

Résolution d'une équation diophantienne

Pierre Lissy

May 11, 2010

Résolution de $x^2 + y^2 = z^2$. Remarquons que tous les nombres de la forme $x = d(u^2 - v^2)$, $y = 2duv$, $z = d(u^2 + v^2)$ avec u et v premiers entre eux conviennent. En effet, $x^2 + y^2 = d^2(u^4 + v^4 - 2d^2u^2v^2 + 4d^2u^2v^2) = (d(u^2 + v^2))^2$. D'abord, remarquons qu'on peut exclure le cas $0, 0, 0$. Ensuite, on peut se restreindre aux solutions dites premières: on suppose x, y, z premiers entre eux dans leur ensemble, car si ils ont un diviseur commun d , on a $dx' = x, dy' = y, dz' = z$ et donc $x'^2 + y'^2 = z'^2$. Une fois qu'on a les solutions premières on multiplie par un d quelconque.

En fait, si l'on suppose x, y, z premiers entre eux dans leur ensemble, ils le sont deux à deux. En effet, la relation précédente que si x et y ne sont pas premiers entre eux alors le diviseur commun divise aussi z (d^2 divise z^2 et donc d divise z car une racine est rationnelle ssi elle est entière). Ils sont donc notamment pas tous pairs. Ils sont aussi pas tous impairs (si x et y sont impairs leur carrés aussi mais alors la somme qui vaut z^2 est paire, donc z est paire, idem pour les autres combinaisons). Ainsi, quitte à permuter x et y on peut supposer x impair, y pair et z impair. Posons $X = x/z, Y = y/z$, alors $X^2 + Y^2 = 1$ avec X et Y rationnels. Cette forme réduite est unique car x, y et z sont premiers entre eux deux à deux. On cherche donc les points rationnels sur le quart en haut à droite du cercle trigonométrique. On paramètre ce cercle de la manière suivante: $\cos(\theta) = (1 - t^2)/(1 + t^2)$ et $\sin(\theta) = 2t/(1 + t^2)$. Si t est rationnel, alors X et Y le sont. Inversement, si X et Y sont rationnels, alors $t^2 = (1 - X)/(1 + X)$ est rationnel et donc $t = 1/(2(1 + t^2)Y)$ aussi. Il suffit donc de choisir un t rationnel pour obtenir les solutions du problème réduit. Ecrivons $t = u/v$ avec u et v premiers entre eux. Alors $X = (u^2 - v^2)/(u^2 + v^2)$ et $Y = 2uv/(u^2 + v^2)$. Pour conclure que $x = u^2 - v^2, y = 2uv, z = u^2 + v^2$, il suffit de montrer que ces nombres sont premiers entre eux dans leur ensemble. Considérons un diviseur premier de ses nombres. Alors p divise $(u^2 + v^2) + (u^2 - v^2) = 2u^2$ et $(u^2 + v^2) - (u^2 - v^2) = 2v^2$. Si l'on suppose p différent de 2 c'est que p divise u^2 et v^2 donc p divise u et v (cf valuation qui doit être paire). C'est exclu car u et v sont premiers entre eux. Donc $p = 2$. Alors u et v ont même parité, ce qui implique qu'ils sont impairs. $u = 2k + 1$ et $v = 2n + 1$. Alors $u^2 + v^2 = 2 + 4k + 4k^2 + 4n + 4n^2$, de même $u^2 - v^2 = 4k + 4k^2 - 4n - 4n^2$ et $2uv = 2(2 + 2k + 2n + 4km)$. On simplifie par le facteur commun 2 et on obtient des nombres premiers entre eux d'après le raisonnement précédent. Alors $x = 2k + 2k^2 - 2n - 2n^2$ est pair ce qui est faux par hypothèse. Ainsi les nombres n'ont effectivement pas de diviseurs communs et $x = u^2 - v^2, y = 2uv$ et $z = u^2 + v^2$.