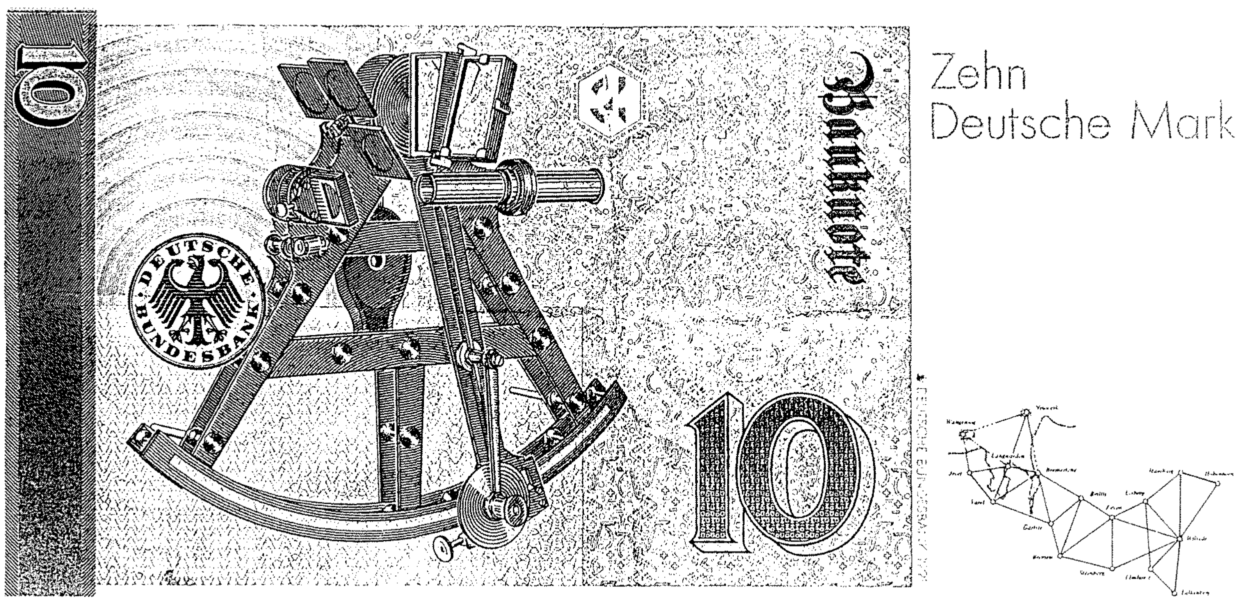
L'OUVERT

JOURNAL DE L'A.P.M.E.P. D'ALSACE ET DE L'I.R.E.M. DE STRASBOURG
n° 72 – SEPTEMBRE 1993 I.S.S.N. 0290 - 0068



NOTRE COUVERTURE :
Billet de 10 DM

Recto et verso du billet de 10 DM à la mémoire de C. F. Gauss. L'œuvre de ce mathématicien de renommée mondiale est immense. La "'Bundesbank" n'a retenu que son travail en statistique (avec le calcul des erreurs) à partir de la courbe qui porte son nom, ainsi que son travail en géodésie avec la cartographie de l'Allemagne du nord et l'amélioration des instruments de mesure.

Le portrait du mathématicien se détache sur quelques monuments de Göttingen, dont l'université sût accueillir et retenir Gauss toute sa vie.

EDITORIAL

Les réformes suivent, chaque ministre veut la sienne. Les raisons pour lesquelles certaines aboutissent et d'autres non, paraissent fort conjoncturelles : la personnalité du ministre, la plus ou moins grande force de l'opposition, l'air du temps ... mais toujours la même idée sous-jacente : "Comment dépenser moins d'argent en accueillant plus d'élèves" ? Les premières victimes ont bien entendu été les disciplines dites mineures : travaux manuels, arts plastiques, musique, instruction civique, E.P.S. ont soit disparu, soit vu leurs horaires réduits (et je ne parle pas de leur position dans l'emploi du temps des élèves) sans que cela soulève d'opposition tant de la part des syndicats que des associations de parents d'élèves ou de l'opinion publique. Au diable le tiers temps pédagogique!

Aujourd'hui, suprême astuce, arts plastiques et musique essentiellement passent de deux à quatre heures hebdomadaires en lycée, mais avec un coefficient proportionnellement moindre au bac. Si ce n'est pas là une illustration du baiser de la mort, c'est au moins un cadeau empoisonné. Les collègues et les parents qui se plaignent de l'aspect trop théorique de notre enseignement pourront toujours mettre leurs enfants dans des conservatoires de musique, des ateliers d'arts plastiques ou des clubs de sport, moyennant finances bien sûr!

Maintenant on s'attaque aux mathématiques. Que n'a-t-on pas dit sur notre discipline? Des critiques souvent fort justes qui ont permis une remise en question de notre enseignement grâce essentiellement aux I.R.E.M. et qui nous placent en pointe dans la recherche en didactique, dans l'histoire de la discipline, dans la formation continue des enseignants. Mais aussi, malheureusement, des critiques non fondées qui risquent de détruire l'école mathématique française et son rôle mondial. Mais voilà, on trouve un prix Nobel (Gilles de Gennes) proclamant bien haut que l'enseignement des maths fait par des physiciens c'est mieux, on trouve un ministre cherchant à économiser des postes des maths tant pour des raisons budgétaires qu'à cause d'un flux insuffisant de certifiés, on trouve des médias, critiquant l'horaire trop important des maths dans notre enseignement alors qu'il ne s'agit que de la section C où les parents s'obstinent à mettre leurs enfants même plus littéraires que scientifiques.

Qui sera la prochaine victime (*)? Mais chacun continue de s'arc-bouter sur sa discipline, persuadé de pouvoir ainsi échapper à la catastrophe alors que la seule solidarité permettrait de faire face et de sauvegarder un enseignement de qualité, équilibré, et qui s'adresse à tous les élèves.

Je rappelle à ce propos ce texte de Martin Niemöller, écrit certes dans des circonstances beaucoup plus dramatiques mais la solidarité comme la liberté ne s'usent que si l'on ne l'utilise pas : "*Il faut se battre sur tous les fronts de la liberté. Quand les nazis s'en sont pris aux communistes, je me suis tu, car je n'étais pas communiste. Quand ils ont emprisonné les sociaux-démocrates, je n'ai rien dit, car je n'étais pas social-démocrate. Quand ce fut le tour des catholiques, je n'ai pas protesté, car je n'étais pas catholique. Quand ils ont emmené les juifs, je n'ai pas bougé, car je n'étais pas juif. Quand ils sont venus chez moi, il n'y avait plus personne pour protester*".

J. LEFORT.

(*) P.S. : Le Ministre vient de proposer la création d'écoles privées de Langue subventionnées par les collectivités locales.

Erratum : Dans le numéro 71, pour les textes relatifs à la couverture, il faut lire systématiquement "Peutinger" et non "Peutiger" .

SOMMAIRE

N° 72 – 1993

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)*

80 F (130 F/2 ans) pour les membres A.P.M. d'Alsace.
120 F (200 F/2 ans) pour la France ou l'Étranger.

◇ *Prix du numéro* : 35.– F
Tarif avion : nous consulter.
Paiement à l'ordre de Monsieur l'Agent Comptable de l'U.L.P. (IREM)

SUR LES CARRÉS DANS CERTAINES SUITES DE FIBONACCI

Maurice Mignotte (*)

Résumé.– Chacun connaît la suite de Fibonacci 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144... En 1964, J.H.E. Cohn a démontré que les seuls carrés de cette suite sont $0, 1$ et 144, démonstration que nous reproduisons au 1er paragraphe.

La suite de Fibonacci vérifie la récurrence $F_n = F_{n-1} + F_{n-2}$ pour $n \geq 2$. On considère ici les suites $u_n = u_n(a)$ définies par $u_0 = 0, u_1 = 1$ et $u_n = au_{n-1} - u_{n-2}$ pour $n \geq 2$, où a est un entier ≥ 3. (On notera que $u_n(3) = F_{2n}$.) Nous montrons que pour $a \geq 4$, alors u_n n'est ni un carré, ni le double, ni le triple d'un carré, ni six fois un carré pour $n > 3$, sauf si $a = 338$ et $n = 4$. Ce travail a été réalité en collaboration avec A. Pethö.

Dans toute la suite, on notera par $\square$ le carré d'un entier non nul. Les lettres p et q désigneront toujours des nombres premiers.

0.– Rappel sur les suites récurrentes linéaires sur deux termes

• On définit une telle suite par

$$\begin{cases} u_n = a\ u_{n-1} - b\ u_{n-2}, & \text{pour } n \geq 2, \\ u_0, u_1 \text{ donnés,} \end{cases}$$

a et b dans $\mathbb{C}$.

On démontre que si α et β sont les racines complexes de l'équation (dite équation caractéristique) $r^2 = ar - b$ alors l'ensemble des solutions est donné par :

a) si $\alpha \neq \beta$: $u_n = A\ \alpha^n + B\ \beta^n$, A et B étant obtenus à l'aide des conditions initiales $u_0 = A + B$ et $u_1 = A\alpha + B\beta$;

b) si $\alpha = \beta$: $u_n = (An + B)\alpha^n$, avec, pour les conditions initiales $u_0 = B$ et $u_1 = (A + B)\alpha$.

• Dans le cas particulier où a et b sont entiers : avec Δ, discriminant de l'équation caractéristique, positif ($a^2 - 4b > 0$) on a : $\alpha = \frac{a+\sqrt{\Delta}}{2}$ et $\beta = \frac{a-\sqrt{\Delta}}{2}$.

Si $u_0 = 0$ et $u_1 = 1$ on trouve alors $u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$. L'exemple fondamental est alors la suite de Fibonacci : $F_n = F_{n-1} + F_{n-2}$, $F_0 = 0$, $F_1 = 1$.

Si $u_0 = 2$ et $u_1 = a$ on trouve alors $u_n = \alpha^n + \beta^n$. L'exemple fondamental est alors la suite de Lucas : $L_n = L_{n-1} + L_{n-2}, L_0 = 2, L_1 = 1$.

(*) Conférence IREM de Strasbourg - Régionale APMEP d'Alsace donnée le 16 décembre 1992.

• Voici les premiers éléments de ces deux suites :

$$F_n : 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144\dots$$
$$L_n : 2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322\dots$$

Ces suites présentent des propriétés remarquables dont voici les plus utiles pour le présent article :

$$\begin{aligned} L_n^2 - 5F_n^2 &= (-1)^n 4 \\ L_{2m} - L_m^2 &= (-1)^{m+1} 2 \\ F_{2m} &= F_m L_m \\ 2L_{m+p} &= 5F_m F_p + L_m L_p \\ 2F_{m+p} &= F_m L_p + L_m F_p \end{aligned}$$

dont les démonstrations sont immédiates en remplaçant F_n et L_n par leur valeur respective $[(\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2})^n]\frac{1}{\sqrt{5}}$ et $[(\frac{1+\sqrt{5}}{2})^n + (\frac{1-\sqrt{5}}{2})^n]$. Ces formules permettent de donner un sens à F_n et L_n pour n négatif.

1.– Les suites de Fibonacci et Lucas

Nous allons d'abord montrer que les seuls carrés de la suite de Fibonacci (F_n) sont 0, 1 et 144 et que les seuls carrés de la suite de Lucas sont 1 et 4.

Modulo 4, ces deux suites sont de période 6 :

n	0	1	2	3	4	5	6	7	...
F_n mod 4	0	1	1	2	3	1	0	1	...
L_n mod 4	2	1	3	0	3	3	2	1	...

De la relation $L_n^2 - 5F_n^2 = (-1)^n 4$ et de la table ci-dessus, on déduit que

$$(F_n, L_n) = \begin{cases} 1, & \text{si } n \not\equiv \pmod 3, \\ 2, & \text{si } n \equiv \pmod 3. \end{cases}$$

a) Considérons d'abord la suite de Lucas. La relation $L_{2m} = L_m^2 - 2(-1)^m$ montre que L_n ne peut être un carré lorsque n est pair. Supposons donc n impair. On peut se limiter à $n > 0$, sinon L_n est négatif. On supposera de plus $n \geq 5$ (on notera que $L_1 = 1$ et $L_3 = 4$ sont des carrés). On peut écrire $n = c + 2tk$, avec $t = 3^r$, $k > 0$, $k \equiv \pm 2 \pmod 6$, ce qui prouve que k est pair, et enfin $c = 1$ ou 3. Les formules

$$2L_{m+2k} = 5F_m F_{2k} + L_m L_{2k} = 5F_m F_k L_k + L_m(L_k^2 - 2) \equiv -2L_m (\text{mod } L_k)$$

jointes au fait que L_k est impair [puisque $k \equiv \pm 2 \pmod 6$ implique $L_k \equiv 3$ (mod 4)] montrent que, par simplification par 2 :

$$L_n = L_{c+2tk} \equiv -L_c \equiv -1 \text{ ou } -4 \pmod{L_k}.$$

Si L_n est un carré, alors -1 est donc un carré modulo L_k, mais, comme $L_k \equiv 3$ modulo 4, ceci est impossible. Donc L_n ne peut être un carré pour $n \geq 5$.

b) Passons maintenant à la suite de Fibonacci.

• Si $n \equiv 1 \pmod 4$. Supposons $n \neq 1$ (sinon $F_n = 1$ est un carré). Comme plus haut, écrivons $n = 1 + 2tk$, avec $t = 3^r$ et $k \equiv \pm 2 \pmod 6$. Les formules

$$2F_{m+2k} = F_m L_{2k} + L_m F_{2k} = F_m(L_k^2 - 2) + F_k L_k L_m \equiv -2F_m \pmod{L_k}$$

et le fait que L_k est impair, impliquent

$$F_n \equiv -1 \pmod{L_k}.$$

Comme nous l'avons déjà vu, cette congruence implique que F_n n'est pas un carré.

• Si $n \equiv 3 \pmod 4$, le changement de n et $-n$ nous ramène au cas précédent.

• Si $n = 2m$ est pair, alors $F_n = F_m L_m = \square$ et on peut supposer $n > 0$.

• Si $m \not\equiv 0 \pmod 3$ on a $(F_m, L_m) = 1$ et donc $F_m = \square$ et $L_m = \square$, ce qui impose $m = 1$ ou 3; le seul carré pour F_n est 1.

• Si $m \equiv 0 \pmod 3$ on a $(F_m, L_m) = 2$ et donc $F_m = 2y^2$ et $L_m = 2z^2$. Si m est impair, on a $z^4 - 5y^4 = -1$, ce qui est impossible modulo 8. Si $m = 2m'$, alors $F_{m'} L_{m'} = 2y^2$. Si m' est impair, on a $F_{m'} = 2\,\square$ et $L_{m'} = \square$, donc $m' = 1$ ou 3; d'où $F_n = 1$ ou 144. Si m' est pair alors $F_{m'} = \square$ et $L_{m'} = 2\,\square$ ...On voit ainsi que les nombres de Fibonacci d'indices $n/4$, $n/16$...sont des carrés. Mais, comme F_6 et F_{48} ne sont pas des carrés, ce dernier cas est impossible. [Il n'est pas nécessaire de calculer F_{48} : si $F_{48} = \square$ alors $F_{24} = 2\,\square$, puis $L_{12} = 2\,\square$, mais $L_{12} = 322$.]

Nous avons donc démontré le résultat suivant dû à J.H.E. Cohn, [C].

THÉORÈME 1.– *Les seuls carrés de la suite de Fibonacci sont 0, 1 et 144, tandis que les seuls carrés de la suite de Lucas sont 1 et 4.*

2.– Énoncés des nouveaux résultats

Soient a et b deux entiers non nuls premiers entre eux. On suppose $\Delta = a^2 - 4b > 0$ et on pose

$$\alpha = \frac{a+\sqrt{\Delta}}{2}, \beta = \frac{a-\sqrt{\Delta}}{2}, u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{\alpha^n - \beta^n}{\sqrt{\Delta}}, v_n = \alpha^n + \beta^n \ (n \text{ entier } \geq 0).$$

Récemment, McDaniel et Ribenboim [McD-R] ont étudié les carrés et les doubles de carrés parmi les valeurs des suites u et v. Ils ont démontré des résultats très précis qui impliquent en particulier l'énoncé suivant.

THÉORÈME 2.– *Si a et b sont impairs et premiers entre eux et si u_n est un carré ou le double d'un carré alors $n \leq 12$.*

Dans ce travail, nous ne considérons que le cas où $b = 1$ (1), mais nous supposons a quelconque et nous indiquons une méthode pour démontrer le résultat suivant.

THÉORÈME 3.– *Soit a un entier ≥ 3, et soit $\Delta = a^2 - 4$. Nous posons $\alpha = (a + \sqrt{\Delta})/2$ et $\beta = (a - \sqrt{\Delta})/2$, et nous considérons la suite de Fibonacci $u_n = u_n(a) = (\alpha^n - \beta^n)/(\alpha - \beta)$. Alors, pour $a \geq 4$, u_n n'est ni un carré, ni le double, ni le triple d'un carré, ni six fois un carré pour $n > 3$, sauf si $a = 338$ et $n = 4$.*

Dans la suite de l'article, nous nous proposons de donner les principales étapes de la démonstration sans entrer dans tous les détails techniques.

3.– Réduction au cas d'un indice impair

Lemme 1.– *Soit $p \geq 5$ un nombre premier. Alors, tout diviseur premier de u_p est $\geq p$. De plus, si $p | u_p$ alors p divise Δ.*

Schéma de la démonstration : Si q est un diviseur premier de u_p alors q ne divise pas u_n pour $0 < n < p$. De plus, p divise $q + (\frac{\Delta}{q})$ (2), donc $q \geq p - 1$. Ainsi $q \geq p$, avec égalité seulement si $q|\Delta$. **CQFD**

Si p est un nombre premier et x un entier non nul, on désignera par $w_p(x)$ le plus grand entier k tel que p^k divise x.

Lemme 2.– *Soit m un entier dont le plus grand diviseur premier est $q > 3$. Si $u_m = \square$ ou $2\,\square$ ou $3\,\square$ ou $6\,\square$, alors $u_q = \square$ ou $u_{q^2} = \square$.*

Schéma de la démonstration : On remarque d'abord que u_q est impair et que $u_q | u_m$.

Soit r un diviseur premier de u_q. Soit $s = w_r(u_q)$ (3), alors $r^{s+1} | u_n$ si, et seulement si, $rq|n$. D'après le Lemme 1, $r \geq q$.

Si $r > q$, alors $w_r(u_m) = s$ et s est pair. Il s'ensuit que u_q est un carré si $q \not| \Delta$.

Reste le cas où $q|\Delta$ et où u_q n'est pas un carré. Alors $w_q(u_q)$ est impair et $w_q(u_{q^2}) = 1 + w_q(u_q)$ est pair. Les autres diviseurs de u_{q^2} sont $> q$ et l'argument précédent montre que u_{q^2} est un carré. **CQFD**

Lemme 3.– *Soient $a \geq 3$ et $m = 2^3 3^t$ avec $s, t \geq 0$ et $s + t \geq 2$. Il existe alors un nombre premier $p \geq 5$ tel que $w_p(u_m)$ soit impair, excepté pour $a = 338$, $m = 4$ et $u_m = 6214^2$ et pour $a = 3$ et $m = 6$, auquel cas $u_m = 12^2$.*

Démonstration : Plus tard, nous démontrerons que l'assertion est vraie pour $m = 4, 6$ et 9. Supposons qu'elle soit vraie pour toutes les paires (s, t) avec $2 \leq s + t < S$. Soient s et t tels que $s + t = S$ et soit $m = 2^3 3^t$. Si $s > 0$ soit $m' = m/2$, sinon soit $m' = m/3$. Dans le premier cas, $u_m = u_{m'} v_{m'}$, tandis que $u_m = u_{m'}(v_{m'}^2 - 1)$ dans le second cas (ces deux formules sont immédiates en

(1) On notera qu'alors α et β, solutions de l'équation caractéristique, sont inverses l'un de l'autre.
(2) Le symbole $(\frac{x}{q})$ est le symbole de Legendre, caractère quadratique de x modulo q.
(3) Si r est un nombre premier et x un entier non nul on désigne par $w_r(x)$ l'entier h tel que $r^h | x$ et $r^{h+1} \not| x$.

utilisant les définitions de u et de v).

L'hypothèse de récurrence prouve qu'il existe p premier > 3 avec $w_p(u_{m'})$ impair. Comme $(u_{m'}, v_{m'}) = 1$ ou 2 et $(u_{m'}, v_{m'}^2 - 1) = 1$ ou 3, on a $w_p(u_m) = w_p(u_{m'})$ et l'assertion est démontrée pour la paire (s,t) considérée.

Considérons d'abord le cas $m = 4$.

Si $u_4 = \square$ alors $a(a^2-2) = \square$. Si a est impair, $(a, a^2-2) = 1$ et $a^2 - 2 = \square$, ce qui est impossible. Si a est pair alors $a = 2x^2, a^2 - 2 = 2y^2$, donc $2x^4 - 1 = y^2$, et Ljungreen [L] a montré que ceci implique $(x,y) = (1,1)$ ou $(13, 239)$. Donc $a = 338$.

On a toujours $v_4 \neq \square$, de plus $v_4(338) \neq 2\,\square$, donc $u_m(338) \neq \square$ et $\neq 2\,\square$ pour $s > 2$. On constate que $w_{113}\{u_{12}(338)\} = w_{9601}\{u_8(338)\} = 1$.

Si $u_4 = 2\,\square$, a doit être pair. Et on a $a = \square$, $a^2 - 2 = 2\,\square$, soit $a = 4x^2$ et $16x^4 - 2 = 2y^2$: impossible modulo 8.

Si $u_4 = 3\,\square$ ou $6\,\square$ alors, comme $u_4 = a(a^2-2)$, on a $3|a$ et $a^2 - 2 = \square$ ou $2\,\square$. Il est clair que la première relation est impossible, et la seconde est impossible modulo 9. D'où le résultat pour $m = 4$.

Supposons maintenant que $u_9 = \square, 2\,\square, 3\,\square$ ou $6\,\square$. Il est facile de voir que

$$u_9 = u_3(v_3^2 - 1) = (a^2-1)(a^3 - 3a + 1)(a^3 - 3a - 1).$$

Le nombre $v_3^2 - 1$ est toujours impair.

Si $3|a$ alors $(u_3, v_3^2 - 1) = 1$ et $3 \not| u_9$, donc, si $u_9 = \square$ alors $u_3 = \square$ et si $u_9 = 2\,\square$ alors $v_3 = \square$, ces deux cas sont donc impossibles.

Si $a \equiv 1 \bmod 3$ alors ni 2, ni 3 ne divisent $a^3 - 3a + 1$ et $a^3 - 3a + 1 = \square$ est impossible modulo 3, il existe donc p premier > 3 avec $w_p(a^3 - 3a + 1) = w_p(u_9)$ impair.

Si $a \equiv -1 \bmod 3$ alors ni 2 ni 3 ne divisent $a^3 - 3a - 1$. L'équation $a^3 - 3a - 1 = x^2$ impose $a \equiv 1 \bmod 4$. Si $a^3 - 3a + 1 = y^2$ alors $x^2 - y^2 = 2$, ce qui est impossible. Donc $a^3 - 3a + 1 = 3y^2$, et ainsi $(\frac{3}{a}) = 1$. Mais, puisque $a \equiv 1 \bmod 4$, on a $(\frac{3}{a}) = (\frac{a}{3}) = (\frac{-1}{3}) = -1$: contradiction.

Enfin, supposons que $u_6 = \square$, $2\,\square$, $3\,\square$ ou $6\,\square$. Notons que $u_6 = u_3 v_3$ et $u_3 = a^2 - 1, v_3 = a(a^2-3)$.

Si $u_6 = \square$ alors $u_3 = 2\,\square$ et $v_3 = 2\,\square$. Donc a impair, $a^2 - 1 = 2x^2, a(a^2-3) = 2y^2$. Ce qui donne $a = 3z^2$ et $a^2 - 3 = 6t^2$. D'où les conditions $9z^4 - 1 = 2x^2$ et $9z^4 - 3 = 6t^2$. On a la solution évidente $z = 1$, le lemme 4 ci-dessous montre que c'est la seule. Ainsi, $a = 3$. On constate que $w_7\{u_{12}(3)\} = w_{17}\{u_{18}(3)\} = 1$.

Si $u_6 = 2\,\square$ alors $u_3 v_3 = 2\,\square$, avec $u_3 \neq \square$, donc $v_3 = \square$, $u_3 = 2\,\square$ et a impair. Comme $v_3 = a(a^2-3)$ et que $a^2 - 1 = 2\,\square$, $a^2 - 3 \neq 2\,\square$, on a $a = 3z^2, a^2 - 3 = 9z^4 - 3 = 3t^2, 9z^4 - 1 = 2x^2$. Modulo 5, ceci implique $z \not\equiv 0$ et donc $z^4 \equiv 1$, puis $6 \equiv 3t^2$, ce qui est impossible.

Restent les cas $u_6 = 3\,\square$ ou $6\,\square$.

• $v_3 = \square$ implique $a = 1$. Dans ce cas $3|u_3$, ainsi $3 \not| a$ et donc $3 \not| v_3$. Donc $a = \square$ et $a^2 - 1 = \square$, ce qui impose $a = 1$.

• $u_3 = \square$ n'est possible que pour $a = 1$.

• $v_3 = 2\,\square$, $u_3 = 3\,\square$ ou $u_3 = 6\,\square$ ne peuvent avoir lieu que pour $a = 2$. En effet $3 \not| a$, et donc $a^2 - 3 = \square$ ou $2\,\square$. La première équation possède la solution unique $a = 2$, la seconde est impossible modulo 3.

• $u_3 = 2x^2$, $v_3 = 3\,\square$ ou $6\,\square$. Alors a est impair et divisible par 3. Donc $w_3(a^2 - 3) = 1$ et $a = y^2$. On aboutit à l'équation $y^4 - 2x^2 = 1$ qui, d'après Ljungreen [L], ne possède que la solution triviale $y = 1$. On constate que $w_7\{u_{12}(3)\} = 1$ et que $u_{18} = u_6(v_6^2 - 1) = u_6 \times 103683$, où $103683 = 3 \times 17 \times 19 \times 107$. Ce qui achève la démonstration du lemme. **CQFD**

Lemme 4.– *Le système d'équations en nombres entiers positifs*

$$3Z^2 - 1 = 2Y^2 \text{ et } 9Z^2 - 1 = 2X^2$$

n'a que la solution banale $Z = 1$.

Démonstration : La première équation implique $6Z^2 - (2Y)^2 = 2$. Or dans l'anneau $\mathbb{Z}[\sqrt{6}]$, 2 admet la décomposition : $2 = (5 - 2\sqrt{6})(2 + \sqrt{6})^2$ où $5 - 2\sqrt{6}$ est une unité (4) et $2 + \sqrt{6}$ est un élément premier. Or dans cet anneau toutes les unités sont de la forme $\pm(5 + 2\sqrt{6})^k$, $k \in \mathbb{Z}$. Par suite la première équation s'écrit aussi

$$(\sqrt{6}Z + 2Y)(\sqrt{6}Z - 2Y) = (2 + \sqrt{6})^2(5 + 2\sqrt{6})^{-1}$$

et donc il existe un entier $s \in \mathbb{Z}$ tel que

$$2Y + \sqrt{6}Z = (2 + \sqrt{6})(5 + 2\sqrt{6})^s$$

et par conjugaison $2Y - \sqrt{6}Z = (2 - \sqrt{6})(5 - 2\sqrt{6})^s$ ce qui conduit à

$$Z = \frac{(2 + \sqrt{6})(5 + 2\sqrt{6})^s - (2 - \sqrt{6})(5 - 2\sqrt{6})^s}{2\sqrt{6}}.$$

De la même façon avec la seconde relation, en se plaçant dans l'anneau $\mathbb{Z}[\sqrt{2}]$ où les unités sont de la forme $\pm(3 + 2\sqrt{2})^k$ on trouve:

$$3Z + \sqrt{2}X = (3 + 2\sqrt{2})^t$$
$$\text{et } 3Z - \sqrt{2}X = (3 - 2\sqrt{2})^t, t \in \mathbb{Z},$$

(4) dans un anneau une unité est un élément inversible.

ce qui conduit à : $Z = \frac{(3+2\sqrt{2})^t+(3-2\sqrt{2})^t}{6}$. L'égalisation des deux expressions permet d'écrire :

$$\frac{(3+\sqrt{6})(5+2\sqrt{6})^s}{(3+2\sqrt{2})^t} = \frac{1+(3-2\sqrt{2})^{2t}}{1+(5-2\sqrt{6})(5-2\sqrt{6})^{2s}}.$$

Il en résulte que la quantité

$$\Lambda = s\log(5+2\sqrt{6}) - t\log(3+2\sqrt{2}) + \log(3+\sqrt{6})$$

vérifie $|\Lambda| \leq 4(5+2\sqrt{6})^{-2s}$. Une application de l'estimation de M. Waldschmidt [W] fournit la borne $t \leq 10^{21}$. Ensuite, on procède comme et Davenport en [B-D] : une première application du lemme ci-dessous avec $q = 337472905923410699064273181$ conduit à la nouvelle borne $t \leq 30$. En choisissant cette fois $q = 264$ on trouve $t \leq 4$. Puis on vérifie que la seule solution est $t = 1$, d'où $Z = 1$. **CQFD**

Lemme 5.– (Baker-Davenport, [B-D]).– *Soit* $\varphi = a_1\xi_1 + \xi_2 + a_2$, *où les* a_i *sont entiers,* $0 < a_1 < B$, *et les* ξ_i *réels, tel que* $|\varphi| < e^{-\lambda a_1}, \lambda > 0$. *Soit* q *un entier positif tel que* $|q\varphi| < 1/q$ *et* $\varepsilon = ||q\xi_2|| - B/q > 0$, *alors* $a_1 \leq \log(q/\varepsilon)/\lambda$ *(où* $||x||$ *est la distance à l'entier le plus proche).*

4.– Principes de la démonstration du théorème

4.1. Etude de certaines unités

Les racines du polynôme $X^2 - aX + 1$ sont α et β. On considère le polynôme $X^4 + \Delta X^2 - \Delta$ dont les racines sont $\theta = i\sqrt{\alpha\sqrt{\Delta}}$, $-\theta$, $\theta_1 = \sqrt{\beta\sqrt{\Delta}}$ et $-\theta_1$.

Le corps $K = \mathbb{Q}(\theta)$ est un corps quartique où les conjugués de θ sont $-\theta, \theta_1$ et $-\theta_1$ et qui admet exactement deux plongements réels. D'après un théorème de Dirichlet (voir, par exemple, [P-K]), le rang du groupe des unités de K est donc égal à deux. On remarque que α et $\varepsilon = 1 + \theta$ sont des unités de K (c'est-à-dire des unités de l'anneau des entiers de K).

On peut montrer que $\{\alpha, \varepsilon\}$ est un système fondamental d'unités de l'anneau $\mathbb{Z}[\theta]$.

4.2. Utilisation de la théorie de Baker

Supposons que le nombre $u_n = (\alpha^n - \beta^n)/(\alpha - \beta)$ soit le carré d'un entier x, alors $\alpha^{n+1} = \alpha\sqrt{\Delta}x^2 + \alpha\beta^n$. Lorsque n est impair, $n = 2m+1$, cette relation implique

$$\alpha^{2(m+1)} = (\theta x + \beta^m)(-\theta x + \beta^m),$$

donc $\theta x + \beta^m$ est une unité. D'où l'existence d'entiers u et v tels que

$$\theta x + \beta^m = \beta^u\varepsilon^v,\ -\theta x + \beta^m = \beta^u\varepsilon^{-v},\ \theta_1 x + \alpha^m = \alpha^u\varepsilon_1^v \text{ et } -\theta_1 x + \alpha^m = \alpha^u\varepsilon_1'^v.$$

En eliminant x entre ces relations, il vient

$$\theta_1\beta^u(\varepsilon^v - \varepsilon^{-v}) = \theta\alpha^u(\varepsilon_1^v - \varepsilon_1'^v).$$

D'où l'on tire facilement

$$u \approx \frac{v-1}{2}\Big(1 - \frac{\log 2}{\log a}\Big) \quad \text{et} \quad m \approx \frac{v-1}{2}\Big(1 + \frac{\log 2}{\log a}\Big).$$

Il existe un entier k tel que

$$\Lambda = v \log(\varepsilon/\bar{\varepsilon}) - ik\pi$$

vérifie $|\Lambda| \le 4\beta^{2m}$. Par ailleurs, en utilisant les résultats de [M-W], on peut minorer la "forme linéaire" $|\Lambda|$ par

$$|\Lambda| \ge \exp(-270 \times 2^4 \times \log(a^2) \times (7.5 + \log v)^2).$$

Il en résulte que $v \le V = 1.1 \times 10^6$. En développant $\log(\varepsilon/\bar{\varepsilon})$, on obtient

$$\Lambda = i\pi\Big(v - \frac{2v}{\pi}(\frac{1}{\theta} + \frac{1}{3\theta^2} + \cdots) - k\Big).$$

On voit que pour $v = k$ on a $|\Lambda| \ge 1/(2a)$, ce qui contredit la majoration précédente de Λ ; on a donc $v \ne k$, ce qui implique $|v| \ge \pi(a-4)/2$. Par ailleurs, $|v| \ge 1.9m$ pour $a \ge 700000$. Donc $a \le 800000$.

Un calcul sur ordinateur montre que $|\Lambda| \ge 3a^{-3}v^{-2}$ pour $16 < a \le 800000$ et $0 < v \le V$. Pour ces valeurs de a, il s'ensuit que l'on a $v \le 5$. D'où $a \le 7$: contradiction.

Pour $4 \le a \le 16$, on a $|\Lambda| \ge 1/(2700v^2)$ si $0 < v \le V$. D'où $v \le 15$, puis $m \le 9$, et une vérification directe montre qu'il n'y a pas de solution.

Le théorème est alors une conséquence directe des lemmes 2 et 3. (On peut remarquer que $u_3 = a^2 - 1$ n'est jamais un carré.)

Références

[B-D] A. BAKER et H. DAVENPORT.– The equations $3x^2 - 2 = y^2$ et $8x^2 - 7 = z^2$; *Quart. J. Math. Oxford*, **2**, 1969, p. 129-137.

[C] J.H.E. COHN.– On square Fibonacci numbers; *J. London Math. Soc.*, **39**, 1957, p. 537-540.

[L] W. LJUNGGREEN.– Zur Theorie der Gleichung $x^2 + 1 = Dy^4$; *Avh. Norske Vid. Akad. Oslo*, No. 5, **1**, 1942.

[McD-R] W.L. McDANIEL et P. RIBENBOIM.– Squares and double-squares in Lucas sequences; *C.R. Math. Rep. Acad. Sci. Canada*, Vol. 14, n° 2, 3, 1992, p. 104-108.

[M-P] M. MIGNOTTE et A. PETHÖ.– Sur les carrés dans certaines suites de Lucas; manuscrit, Strasbourg, sept. 1992.

[M-W] M. MIGNOTTE et M. WALDSCHMIDT.– Linear forms in two logarithms and Schneider's method, III; *Annales Fac. Sci. Toulouse*, 1990, p. 43-75.

[P-Z] M. POHST & H. ZASSENHAUS.– *Algorithmic algebraic number theory*, Cambridge University Press, 1989.

[W] M. WALDSCHMIDT.– Minorations de combinaisons linéaires de logarithmes de nombres algébriques; *Canadian J. Math.*, à paraître.

ÉQUATIONS DIOPHANTIENNES

Marc HINDRY (*)

INTRODUCTION

Si on se donne une équation polynomiale à deux variables $P(x, y) = 0$, on peut considérer cette équation comme celle d'une courbe $(\mathcal{C})$ dans le plan affine $\mathbb{A}^2$. La recherche des solutions en nombres rationnels se traduit par la recherche des points à coordonnées rationnelles de $(\mathcal{C})$. C'est un exemple fondamental d'équation diophantienne.

Il est préférable, d'un point de vue géométrique, de se placer dans le plan projectif $\mathbb{P}^2$ (que l'on peut définir comme l'ensemble des droites de $\mathbb{A}^3$ passant par l'origine). Pour cela, si le polynôme P s'écrit $\Sigma_{i,j} a_{i,j} x^i y^j$ et si d est son degré total, on construit le polynôme homogène associé : $\bar{P}(X, Y, Z) = \Sigma_{i,j} a_{i,j} X^i Y^j Z^{d-i-j}$.

L'équation $\bar{P}(X, Y, Z) = 0$ définit alors une courbe dans le plan projectif qui contient d'ailleurs la courbe affine de départ mais à laquelle on a rajouté des "points à l'infini" (les points de $\mathbb{P}^2$ avec $Z = 0$).

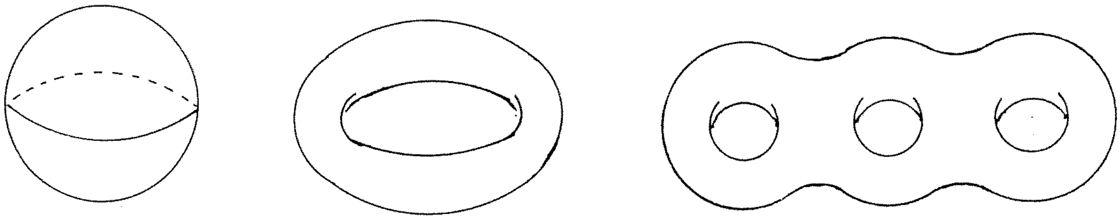
L'étude diophantienne de ces courbes mélange arithmétique et géométrie. En particulier, les travaux sont guidés par l'analogie entre corps de nombres et corps de fonctions. Par exemple on construit $\mathbb{Q}$ à partir de $\mathbb{Z}$ et de même on construit $\mathbb{C}(T)$, l'ensemble des fractions rationnelles à coefficients dans $\mathbb{C}$ à partir de $\mathbb{C}[T]$ l'anneau des polynômes. Cette analogie féconde n'est d'ailleurs pas entièrement comprise bien que largement exploitée.

I.– GENRE D'UNE COURBE ALGÉBRIQUE

Les points complexes du plan projectif $\mathbb{P}^2(\mathbb{C}) = \{(X, Y, Z) \in \mathbb{C}^3 - \{(0,0,0)\}/\{(X, Y, Z) = (\lambda X, \lambda Y, \lambda Z)\}$ forment un espace compact et la courbe $\bar{P}(X, Y, Z) = 0$ est également compacte. On est obligé de constater le conflit de deux vocabulaires : pour le géomètre algébriste il s'agit d'une courbe alors que pour le géomètre différentiel c'est une surface de Riemann! Comme telle, c'est une sphère à g trous.

On distingue trois cas selon que $g = 0$, $g = 1$ ou $g \geq 2$.

(*) Conférence IREM de Strasbourg - Régionale APMEP d'Alsace donnée le 17 mars 1993



$g = 0$
droite ou conique
dans $\mathbb{P}^2$

$g = 1$
cubique
dans $\mathbb{P}^2$

$g = 3$
quartique
dans $\mathbb{P}^2$

1) $g = 0$. Voici deux exemples :

$$X^2 + Y^2 - Z^2 = 0\ (C_1)$$
$$X^2 + Y^3 - 3Z^2 = 0\ (C_2).$$

D'un point de vue diophantien, l'étude de ces courbes est bien comprise; on dispose du théorème suivant :

> **Théorème :** *Si $(\mathcal{C})$ est une courbe de genre 0 alors ou bien $(\mathcal{C})$ ne possède aucun point rationnel ou bien $(\mathcal{C})$ admet une infinité de points rationnels que l'on peut paramétrer explicitement.*

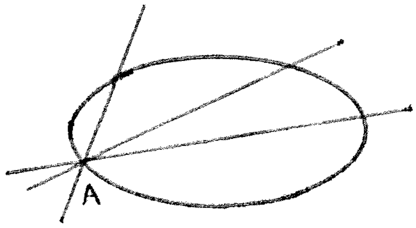
On peut voir aisément par une étude modulo 4 que la courbe $\mathcal{C}_2$ ne possède pas de points rationnels (le point $(0, 0, 0)$ est interdit!). Quant à la courbe $\mathcal{C}_1$ on peut la traiter de manière arithmétique : on écrit $Y^2 = Z^2 - X^2 = (Z + X)(Z - X)$, on peut supposer que $pgcd(X, Y, Z) = 1$ et on voit facilement que Z est impair et X, Y de parités opposées. Quitte à échanger X et Y on peut supposer X pair et Y impair. Ensuite si $d = pgcd(X + Z, Z - X)$ alors $d = 1$. En effet d divise $X + Z$ et $Z - X$ dont $2X$ et $2Z$ et donc 2. Mais $d = 2$ est impossible car $X + Z$ est impair.

Ainsi $Z + X$ et $Z - X$ doivent être des carrés et on obtient :

$$\begin{cases} Z + X = U^2 \\ Z - X = V^2 \end{cases} \quad \text{ou encore} \quad \begin{cases} X = 1/2(U^2 - V^2) \\ Y = UV \\ Z = 1/2(U^2 + V^2) \end{cases}$$

avec U et V entiers impairs premiers entre eux.

De manière plus géométrique, si la conique $\mathcal{C}_1$ possède un point rationnel A, le faisceau de droites passant par A et de pente rationnelle recoupe la courbe en un point rationnel et tous les points rationnels s'obtiennent ainsi :



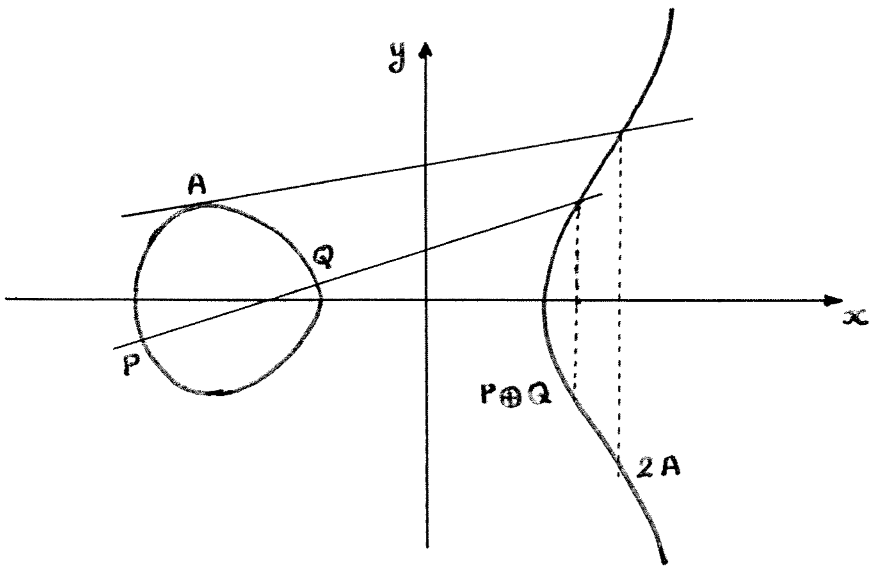
En prenant $A = (1,0,1)$ et en coupant par la famille de droites $D_{U,V}$: $U(X-Z)+VY=0$ on retrouve les mêmes solutions.

2) $g=1$. Ici encore on distingue deux cas : ou bien la courbe n'a pas de points rationnels ou bien elle en a un (au moins). Dans le deuxième cas il existe une loi de groupe naturelle sur l'ensemble des points rationnels que l'on peut mettre en évidence ainsi :

On démontre que l'on peut transformer la courbe pour obtenir une équation dite de Weierstrass :

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

avec $4a^3+27b^2 \neq 0$. L'élément neutre est le point à l'infini $e=(0,1,0)$. On construit le point $P \bigoplus Q$ ainsi : on trace la droite passant par P et Q (si $P=Q$ on choisit la tangente en P à la courbe) ; elle coupe la courbe en un troisième point R. Le point $P \bigoplus Q$ est le symétrique de R par rapport à l'axe des X. On peut tracer la courbe affine (où le point e est à l'infini) :



(la loi de groupe sur la courbe $y^2 = x^3 + ax + b$)

Il est facile de voir que les coordonnées de $P \bigoplus Q$ s'expriment rationnellement en fonction des coordonnées de P et de Q.

Théorème (Mordell 1922) *Le groupe des points rationnels est de type fini; c'est-à-dire que toutes les solutions s'obtiennent à partir d'un nombre fini de points par le procédé des cordes et tangentes.*

Malheureusement on ne sait pas, à l'heure actuelle, trouver a priori les générateurs.

3) $g \geq 2$. Dans l'article de 1922, Mordell avait conjecturé le théorème suivant :

Théorème (Faltings 1983). *Soit C une courbe de genre ≥ 2, alors elle possède seulement un ensemble fini (éventuellement vide) de points rationnels.*

Exemple : pour $n \geq 4$ l'équation de Fermat $X^n + Y^n = Z^n$ ne possède qu'un nombre fini de solution. Malheureusement, on ne sait pas déterminer effectivement les solutions dont le théorème garantit la finitude. Une curieuse application est la remarque suivante dûe à Heath-Brown : Soit $\mathcal{F}$ l'ensemble des entiers pour lesquels le "grand" théorème de Fermat est vrai alors si p est un nombre premier, il existe m_0 (dépendant de p) tel que pour $m \geq m_0$ on ait $mp \in \mathcal{F}$. Moyennant quelques calculs on s'aperçoit que :

$$\lim_{X \to \infty} X^{-1} \text{ cardinal } \{n \leq X \text{ tel que } n \in \mathcal{F}\} = 1.$$

C'est-à-dire : "le grand théorème de Fermat est vrai avec probabilité un".

II.– ANALOGIES ENTRE $\mathbb{Z}$ et $\mathbb{C}[T]$.

Tout nombre entier non nul peut s'écrire (dans $\mathbb{Z}$)

$$n = \varepsilon p_1^{m_1} \dots p_r^{m_r}$$

où les p_i sont des nombres premiers, les m_i sont dans $\mathbb{N}^*$ et ε vaut $+1$ ou -1.

De la même façon tout polynôme non nul de $\mathbb{C}[T]$ s'écrit : $P = \varepsilon p_1^{m_1} \dots p_r^{m_r}$ où les p_i sont des polynômes unitaires du premier degré $p_i = T - \alpha_i$, les m_i sont dans $\mathbb{N}^*$ et ε est une constante non nulle.

Sur $\mathbb{Z}$ on dispose de la valeur absolue usuelle que nous notons $|n|_\infty$. On peut aussi définir pour chaque p un ordre de divisibilité

$$\text{ord}_p(n) = \max\{m/p^m \text{ divise } n\}.$$

Sur $\mathbb{C}[T]$ on dispose du degré noté *deg* et pour chaque $\alpha \in \mathbb{C}$ de l'ordre de divisibilité

$$\text{ord}_\alpha(P) = \max\{m|(T-\alpha)^m \text{ divise } P\}.$$

Pour un entier nous avons la formule du produit :

$$\log |n|_\infty - \sum_p \text{ord}_p(n) \log p = 0.$$

Analogue de celle valable pour les polynômes :

$$\deg(P) - \sum_{\alpha} \mathrm{ord}_{\alpha}(P) = 0.$$

Si l'on pose $|n|_p = p^{-\mathrm{ord}_p(n)}$, la formule du produit s'écrit

$$\sum_{v} \log |n|_v = 0$$

où v est soit le symbole ∞ soit un nombre premier. Dans $\mathbb{Z}$, sauf pour $v = \infty$ on a

$$|a+b|_v \leq \max\left(|a|_v, |b|_v\right)$$

ce qui montre que $|.|_p$ est une norme ultramétrique. Par contre dans $\mathbb{C}[T]$, la relation d'ultramétricité est vraie même pour le degré. En fait on peut interpréter le degré comme l'ordre en un certain point en se plaçant sur la droite projective $\mathbb{P}^1 = \mathbb{C} \cup \{\infty\}$. Alors $\deg(P) = \mathrm{ord}_{\infty}(P)$.

On trouve ainsi certaines limites aux analogies. En fait on peut dire que travailler sur $\mathbb{Z}$ est plus difficile que sur $\mathbb{C}[T]$.

La théorie de schémas de Grothendieck permet de considérer $\mathcal{P} = \{p \text{ premier}\}$ comme les points d'une courbe appelée le spectre de $\mathbb{Z}$, mais les recherches dues notamment à Arakelov permettant de travailler sur l'objet $\mathcal{P} \cup \{\infty\}$ sont encore bien incomplètes!

III.– THÉORÈME DE FERMAT POUR LES POLYNÔMES

Nous choisissons d'illustrer la puissance que donne d'une part l'ultramétrisation et d'autre part l'existence d'une dérivation dans $\mathbb{C}[T]$ en donnant la preuve du théorème suivant, où $r(P)$ désigne le nombre de racines distinctes d'un polynôme P.

> **Théorème** (Mason) *Si $P + Q + R = 0$ où P, Q, R sont des polynômes non constants premiers entre eux de $\mathbb{C}[T]$ alors :*
>
> $$\max(\deg P, \deg Q, \deg R) \leq r(PQR) - 1.$$

Voyons d'abord comment ce théorème entraîne “Fermat pour les polynômes”. Supposons que A, B, C soient des polynômes non constants premiers entre eux tels que :

$$A^n + B^n + C^n = 0$$

alors comme deg $A^n = n \deg A$ et $r(A^n) = r(A)$ on a :

$$n \max(\deg A, \deg B, \deg C) \leq r(ABC) - 1 \leq \deg A + \deg B + \deg C - 1$$

ce qui est clairement impossible dès que $n \geq 3$ puisque par hypothèse $\deg A \geq 1, \deg B \geq 1, \deg C \geq 1$.

Venons-en à la preuve du théorème, écrivons :

$$\begin{array}{lll} P(T) = \alpha_0 \Pi_{i=1}^{p} (T - \alpha_i)^{l_i} & \text{avec donc} & p = r(P) \\ Q(T) = \beta_0 \Pi_{i=1}^{q} (T - \beta_i)^{m_i} & & q = r(Q) \\ R(T) = \gamma_0 \Pi_{i=1}^{s} (T - \gamma_i)^{n_i} & & s = r(R). \end{array}$$

Considérons alors le déterminant $\Delta = \left|\begin{smallmatrix} P & P' \\ Q & Q' \end{smallmatrix}\right|$. Il est clair que $\deg \Delta \leq \deg P + \deg Q - 1$ et il est facile de voir que Δ est non nul. D'autre part $\Pi_{i=1}^{p} (T - \alpha_i)^{l_i - 1}$ divise P et P' et donc Δ. De même $\Pi_{i=1}^{q} (T - \beta_i)^{m_i - 1}$ divise Q et Q' et donc Δ et de même $\Pi_{i=1}^{q} (T - \beta_i)^{m_i - 1}$ divise R et R' et donc Δ.

Pour ce dernier pas, observer que $P = -Q - R$ donc $\Delta = \left|\begin{smallmatrix} -Q-R & -Q'-R' \\ Q & Q' \end{smallmatrix}\right| = -\left|\begin{smallmatrix} R & R' \\ Q & Q' \end{smallmatrix}\right|$.

Par suite, comme les trois produits sont premiers entre eux, on obtient que Δ est divisible par

$$\Pi_{i=1}^{p} (T - \alpha)^{l_i - 1} \Pi_{i=1}^{q} (T - \beta_i)^{m_i - 1} \Pi_{i=1}^{s} (T - \gamma_i)^{n_i - 1}$$

d'où une inégalité de degré

$$(\deg P - p) + (\deg Q - q) + (\deg R - s) \leq \deg P + \deg Q - 1$$

d'où $\deg R \leq p + q + s - 1 = r(PQR) - 1$.
En procédant de même avec P et Q on obtient l'énoncé du théorème.

L'analogue immédiat sur $\mathbb{Z}$ serait de penser que si $a+b+c = 0$ avec $\text{pgcd}(a, b, c) = 1$ alors $\max(|a|, |b|, |c|) \leq$ constante $\times r(abc)$ avec

$$r(abc) = \prod_{\substack{p \text{ premier} \\ p \text{ divise } abc.}} p$$

Ceci est faux (voir l'exposé Oesterlé à Bourbaki) mais on peut conjecturer avec Oesterlé et Masser.

Conjecture a - b - c (Oesterlé-Masser).
Il existe deux constantes γ et δ telles que si $a + b + c = 0$ avec $\text{pgcd}(a, b, c) = 1$ alors

$$\max(|a|, |b|, |c|) \leq \gamma r(abc)^{\delta} \text{ ?}$$

Une preuve de cette conjecture serait un grand progrès; par exemple il est facile d'en déduire le théorème de Fermat asymptotique (id est pour n assez grand).

NB : Après cet exposé, Wiles a annoncé le preuve de la conjecture de Tariyama-Weil qui entraîne Fermat. Cela donne de l'espoir de démontrer la conjecture $a-b-c$ (affirmation optimiste bien sûr).

BIBLIOGRAPHIE (succinte)

Des articles originaux :

Mordell L.J.- *"On the rational solutions of the indetermidate equation of the third and the fourth degrees"*, Proc. Cambridge Philos. Soc., 21 (1922), pp. 179-182.

Faltings G.- *"Endlichkeitssätze für Abelsche Varietäten über Zahlkörpen"*, Inv. Math. 73 (1983), pp. 349-366.

Des "surveys" ou articles de "vulgarisation" :

Oesterlé J.- *Nouvelles approches du théorème de Fermat*, exposé Bourbaki n° 694 (1988).

Hindry M.- *Géométrie arithmétique* Cahier du Séminaire d'Histoire des Mathématiques, vol. 3 (1993) Univ. P. et M. Curie.

Mason.- *Diophantine equations over function fields*, Lecture notes, n° 96, London, Math. Soc. (1984).

Boutot et Moret-Bailly.- *Equations diophantiennes : la conjecture de Mordell*, Courrier du CNRS, Images des mathématiques (1985).

AUTO-RÉFÉRENCE!

Le contraire du vrai peut être vrai comme le montrent les deux phrases suivantes :

Cette phrase comporte exactement dix lettres "e".

Cette phrase ne comporte pas exactement dix lettres "e".

De même le contraire du faux peut être faux comme le montrent les deux phrases suivantes :

Cette phrase comporte exactement treize lettres "e".

Cette phrase ne comporte pas exactement treize lettres "e".

Deux expressions contradictoires peuvent être vraies simultanément :

Cette phrase comporte exactement dix lettres "e".

Cette phrase comporte exactement onze lettres "e".

Ou bien encore fausses simultanément :

Cette phrase comporte exactement douze lettres "e".

Cette phrase comporte exactement treize lettres "e".

ASPECTS GESTALTISTES DE LA RÉSOLUTION DES PROBLÈMES

Georges GLAESER

Le rêve de Descartes est une illusion! Il n'existe pas de Méthode Universelle. Certes, l'informatique (lorsqu'elle s'intitule abusivement "Intelligence Artificielle") sait construire des algorithmes qui répondent à des questions-types de plus en plus subtiles.

Elle est capable de programmer des *détections d'analogies* usuelles qui s'apparentent à des *associations d'idées.* Mais elle échoue devant un *problème.* [I fasc. 1]

Définition :

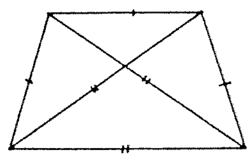
Un problème est une question à laquelle on ne peut répondre en disposant a priori d'une stratégie de recherche infaillible, toute préparée.

L'heuristique est la branche fondamentale de la didactique : elle étudie comment se construit la compréhension; dans les cas où le dressage préalable du chercheur s'avère impuissant!

I.— UN EXEMPLE

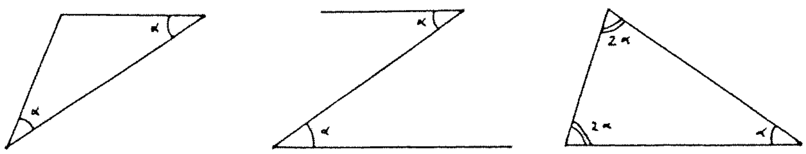
> Construire à la règle et au compas, un trapèze isocèle, dont les diagonales sont égales à la grande base, tandis que les côtés obliques sont égaux à la petite base.

On peut dresser des élèves à produire rapidement, face à cet énoncé, la maquette suivante :



Article extrait des actes du "Colloque international sur l'enseignement de la géométrie" (Mons, 31 août - 2 septembre 1982), pp. 241-254.

On peut même les provoquer à extraire de ce dessin les sous-figures suivantes :



pour en conclure que l'angle α vaut 36^o.
Mais souvent, "l'intelligence artificielle" s'arrête là! Personnellement, la seule évocation d'un angle de 36^o provoque chez moi depuis l'âge de 15 ans une association d'idées avec un pentagone régulier! L'exercice est alors *automatiquement* résolu : les sommets du trapèze appartiennent à une figure solidement ancrée dans ma mémoire, que je sais construire.

Mais pour la plupart des personnes, cet énoncé constitue un **problème**.

Nous l'avons encore constaté cette année, en observant des lauréats du Rallye Mathématique : ce n'est qu'après une heure de tâtonnements qu'ils ont aperçu le lien qui unit ce genre de figure, avec une notion qu'ils connaissent : le Nombre d'Or.

Certes, on peut banaliser la question en réintroduisant dans les programmes scolaires l'étude du pentagone régulier. Mais on ne peut songer à stocker dans la mémoire de tous les élèves les millions d'associations d'idées qui pourraient leur être utiles un jour, pour résoudre un problème.

N'en déplaise à certains behavioristes, il est *impossible d'enseigner* le *problem-solving*; on ne peut qu'enseigner le *drill-solving*, avec des drills [I, fasc. 1] plus ou moins sophistiqués.

Evidemment, on peut familiariser nos élèves avec les *tables heuristiques de Polya* [P]. Mais lorsqu'on conseille : "Connaissez-vous un problème qui se rattache à la question posée?" on ne fait que développer une saine attitude de recherche, indépendante de l'énoncé précis. Le chercheur peut d'ailleurs répondre négativement soit parce qu'en fait, il ne connaît pas de problèmes analogues, soit parce qu'il ne pense pas à un problème qu'il connaît bien, mais qui ne se relie pas à l'énoncé par des associations d'idées bien conditionnées. Lorsqu'on suggère : "Dessinez une figure", on ne fournit pas d'instruction algorithmique pour faire produire un dessin efficace. Et, en fait, dans l'exemple 3 ci-dessous, la découverte du mode de représentation souverain constitue à lui seul la solution du problème!

Par contre, on peut se livrer à un *entraînement heuristique systématique*. A force de résoudre des problèmes variés, on améliore les performances ultérieures. C'est particulièrement vrai si l'on prend soin de tirer les leçons de ces longues aventures.

Mais il est dans la nature des choses, qu'un chercheur bien entraîné, "*sèche*" de temps en temps, devant un problème insolite.

Seul le succès est significatif. On ne peut rien conclure, au sujet de l'aptitude à résoudre des problèmes, à l'occasion d'un échec isolé.

L'objet de mon exposé est la description de quelques-unes des démarches de pensées liées à la *reconnaissance de forme.*

II.— L'INTUITION

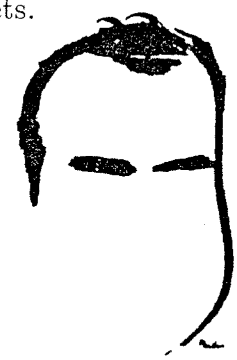
Le livre classique de Westcott [W] distingue les nombreuses significations du mot "intuition". En heuristique, je ne retiens que le sens suivant :

Définition
L'intuition est l'aptitude à conclure à partir d'informations incomplètes.

Dans l'exemple précédent, la seule évocation d'un angle de 36° m'a fourni la solution. Bien entendu, c'est une information incomplète, insuffisante pour fournir des certitudes. Il a bien fallu que je démontre que les sommets du trapèze cherché sont bien quatre sommets consécutifs d'un pentagone régulier qui n'apparaît même pas sur la figure. Mais cette *mise en logique* n'est plus qu'une activité de routine, une simple *vérification.*

EXEMPLE 2

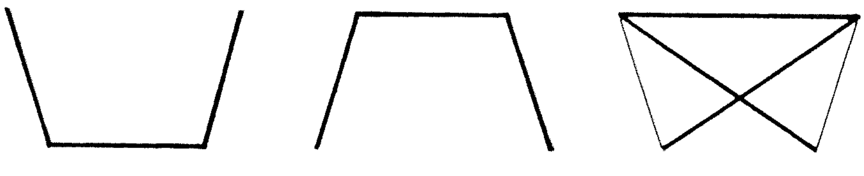
Dans ces caricatures, des taches caractéristiques permettent de reconnaître des personnages connus, grâce à des indices incomplets.



[Pa]

Le succès de l'opération dépend d'ailleurs de la familiarité que le spectateur peut avoir avec l'individu représenté. L'intuition est plus ou moins puissante selon la quantité d'informations nécessaires pour la déclencher. Dans le portrait de Chaplin, la reconnaissance est parfois obtenue à la seule vue du chapeau melon : il s'agit donc ici d'une information redondante. Il me semble que la caricature de Nixon est remarquable en ce qu'elle réduit les indices à leur plus simple expression. Edgar Poe, Conon Doyle ou Ellery Queen décrivent des détectives fictifs qui se contentent d'indices imperceptibles pour résoudre leurs énigmes. Des chercheurs moins géniaux exigent des *faisceaux d'indices.*

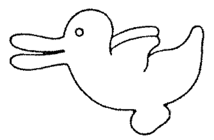
Des expériences montrent que les dessins ci-dessous ne sont pas équivalents pour provoquer l'émergence de l'intuition (ici le pentagone régulier) (cf. [DDP]).



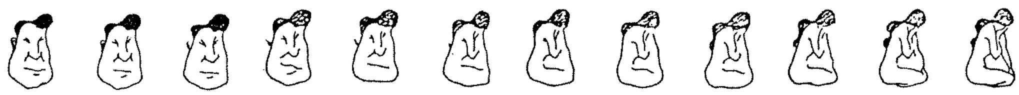
L'emploi de la couleur peut être décisif.

Face à des chercheurs novices, on peut accélérer l'intuition, en "soufflant" avec une sage lenteur des éléments de réponse jusqu'à ce que jaillisse l'eureka.

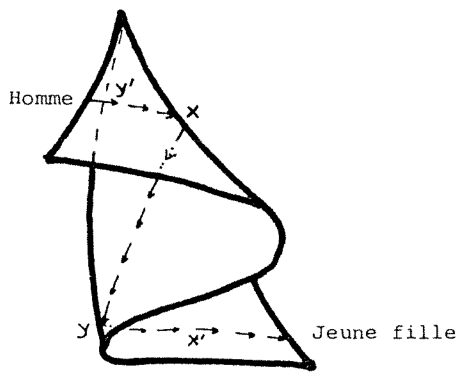
Parfois, l'information varie continuellement et il est possible d'observer comment la fourniture d'indices gradués provoque les phénomènes décrits par la *théorie des catastrophes* :



En faisant pourner lentement le dessin ci-dessus, on constate que la rupture ne s'effectue pas au même moment à l'aller et au retour. Dans la bande dessinée suivante, le dessinateur a introduit des modifications imperceptibles depuis la tête d'homme jusqu'à l'image de la jeune fille. Le changement brusque de vision n'apparaît pas au même moment à l'aller et au retour, conformément au modèle d'hystérésis de la *fronce* :



Les ruptures s'effectuent, à l'aller de X et X' et au retour à partir de Y et Y'.



III. L'"INSIGHT"

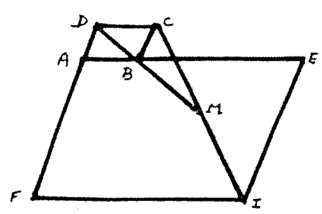
Ce mot anglais est presque intraduisible en français : on pourrait le rendre par "perspicacité" ou "pénétration d'esprit".

Définition

L'insight est l'aptitude à conclure en présence d'informations surabondantes.

Il s'agit donc d'une espèce de reconnaissance de formes, opposée à l'intuition!

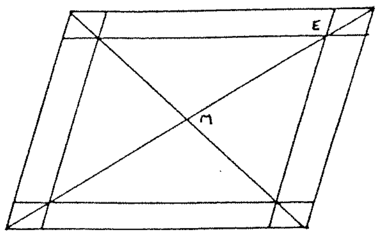
EXEMPLE 3 [I fasc. 2]



Voici une figure, où $ABCD$ et $AEIF$ sont des parallélogrammes et où le point M situé sur DB est au milieu de CI. On demande de prouver que F, M et E sont alignés.

Lorsque nous préparions le fascicule 2 de notre '*Livre du Problème*', notre chère collaboratrice Lucienne Félix, contemplant cet énoncé s'écria : "Qu'est-ce que c'est que ce fouillis!" Et elle se mit en devoir de découvrir ce qui se cachait sous cette horreur.

D'abord on vit *l'intuition* à l'œuvre. L'hypothèse que M est au milieu de CI s'avéra un indice suffisant pour l'inciter à effectuer une symétrie de centre M. C'est alors qu'apparut, dans toute sa simplicité, la figure ci-contre qui résoud trivialement le problème! Elle dévoile la structure sous-jacente.



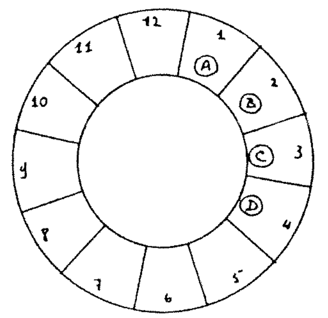
EXEMPLE 4

> Je vous invite à dessiner l'intéressante figure suivante : les sommets A, B, C, D d'un quadrilatère inscriptible déterminent, pris 3 par 3, quatre triangles. Chacun possède quatre cercles tritangents (inscrit ou exinscrits). Les 16 centres de ces cercles constituent une configuration remarquable que l'on demande d'étudier [D].

Il faut de l'"insight" pour découvrir dans l'enchevêtrement des lignes de constructions les sous-figures simples qui expliquent ce "miracle".

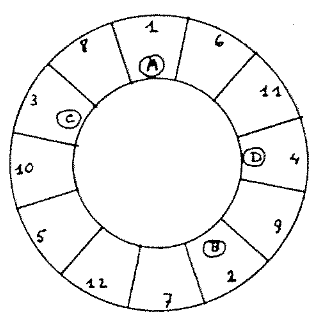
EXEMPLE 5

On place sur les cases (1, 2, 3, 4) du cadran ci-dessous quatre jetons A, B, C, D. On déplace un jeton en le faisant sauter par-dessus quatre cases (vides ou non), pour atterrir sur une case inoccupée. Quelles permutations des jetons peut-on obtenir à la suite de déplacements qui aboutissent finalement à une nouvelle occupation des cases initiales?



Ce problème est difficile parce que la numérotation "normale" des cases s'adapte mal à la description des déplacements par sauts précisés dans l'énoncé. Mais si on a l'idée de renuméroter le cadran comme ceci :

le déplacement se réduit au passage d'une case à une case vide contigüe. Il apparaît alors que les permutations obtenues sont exactement les permutations circulaires (sur la seconde figure) qui fournissent la liste des quatre permutations possibles sur la figure 1.



Ici l'insight (complété par une "traduction" dans une nouvelle représentation) a révélé la simplicité de la structure sous-jacente, masquée par la représentation de l'énoncé.

IV.— LE TRANSFERT

Ce dernier exemple montre qu'un énoncé est généralement présenté dans un langage (un "habillement") qui évoque un certain contexte.

Définition

Un transfert est une traduction d'un langage à un autre, avec modification du contexte.

On passe ainsi d'un énoncé à un énoncé équivalent. Il semblerait *du point de vue logique*, que l'on ne gagne (ni perd) rien à une telle reformulation. Mais il est fréquent que les indices susceptibles de déclencher une association d'idées sont plus évocateurs dans un contexte que dans un autre. **Du point de vue heuristique**, le transfert est souvent une opération mentale efficace.

Par exemple, la *géométrie analytique* est l'organisation du transfert entre une situation géométrique et une situation algébrique.

En raisonnant tour à tour sur des figures et des formules, on multiplie les opportunités de faire jaillir des éclairs d'intuition.

EXEMPLE 6

> Le groupe de Galois de l'équation générale du cinquième degré est isomorphe au groupe des isométries d'un icosaèdre régulier. En jouant sur les transferts entre ces deux contextes, Félix Klein a exposé d'une façon très évocatrice l'impossibilité de résoudre les équations générales de degré supérieur à 5, par radicaux [K].

EXEMPLE 7

> Quelles sont les matrices réelles inversibles, dont tous les termes (ainsi que ceux de la matrice inverse) sont non-négatifs? Cet énoncé présenté dans un contexte algébrique, peut se résoudre sans aucun calcul lorsqu'on l'interprète géométriquement, en termes d'applications linéaires d'un espace R^n sur lui-même.

L'hypothèse signifie que l'application cherchée applique le "premier quadrant" (ensemble de points dont toutes coordonnées sont positives ou nulles) sur lui-même.

On aboutit alors à la caractérisation des "matrices stochastiques", dont un seul terme par ligne (et par colonne) n'est pas nul.

V.— LA RUSE

L'intuition est, par définition, une *conclusion hâtive. De faux indices* engagent souvent la recherche sur une *fausse piste*. Cet effet de ruse est souvent exploité de façon intentionnelle voir machiavélique.

Au jeu de bridge, par exemple, on peut inciter un joueur *expérimenté* à échafauder un plan fautif, en lui fournissant habilement des indices trompeurs.

Le maître du puzzle, Sam Lyod, avait le génie de faire surgir de redoutables casse-têtes à partir de situations apparemment banales. Une ruse peut être une simple farce. Voici un exemple amusant (non géométrique) dû à la malice de l'équipe américaine, aux Olympiades Internationales de Mathématiques d'Erfurt (1974).

EXEMPLE 8

Démontrer l'inégalité :

$$\sqrt{\pi} \prod_{n>1} \prod_{m>1}^{n \neq m} \frac{(n^m - m^n)^2}{n^m + m^n} < \sum_{p=2}^{\infty} \frac{p^p}{(p!)!}.$$

Il fallait faire preuve de perspicacité pour déceler que ce brouillard n'était destiné qu'à dissimuler le fait, très connu :

$$2^4 = 4^2.$$

Mais la ruse est aussi un outil pédagogique. Des questions-pièges peuvent être destinées à provoquer des erreurs, qui attirent l'attention sur les conditions d'application d'un théorème.

EXEMPLE 9

Identifier la surface d'équation

$$(\mu z - \nu y)^2 + (\nu x - \lambda z)^2 + (\lambda y - \mu x)^2 = 1$$

(où λ, μ, ν sont des nombres réels effectivement donnés).

Un étudiant distrait conclura peut-être trop hâtivement sans s'apercevoir que les trois formes linéaires élevées au carré ne sont pas indépendantes!

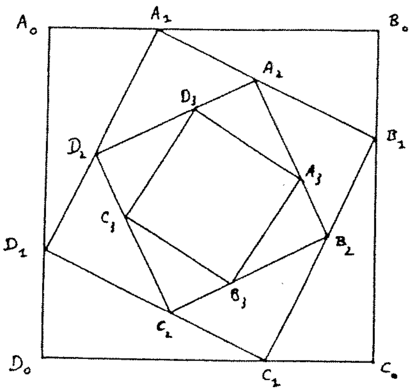
Mais il existe aussi des "ruses du destin", non provoquées par le désir de tromper.

EXEMPLE 10

Quelle est l'enveloppe convexe de la réunion d'une droite et d'un point (non situé sur la droite)? [I fasc. 4].

Ce sont généralement les élèves les plus brillants qui, jugeant cette question trop facile, produiront par inattention la réponse évidente ...mais fausse!

EXEMPLE 11



Dans la figure ci-jointe, le carré $A_{i+1}B_{i+1}C_{i+1}D_{i+1}$ se construit à partir du carré $A_iB_iC_iD_i$, en reportant sur les côtés de ce dernier des segments $[A_{i+1}A_i], [B_{i+1}B_i], [C_{i+1}C_i], [D_{i+1}D_i]$ de longueur 1.

Un mathématicien sans méfiance se trompera parfois, sur ce qui se produit à la limite, par analogie avec un autre problème trivial.

VI.— PENSÉE LATÉRALE

A chaque problème est généralement lié un *domaine de recherche*. Les solutions correctes appartiennent à l'ensemble des solutions plausibles. L'intuition puise généralement ses idées dans un domaine de recherche naturel.

Edouard de Bono a décrit une démarche heuristique particulière dont le ressort est la *sortie* du domaine de recherche naturelle.

Définition

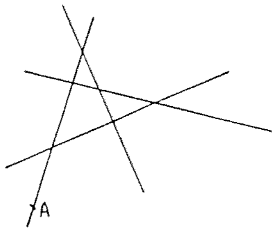
La pensée latérale est une extention du domaine de recherche par l'abandon de contraintes parasites, non formulées dans l'énoncé, que le chercheur se fixait implicitement et inconsciemment.

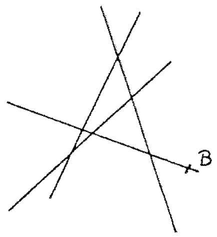
L'exemple-type est l'œuf de Christophe Colomb. On demande de placer un œuf sur une table. Le chercheur admet d'abord implicitement que la coquille doit rester intacte. La solution s'obtient par contre en acceptant de briser légèrement la coquille.

EXEMPLE 12

> Disposer 8 segments de droite (mesurant 4 cm chacun) dans un plan, en sorte que trois segments distincts arbitraires ne soient pas concourants et que chacun de ces segments rencontre exactement trois autres segments [I fasc. 6]
> C'est facile! Et pour corser la question on demande en outre que deux de ces segments contiennent respectivement les points A et B, distants de 30 cm.

Maintenant, on ne dispose plus de marge de manœuvre entre 30 cm et 4 cm $\times$ 8 $=$ 32 cm. Le problème serait-il impossible? On pourrait le croire, tant que l'on s'imagine implicitement que la figure produite doit être *connexe.* L'abandon de cette contrainte conduit facilement à des solutions où A et B peuvent être encore plus distants.



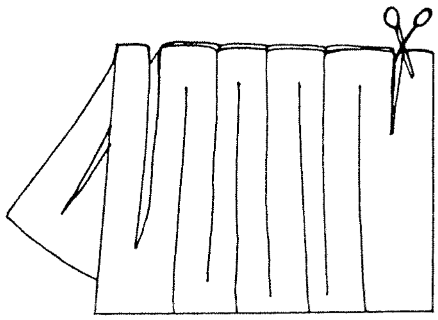


EXEMPLE 13

> Découper un trou dans une carte à jouer, en sorte qu'un obèse puisse passer à travers.

Il semble que la carte est trop petite et l'obèse trop gros pour que ce soit possible. Mais on admet ainsi, implicitement, qu'il est interdit de plier la carte.

Voici la solution classique, proposée au siècle dernier par Tom Tit, dans sa célèbre "Science amusante".



On produit ainsi un anneau extensible de carton, de longueur suffisamment grande.

CONCLUSION

Les démarches de pensées décrites ici, sont des éléments essentiels d'une *éducation* mathématique réussie. (Elles ne se réduisent pas à des *connaissances* comme dans un *enseignement*. On notera qu'elles ne figurent pas dans les programmes scolaires officiels!

Et pourtant elles présentent plus d'importance que l'amas de connaissances exigées de tous les élèves.

BIBLIOGRAPHIE

A l'origine de cet article, se trouvent les deux intéressantes références suivantes : elles développent une conception de *l'intuition* et de *l'insight* qui ne me satisfait pas.

H.B. GRIFFITHS and A.G. HOWSON, Mathematics : Society and Curricula, *Cambridge University Press* (1974).

MacDONALD, Insight and Intuition in Mathematics, *Educational Studies in Mathematics*, 9, (1978), pp. 411-420.

[B] Edouard de BONO, La pensée latérale, *Dunod*, 1972, Paris.

[D] Jean DREYER, Drapeaux danois, in : *'L'Ouvert'* n°26, 1982, publ. de l'IREM de Strasbourg et de la Régionale alsacienne de l'APMEP.

[I] IREM de Strasbourg, Le livre du problème (6 fascicules parus), *Editions Cédic*, Paris.

[K] Félix KLEIN, Uber das Ikosaeder, *Teubner*, 1884, Leipzig.

[P] Georges POLYA, Comment poser et résoudre un problème, *Dunod*, 1965, Paris

[W] Malcolm WESTCOTT, Psychology of Intuition, *Rihahart and Winston*, 1968 New-York.

[DDP] Claire DUPUIS, Raymond DUVAL et François PLUVINAGE, Etude sur la stabilité de la géométrie en fin de 3e, in Géométrie au Premier Cycle, Tome II, *Brochure APMEP n°22*, 1978, pp. 65–100.

[Pa] PASTECCA, Dibujando caricaturas, *Ed. Ceac Barcelona*, 1980.

La nouvelle algèbre de Viète (traduction de Vaulézard)

28. La ligne droite n'est comparée à la courbe, parce que l'angle est quelque chose de moyen entre la ligne droite et une figure plaine ; c'est pourquoy la Loy des Homogenes est venue repugner aux deux problemes precedens.

Que l'angle soit moyen entre la ligne et la superficie, il est evident : dautant que la ligne n'est qu'une simple longueur, et l'angle outre ce qu'il participe de la ligne pour estre fait par l'inclination d'icelle, il a de plus l'espace d'entre les lignes inclinées : car c'est cela qui est dit proprement angle ; et cet espace participe de la superficie sans neantmoins estre superficie, en ce qu'elle est contenue de deux lignes par laquelle elle est terminée de deux costés, et de l'autre indeterminée, ce qui l'empesche d'estre superficie ; c'est pourquoy puis que l'angle participe et de la ligne sans estre ligne, et de la superficie sans estre superficie, ayant quelque chose selon le genre des grandeurs moins que cete-cy et plus que cete-là ; il s'ensuivra que l'angle sera quelque chose de moyen entre la ligne droite et la superficie, par consequent incommunicable à la ligne droite. Il s'ensuit aussi, que la ligne circulaire estant la mesure de l'angle, qu'elle sera incommunicable à la droite.

29. Finalement l'art Analitic, introduit soubs la triple forme du Zetetique, Poristique et Exegetic, abrogé de son authorité, le plus ampoulé Probleme des Problemes, qui est,

DONNER SOLUTION DE TOUT PROBLEME.

SUR LES POLYGONES ENTIERS OU RATIONNELS

Eugène EHRHART

Minkowski est connu surtout pour avoir introduit son espace-temps à quatre dimensions, utile en théorie de la relativité. Mais vers 1900 il crée aussi de toutes pièces la *"géométrie des nombres"*. De nos jours le jumelage fécond de l'arithmétique et de la géométrie s'est considérablement développé et s'appelle maintenant l'*arithmo-géométrie*. Elle a récemment donné naissance à de nombreux travaux.

Nous limitant en gros à la géométrie plane, nous abordons un chapitre de cette jeune branche mathématique, qui s'occupe des *systèmes diophantiens linéaires homothétiques*. Nous exposons quelques résultats essentiels, éclairés par des exemples numériques simples. Pour les démonstrations, trop longues pour figurer ici, on peut consulter nos publications [1], [2] et [3].

Dans un plan rapporté à des axes orthonormés un point est dit *entier* ou *rationnel* si ses coordonnées sont des nombres entiers ou rationnels. Un polygone (convexe ou non) est dit entier ou rationnel si ses sommets le sont.

I.– Polygones entiers

Un résultat classique est la *formule de Pick* :

$$S = i + \frac{p}{2} - 1$$

où i et p sont les nombres de points entiers intérieurs ou périphériques du polygone entier P. Cette relation ramène la mesure de l'aire S de P à deux dénombrements. Nous en avons déduit une formule qui ramène par contre un dénombrement à deux mesures.

Soit P_n le dilaté de P par rapport à l'origine dans le rapport n, entier positif. Soient i_n et j_n les nombres de points entiers de P_n ouvert (sans le bord) ou fermé (avec le bord). Alors

$$i_n = Sn^2 - \frac{\ell}{2}n + 1 \qquad j_n = Sn^2 + \frac{\ell}{2}n + 1(*)$$

(*) où S est l'aire de P et ℓ la *"longueur réticulaire"* de son bord, obtenue en comptant pour 1 la distance de deux points entiers consécutifs.

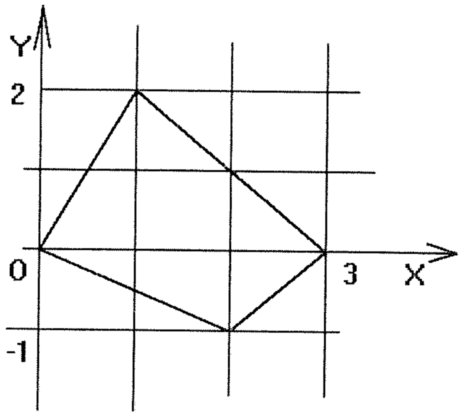
(*) NDLR : On a $S = i + \frac{p}{2} - 1 = j - \frac{p}{2} - 1$ dans une homothétie de centre O et de rapport n, $p \to np$ et $S \to n^2 S$.

Or on a : $i = S - \frac{p}{2} + 1 \qquad j = S + \frac{p}{2} + 1$

donc : $i_n = S_n^2 - \frac{p}{2}n + 1 \qquad j_n = S_n^2 + \frac{p}{2}n + 1.$

Exemple :

$$\begin{aligned} 2X - Y &> 0 \\ X + Y &< 3n \\ X - Y &< 3n \\ X + 2Y &> 0 \end{aligned}$$



$$\begin{aligned} 2X - Y &\geq 0 \\ X + Y &\leq 3n \\ X - Y &\leq 3n \\ X + 2Y &\geq 0. \end{aligned}$$

Le trinôme i_n *ou* j_n *donne le nombre de solutions entières du système strict ou large* :

$$i_n = \frac{9}{2}n^2 - \frac{5}{2}n + 1 \qquad j_n = \frac{9}{2}n^2 + \frac{5}{2}n + 1.$$

Pour tout polygone entier on a aussi

$$S = \frac{i_2 - 2i_1 + 1}{2} = \frac{j_2 - 2j_1 + 1}{2}(**).$$

II.— Polygones rationnels

P étant un polygone rationnel, le nombre i_n de points entiers de P_n est alors un "*trinôme arithmétique*" en n :

(1) $$i_n = Sn^2 - bn + a.$$

S est encore l'aire de P, mais a et b peuvent présenter des "*nombres périodiques*". Un nombre de période 3, par exemple, s'écrit

$$[a, b, c] = \begin{cases} a & \text{si } n = 1 \bmod 3 \\ b & \text{si } n = 2 \bmod 3 \\ c & \text{si } n = 0 \bmod 3 \end{cases}$$

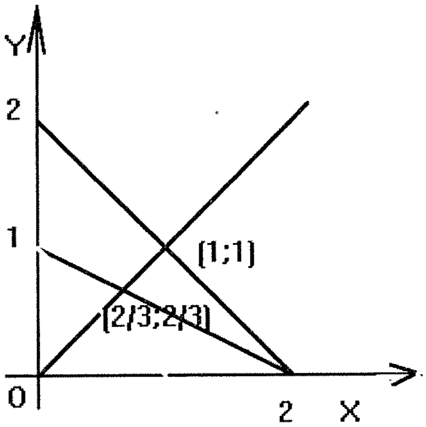
Si les droites supports de côtés du polygone sont toutes "réticulaires" (c'est-à-dire passent par deux points entiers et donc par une infinité), *le coefficient b dans* (1) *est constant.*

(**) NDLR :

$$\begin{aligned} i_2 &= 4S - p + 1 & j_2 &= 4S + p + 1 \\ i_1 &= S - \tfrac{p}{2} + 1 & j_1 &= S + \tfrac{p}{2} + 1 \\ \text{donc } S &= \tfrac{i_2 - 2i_1 + 1}{2} & &= \tfrac{j_2 - 2j_1 + 1}{2}. \end{aligned}$$

Exemple 1 :

$$\begin{aligned} X &> Y \\ X + Y &< 2n \\ X + 2Y &> 2 \end{aligned}$$



Le domaine primitif P_1 est un triangle, dont un sommet rationnel a pour dénominateur 3. Son aire est $S = \frac{1}{3}$ et les supports des côtés sont des droites réticulaires. Par suite i_n est de la forme (***)

(2) $$i_n = \frac{n^2}{3} - bn + [\alpha, \beta, \gamma].$$

(***)

On dénombre directement $i_1 = i_2 = 0, i_3 = 1, i_4 = 2$. En écrivant (2) pour n de 1 à 4, on obtient quatre équations pour calculer b, α, β, γ. D'où

$$i_n = \frac{n^2}{3} - n + \frac{[2,2,3]}{3} = ||\frac{(n-1)(n-2)}{3}||$$

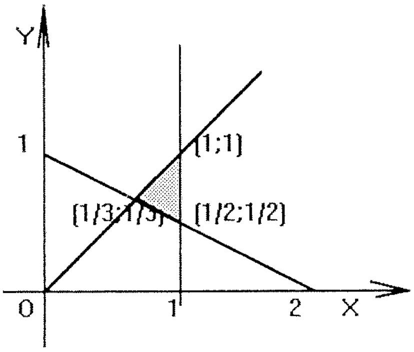
où $||A||$ désigne l'entier le plus proche de A.

La "*loi de réciprocité*" $j_n = i(-n)$ donne immédiatement le nombre de solutions entières du système large (les $\geq$ remplacent les $>$) :

$$j_n = ||\frac{(n+1)(n+2)}{3}||.$$

Exemple 2:

$$\begin{aligned} X &> Y \\ X &< n \\ X + 2Y &> 2n \end{aligned}$$



(***) NDLR : On comprend mieux l'apparition d'un nombre périodique dans l'expression quand on réfléchit au fait que si d est le pgcd des sommets rationnels, alors le dilaté de rapport kd ($k \in \mathbb{N}$) est à sommets entiers. On peut lui appliquer la formule de Pick.
Si on a toujours $S_n = n^2 S$ et $p_n = np$, les formules trouvées dans le cas des polygônes entiers ne sont valables que pour n multiple de d sinon il faudra sans doute modifier le terme constant ce qui fait apparaître un nombre périodique de période d.

Le domaine primitif est un triangle P_1, dont deux sommets rationnels ont pour dénominateurs 2 et 3, de sorte que le dénominateur de P_1 est 6. Son aire est $S = \frac{1}{12}$ et les supports des côtés sont des droites réticulaires. Par suite le trinôme i_n est de la forme

$$i_n = \frac{n^2}{12} - bn + [a_1, a_2, a_3, a_4, a_5, a_6]. \tag{3}$$

On dénombre directement $i_1 = i_2 = i_3 = i_4 = i_5 = 0, i_6 = i_7 = 1$. En écrivant (3) pour n de 1 à 7, on obtient sept équations pour calculer b et les six a_r. D'où

$$i_n = \frac{n^2 - 6n + [5, 8, 9, 8, 5, 12]}{12} = ||\frac{(n-3)^2}{12}||.$$

Par la loi de réciprocité le nombre de solutions entières du système large est donc

$$j_n = ||\frac{(n+3)^2}{12}||.$$

Généralisation. Pour un polyèdre entier on peut également calculer le volume V par des dénombrements :

$$V = \frac{i_3 - 3i_2 + 3i_1 - 1}{6}.$$

Suivant que le polyèdre est entier ou seulement rationnel les dénombrants i_n et j_n sont des polynômes ou des polygômes arithmétiques débutant par Vn^3. Ils vérifient une "**loi de réciprocité**" *élégante et efficace :*

$$\boxed{j_n = -i(-n)}$$

$$i_n = -j(-n).$$

Bibliographie

[1] Thèse, "*Sur un problème de géométrie diophantienne linéaire*", Journal de Crelle, t. 226 et 227 (1967).

[2] "*Polynômes arithmétiques et méthode des polyèdres en combinatoire*", Birkhäuser Verlag (1977)

[3] "*Histoire et leçons d'une recherche*", in : Articles de Mathématiques, Cédic/Nathan (1985).

L'INTERPRÉTATION DE L'ANALYSE EN TERMES D'ORDRES DE GRANDEUR : FONDEMENTS POUR UNE NOUVELLE PÉDAGOGIE

Robert LUTZ - Abdenacer MAKHLOUF - Etienne MEYER

L'enseignement de l'analyse mathématique dans les classes de lycée se heurte à de multiples difficultés dues essentiellement au hiatus profond entre l'idée intuitive d'approximation et la notion formelle de convergence, selon le sens qui a prévalu au 19[e] siècle après une longue maturation. Une manière scientifique cohérente d'atténuer ce hiatus consiste à donner un statut mathématique précis à la vieille et féconde notion leibnizienne de nombre "petit" ou "grand". On sait que, par un curieux détour de l'histoire, la quête d'un tel statut n'a abouti qu'il y a une trentaine d'années, dans le contexte de l'Analyse non standard d'Abraham Robinson fondée sur les acquis de la logique mathématique au cours de la première moitié du 20[e] siècle. Mise sous forme syntaxique par Edward Nelson en 1977, la solution est suffisamment simple et naturelle pour que la tentation de l'aménager en vue d'une pédagogie renouvelée de l'analyse élémentaire devienne irrésistible. Encouragés par une telle demande de la part de nos collègues et les incitations enthousiastes de notre ami André Deledicq (IREM de Paris) qui mène depuis plusieurs années une expérimentation sur le terrain dans cet esprit, nous avons voulu réfléchir sur les aspects essentiels d'une telle tentative.

Deux d'entre nous sont des praticiens de l'ANS au niveau de la recherche mathématique, où elle a permis des outils nouveaux d'une grande fécondité; le troisième est un professeur rompu à la pédagogie des classes de lycée.

Nous pensions initialement à une simple amélioration de la pédagogie, où l'évidente facilité que donne le calcul des limites à l'aide des quantités infinitésimales rendrait aux élèves le service d'une approche directement en prise avec l'intuition. Mais, chemin faisant, nous nous sommes aperçus que, malgré le charme de la chose, il n'était pas possible d'échapper à un certain bricolage si l'on n'allait pas jusqu'au bout de la tentative; il fallait reprendre radicalement la base des mathématiques enseignées, en ce qui concerne les nombres (des entiers aux réels), les suites et les fonctions. Dès lors l'objectif premier est devenu une didactique de l'analyse, en tant que *préalable* à une nouvelle pédagogie. Et nous avons rapidement été entraînés vers une réflexion de fond où le dialogue permament entre mathématiques intuitives et mathématiques axiomatisées apparaît comme le moteur de cette future pédagogie. Le fruit de nos efforts, non dénués de passion et de plaisir esthétique, se concrétisera à la rentrée 93 sous la forme d'une brochure de l'APMEP où nous offrirons les bases d'un débat que nous espérons fécond et animé.

Dans ce petit article, dont l'objectif est de susciter l'intérêt de nos collègues envers notre tentative, nous évoquons les grandes lignes du projet assorties de quelques échantillons typiques qui en donnent la tonalité générale.

1. Les fondements de l'approche que nous proposons : version faible

L'idée générale, inspirée de la version axiomatique de l'Analyse non standard, est d'enrichir les mathématiques en y introduisant, sans rien enlever, une modélisation axiomatique du concept *intuitif* d'objet mathématique "véritable". Il s'agit d'un concept informel, qui ne peut pas être défini par rapport à des concepts plus primitifs. Intuitivement, un objet mathématique est "véritable" si on peut en décrire explicitement le mode de construction à partir des objets de base des mathématiques. Ainsi les nombres entiers 0, 1, 2, 3, 1993, 187654328976543, 10^{1000} sont "véritables". Les réels $e, \pi, \ln(\sin 9)$ sont "véritables" (bien que leur mode de construction soit compliqué); les ensembles N, Q, Z, R, C sont des objets "véritables", de même que les fonctions $\sin, \cos, \tan, \cot, \exp, \ln$ et, par exemple, la suite définie par la relation de récurrence $U_{n+1} = \frac{2U_n+6}{4U_n+7}, U_0 = 1$.

Il est clairement impossible *d'écrire* un entier qui ne soit pas "véritable", aussi est-on tenté de croire que tout objet mathématique est "véritable". Mais il n'est pas possible d'exprimer une telle affirmation sans disposer d'une définition de ce concept. A défaut il faudrait dresser la liste de tous les objets "véritables", ce qui est exclu pour des raisons matérielles.

Cette impossibilité laisse la porte ouverte à une extension des mathématiques axiomatisées dans laquelle le concept de "véritable" objet serait introduit dans le langage formel et assorti d'axiomes inspirés de ses propriétés informelles. Nous proposons pour cela d'introduire le qualificatif *bien déterminé* (car il est plus évocateur que *standard*). Nous noterons en abrégé "bd".

La version faible de ce processus d'extension des mathématiques consiste à le restreindre aux entiers naturels et à définir à partir de là une hiérarchie des nombres qui permette une version infinitésimale de l'Analyse en termes d'ordres de grandeur et d'approximation absolue portant sur les nombres réels. La version forte permet d'établir le lien de cette Analyse avec l'Analyse des limites de suites et de fonctions. La distinction de ces deux niveaux de l'Analyse – le numérique et le fonctionnel – ouvre des perspectives vraiment nouvelles en matière pédagogique. En effet, dans la situation actuelle on pense intuitivement l'Analyse en termes numériques et on l'exprime formellement en termes fonctionnels. Ici nous pouvons l'exprimer en termes numériques et *ensuite* l'insérer dans le contexte fonctionnel, lorsque cela devient utile pour établir des théorèmes généraux sur les limites, la continuité etc ..., mais pas pour étudier une expression particulière.

Pour exprimer les axiomes de la version faible, il faut distinguer les *propriétés arithmétiques pures* (en un sens qui rappelle le désir de pureté classique "à la manière des anciens", cher aux analystes du 18^{e} siècle) concernant les entiers naturels de leurs *propriétés élargies* à des phrases où intervient le qualificatif *bien déterminé* ou des qualificatifs dérivés que nous définirons ultérieurement. Les premières ne contiennent dans leur expression que les opérations et la relation d'ordre. Ce sont les propriétés relatives à l'arithmétique classique. Nous ne changeons rien aux théorèmes de celle-ci, mais adjoignons les axiomes (ou principes) suivants qui régissent le qualificatif "bd".

Principes

(bd_1) *L'entier 1 est bien déterminé.*
(bd_2) *Tout entier défini de manière unique par une propriété purement arithmétique à partir d'un ou plusieurs entiers "bien détermminés" est "bien déterminé".*
(bd_3) *Pour chaque propriété arithmétique élargie P_n indexée par un entier variable n, si pour tout n bien déterminé à partir de n_0, P_n implique P_{n+1} (propriété héréditaire), et si P_n est vraie pour $n = n_0$, alors P_n est vraie pour tout n bien déterminé supérieur à n_0.*
(bd_4) *Il existe un entier qui n'est pas bien déterminé.*

Le dernier principe est la clé de voûte de tout l'édifice. Sa justification intuitive est l'impossibilité d'écrire formellement le contraire ... Le troisième est le *principe de récurrence élargie.*

Voici quelques conséquences de ces principes.

— *Si n est bien déterminé alors $n+1$ est bien déterminé.*
Appliquer (bd_1) et (bd_2). Noter que ceci ne contredit pas le principe de récurrence usuel, qui s'applique seulement aux propriétés arithmétiques pures.

— *Tout entier inférieur à un entier bien déterminé n est bien déterminé.*
En effet, appliquons le principe (bd_3) à la propriété "tout entier inférieur à n est bd". Elle est vraie pour $n = 0$ puisqu'il n'existe pas d'entier inférieur à 0, et elle est héréditaire, d'après la conséquence précédente.

— *La somme et le produit de deux entiers bien déterminés sont bien déterminés.*

— *Si n et p sont bien déterminés alors $n!$ et n^p le sont aussi.*

— *Tout entier qui n'est pas bien déterminé est supérieur à tous les entiers bien déterminés.*
En ce sens cet entier mérite d'être appelé *très grand* et un entier non très grand est dit *modéré* (*).

Nous obtenons ainsi une nouvelle vision de l'ensemble $\mathbb{N}$ des entiers naturels : on y trouve des entiers modérés comme 1, 10, 100^{50} et tous ceux qu'on obtient en y ajoutant 1; on y trouve aussi des entiers très grands qui restent très grands lorsqu'on leur enlève 1. Tout entier très grand est supérieur à tout entier modéré, mais il n'y a pas de plus grand entier modéré ni de plus petit entier très grand! Cette situation surprenante n'est pas contradictoire avec les connaissances usuelles et traduit le phénomène de transition floue omniprésent dans la vie courante : à

(*) NDLR : Les termes "modéré" et "bien déterminé" sont, pour les entiers, synonynes. Le qualificatif "modéré" ne prend tout son sens qu'avec l'étude des réels.

quel moment un enfant devient-il adulte? A quel moment un tas de sable cesse-t-il d'être un tas de sable lorsqu'on lui enlève un grain? Il est rassurant que la mathématique soit à ce point humaine qu'elle intègre le flou dans ses modes opératoires.

Les principes ci-dessus sont inspirés des propriétés intuitives des entiers "véritables". On peut montrer que toute propriété arithmétique pure qui serait un théorème dans la théorie élargie (c'est-à-dire que l'on pourrait démontrer en utilisant les principes (bd_1) à (bd_4) en plus des axiomes classiques) admet aussi une démonstration classique. Notre mathématique élargie est donc ce qu'on appelle *une extension conservative* de la mathématique classique. Il en est de même de l'extension forte que nous évoquerons plus loin. Il en résulte en particulier qu'aucune contradiction ne peut apparaître à cause de l'introduction des nouveaux principes. Ceci est proprement révolutionnaire, si l'on songe que jusque vers 1960, on a cru que les ordres de grandeur imaginés par Leibniz ne pouvaient admettre un fondement logique cohérent. Or nous pouvons les définir à partir du qualificatif "bd" de la manière suivante :

Définition

(i) *Un réel positif est dit très grand (tg) si sa partie entière n'est pas bien déterminée.*
(ii) *Un réel est dit modéré si sa valeur absolue n'est pas très grande (**).*
(iii) *Un réel est dit très petit (tp) s'il est nul ou si son inverse est très grand en valeur absolue.*
(iv) *Deux réels sont dits très proches (en abrégé $x \simeq y$) si leur différence est très petite.*

Ainsi un réel positif très petit est inférieur à $1/n$ pour n'importe quel entier explicite n, par exemple 1000000000000000000000000 . Le "très petit" formel modélise bien le très petit intuitif!

A partir de là on obtient un calcul sur les ordres de grandeur qui se déduit aisément des principes (bd_1) à (bd_3). Voici, en vrac, quelques unes de ces propriétés, écrites en langage abrégé :
– *Concernant l'addition*

$$\text{tp} + \text{tp} = \text{tp}; \ \text{tg} + \text{modéré} = \text{tg}; \ \text{modéré} + \text{modéré} = \text{modéré},$$
$$\text{tg positif} + \text{tg positif} = \text{tg positif}.$$

Mais il n'y a pas de résultat général pour tg positif - tg positif, ce qui ne devrait surprendre personne.

– *Concernant la multiplication*

$$\text{tp} \times \text{modéré} = \text{tp}; \ \text{modéré} \times \text{modéré} = \text{modéré},$$
$$\text{“non tp} \times \text{tg} = \text{tg” car les inverses vérifient “modéré} \times \text{tp} = \text{tp”}.$$

– Soient x, x', y, y' des réels modérés. Si $x \simeq x'$ et $y \simeq y'$, on a $x + y \simeq x' + y'$ et

(**) NDLR : On voit ici qu'un réel modéré peut ne pas être bien déterminé. Il peut en effet être très proche (définition IV) d'un réel bien déterminé.

$xy \simeq x'y'$.

A partir de là on peut développer l'Analyse sur les nombres. Elle consiste à trouver un réel explicite très proche de la valeur d'une expression où interviennent des réels très petits ou très grands dont on ne sait rien de plus, en d'autres termes à "lever des indéterminations".

Exemples

– Soit ω un entier tg. Alors $\frac{1+\omega}{2+3\omega} \simeq \frac{\frac{1}{\omega}+1}{\frac{2}{\omega}+3} \simeq \frac{1}{3}$.

– Même chose pour $\frac{1+\omega^2}{2+3\omega^2}$.

– Que peut-on dire de $\frac{1+\omega^3}{2+3\omega^2}$, $\frac{1+\omega^2}{2+3\omega^3}$ et $\omega - \frac{1+\omega^2}{2+3\omega^3}$?

– Evaluons $y = (1+x)^{1/3}$ lorsque x est très petit. Cela veut dire $y > 0$ et $y^3 = 1 + x$ d'où $x = (y-1)(y^2+y+1)$, x étant très petit et y^2+y+1 non très petit, on a nécessairement $y - 1 \simeq 0$. Posons $y = 1 + z$ et évaluons z; $z = y - 1 = \frac{y^3-1}{y^2+y+1} = \frac{x}{y^2+y+1}$. Comme $y \simeq 1$, on a $\frac{1}{y^2+y+1} \simeq \frac{1}{3}$. Et donc $\frac{1}{y^2+y+1} = \frac{1}{3} + \varepsilon$ où $\varepsilon \simeq 0$; d'où $z = x(\frac{1}{3}+\varepsilon)$ et $y = 1 + \frac{x}{3} + x\varepsilon$.

On peut continuer le calcul pour préciser l'ordre de ε par rapport à x. On peut faire de même pour la racine n-ième lorsque n est bien déterminé. Cet exemple montre la puissance de la méthode, qui permet de préparer les élèves aux propriétés asymptotiques des fonctions en faisant seulement des petits calculs sur les nombres ... En fait la plupart des exercices sur les limites que l'on pratique en première et terminale pourraient être interprétés de cette façon, plutôt qu'à travers l'utilisation d'un assortiment artificiel de règles sur les fonctions.

2. La version forte : extension aux suites et aux fonctions

Nous poursuivons le processus d'extension des mathématiques en étendant le qualificatif bien déterminé à tous les objets mathématiques. On parlera de réels bien déterminés. (Nous proposons d'ailleurs une construction de l'ensemble des réels, pour ne pas passer sous silence, comme cela est traditionnellement le cas, une certaine compréhension de ces nombres sans lesquels l'Analyse serait toute autre. Cette construction s'appuie sur les nouvelles notions et sur l'idée de place manquante.) On parlera également de suites bien déterminées et de fonctions bien déterminées, et l'on évoquera des *propriétés mathématiques pures* (celles des mathématiques classiques) et des *propriétés élargies* qui utilisent le qualificatif "bd" ou ses dérivés. La manipulation du qualificatif bien déterminé est complétée par *le principe de transfert* et le *principe de détermination.* Présentons succintement le principe de transfert : celui-ci traduit l'idée somme toute assez naturelle, que, pour qu'une propriété pure dépendant d'une variable x soit vraie, il suffit qu'elle le soit pour toutes les valeurs bien déterminées de x. La contraposée de ce principe (appliquée à la négation d'une propriété) fournit le résultat très utile suivant : s'il existe un objet satisfaisant une propriété pure, on peut affirmer l'existence d'un tel objet qui soit bien déterminé (et par conséquent, s'il existe un unique objet vérifiant cette propriété, il est bien déterminé : il en est de même des nombres explicites, des ensembles N, Z, Q, R, de l'ensemble des nombres premiers, etc ...).

Le fait central de l'Analyse réelle est alors le **théorème de complétude** qui peut revêtir la forme bien expressive suivante :

Pour tout réel modéré x, il existe un et un seul réel bien déterminé qui soit très proche de x. On le note $^\circ x$ (lire "ombre de x").

Le comportement de l'ombre par rapport à la relation d'ordre et aux opérations est résumé ainsi :

Théorème

Soient x et y deux réels modérés. Alors
(i) Si $x < y$ on a $^\circ x \leq^\circ y$ et si $x < y$ et x non très proche de y on a $^\circ x <^\circ y$.
(ii) $^\circ(x+y) =^\circ x +^\circ y$.
(iii) $^\circ(xy) = (^\circ x)(^\circ y)$.
(iv) $^\circ(x^y) = (^\circ x)^{(^\circ y)}$.

A partir de là on peut développer l'analyse des suites et des fonctions, le calcul des dérivées et le calcul intégral en utilisant des caractérisations dont voici quelques échantillons significatifs :

Soient $(U_n)_n$ une suite, l, a, b des réels, f, g des fonctions et I un intervalle, tous bien déterminés.

– La suite $(U_n)_n$ tend vers l si et seulement si pour tout entier n très grand U_n est très proche de l. Cette caractérisation est équivalente à : il existe n_0 très grand tel que pour tout $n > n_0, U_n \simeq l$.
– La suite $(U_n)_n$ a pour limite $+\infty$ si et seulement si pour tout entier n très grand U_n est très grand positif.
– La suite $(U_n)_n$ est bornée si et seulement si pour tout entier n très grand U_n est modéré.
– La fonction $f(x)$ tend vers l si et seulement si pour tout réel h très petit (non nul) $f(x+h)$ est très proche de l.
– La fonction $f(x)$ est continue sur I si et seulement si pour tout réel bien déterminé a de I et tout réel h très petit (avec $a+h$ dans I), $f(a+h)$ est très proche de $f(a)$.
– La fonction $g(x)$ est la dérivée de $f(x)$ sur l'intervalle ouvert I si et seulement si pour tout réel bien déterminé a de I et tout h très petit (non nul), $\frac{f(a+h)-f(a)}{h} \simeq g(a)$.
– Pour f continue sur $[a, b]$, l'intégrale de f sur $[a, b]$ est l'ombre de $\frac{b-a}{\omega}\Sigma_{i=1}^{\omega} f(a + i\frac{b-a}{\omega})$ (avec ω très grand).

Exemple

Nous avons vu au paragraphe 1 que pour x très petit $(1+x)^{1/3} = 1 + \frac{x}{3} + x\varepsilon$ avec

ε *tp*. Ce qui signifie $\lim_{x \to 0} \frac{(1+x)^{1/3}-1}{x} = \frac{1}{3}$.

Précisons maintenant l'ordre de ε par rapport à x pour poursuivre le développement de la fonction $(1+x)^{1/3}$ pour x très petit.

Posons $y = (1+x)^{1/3}$. On a $y - 1 = \frac{x}{y^2+y+1}$ et pour x *tp*, $y \simeq 1$.

D'où $\varepsilon = \frac{y-1}{x} - \frac{1}{3} = \frac{1}{y^2+y+1} - \frac{1}{3} = \frac{2-y^2-y}{3(y^2+y+1)} = -\frac{(y-1)(y+2)}{3(y^2+y+1)} = -\frac{x}{3}\frac{y+2}{(y^2+y+1)}$.

On a donc, pour x tp, $\varepsilon = -\frac{x}{9}(1+\varepsilon')$ avec $\varepsilon' \simeq 0$; ce qui signifie que pour x tp $(1+x)^{1/3} = 1 + \frac{x}{3} - \frac{x^2}{9} + x^2\varepsilon''$ avec ε'' tp.

Pour terminer cette brève présentation, voici l'idée de quelques démonstrations particulièrement jolies concernant les suites et les fonctions dans ce contexte.

– Dans R toute suite croissante et majorée a une limite.

Soit $(U_n)_n$ une suite bien déterminée majorée.

D'après le principe de transfert, il existe un majorant M bien déterminé. On subdivise l'intervalle $[U_0, M]$ en un nombre très grand w de parties égales et on considère le plus grand entier i, noté s, tel que $U_0 + i\frac{M-U_0}{w}$ ne majore pas la suite. Il existe alors n_0 tel que U_{n_0} appartient à $I_s = [u_0 + s\frac{M-U_0}{w}, u_0 + (s+1)\frac{M-U_0}{w}[$.

La suite étant croissante, on a donc pour tout $n \geq n_0, U_n$ appartient à I_s. Et donc, pour tout $n \geq n_0, U_n$ est très proche de l'ombre l de $U_0 + s\frac{M-U_0}{w}$ (car I_s est de longueur très petite). l est par conséquent la limite de la suite $(U_n)_n$.

– Toute fonction continue sur un intervalle fermé d'extrémités a et b, négative en a et positive en b s'annule au moins une fois entre a et b.

Soient f, a, b bien déterminés.

On fixe un entier très grand ω et on considère le plus grand indice i tel que $f(a + i(b-a)/\omega) < 0$. Alors $f(a + (i+1)(b-a)/\omega) \geq 0$, de sorte que l'ombre c commune aux deux points a une image $f(c)$ à la fois très proche d'un nombre négatif et d'un nombre positif ou nul. Comme le nombre $f(c)$ est bien déterminé, il est nul.

– Toute fonction continue sur un intervalle fermé $[a, b]$ est bornée et atteint un maximum et un minimum.

Même principe : subdivision fine qui discrétise le problème, maximum et minimum sur un ensemble fini, passage à l'ombre et comparaison avec la valeur de la fonction en tout point bien déterminé de l'intervalle.

Le lecteur qui sortira victorieux de cette démonstration aura tout compris et pourra utiliser les caractéristiques des dérivées et intégrales pour jouer avec les fonctions ln et exp qui constituent un gros morceau de l'étude développée dans notre brochure. La riche matière première que nous y proposons en vue d'une future pédagogie demandera évidemment l'élaboration de cours pour l'élève, graduels et bien pensés, pour éviter les artifices aussi bien que les délires qui peuvent naître d'un enthousiasme excessivement mystique pour les notions infinitésimales. C'est pour cela que nous évitons dans notre vocabulaire les connotations qui pourraient y inciter.

La nouvelle algèbre de Viète (traduction de Vaulézard)

26. Mais quoy, dautant que toutes les grandeurs sont ou lignes, ou superficies, ou corps. La proportion d'une triplée ou quadruplée raison, peut sufire en l'usage des choses humaines, sinon par hazard en la section des angles, ou en la recherche des angles par les costés des figures, ou les costés par les angles.

Tous ceux qui ont traité des choses Mathematiques n'ont jamais estably (comme aussi la nature y repugne) plus de 3. genres de grandeurs, sçavoir la ligne, la superficie, et le corps outre lesquels il ne s'en rencontre point, cela peut estre demonstré facilement, demeurant constant que tant la longueur, largeur, que profondité d'une figure est mesurée par une perpendiculaire (cecy sera facilement conceu, dautant que la mesure de quelque chose doit estre tousjours certaine et arrestée, ce qui ne peut estre qu'en la perpendiculaire qui est unique en la determination de quelque chose). Or est-il qu'à un mesme point ne peuvent estre menees plus de 3. lignes perpendiculaires, lesquels ne sçauroient marquer que 3. dimensions, sçavoir longueur, largeur, et profondité, ce qui convient au corps ou solide, et deux d'icelles, sçavoir longueur et largeur à la superficie, et une à la ligne. Cecy premis, ce que l'Autheur dit que la proportion constituee de 3. ou 4. raisons egales peut suffire aux choses qui arrivent entre les hommes est aparent, pour autant que les Equations qui arrivent en la recherche des choses solides proposées se peuvent resoudre du moins par l'invention de 2. ou 3. moyennes proportionnelles, c'est à dire par la constitution de 4. ou 5. quantités continuelles proportionnelles. Or est-il que 4. grandeurs continuelles proport. constituent 3. raisons egales, et 5. grandeurs, 4. raisons egales. Donc telle proportion peut suffire ainsi que dit l'Autheur : mais en la section des angles, ou bien en la recherche des angles d'une figure par les costés d'icelle, ou les costés par les angles ils arrivent d'autres proportions comme il se peut voir en la constitution des Equations ausquelles tombent la solution en la recherche de ces choses. Il advient neantmoins en quelques-unes que ces proportions peuvent suffire, comme en la division des angles en 2, 3, 4, parties egales, etc.

LEGENDRE ET LE POSTULAT DES PARALLELES

Gerardo AVILA

1.— INTRODUCTION

Bien des gens pensent que les mathématiciens les plus compétents sont assez sûrs dans leurs activités professionnelles et ne commettent pas d'erreurs. Ceci est faux; les mathématiciens qui s'adonnent à la recherche font fréquemment des erreurs qui restent enregistrées dans leurs écrits et sont découvertes et corrigées plus tard soit par eux-mêmes soit par d'autres mathématiciens dans de nouvelles publications. Ceci est très naturel puisque le progrès scientifique ne suit pas une trajectoire rectiligne faite seulement d'avancées. Au contraire, le chemin des découvertes est tortueux, plein de réussites et d'échecs. Et l'étude de l'évolution des idées, du développement des connaissances qui amènent aux découvertes est très souvent riche d'enseignement.

L'objet de cet article est justement de décrire l'un des épisodes dont le mathématicien **Legendre** fut le protagoniste et qui renferme quelques leçons de grande valeur pédagogique. Le fait que nous allons exposer est une belle tentative de démonstration de ce qu'on appelle "le postulat des parallèles". Pendant de nombreuses années **Legendre** publia et republia ses "démonstrations", réparant sempiternellement ses erreurs antérieures alors qu'en vérité ce qu'il tentait de démontrer était indémontrable. Cependant, suivre son raisonnement dans une de ces "démonstrations" est une tâche intéressante autant à cause des arguments de son génie créateur qu'à cause des savantes leçons que nous pouvons en tirer.

2.— QUI FUT LEGENDRE?

Adrien Marie Legendre (1752-1833) fut un illustre mathématicien français des XVIII^{e} et XIX^{e} siècles. Bien qu'il ne fut pas tellement riche, il possédait des ressources suffisantes pour se consacrer à l'étude et à la recherche sans avoir à se préoccuper de "gagner sa vie". Mais il ne resta jamais sans avoir un emploi rémunéré puisqu'il occupa différents postes publics comme professeur, enseignant ou assistant scientifique. Il fit partie, par exemple, de la commission chargée de proposer un système rationnel de poids et mesure dont le travail aboutit au système métrique comme nous le connaissons aujourd'hui.

Legendre effectua de nombreuses études de grande importance en mathématique pure et appliquée. C'est ainsi que son nom est lié aussi bien à des questions d'astronomie, de mécanique et de physique mathématique qu'à des questions d'analyse, d'équations différentielles et de théorie des nombres.

Avec l'aimable autorisation de la "Sociedade Brasileira de Matemática" qui a publié cet article dans la 'Revista do Professor de matemática' n° 22 (3° trimestre 1992). Traduction de Jean Lefort

En plus d'être un scientifique de grand mérite, Legendre fut aussi un véritable "professeur" qui alla jusqu'à se préoccuper des questions relatives à l'enseignement élémentaire. Dans ce domaine, son travail le plus important fut un livre intitulé "*Eléments de Géométrie*" publié à la fin du XVIII^e siècle et qui domina l'enseignement de la géométrie pendant près de 100 ans. Ce livre fut très populaire, car il était bien plus accessible aux étudiants que l'antique et difficile traité original d'**Euclide**. A tel point que le livre de Legendre, outre son usage dans les écoles françaises fut traduit dans différents pays y compris le Brésil où il fut largement utilisé, atteignant plus de 25 éditions.

Les diverses tentatives que fit Legendre pour démontrer le postulat des parallèles apparaissent, de 1794 à 1833, dans diverses éditions successives de son livre cité ci-dessus. En 1833, année de sa mort, on voit également apparaître sa monographie : "*Réflexions sur différentes manières de démontrer la théorie des parallèles ou le théorème sur la somme des trois angles d'un triangle*".

3.— EUCLIDE ET LE POSTULAT DES PARALLÈLES

Il existe plusieurs formulations équivalentes du postulat des parallèles parmi lesquelles nous donnerons d'abord une des plus simples et celle qui est le plus souvent donnée dans les livres. Bien qu'elle ait été déjà connue de Proclus (410-485) dans l'antiquité, elle ne fut vulgarisée aux temps modernes que par un livre du mathématicien écossais **John Playfair** (1748-1819) dont elle porte le nom :

Postulat de Playfair : *Par un point extérieur à une droite on ne peut tracer qu'une droite parallèle à la droite donnée.*

Le postulat des parallèles est aussi connu comme "le 5^e postulat d'Euclide" puisqu'il occupe justement la dernière place d'un groupe de cinq postulats énoncés dans "les éléments d'Euclide".

Parlons un peu des **Eléments** d'Euclide, écrits aux alentours de l'année 300 av. J.-C. Cette œuvre est un ensemble de treize unités ou chapitres, chacun d'eux étant appelé "livre". Livre I, Livre II, Livre III etc...jusqu'au livre XIII. Il s'agit d'une des œuvres les plus réputées de l'histoire des sciences qui rassemble presque tout ce qui se savait en mathématiques à l'époque où il fut écrit, non seulement en géométrie mais aussi en arithmétique et en algèbre bien que la présentation de ces disciplines soit aussi faite en un langage fortement géométrique. Cet ouvrage fut largement utilisé dans les écoles jusqu'il y a à peu près 200 ans.

Ce livre donne une présentation admirablement bien faite de la géométrie, très bien organisée sur le plan de la logique. Les résultats apparaissent comme "propositions" (nous dirions aujourd'hui "théorèmes") chacune d'elles étant démontrée en utilisant les précédentes. Ainsi chaque proposition dépend d'une ou plusieurs propositions antérieures de sorte que, pour que le processus puisse commencer, il est nécessaire de formuler quelques propositions initiales que l'on donne sans démonstrations. Ce sont ce qu'on appelle des "postulats" ou "axiomes". Euclide formule cinq postulats, dont les quatre premiers traduits et interprétés dans le langage actuel peuvent être énoncés ainsi :

1) *Par deux points passe une droite et une seule.*

2) *A partir d'un point quelconque d'une droite donnée, il est possible de construire un segment de longueur donnée sur la droite donnée.*

3) *Il est possible de tracer un cercle de centre et de rayon donnés.*

4) *Tous les angles droits sont égaux.* (Euclide définit l'angle droit comme étant égal à l'angle formé par deux droites qui se coupent de manière à former quatre angles égaux.)

Finalement le 5^e postulat est ainsi énoncé par Euclide :

Postulat d'Euclide : *Si une droite t coupe deux autres droites r et s (toutes coplanaires) de manière à former d'un même côté de t deux angles internes dont la somme est inférieure à deux angles droits, alors les droites r et s, prolongées suffisamment se rencontrent de ce même côté de t où la somme des angles internes est moindre que deux droits.*

Bien que plus compliqué que le postulat de Playfair, cet énoncé est clair si on l'accompagne d'une observation attentive de la figure 1.

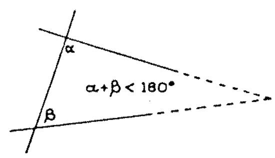


Figure 1

Dorénavant nous indiquerons par (P) et (E) les énoncés respectifs de Playfair et d'Euclide du postulat des parallèles. Nous démontrerons qu'ils sont équivalents. Pour cela nous aurons besoin des propositions 16, 17 et 27 d'Euclide. Nous allons les énoncer et les démontrer.

Proposition 16 (Théorème de l'angle externe). *Tout angle externe d'un triangle est plus grand que l'un quelconque des angles internes non adjacents (à l'angle externe considéré).*

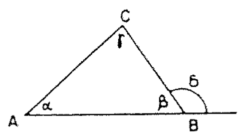


Figure 2

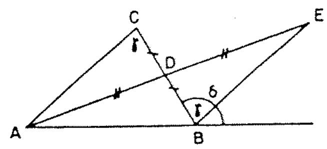


Figure 3

Cela signifie, en se reportant à la figure 2 que $\delta > \alpha$ et $\delta > \gamma$. Observez que nous ne pouvons pas écrire $\delta = \alpha + \gamma$ ce qui n'a pas encore été prouvé. D'autant plus que c'est une autre façon de formuler le postulat des parallèles que nous appellerons (P3) plus loin.

Démonstration : Dans le triangle ABC (fig. 3), soit D le milieu du segment BC. Prolongeons AD d'une largeur $DE = AD$ (ce qui est possible d'après le

2e postulat). Les triangles ACD et EBD sont égaux, ayant un angle égal compris entre deux côtés égaux (4e proposition d'Euclide), ce qui prouve en particulier que l'angle γ est égal à l'angle EBC et par suite $\delta > \gamma$, ce que nous voulions démontrer.

Reste à prouver que $\delta > \alpha$. Ce que l'on fait par le même raisonnement appliqué cette fois à l'égalité des triangles ACD et BED (fig. 4) à cause de la construction des points $D(AD = BD)$ et $E(CD = DE)$.

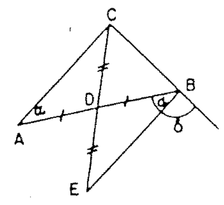


Figure 4

Proposition 17 *La somme de deux angles d'un triangle est toujours moindre que deux droits.*

Démonstration : D'après la figure 5 et en utilisant la proposition précédente, $\alpha < \delta$, et comme $\beta + \delta = \varpi$ (ϖ signifie toujours deux angles droits ou un angle plat), nous avons $\alpha + \beta < \delta + \beta = \varpi$; ce que nous voulions démontrer.

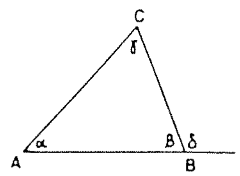


Figure 5

Proposition 27 *Soient deux droites r et s (coplanaires) coupées par une troisième t. Si les angles alternes-internes α et β sont égaux (fig. 6) les droites r et s sont parallèles.*

Démonstration : Supposons que r et s se coupent, disons en un point C. Nous aurions alors un triangle ABC donc les angles γ et β auraient une somme inférieure à deux droits (d'après la proposition 17), c'est-à-dire $\gamma + \beta < \varpi$.

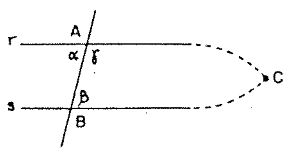


Figure 6

Mais $\beta = \alpha$ d'où nous tirons $\gamma + \alpha < \varpi$; ce qui est absurde. Nous sommes ainsi conduit à conclure que r et s ne se coupent pas; par suite elles sont parallèles comme nous voulions le démontrer.

Il est intéressant d'observer que cette proposition 27 garantit que *par un point P extérieur à une droite r on peut mener une parallèle à cette droite.* Pour cela, il suffit de construire par P une droite t rencontrant r en Q (fig. 7) et une droite s faisant avec t un angle α tel que $\alpha + \beta = \varpi$.

Comme $\alpha + \gamma = \varpi$; nous voyons que $\gamma = \beta$. Alors r et s ne peuvent se couper sous peine de contredire la proposition 27.

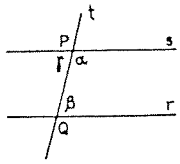


Figure 7

Ce que nous venons d'observer est important. Euclide savait qu'il n'avait pas besoin de postuler la possibilité de *tracer une parallèle à une droite donnée par un point extérieur à cette droite.* Il savait que cela pouvait être démontré comme de fait il le démontra!

Euclide n'utilise le postulat des parallèles que dans sa proposition 29 où il démontre que *deux parallèles coupées par une transversale forment des angles alternes-internes égaux.* Ici seulement il a besoin du postulat des parallèles! La géométrie avait déjà atteint un grand degré de développement et de sophistication au temps d'Euclide.

Observez encore, cher lecteur, que l'énoncé de Playfair ne dit pas que "par un point extérieur à une droite *on peut tracer une*" mais qu'il dit que "par un point extérieur à une droite **on ne peut tracer qu'une** ...". La possibilité de tracer une parallèle, nous y insistons à nouveau, est déjà garantie par la proposition 27.

4.— L'EQUIVALENCE DE (P) ET DE (E)

Nous pouvons maintenant établir l'équivalence de (P) et de (E).

La preuve de (P) $\Longrightarrow$ (E). Nous supposons vraie la proposition (P) et nous voulons démontrer la proposition (E). Soient r et s deux droites coupées par une transversale t (fig. 8) avec $\alpha+\beta < \varpi$. Nous voulons prouver qu'elles se rencontrent en un point P. Par le point A traçons une droite r' telle que les angles alternes-internes α' et γ soient égaux, de sorte que, à cause de la proposition 27, r' et s sont parallèles. Comme $\alpha' = \gamma$, $\gamma + \beta = \varpi$, nous avons $\alpha' + \beta = \varpi$. De ceci et de $\alpha + \beta < \varpi$ nous en concluons que $\alpha < \alpha'$. Alors r et r' sont des droites distinctes passant par le même point A et comme r' est parallèle à s, d'après (P), r ne peut pas être parallèle à s et par suite rencontre s en un certain point P, comme nous voulions le démontrer.

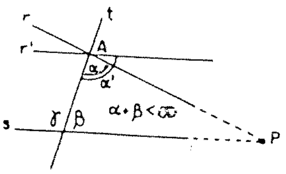


Figure 8

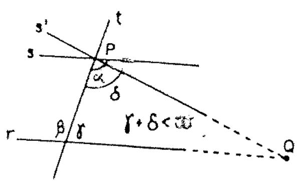


Figure 9

La preuve de (E) $\Longrightarrow$ (P). Etant donnés une droite r et un point P non sur r, nous voulons prouver que par P on ne peut mener qu'au plus une parallèle à la droite r. Nous savons déjà que par P il passe une droite s parallèle à la droite r, que l'on construit comme nous l'expliquons juste après la démonstration de la proposition 27 (fig. 9), avec $\alpha = \beta$ de manière que $\alpha + \gamma = \varpi$. Toute autre droite passant par

P, telle que s' fera un angle $\delta < \alpha$, où $\delta + \gamma < \varpi$. En conséquence, à cause de (E), s' devra couper r en un point Q. Ce qui prouve que par P il ne passe qu'au plus une parallèle à la droite r ce que nous voulions démontrer.

5.— LA "DEMONSTRATION" DE LEGENDRE

Nous allons noter (P3) un autre énoncé du postulat des parallèles, équivalent à (P) et qui sera utilisé dans la "démonstration" de Legendre.

Enoncé (P3) *La somme des angles intérieurs d'un triangle quelconque vaut* ϖ.

Il est facile de vérifier que (P) $\Longrightarrow$ (P3). En effet, étant donné un triangle quelconque ABC traçons par son sommet C une droite r parallèle au côté AB (fig. 10).

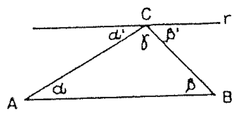


Figure 10

De cette façon, nous formons les angles α' et β' respectivement égaux aux angles α et β du triangle ABC. Nous obtenons ainsi $\alpha + \beta + \gamma = \alpha' + \beta' + \gamma = \varpi$; cqfd.

La démonstration du fait que (P3) $\Longrightarrow$ (P) est plus longue et nous ne la ferons pas ici. (Le lecteur intéressé pourra la trouver dans [1] page 103 et suivantes. Dans cette référence, l'auteur appelle le postulat de Playfair "Postulat de Hilbert".)

Avec le théorème suivant (que nous énonçons sous forme de "lemme") nous entrons dans la "démonstration" de Legendre du postulat des parallèles.

Lemme de Legendre *Etant donné un triangle quelconque, il est toujours possible de construire un nouveau triangle dont la somme des angles intérieurs est égal à la somme des angles intérieurs du triangle donné et dans lequel un des angles est inférieur ou égal à la moitié d'un angle donné du triangle initial.*

Explication : L'idée est la suivante : étant donné un triangle quelconque ABC, nous souhaitons montrer qu'il est possible de construire un nouveau triangle $A_1B_1C_1$ tel que

$$\alpha_1 + \beta_1 + \gamma_1 = \alpha + \beta + \gamma \text{ et } \alpha_1 \leq \alpha/2.$$

Une fois ceci démontré, nous pouvons construire un deuxième triangle $A_2B_2C_2$ tel que :

$$\alpha_2 + \beta_2 + \gamma_2 = \alpha_1 + \beta_1 + \gamma_1 \text{ et } \alpha_2 \leq \alpha_1/2$$

et en reportant

$$\alpha_2 + \beta_2 + \gamma_2 = \alpha + \beta + \gamma \text{ et } \alpha_2 \leq \alpha/2^2.$$

En continuant ce processus de construction de triangles successifs, nous arrivons à un triangle $A_nB_nC_n$ tel que

$$\alpha_n + \beta_n + \gamma_n = \alpha + \beta + \gamma \text{ et } \alpha_n \leq \alpha/2^n \qquad (1).$$

De cette manière nous pouvons obtenir un angle α_n aussi petit que nous voulons, en prenant n assez grand, de façon que dans la somme $\alpha_n + \beta_n + \gamma_n$ l'angle α_n ne compte que très peu, la contribution essentielle provenant de $\beta_n + \gamma_n$ que nous savons être moindre que ϖ d'après la proposition 17. Voilà l'idée qui permet d'arriver à la démonstration que la somme $\alpha + \beta + \gamma$ est inférieure ou égale à ϖ.

Démonstration du lemme de Legendre :

Etant donné un triangle quelconque ABC d'angles α, β et γ (voir fig. 11 où $\alpha = \alpha_1 + \alpha'$), répétons la construction faite figure 2, nous obtenons deux triangles égaux ADC et EDB. Alors $\alpha' = \beta_1$ et $\gamma = \delta$ de sorte que $\alpha + \beta + \gamma = (\alpha_1 + \alpha') + \beta + \delta = \alpha_1 + \beta_1 + \beta + \delta = \alpha_1 + \beta_1 + \gamma_1$.

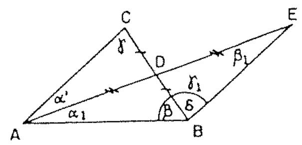


Figure 11

D'autre part, comme $\alpha_1 + \beta_1 = \alpha$, nous devons avoir $\alpha_1 \leq \alpha/2$ ou $\beta_1 \leq \alpha/2$. Si nous nous trouvons dans ce dernier cas, il suffit d'échanger les symboles α_1 et β_1 pour nous ramener dans tous les cas à $\alpha_1 \leq \alpha/2$. Ceci achève la démonstration du lemme.

Théorème de Legendre. *La somme des angles d'un triangle quelconque n'est jamais supérieure à deux droits.*

Démonstration. Soit ABC un triangle quelconque, d'angles α, β et γ. Nous allons démonter que $\alpha + \beta + \gamma \leq \varpi$, en démontrant que $\alpha + \beta + \gamma > \varpi$ nous conduit à une contradiction. Supposons donc que $\alpha + \beta + \gamma = \varpi + \varepsilon$, où $\varepsilon > 0$.

En procédant comme dans l'explication ci-dessus donnée après l'énoncé du lemme de Legendre, nous construisons un triangle $A_nB_nC_n$ d'angles α_n, β_n et γ_n avec n tel que $\alpha/2^n < \varepsilon$. Ceci joint à (1) implique $\alpha_n < \varepsilon$ et en reportant, comme nous avons aussi $\alpha_n + \beta_n + \gamma_n = \alpha + \beta + \gamma = \varpi + \varepsilon$, nous obtenons $\beta_n + \gamma_n = \varpi + (\varepsilon - \alpha_n) > \varpi$. Ceci est en contradiction avec la proposition 17, ce qui achève la démonstration du théorème.

Nous sommes finalement en état de voir comment Legendre procéda dans sa tentative de démontrer le postulat des parallèles. Pour cela, en prenant en compte l'énoncé (P3) il suffit de démontrer que **la somme des angles d'un triangle quelconque est** ϖ. C'est cela que Legendre se proposa de faire. En raisonnant par l'absurde nous supposons que ABC est un triangle dont la somme des angles intérieurs est inférieur à ϖ et donc égal à $\varpi - \varepsilon$ où $\varepsilon > 0$.

Par le sommet C traçons $CP = AB$ de façon que l'angle PCB soit égal à l'angle ABC et que le point P soit du même côté de la droite AC que le point B (fig. 12). Les triangles ABC et PCB sont égaux comme ayant un angle égal compris entre deux côtés égaux et par suite ils possèdent la même somme des angles : $S_1 = S_2 = \varpi - \varepsilon$.

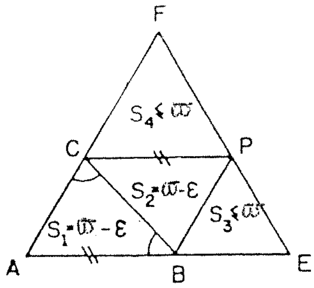


Figure 12

Par le point P traçons une droite qui coupe les droites AB et AC respectivement en E et F formant ainsi les triangles BEP et CPF. Les sommes S_3 et S_4 des angles de ces triangles sont telles que $S_3 \leq \varpi$ et $S_4 \leq \varpi$. Par suite

$$S_1 + S_2 + S_3 + S_4 \leq 4\varpi - 2\varepsilon \qquad (2).$$

Remarquez que la somme S des angles du triangle AEF est $S_1 + S_2 + S_3 + S_4$ moins les angles des sommets B, C et P. Maintenant, la somme des angles en chacun de ces sommets vaut ϖ de sorte que nous devons soustraire 3 ϖ de $S_1 + S_2 + S_3 + S_4$ pour obtenir la somme S cherchée. Et par suite, d'après (2) nous pouvons conclure que $S \leq \varpi - 2\varepsilon$.

Ceci montre que s'il existait un triangle ABC dont la somme des angles soit $\varpi - \varepsilon$, nous arriverions à construire un triangle plus grand AEF dont la somme des angles serait $\varpi - 2\varepsilon$. En poursuivant, nous pourrions construire un autre triangle, plus grand encore dont la somme des angles serait inférieure ou égale à $\varpi - 4\varepsilon$ et ainsi de suite. Maintenant nous arriverions ainsi à construire un n-ième triangle dont la somme des angles serait inférieure ou égale à $\varpi - n\varepsilon$. Et il est clair que ceci est absurde puisque, n pouvant être aussi grand que l'on veut, $\varpi - n\varepsilon$ deviendrait négatif. Nous sommes ainsi amenés à conclure que la somme des angles d'un triangle quelconque ne peut pas être moindre que ϖ. Comme nous avons déjà démontré qu'elle ne peut pas être non plus supérieure à ϖ, nous en concluons qu'elle vaut exactement ϖ.

Comme le lecteur le voit, Legendre, par ce raisonnement aurait prouvé le postulat des parallèles dans sa version (P3). Maintenant, comme nous l'avons dit, il est impossible de prouver ce postulat comme cela fut clairement établi par les inventeurs des géométries non-euclidiennes. Il doit donc y avoir une erreur dans le raisonnement de Legendre que nous venons de présenter. En fait, si erreur il y a, elle est assez subtile et par là même échappa à la perspicacité de Legendre. Comme nous le verrons ci-après, elle se trouve dans ce que les logiciens appellent "tautologie" ou "cercle vicieux" et qui consiste à supposer vrai cela même que l'on désire prouver. Ceci est bien sûr inadmissible!

A une certaine étape du raisonnement ci-dessus, en rapport avec la figure 12, nous avons dit : "Par le point P traçons une droite qui coupe les droites AB et AC respectivement en E et F". Enonçons cette proposition sous la forme générale :

Enoncé (P4). *Par un point P intérieur d'un angle quelconque BAC, il est toujours possible de tracer une droite qui coupe les deux côtés de l'angle en E et F respectivement.*

Bien que Legendre ne s'en soit pas aperçu, cet énoncé est équivalent au postulat des parallèles comme nous allons le démontrer. Bien sûr, s'il est équivalent, on ne peut, comme le fit Legendre, l'utiliser dans une quelconque démonstration de ce postulat.

La démonstration de (P4) $\Longrightarrow$ (P) est exactement celle que nous avons faite ci-dessus, dans le raisonnement relatif à la figure 12. Pour démontrer que (P) $\Longrightarrow$ (P4), supposons (P) vraie. Soit BAC un angle quelconque et P un point intérieur à cet angle. Nous devons montrer qu'il existe une droite passant par P et rencontrant les deux côtés de l'angle.

Par P traçons la droite t parallèle au côté AC (fig. 13). Elle doit couper le côté AB, sinon nous aurions deux droites AB et AC passant par le point A et parallèles à t ce qui contredit (P). Soit D le point de rencontre de t et de AB. Soit E un point du côté AB tel que D soit entre A et E. Démontrons que la droite PE coupe le côté AC en un point F.

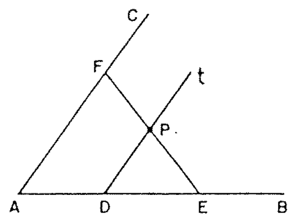


Figure 13

Sinon par P il passerait deux droites PE et t toutes deux parallèles à la même droite AC ce qui à nouveau contredit (P). Ceci achève la démonstration du fait que (P4) est équivalent à (P).

6.— UNE REFLEXION CRITIQUE

Des épisodes comme celui que nous venons de décrire montrent que, bien que la visualisation géométrique soit un puissant auxiliaire dans l'apprentissage de la géométrie, elle peut, très souvent, nous conduire à des conclusions ou des raisonnements faux. En outre, avant même Legendre, d'autres mathématiciens commirent des erreurs analogues, l'une d'elles ayant eu pour acteur Girolamo Saccheri (1667-1733) qui fut également l'auteur d'un écrit dont l'objectif était la démonstration du postulat des parallèles. Ce fut à cause d'erreurs de ce type que les mathématiciens commencèrent à percevoir qu'ils étaient mal guidés par la façon dont ils avaient visualisé les entités géométriques – essentiellement la ligne droite – tout au long des siècles. Et ils finirent par découvrir que cette visualisation était seulement **une façon d'être** de ces entités. D'autres **modèles** devaient exister, obéissant aux mêmes quatre premiers postulats d'Euclide mais non au cinquième. Ainsi naquirent ce que l'on appela les géométries non-euclidiennes. Au lecteur qui s'intéresse à de plus amples renseignements sur ces géométries nous conseillons de consulter l'article du professeur Waldyr Oliva dans '*Revista do professor de matemática 2*' et celui du professeur Manfredo do Carmo dans [2].

Les expériences de Saccheri, Legendre et autres mathématiciens stimulèrent les études critiques des fondements tant en géométrie qu'en analyse et dans d'autres parties des mathématiques. Dans le domaine de la géométrie, ces études culminèrent en 1899 avec la parution du livre de Hilbert : '*Fondements de la géométrie*' qui fut le premier travail complet sur l'organisation axiomatique de la géométrie.

Hilbert et d'autres mathématiciens du siècle passé finirent par découvrir que l'œuvre d'Euclide, malgré son admirable structure et son organisation, contenait différentes failles; bien des démonstrations étaient incomplètes, car elles s'appuyaient fréquemment sur la vision géométrique et non uniquement sur les postulats comme cela devrait être. Bien plus, ils constatèrent que les cinq postulats d'Euclide étaient insuffisants et que bien d'autres étaient nécessaires pour construire l'édifice de la géométrie.

Du point de vue de l'enseignement secondaire ceci renferme une leçon très importante : si les mathématiciens les plus éminents mettent tant de temps pour découvrir les failles de l'enchaînement logico-déductif de la géométrie et les "pièges" de l'intuition, comment alors attendre qu'un élève du 2^{e} cycle ait assez de sensibilité pour ces subtilités! Le collège ou le lycée ne sont pas des lieux adéquats pour l'étude des fondements et de l'axiomatique et cela même parce qu'il est impossible d'apprécier ces études et de comprendre leur nécessité sans une solide connaissance des faits géométriques et des processus de déductions. Le professeur doit d'abord s'occuper de l'enseignement de ces derniers puisque sans eux l'élève ne peut développer son esprit critique et se mettre en condition de percevoir les failles et les lacunes de certaines démonstrations. Et même alors cette perception ne sera possible qu'avec l'aide du professeur, puisqu'il serait tout de même surprenant que quelqu'un ayant si peu d'expérience puisse découvrir la faille d'un raisonnement comme celui de Legendre que nous venons d'exposer.

L'axiomatisation de la géométrie est une longue tâche qui requiert suffisamment de temps et qui ne peut s'achever au lycée. Importuner l'élève avec des subtilités pour lesquelles il n'est pas encore prêt est un contresens pédagogique. Par contre, le professeur de lycée doit être informé sur ce qu'il enseigne, y compris sur les fondements et l'axiomatique, justement pour qu'il puisse acquérir le sens critique qui l'aide à décider avec bon sens ce qu'il doit enseigner et comment.

REFERENCES BIBLIOGRAPHIQUES

[1] GREENBERG M.-J. *Euclidean and non-euclidean geometries*, New Yord, W.-H. Freeman and Co., 1980.

[2] CARMO M.-P. *Do geometrias não-euclidianas* 'Revista matematica universitaria', Rio de Janeiro (6) dez. 1987.

A VOS STYLOS

PROBLÈME 24

Énoncé

Un faisceau de droites parallèles fournit un exemple de partition du plan en droites.

a) Existe-t-il une partition du plan en cercles (non dégénérés, c'est-à-dire de rayon ni nul ni infini) ?

b) Existe-t-il une partition du plan en figures formées chacune de deux cercles (distincts et non dégénérés) tangents intérieurement ou extérieurement ?

Solution

La réponse aux deux questions est non. Pour le a) M. Renfer (Strasbourg) propose la démonstration suivante : il suffit d'établir que toute partition du plan en cercles (de rayons finis) comporte au moins un cercle de rayon nul. Soit C_0 un cercle d'une telle partition; on construit par récurrence une suite $(C_n)_{n\in\mathbb{N}}$ de cercles de la partition en prenant pour C_{n+1} le cercle passant par le centre de C_n ; C_{n+1} est intérieur à C_n (avec égalité si C_n est de rayon nul), et a un rayon au plus égal à la moitié de celui de C_n. Les disques fermés limités par les C_n forment une suite décroissante de compacts non vide; leur intersection est donc non vide; comme son diamètre est nul, elles est réduite à un singleton $\{\Omega\}$. Celui des cercles de la partition qui passe par $\{\Omega\}$ est intérieur à tous les C_n et possède donc un rayon nul.

Pour le b), M. Renfer remarque que la même méthode est facile à adapter.

Nous avons également reçu de M. Kern (Strasbourg) une magnifique solution, sous forme d'un théorème très général dont les réponses négatives aux deux questions posées sont des corollaires. Voici ce théorème.

Soit $\mathcal{P}$ une partition du plan (ou de $\mathbb{R}^n$ pour $n \geq 2$) en ensembles fermés connexes. Si, parmi les éléments de $\mathcal{P}$ se trouve un compact, il s'y trouve aussi un compact de complémentaire connexe.

Démonstration. Le complémentaire d'une partie E du plan sera noté E^c; rappelons qu'un ensemble connexe rencontrant E et E^c rencontre également la frontière de E. Si K est un compact, il est inclus dans une boule; une et une seule des composantes connexes de l'ouvert K^c est un voisinage de l'infini. Nous noterons $\tilde{K}$ cette composante; les autres, s'il y en a, sont bornées. Le complémentaire $\hat{K}$ de $\tilde{K}$ est compact; la frontière de $\tilde{K}$ est incluse dans K.

Notons $\mathcal{P}'$ l'ensemble, non vide par hypothèse, des éléments compacts de $\mathcal{P}$. Si $K_1 \in \mathcal{P}'$ et $K_2 \in \mathcal{P}'$ sont tels que $\tilde{K}_1 = \tilde{K}_2$, tout point de la frontière de $\tilde{K}_1$ est à la fois dans K_1 et K_2, donc, $\mathcal{P}$ étant une partition, $K_1 = K_2$. Il en résulte que la relation définie sur $\mathcal{P}'$ par

$$K_1 \prec K_2 \Longleftrightarrow \tilde{K}_1 \subset \tilde{K}_2$$

est une relation d'ordre. Soit $\mathcal{A}$ une partie non vide de $\mathcal{P}'$ telle que l'ordre $\prec$ restreint à $\mathcal{A}$ soit un ordre total. Quand K décrit $\mathcal{A}$, les ouverts $\tilde{K}$ forment une famille totalement ordonnée par inclusion; les compacts $\hat{K}$ aussi, donc leur intersection n'est pas vide : soient $x \in \bigcap_{K \in \mathcal{A}} \hat{K}$ et L l'élément de $\mathcal{P}$ passant par x. Pour $K \in \mathcal{A}$, L ne peut rencontrer $\tilde{K}$ (connexe et rencontrant à la fois $\tilde{K}$ et son complémentaire, il devrait aussi rencontrer sa frontière, donc K, donc être égal à K, et K rencontrerait $\tilde{K}$, ce qui est absurde). Ceci a deux conséquences : d'abord, L est compact; ensuite, $L^c \supset \tilde{K}$, donc $\tilde{L} \supset \tilde{K}$ et $K \prec L$. Nous avons ainsi montré que L est un majorant de $\mathcal{A}$; il en résulte que l'ordre $\prec$ sur $\mathcal{P}'$ est inductif.

Le lemme de Zorn affirme donc que $\mathcal{P}'$ a un élément maximal, M. C'est un compact non vide. Si Ω était une composante connexe bornée de l'ouvert M^c et y un point de Ω, l'élément de $\mathcal{P}$ passant par y serait inclus dans Ω (sinon il rencontrerait la frontière de Ω, donc M), ce serait donc un compact N tel que $\tilde{n} \supset \Omega^c \supset \tilde{M}$. Comme en outre $\Omega^c \neq \tilde{M}$, ceci contredirait la maximalité de M. La seule composante connexe de M^c est donc $\tilde{M}$ et le théorème est établi.

PROBLÈME 25

Énoncé

Etant donné un triangle, trouver tous les centres
a) des ellipses inscrites dans le triangle,
b) des ellipses ex-inscrites dans le triangle,
c) des hyperboles dont une branche est tangente aux trois côtés du triangle,
d) des hyperboles dont une branche est tangente à deux côtés du triangle et l'autre branche au troisième.

Indication

On peut prendre comme paramètres les points de contact de la conique avec deux des côtés.

PROBLÈME 26

Énoncé

Etant donnés n points distincts sur un cercle, on trace un polygone ayant ces points pour sommets. On suppose que p couples de côtés, et p seulement, ont un point commun autre qu'un sommet, et qu'aucun triplet de côtés n'a de point commun.

1) Ce polygone partage l'intérieur du cercle en r régions. Calculer r en fonction de n et de p.

2) Pour un nombre n donné de côtés, déterminer la valeur maximum du nombre p des points d'intersection des côtés.

PROBLÈME 27

Énoncé

Soient α et x_0 des nombres strictement positifs. On définit une suite $(x_n)_{n \in \mathbb{N}}$ par

$$x_{n+1} = x_n + \frac{\alpha}{x_n}.$$

Donner un équivalent de x_n quand n tend vers l'infini.

La nouvelle algèbre de Viète (traduction de Vaulézard)

Il est possible de quelque poinct donné mener une ligne droicte, de laquelle le segment compris entre deux autres lignes donnees soit donné.

Cecy est une concession tres fameuse, mais elle est seulement αιτημα *demande et* δυσμηχανον *de difficile invention, laquelle jusques à present a esté dite* αλογα *sans raison ; elle solut* εντεχνῶς *artificiellement le probleme mesographic, comprenant la section de l'angle en trois parties egales, l'invention du costé de l'heptagone, et autres quelconques problemes tombant és formules d'equations, ausquelles les cubes sont comparés aux solides, le quarré-quarré, au plans-plans, soient purs, soient avec affection.*

Que l'angle puisse estre divisé en trois parties egales, si une ligne droite est menée d'un point donné, de laquelle le sequent compris entre deux autres donnés soit donné, il est evident et sera demonstré.

Soit l'angle donné DBC sur le costé prolongé DB, et au poinct B estant elevée la perpendiculaire BH ; et du mesme poinct B, comme centre descrit le cercle AED, je dis que si du point C ou le costé BC est coupé par la circonference du cercle est menée une ligne droite de laquelle le segment compris entre les lignes BA BF, est egal au diametre, ED, je dis que l'angle BFH est egal au tiers de l'angle DBC.