C \Rightarrow \begin{matrix} B \mapsto B \\ F \mapsto D \end{matrix}$ formules analytiques $\begin{cases} x' = x \\ y' = \frac{1}{2}x + y \end{cases}$ | $E \mapsto C \Rightarrow \begin{matrix} B \mapsto A \\ F \mapsto D \end{matrix}$ $f$ est une symétrie d'axe $KL$ (où $K$ et $L$ sont les milieux de $EC$ et $FD$), de direction $\vec{f}$ | $E \mapsto A \Rightarrow \begin{matrix} B \mapsto D \\ F \mapsto B \end{matrix}$ formules analytiques $\begin{cases} x' = -\frac{1}{2}x - y \\ y' = -x \end{cases}$ | $E \mapsto A \Rightarrow \begin{matrix} B \mapsto C \\ F \mapsto B \end{matrix}$ formules analytiques $\begin{cases} x' = \frac{1}{2}x + y \\ y' = +x \end{cases}$ |
| $E \mapsto D \Rightarrow \begin{matrix} B \mapsto B \\ F \mapsto C \end{matrix}$ $f$ est une symétrie d'axe $AB$ et de direction $\overrightarrow{ED}$ | $E \mapsto D \Rightarrow \begin{matrix} B \mapsto A \\ F \mapsto C \end{matrix}$ formules analytiques $\begin{cases} x' = -x \\ y' = -\frac{1}{2}x - y \end{cases}$ | $E \mapsto B \Rightarrow \begin{matrix} B \mapsto D \\ F \mapsto A \end{matrix}$ formules analytiques $\begin{cases} x' = -\frac{1}{2}x - y \\ y' = x \end{cases}$ | $E \mapsto B \Rightarrow \begin{matrix} B \mapsto C \\ F \mapsto A \end{matrix}$ formules analytiques $\begin{cases} x' = \frac{1}{2}x + y \\ y' = x \end{cases}$ |

Huit applications affines répondent à la question, dont deux symétries axiales.

2.– L'image de $\Gamma$ par $\sigma$ est $\mathcal{C}$ :

Les formules analytiques sont :

$$\begin{cases} x' &= x \\ y' &= -0,5x - y \end{cases}$$

Comme $\sigma$ est une involution, $\sigma^{-1} = \sigma$, donc on a aussi :

$$\begin{cases} x &= x' \\ y &= -0,5x' - y'. \end{cases}$$

Alors

$$\begin{aligned} M \in \Gamma &\Longleftrightarrow 1,25x^2 + y^2 + xy - 1 = 0 \\ &\Longleftrightarrow 1,25x'^2 + (-0,5x' - y')^2 - x'(0,5x' + y') - 1 = 0 \\ &\Longleftrightarrow 1,25x'^2 + 0,25x'^2 + x'y' + y'^2 - 0,5x'^2 - x'y' - 1 = 0 \\ &\Longleftrightarrow x'^2 + y'^2 - 1 = 0 \\ &\Longleftrightarrow (M) \in \mathcal{C} : \text{l'image de } \Gamma \text{ est donc } \mathcal{C}. \end{aligned}$$

3.– Transformation $M_n \to M_{n+1}$ :

Posons $\varphi : m \to m'$ définie par :

$$\begin{cases} x' &= x + 0,8y \\ y' &= -x + 0,2y. \end{cases}$$

c'est-à-dire qu'on a $\varphi(m_n) = m_{n+1}$.
Alors on peut résumer la situation par le diagramme suivant :

$$\begin{array}{lccc} & & \varphi & \\ \text{sur } \Gamma : & m_n & \mapsto & m_{n+1} \\ & \sigma \downarrow & & \downarrow \sigma \\ & & ? & \\ \text{sur } \mathcal{C} : & M_n & \to & M_{n+1} \end{array}$$

Il s'ensuit que l'application qui transforme $M_n$ en $M_{n+1}$ est la composée

$$\sigma \circ \varphi \circ \sigma^{-1}.$$

Or $\sigma^{-1} = \sigma$ : c'est donc

$$\sigma \circ \varphi \circ \sigma.$$

Il suffit alors de calculer les formules analytiques de $\sigma \circ \varphi \circ \sigma$ : cela donne :

$$\begin{pmatrix} x \\ y \end{pmatrix} \xrightarrow{\sigma} \begin{pmatrix} x \\ -0,5x - y \end{pmatrix} \xrightarrow{\varphi} \begin{pmatrix} x + 0.8(-0.5x - y) \\ -x + 0.2(-0.5x - y) \end{pmatrix} = \begin{pmatrix} 0.6x - 0.8y \\ -1.1x - 0.2y \end{pmatrix} \xrightarrow{\sigma} \begin{pmatrix} 0.6x - 0.8y \\ 0.8x + 0.6y \end{pmatrix}$$

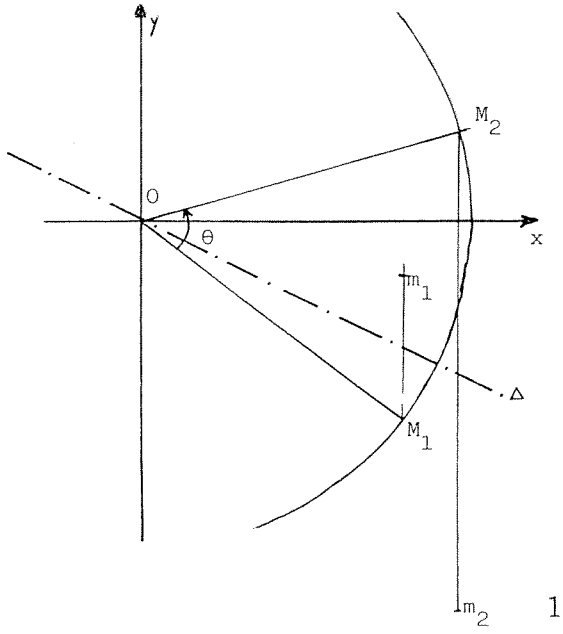
$\sigma \circ \varphi \circ \sigma$ a donc pour formules analytiques : $\begin{cases} x' = 0.6x - 0.8y \\ y' = 0.8x + 0.6y \end{cases}$

soit en posant $\cos\theta = 0.6$ et $\sin\theta = 0.8$ : $\begin{cases} x' = \cos\theta x - \sin\theta y \\ y' = \sin\theta x + \cos\theta y \end{cases}$

**On reconnaît les formules d'une rotation de centre $O$ et d'angle $\theta$**

Si on la note $r$, on a donc $M_n \overset{r}{} M_{n+1}$.

• **Construction géométrique de $m_{n+1}$ à partir de $m_n$.**




A partir de $m_n$ on construit $M_n$, symétriquement de $m_n$ par rapport à $\Delta$.
Puis $M_{n+1}$ est obtenu à partir de $M_n$ par rotation d'angle $\theta$.
Enfin $m_{n+1}$ est le symétrique de $M_{n+1}$.

4.– Evolution quand $n \to +\infty$
Les points $M_n$ et $M_{n+1}$ sont à distance constante :

$$M_n M_{n+1} = 2 \sin \frac{\theta}{2}.$$

Donc $M_n$ et $M_{n+1}$ ne peuvent jamais se rapprocher.
Il s'ensuit que leurs symétriques $m_n$ et $m_{n+1}$ ne peuvent pas non plus se rapprocher : la suite $(m_n)_{n\in\mathbb{N}}$ n'est pas convergente.
Donc les suites $(x_n)$ et $(y_n)$ ne sont pas non plus convergentes.

5.– La suite $(m_n)_{n\in\mathbb{N}}$ peut-elle être périodique? (Raisonnement par l'absurbe)

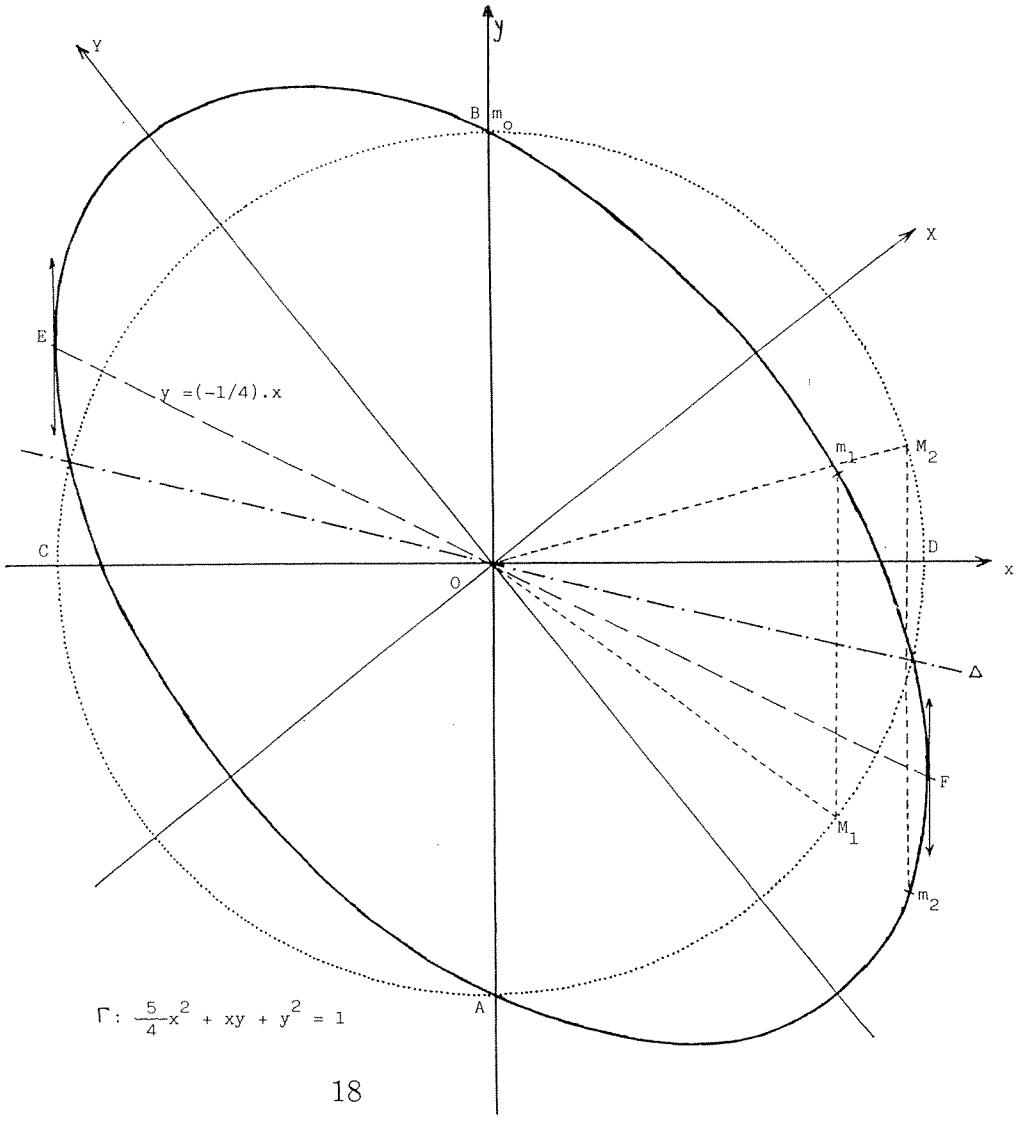
Supposons qu'il existe $p$ tel que $m_{n+p} = m_n$, alors $M_{n+p} = M_n$.

Or pour passer de $M_n$ à $M_{n+p}$, on a effectué $p$ fois une rotation d'angle $\theta$ : donc une rotation de $p\theta$.

Alors $M_{n+p} = M_n \Rightarrow p\theta = 2k\pi \Rightarrow \theta = \frac{2k}{p} \times \pi$.

D'après l'énoncé, si $2k > l$ et $p > 2$, alors $\sin\theta$ est irrationnel. Or $\sin\theta = 0,8 \in \mathbb{Q}$ : il y a une contradiction. La suite $(m_n)_{n\in\mathbb{N}}$ ne peut pas être périodique.

Les points $(M_n)$ se répartissent donc sur le cercle et les points $(m_n)$ sur l'ellipse. On peut montrer que cette répartition est "uniforme" dans le sens où tout point du cercle peut être approché aussi près qu'on veut par un point $(M_n)$ pour un $n$ bien choisi : on dit alors que l'ensemble des points $(M_n)$ est "**dense**" dans le cercle.



# LA GRANDE SAGA DES CALENDRIERS

Jean LEFORT

## 6.— LES CALENDRIERS LUNI-SOLAIRES

### 1) Quelques hypothèses

Le calendrier luni-solaire apparaît souvent, d'un point de vue historique, comme un calendrier de transition entre un calendrier purement lunaire et un calendrier purement solaire. Cette phase de transition peut durer plus ou moins longtemps et semble dépendre du degré de civilisation atteint par le peuple qui l'utilise au moment de cette transition.

Par exemple, l'apogée de la civilisation grecque a eu lieu au moment de la transition ce qui a valorisé le calendrier luni-solaire. Au contraire, chez les égyptiens la civilisation est apparue après la transition et chez les romains vers la fin de la transition ce qui a entraîné l'adoption d'un calendrier de type solaire. A l'inverse, chez les musulmans, la transition venait juste de débuter à l'avènement du prophète et il ne lui a pas été difficile d'imposer le retour au calendrier purement lunaire que certaines tribus n'avaient d'ailleurs pas abandonnées.

Sans doute les hypothèses que je viens de développer mériteraient-elles d'être nuancées. On peut toutefois remarquer que les peuples sont très conservateurs en matière d'unités de mesure. Nous avons vu que les égyptiens refusèrent l'abandon de l'année vague et que les anglais (et les polonais) se révoltèrent quand le gouvernement imposa le calendrier grégorien. Il est donc nécessaire qu'un phénomène marquant et durable apparaisse pour qu'une réforme du calendrier soit possible.

### 2) Des méthodes empiriques

Essayons maintenant de comprendre comment a pu s'effectuer la transition : au début, surtout quand la nouvelle lune était constatée visuellement, il s'est agit de regrouper les mois lunaires de façon à ce qu'une même mois, ou plus exactement un mois de même nom (et pour cela ils étaient regroupés par 12) tombe toujours à peu près à la même saison. Quand il s'avérait que le retard était trop important, un décret royal ou impérial imposait le redoublement d'un mois particulier.

Par exemple, 2000 ans avant notre ère une tablette du roi Hammourabi de Babylone nous révèle :

"*Hammourabi, à son ministre Sin-Idinnam, dit ceci : l'année est hors de place. Fais enregistrer le prochain mois sous le nom de second Ululu. Le paiement des impôts à Babylone, au lieu de se terminer le 25 Tasritu, devra s'achever le 25 du second Ululu.*"

Ceci prouve aussi que les exigences du fisc, 4000 ans plus tard n'ont pas changées. Il n'aurait pas fallu que les rentrées d'argent aient lieu un mois plus tard (Tasritu suit normalement Ululu).

Malheureusement pour l'historien et le chronologiste les redoublements des mois ne sont pas toujours enregistrés et les règles d'intercalation rarement fixes. Le lien des mois avec les constellations comme dans cette tablette chaldéenne :

"*Dilgan (le Bélier) doit effectuer son lever héliaque du mois de Nissanu. Quand il n'en sera pas ainsi, le mois sera changé*",

est toujours empirique et la largeur des constellations permet beaucoup de variations. C'était souvent les saisons qui permettaient de savoir s'il fallait ou non redoubler un mois. Dans la bible, il est précisé que la Pâque doit avoir lieu au moment où les orges précoces sont bonnes à couper. Le Grand Prêtre décidait donc si le mois précédent : Adar (Pâque a lieu le 15 Misan) devait ou non être redoublé en Véadar. Cette méthode est très empirique et l'on connaît les printemps pourris ou au contraire trop précoces. Il est vraissemblable que les aléas des variations climatiques ont entraîné des années de 14 mois (à cause de deux redoublements dans la même année) et sûrement plusieurs années consécutives de 13 mois comme le prouvent des documents écrits.

Pour revenir à l'influence de l'administration, expliquons un peu mieux ce qui se passait à Rome quelques années avant l'adoption du calendrier Julien : les mois étaient les suivants :

| | | |
|---|---|---|
| Martius | (31 jours) | |
| Aprilis | (29 jours) | |
| Maius | (31 jours) | |
| Junius | (29 jours) | |
| Quintilis | (31 jours) | |
| Sextilis | (29 jours) | Total : 355 jours |
| September | (29 jours) | |
| October | (31 jours) | |
| November | (29 jours) | |
| December | (29 jours) | |
| Januarius | (29 jours) | |
| Februarius | (28 jours) | |

Les nombres impairs portaient bonheur, d'où l'alternance 29 et 31 jours. Seul Février avait la malchance de n'avoir que 28 jours. C'était le mois des morts!

Pour compléter à 365 jours on ajoutait tous les deux ans un mois de 22 jours appelé Mercedonicus, qui s'intercalait tout entier entre le 23 et le 24 Février (le 24 Février s'appelait "sexto ante calendes Martis").

Le lecteur aura remarqué que $355 + 355 + 22 = 732$ alors que $365 + 365 = 730$. Le décalage avec le soleil est de près de 1 jour par an. Pour remédier à cet excès sur l'année tropique, le collège des pontifes reçut le droit de donner au mois

Mercedonius la longueur qu'il fallait. Et ceux-ci n'hésitèrent pas à allonger ou raccourcir l'année selon que leurs amis ou ennemis politiques étaient aux postes soumis à renouvellement.

### 3) Les calendriers grecs

Pendant longtemps les grecs utilisèrent en concomitance avec un calendrier purement lunaire un calendrier basé sur les saisons pour régler les fêtes agricoles. Mais ces calendriers très pragmatiques, plutôt solaires et dits "parapegmes" variaient d'une ville à l'autre et surtout au sein d'une même ville, changeaient au bout de quelques années pour des questions de mode.

Le calendrier lunaire comportait une année de 12 mois de 354 jours :

| | | | |
|---|---|---|---|
| Hécatombéon | (30 j) | Gamélion | (30 j) |
| Metagitnion | (29 j) | Anthestérion | (29 j) |
| Boédromion | (30 j) | Elaphébolion | (30 j) |
| Pyanepsion | (30 j) | Munychion | (29 j) |
| Mœmactérion | (29 j) | Thagélion | (30 j) |
| Posidéon | (29 j) | Scirophorion | (29 j) |

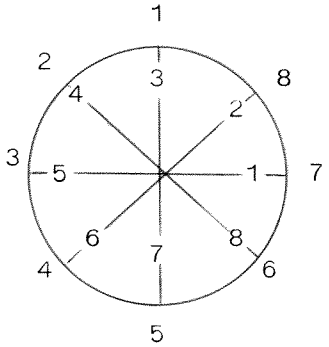
Quand les grecs décidèrent d'ajouter un 13$^{e}$ mois de temps en temps, ce fut Posidéon qui fut redoublé, le deuxième Posidéon ayant 30 j. Les années de 13 mois furent appelées logiquement embolismiques (embolismos = ajouté, en grec).

Au temps de Solon, vers 600 avant notre ère, l'année embolismique avait lieu tous les deux ans. C'était une alternance simple, beaucoup trop simple pour être exacte et durer. Mais elle n'est pas illogique puisqu'elle correspond à la première meilleure approximation de l'expression de l'année solaire en année lunaire (l'année vaut alors en moyenne 369 j).

Un siècle plus tard, des progrès dans la mesure du temps permirent de prendre la meilleure approximation suivante, ce qui correspond à une année embolismique tous les 3 ans (l'année est alors trop courte et vaut en moyenne 364 j).

Au temps de Herodote, vers 450 avant notre ère, les grecs adoptèrent un cycle de 8 ans appelé pour cela octaéride ou cycle octaétérique ($\omicron\kappa\tau\alpha\varepsilon\tau\eta\rho\iota\sigma$) durant laquelle 3 années étaient embolismiques. On retrouve bien à nouveau le rapport 3/8 qui correspond à la 3$^{e}$ réduite de la décomposition en fraction continue (ou bien 4$^{e}$ meilleure approximation – la 3$^{e}$ correspondant à 5 ans).

Si on cherche à placer un 13$^{e}$ mois dès que l'écart risque d'être supérieur à 15 jours on placera les années embolismiques aux rangs 2, 5 et 7.




Les grecs les placèrent aux rangs 3, 5 et 8 ce qui correspond exactement au même cycle décalé de deux années.

La valeur moyenne de l'année fut alors de $354 + 30 \times (3/8) = 365,25$ j, ce qui est, nous l'avons vu, une valeur excellente. Mais la durée du mois était

$$\frac{8 \times 354 + 3 \times 30}{8 \times 12 + 3} = 29,5151\ldots$$

est trop faible (erreur de 1 jour en 5 ans).

**Les cycles de Meton et de Callipe**

Quand on prend la suite des meilleures approximations rationnelles du nombre de lunaisons dans une année tropique on voit que la valeur $12 + (7/19)$ est excellente puisque la valeur suivante nécessite la fraction 67/182.

c'est à Meton d'Athènes que l'on doit cette découverte : 19 années solaires valent 235 lunaisons, soit 6940 jours. La légende veut que, publiée en l'an 433 avant notre ère, au siècle de Périclès, à l'occasion des jeux olympiques, cette découverte fut gravée en lettre d'or sur les colonnes du temple de Minerve. C'est pourquoi le rang d'une année dans le cycle de 19 fut baptisé "nombre d'or".

Dans ce cycle on trouve quatre sortes d'années. Cela paraît compliqué, mais assez logique puisque 12 mois lunaires font 354,367 056 jours, on trouvera des années **communes** de 354 ou 355 jours que nous appellerons respectivement **régulière** et **abondante**. De même l'année de 13 mois lunaires, compte 383,897 644 jours et nous les appellerons respectivement **defectives** et **régulières**. Le lecteur trouvera ma notation originale. Je préfère prendre celle-ci de manière à ne pas la changer quand je parlerai du calendrier juif.

Essayons de placer ces années de façon qu'en fin d'année l'écart avec la lune soit inférieur à la demi-journée et avec le soleil inférieur à la demi-lunaison. Nous aboutissons au tableau de la page suivante.

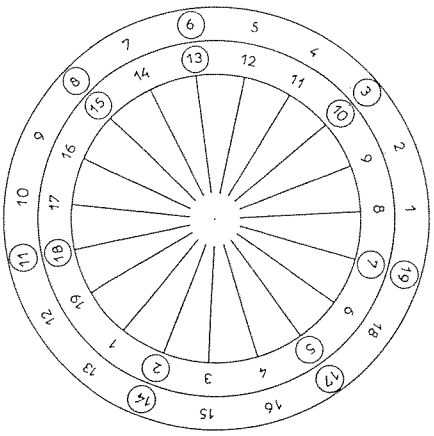
J'ai pris ici les valeurs actuelles de la lunaison et de l'année tropique. L'écart qu'il pouvait y avoir au siècle de Périclès, même s'il atteint quelques secondes, ne remet pas en question le cycle obtenu.

La valeur moyenne attribuée à la lunaison ($29 + 25/47 \simeq 29,531\ 915$) et à l'année ($365 + 5/19 \simeq 365,263\ 158$) sont trop longues toutes les deux. Dans les deux cas l'erreur est de l'ordre de 1/3 de jours en un cycle.

Malgré l'accueil enthousiaste de la découverte de Méton, son cycle ne fut guère appliqué, ingratitude des peuples, tout au moins au début.

Nous trouvons sa première mention un siècle plus tard environ vers 342 avant notre ère. Mais déjà la Grèce atteignait son apogée et il faut citer le nom de Callipe qui vers la fin de se vie repris et améliora le cycle de Meton.

| année | lunaisons | jours | nature de l'année | écart à la lune en fin d'année | écart au soleil en fin d'année |
|---|---|---|---|---|---|
| 1 | 12 | 354 | CR 354 j = 12 m | + 0,367 056 | + 11,242 199 |
| 2 | 25 | 738 | ER 384 j = 13 m | + 0,264 700 | − 7,515 602 |
| 3 | 37 | 1093 | CA 355 j = 12 m | − 0,368 244 | + 2,726 597 |
| 4 | 49 | 1447 | CR 354 j = 12 m | − 0,001 188 | + 13,968 796 |
| 5 | 62 | 1831 | ER 384 j = 13 m | − 0,103 544 | − 4,789 005 |
| 6 | 74 | 2185 | CR 354 j = 12 m | + 0,263 512 | + 6,453 194 |
| 7 | 87 | 2569 | ER 384 j = 13 m | + 0,161 156 | − 12,304 607 |
| 8 | 99 | 2924 | CA 355 j = 12 m | − 0,471 788 | − 2,062 408 |
| 9 | 111 | 3278 | CR 354 j = 12 m | − 0,104 732 | + 9,179 791 |
| 10 | 124 | 3662 | ER 384 j = 13 m | − 0,207 088 | − 9,578 010 |
| 11 | 136 | 4016 | CR 354 j = 12 m | + 0,159 968 | + 1,664 189 |
| 12 | 148 | 4371 | CA 355 j = 12 m | − 0,472 976 | + 11,906 388 |
| 13 | 161 | 4754 | ED 383 j = 13 m | + 0,424 668 | − 5,851 413 |
| 14 | 173 | 5109 | CA 355 j = 12 m | − 0,208 276 | + 4,390 786 |
| 15 | 186 | 5493 | ER 384 j = 13 m | − 0,310 632 | − 14,367 015 |
| 16 | 198 | 5847 | CR 354 j = 12 m | + 0,056 424 | − 3,124 816 |
| 17 | 210 | 6201 | CR 354 j = 12 m | + 0,423 480 | + 8,117 383 |
| 18 | 223 | 6585 | ER 384 j = 13 m | + 0,321 124 | − 10,640 418 |
| 19 | 235 | 6940 | CA 355 j = 12 m | − 0,311 820 | − 0,398 219 |



Au moment donc où le cycle de Meton est amélioré, le cycle est fixé et l'on trouve les années embolismiques placées aux rangs 2, 5, 7, 10, 13, 15 et 18 à une translation près dans le cycle (nous verrons que le calendrier juif adopte les rangs 3, 6, 8, 11, 14, 17 et 19, ce qui est le même ordre comme le prouve la figure ci-contre).

Callipe proposa de regrouper quatre cycles de Méton soit 76 années et en supprimant un jour sur les quatre cycles soit 27 759 jours l'année avait alors 365,25 jours en moyenne et le mois 29,530 851 jours, valeurs toutes deux excellentes. L'écart au soleil était de 0,6 jours au bout du cycle et l'écart à la lune 0,25 jours.

Cette période de 76 ans fut largement utilisée par les astronomes grecs et leurs permit de profiter des observations babyloniennes qu'ils rattachèrent à leur calendrier.

Hipparque, vers l'an 130 avant notre ère se rendit compte que l'année est plus courte que 365 jours 1/4. Il lui attribua la valeur de 365 j 5 h 55 min (il y a encore 6 min de trop) soit 365,246 528. Quand à la lunaison il lui donna la valeur de 29 j 12 h 44 min 2 s (il n'y a qu'une seconde de moins) soit 29,530 579.

Pour ajuster le calendrier à cette nouvelle précision il proposa de retrancher un jour en quatre cycles de Callipe soit 304 ans.

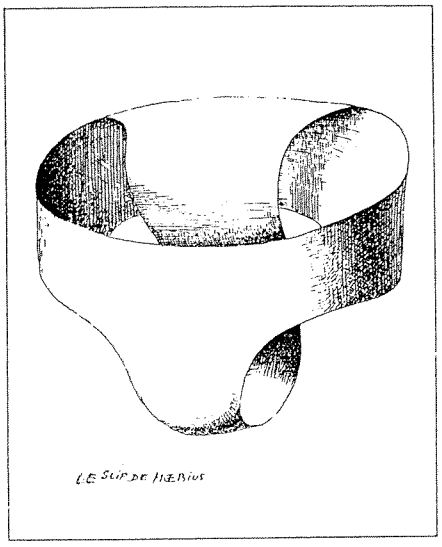
Dans la pratique, cette remarque ne fut jamais utilisée et les astronomes se contentèrent des périodes callipiques.

---

Marc GUINOT de Bourg en Bresse me fait remarquer, avec juste raison, qu'il faut maintenant parler de "suites" de FAREY et non de "séries" de FAREY malgré l'utilisation de ce dernier terme dans "Theory of numbers" de HARDY et WRIGHT.

Ce souci de l'exactitude honore ce fidèle lecteur.

---



Dessin de Gourmelin extrait d'"Un souvenir d'enfance d'Evariste Galois" (Balland)

NOUVELLE PARUTION INTER-I.R.E.M. (1988 – 1989) :

**SUIVI SCIENTIFIQUE – CLASSE DE 3ème**

Prix de vente : 50.- F (65.- F si envoi postal)

# THÉORÈMES DE BASE EN ARITHMÉTIQUE

Maurice MIGNOTTE

## 1.— Introduction

Ce papier correspond à un exposé donné à l'IREM de Niamey en février 1989. Le but est de montrer que plusieurs théorèmes de base de l'arithmétique élémentaire (celle qui était jadis enseignée dans les lycées) sont en fait équivalents. On donne ici neuf énoncés, numérotés de 1 à 9, et on montre les implications

$$(\mathbf{1}) \Longrightarrow (\mathbf{2}),\ (\mathbf{2}) \Longrightarrow (\mathbf{3}),\ \ldots\ ,(\mathbf{8}) \Longrightarrow (\mathbf{9}),\ (\mathbf{9}) \Longrightarrow (\mathbf{1}).$$

En raison de ce souci d'économie, certaines de ces démonstrations sont assez artificielles, voire laborieuses. Le tout constitue un ensemble qu'il est hors de question de présenter aux élèves, il est particulièrement anti-pédagogique! Il s'agit d'un texte destiné au maître, qui montre la grande liberté que peut avoir l'enseignant dans l'ordre de présentation de ces résultats et qui prouve qu'aucun de ces théorèmes n'est plus "*fondamental*" qu'un autre.

Voici deux manières possibles de présenter ces théorèmes. De manière classique, on peut partir du théorème d'EUCLIDE-GAUSS (appelé aussi théorème fondamental de l'arithmétique) : soient $a, b$ et $c$ des entiers non nuls, si $a$ divise $bc$ et si $a$ est premier avec $b$ alors il divise $c$; en déduire ensuite l'unicité de la décomposition en facteurs premiers, puis l'existence du p.g.c.d., la relation de BÉZOUT ... De manière plus algébrique, on peut d'abord étudier les sous-groupes de $\mathbb{Z}$ (en utilisant la division euclidienne, on montre aussitôt qu'un tel sous-groupe est de la forme $d\mathbb{Z}$), puis en déduire l'existence du p.g.c.d. et la relation de BÉZOUT.

Il reste le point de vue algorithmique. Dans cette optique, on doit présenter l'algorithme d'EUCLIDE (dans sa version qui fournit aussi les coefficients de la relation de BÉZOUT); on peut parler un peu des tests de primalité, de la factorisation; il est bien sûr intéressant de donner quelques informations sur le coût de ces différents algorithmes. Une conséquence de la comparaison de ces différents coûts est que la présentation du p.g.c.d. via l'unicité de la factorisation est inadaptée aux calculs effectifs (sauf pour des entiers très petits).

## 2.— Enoncés

Dans toute la suite la lettre $p$ désigne un nombre premier. Nous admettrons le résultat suivant

**(0).** *Pour tout entier $n$ il existe $p$ premier qui divise $n$.*

Nous aurons aussi besoin de l'asssertion ci-dessous.

**(0')**. *Tout entier positif $n$ est un produit de facteurs premiers.*

Il est clair que **0'** implique **0**. Réciproquement, en raisonnant par récurrence sur $n$, on voit facilement que **0** implique **0'**. Ainsi, les assertions **0** et **0'** sont équivalentes.

**(1)**. (EUCLIDE - GAUSS) *Si $a$ divise $bc$ et si $a$ et $b$ sont premiers entre eux alors $a$ divise $c$.*

**(2)**. *Si d'une part $a$ et $b$ sont premiers entre eux et si d'autre part $a$ et $c$ sont aussi premiers entre eux alors $a$ et $bc$ sont premiers entre eux.*

**(3)**. *L'anneau quotient $\mathbb{Z}/p\mathbb{Z}$ est intègre.*

**(4)**. *Si $x$ est un entier non divisible par $p$ alors il existe un entier positif $k$ tel que l'on ait*

$$x^k \equiv 1 (\text{mod } p).$$

**(5)**. *L'anneau quotient $\mathbb{Z}/p\mathbb{Z}$ est un corps.*

**(6)**. (BÉZOUT) *Si $a$ et $b$ sont deux entiers premiers entre eux alors il existe des entiers $u$ et $v$ tels que l'on ait*

$$ua + vb = 1.$$

**(7)**. (Théorème chinois) *Si $m$ et $n$ sont deux entiers premiers entre eux alors pour tout couple d'entiers $a$ et $b$ il existe un entier $x$ qui vérifie simultanément*

$$x \equiv a (\text{mod } m) \text{ et } x \equiv b (\text{mod } n).$$

**(8)**. *Si $b$ et $c$ sont deux entiers premiers entre eux et si $b$ divise $a$ et $c$ divise $a$ alors le produit $bc$ divise aussi $a$.*

**(9)**. *Tout entier positif est égal à un produit de facteurs premiers et ceci de manière unique, à l'ordre près des facteurs.*

## 3.— Démonstration

Nous utiliserons la notation $(a, b) = 1$ qui signifie : $a$ et $b$ sont premiers entre eux.
**(1)** $\Longrightarrow$ **(2)**
Supposons que **(1)** soit vrai et que $a, b$ et $c$ soient tels que $(a, b) = (a, c) = 1$. Si **(2)** est faux (d'après **(0)**), il existe un nombre premier $p$ qui divise $bc$ et $a$; d'après **(1)**, puisque $a$ et $b$ sont premiers entre eux, ce nombre $p$ divise $c$. Le fait que $p$ divise à la fois $a$ et $c$ contredit l'hypothèse $(a, c) = 1$.

**(2)** $\Longrightarrow$ **(3)**
Si $a$ et $b$ sont premiers avec $p$, l'assertion **(2)** montre que leur produit est encore premier avec $p$. D'où l'implication.

**(3)** $\Longrightarrow$ **(4)**
Soit $x$ un entier non divisible par $p$. Considérons les puissances de $x$ modulo $p$. Comme il n'y a qu'un nombre fini de classes modulo $p$, il existe deux exposants $m$ et $n$, $0 \leq m < n$, tels que $x^m \equiv x^n (\text{mod } p)$. Donc, $x^m(x^{n-m} - 1) \equiv 0 (\text{mod } p)$. Si l'anneau $\mathbb{Z}/p\mathbb{Z}$ est intègre, on en déduit, par récurrence sur $m$, la relation $x^{n-m} \equiv 0$ modulo $p$.

**(4)** $\Longrightarrow$ **(5)**
C'est immédiat.

**(5)** $\Longrightarrow$ **(6)**
Soient $a$ et $b$ deux entiers premiers entre eux. Grâce à la propriété **(0')** on peut écrire

$$a = p_1^{\alpha_1} \dots p_r^{\alpha_r} \text{ et } b = q_1^{\beta_1} \dots q_s^{\beta_s},$$

où les nombres $p_1, \dots, p_r, q_1, \dots, q_s$ sont premiers et deux à deux distincts. En appliquant **(5)** on voit que pour tout $i$ et $j$, $1 \leq i \leq r$ et $1 \leq j \leq s$, il existe des entiers $u_{ij}$ et $v_{ij}$ tels que l'on ait

$$u_{ij}p_i + v_{ij}q_j = 1.$$

On en déduit

$$(u_{ij}p_i + v_{ij}q_j)^{\alpha_i + \beta_j} = 1,$$

d'où l'existence d'entiers $U_{ij}$ et $V_{ij}$ tels que

$$U_{ij}p_i^{\alpha_i} + V_{ij}q_j^{\beta_j} = 1, 1 \leq i \leq r \text{ et } 1 \leq j \leq s.$$

En effectuant le produit sur $j, 1 \leq j \leq s$, des relations précédentes, on constate qu'il existe des entiers $U_i$ et $V_i$ tels que

$$U_i p_i^{\alpha_i} + V_i b = 1, 1 \leq i \leq r.$$

En faisant le produit sur $i, 1 \leq i \leq r$, de ces dernières relations on conclut qu'il existe des entiers $u$ et $v$ tels que

$$ua + vb = 1.$$

**(6)** $\Longrightarrow$ **(7)**
Si $um + vn = 1$ alors le nombre $x = avn + bum$ est une solution du système

$$x \equiv a (\text{mod } m) \text{ et } x \equiv b (\text{mod } n).$$

**(7) $\Longrightarrow$ (8)**
Le théorème chinois montre que l'application naturelle $f : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ qui à un entier $x$ associe le couple ($x$ mod $m, x$ mod $n$) est surjective. De plus $f$ est un homomorphisme d'anneaux qui est nul sur l'ensemble des multiples du produit $mn$. D'où, par passage au quotient, une application $\varphi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, qui est encore surjective. Mais, comme les ensembles de départ et d'arrivée de $\varphi$ sont finis et comportent le même nombre d'éléments (à savoir $mn$ éléments), $\varphi$ est en réalité une bijection. Le fait que $\varphi$ soit injective montre que tout nombre à la fois divisible par $m$ et par $n$ est divisible par le produit $mn$.

**(8) $\Longrightarrow$ (9)**
Supposons que la factorisation ne soit pas unique. Il existe alors un entier positif minimal $n$ tel que

$$n = p_1^{\alpha_1} \dots p_r^{\alpha_r} = q_1^{\beta_1} \dots q_s^{\beta_s},$$

où les nombres $p_1, \dots p_r, q_1, \dots q_s$ sont premiers et deux à deux distincts.
Alors $p_1$ et $q_1$ divisent $n$, avec $(p_1, q_1) = 1$ . L'assertion (**8**) montre que le produit $p_1 q_1$ divise $n$. Ainsi, $n = p_1 q_1 n'$. Ecrivons

$$n' = l_1^{\gamma_1} \dots l_r^{\gamma_r}.$$

On a donc

$$p_1 l_1^{\gamma_1} \dots l_r^{\gamma_r} = q_1^{\beta_1 - 1} q_2^{\beta_2} \dots q_s^{\beta_s}.$$

D'après la minimalité de $n$, $p_1$ n'admet une décomposition en facteurs premiers qui est unique; ceci impose à $p_1$ d'être égal à l'un des $q_j$ : contradiction.

**(9) $\Longrightarrow$ (1)**
Soient $a, b$ et $c$ trois entiers tels que $a$ divise $bc$ et que $a$ et $b$ soient premiers entre eux. On peut supposer $a > 1$, sinon l'assertion (**1**) est triviale.
Grâce à la décomposition unique en facteurs premiers, puisque $a$ divise $bc$ on peut écrire

$$bc = p_1^{\alpha_1} \dots p_r^{\alpha_r} \text{ et } a = p_1^{\beta_1} \dots p_s^{\beta_s},$$

avec $s \leq r$ et $1 \leq \beta_i \leq \alpha_i$ pour $1 \leq i \leq s$.
Puisque $a$ et $b$ sont premiers entre eux, l'entier $b$ est nécessairement de la forme

$$b = p_{s+1}^{\gamma_{s+1}} \dots p_r^{\gamma_r}, 0 \leq \gamma_i \leq \alpha_i \text{ pour } s < i \leq r.$$

On en déduit que $a$ divise $c$.

## 4.— Une question

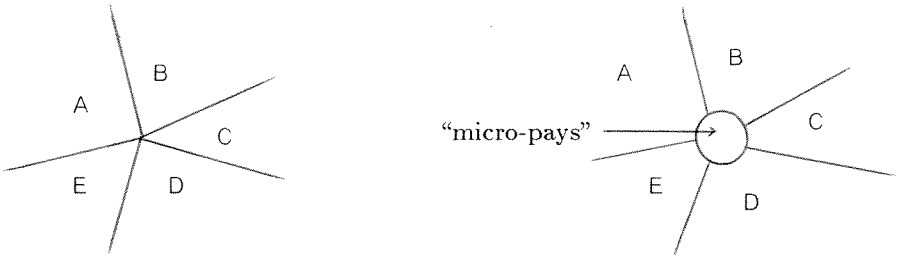
A la suite de cet exposé, M. TRAOURÉ a posé la question suivante : étudier, dans un anneau plus général que $\mathbb{Z}$, les implications qui peuvent exister entre les généralisations des propriétés (**1**) à (**9**).

# VARIATIONS SUR LE THÉORÈME DES 4 COULEURS

Jean LEFORT

Depuis 1977 on sait, grâce à Wolfgang HAKEN et Kenneth APPEL, qu'on peut colorier toute carte plane (ou sphérique) de pays connexes (c'est-à-dire en un seul morceau) à l'aide de quatre couleurs de façon que deux pays ayant une frontière commune n'aient pas la même couleur.

Dans leur démonstration, les deux mathématiciens ont travaillé sur des cartes simplifiées. La première simplification consiste à ne considérer que des cartes où les points frontières ne sont jamais communs à plus de trois pays. C'est ce qu'on appelle une **carte normale** (*).




Point frontière commun à cinq pays.

Normalisation d'un point frontière commun à cinq pays.

*Figure 1*

Il est toujours possible de normaliser une carte en ajoutant des "micro-pays" comme sur la figure 1. Si on a trouvé un coloriage avec quatre couleurs d'une carte normalisée alors, en supprimant les "micro-pays", on obtient un coloriage en quatre couleurs de la carte originale.

Nous appellerons **nœuds** les points communs à trois frontières et nous limiterons le sens du mot "frontière" à la ligne frontière qui joint deux nœuds consécutifs. Une frontière est donc adjacente à deux pays et à deux nœuds exactement; un nœud est adjacent à trois pays et trois frontières exactement.

L'objet du présent article est la démonstration du théorème suivant :

---



(*) En toute rigueur il faut aussi imposer aux pays d'être simplement connexes sur la sphère, mais cette propriété n'intervient pas dans les présentes démonstrations.

Sur une carte normale les trois propositions suivantes sont équivalentes :
1) On peut colorier les pays à l'aide de quatre couleurs de façon que deux pays voisins n'aient pas la même couleur.
2) On peut colorier les frontières à l'aide de trois couleurs de façon que tout nœud soit adjacent aux trois couleurs.
3) On peut colorier les nœuds de deux couleurs de façon que pour tout pays, la différence entre le nombre de nœuds adjacents d'une couleur et ceux de l'autre couleur soit divisible par trois.

Ce résultat peut paraître paradoxal. Il l'est moins quand on remarque que s'il y a quatre types de pays, selon sa couleur, il y a alors $6 = 2 \times 3$ types de frontières selon la couleur des pays adjacents; de plus s'il y a trois types de frontières, selon sa couleur, il y a deux types de nœuds selon l'ordre dans lequel se succèdent les frontières autour de chaque nœud. La figure 2 donne un exemple d'un tel coloriage.

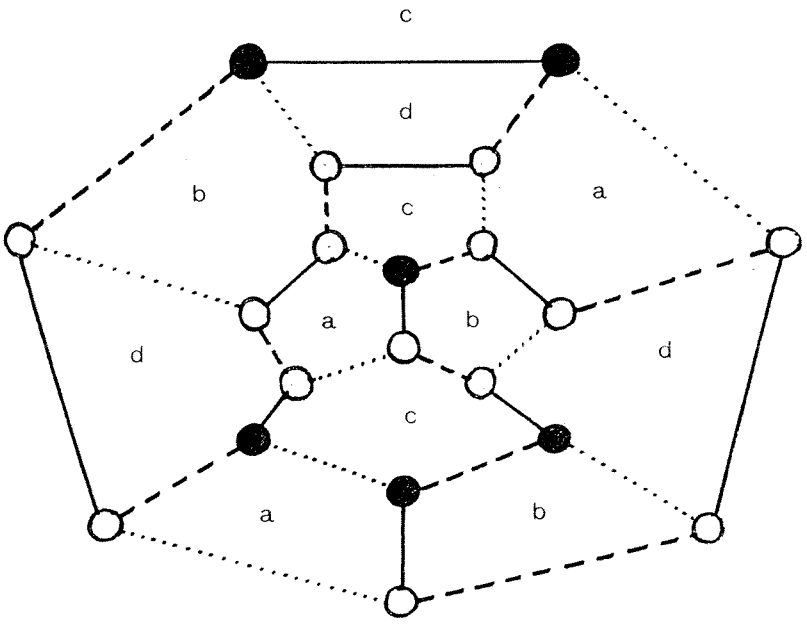



*Figure 2*
Un exemple de coloriage de pays, frontières et nœuds.

Nous allons démontrer l'équivalence de ces trois propositions selon le schéma $(1) \Longrightarrow (2) \Longrightarrow (3) \Longrightarrow (1)$.

### (A) 4 couleurs pour les pays implique 3 couleurs pour les frontières

Soit $(a), (b), (c), (d)$ les quatre couleurs affectées aux pays et $(x), (y), (z)$ les 3 couleurs que nous affecterons aux frontières. La figure 3 indique de quelle façon nous devons colorier les frontières en fonction des couleurs des pays adjacents. Par exemple nous attribuons la couleur $(z)$ à une frontière adjacente à des pays de couleur $(a)$ et $(d)$ ou bien $(b)$ et $(c)$ ...

Maintenant, un nœud est adjacent à trois pays de couleurs distinctes et cette même figure 3 montre que quel que soit le choix de ces trois couleurs parmi les quatre, les trois frontières adjacentes à ce nœud auront exactement une fois chacune des trois couleurs $(x), (y)$ et $(z)$.

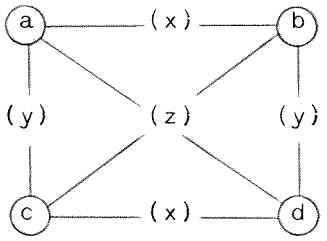



*Figure 3*
Le coloriage des frontières

### (B) 3 couleurs pour les frontières implique 2 couleurs pour les nœuds

Soit (0), (1), (2) les trois couleurs affectées aux frontières et $(+1)$ et $(-1)$ les deux couleurs que nous affecterons aux nœuds. (On ne confondra pas les couleurs (1) et $(+1)$.)

Atribuons à un nœud la couleur $(+1)$ si les couleurs (0), (1), (2) des frontières adjacentes se succèdent dans le sens trigonométrique et la couleur $(-1)$ dans le cas contraire.

Regardons ce qui se passe pour les nœuds adjacents d'un pays donné. La connaissance des couleurs des frontières successives de ce pays permet de déterminer la couleur de chacun des nœuds adjacents puisqu'en chaque nœud il n'y a qu'une troisième frontière qui est évidemment coloriée avec la troisième couleur encore disponible. Parcourons les frontières d'un pays dans le sens des aiguilles d'une montre : alors un nœud est de couleur $(+1)$ si la frontière passe de la couleur (0) à la couleur (1) ou bien de (1) à (2) ou bien de (2) à (0) et il est de couleur $(-1)$ dans les autres cas (fig. 4). Une autre façon de voir, consiste à remarquer que si la $\mathrm{i}^{\mathrm{ième}}$ frontière (en partant d'une origine arbitraire) est de couleur $x_i$ alors la couleur du nœud adjacent aux frontières numéro $i$ et $i+1$ est de couleur $(x_{i+1} - x_i$ modulo 3) en identifiant les couleurs (tant des frontières que des nœuds) leur valeur numérique. Maintenant si on fait la "somme" des couleurs des nœuds successifs, on trouve :

$$(x_2 - x_1) + (x_3 - x_2) + \cdots + (x_n - x_{n-1}) + (x_1 - x_n) = 0 \text{ modulo } 3.$$

Cela revient bien à dire que la différence du nombre de nœuds de chaque couleur est divisible par 3.

### (C) 2 couleurs pour les nœuds implique 4 couleurs pour les pays

Soit $(+1)$ et $(-1)$ les couleurs affectées aux nœuds (avec la règle de divisibilité par trois pour les nœuds adjacents à un pays donné) et notons (0), (1), (2), (3) les couleurs que nous affecterons aux pays. (Ici non plus on ne confondra pas les couleurs $(+1)$ et (1).)

Attribuons les couleurs (0) et (1) à deux pays arbitraires adjacents, puis continuons à colorier les pays selon la règle suivante :

Soit $N$ un nœud adjacent aux trois pays P1, P2 et P3 numérotés dans le sens trigonométrique autour de $N$. On attribue à P3 la couleur indiquée dans le tableau de la figure 5 selon les couleurs de $N$, P1 et P2.

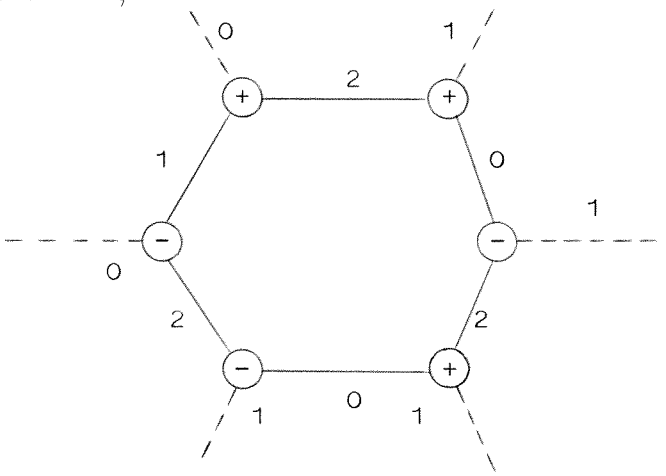



*Figure 4*
Le coloriage des nœuds

| N | P1 | P2 | P3 |
|---|---|---|---|
| +1 | 0 | 1 | 2 |
| | 1 | 2 | 0 |
| | 2 | 0 | 1 |
| | 3 | 2 | 1 |
| | 2 | 1 | 3 |
| | 1 | 3 | 2 |
| | 0 | 2 | 3 |
| | 2 | 3 | 0 |
| | 3 | 0 | 2 |
| | 3 | 1 | 0 |
| | 1 | 0 | 3 |
| | 0 | 3 | 1 |

| N | P1 | P2 | P3 |
|---|---|---|---|
| −1 | 2 | 1 | 0 |
| | 0 | 2 | 1 |
| | 1 | 0 | 2 |
| | 1 | 2 | 3 |
| | 3 | 1 | 2 |
| | 2 | 3 | 1 |
| | 3 | 2 | 0 |
| | 0 | 3 | 2 |
| | 2 | 0 | 3 |
| | 0 | 1 | 3 |
| | 3 | 0 | 1 |
| | 1 | 3 | 0 |

Les lignes ont été regroupées trois par trois.
Dans un tel regroupement les couleurs ne diffèrent que d'une permutation circulaire.
Par conséquent dès qu'il est attribué une couleur à deux pays adjacents à $N$, la couleur du troisième pays est déterminée de manière unique.
Le problème est maintenant de savoir si en coloriant les pays successifs adjacents à un pays donné, on retombe sur la couleur du premier pays après un tour complet ?

*Figure 5*
Règle de coloriage des pays

Effectuons le raisonnement autour d'un pays $P$ de couleur (0) dont on notera P1, P2 ... les pays adjacents successifs en tournant dans le sens trigonométrique. Alors la règle énoncée à la figure 5 montre que si le nœud est de couleur (+1) alors on passera de la couleur (1) à (2) ou bien (2) à (3) ou bien (3) à (1) et si le nœud est de couleur (−1) on passera pour les pays de la couleur (3) à (2) ou bien (2) à (1)

ou bien (1) à (3). En identifiant à nouveau les couleurs avec leur valeur modulo 3, on remarque que la couleur $(x_1)$ du pays $P_i$ est donnée par la formule :

$$(x_i) = (x_{i-1}) + (s_{i-1}) \text{ modulo } 3$$

étant entendu qu'on choisi le résultat dans l'ensemble $\{1, 2, 3\}$ et où $(s_i)$ est la couleur du nœud adjacent aux pays $P$, $P_{i-1}$ et $P_i$. Maintenant notons $(x'_1)$ la couleur que nous devrons attribuer à P1 après un tour complet autour de P. Nous avons :

$$\begin{array}{lll}
(x_2) & = (x_1) + (s_1) & \text{modulo } 3 \\
(x_3) & = (x_2) + (s_2) & \text{modulo } 3 \\
\ldots & & \\
(x_n) & = (x_{n-1}) + (s_{n-1}) & \text{modulo } 3 \\
(x'_1) & = (x_n) + (s_n) & \text{modulo } 3 \\
\hline
\text{par addition :} \ (x'_1) & = (x_1) + \Sigma(s_i) & \text{modulo } 3
\end{array}$$

ce qui prouve l'égalité de $(x_1)$ et $(x'_1)$ en raison de la condition imposée sur le coloriage des sommets ($\Sigma(s_i) = 0$ modulo 3) : figure 6.

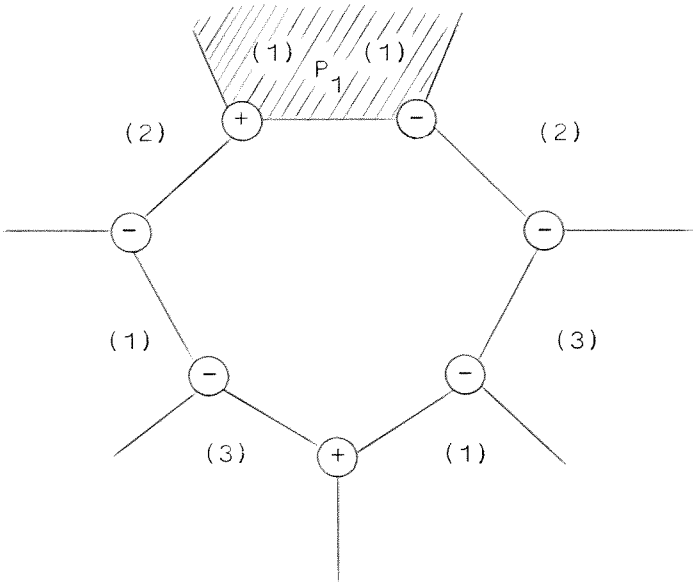



*Figure 6*
Coloriage des pays adjacents à un pays P donné.

Si maintenant le pays P est d'une couleur différente de (0), effectuons deux transpositions sur les couleurs (par exemple (0,1,2,3) → (1,0,3,2)), pour attribuer à P, provisoirement, la couleur (0). Comme la figure 5 permet de la voir, la double transposition évite de s'inquiéter de la couleur des nœuds. Alors le même raisonnement nous autorise à affirmer qu'après un tour complet autour de P, nous retombons sur les mêmes couleurs pour les pays adjacents.

Nous laissons le soin au lecteur de réinterpréter ce théorème soit en termes de graphes, soit en terme de polyèdres.

# CONCOURS MATHÉMATIQUES DU YORKSHIRE

YORKSHIRE TELEVISION

UNIVERSITÉ DE LEEDS

Depuis maintenant quelques années, l'université de Leeds en coopération avec la "*Yorkshire branch of the mathematical association*" a organisé des concours mathématiques pour les écoles. Presque tous les concours sont parrainés par la télévision du Yorkshire même si au début ils le furent par Waddingtons Ltd.

Les concours diffèrent selon l'âge des élèves. Celui concernant les 16-18 ans (c'est-à-dire les "*sixth-formers*" (*)) est baptisé "*projet*" et conduit à la présentation d'un rapport. Le travail se fait par équipe pendant plusieurs semaines pour être présenté à une date convenue à l'avance à l'université de Leeds. Les équipes y exposent alors leur travail et leur matériel éventuel, expliquent les problèmes qu'elles ont résolus et les progrès qu'elles ont réalisés. Le jury opère incognito parmi le public.

Les "*projets*" sont semi-ouverts, ils comportent souvent des questions dont on ne connaît la réponse que dans des cas particuliers. Ainsi le jury n'atten pas "*la solution*" au sens habituel. Les élèves trouvent cela plutôt déconcertant de prime abord. Cependant ils ont beaucoup de plaisir quand, comme c'est souvent le cas, ils découvrent que ce qui leur semblait une remarque presque triviale n'avait fait l'objet d'aucun travail de qui que ce soit auparavant. Parfois, ils découvrent, ce qui leurs occasionne encore plus de satisfaction, une méthode ou un point de vue qui leurs ouvre de nouveaux horizons mathématiques.

Cette année, trois thèmes étaient proposés à la sagacité des candidats :

1) **Dodos et manchoins** : c'est un problème de proies et prédateurs. L'analyse du cas présenté introduit à la notion de fractal.

2) **Les pentistes et le sol du temple** : c'est un problème de pavage du plan à l'aide de pentagones, pentagrammes et losanges.

3) **Un problème de codage** : où cinq messages doivent être décodés en utilisant diverses techniques, toutes basées sur le fait que les 32 symboles peuvent être considérés comme les éléments d'un corps fini. Les élèves doivent construire les tables d'addition et de multiplication dans ce corps.



(*) ce qui correspond sensiblement à notre première et terminale.

## DODOS ET MANCHOINS

Le dodo prospérait sur une île éloignée et son seul vrai problème était la quête de nourriture. Pendant la plus grande partie de l'année il y avait suffisamment à manger et le dodo se reproduisait lors de la courte saison des amours en pondant des œufs. Si on prend en compte les quelques accidents qui pouvaient arriver, aussi bien aux dodos qu'à leurs œufs, le nombre des dodos, après la saison de reproduction, avait été multiplié par $k$.

Mais il y avait l'hiver à affronter. Plus rien ne poussait et les dodos devaient se nourrir de baies. C'était une période dure et beaucoup mourraient. L'île aurait produit assez de baies pour nourrir 1000 couples de dodos pendant l'hiver si malheureusement pendant la saison de croissance les dodos ne mangeaient pousses et fleurs des buissons à baies et ne réduisaient ainsi leurs provisions de nourriture d'hiver.

Comptons dorénavant les dodos par couples pour éviter toute discussion sur leurs habitudes matrimoniales! Dans ce qui suit "*dodo*" signifie "*couple de dodos*". Supposons que $x$ dodos survivent après l'hiver. Pendant la saison de croissance et de reproduction ces $x$ dodos grignottent les buissons à baies et gâchent la nourriture qui aurait permis à $x$ dodos de passer l'hiver.

Mais après la reproduction, c'est pire car les jeunes aussi, dès qu'ils sont assez grands se mettent à manger les fleurs des baies. Les jeunes sont certes plus nombreux que les adultes, mais comme ils ont moins de temps pour endommager les buissons, ce sont tout compte fait, les réserves de $(x + kx/10)$ dodos qui sont irrémédiablement perdues au début de l'hiver.

Les dodos ne peuvent pas voler et ne sauraient gagner une autre île. Aussi au plus $1000 - x - kx/10$ dodos peuvent survivre à l'hiver.

Ainsi si le nombre de dodos après l'hiver, juste au début de la saison de reproduction est $x$, alors l'année suivante, à la même époque, ou bien il y a $[kx]$ dodos, si il y avait assez à manger pour tous durant l'hiver, ou bien seulement $[1000 - x - kx/10]$ dodos si certains dodos meurent de faim ou bien finalement il y a extinction totale des dodos s'il n'y a pas de nourriture du tout pendant l'hiver, c'est-à-dire si $x + kx/10 \geq 1000$. Comme il n'y a aucune raison que $k$ soit entier nous prendrons la partie entière du nombre entre crochets.

La première question est de savoir s'il y aura extinction de la race des dodos. Cela dépend d'abord de $k$. Et si extinction il y a, nous voudrions savoir combien de temps cela prendra. Ce qui dépend du nombre de dodos qu'il y a l'année 0.

La situation devînt bien plus compliquée quand l'île fut découverte par les manchoins. Ce sont des mammifères marins qui n'interfèrent pas normalement avec les dodos, cependant les manchoins doivent se reproduire sur terre et les jeunes sont, pendant quelques temps, incapables d'aller en mer. Les œufs de dodos sont alors une excellente source de nourriture pour eux et ils apprirent vite à dévaster les nids.

Normalement les manchoins augmentent d'année en année (ici encore, pour éviter de discuter de leurs habitudes sexuelles "*manchoins*" signifiera "*couples de manchoins*"). Ils n'augmentent pas très rapidement car ils n'ont qu'un ou deux petits et certains se perdent en mer. Si il y a $y$ manchoins au début de la saison de reproduction et que les jeunes ne soient pas détruits, ils seront $[3y/2]$ au début de la saison de reproduction suivante.

Cependant les jeunes manchoins doivent se nourrir. S'il n'y a pas assez d'œufs, ils meurent, chaque manchoin mangeant en moyenne 10 œufs avant de prendre la mer. Heureusement les dodos ne savent pas compter et un dodo n'est contrarié que si les manchoins mangent tous les œufs du nid. Ceci n'arrive pas souvent sauf si la proportion de manchoins par rapport aux dodos est suffisamment élevée.

D'un autre côté les dodos sont nettement plus gros que les jeunes manchoins et un dodo contrarié est très dangereux. Les attaques des manchoins par les dodos entraînent une diminution de la population des manchoins. La formule $[(x-2y)/10]$ donne le nombre de manchoins survivants à ces attaques sauf si : soit $2y \geq x$ auquel cas tous les jeunes manchoins sont tués et alors les adultes ne reviennent plus sur l'île; soit $x \geq 17y$ auquel cas les dodos laissent les manchoins tranquilles.

Les œufs mangés par les manchoins modifient bien sûr le nombre de dodos survivants lors de la saison de reproduction suivante. Ce nombre est alors, selon les cas : $[kx - 10y]$ s'il y a assez de nourriture pour tous durant l'hiver; $[1000 - x - y - kx/10]$ si certains dodos meurent de faim; d'un autre côté si $10y \geq kx$, les manchoins mangent tous les dodos dont la race disparaît; et enfin, si $x - y + kx/10 \geq 1000$, les dodos meurent tous de faim et leur race disparaît également de l'île.

Les manchoins peuvent donc contrôler le nombre de dodos de façon à ce qu'il n'excède jamais le nombre correspondant aux réserves hivernales. Mais d'autre part s'il y a trop de manchoins cela peut poser des problèmes de survie aux dodos. La race des dodos s'éteindra-t-elle? La réponse dépend de $k$ aussi bien que du nombre de dodos et de manchoins.

$\star\star\star\star\star\star\star\star\star$

Vous considérez d'abord la situation avant la découverte de l'île par les manchoins. La façon la plus simple d'aborder le problème est de faire quelques calculs pour voir ce qui se passe pour différentes valeurs de $k$ en partant de $x_0$ dodos l'année 0. Il n'est pas difficile de construire un diagramme montrant les valeurs de $x_0$ pour lesquelles il y a extinction des dodos au bout de deux ans, celles pour lesquelles il y a extinction en 4 ans ...

Je suggère que vous examiniez le cas $k = 4$. Vous verrez que le cas $k = 3$ est tout à fait différent du cas $k = 4$. Vous chercherez et trouverez pourquoi. Vous chercherez aussi à voir ce qui arrive quand $k = 2$ ou 5.

Une approche plus efficace du problème consiste à tracer les droites $y = x$, $y = kx$ et $y = 1000 - x - kx/10$ sur le même graphique et à voir comment on peut

construire les valeurs $x_0, x_1, \ldots$ successives. Vous serez peut-être alors capable de prédire graphiquement quand la race des dodos s'éteindra.

Ensuite vous pourrez considérer la situation après la découverte de l'île par les manchoins. Ce cas peut également se traiter par une méthode graphique ou bien par une méthode d'essais et d'erreurs. On étudiera d'abord le cas $k = 4$.

Voici quelques suggestions : supposons qu'il y ait, l'année 0, $x_0$ dodos et $y_0$ manchoins. Vous pourrez construire un graphique en coloriant d'une certaine façon ceux des points $(x_0, y_0)$ pour lesquels les dodos disparaissent en moins de cinq ans, d'une autre façon s'ils survivent au moins cinq ans mais meurent tous avant dix ans, etc ...

Il n'est pas du tout évident que l'allure de la carte change beaucoup pour $k = 3$, il y aura moins d'œufs pour les manchoins et un plus grand risque qu'ils tuent tous les dodos, mais alors il y aura un moindre risque que les dodos meurent d'inanition pendant l'hiver. Y-a-t-il des changements radicaux par rapport à cette situation si $k = 1, 2, 3, 5$ ou $6$?

## LES PENTISTES ET LE SOL DU TEMPLE

Il y a longtemps, les prêtres des pentistes voulurent construire un temple. Pour eux, 5 était un nombre sacré tandis que 4 devait être évité autant que possible, aussi toutes les céramiques qu'ils cuisirent pour paver le sol du temple carré furent des pentagones réguliers dont le côté avait une unité de longueur. Dans le sol on devait placer une céramique spéciale, dorée, ayant la forme d'une étoile régulière à cinq branches, ayant à nouveau des côtés d'une unité de longueur.

Le grand prêtre fut très chagriné quand il appris que quel que soit le nombre de céramiques pentagonales qu'ils cuisent, le sol ne pourrait être recouvert sans laisser de trous. (Ils n'avaient aucun moyen de couper les céramiques, bien qu'ils puissent en noyer des parties dans les murs.)

Après la décollation rituelle de quelques architectes, il admit finalement qu'il devait leurs permettre d'utiliser quelques céramiques ayant la forme d'un losange de côté unité et ayant un angle aigu de $\pi/5$ radian. Ces céramiques avaient bien sûr quatre côtés et cela fut considéré comme un événement de très mauvais augure. Cependant le prêtre essaya de limiter le pouvoir maléfique de ces carreaux en exigeant qu'on en utilise exactement cinq.

Après plusieurs expériences, les artistes ès-sol revinrent devant le grand prêtre pour l'informer de la taille maximum que pourrait avoir le temple. Il était évident que ce dernier serait beaucoup trop petit, aussi le prêtre accepta-t-il qu'on utilise vingt-cinq de ces carreaux porte-malheur : ni plus, ni moins.

Ceci ne permettait pas au temple d'être encore assez grand, mais les prêtres refusèrent absolument d'avoir un quelconque losange supplémentaire. Finalement ils décidèrent de lever des fonds de façon primitive et par des méthodes dont nous ne parlerons pas, ils récoltèrent l'argent pour une autre étoile d'or à cinq

branches, identique à la précédente. Ils construisirent le plus grand temple qu'ils purent avec les céramiques qu'ils avaient et la dimension satisfit tout un chacun pendant longtemps.

Cependant, au bout d'un siècle ou plus, les pentistes devenus très riches et très nombreux, décidèrent de doubler la taille du temple en en faisant un rectangle. Ils abattirent un mur du vieux temple et l'agrandirent en ajoutant un autre carré et, bien sûr, voulurent étendre le vieux pavage du sol. Cette fois-ci ils refusèrent d'utiliser davantage de losanges mais ils étaient assez riches pour se payer le luxe d'autant d'étoiles dorées que nécessaire, plus un nombre illimité de céramiques pentagonales ordinaires qu'ils cuisirent sur le champ.

Cela se révéla plus difficile qu'ils ne l'avaient pensé et finalement ils déposèrent le sol du vieux temple et le refirent complètement. Aussi durent-ils se contenter d'un nouveau temple rectangulaire de même largeur que le vieux et aussi long que possible.

Quelles sont les tailles maximum des temples qu'ils purent construire avec les céramiques qui étaient autorisées aux différentes étapes de cette histoire? Pouvaient-ils réellement prolonger le pavage du sol comme ils le pensaient en utilisant seulement des étoiles d'or? Combien d'étoiles d'or ont-ils utilisé pour le sol du dernier temple?

*********

En faisant des dessins ou en assemblant des pavés comme ceux indiqués, il est très facile d'accumuler les imperfections et d'obtenir ainsi des modèles qui sont grossièrement faux sur les bords. Notez que si une droite contient le côté d'un quelconque des pavés de céramiques, elle doit contenir plusieurs sommets et côtés d'autres pavés. Ainsi il y a bien des lignes qui vous guident et vous permettent de garder au modèle toute sa justesse.

## UN PROBLÈME DE CODAGE

Le problème est de décoder un ensemble de messages. Le code utilise 32 symboles qui sont : *, +, =, -, . et / ainsi que les lettres $A, B, C, \ldots, Z$. Le symbole / dénote aussi bien l'espace que, si nécessaire, la division. Le symbole * dénote la multiplication. De cette façon les messages peuvent contenir des formules algébriques.

Le code dépend du fait qu'on peut définir une arithmétique sur ces 32 symboles. C'est-à-dire qu'on peut dresser une **table d'addition** qui nous dit quel symbole nous obtenons si nous ajoutons ensemble deux symboles et on peut dresser une **table de multiplication** qui nous dit quel symbole nous obtenons si nous multiplions entre eux deux symboles.

Il y a donc un symbole qui joue le rôle de "*zéro*", c'est-à-dire que si nous prenons un symbole quelconque et que nous lui ajoutons le symbole "*zéro*" nous obtenons le symbole de départ. De même si nous multiplions un symbole quelconque par

le symbole "*zéro*", nous obtenons le symbole "*zéro*". Cela nous permet de définir l'**opposé** et la **soustraction** de la façon habituelle.

De façon analogue, il y a un symbole qui joue le rôle du "*un*", c'est-à-dire que si nous prenons un symbole quelconque et le multiplions par le symbole "*un*" nous obtenons le symbole de départ. Nous pouvons définir l'**inverse** et la **division** par n'importe quel symbole (sauf par le symbole "*zéro*") de la façon habituelle.

Ainsi nous pouvons calculer des puissances, trouver les racines de polynômes, etc ... tout comme dans l'arithmétique ordinaire.

Il y a bien sûr quelques résultats inhabituels puisqu'il n'y a qu'un nombre fini de symboles. Par exemple, si $x$ représente un symbole quelconque alors il est naturel d'écrire $2x = x + x, 3x = x + x + x \ldots$ mais comme il n'y a qu'un nombre fini de symboles, les symboles correspondants à $2x, 3x, \ldots$ ne sauraient être tous différents. De façon analogue, on peut calculer les puissances $x, x^2 = x * x, x^3 = x * x * x, \ldots$ qui là aussi ne peuvent être toutes différentes.

En comptant les éléments distincts que nous pouvons obtenir par ce moyen à partir d'un même élément $x$ nous pouvons apprendre bien des choses sur les tables d'addition et de multiplication. En fait nous avons seulement besoin de savoir quel est l'élément "*zéro*", quel est l'élément "*un*" et le comportement des puissances d'un seul autre élément pour déterminer ces tables complètement. Vous en aurez besoin pour décoder tous les messages.

Les messages 1 et 2 sont codés par remplacement. C'est-à-dire qu'un symbole donné est remplacé par le même symbole dans tout le texte. Ainsi le symbole le plus fréquent dans le message est remplacé par un symbole qui est celui qui apparaît le plus souvent dans le message codé.

Il en est de même en ce qui concerne le symbole le moins fréquent. De tels codes peuvent être déchiffrés en comparant la fréquence de chaque symbole du message codé avec la fréquence des lettres dans un texte ordinaire (*). Souvenez-vous que les espaces sont représentés par / et apparaissent souvent.

Les messages 3, 4 et 5 ne sont pas codés par remplacement et vous devez connaître les tables d'addition et de multiplication pour les décoder. Chaque méthode de codage est décrite dans un message antérieur.

---

(*) Attention! Les messages 1, 2, 3, 4 et 5 sont codés d'après un texte anglais. L'adaptation en français de tels messages est possible mais n'a pas été faite ici faute de temps.

# CONCOURS MATHÉMATIQUES DU YORKSHIRE

MESSAGE 1

GZ/WLE=OZ=WAOGIZMIGA/-XILGMWXAZHG/Z+/OBZMXZKXBOZMJW/ZLO//GSOCZZMJO
/DLVX=ZMXZVOZKXBOBZHG/ZL+=MWE=WOBZVDZMJOZ/DLVX=ZUZGABZMJOAZMJOZ/DLVX=ZDZHG/
GBBOBZMXZMJOZIO/+=MCZZMJW/ZKGAZVOZOUEIO//OBZVDZMJOZGIWMJLOMWKZ-XIL+=G
AOH/DLVX=.U*X=B/DLVX=RDC
/XLOZKGIOZJG/ZMXZVOZ+/OBZWAZWAMOIEIOMWASZMJW/Z/WAKOZMJOZ/DLVX=ZUZW/ZG
KXA/MGAMZ/DLVX=ZGABZKGAAXMZVOZ+/OBZMXZIOEIO/OAMZGAZ+APAXHACZZMJW/ZW/ZHJDZW
JGQOZ+/OBZMJOZHXIB/ZAOH/DLVX=ZXIZX=B/DLVX=ZMXZIOEIO/OAMZ+APAXHAZ/DLVX=/CZZMX
BOKXBOZWMZW/ZAOKO//GIDZMXZIOQOI/OZMJOZEIXKO//CZZDX+Z-WI/MZKG=K+=GMO
/DLVX=.AOH/DLVX=NDZGABZMJOAZX=B/DLVX=./DLVX=ZUCZZHOZJGQOZMXZVOZKGIO-+=ZJOIO
VOXG+/OZHOZJGQOZAXZ/DLVX=Z-XIZVIGKPOM/C
HJOAZDX+ZJGQOZBOKXBOBZMJW/ZLO//GSOZDX+ZHW==ZO--OKMWQO=DZPAXHZHJGM
U*/DLVX=RDZW/Z-XIZGADZ/DLVX=CZZMJW/ZLGPO/ZWMZOG/DZMXZ/OOZHJWKJZ/DLVX=
IOEIO/OAM/ZMJOZYOIXC
GAXMJOIZWLEXIMGAMZ/DLVX=ZW/ZMJOZXAOZ/X=QWASZMJOZOT+GMWXA
U*/DLVX=RD./DLVX=CZZDX+ZLGDZF+LEZMXZMJOZKXAK=+/WXAZ-IXLZMJOZSIOGMZBOG=ZX-
WA-XILGMWXAZMJGMZDX+ZSOMZMJGMZMJW/ZW/ZG==ZDX+ZAOOBZMXZXVMGWAZMJOZGBBWMWXAZGAB
L+=MWE=WKGMWXAZMGV=O/CZZMJGMZW/ZAXMZ/XCZZDX+ZHW==ZAOOBZMXZPAXHZMJGMZMJO
/DLVX=ZWZWAZMJW/ZGIWMJLOMWKZGKM/Z=WPOZMJOZA+LVOIZXAOZG/Z-GIZG/ZL+=MWE=WKGMWXA
W/ZKXAKOIAOBCZZMJGMZW/ZIOG==DZG==ZMJOZWA-XILGMWXAZDX+ZAOOBCZZDX+ZKGAZBOB+KO
MJGMZWRWZW/ZMJOZYOIXZ/DLVX=Z+/WASZMJOZIOLGIP/ZHOZLGBOZGVX+MZGBBWASZGAZO=OLOAM
MXZWM/O=-CZZWAZ-GKMZDX+ZHW==ZT+WKP=DZVOZGV=OZMXZOUEIO//ZOGKJZ/DLVX=ZG/ZG
EX=DAXLWG=ZWAZUZBWQWBOBZVDZGAXMJOIZEX=DAXLWG=ZWAZUC
DX+ZHW==ZEOIJGE/Z-WABZMHXZOUEIO//WXA/Z-XIZMJOZ/GLOZ/DLVX=CZZMJW/ZW/
OAX+SJZMXZMO==ZDX+ZG==ZDX+ZHGAMZV+MZWMZW/ZJGIBZMXZ/OOZJXHZMXZBOB+KOZMJO
GBBWMWXAZGABZL+=MWE=WKGMWXAZMGV=OC
MJOZAOUMZLO//GSOZSWQO/ZGBBWMWXAG=ZWA-XILGMWXACZZDX+ZBXZAXMZIOG==DZAOOB
WMZV+MZWMZHW==ZLGPOZDX+IZMG/PZL+KJZOG/WOICZZMJOZLOMJXBZ+/OBZWAZMJOZKXBOZW/
GSGWAZGZ/WLE=OZ=WAOGIZMIGA/-XILGMWXACZZMJW/ZMWLOZWMZW/ZSWQOAZVD
AOH/DLVX=.Q*X=B/DLVX=RDC

MESSAGE 2

CUV=EDKH*DSUNNDWJIEDAHD*CEDJDCAJAUCAU=JNDPEAWHGDAHDGE=HGEDAWECED.UFCA
ASHDPECCJMECDAWEKDWJIEDAHD+ED/*UAEDNHVMBDD+HAWDPECCJMECD=HVAJUVDEIEFKDCKP+HN
CHPESWEFEDHFDHAWEFDJVGDEIEVDUV=N*GEDODJVGDYDJVGDLB
HV=EDKH*DWJIEDGE=HGEGDAWUCDPECCJMEDUADCWH*NGDPJXEDUADEJCUEFDAHDSFUAE
EIEFKDCKP+HNDJCDJD-HSEFDH.DQDJVGDWEV=EDAHD=HP-NEAEDAWEDP*NAU-NU=JAUHVDAJ+NEB
XVHSUVMDAWJADIDFE-FECEVACDQDC/*JFEGDCWH*NGDPJXEDUADEIEVDEJCUEFB
AHD=HP-NEAEDAWEDJGGUAUHVDAJ+NEDKH*DVEEGDAHDXVHSDJDFENJAUHVD+EASEEVDAWE
-HSEFCDH.DQBDDUVD.J=AD.FHPDAWEDFEPJFXCDPJGEDJ+H*AD=H*VAUVMDAWEDGUCAUV=A
ENEPEVACDHVEDMEACD+KDAJXUVMD-HSEFCDUADUCD-HCCU+NEDAHDGEG*=EDAWJADQDP*CA
CJAUC.KDJD-HNKVHPUJNDSUAWD=HE..U=UEVACDJNNDE/*JNDAHDUDH.DGEMFEEDJADPHCAD.UIEB
.UVGUVMDAWUCD-HNKVHPUJNDCWH*NGD+EDJDMFEJADWEN-DAHDKH*B
AWEDVEQADPECCJMED=JVVHAD+EDGE=HGEGD+KDJDCAJAUCAU=JNDPEAWHGDJCDUADUCDVHA
JDFE-NJ=EPEVAD=HGEBDD+JCU=JNNKDUADUCDH+AJUVEGD+KDJVDH-EFJAUHVDHVD-JUFCDH.
CKP+HNCDSWU=WD=JVD+EDGEC=FU+EGD+K
VESCKP+HNQZJRHNGCKP+HNQT+RHNGCKP+HNKT=
VESCKP+HNKZGRHNGCKP+HNQTERHNGCKP+HNKT.B
UADCAJFACDSUAWDAWED.UFCAD-JUFDH.DCKP+HNCDUVDAWEDPECCJMEDJVGDFE-NJ=EC
AWECED+KDAWEDVESDCKP+HNCDH+AJUVEGD+KDAWUCD.HFP*NJBDDAWEVDAWEDCE=HVGDJVGDAWUFG
CKP+HNCDJFEDAJXEVD.FHPDAWED-JFAUJNNKD=HGEGDPECCJMEDJVGDMUIEVDAWEDCJPE
AFEJAPEVADJVGDCHDHVBDDAHDGE=HGEDKH*DSUNNDWJIEDAHDCHNIEDJD-JUFDH.DCUP*NAJVEH*C
E/*JAUHVCDUVDCKP+HNU=DJFUAWPEAU=B

YORKSHIRE TELEVISION - UNIVERSITÉ DE LEEDS

MESSAGE 3

```
=IBGS-WIIBPZFTF/CZNGDV*NS=*R.T/DSAVOQFFDALSQARGKCQIQYLFPUADQAEYBGKCQIYPXDELG
Z=IUYBOFHJFTF/CVNTAL*+/TELGRNWRYVSMZXWRVRW=FZHC/PGAAANUJGQT*NDZXSJOXT+B-WBC
+-P+*+/TELWTU
```

MESSAGE 4

```
TAKEFHFDTO+CGFWN+VORS.IKOWGPUUIEGUNPJBIRTAKQOCQMDOUJ+U=-YIA-+IRDJWB
..VNLDOQ=WL+RAJDGF.G/FKMQISTJ*KHYANLO=Y
W-W*F=+RMRMJKNJWKI//KPPAE-N.PFLNC==FA=NP+J=.AU-KIDBHQLRUHTDJV+*PHH=AQ*CFHYEC
-QSIIXJCMX=TRE=KIXCQMDOPWQ.BXKSNBEIAEKKM*/JTWBSRVKP*F/IXMRHHLPHHTITAICM/WU
OCYALVP=APVQNL/NLFCL
```

MESSAGE 5

```
O=G-M=XMBYWJQA-MEBX
ZNYYY=PP=RYWZLZN=VVNS
=BZN+JOW+-DQXWGKGFA=GFJDFX
QHLB=WH-=KTPJPDJ+ET
INRY-=BDOBSL*J.W=NT+ET
F/AR/Q*G.+Y=AK*GTVIUDMH=
/ZXJDJDWHMVLVWBMWHMH.HP.EL
OFTQZBL/QHEKYA*GZL/RIUOEBMGH
EBBTVSAOMVH.TFSXPD-MG/BMU
.*+-J*SXKKHHRPGF*G.F/ZE+E
SUGTU*PJPDMWHA=GFBZHMWMS*GS=A/Y
MF*A=XZ-M+J=KE=VNVNOKEKYGMH=
```

...et nous eûmes deux services de trois plats chacun. Le premier se composait d'une épaule de mouton coupée en triangle équilatéral, d'une pièce de bœuf en rhomboïde et d'un pudding cycloïde. Le second service amena sur la table deux canards montés en forme de violon, des saucisses et des boudins affectant l'allure de flûtes et de hautbois, une poitrine de veau en harpe et des pains coniques, cylindriques, en forme de parallélogrammes et autres figures géométriques...

Ma connaissance des mathématiques m'aida beaucoup à comprendre leur syntaxe, basée sur cette science et celle de la musique, art dans lequel j'ai quelque habileté. Ils expriment leurs idées en lignes et figures, parlant du beau demi-cercle d'un sourcil ou de l'ellipse des yeux pour flatter une jolie femme et faisant entrer sinus, tangente, ovale, parabole ou diamètre dans le bagage poétique de l'amour...

Les voyages de Gulliver
Jonathan SWIFT.

# A VOS STYLOS

Dix problèmes vous ont déjà été proposés dans cette rubrique. C'est certainement trop tôt pour un bilan, mais l'expérience acquise depuis deux ans et demi est une bonne occasion pour rectifier un peu le tir.

1) Nous recevons peu de réponses pour chaque problème. Ceci pouvant être dû au délai finalement assez court entre la parution d'un énoncé et l'impression de sa solution, nous allons vous laisser chercher un peu plus longtemps en différant de trois mois la solution de chaque problème. C'est pourquoi vous trouvez aujourd'hui deux nouveaux énoncés, le 11 qui sera corrigé selon l'ancien régime dans deux numéros et le 12 qui le sera seulement dans trois numéros.

2) Nous recevons encore bien moins de propositions d'énoncés. Vos contributions seraient pourtant d'autant mieux venues qu'elles élargiraient l'éventail des sujets proposés et seraient, sans doute, plus proches des préoccupations des lecteurs.

---

## PROBLÈME 9

### Enoncé

Soit $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ telle que $f(0,0) = 0$ et que $f(x,y)$ soit le plus petit entier qui ne soit pas de la forme $f(x',y)$ avec $x' < x$ ou $f(x,y')$ avec $y' < y$. Fournir une méthode de calcul de $f$ aussi simple que possible.

### Solution

A partir des écritures binaires de $x$ et $y$, on obtient celle de $f(x,y)$ en effectuant, chiffre à chiffre, l'addition sans retenue, c'est-à-dire suivant la table

| | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

La démonstration peut se faire en vérifiant, par récurrence sur $n$, que

- pour $x, y < 2^n, f(x,y)$ existe, est unique et donnée par l'algorithme ci-dessus;
- $\forall x < 2^n \{f(x,y), y < 2^n\} = \{0, 1, \ldots 2^n - 1\}$
- $\forall y < 2^n \{f(x,y), x < 2^n\} = \{0, 1, \ldots 2^n - 1\}$.

C'est en effet vrai pour $n = 0$ (car $f(0,0) = 0$); et si c'est vrai pour $n$, alors pour $x$ et $y$ plus petits que $2^n$,

$$f(x + 2^n, y) = 2^n + f(x,y)$$

(appliquer l'hypothèse de récurrence à $g(x,y) = f(x+2^n, y) - 2^n$)

$$f(x, y+2^n) = 2^n + f(x,y)$$

(appliquer l'hypothèse de récurrence à $h(x,y) = f(x, y+2^n) - 2^n$) et

$$f(x+2^n, y+2^n) = f(x,y);$$

d'où le résultat $n+1$.

---

## PROBLÈME 10

(proposé par D. DUMONT)

Soit l'ensemble $E = \{0,1,3,4,7,9,12,13,16,19,\ldots\}$ dont on propose trois définitions :

**Définition 1** : $E$ est l'ensemble des entiers $n$ pouvant s'écrire sous la forme

$$n = x^2 + xy + y^2 \text{ avec } x, y \text{ entiers } \geq 0.$$

**Définition 2** : $E$ est l'ensemble des entiers $n$ pouvant s'écrire sous la forme

$$n = x^2 - xy + y^2 \text{ avec } x, y \text{ entiers } \geq 0.$$

**Définition 3** : $E$ est l'ensemble des entiers $n$ pouvant s'écrire sous la forme

$$n = x^2 + 3y^2 \text{ avec } x, y \text{ entiers } \geq 0.$$

**1°)** Montrer que ces trois définitions sont bien équivalentes.

**2°)** Montrer que $E$ est stable pour la multiplication, c'est-à-dire que $n_1 \in E$ et $n_2 \in E \Rightarrow n_1 n_2 \in E$.

**3°)** Soit $P = \{3,7,13,19,31,37,\ldots\}$ l'ensemble des nombres premiers appartenant à $E$. Montrer que $P$ se compose de 3 et de l'ensemble des nombres premiers de la forme $6k+1$, et que pour ces nombres premiers la représentation sous la forme $x^2+3y^2$ est unique. En outre, si $p$ est de la forme $6k+1$ alors $4p$ s'écrit de manière unique comme suit :

$$4p = x^2 + 27y^2 \qquad (x, y \text{ entiers } > 0).$$

**Indication** Penser à FERMAT pour démontrer que $p$ premier de la forme $6k+1$ implique $p$ est de la forme $x^2+3y^2$.

---

## PROBLÈME 11

**Enoncé**

Trouver le plus petit entier positif $k$ pour lequel il existe un polynôme à coefficients entiers, de degré $k$, de la forme

$$P(x) = x^k + a, x^{k-1} + \cdots + a_k$$

et tel que, pour tout entier $x \in \mathbb{Z}$, $P(x)$ soit divisible par un milliard.

---

## PROBLÈME 12

**Enoncé**

Soit $\Omega$ un ouvert non vide du plan. Deux points $C$ (chat) et $S$ (souris) sont mobiles dans $\Omega$ et choisissent chacun à chaque instant leur vitesse, le module de cette dernière étant toutefois limité à un intervalle $[O, V]$, où la vitesse maximale $V$ est la même pour $C$ et $S$. On demande, selon la forme de $\Omega$, si $C$ a une stratégie imparable pour finir par rattraper $S$, si au contraire $S$ a un moyen certain de toujours échapper à $C$, ou si ni l'un ni l'autre de ces deux cas ne se présente.

---

## HOMMAGE AUX MATHÉMATIQUES

Ô chiffres, ô axiomes, ô théorèmes,
Je voudrais vous dire "Je t'aime" (ô hypocrisie!!)
Et pourtant j'ai souvenance
De quelques mémorables nuits blanches,
Où Thalès et son compère Pythagore
Se disputaient mon esprit tourmenté.
Les chiffres se livraient à une danse
aussi diabolique que frénétique.
Dans l'enfer de l'algèbre,
les suites se déchaînaient.
Ô combien j'ai souffert pour vous,
cruelles équations!
Mais je ne vous en tiendrai pas rigueur.
Mathématiques, je vous aime.

Camille HAUPTMANN
Annick ZECHEL
élèves du Lycée J. Monnet.

Jean-Pierre BOUDINE, Francis CASIRO, Roger CUCULIÈRE et Pierre AUDIN, avec l'A.L.T.M. (*) ont le plaisir de vous informer de la parution prochaine d'un nouveau magazine de mathématiques qui complètera la gamme inaugurée par TANGENTE :

## QUADRATURE

**QUADRATURE** est destiné aux étudiants (DEUG, Licence), aux élèves des classes préparatoires, aux enseignants, et pourra intéresser tout un public curieux de Mathématiques, souhaitant rester en contact avec une discipline toujours en mouvement.

**QUADRATURE** paraîtra six fois par an, sur 64 pages par numéro.

SOMMAIRE du numéro 1 :

*Fractions continues (1), par F. Jabœuf – Actualités des fractions continues, par R. Douady – Groupe de frise, par Y. Hellegouarch – Brachysto... Tauto... Iso... chrone, par P. Audin – Alan Turing, vue de l'homme, vue de la machine, par F. Casiro – Quelles formules pour les Instituts financiers ?, par G. Pagès et F. Carrance – Pas à Pas... cal (1 : d'Euclide à Bézout), par J. Césaro.*

et

*Questions de Cosmologie, par J.-P. Petit – Calcul logique chez les Indiens des Prairies, par G.-Th. Guilbaud – Etymologie du mot "UN", par G. d'Hauterive – Voir la forme du nombre "e", traduit de l'American Math. Monthly, par F. Casiro – La plus ancienne quadrature connue, par J. Itard – et : Informations, interview (journées 89 de l'A.P.M.E.P., salon Mathécom), tuyaux, adresses, échos, notes de lecture, enfin la rubrique problèmes et solutions par R. Cuculière.*

**Le numéro un de QUADRATURE est paru à l'occasion du salon"MATHECOM" qui s'est tenu les 27, 28 et 29 octobre 1989 au lycée Henri IV, à Paris à l'initiative de la régionale Ile-de-France de l'APMEP et de la SMF.**

L'abonnement annuel, à adresser aux éditions du choix, 4 rue des Carmélites 95640 Breancon, se montera à 180 F, mais est fixé à 150 F seulement jusqu'au 15 janvier 1990.

On peut recevoir un spécimen sur demande
contre 10 F en timbres pour frais d'envoi.

(*) L'A.L.T.M. : Association pour la Lecture de Textes de Mathématiques, association régie par la loi de 1901