



QUIZZ MATH 2002

<http://www.univ-orleans.fr/quizz/>

Les solutions de $x^2 + y^2 = z^2$.



Ce texte a été rédigé par A. Chambert-Loir, professeur à l'école Polytechnique, comme complément d'information pour le QUIZZ MATH 2002.

La solution générale pour ce problème existe. En effet, on peut démontrer (voir plus bas) que si x, y, z sont trois entiers tels que $x^2 + y^2 = z^2$, alors il existe trois autres entiers a, b, d , où a et b sont sans facteur commun, de sorte que

$$x = d(a^2 - b^2), \quad y = 2abd, \quad z = d(a^2 + b^2). \quad (*)$$

(Il faut éventuellement échanger x et y .) Dans notre cas, on doit avoir $15 = d(a^2 + b^2) = 3 \cdot 5$. On remarque que $a^2 + b^2$ ne peut pas être multiple de 3, si bien que d est multiple de 3, d'où $5 = (d/3)(a^2 + b^2)$. Si $d/3 = 5$, on trouve $a^2 + b^2 = 1$, ce qui nécessite $a = 0$ ou $b = 0$. Donc $d = 3$ et $a^2 + b^2 = 5$. C'est une nouvelle équation en nombres entiers à résoudre, dont une solution est $a = 1, b = 2$ (ou le contraire).

En fait, Fermat savait déjà écrire un nombre premier sous la forme d'une somme de deux carrés, à condition que ce nombre premier soit, ou 2, ou de la forme $4n + 1$. Dans les cas restant, c'est impossible. En général, un entier N est somme de deux carrés si et seulement si ses facteurs premiers de la forme $4n + 3$ apparaissent avec un exposant pair. Au 19^e siècle, Jacobi a d'ailleurs donné une formule pour le nombre d'expressions d'un entier comme somme de deux carrés.

Démontrons maintenant les formules (*) annoncées au début de ce texte. Soient x, y, z trois entiers tels que $x^2 + y^2 = z^2$. Soit d le pgcd de x et y . On écrit $x = dX, y = dY$, où X et Y sont des entiers premiers entre eux, d'où $z^2 = d^2(X^2 + Y^2)$, ce qui implique que d divise z . Posons $Z = z/d$. On a ainsi $X^2 + Y^2 = Z^2$, et X et Y sont des entiers sans facteur commun. On remarque qu'alors, X et Z d'une part, Y et Z d'autre part, sont sans facteur commun.

Le carré d'un entier est ou un multiple de 4, ou un multiple de 4 plus un. La somme de deux carrés est donc un multiple de 4 plus 0, 1 ou 2. En regardant tous les cas possibles, on trouve Z est impair et que l'un des deux entiers X et Y est pair, l'autre étant impair. Supposons que Y soit pair et écrivons $Y^2 = Z^2 - X^2 = (Z - X)(Z + X)$. Le pgcd de $Z - X$ et $Z + X$ divise leur somme $2Z$ et leur différence $2X$, donc divise 2. C'est donc 1 ou 2, mais comme $Z - X$ et $Z + X$ sont tous deux pairs, c'est 2. Les entiers $(Z - X)/2$ et $(Z + X)/2$ sont sans facteur commun et leur produit est égal au carré $(Y/2)^2$. Chacun d'eux est nécessairement un carré. On écrit ainsi $Z - X = 2b^2$, $Z + X = 2a^2$, d'où $Z = a^2 + b^2$, $X = a^2 - b^2$ et $Y = 2ab$. Finalement, $x = d(a^2 - b^2)$, $y = 2abd$ et $z = d(a^2 + b^2)$.

Le cas où X est pair fournit la solution où x et y sont échangés.

Une dernière remarque : si $x^2 + y^2 = z^2$, les formules données ci-dessus impliquent que

$$\frac{x}{z} = \frac{a^2 - b^2}{a^2 + b^2}, \quad \frac{y}{z} = \frac{2ab}{a^2 + b^2},$$

soit en posant $y = b/a$,

$$\frac{x}{z} = \frac{1 - t^2}{1 + t^2}, \quad \frac{y}{z} = \frac{2t}{1 + t^2},$$

ce qui est la paramétrisation du cercle unité par la tangente de l'angle moitié !

Une interprétation de cette paramétrisation est la suivante. Considérons un point $M = (x, y)$ du cercle unité et soit t la pente de la droite joignant le point M au point A de coordonnées $(-1, 0)$. Si M est à coordonnées rationnelles, $t = y/(x + 1)$ est rationnel. Réciproquement, si t est rationnel, la droite de pente t passant par A coupe le cercle en un autre point dont les coordonnées sont justement $x = (1 - t^2)/(1 + t^2)$ et $y = 2t/(1 + t^2)$.

Plus généralement, cette méthode fournit une paramétrisation des points à coordonnées rationnelles d'une conique plane d'équation à coefficients rationnels *pourvu* qu'il existe au moins un tel point.

