équation de Pell-Fermat

par Emilie Beaudoin, Marine Bignon, Béryl Boissavy, Marine Chambard, Elodie Charpentier, Virginie Montero, Delphine Pissavin, Aurélie Silondie, élèves de Seconde du Lycée Pablo Picasso de Fontenay-sous-Bois (94) et Mohammed Talmoudi du Lycée Romain Rolland d'Ivry (94)

enseignantes : Claude Parreau, Christiane Guedj et Monique Corlay

chercheur : Olivier Piltant

lycées d'Ivry (94) & de Fontenay sous Bois (94) — ***problème de Pell-Fermat***

Quels sont les nombres entiers qui ont un inverse également entier ? Ce problème très simple devient l'équation de Pell-Fermat quand on s'intéresse non plus aux nombres entiers mais à tous les nombres de la forme $a + b\sqrt{p}$ où a et b sont des entiers (positifs ou négatifs) et p est un nombre premier.

Bordeaux :

<u>COMPTE RENDU sur l'exposé du problème de PELL-FERMAT</u>

Combien y a-t-il de nombres dont l'inverse est entier ? Dans N, un seul :1 ; dans Z deux: -1 et 1. Et dans R ?
L'exposé fut très méthodique et organisé, et surtout compréhensible par tous.
De plus, coup de chapeau aux élèves qui, bien que nombreux, ont réussi à nous présenter leurs recherches le plus clairement possible et à répartir équitablement leur temps de parole.

Le problème ressemble à celui-ci qui est très simple : quels sont les nombres entiers (positifs ou négatifs), qui ont un inverse également entier, c'est-à-dire quels sont les a dans Z tels qu'il existe b dans Z et $ab = 1$?

Soit p un nombre premier, considérons tous les nombres de la forme $a + b\sqrt{p}$ où a et b sont des entiers positifs ou négatifs.

Cherchons les nombres $a + b\sqrt{p}$ tels qu'il existe un nombre $c + d\sqrt{p}$ où $(a + b\sqrt{p})(c + d\sqrt{p}) = 1$. Autrement dit, nous recherchons les nombres de la forme $a + b\sqrt{p}$ qui admettent un inverse $1/(a + b\sqrt{p})$ de la même forme.

Somme et produit des nombres de la forme $a + b\sqrt{p}$ ***où*** a ***et*** b ***sont des entiers relatifs.***

$(3+4\sqrt{2}) + (1+\sqrt{2}) = 4+5\sqrt{2}$

Soit $a + b\sqrt{p}$ où a et b sont des entiers relatifs.
Soit $c + d\sqrt{p}$ où c et d sont des entiers relatifs.

Calculons leur somme :

$(a + b\sqrt{p}) + (c + d\sqrt{p}) = (a + c) + (b + d)\sqrt{p}$ où $a + c$ et $b + d$ sont des entiers relatifs.

$(3 + 4\sqrt{2}) \times (1+ \sqrt{2}) = 11 + 7\sqrt{2}$
$(-3 + 4\sqrt{2}) \times (1 - \sqrt{2}) = -11+7\sqrt{2}$

Soit $a + b\sqrt{p}$ où a et b sont des entiers relatifs.
Soit $c + d\sqrt{p}$ où c et d sont des entiers relatifs.

Calculons le produit :

$(a+b\sqrt{p}) \times (c+d\sqrt{p}) = ac + ad\sqrt{p} + bc\sqrt{p} + bdp = (ac + bdp) + (ad + bc)\sqrt{p}$ où $ac + bdp$ et $ad + bc$ sont des entiers relatifs.

Calcul de l'inverse de $a + b\sqrt{p}$ ***où*** a ***et*** b ***sont des entiers relatifs.***

exemples

Le nombre $3+4\sqrt{2}$ admet pour inverse $1/(3+4\sqrt{2})$ …

$$\frac{1}{3+4\sqrt{2}} = \frac{3-4\sqrt{2}}{(3+4\sqrt{2})(3-4\sqrt{2})}$$
$$\frac{1}{3+4\sqrt{2}} = \frac{3-4\sqrt{2}}{9-32}$$
$$\frac{1}{3+4\sqrt{2}} = \frac{3-4\sqrt{2}}{-23}$$
$$\frac{1}{3+4\sqrt{2}} = \frac{-3}{23} + \frac{4}{23}\sqrt{2}$$

Le nombre 3+4√2 a pour inverse (–3/23)+(4/23)√2. Les nombres (–3/23) et (4/23) ne sont pas des entiers, le nombre 3+4√2 ne convient pas

Autre exemple : le nombre 1+ √2 admet pour inverse 1/(1+ √2).

$$\frac{1}{1+\sqrt{2}} = \frac{1-\sqrt{2}}{(1+\sqrt{2})(1-\sqrt{2})}$$
$$\frac{1}{1+\sqrt{2}} = \frac{1-\sqrt{2}}{1-2}$$
$$\frac{1}{1+\sqrt{2}} = \frac{1-\sqrt{2}}{-1}$$
$$\frac{1}{1+\sqrt{2}} = -1+\sqrt{2}$$

Le nombre 1+ √2 admet pour inverse –1+ √2. Ce nombre 1+ √2 convient.

Cas général :

$$\frac{1}{a+b\sqrt{p}} = \frac{a-b\sqrt{p}}{(a+b\sqrt{p})\times(a-b\sqrt{p})}$$

Comme $(a+b\sqrt{p})\times(a-b\sqrt{p}) = a^2 - p\,b^2$

$$\frac{1}{a+b\sqrt{p}} = \frac{a-b\sqrt{p}}{a^2-p\,b^2}$$
$$\frac{1}{a+b\sqrt{p}} = \frac{a}{a^2-p\,b^2} + \left(\frac{-b}{a^2-p\,b^2}\right)\sqrt{p}$$

Nous cherchons a et b pour que les nombres

$$\frac{a}{a^2-p\,b^2} \text{ et } \frac{-b}{a^2-p\,b^2}$$

soient des entiers relatifs.

Théorème. Pour qu'un nombre $a + b\sqrt{p}$ où a et b sont des entiers relatifs admette un inverse de la même forme, il faut et il suffit que $a^2 - p\,b^2 = 1$ ou $a^2 - p\,b^2 = -1$.

Démonstration :

$$\frac{1}{a+b\sqrt{p}} = \frac{a}{a^2-p\,b^2} + \left(\frac{-b}{a^2-p\,b^2}\right)\sqrt{p}$$

Soit un nombre $a + b\sqrt{p}$ tel que $a^2 - p\,b^2 = 1$, alors $\frac{1}{a+b\sqrt{p}} = a - b\sqrt{p}$.

Soit un nombre $a + b\sqrt{p}$ tel que $a^2 - pb^2 = -1$, alors $\frac{1}{a+b\sqrt{p}} = -a + b\sqrt{p}$.

Réciproquement :

Soit un nombre $a + b\sqrt{p}$ tel que $a^2 - p\,b^2 = k$ où k est un entier relatif.

$$\frac{1}{a+b\sqrt{p}} = \frac{a}{k} + \frac{-b}{k}\sqrt{p}$$

a/k et $-b/k$ sont des nombres entiers que l'on appelle n et m. ($a = k\,n$ et $b = k\,m$.)

On remplace a par $k\,n$ et b par $k\,m$ dans l'égalité $a^2 - p\,b^2 = k$:

$$a^2 - p\,b^2 = k$$
$$k^2n^2 - p\,k^2\,m^2 = k$$
$$k^2\,(n^2 - p\,l^2) = k$$
$$k\,(n^2 - p\,l^2) = 1$$

Deux entiers dont le produit est égal à 1 sont égaux à 1 ou à – 1, donc k est égal à 1 ou à – 1.

Corollaire. Dès qu'on a une solution (différente de 1 et de – 1), on en a trois autres :

$a + b\sqrt{p}$
puis $-a + b\sqrt{p}$
et $a - b\sqrt{p}$
et $-a - b\sqrt{p}$.

Recherche de nombres.

Dans le cas où $p = 2$, l'équation devient : $a^2 - 2b^2 = 1$. a donné, calculons b :

$$a^2 = 2b^2 + 1$$
$$a^2 - 1 = 2b^2$$
$$\frac{1}{2}(a^2 - 1) = b^2$$

Cherchons a^2 tel que $\frac{1}{2}(a^2 - 1)$ soit un carré d'entier.

Nous avons trouvé $a^2 = 9$ d'où $\frac{1}{2}(a^2 - 1) = 4$ c'est-à-dire $b^2 = 4$.

Ce qui donne les nombres $3+2\sqrt{2}$, $3-2\sqrt{2}$, $-3+2\sqrt{2}$, $-3-2\sqrt{2}$. De même $a^2 = 289$ d'où $b^2 = 144$, ce qui donne les nombres $17+12\sqrt{2}$, $17-12\sqrt{2}$, $-17+12\sqrt{2}$, $-17-12\sqrt{2}$.

Dans le cas où $p = 2$, l'équation peut aussi être : $a^2 - 2b^2 = -1$. a donné, calculons b :

$$a^2 = 2b^2 - 1$$
$$a^2 + 1 = 2b^2$$
$$\frac{1}{2}(a^2 + 1) = b^2$$

Cherchons a^2 tel que $\frac{1}{2}(a^2 + 1)$ soit un carré d'entier.

Nous avons trouvé $a^2 = 1$ d'où $\frac{1}{2}(a^2 + 1) = 1$ c'est-à-dire $b^2 = 1$.

Ce qui donne les nombres $1+\sqrt{2}$, $1-\sqrt{2}$, $-1+\sqrt{2}$, $1-\sqrt{2}$. De même $a^2 = 49$ d'où $b^2 = 25$, ce qui donne les nombres $7+5\sqrt{2}$, $7-5\sqrt{2}$, $-7+5\sqrt{2}$, $-7-5\sqrt{2}$.

Cette méthode ne nous permet pas de trouver beaucoup de solutions.

Puissance d'une solution.

THEOREME : Dans le cas où $p = 2$, les nombres $(1 + \sqrt{2})^n$, avec n entier relatif, sont des solutions.

$$(1 + \sqrt{2})(-1 + \sqrt{2}) = 1$$

$$\frac{1}{1 + \sqrt{2}} = -1 + \sqrt{2}$$

$$(1 + \sqrt{2})^2 (-1 + \sqrt{2})^2 = 1$$
$$(3 + 2\sqrt{2})(3 - 2\sqrt{2}) = 1$$

$$\frac{1}{3 + 2\sqrt{2}} = 3 - 2\sqrt{2}$$

$$(1 + \sqrt{2})^n (-1 + \sqrt{2})^n = 1$$

$$\frac{1}{\left(1 + \sqrt{2}\right)^n} = \left(-1 + \sqrt{2}\right)^n$$

Exemple : A quelle puissance de $1+\sqrt{2}$ le nombre $19601+13860\sqrt{2}$ est-il égal ?

Le nombre $19601+13860\sqrt{2}$ est-il une puissance de $1+\sqrt{2}$? S'il existe un entier k tel que $A^k = 19601+13860\sqrt{2}$, comme $A^{k-1} = A^k / A = A^k \times (1/A)$:

$$A^{k-1} = (19601+13860\sqrt{2}) \times (-1 + \sqrt{2})$$
$$A^{k-1} = (2\times 13860-19601) + (19601-13860)\sqrt{2}$$
$$A^{k-1} = 8119 + 5741\sqrt{2}$$

De même :

$$A^{k-2} = 3363 + 2378\sqrt{2}$$
$$A^{k-3} = 1393 + 985\sqrt{2}$$
$$A^{k-4} = 577 + 408\sqrt{2}$$
$$A^{k-5} = 239 + 169\sqrt{2}$$
$$A^{k-6} = 99 + 70\sqrt{2}$$
$$A^{k-7} = 41 + 29\sqrt{2}$$
$$A^{k-8} = 17 + 12\sqrt{2}$$
$$A^{k-9} = 7 + 5\sqrt{2}$$
$$A^{k-10} = 3 + 2\sqrt{2}$$
$$A^{k-11} = 1 + \sqrt{2}$$

Conclusion :

$$19601+13860\sqrt{2} = (1 + \sqrt{2})^{12}.$$

Quels sont les inversibles ?

Soit A l'ensemble des nombres de la forme $a + b\sqrt{2}$ avec a et b entiers.

Soit B l'ensemble des éléments de A, inversibles dans A. Nous savons que, parmi les éléments de B, il y a : 1, –1, $1+\sqrt{2}$, $-1+\sqrt{2}$, $-1-\sqrt{2}$, $1-\sqrt{2}$ ainsi que toutes les puissances de ces nombres. Maintenant, il s'agit de voir si seules les puissances de $(1+\sqrt{2})$, $(1-\sqrt{2})$, $(-1+\sqrt{2})$ et de $(-1-\sqrt{2})$, 1 et –1, sont des éléments de B.

Plaçons nous ici dans T, le sous-ensemble de B où $a > 0$ et $b > 0$. Dans T, il y a les nombres de la forme $(1+\sqrt{2})^n$. (n entier strictement plus grand que 0). Supposons qu'il y ait dans T, au moins un nombre m, qui ne soit pas une puissance de $(1+\sqrt{2})$. Parmi ceux-là, je choisis le nombre $m = x + y$ tel que $x > 0$, $y > 0$ et m le plus petit possible. Divisons ce nombre par $(1+\sqrt{2})$. Soit g, le résultat obtenu : g est forcément plus petit que m, car $(1+\sqrt{2}) > 1$, et g est positif car la division de deux positifs donne un positif. De plus, g est un élément de B car la division de deux inversibles donne un inversible.

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

Je veux prouver que ce nombre g appartient à T, donc je vais prouver que $x - y$ et $2y - x$ sont des nombres strictement positifs.

Prouvons d'abord que $x - y$ est strictement positif.

Repartons de l'équation de Pell-Fermat :

$$x^2 - 2y^2 = \pm 1$$

Nous pouvons considérer que $y > 2$. En effet, nous sommes, d'une part, dans le cas où $b > 0$ et donc $y > 0$. De plus, y ne peut être égal à 1, sinon on aurait $x + y\sqrt{2} = 1+\sqrt{2}$ alors que $x + y\sqrt{2}$ ne peut être égal à une puissance de $1+\sqrt{2}$.

$$x^2 - 2y^2 = \pm 1$$
$$x^2 - y^2 = \pm 1 + y^2$$

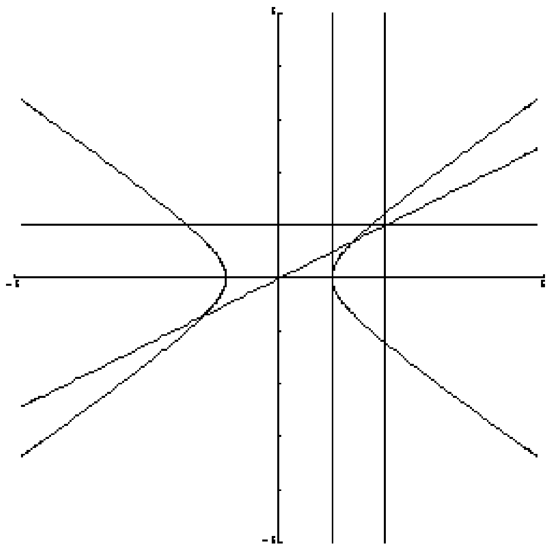
Or $y > 2$ et donc $y^2 \pm 1 > 0$. Il s'ensuit que $x^2 - y^2 > 0$; donc $x^2 > y^2$, soit $x > y$ car x et y positifs. **Donc $x - y$ est strictement positif.**

Prouvons ensuite que $2y - x$ est strictement positif.

On a 2 cas :
• soit $y > x/2$ et $2y - x$ est strictement positif
• soit $y \le x/2$ et $2y - x$ est strictement négatif. Or, dans ce cas-là, $x^2 - 2y^2 = 1$ car, $2y \le x$ et $4y^2 \le x^2$ et a fortiori $2y^2 \le x^2$ et $x^2 - 2y^2$ est strictement positif. En conclusion, dans ce cas, x et y doivent vérifier les conditions suivantes :

$x > 0$;
$0 < y$;
$x^2 - 2y^2 = 1$;
x et y entiers naturels.

Résolvons ce système graphiquement :



Il n'y a aucun point de coordonnées entières qui vérifie le système. **Donc $2x - y$ est strictement positif.**

<u>Conclusion</u> : Nous avons prouvé que le nombre g appartient à T. Comme il est plus petit que m; il est donc une puissance de $(1+\sqrt{2})$. Or $m = g\,(1+\sqrt{2})$. Donc m est lui aussi une puissance de $1+\sqrt{2}$. Nous avons démontré par la méthode de raisonnement par l'absurde que **les inversibles de A sont donc uniquement :** 1, –1, $1+\sqrt{2}$, $-1+\sqrt{2}$, $-1-\sqrt{2}$, $1-\sqrt{2}$ **ainsi que toutes les puissances de ces nombres.**