La géométrie arithmétique : Une tentative de vulgarisation

David A. Madore

7 juillet 2004

Avant-propos

Le but — peut-être assez farfelu — de ce texte est de donner un aperçu, pour des personnes dont les connaissances mathématiques s'arrêtent, en gros, au baccalauréat (mais certaines parties du texte pourront aller plus ou moins loin), de ce qu'est la géométrie arithmétique et de ce que sont les méthodes modernes pour étudier les équations diophantiennes. Notamment, il s'agit de tenter de donner une idée de ce que peut signifier l'affirmation (*a priori* complètement byzantine) suivante :

> Sur une variété (sur un corps de nombres) projective, lisse, (géométriquement) rationnellement connexe, l'obstruction de Brauer-Manin au principe de Hasse est la seule pour l'existence d'un point rationnel.

Il s'agit d'une conjecture due (notamment) à Jean-Louis Colliot-Thélène, et qu'on est encore très loin de savoir prouver, sauf dans des cas particuliers. Évidemment, il ne s'agit pas d'expliquer ce que signifie chacun de ces mots, ni quel est le sens *exact* de cette affirmation. En attendant, il nous faut montrer un certain nombre d'exemples pour amener les différentes situations qui peuvent se présenter.

Il manque dans cette version du texte beaucoup de figures explicatives qui rendraient beaucoup plus clairs certains passages. Je ne sais pas si j'aurai la patience de les faire.

1 Le problème des triplets pythagoriciens

1.1 Introduction

Commençons par une observation très simple. Prenons une feuille de papier quadrillé (par des carrés réguliers), et marquons un point du quadrillage comme origine. Traçons un cercle dont le centre est ce point choisi comme origine et dont le rayon est cinq fois le côté d'un carreau (par exemple, 2.5 cm s'il s'agit d'un papier « petits carreaux », ou 4 cm s'il s'agit d'un papier d'écolier dont les carreaux font 0.8 cm de côté). Ce cercle passe par précisément douze points du quadrillage : les points (dont les coordonnées peuvent se noter $(5,0)$, $(0,5)$, $(-5,0)$ et $(0,-5)$) situés à cinq unités de distance de l'origine dans les quatre directions principales du quadrillage (droite, haut, gauche, bas), mais aussi huit autres points dont les coordonnées sont $(4,3)$ (c'est-à-dire quatre carreaux vers la droite et trois vers le haut à partir de l'origine), $(3,4)$, $(-3,4)$, $(-4,3)$, $(-4,-3)$, $(-3,-4)$, $(3,-4)$ et $(-4,3)$ (en tournant sur le cercle dans le sens contraire des aiguilles d'une montre).

La raison de la présence de ces points sur le cercle est simplement le théorème de Pythagore ; considérons par exemple le triangle rectangle dont les sommets sont les points de coordonnées respectivement $A = (0,0)$ (l'origine), $C = (4,0)$ (point où se trouve l'angle droit) et $B = (4,3)$: sa base est de longueur $b = AC = 4$, sa hauteur de longueur $a = BC = 3$ et le théorème de Pythagore assure que son hypoténuse $c = AB$ doit alors vérifier $c^2 = a^2 + b^2$ (« le carré de la longueur de l'hypoténuse d'un triangle rectangle est égal à la somme des carrés des longueurs des deux autres côtés »), donc $c^2 = 3^2 + 4^3 = 9 + 16 = 25$, ce qui donne $c = 5$, autrement dit la longueur AB vaut cinq unités, et comme A est le centre du cercle considéré dont le rayon est cinq, le point $B = (4,3)$ est bien situé sur ce cercle.

1.2 Définition ; triplets primitifs

De façon générale, lorsqu'on trouve trois entiers a, b, c (qui ne sont pas tous les trois égaux à zéro) tels que $c^2 = a^2 + b^2$, ou, ce qui revient au même, un point (b, a) de coordonnées entières sur le cercle (de centre l'origine) de rayon c entier, on dit qu'on a trouvé un *triplet pythagoricien*. Comme on vient de le voir, cela revient à trouver un triangle équilatéral dont les trois côtés ont des longueurs entières (on parle de « triplet pythagoricien » à cause du théorème de Pythagore, bien entendu, mais de telles figures étaient déjà

connues des Babyloniens qui s'en servaient pour former des angles droits — par exemple, si on forme treize nœuds à distance égale les uns des autres sur une ficelle, qu'on rassemble et relie le premier et le dernier et qu'on prend les nœuds séparés de 3, 4 puis 5 intervalles sur la ficelle, on obtient en la tendant un triangle rectangle).

Ainsi, les trois nombres $3, 4, 5$ forment un triplet pythagoricien. Il en existe d'autres : évidemment, on peut toujours permuter les deux premiers nombres, ou ajouter des signes moins comme on veut — on peut encore multiplier tous les nombres par un même entier (par exemple par 2, cela donne $6, 8, 10$, ou par 3 cela donne $9, 12, 15$, qui sont encore des triplets pythagoriciens) ; mais il existe aussi des triplets « vraiment » différents de $3, 4, 5$, comme $5, 12, 13$ (qui donne donc un (des) point(s) entiers sur un cercle de rayon 13) ou $8, 15, 17$. On dira qu'un triplet pythagoricien est *réduit*, ou *primitif* lorsque les trois entiers qui le constituent ne sont pas multiples d'un entier commun (autre que 1 ou -1) — on dit encore que les trois nombres sont premiers dans leur ensemble ; c'est-à-dire qu'un triplet pythagoricien primitif est un triplet qui ne s'obtient pas en multipliant simplement un triplet plus petit par un certain nombre (ainsi, $6, 8, 10$ ou $9, 12, 15$ ne sont pas primitifs car ce sont simplement le double et le triple de $3, 4, 5$; en revanche, $5, 12, 13$ et $8, 15, 17$, eux, sont bien primitifs).

1.3 Équations homogène et inhomogène

On a dit que trois nombres entiers X, Y, Z forment un triplet pythagoricien lorsqu'ils vérifient l'équation $X^2 + Y^2 = Z^2$. Considérons maintenant les quantités $x = \frac{X}{Z}$ et $y = \frac{Y}{Z}$: ce sont des nombres rationnels (c'est-à-dire les quotients de deux entiers : des fractions dont le numérateur et le dénominateur sont des entiers), et ils vérifient $x^2 + y^2 = 1$ (on a divisé par Z^2 l'équation précédente). Ceci signifie que le point de coordonnées (x, y) (cette fois-ci il ne s'agit plus de coordonnées entières, mais rationnelles) est situé sur le cercle unité (le cercle dont le centre est l'origine et dont le rayon est une unité). Par exemple, $(\frac{3}{5}, \frac{4}{5})$ est sur ce cercle, car $(\frac{3}{5})^2 + (\frac{4}{5})^2 = 1$, qui correspond au triplet pythagoricien $3, 4, 5$ (avec $3^2 + 4^2 = 5^2$) déjà mainte fois remarqué. Si on part, réciproquement, d'une solution de l'équation $x^2 + y^2 = 1$ où x et y sont rationnels, alors en appelant Z leur plus petit dénominateur commun, et X et Y les numérateurs de x et y sur ce dénominateur, on trouve un triplet pythagoricien X, Y, Z, et il est de plus primitif (sans quoi Z ne serait pas le plus petit dénominateur commun), et tout triplet multiple de ce triplet

primitif (par exemple $2X, 2Y, 2Z$ ou $3X, 3Y, 3Z$) correspond au même point rationnel (x, y) sur le cercle unité. Il y a donc *équivalence* entre chercher les triplets pythagoriciens primitifs et chercher les solutions rationnelles (x, y) de l'équation $x^2 + y^2 = 1$, c'est-à-dire les points rationnels (i.e., à coordonnées rationnelles) sur le cercle unité.

On dira que $x^2 + y^2 = 1$ est l'équation *inhomogène*, ou *affine*, du cercle unité. Lorsqu'on considère une telle équation, on en recherche les solutions rationnelles. L'équation $X^2+Y^2 = Z^2$, elle, est dite *homogène* ou *projective* (le mot « homogène » fait référence au fait que tous les termes de l'équations ont le même degré total, c'est-à-dire la somme des exposants dans les différentes variables, soit 2 ici, ce qui permet précisément de multiplier une solution — non nulle — par un nombre — non nul — pour obtenir une solution différente, et donc de parler de solutions primitives). Pour une telle équation, on considérera les solutions entières primitives (donc, sans diviseur commun). Remarquons au passage qu'il y avait plusieurs façons de rendre inhomogène l'équation homogène $X^2+Y^2 = Z^2$: une autre consistait à écrire $u^2+1 = v^2$, où $u = \frac{X}{Y}$ et $v = \frac{Z}{Y}$ — dans ce cas, on cherche des points rationnels non sur le cercle unité mais sur la courbe (qui se trouve être une hyperbole) d'équation $u^2 + 1 = v^2$, c'est-à-dire que $X^2 + Y^2 = Z^2$ peut s'interpréter aussi bien comme l'équation projective de l'une ou de l'autre (en clair, il n'y a pas de différence importante, du point de vue de la géométrie arithmétique, entre le cercle d'équation $x^2 + y^2 = 1$ et l'hyperbole d'équation $u^2 + 1 = v^2$, trouver des points rationnels sur l'une de ces courbes ou en trouver sur l'autre équivaut, dans les deux cas, à trouver des triplets pythagoriciens).

1.4 Paramétrage rationnel du cercle

Reprenons un peu de géométrie plane élémentaire. Soit C le cercle de centre O (l'origine) et de rayon 1. Soit P le point de coordonnées $(-1, 0)$, qui est donc un point de C, et Q de coordonnées $(1, 0)$ son symétrique par rapport à O. Soit D la droite tangente à C passant par P. Considérons un point M, mobile sur D, de coordonnées $(-1, 2t)$ (ce 2 n'a pas de raison particulière d'être, sinon conventionnelle). La droite $\Delta = MQ$ rencontre C en deux points : Q est l'un d'entre eux, appelons N le second de ces points, dont les coordonnées seront notées (x, y). Appliquant le théorème de Thalès aux triangles QMP et QNR (où R, de coordonnées $(x, 0)$, est la projection de N sur l'axe des abscisses), on voit que $QR/NR = QP/MP$, soit $\frac{1-x}{y} = t$, ce qui s'écrit encore $x = 1 - ty$ (c'est l'équation de la droite $\Delta = MQ$, sur laquelle

N est situé). Mais comme N est sur le cercle C d'équation $x^2+y^2=1$, on a $(1-ty)^2+y^2=1$, soit $1-2ty+(1+t^2)y^2=1$, soit encore $-2ty+(1+t^2)y^2=0$, et comme y n'est pas nul (à moins que t lui-même le soit), $-2t+(1+t^2)y=0$, soit enfin $y=\frac{2t}{1+t^2}$, et comme $x=1-ty$ on trouve $x=\frac{1-t^2}{1+t^2}$. Réécrivons ces deux équations, qui donnent donc les coordonnées (x,y) de N en fonction de celles $(-1,2t)$ de M (appelé « projection stéréographique » de N par la projection de centre Q sur la droite D tangente à P en C) :

$$x=\frac{1-t^2}{1+t^2} \quad \text{et} \quad y=\frac{2t}{1+t^2}$$

Quel est l'intérêt de ces équations ? Elles constituent un *paramétrage rationnel* du cercle (unité). Si on insère n'importe quelle valeur de t dans ces deux équations, on trouve deux valeurs x et y telles que le point N de coordonnées (x,y) soit sur le cercle unité C ; et si le t choisi est rationnel, alors ce couple (x,y) est également constitué de nombres rationnels (car on ne fait qu'ajouter, soustraire, multiplier et diviser des nombres rationnels). Or on a expliqué qu'un point rationnel sur le cercle unité revenait à donner un triplet pythagoricien (primitif). Voici donc une machine à produire des triplets pythagoriciens : prendre n'importe quelle valeur rationnelle de t, l'insérer dans les formules ci-dessus, placer x et y sur un dénominateur commun, et lire les numérateurs et le dénominateur comme un triplet pythagoricien. Par exemple, si on prend $t=\frac{2}{3}$, on trouve $x=\frac{5}{13}$ et $y=\frac{12}{13}$, ce qui donne le triplet pythagoricien $5,12,13$. Réciproquement, n'importe quel triplet pythagoricien correspond, on l'a vu, à un point (x,y) sur le cercle unité, et celui-ci à son tour, si on pose $t=\frac{1-x}{y}$ (à l'exception du seul point $Q=(1,0)$), à un point déterminé par le paramétrage rationnel que nous venons d'établir. C'est-à-dire que ce paramétrage donne bien *tous* les triplets pythagoriciens (primitifs).

Une courbe (plane, par exemple) qui peut se paramétrer (à l'exception éventuelle de quelques points de non définition) par des fonctions rationnelles comme nous venons de le faire pour le cercle est dite *rationnelle* ou *unicursale*. Nous venons donc d'expliquer que le cercle est une courbe rationnelle. Il est à signaler que le paramétrage « habituel » du cercle (unité), à savoir

$$x=\cos\theta \quad \text{et} \quad y=\sin\theta$$

(où θ est l'angle orienté mesuré sur le cercle) n'est pas du tout de la même nature, car les fonctions cosinus et sinus sont des fonctions « transcendantes »

(en tout cas, ce ne sont pas des fractions rationnelles). Si on prend des valeurs rationnelles (ou bien même commensurables à π) de l'angle θ, on n'obtient pas des valeurs rationnelles de x et y. Il y a cependant un lien entre les deux paramétrages, c'est que $1/t = \tan\frac{\theta}{2}$ (cela se voit en utilisant la relation entre angle au centre d'un cercle et angle inscrit : si $\theta = \widehat{QON}$, alors $\widehat{NQP} = \frac{\pi}{2} - \theta$), et les formules de x et y sont alors à rapprocher des formules exprimant le cosinus et le sinus en fonction de la tangente de l'angle moitié.

2 Obstructions locales à l'existence d'une solution

2.1 Un exemple (« obstruction 2-adique »)

Considérons à présent l'équation $X^2 = 2Y^2$, dont on cherche des solutions entières (primitives). Autrement dit, on cherche deux entiers X et Y, non tous les deux nuls, et sans facteur commun (autres que 1 et -1), tels que le carré de X soit le double du carré de Y. Posant $x = \frac{X}{Y}$, et en divisant par Y^2 les deux membres de l'équation, on voit que l'on cherche à résoudre $x^2 = 2$ (équation inhomogène associée à $X^2 = 2Y^2$) avec x un nombre rationnel : c'est-à-dire que l'on cherche à savoir si la racine carrée de 2 peut s'écrire comme un rationnel x (dont X serait le numérateur réduit et Y le dénominateur réduit). Le raisonnement classique (dû aux pythagoriciens, semble-t-il) prouvant que cela n'est pas possible est le suivant : X^2 serait alors pair (car c'est le double de Y^2) donc X serait pair (car le carré d'un nombre impair est impair, ce qui montre que X ne peut pas être impair) donc on peut écrire $X = 2X'$, mais alors $X^2 = 4X'^2$, donc $Y^2 = 2X'^2$, donc Y^2 est lui aussi pair, donc Y l'est, donc X et Y ne sont pas sans facteur commun (car ils ont 2 comme facteur commun). Bref, on ne peut pas trouver de solution primitive (c'est-à-dire d'écriture $\frac{X}{Y}$ réduite), et ceci constitue une contradiction. Cela prouve que x vérifiant $x^2 = 2$ ne peut pas être un rationnel (donc que la racine carrée de 2 est irrationnelle).

2.2 Autre exemple (« obstruction 3-adique »)

Considérons maintenant l'équation $X^2 + Y^2 = 3Z^2$, dont on cherche de nouveau à montrer qu'elle n'a pas de solution entière X, Y, Z autre que la

solution (« triviale ») $0, 0, 0$. Imaginons pour cela qu'on ait trouvé une solution primitive X, Y, Z de l'équation. Remarquons maintenant que le reste de la division par 3 d'un carré parfait (X^2, ou Y^2, notamment) ne peut jamais être 2 : il ne peut être que 0 (lorsque le nombre élevé au carré est multiple de 3, donc il l'est encore après élévation au carré) ou 1 (lorsque le nombre élevé au carré n'est pas multiple de 3). Or ici $X^2 + Y^2$ est censé être un multiple de 3, ce qui n'est donc possible que si X^2 et Y^2 le sont tous les deux (sinon, le reste de la division par 3 de $X^2 + Y^2$ serait $0 + 1 = 1$, $1 + 0 = 1$ ou $1 + 1 = 2$). Bref, X^2 et Y^2, donc X et Y eux-mêmes, sont multiples de 3, disons $X = 3X'$ et $Y = 3Y'$. Mais alors $X^2 = 9X'^2$ et $Y^2 = 9Y'^2$ donc $Z^2 = 3(X'^2 + Y'^2)$ ce qui prouve que Z^2 est multiple de 3, donc Z aussi. Donc finalement X, Y, Z sont tous multiples de 3, et comme précédemment cela constitue une contradiction. Ceci prouve que l'équation $x^2 + y^2 = 3$ n'a pas de solution rationnelle, c'est-à-dire que le cercle (centré à l'origine) de rayon $\sqrt{3}$ ne passe par *aucun* point rationnel du plan (ce qui est notamment plus fort que d'affirmer que $\sqrt{3}$ est irrationnelle).