DOMAINE : Arithmétique
NIVEAU : Intermédiaires
CONTENU : Exercices

AUTEUR : François LO JACOMO
STAGE : Cachan 2011 (junior)

Equations diophantiennes

- Équations diophantiennes-

Les équations diophantiennes sont des équations dont on recherche des solutions entières (ou rationnelles). Trouver deux réels x et y tels que $y^2 = x^2 + x + 1$ est facile, il suffit de choisir par exemple : $x = 1$ et $y = \sqrt{3}$, mais on ne peut pas trouver deux entiers (hormis $x = 0$ et $y = 1$) vérifiant cette équation car x^2+x+1 est compris entre x^2 et $(x+1)^2 = x^2+2x+1$ et il ne peut pas exister de carré entre ces deux carrés consécutifs. Certaines équations diophantiennes sont parmi les problèmes les plus difficiles de toute l'histoire des mathématiques, par exemple le célèbre "grand théorème de Fermat" : montrer que pour $n \geqslant 3$, on ne peut pas trouver d'entiers strictement positifs x, y et z tels que $x^n + y^n = z^n$, que les plus grands mathématiciens du monde ont cherché pendant plus de trois siècles, découvrant à cette occasion beaucoup de nouveaux outils mathématiques, jusqu'à ce que l'équation soit totalement résolue en 1995.

Exercice 1 Trouver tous les triplets d'entiers strictement positifs (x, y, z) avec $x \leqslant y \leqslant z$, tels que $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1$

Exercice 2 Résoudre dans $\mathbb{Z}$, puis dans $\mathbb{Q}$, l'équation : $2x^3 + xy - 7 = 0$

Exercice 3 Trouver deux solutions simples de l'équation : $(x-1)^2 + (x+1)^2 = y^2 + 1$, x et y étant des entiers positifs ou nuls.

Trouver trois entiers a, b et c tels que, si (x, y) est solution de l'équation, $(ax + by, cx + ay)$ est lui aussi solution.

En déduire que l'équation admet une infinité de solutions.

Exercice 4 Trouver tous les entiers x solutions de l'équation : $x^3 + (x+1)^3 + (x+2)^3 = (x+3)^3$

Solution de l'exercice 1 Comme $\frac{1}{x} \geqslant \frac{1}{y} \geqslant \frac{1}{z}$, on doit avoir nécessairement $\frac{1}{x} \geqslant \frac{1}{3}$ soit $x \leqslant 3$. Si $x = 3$, $\frac{1}{y} + \frac{1}{z} = \frac{2}{3}$, donc $y \leqslant 3$: seule solution possible $(3,3,3)$. Si $x = 2$, $\frac{1}{y} + \frac{1}{z} = \frac{1}{2}$, donc $y \leqslant 4$: deux solutions, $(2,4,4)$ et $(2,3,6)$. Et il est clair que $x = 1$ ne convient pas, car $\frac{1}{y} + \frac{1}{z}$ ne peut pas être nul.

Solution de l'exercice 2 L'équation peut s'écrire : $x\left(2x^2 + y\right) = 7$. Dans $\mathbb{Z}$, cela nécessite que x soit un diviseur de 7, auquel cas $y = \frac{7}{x} - 2x^2$, d'où quatre possibilités :

$x = 1, y = 5, x = -1, y = -9, x = 7, y = -97, x = -7, y = -99.$

Dans $\mathbb{Q}$, x peut être quelconque (non nul) : pour tout x rationnel non nul, $y = \frac{7}{x} - 2x^2$ est un rationnel tel que (x,y) vérifie l'équation.

Solution de l'exercice 3 Les solutions les plus simples sont celles vérifiant : $(x-1)^2 = 1$, $y = x+1$, mais il n'y en a que deux : $(0,1)$ et $(2,3)$. C'est à partir d'elles qu'on peut construire une infinité d'autres solutions de l'équation diophantienne.

Si l'on développe, l'équation s'écrit : $y^2 - 2x^2 = 1$. Pour que $(ax+by, cx+ay)$ soit solution lorsque (x,y) est solution, il suffit donc que pour tout (x,y), $(cx+ay)^2 - 2(ax+by)^2 = y^2 - 2x^2$. En étudiant séparément le terme en x^2, celui en xy et celui en y^2, on remarque que ceci est vrai si l'on a simultanément : $c^2 - 2a2 = -2$,$2ac - 4ab = 0$, $a^2 - 2b^2 = 1$. La condition du milieu entraîne $c = 2b$ auquel cas les deux autres conditions sont équivalentes. Or $a^2 - 2b^2 = 1$ est précisément l'équation que l'on étudie, dont on connait une racine autre que $(1,0)$: $(3,2)$. Si (x,y) est solution, $(3x+2y, 4x+3y)$ est aussi solution, strictement supérieure $(3x+2y > x, 4x+3y > y)$, ce qui permet de construire une infinité de solutions : à partir de $(2,3)$, on obtient $(12,17)$, puis $(70,99)$ etc... car $12 = (3\times 2)+(2\times 3)$, $17 = (4\times 2)+(3\times 3)$, et l'on a bien $17^2 - (2\times 12^2) = 1$, et ainsi de suite... On pourrait montrer qu'on atteint ainsi toutes les solutions de l'équation diophantienne, mais ce n'est pas demandé.

Solution de l'exercice 4 En développant le membre de gauche, on a : $3x^3 + 9x^2 + 15x + 9 = (x+3)^3$. Il en résulte que $x+3$ est divisible par 3, donc x également, et on peut poser : $x = 3t$, ce qui nous conduit à : $81t^3 + 81t^2 + 45x + 9 = 27\left(t^3 + 3t^2 + 3t + 1\right)$ soit, après simplifications : $3t^3 - 2t - 1 = 0$. 1 est racine évidente, et on peut factoriser : $3t^3 - 2t - 1 = (t-1)\left(3t^2 + 3t + 1\right)$. Le terme $3t^2 + 3t + 1$ étant toujours strictement positif, cette équation admet pour unique racine (entière ou non) : $t = 1$, donc l'équation initiale admet pour unique racine, a fortiori pour unique racine entière : $x = 3$. La relation ; $3^3 + 4^3 + 5^3 = 6^3$ est classique.

- Rappel sur les congruences-

Deux entiers a et b sont congrus modulo n : $a \equiv b \pmod{n}$ si leur différence est divisible par n. C'est une relation d'équivalence, permettant de répartir tous les entiers en n classes de congruences : ceux de la forme nk, $nk+1$, ... $nk+(n-1)$. Ces classes se manipulent presque comme des nombres, avec des propriétés supplémentaires, notamment le (petit) théorème de Fermat : si p est un nombre premier et a un entier non divisible par p, $a^{p-1} \equiv 1 \pmod{p}$. Ceci se démontre en remarquant que modulo p, a, $2a$, ... $(p-1)a$ sont chacun dans une classe différente, donc $a \times 2a \times ... \times (p-1)a \equiv 1 \times 2 \times ... \times (p-1)$ (car à gauche et à droite, on retrouve toutes les classes non nulles modulo p), ce qui se simplifie.

Exercice 5 Montrer que, modulo 13, x^3 ne peut prendre que 5 valeurs distinctes.

Existe-t-il des couples (x, y) d'entiers tels que $x^4 + 6 = y^3$?

Exercice 6 Montrer que l'équation : $4xy - x - y = z^2$ n'admet pas de solutions entières strictement positives, mais qu'elle admet une infinité de solutions dans $\mathbb{Z}$.

Exercice 7 Trouver tous les couples d'entiers positifs (x, y) tels que $7^x - 3.2^y = 1$

<u>*Solution de l'exercice 5*</u> Pour trouver toutes les valeurs possibles de x^3 modulo 13, il suffit de faire le calcul pour $0, 1, ...12$ car au delà, si $a \equiv b \pmod{13}$, $a^3 \equiv b^3 \pmod{13}$. On fait un tableau :

$x \mod 12$	$x^3 \mod 13$	$x^4 \mod 13$
0	0	0
1	1	1
2	8	3
3	1	3
4	12	9
5	8	1
6	8	9
7	5	9
8	5	1
9	1	9
10	12	3
11	5	3
12	12	1

Les valeurs 1, 5 et 8 12 sont chacune prises trois fois : un cube est obligatoirement congru à 0, 1, 5 ou 12 modulo 13, et de même x^4 est obligatoirement congru à 0, 1, 3 ou 9 modulo 13, les valeurs 1, 3 et 9 étant chacune prises quatre fois. Ceci n'est pas une coïncidence : d'après le théorème de Fermat, tout a non multiple de 13 vérifie : $a^{12} \equiv 1 \pmod{13}$, or $12 = 3 \times 4$, donc par $a^3 \equiv b \pmod{13}$ entraine $b^4 \equiv a^{12} \equiv 1 \pmod{13}$ tout comme $a^4 \equiv b \pmod{13}$ entraine $b^3 \equiv a^{12} \equiv 1 \pmod{13}$.

Toujours est-il que $x^4 + 6$ est nécessairement congru, modulo 13, à 6, 7, 9 ou 2, et un cube ne peut pas être congru à l'une de ces valeurs, donc x^4+6 ne peut pas être un cube.

<u>*Solution de l'exercice 6*</u> Il faut d'abord transformer l'équation avant de pouvoir dire quelque chose : dans le membre de gauche, on remarque le début d'un produit du type $a(x-b)(y-c) = axy - acx - aby + abc$. En comparant terme à terme, on trouve $a = 4$, $c = \frac{1}{4}$, $b = \frac{1}{4}$, mais il faut ôter le terme constant $abc = \frac{1}{4}$. Autrement dit, $4xy - x - y = 4\left(x - \frac{1}{4}\right)\left(y - \frac{1}{4}\right) - \frac{1}{4} = z^2 - \frac{1}{4}$. Ou encore, en multipliant par 4 : $(4x-1)(4y-1) = 4z^2 + 1$.

Les deux termes $(4x-1)$ et $(4y-1)$ du produit de gauche sont tous deux congru à 3 modulo 4, et c'est cela qui pose problème. En effet, un entier positif congru à 3 modulo 4 possède nécessairement au moins un facteur premier congru à 3 modulo 4, puisque un nombre impair a tous ses facteurs premiers impairs, donc congrus à 1 ou 3 modulo 4, et un produit de nombres tous congrus à 1 modulo 4 est nécessairement lui-même congru à 1 modulo 4. Soit p un facteur premier de $4x-1$ congru à 3 modulo 4 : $p = 4k+3$. Dire que p divise $4z^2+1$ revient à dire que $4z^2 \equiv -1 \pmod{p}$. Donc $\left(4z^2\right)^{2k+1} \equiv (-1)^{2k+1} \equiv -1 \pmod{p}$. C'est impossible, car $\left(4z^2\right)^{2k+1} = (2z)^{2(2k+1)} = (2z)^{p-1} \equiv 1 \pmod{p}$, d'après le théorème de Fermat, et hormis pour $p = 2$, on ne peut pas avoir $-1 \equiv 1 \pmod{p}$. Ceci suffit à prouver que l'équation diophantienne n'admet pas de solution strictement positive.

En revanche, mis à part la solution triviale : $x = y = z = 0$, il existe des solutions négatives. En effet, si l'on choisit par exemple $x = -1$, l'équation devient : $-5y + 1 = z^2$. Il suffit de choisir par exemple $z = 5k+1$, soit $z^2 = 25k^2 + 10k + 1$ pour voir que l'équation est vérifiée avec $y = -5k-2$. Quel que soit k, $(-1, -5k-2, 5k+1)$ est solution de l'équation diophantienne.

<u>*Solution de l'exercice 7*</u> L'équation possède une première solution assez évidente : $x = y = 1$, manifestement la seule solution pour $y = 1$. L'énoncé n'exclut pas la possibilité que y soit nul, mais pour $y = 0$, il est clair qu'on ne peut pas

avoir $7^x = 4$. Supposons maintenant $y \geqslant 2$: 3.2^y est divisible par $3.2^2 = 12$, donc une condition nécessaire pour que l'équation soit vérifiée est que $7^x \equiv 1 \pmod{12}$. Modulo 12, 7^x ne prend que deux valeurs : 7 lorsque x est impair, 1 lorsque x est pair. Donc pour $y \geqslant 2$, toute solution (x, y) vérifie nécessairement : x pair. Or si $x = 2k$, l'équation s'écrit : $3.2^y = 7^{2k} - 1 = \left(7^k + 1\right)\left(7^k - 1\right)$. Le facteur 3 divise nécessairement $7^k - 1$ car $7 \equiv 1 \pmod 3$, donc pour tout k, $7^k \equiv 1 \pmod 3$. Donc $7^k - 1 = 3.2^z$ et $7^k + 1 = 2^{y-z}$. A priori, on ne connait pas z, mais pour que $7^k + 1 = 2^{y-z} > 3.2^z = 7^k - 1$, il faut que $y - z > z$. Dès lors, $2^{y-z} - 3.2^z = \left(7^k + 1\right) - \left(7^k - 1\right) = 2$ est nécessairement divisible par 2^z, ce qui entraîne $z = 1$ ou $z = 0$, soit $7^k - 1 = 6$ ou $7^k - 1 = 3$. Seule la possibilité première fournit une solution : $k = 1$ donc $x = 2$ et $y = 4$. L'équation diophantienne admet donc en tout deux solutions : $(1, 1)$ et $(2, 4)$.