Soyons carrés !

RICHARD CHOULET
Lycée Augustin Fresnel, Caen

Les numéros 153 et 154 de *M&P* (voir [2] et [3]) m'ont ouvert les yeux sur ce résultat qui ne bouleversera les mathématiques mais est assez amusant pour être signalé. Sa formulation est malaisée sans quelques petites remarques préalables.

Expliquons sur un exemple la notation qui va servir et illustre ce qu'on pourrait appeler une conversion de base mais qui n'est pas un changement de base, au sens où on le conçoit d'habitude.

Partons du nombre 315 (écriture habituelle, en base 10). C'est donc $3 \times 10^2 + 1 \times 10 + 5$. Son *converti* par $\Phi_{b/10}$ ($b > 1$, entier) est le nombre $3 \times b^2 + 1 \times b + 5$, qu'on écrira $(315)_b$. L'introduction de $\Phi_{b/10}$ se justifie dès qu'on utilise des expressions littérales : écrire $(n^2)_b$, en effet, n'a pas de sens, car n^2 n'est pas une liste de chiffres ; si je veux désigner le nombre dont l'écriture en base b a les mêmes chiffres que l'écriture de n^2 en base 10, c'est $\Phi_{b/10}(n^2)$ que je dois utiliser.

Voici donc le résultat annoncé :

Il existe un seul entier n compris entre 2 *et* 31 *(on verra plus loin pourquoi le résultat est si modeste) pour lequel $\Phi_{b/10}(n^2)$ n'est un carré que dans une seule base : c'est* 14 *et la base est* 10.

En fait il faut systématiser l'étude faite dans le problème 304 ([2]), avec un peu d'outils théoriques, sur tous les carrés de 2 à 31 en posant l'équation diophantienne à deux inconnues du premier ou du second degré qui en résulte. Au-delà on tombe au mieux sur des équations « à la Mordell » (cube = premier degré) avec des difficultés irrésolues même si l'on sait déjà trouver $b = 10$!

Adresse de l'auteur : Richard Choulet, 27 rue du Quatre Août, F - 14 210 Avenay, France ; courriel : `richardchoulet@wanadoo.fr`.

1. Explorations

J'ai fait l'inventaire des équations auxquelles on arrive et dans tous les cas sauf un, celles-ci ont une infinité de solutions car on a la chance d'avoir une solution évidente au problème avec les conditions de départ où intervient $b = 10$.

1.1. Pour n de 2 à 10

Pour chaque nombre entier n ($2 \leqslant n \leqslant 10$), la recherche des bases $b \geqslant 2$ pour lesquelles $\Phi_{b/10}(n^2)$ est un carré d'entier conduit à une infinité de solutions. Les calculs sont résumés dans le tableau 1.

Équation	Cond. sur b	Valeurs de a	Valeurs de b
$(4)_b = 4 = a^2$	$b \geqslant 5$	$a = 2$	b quelconque
$(9)_b = 9 = a^2$	$b \geqslant 10$	$a = 3$	b quelconque
$(16)_b = b + 6 = a^2$	$b \geqslant 7$	$a \geqslant 4$ quelconque	$b = a^2 - 6$
$(25)_b = 2b + 5 = a^2$	$b \geqslant 6$	$a = 2k + 1$, $k \geqslant 2$	$b = 2k^2 + 2k - 2$
$(36)_b = 3b + 6 = a^2$	$b \geqslant 7$	$a = 3k$, $k \geqslant 2$	$b = 3k^2 - 2$
$(49)_b = 4b + 9 = a^2$	$b \geqslant 10$	$a = 2k + 1$, $k \geqslant 3$	$b = k^2 + k - 2$
$(64)_b = 6b + 4 = a^2$	$b \geqslant 7$	$a = 6k + 2$, $k \geqslant 1$ ou $a = 6k - 2$, $k \geqslant 2$	$b = 6k^2 \pm 4k$
$(81)_b = 8b + 1 = a^2$	$b \geqslant 9$	$a = 2k + 1$, $k \geqslant 4$	$b = \dfrac{k(k+1)}{2}$
$(100)_b = b^2 = a^2$	$b \geqslant 2$	a quelconque	$b = a$

Tab. 1 –

1.2. Pour n de 11 à 31

1.2.1. L'évidence

On voit effectivement tout de suite, que certains des nombres précédents sont toujours des carrés, quelle que soit la base considérée :

$$(121)_b = (b+1)^2 \qquad (b \geqslant 3)\ ;$$
$$(144)_b = (b+2)^2 \qquad (b \geqslant 5)\ ;$$

$$
\begin{aligned}
(169)_b &= (b+3)^2 && (b \geqslant 10)\ ;\\
(441)_b &= (2b+1)^2 && (b \geqslant 5)\ ;\\
(484)_b &= (2b+2)^2 && (b \geqslant 9)\ ;\\
(961)_b &= (3b+1)^2 && (b \geqslant 10).
\end{aligned}
$$

1.2.2. Présentation des types d'équations auxquelles on arrive

Avec les notations ci-dessus, nous avons les équivalences :

$$
\begin{aligned}
&(196)_b = a^2 \Leftrightarrow (2b+9)^2 - 4a^2 = 57\\
&(225)_b = a^2 \Leftrightarrow (2b+1)^2 - 2a^2 = -9\\
&(256)_b = a^2 \Leftrightarrow (4b+5)^2 - 2(2a)^2 = -23\\
&(289)_b = a^2 \Leftrightarrow a^2 - 2(b+2)^2 = 1\\
&(324)_b = a^2 \Leftrightarrow (3b+1)^2 - 3a^2 = -11\\
&(361)_b = a^2 \Leftrightarrow a^2 - 3(b+1)^2 = -2\\
&(529)_b = a^2 \Leftrightarrow (5b+1)^2 - 5a^2 = -44\\
&(576)_b = a^2 \Leftrightarrow (10b+7)^2 - 20a^2 = -71\\
&(625)_b = a^2 \Leftrightarrow (6b+1)^2 - 6a^2 = -29\\
&(676)_b = a^2 \Leftrightarrow (12b+7)^2 - 6(2a)^2 = -95\\
&(729)_b = a^2 \Leftrightarrow (7b+1)^2 - 7a^2 = -62\\
&(784)_b = a^2 \Leftrightarrow (7b+4)^2 - 7a^2 = -12\\
&(841)_b = a^2 \Leftrightarrow (4b+1)^2 - 2a^2 = -1
\end{aligned}
$$

1.2.3. Le cas de 14 : l'équation $(196)_b = a^2$

En factorisant, cela équivaut à $(2(b-a)+9)(2(b+a)+9) = 3 \times 19$ d'où :

$2(b-a)+9$	1	-1	3	-3	19	-19	57	-57
$2(b+a)+9$	57	-57	19	-19	3	-3	1	-1
a	14	-14	4	-4	-4	4	-14	14
b	10	-19	1	-10	1	-10	10	-19

La seule solution avec des entiers naturels est donc $b = 10$ et $a = 14$, c'est-à-dire notre point de départ.

2. Quelques apports théoriques

2.1. Anneau des entiers d'un corps de nombres quadratiques $\mathbf{Q}(\sqrt{d})$ (d naturel non carré d'entier)

Rappelons pour commencer que sur $\mathbf{Q}(\sqrt{d})$, on définit la *norme* d'un élément $x = \alpha + \beta\sqrt{d}$ comme étant $N(x) = \alpha^2 - d\beta^2$. Cette norme N vérifie pour tous éléments x et y du corps :

- $N(x) \in \mathbf{Q}$;
- $N(xy) = N(x)N(y)$;
- $N\left(\dfrac{x}{y}\right) = \dfrac{N(x)}{N(y)}$ (ici $y \neq 0$) ;
- $N(x) = xx^*$ où $x^* = \alpha - \beta\sqrt{d}$ est le conjugué de x.

Qu'est-ce d'abord qu'un entier ? C'est un élément x du corps, donc de la forme $\alpha + \beta\sqrt{d}$ (α et β dans $\mathbf{Q}$), qui satisfait une relation du type $x^2 + ux + v = 0$ avec u et v dans $\mathbf{Z}$.

L'anneau des entiers de $\mathbb{K} = \mathbf{Q}(\sqrt{d})$ est constitué ainsi :

- Si $d \equiv 2$ ou $3 \pmod 4$, c'est $\mathbb{A}_{\mathbb{K}} = \{\alpha + \beta\sqrt{d} : \alpha, \beta \in \mathbf{Z}\} = \mathbf{Z}(\sqrt{d})$;
- Si $d \equiv 1 \pmod 4$, c'est $\mathbb{A}_{\mathbb{K}} = \mathbf{Z}\left(\dfrac{1+\sqrt{d}}{2}\right)$.

2.2. Unités de l'anneau des entiers de $\mathbf{Q}(\sqrt{d})$

Ce sont les éléments inversibles de l'anneau ; ils forment un groupe qu'on note $\mathbb{A}_{\mathbb{K}}^{\times}$ et l'on a :

$$\varepsilon \in \mathbb{A}_{\mathbb{K}}^{\times} \Leftrightarrow |N(\varepsilon)| = 1.$$

Ceci peut être détaillé dans le cas qui nous occupe ($d \in \mathbf{N}^*$) par le résultat suivant : *Il existe une unité $\omega \neq 1$ (appelée unité fondamentale) telle que*

$$\mathbb{A}_{\mathbb{K}}^{\times} = \{\pm\omega^n : n \in \mathbf{Z}\}.$$

2.3. L'équation de Fermat-Pell : $a^2 - db^2 = 1$ $(a,\ b \in \mathbf{N})$

La plus petite solution (x_1, y_1) non triviale, donc autre que $(1, 0)$, est appelée *solution fondamentale*. On démontre qu'elle se recherche en formant les réduites successives dans le développement de $\sqrt{d}$ en fractions continues régulières.

Le résultat suivant vient alors donner toutes les solutions à l'équation ci-dessus :

Soient (x_n, y_n) les solutions de l'équation vérifiant $x_n \geqslant 0$, $y_n \geqslant 0$, rangées dans l'ordre croissant. Alors :
– *Pour tout n, $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$;*
– *Pour tout n, $x_{n+2} = (2x_1)x_{n+1} - x_n$ et $y_{n+2} = (2x_1)y_{n+1} - y_n$*
(on a posé $x_0 = 1$ et $y_0 = 0$).

On peut calculer explicitement x_n et y_n par les formules :

$$x_n = \frac{1}{2}\Big[\big(x_1 + y_1\sqrt{d}\big)^n + \big(x_1 - y_1\sqrt{d}\big)^n\Big],$$
$$y_n = \frac{1}{2\sqrt{d}}\Big[\big(x_1 + y_1\sqrt{d}\big)^n - \big(x_1 - y_1\sqrt{d}\big)^n\Big].$$

2.4. Le produit de Brahmagupta

C'est là qu'intervient ([3]) le produit de Brahmagupta pour écrire encore autrement les solutions.

Pour d non carré d'entier, on le définit sur $\mathbf{Q}^2$ par

$$(a, b) \odot (a', b') = (aa' + dbb', ab' + a'b)$$

qui munit $\mathbf{Q}^2$, privé de $(0, 0)$, d'une structure de groupe abélien isomorphe à $(\mathbf{Q}(\sqrt{d}), \cdot)$.

Par exemple, on a pour $d = 2$: $(1, 1)^{(2)} = (3, 2)$, $(1, 1)^{(3)} = (7, 5)$ et $(1, 1)^{(5)} = (41, 29)$.

Cette notation permet d'écrire commodément les solutions de l'équation de Fermat-Pell.

Prenons l'équation $a^2 - 19b^2 = 1$. La solution fondamentale est $(170, 39)$. Toutes les solutions sont les $(170, 39)^{(n)}$ où $n \in \mathbf{N}$.

Cette suite commence donc par

$$\begin{aligned}(170,39)^{(2)} &= (57\,799, 13\,260),\\ (170,39)^{(3)} &= (19\,651\,490, 4\,508\,361),\\ &\vdots\end{aligned}$$

Remarquons que, dans le cas simple par exemple de $d = 2$ pour lequel $\sqrt{2} = [1, 2, 2, 2 \cdots]$, les réduites sont successivement $1 = \frac{1}{1}$, $1 + \frac{1}{2} = \frac{3}{2}$ puis $1 + \dfrac{1}{2 + \frac{1}{2}} = \dfrac{7}{5}$, $1 + \dfrac{1}{2 + \frac{1}{2+\frac{1}{2}}} = \dfrac{17}{12}$, ..., c'est-à-dire données par les couples puissances de $(1, 1)$.

2.5. « D'où » la résolution de $a^2 - db^2 = c$

Supposant que l'équation : $a^2 - db^2 = c$ ($d \neq 0$ non carré d'entier) admet (ce qui n'est pas évident : voir par exemple [1]) une solution $\gamma_0 = (a_0, b_0)$, alors tout γ du type $\gamma = \pm\gamma_0\omega^n$, où ω est une unité fondamentale de $\mathbf{Q}\big(\sqrt{d}\big)$ et $n \in \mathbf{Z}$, est solution de l'équation.

Donnons un exemple concret de ce résultat : soit à résoudre $(361)_b = a^2$.

On a vu que cela se ramène à :

$$B^2 - 3A^2 = -2 \tag{1}$$

avec $B = a$ et $A = b + 1$.

Cette équation a pour couples solutions (B, A) : $(1, 1)$, $(5, 3)$, $(19, 11)$, et plus généralement tout $(1, 1)\odot(2, 1)^{(n)}$, puisque $(2, 1)$ est unité fondamentale de $\mathbf{Q}(\sqrt{3})$.

Le retour à notre problème concret donne ensuite, outre $b = 10$ et $a = 19$, $b = 40$ et $a = 71$... Nous y reviendrons dans le paragraphe 4.

3. Les résultats

Les résultats figurent dans le tableau 2.

Problème	Équation	Cond. sur b	Valeurs de b	Valeurs de a
$(121)_b = a^2$	$(2b+9)^2 - 4a^2 = 57$	$b \geqslant 3$	b quelconque	$a = b+1$
$(144)_b = a^2$	$(2b+9)^2 - 4a^2 = 57$	$b \geqslant 5$	b quelconque	$a = b+2$
$(169)_b = a^2$	$(2b+9)^2 - 4a^2 = 57$	$b \geqslant 10$	b quelconque	$a = b+3$
$(196)_b = a^2$	$(2b+9)^2 - 4a^2 = 57$	$b \geqslant 10$	$\boldsymbol{b = 10}$	$\boldsymbol{a = 14}$
$(225)_b = a^2$	$(2b+1)^2 - 2a^2 = -9$	$b \geqslant 6$	$b = 10, 61, 358, \dots$	$a = 15, 87, 507, \dots$
$(256)_b = a^2$	$(4b+5)^2 - 2(2a)^2 = -23$	$b \geqslant 7$	$b = 10, 213, 382, \dots$	$a = 16, 303, 542, \dots$
$(289)_b = a^2$	$a^2 - 2(b+2)^2 = 1$	$b \geqslant 10$	$b = 10, 68, 406, \dots$	$a = 17, 99, 577, \dots$
$(324)_b = a^2$	$(3b+1)^2 - 3a^2 = -11$	$b \geqslant 5$	$b = 10, 144, 2010, \dots$	$a = 18, 250, 3482, \dots$
$(361)_b = a^2$	$a^2 - 3(b+1)^2 = -2$	$b \geqslant 7$	$b = 10, 40, 152, \dots$	$a = 19, 71, 265, \dots$
$(400)_b = a^2$	$(2b)^2 - a^2 = 0$	$b \geqslant 5$	b quelconque	$a = 2b$
$(441)_b = a^2$	$(2b+1)^2 - a^2 = 0$	$b \geqslant 5$	b quelconque	$a = 2b+1$
$(484)_b = a^2$	$(2b+2)^2 - a^2 = 0$	$b \geqslant 9$	b quelconque	$a = 2b+2$
$(529)_b = a^2$	$(5b+1)^2 - 5a^2 = -44$	$b \geqslant 10$	$b = 10, 36, 70, \dots$	$a = 23, 81, 157, \dots$
$(576)_b = a^2$	$(10b+7)^2 - 20a^2 = -71$	$b \geqslant 8$	$b = 10, 95, 3450, \dots$	$a = 24, 294, 7716, \dots$
$(625)_b = a^2$	$(6b+1)^2 - 6a^2 = -29$	$b \geqslant 7$	$b = 10, 19, 998, \dots$	$a = 25, 47, 2445, \dots$
$(676)_b = a^2$	$(12b+7)^2 - 6(2a)^2 = -95$	$b \geqslant 8$	$b = 10, 355, \dots$	$a = 26, 871, \dots$
$(729)_b = a^2$	$(7b+1)^2 - 7a^2 = -62$	$b \geqslant 10$	$b = 10, 429, \dots$	$a = 27, 162, \dots$
$(784)_b = a^2$	$(7b+4)^2 - 7a^2 = -12$	$b \geqslant 9$	$b = 10, 168, 2686, \dots$	$a = 28, 446, 7108, \dots$
$(841)_b = a^2$	$(4b+1)^2 - 2a^2 = -1$	$b \geqslant 9$	$b = 10, 348, \dots$	$a = 29, 985, \dots$
$(900)_b = a^2$	$(3b)^2 - a^2 = 0$	$b \geqslant 10$	b quelconque	$a = 3b$
$(961)_b = a^2$	$(3b+1)^2 - a^2 = 0$	$b \geqslant 10$	b quelconque	$a = 3b+1$

TAB. 2 –

4. Étude détaillée de deux exemples, et quelques formules inoubliables !

4.1. Retour sur $(361)_b = a^2$

Nous avons obtenu toutes les solutions de $B^2 = 3A^2 - 2$ (Attention : on cherche les couples (B, A)), qui assurent une solution du problème posé, sous la forme $(19, 11) \odot (2, 1)^{(n)}$. Nous savons que les B et A obtenus sont les termes consécutifs d'une suite récurrence linéaire d'ordre deux satisfaisant la même relation :

$$u_{n+2} = 4u_{n+1} - u_n.$$

Il en est « presque » de même pour a et b. Plus précisément les solutions (a, b) de $(361)_b = a^2$ sont les couples (a_n, b_n) tels que

- (a_n) vérifie la récurrence : $a_{n+2} = 4a_{n+1} - a_n$ avec $a_1 = 19$ et $a_2 = 71$;
- (b_n) vérifie la récurrence : $b_{n+2} = 4b_{n+1} - b_n + 2$ avec $b_1 = 0$ et $b_2 = 40$.

Pour de amples renseignements sur ce genre de problèmes diophantiens et sur les suites, qui inévitablement apparaissent, ayez la curiosité d'aller voir le site [4] de Neil Sloane.

4.2. Un exemple de suites imbriquées : $(256)_b = a^2$

En ayant posé $X = 4b + 5$ et $Y = 2a$, on cherche d'abord les solutions de $X^2 = 2Y^2 - 23$ sur les entiers naturels. Les solutions en sont les couples (X_n, Y_n) tels que les sous-suites des termes de rangs pair et celle des termes de rang impair satisfont la même relation de récurrence :

$$u_{n+2} = 6u_{n+1} - u_n.$$

Ceci s'explique par le fait, dans cet exemple et contrairement à 4.1, qu'il y a deux solutions de base $(3, 4)$ et $(7, 6)$ qui permettent de générer l'ensemble des solutions par réunion des deux sous-ensembles associés à chacune d'elles avec $(3, 4) \odot (3, 2)^{(n)}$ et $(7, 6) \odot (3, 2)^{(n)}$.

Le retour à a et b n'est pas automatique du moins pour ce qui est de b puisque $b = (X - 5)/4$. C'est ainsi que les couples (a, b) apparaissent comme les termes consécutifs de la suite (a_{n+1}, b_{n+1}), $n \geqslant 1$ pour laquelle

- (a_n) a ses deux sous-suites des termes de rang pair et de rang impair qui satisfont la même récurrence : $u_{n+2} = 34u_{n+1} - u_n$ avec $a_1 = 9$,

$a_2 = 16$, $a_3 = 303$ et $a_4 = 542$ d'où $a_5 = 10293$ et $a_6 = 18412$ par exemple ;

– (b_n) a ses deux sous-suites des termes de rang pair et de rang impair qui satisfont la même récurrence : $u_{n+2} = 34u_{n+1} - u_n + 40$ avec $b_1 = 5$, $b_2 = 10$, $b_3 = 213$ et $b_4 = 382$ d'où $b_5 = 7277$ et $b_6 = 13018$ par exemple.

4.3. Quelques morceaux choisis

Vous découvrirez ici quelques relations qui auraient paru stupéfiantes sans toutes les précautions précédentes !

$$\begin{aligned}(256)_{13\,018} &= 18\,412^2,\\ (676)_{101\,770} &= 249\,286^2,\\ (784)_{682\,318} &= 1\,805\,404^2.\end{aligned}$$

5. Et au-delà de 31 ?

Après 31, la situation n'est pas brillante, comme on l'a dit, car l'équation obtenue, malgré sa solution évidente, ne se laisse pas démonter.

En reprenant des notations plus classiques, le tableau 3 indique pour les entiers considérés, à partir de 32, uniquement ceux pour lesquels il y a une autre solution que la triviale obtenue avec $Y = 10$ dans un « temps machine raisonnable », en ayant testé tous les entiers dans la fourchette proposée, ce qui ne veut pas dire qu'il n'y a pas des solutions plus grandes.

6. Moralité : Vive le Calvados

Évidemment pour les esprits et les estomacs sensibles, je ne prône pas la consommation de ce délicieux breuvage qu'on sert chez nous, sous le nom poétique (?) de trou normand, mais je voulais attirer l'attention de manière provocante sur une particularité du nombre 14 qui, comme personne ne l'ignore, du moins je l'imagine, est le numéro de mon département.

Post scriptum :

1) Avec [4], vous découvrirez que 361 en base $4 \times A046178(n) - 2$ est le carré

X	X^2 en base Y	Équation	Valeurs de X	et de $Y < 4000$
32	$(1024)_Y = X^2$	$Y^3 + 2Y + 4 = X^2$	32	10
			4486	272
			40 277	1175
35	$(1225)_Y = X^2$	$Y^3 + 2Y^2 + 2Y + 5 = X^2$	35	10
			40	11
40	$(1600)_Y = X^2$	$Y^3 + 6Y^2 = X^2$	$n(n^2 - 6)$	$n^2 - 6$
41	$(1681)_Y = X^2$	$Y^3 + 6Y^2 + 8Y + 1 = X^2$	41	10
			89	18
			1217	112
			45 473	1272
45	$(2025)_Y = X^2$	$2Y^3 + 2Y + 5 = X^2$	45	10
			221	29
			641	59
47	$(2209)_Y = X^2$	$2Y^3 + 2Y^2 + 9 = X^2$	47	10
			111	18
			297	85
			5073	234
50	$(2500)_Y = X^2$	$2Y^3 + 5Y^2 = X^2$	$(2n+1)(2n^2 + 2n - 2)$	$2n^2 + 2n - 2$
53	$(2809)_Y = X^2$	$2Y^3 + 8Y^2 + 9 = X^2$	53	10
			3453	180

TAB. 3 –

de $6 \times A046179(n) - 1$!
2) Petit bijou final : $(1225)_{5602} = 419\,365^2$.

Bibliographie

[1] Daniel DUVERNEY, *Théorie des nombres*, Dunod, Paris, 1998.

[2] P. LE GALL, Problème 304, *M&P*, **153** (2005), 57–59.

[3] Pierre PAQUAY, Petite étude des fractions continues et leur application à l'équation de Pell-Fermat, *M&P*, **154** (2005), 21–37.

[4] `http://www.research.att.com/~njas/sequences`