de la recherche jusqu'à nos classes : représentation diophantienne des nombres de Fibonacci

par Roger Cuculière
Lycée Carnot, Paris

Dans le livre de François le Lionnais et Jean Brette consacré aux nombres remarquables [49], *on voit apparaître en page* 146 *le polynome*

$$-y^5 + 2y^4x + y^3x^2 - 2y^2x^3 - y(x^4 - 2)$$

qui présente la particularité suivante : lorsque x *et* y *décrivent l'ensemble* **N** *des entiers naturels, l'ensemble des valeurs non-négatives de ce polynome est exactement l'ensemble des termes de la suite de Fibonacci.*

Rappelons que cette suite est définie par : $F_0 = 0$, $F_1 = 1$ *et, pour* $n \geqslant 2$, $F_n = F_{n-1} + F_{n-2}$, *et qu'elle possède un grand nombre de propriétés (voir par exemple* [1] *et* [5].*)*

Dans cet article, nous voudrions retracer l'histoire de ce résultat et en donner une démonstration accessible aux classes de Terminale.

1. Le dixième problème de Hilbert et sa solution

Tout est parti du 2e Congrès International des Mathématiciens tenu à Paris en 1900, où David Hilbert énonça vingt-trois grands problèmes qu'il jugeait essentiels pour le développement des mathématiques ([6]).

Le dixième de ces problèmes s'énonçait ainsi : *"De la possibilité de résoudre une équation de Diophante.* On donne une équation de Diophante à un nombre quelconque d'inconnues et à coefficients entiers rationnels. *On demande de trouver une méthode par laquelle, au moyen d'un nombre fini d'opérations, on pourra distinguer si l'équation est résoluble en nombres entiers rationnels".*

Une "équation de Diophante" ou "équation diophantienne", c'est justement une équation que l'on se propose de résoudre en nombres entiers (ou en nombres rationnels).

Il a fallu arriver en 1970 pour que ce problème reçoive sa solution, avec les travaux du mathématicien soviétique Yuri Matijasevič. Il n'est pas dans notre propos d'exposer en détail cette solution, que l'on trouvera dans [3], mais nous pouvons tout de même en donner une idée. Il faut pour cela poser trois définitions.

Si $P(a_1, a_2 \ldots, a_m, x_1, x_2, \ldots x_n)$ est un polynôme à coefficients entiers par rapport aux variables $a_1, a_2, \ldots a_m, x_1, x_2, \ldots x_n$, on peut considérer que l'équation diophantienne

$$P(a_1, a_2, \ldots a_m, x_1, x_2, \ldots x_n) = 0$$

définit l'ensemble des m-uplets $(a_1, a_2, \ldots a_m)$ pour lesquels cette équation admet au moins une solution en entiers *naturels* ($a_1, a_2, \ldots a_m$ sont les paramètres, et $x_1, x_2, \ldots x_n$ les inconnues). Tout ensemble que l'on peut définir ainsi est dit *diophantien*.

Un ensemble de m-uplets d'entiers naturels sera dit *récursivement énumérable* s'il existe un algorithme bien défini pour dresser une liste des éléments de cet ensemble.

Il n'est pas trop malaisé de montrer que tout ensemble *diophantien* est *récursivement énumérable* car l'équation diophantienne qui le définit fournit assez rapidement l'algorithme désiré.

Mais ce qui est moins immédiat, et qui constitue le *principal théorème* de Matijasevič, c'est la *réciproque*, en vertu de laquelle *les* ensembles diophantiens sont *les* ensembles récursivement énumérables.

Une partie S de **N** est *calculable* s'il existe un algorithme permettant de déterminer en un nombre fini d'opérations si un entier naturel arbitraire est élément de S. On peut montrer que S est calculable si et seulement si S et $\mathbf{N} - S$ sont récursivement énumérables.

Or, un résultat fondamental de la théorie des algorithmes dit qu'il existe une partie K de **N** qui est récursivement énumérable sans être calculable. Ce théorème donne donc la réponse au dixième problème de Hil-

bert, une réponse *négative*. Car cette partie K de N est diophantienne, donc elle admet une définition diophantienne de la forme $P(a, x_1, \dots x_n) = 0$, c'est-à-dire que K est l'ensemble des valeurs du paramètre a pour lesquelles cette équation admet des solutions en entiers naturels. Mais puisque K n'est pas calculable, il n'existe donc pas d'algorithme permettant de vérifier si cette équation a des solutions pour certaines valeurs de a.

Voilà qui règle le cas des équations diophantiennes polynomiales. On trouvera dans [3] des considérations analogues concernant les équations diophantiennes exponentielles.

2. Représentation diophantienne d'un ensemble diophantien

Ce résultat négatif ne clôt pas la question, car les recherches autour de ce sujet ont produit des résultats auxiliaires très intéressants. En 1960, l'américain Hilary Putnam a formulé une remarque qui permet de définir les ensembles diophantiens d'une manière particulièrement frappante. Si S est l'ensemble des entiers naturels a pour lesquels l'équation $P(a, x_1, x_2, \dots x_n) = 0$ admet au moins une solution en entiers naturels, on pose :

$$Q(y, x_1, x_2, \dots x_n) = (y + 1)(1 - (P(y, x_1, \dots x_n))^2) - 1.$$

On vérifie rapidement que S est l'ensemble des valeurs positives ou nulles prises par le polynome Q lorsque $y, x_1, x_2, \dots x_n$ décrivent N. On dit que ce polynome Q constitue une *représentation diophantienne* de l'ensemble S.

Or, il faut remarquer que les ensembles d'entiers naturels dont on s'occupe ordinairement en Théorie des nombres sont en général récursivement énumérables. Tels sont par exemple les *nombres premiers* ou les *nombres de Fibonacci*. Il résulte du théorème principal de Matijasevič que ces ensembles sont diophantiens et la remarque de Hilary Putnam nous assure qu'ils admettent une représentation diophantienne. Une démonstration longue et astucieuse permet de construire une telle représentation pour l'ensemble des nombres premiers : c'est un polynome de degré 25 à 26 variables, dû à l'américain James P. Jones (1976). Le voici à titre de curiosité :

$$\begin{aligned}
&(k+2)\{1-([wz+h+j-q]^2 + [(gk+2g+k+1)\cdot(h+j)+h-z]^2 \\
&+ [16(k+1)^3\cdot(k+2)(n+1)^2 \\
&+ 1-f^2]^2 + [2n+p+q+z-e]^2 + [e^3\cdot(e+2)\cdot(a+1)^2+1-o^2]^2 + \\
&[(a^2-1)y^2+1-x^2]^2 \\
&+ [16r^2y^4\cdot(a^2-1)+1-u^2]^2 + [((a+u^2\cdot(u^2-a))^2-1)\cdot(n+4dy)^2+1-(x+cu)^2]^2 \\
&+ [(a^2-1)l^2+1-m^2 + [ai+k+1-l-i]^2 + [n+l+v-y]^2 + \\
&[p+l(a-n-1) \\
&+ b(2an+2a-n^2-2n-2)-m]^2 + [q+y(a-p-1)+ \\
&s\cdot(2ap+2a-p^2-2p-2)-x]^2 \\
&+ [z+pl(a-p)+t(2ap-p^2-1)-pm]^2)\}
\end{aligned}$$

Des variables au nombre de 26, cela tombe bien pour les appeler $a,b,c,\ldots z$! Regardez ce polynome, et dites-vous bien que l'ensemble des valeurs *positives* qu'il prend lorsque ses 26 variables décrivent N est *exactement* l'ensemble des nombres premiers... Et il commence par le facteur $(k+2)$: étrange, non ?

Ce qui est difficile dans le cas des nombres premiers, et qui donne au résultat ce caractère si gigantesque, c'est de rendre *effectif* le théorème de Matijasevič, c'est-à-dire de passer effectivement du caractère récursivement énumérable de cet ensemble à son caractère diophantien : il est aisé de présenter un algorithme fournissant la liste des nombres premiers, mais il l'est moins d'en déduire une condition de primalité s'exprimant en termes d'équations diophantiennes polynomiales. C'est pourtant ce qu'a réussi J.-P. Jones (pour le détail de la démonstration, voir [8]).

Le cas de l'ensemble $\mathcal{F}$ des nombres de Fibonacci est beaucoup plus facile car leur *définition diophantienne* est beaucoup plus simple, et connue depuis longtemps. Elle découle du :

Théorème de Lucas (1876) :

Les solutions en nombres entiers naturels de l'équation diophantienne $|x^2 + xy - y^2| = 1$ sont exactement les couples $(x,y) = (F_{n-1}, F_n)$ avec $n \geqslant 1$, plus le couple (1,0).

Voici donc une définition diophantienne de $\mathcal{F}$:

$$(x^2 + xy - y^2)^2 - 1 = 0.$$

Si nous lui appliquons la remarque de H. Putman, nous en déduirons la représentation diophantienne suivante :

$$(y + 1)(1 - ((x^2 + xy - y^2)^2 - 1)^2) - 1,$$

un polynome de degré 9 à 2 variables.

Mais J.-P. Jones a fait mieux, il a trouvé le polynome de degré 5 à 2 variables par lequel nous avons commencé cet article :

$Q(x,y) = -y^5 + 2y^4x + y^3x^2 - 2y^2x^3 - y(x^4 - 2)$, publié dans [7].

Observons que $Q(x,y) = y[2 - (x^2 + xy - y^2)^2]$. Sous cette forme, il apparaît que ce polynome vérifie la propriété annoncée : $Q(\mathbf{N},\mathbf{N}) \cap \mathbf{N} = \mathcal{F}$.

Démonstration : Si l'on a $z = Q(x,y)$ avec x,y,z entiers naturels, ou bien y est nul et z aussi, et c'est terminé puisque $0 \in \mathcal{F}$; ou bien $y > 0$, ce qui implique : $2 - (x^2+xy-y^2)^2 \geqslant 0$. Pour cela, deux possibilités : $x^2 + xy - y^2 = 0$ ou $|x^2+xy-y^2| = 1$. Dans le premier cas, il vient $x = y = 0$ parce que x et y sont entiers, d'où $z = 0 \in \mathcal{F}$. Dans le second cas, x et y sont des nombres de Fibonacci d'après le théorème de Lucas et l'on a : $z = y \in \mathcal{F}$.

Réciproquement, tout nombre de Fibonacci est atteint car $Q(F_{n-1}, F_n) = F_n$.

Remarquons que y doit être un entier *naturel* : s'il est négatif, $Q(x,y)$ peut être positif sans être un nombre de Fibonacci (exemple : $Q(1,-2) = 46$). On a en fait : $\mathbf{Q(Z,N)} \cap \mathbf{N} = \mathcal{F}$.

Il reste à démontrer le théorème de Lucas. Dans [7], J.P. Jones le fait par récurrence, mais nous allons procéder différemment.

3. Une démonstration du théorème de Lucas

On pose $\alpha = \frac{1+\sqrt{5}}{2}$ et $\beta = \frac{1-\sqrt{5}}{2}$; ce sont les zéros du polynome $X^2 - X - 1$, qui interviennent très souvent dans la théorie des nombres de Fibonacci. Le réel α est le célèbre Nombre d'Or. On a : $\alpha+\beta = 1$ et $\alpha\beta = -1$. On considère l'ensemble $A = \{x+y\alpha / x \in \mathbf{Z}, y \in \mathbf{Z}\}$.

Puisque $\alpha^2 = 1+\alpha$ et que $\beta = 1-\alpha$, les nombres α^2 et β sont des éléments de A, et A est un *sous-anneau* de **R**. Si $x \in \mathbf{Z}$ et $y \in \mathbf{Z}$, alors $x+y\beta \in A$.

On dit que $x+y\beta$ est le *conjugué* de $x+y\alpha$. L'application σ de A dans A définie par $\sigma(x+y\alpha) = x+y\beta$ est un *automorphisme involutif* de l'anneau A. On peut poser, si $z \in A$, $\sigma(z) = \overline{z}$.

Si $z = x+y\alpha$, avec $x \in \mathbf{Z}$ et $y \in \mathbf{Z}$, on appelle *norme* de z le nombre $N(z) = z\overline{z} = (x+y\alpha)(x+y\beta) = x^2+xy-y^2$: on voit déjà poindre un certain rapport avec la question posée. Si $z \in A$ et $z' \in A$, on a : $N(zz') = N(z)N(z')$.

Nous allons chercher à déterminer l'ensemble U des éléments de A qui possèdent un inverse, lui aussi élément de A. C'est un groupe multiplicatif que l'on appelle le *groupe des unités* de A.

Il est clair que U est précisément l'ensemble des $z \in A$ tels que $|N(z)| = 1$. En effet, si $N(z) = \pm 1$, cela signifie que $z\overline{z} = \pm 1$ et donc que $\frac{1}{z} = \pm \overline{z}$, qui est élément de A. Réciproquement, si $z \in U$, il existe $z' \in A$ tel que $zz' = 1$. Il en résulte $N(z)N(z') = N(zz') = N(1) = 1$ et puisque $N(z)$ et $N(z')$ sont éléments de **Z**, ceci conduit à $N(z) = \pm 1$.

Dire que $z = x+y\alpha$, avec $x \in \mathbf{Z}$ et $y \in \mathbf{Z}$, est élément de U, c'est donc dire que $|x^2+xy-y^2| = 1$, et nous cherchons justement les x et y entiers vérifiant cette équation.

Ce problème possède une interprétation géométrique intéressante, puisqu'il s'agit de déterminer les points à coordonnées entières situés sur les hyperboles H_1 et H_2 d'équations : $x^2+xy-y^2 = -1$ et $x^2+xy-y^2 = 1$. (Voir figure).

Pour caractériser U, nous démontrerons successivement trois propositions :

Proposition 1 **: Si $V = U \cap]1, +\infty[$, alors α est le plus petit élément de V.**

Démonstration : Si $z = x + y\alpha$, avec $x \in \mathbf{Z}$ et $y \in \mathbf{Z}$, est élément de V, on a $|x^2 + xy - y^2| = 1$ et $x + y\alpha > 1$. Le point M de coordonnées (x, y) est situé à la fois sur la réunion des hyperboles H_1 et H_2 et dans le demi-plan ouvert supérieur limité par la droite Δ d'équation $x + y\alpha = 1$. Cette droite Δ coupe les hyperboles en deux points B et C de coordonnées respectives (1,0) et $(-\frac{\sqrt{5}}{5}, \frac{2\sqrt{5}}{5})$. On voit sur la figure ci-contre que tout point $M(x, y)$ répondant à la question a ses coordonnées qui vérifient :
$x > -\frac{\sqrt{5}}{5}$, $y > 0$. Et si de plus x et y sont entiers, ceci implique : $x \geqslant 0, y \geqslant 1$ d'où $z = x + y\alpha \geqslant \alpha$, CQFD.

Ceux qui seraient froissés par ce recours à une figure géométrique peuvent noter que la condition $|x^2 + xy - y^2| = 1$ s'écrit aussi :
$|x + y\alpha| \cdot |x + y\beta| = 1$, et que les deux conditions requises impliquent donc : $x + y\alpha > 1$ et $|x + y\beta| < 1$, ce qui peut d'ailleurs être encore représenté graphiquement à l'aide d'un régionnement du plan par des droites. Ils montreront par un simple calcul que $x + y\alpha > 1$ et $x + y\beta < 1$ impliquent $y > 0$, puis que $x + y\alpha > 1$ et $x + y\beta > -1$ impliquent $x > \frac{-\alpha - \beta}{\alpha - \beta} = -\frac{\sqrt{5}}{5}$ (ne pas oublier que α est positif et β négatif...).

Proposition 2 : $\mathbf{V} = \{\alpha^n ; n \in \mathbf{N}^*\}$.

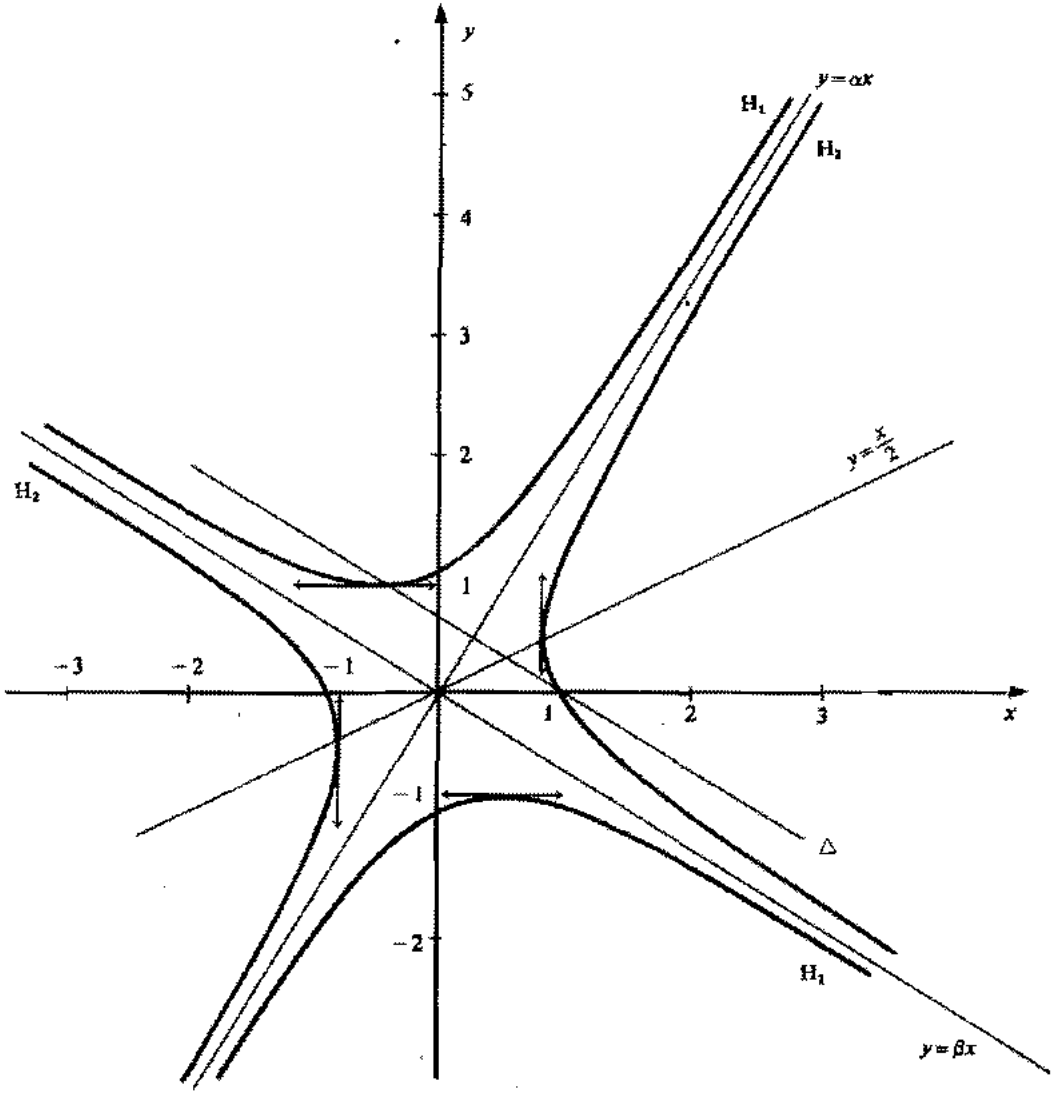
Démonstration : il est évident que, si $n \in \mathbf{N}^*$, alors $\alpha^n \in U$ parce que U est un groupe multiplicatif et $\alpha^n > 1$; donc $\alpha^n \in V$.

Réciproquement, soit $z \in V$. Puisque $z > 1$, il existe $n \in \mathbf{N}^*$ (unique) tel que $\alpha^n \leqslant z < \alpha^{n+1}$ (prendre pour n la partie entière de $\frac{\log z}{\log \alpha}$). Il en résulte : $1 \leqslant \frac{z}{\alpha^n} < \alpha$. Puisque z et α sont éléments du groupe multiplicatif U, il en est de même de $\frac{z}{\alpha^n}$. Si l'on avait $\frac{z}{\alpha^n} > 1$, cela entraînerait donc $\frac{z}{\alpha^n} \in V$, d'où $\frac{z}{\alpha^n} \geqslant \alpha$ d'après la proposition 1. Mais ceci n'est pas vrai, d'où $\frac{z}{\alpha^n} = 1$ et $z = \alpha^n$, CQFD.

Proposition 3 : **pour tout** $n \in \mathbf{N}^*$, $\alpha^n = F_{n-1} + F_n \alpha$.

Démonstration : récurrence sur n...

A ce stade, on observera que le *théorème de Lucas* est démontré : si l'on a $|x^2 + xy - y^2| = 1$ avec $x \in \mathbf{N}$ et $y \in \mathbf{N}^*$, alors $z = x + y\alpha$ est élément de V, d'où : $x + y\alpha = z = \alpha^n = F_{n-1} + F_n\alpha$, et enfin : $x = F_{n-1}$, $y = F_n$.


y
x
5
4
3
2
1
−1
−2
−3
−2
−1
1
2
3
H₁
H₂
y = αx
y = x/2
y = βx
Δ

Réciproquement,
$F_{n-1}^2 + F_{n-1}F_n - F_n^2 = N(F_{n-1} + F_n\alpha) = N(\alpha^n) = (N(\alpha))^n = (-1)^n$.

Si l'on veut en finir avec le groupe U, on peut montrer sans mal que son sous-groupe $U_+ = U \cap \mathbb{R}_+$ n'est autre que $\{\alpha^n / n \in \mathbb{Z}\}$ et en déduire immédiatement que $U = \{\pm\alpha^n / n \in \mathbb{Z}\}$.

4. Dans nos classes

Il semble que nous soyons ici à cent lieues de nos classes. Mais en fait, nous n'en sommes pas si loin, car si tout cela fonctionne, il y a des raisons.

Nous avons procédé à une *extension* du corps Q en lui adjoignant un élément α qui n'appartient pas à Q, mais qui est un zéro d'un polynome à coefficients rationnels : $X^2 - X - 1$. Rajouter α ne suffit pas ; il faut encore rajouter tous les éléments propres à constituer un nouveau corps $K = \{x + y\alpha / x \in Q, y \in Q\}$, extension de Q puisque c'est un corps contenant Q, extension *quadratique* parce que α, et avec lui tout élément de K, est un zéro d'un polynome à coefficients rationnels, *du second degré*. On pose $K = Q(\alpha)$, et au fond, ce que l'on a fait ressemble beaucoup au passage du corps R au corps C, qui n'est autre que $R(i)$. Dans K, le conjugué de α est β, comme dans C celui de i est $-i$, ou celui de j est j^2. La norme dans K ressemble aussi à la norme dans C : $N(z) = z\overline{z} = |z|^2$. Le corps des complexes est un autre exemple d'extension, un exemple connu de nos élèves, et celui que nous étudions ici est tout aussi fécond. Au paragraphe 3, on ne considère pas K tout entier, mais seulement l'anneau A des *entiers* de K, que l'on note aussi $A = Z[\alpha]$. En remplaçant α par i, j, $\sqrt{2}$ ou autre, on peut de même construire d'autres anneaux entiers quadratiques, tout aussi intéressants, tout aussi accessibles, et dont l'étude fournit aussi certaines propriétés des entiers naturels.

Pour en savoir plus, voir [10], [11] et surtout [12].

La démonstration que nous venons de voir ne fait intervenir aucun théorème bien profond, aucun Deus ex Machina. Elle peut être comprise par un élève de Terminale. Mieux, on peut la lui faire trouver en fabriquant un problème en plusieurs questions qui reproduise le plan de cette démonstration.

Ceux qui s'intéressent aux "vrais problèmes", aux problèmes bruts, façon Rallyes ou Olympiades, ont parfois tendance à mépriser les problèmes traditionnels en plusieurs questions. Et l'on doit observer que le triste spectacle de beaucoup de ces énoncés tendrait à leur donner raison. Mais nous tenons ici un moyen de réhabiliter le "problème en questions", qui se légitime lorsqu'il devient un vrai problème, présentant une unité et un but, et qui a été partagé en sous-problèmes (questions) afin de le rendre accessible. Mieux, ceci peut fournir un modèle d'analyse propre à inciter les élèves à mettre en œuvre eux-mêmes un partage analogue lorsqu'ils ont affaire à un problème brut (sur ce sujet, voir [2]).

La démarche ici mise en œuvre est moderne à plus d'un titre. D'abord, nous utilisons largement les concepts de l'algèbre dite moderne, c'est-à-dire les structures telles qu'anneaux et corps. Nous ne les utilisons pas pour elles-mêmes, pour imposer à nos élèves des listes d'axiomes à étudier, mais pour résoudre un problème, un simple problème concernant les bons vieux nombres entiers naturels. Ensuite, dans le cours de notre résolution de ce problème, nous utilisons des notions appartenant à des domaines mathématiques divers : géométrie et même analyse. Le lecteur intéressé trouvera un exemple analogue dans [4], p. 120 : le problème du Baccalauréat C posé à Bordeaux en 1978 portait sur l'anneau $\mathbb{Z}[\sqrt{2}]$ présenté sous forme matricielle (comme naguère les complexes) et utilisé pour résoudre dans $\mathbb{Z}$ l'équation $|x^2 - 2y^2| = 1$.

Cette liberté de méthode est sans doute la principale caractéristique de la modernité en mathématiques depuis Gauss. Ainsi, ce modeste exemple donne une idée de l'unité de notre discipline, et des raisons que nous avons de la présenter aujourd'hui au singulier.

Enfin, un tel problème relié à ses origines telles que nous les avons décrites, permet d'évoquer l'*aventure mathématique*, ce combat constant pour faire reculer l'inconnu. Ce n'est pas tous les jours que nous pouvons exposer un résultat récent à nos élèves : celui-ci, qui date seulement de 1975, aidera peut-être à convaincre les sceptiques qui croient qu'en mathématiques, tout a déjà été trouvé. Présenter des problèmes, les faire résoudre, relater leur histoire, tout cela permet de restituer à la mathématique cette dimension *humaine* et *culturelle* dont l'opinion commune se refuse souvent à la créditer. Bien entendu, ceci exige des élèves capables et désireux de se prêter au jeu : mais c'est là une autre question.

Bibliographie

[1] R. CUCULIÈRE : *A propos de la suite de Fibonacci,* Bulletin A.P.M.E.P. n° 329, juin 1981, pp. 419-422.

[2] R. CUCULIÈRE : *Exemples d'utilisation de problèmes dans un enseignement mathématique : objectifs, méthodes, résultats,* in "Colloque inter-IREM : la place du problème dans l'enseignement des mathématiques, Lyon, les 21 et 22 mai 1982", IREM de Lyon, 1982, pp. 43-62.

[3] M. DAVIS, Y. MATIJASEVIČ, J. ROBINSON : *Hilbert's tenth problem. Diophantine equations : positive aspects of a negative solution*, in "Mathematical developments arising from Hilbert problems", proceedings of symposia in pure mathematics, vol. XXVIII, part 2, AMS 1976, pp. 323-378.

[4] M. DOURAKINE : *Fastes de Mathématiques, Baccalauréat - Séries C et E,* Collection DIA, Belin, 1978.

[5] E. EHRHART : *Identités hyperboliques et fibonacciennes associées,* Bulletin A.P.M.E.P. n° 325, septembre 1980, pp. 652-658.

[6] D. HILBERT : *Sur les problèmes futurs des mathématiques,* in "Compte rendu du 2e Congrès International des mathématiciens, tenu à Paris du 6 au 12 août 1900", Gauthier-Villars, 1902, pp. 58-114.

[7] J.P. JONES : *Diophantine representation of the Fibonacci numbers,* Fibonacci quarterly, vol. 13, n° 4, february 1975, pp. 84-88.

[8] J.P. JONES, D. SATO, M. WADA, D. WIENS : *Diophantine representation of the set of prime numbers,* American Mathematical Monthly, June-July 1976, pp. 449-464.

[9] F. LE LIONNAIS, J. BRETTE : *Les nombres remarquables,* Hermann, 1983.

[10] C. MUTAFIAN : *Le défi algébrique,* tome 2, Vuibert, 1976.

[11] P. SAMUEL : *Théorie algébrique des nombres,* Hermann, 1967.

[12] I. STEWART & D.O. TALL : *Algebraic Number Theory,* Chapman & Hall, London, 1979.