DOMAINE : Arithmétique
NIVEAU : Avancé
CONTENU : Exercices

AUTEUR : François LO JACOMO
STAGE : Montpellier 2012

Equations diophantiennes

Exercice 1

On considère deux réels non tous deux nuls a et b vérifiant :

$$a^2b^2(a^2b^2+4) = 2(a^6+b^6)$$

Montrer qu'ils ne sont pas simultanément rationnels.

Solution de l'exercice 1

En ramenant tous les termes dans le membre de gauche : $a^4b^4+4a^2b^2-2a^6-2b^6 = 0$ on découvre une possibilité de factorisation : $(a^4-2b^2)(b^4-2a^2) = 0$. Sous cette forme, l'équation est vérifiée si et seulement si : $a^4 = 2b^2$, soit $a^2 = \pm b\sqrt{2}$ ou $b^4 = 2b^2$, soit $b^2 = \pm a\sqrt{2}$. Dans le premier cas, si b est rationnel, comme $\sqrt{2}$ est irrationnel, a est irrationnel. De même dans le second cas.

Exercice 2

Montrer qu'il existe une infinité de quadruplets (x, y, z, t) d'entiers strictement positifs premiers entre eux dans leur ensemble (c'est-à-dire sans facteur commun aux quatre entiers) et tels que :

$$x^3+y^3+z^2 = t^4$$

Solution de l'exercice 2

On peut supposer que $z = u^2$, donc se ramener à : $x^3+y^3 = t^4-u^4$, et même imposer à t et u d'être de même parité afin de pouvoir poser : $t = a+b, u = a-b$. $(a+b)^4-(a-b)^4 = 8a^3b+8b^3a$, et il suffit que a et b soient des cubes pour que l'on y voie la somme de cubes cherchée. Si $a = r^3$ et $b = s^3$, $x = 2r^3s$ et $y = 2s^3r$, $t = r^3+s^3$ et $u = r^3-s^3$, donc $z = \left(r^3-s^3\right)^2$. Pour que ces quatre nombres soient premiers entre eux dans leur ensemble, il suffit que r et s soient premiers entre eux et de parités distinctes.

Exercice 3

Trouver tous les couples de nombres premiers p et q tels que

$$(p-q)^3 = p+q$$

.

Solution de l'exercice 3

$(p-q)\left((p-q)^2-1\right) = 2q$. Comme p et q sont premiers, ils sont premiers entre eux, donc $p-q$ et q sont eux aussi premiers entre eux, d'où l'on déduit que $p-q$ divise 2. $p-q=1$ entraînerait $q=0$, ce qui est absurde : reste $p-q=2$, $q=3$ donc $p=5$, qui est effectivement solution.

Exercice 4

Trouver tous les triplets d'entiers (x,y,z) tels que :

$$5x^2 - 14y^2 = 11z^2$$

Solution de l'exercice 4

Soit (x,y,z) la plus petite solution (x,y,z non tous nuls). Modulo 7, $-2x^2 \equiv 4z^2$ donc $x^2 \equiv -2z^2$. Mais -2 n'est pas résidu quadratique modulo 7 : cette congruence n'est possible que si z, donc également x, sont multiples de 7, auquel cas $14y^2 = 5x^2 - 11z^2$ est divisible par 49, ce qui entraîne que y lui aussi est multiple de 7. (x,y,z) n'est donc pas la solution minimale car $\left(\frac{x}{7}, \frac{y}{7}, \frac{y}{7}\right)$ est encore solution, d'où le résultat par descente infinie.

Exercice 5

Déterminer tous les nombres premiers p tels qu'il existe n, x, y entiers strictement positifs vérifiant :

$$p^n = x^3 + y^3$$

Solution de l'exercice 5

$p=2$ convient, car $2^1 = 1^3+1^3$, et $p=3$ également, car $3^2 = 1^3+2^3$. Supposons $p \geqslant 5$, et considérons une solution minimale (telle qu'il n'existe pas de solution avec n plus petit). $p^n = (x+y)(x^2-xy+y^2)$, avec $x+y \geqslant 3$ et $x^2-xy+y^2 \geqslant xy \geqslant 2$. En effet, si x et y étaient tous deux égaux à 1, $x^3+y^3 = 2 < p$. Comme un diviseur de p^n autre que 1 est nécessairement multiple de p, p divise (x^2-xy+y^2) et p divise $x+y$, donc $x^2+2xy+y^2 = (x+y)^2$, donc également $3xy$. p est premier avec 3, donc p divise x ou y, mais p divise $x+y$: il divise chacun des deux. On peut ainsi trouver une solution plus petite que

la nôtre : $\left(n-3, \frac{x}{p}, \frac{y}{p}\right)$, ce qui contredit l'hypothèse qu'elle est minimale. D'où le résultat, par descente infinie.

Exercice 6

Soit p un nombre premier congru à 3 modulo 4. Montrer que l'équation :

$$(p+2)x^2 - (p+1)y^2 + px + (p+2)y = 1$$

admet une infinité de solutions, et que pour toute solution (x, y), p divise x.

Solution de l'exercice 6

Il faut dissocier la partie principale de l'équation : $(p+2)x^2 - (p+1)y^2$ des autres termes que l'on doit s'efforcer de réduire au maximum. Pour ce faire, posons : $y = z+1$. L'équation devient : $(p+2)x^2-(p+1)z^2+p(x-z) = 0$, soit : $x^2 = (z-x)((p+1)(z+x)+p)$. Si les deux termes $z-x$ et $(p+1)(z+x)+p$ étaient premiers entre eux, leur produit étant un carré, ils seraient tous deux des carrés, ce qui n'est pas possible car $p \equiv 3 \pmod 4$ entraîne $(p+1)(z+x)+p \equiv 3 \pmod 4$. Donc leur PGCD d est strictement supérieur à 1. d divise manifestement x, il divise $z-x$ donc également z et $z+x$: en définitive il divise p, et comme il est strictement supérieur à 1, $d = p$. D'où le premier résultat que x est divisible par p.

Divisons chaque terme par p : posons $x = px', z = pz'$, l'équation devient : $x'^2 = (z'-x')((p+1)(z'+x')+1)$, mais cette fois-ci, les deux facteurs $z'-x'$ et $(p+1)(z'+x')+1$ sont premiers entre eux, tous deux sont des carrés parfaits : $z'-x' = u^2, (p+1)(z'+x')+1 = v^2, x' = uv$. En définitive : $(p+1)(u^2+2uv)+1 = v^2$, ou encore : $(p+2)v^2-(p+1)(u+v)^2 = 1$. Nous avons là une équation de Pell-Fermat, qui admet une infinité de solutions. En effet, on prouve aisément par récurrence qu'il existe deux suites d'entiers (v_k) et (w_k) telles que $\left(\sqrt{p+2}+\sqrt{p+1}\right)^{2k+1} = v_k\sqrt{p+2}+w_k\sqrt{p+1}$ et $\left(\sqrt{p+2}-\sqrt{p+1}\right)^{2k+1} = v_k\sqrt{p+2}-w_k\sqrt{p+1}$. En faisant le produit de ces deux termes, on trouve bien pour tout k : $1 = v_k^2(p+2)-w_k^2(p+1)$, donc pour tout entier k on détermine ainsi une solution : $v = v_k, u = w_k - v_k$ de l'équation cherchée, d'où l'on remonte à x', z', x, z et y.

- À propos de la divisibilité -

Pour conclure ce cours d'arithmétique avancée, je voudrais présenter une propriété spectaculaire de la divisibilité des entiers algébriques.

On vous a introduit les entiers de Gauss $\mathbb{Z}[i]$, nombres de la forme $a + bi$ avec a et b entiers relatifs. Dans cet anneau, il existe une division euclidienne, et il en résulte les mêmes propriétés de la divisibilité que dans $\mathbb{Z}$: théorème de Gauss, relation de Bézout, unicité de la décomposition en facteurs premiers (aux éléments inversibles près, en l'occurrence $\{1, -1, i, -i\}$). On démontre ainsi que tout nombre premier (de $\mathbb{N}$) congru à 1 modulo 4 se décompose d'une et d'une seule manière en somme de carrés. En effet, comme -1 est résidu quadratique (car $(-1)^{\frac{p-1}{2}} = 1$: tout résidu quadratique u^2 vérifie nécessairement $\left(u^2\right)^{\frac{p-1}{2}} \equiv u^{p-1} \equiv 1 \pmod{p}$, or il y a autant de résidus quadratiques que de racines de cette équation), p divise un entier de la forme $n^2 + 1 = (n + i)(n - i)$. Or p ne divise ni $n + i$ ni $n - i$: s'il était premier dans l'ensemble des entiers de Gauss, cela contredirait le théorème de Gauss. Il possède donc des diviseurs, et en séparant chaque diviseur de son conjugué on peut écrire : $p = (a + ib)(a - ib) = a^2 + b^2$. L'unicité provient du fait que si $p = a^2 + b^2 = a'^2 + b'^2$, $a + bi$ ne peut pas être premier simultanément avec $a' + b'i$ et $a' - b'i$, en vertu du théorème de Gauss. Il possède au moins un facteur $c + di$ en commun avec l'un de ces nombres, et $c^2 + d^2$ divise p.

Mais toutes ces propriétés résultent de l'égalité de division euclidienne dans $\mathbb{Z}[i]$: si $a + bi$ et $c + di$ sont deux entiers de Gauss, $c + di$ non nul, il existe $p + qi$ et $r + si$ tels que : $a + bi = (c + di)(p + qi) + (r + si)$ et $|r + si| < |c + di|$, cette dernière inégalité étant fondamentale car c'est elle qui permet à l'algorithme d'Euclide de prendre fin. Ceci revient à dire que dans le corps des $\alpha + \beta i$ avec α et β rationnels, il existe un entier $p + qi$ dont la distance à $\frac{a+bi}{c+di}$ est strictement inférieure à 1. Et cette dernière relation est assez claire : tout point du plan est à une distance strictement inférieure à 1 d'un point à coordonnées entières. Les points du type $\left(a + \frac{1}{2}\right) + \left(b + \frac{1}{2}\right) i$, les plus éloignés des points entiers, sont à une distance $\frac{\sqrt{2}}{2}$. La même propriété vaut pour l'anneau $\mathbb{Z}[i\sqrt{2}]$ des nombres de la forme $a + bi\sqrt{2}$ avec a et b entiers relatifs, car les mailles de ce réseau d'entiers sont des rectangles $1 \times \sqrt{2}$ dont la diagonale $\sqrt{3}$ est encore strictement inférieure à 2.

Mais cela ne vaut plus pour l'ensemble $\mathbb{Z}[i\sqrt{5}]$ des entiers de la forme $a + bi\sqrt{5}$: la diagonale des mailles du réseau vaut alors $\sqrt{6} > 2$, il n'y a donc ni division euclidienne ni les propriétés qui s'ensuivent. En particulier, il n'y a pas d'unicité de décomposition en facteurs premiers : $\left(1 + i\sqrt{5}\right) \times \left(1 - i\sqrt{5}\right) = 6 = 2 \times 3$. Or dans cet anneau, $1 + i\sqrt{5}$ n'a de diviseur commun ni avec 2 ni avec 3. Pour contourner cette difficulté, Richard Dedekind introduisit des "idéaux" :

en quelque sorte il créait un PGCD de $1+i\sqrt{5}$ et 2. Plus précisément, un idéal est l'ensemble des combinaisons linéaires de deux ou plusieurs éléments, à coefficients dans l'anneau en question. L'idéal peut être principal : l'ensemble des multiples d'un élément donné, mais il peut être engendré par deux ou plusieurs éléments. Ainsi, dans $\mathbb{Z}[i\sqrt{5}]$, l'idéal $[2, 1+i\sqrt{5}]$ n'est pas principal, ses éléments ne sont pas les multiples d'un élément donné, en particulier ils ne couvrent pas tout l'anneau bien que les deux entiers 2 et $1+i\sqrt{5}$ n'aient pas de diviseur commun. On peut multiplier les idéaux : cela revient à multiplier chaque générateur du premier idéal par chaque générateur du deuxième idéal, ce qui engendre l'idéal produit (ensemble des combinaisons linéaires de ces produits de générateurs). Et dans le cas d'anneaux d'entiers algébriques, on retrouve sur les idéaux des propriétés comparables à celles de la divisibilité des entiers relatifs, à savoir l'unicité de décomposition en idéaux et la notion d'idéal premier.

Un entier algébrique est, de manière très générale, un nombre complexe racine d'une équation à coefficients entiers relatifs, dont le premier coefficient est égal à 1. C'est ce premier coefficient (coefficient du terme de plus haut degré) qui caractérise le fait que c'est un entier. $x = \frac{1}{\sqrt{2}}$ n'est pas entier car il est racine de $2x^2-1=0$, avec un premier coefficient 2. En revanche, $j = \frac{-1+i\sqrt{3}}{2}$ est entier car il est racine de $x^2+x+1=0$, avec premier coefficient 1. Et ces entiers algébriques possèdent une propriété remarquable : deux entiers algébriques quelconques x et y possèdent toujours un PGCD d pour lequel on peut écrire la relation de Bézout : d divise x et d divise y et il existe deux entiers algébriques u et v tels que $d = xu + yv$. Pourtant, dans cet ensemble de tous les entiers algébriques, il n'existe pas de facteurs premiers : la racine carrée d'un entier algébrique est encore un entier algébrique (si l'on remplace x par x^2 dans l'équation), donc il n'existe pas d'entier algébrique qui n'ait aucun diviseur hormis lui-même et les unités (les entiers inversibles, comme $\frac{-1+i\sqrt{3}}{2}$).

Quel est le PGCD de $1+i\sqrt{5}$ et 2, par exemple ? C'est $\sqrt{2}$! Cela peut sembler étonnant, mais la démonstration donne une idée de la démonstration générale du théorème énoncé ci-dessus. Considérons les puissances de l'idéal $[2, 1+i\sqrt{5}]$. Un théorème dit qu'une des puissances d'un tel idéal est principale : en l'occurrence, le carré de cet idéal est l'idéal engendré par 2. En effet, les produits des générateurs : $2\times2, 2\times\left(1+i\sqrt{5}\right)$ et $\left(1+i\sqrt{5}\right)\times\left(1+i\sqrt{5}\right)$ sont tous trois divisibles par 2, et 2 est combinaison linéaire de ces trois générateurs ($2 = \left(1+i\sqrt{5}\right)\left(1+i\sqrt{5}\right) - 2\left(1+i\sqrt{5}\right) + 4\times2$), donc il appartient à l'idéal. Con-

struisons alors un nouvel ensemble d'entiers algébriques : $\mathbb{Z}[i\sqrt{5}, \sqrt{2}]$. Attention ! il s'agit de l'ensemble de tous les entiers algébriques qui s'écrivent sous forme $\alpha + \beta i\sqrt{5} + \gamma\sqrt{2} + \delta\left(i\sqrt{5})(\sqrt{2}\right)$ avec $\alpha, \beta, \gamma, \delta$ pas nécessairement entiers, mais rationnels ($\in \mathbb{Q}$). Il contient par exemple $\frac{1+i\sqrt{5}}{\sqrt{2}} = \frac{1}{2}\sqrt{2} + \frac{1}{2}\left(i\sqrt{5}\right)\sqrt{2}$ car $z = \frac{1+i\sqrt{5}}{\sqrt{2}}$ est un entier algébrique : $z^2 = -2 + i\sqrt{5}$ donc $z^4 + 4z^2 + 9 = 0$. Dans ce nouvel ensemble, l'idéal principal engendré par 2 est toujours le carré de l'idéal engendré par 2 et $1 + i\sqrt{5}$, mais c'est aussi le carré de l'idéal engendré par $\sqrt{2}$. Et étant donné l'unicité de décomposition en produit d'idéaux, ces deux idéaux sont obligatoirement égaux. Ce qui signifie que $\sqrt{2}$ divise chacun des générateurs 2 et $1 + i\sqrt{5}$ et qu'il s'écrit comme combinaison linéaire de ces deux générateurs, à coefficients dans cet anneau. En l'occurrence : $\sqrt{2} = \left(\frac{1-i\sqrt{5}}{\sqrt{2}}\right)\left(1 + i\sqrt{5}\right) - \left(\sqrt{2}\right)2$: c'est manifestement une relation de Bézout. Et ceci vaut pour deux entiers algébriques quelconques !