Points rationnels d'une conique

Samuel Rochetin

Dimanche 11 mars 2018

Résumé

Le but de ce document est de présenter une méthode de résolution d'une équation diophantienne se ramenant à l'étude des points rationnels d'une conique. Il s'agit d'une introduction élémentaire aux courbes algébriques de genre nul sur un exemple.

1 Équation diophantienne de départ

Nous cherchons à résoudre l'équation diophantienne suivante :

$$2x^2 + 3y^2 = 5z^2, (x, y, z) \in \mathbb{Z}^3 \qquad (*)$$

Notre premier réflexe consiste à chercher des solutions évidentes. Nous trouvons $(0; 0; 0)$ et $(\pm 1; \pm 1; \pm 1)$. Nous constatons que $\forall n \in \mathbb{Z}$, le triplet $n \times (\pm 1; \pm 1; \pm 1)$ est solution. Cela nous conduit à étudier la structure de l'ensemble des solutions.

Autre observation immédiate, si $z = 0$, alors $2x^2 + 3y^2 = 0$ donc $x = y = 0$ car une somme de nombres positifs est nulle si et seulement si chacun de ses termes est nul. La solution triviale $(0; 0; 0)$ est donc un peu à part des autres solutions.

1.1 Structure de l'ensemble des solutions

Nommons S l'ensemble des solutions de l'équation $(*)$. Posons $E \coloneqq \left\{(x, y, z) \in \mathbb{Z}^3, \text{PGCD}(x, y, z) = 1 \text{ et } 2x^2 + 3y^2 = 5z^2\right\}$. E est non vide car $(1; 1; 1) \in E$. Soit $n \in \mathbb{Z}$. Nommons $nE \coloneqq \{n \times (x, y, z), (x, y, z) \in E\}$.

Montrons que $S = \bigsqcup_{n\in\mathbb{Z}} nE$.

Démonstration. Soit $(x, y, z) \in S$. Si $(x, y, z) = (0; 0; 0)$, alors $(x, y, z) \in 0E \subset \bigcup_{n\in\mathbb{Z}} nE$. Sinon, posons $d \coloneqq \text{PGCD}(x, y, z)$. Posons $(x', y', z') \coloneqq \left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right)$. Alors $(x, y, z) = d \times (x', y', z')$, avec $\text{PGCD}(x', y', z') = 1$ et (x', y', z') solution de $(*)$ car $x^2 + 3y^2 = 5z^2 \iff \frac{x^2 + 3y^2}{d^2} = \frac{5z^2}{d^2} \iff 2\left(\frac{x}{d}\right)^2 + 3\left(\frac{y}{d}\right)^2 = 5\left(\frac{y}{d}\right)^2$. Donc $(x, y, z) \in dE \subset \bigcup_{n\in\mathbb{Z}} nE$. Réciproquement, soit $(x, y, z) \in \bigcup_{n\in\mathbb{Z}} nE$. Alors $\exists n \in \mathbb{Z}, \exists (x', y', z') \in$

$E, (x,y,z) = n \times (x',y',z')$. Or, $x'^2+3y'^2 = 5z'^2 \implies n^2 \times \left(2x'^2+3y'^2\right) = n^2 \times 5z'^2 \iff 2(nx')^2+3(ny')^2 = 5(nz')^2 \iff (x,y,z) \in S$. Montrons enfin que l'union est disjointe. $(0;0;0) \notin E$ car $\mathrm{PGCD}(0;0;0)$ n'existe pas donc $(0;0;0)$ n'appartient qu'à $0E$. Soit $(x,y,z) \neq (0;0;0)$. Supposons que $\exists (m,n) \in \mathbb{Z}^2, (x,y,z) \in mE \cap nE$. Alors il vient aisément que $\mathrm{PGCD}(x,y,z) = m = n$. □

Pour déterminer S, il suffit donc de déterminer E.

1.2 Lien avec les coniques

Montrons que déterminer E revient à déterminer les points à coordonnées rationnelles de la conique d'équation :

$$2X^2 + 3Y^2 = 5 \qquad (**)$$

Démonstration. Soit $(x,y,z) \in E$. Nous avons $z \neq 0$ sinon $(x,y,z) = (0;0;0)$ d'après l'observation faite plus haut, et $(0;0;0) \notin E$. Donc en divisant par z^2, l'équation $(*)$ devient $2\left(\frac{x}{z}\right)^2 + 3\left(\frac{y}{z}\right)^2 = 5$. Autrement dit, $\left(\frac{x}{z}, \frac{y}{z}\right)$ est solution rationnelle de $(**)$. Réciproquement, soit $(X,Y) \in \mathbb{Q}^2$ solution de $(**)$. Remarquons que $XY \neq 0$ car $\pm\sqrt{\frac{5}{3}}$ et $\pm\sqrt{\frac{5}{2}}$ sont irrationnels et $0 \neq 5$. En réduisant X et Y au même dénominateur, $\exists (x,y,z) \in (\mathbb{Z}^*)^3, (X,Y) = \left(\frac{x}{z}, \frac{y}{z}\right)$. Quitte à considérer $\frac{1}{\mathrm{PGCD}(x,y,z)}(x,y,z)$, nous pouvons supposer que $\mathrm{PGCD}\,(x,y,z) = 1$. Il s'ensuit que (x,y,z) est solution de $(*)$ donc que $(x,y,z) \in E$. Nous avons obtenu au passage que $(x,y,z) \in E \implies xyz \neq 0$. Nommons T l'ensemble des solutions rationnelles de $(**)$. Nous avons donc une application $\varphi : E \to T, (x,y,z) \mapsto \left(\frac{x}{z}, \frac{y}{z}\right)$ surjective. Montrons que φ est injective. Soit $((x,y,z),(x',y',z')) \in E^2, \varphi\left((x,y,z)\right) = \varphi\left((x',y',z')\right)$. Alors $\frac{x}{x'} = \frac{y}{y'} = \frac{z}{z'} \coloneqq k \in \mathbb{Z}^*$. Donc $\mathrm{PGCD}(x,y,z) = k\,\mathrm{PGCD}(x',y',z') \iff k = 1 \implies (x,y,z) = (x',y',z')$. Ainsi, $E \overset{\varphi}{\simeq} T$. □

2 Points rationnels de la conique

L'équation $(**)$ est celle d'une ellipse passant par $A(1;1)$. L'idée est d'obtenir une paramétrisation rationnelle de l'ellipse à partir de ce point A à coordonnées entières.

2.1 Paramétrisation rationnelle de la conique

Soit $M(X,Y)$ un point courant de l'ellipse.

Si $X \neq 1$, alors A et M sont distincts et le coefficient directeur de la droite (AM) est le réel $t = \frac{Y-1}{X-1}$.

Or, $2X^2+3Y^2=5$, donc en exprimant $Y=(X-1)t+1$ et en injectant, il vient $(X-1)(3t^2(X-1)+6t+2(X+1)=0$.

Or, $X\neq 1$ donc $3t^2(X-1)+6t+2(X+1)=0$ ce qui donne $X=\dfrac{3t^2-6t-2}{3t^2+2}$, car $3t^2+2$ ne s'annule pas sur $\mathbb{R}$.

En injectant dans $Y=(X-1)t+1$, il vient $Y=\dfrac{-3t^2-4t+2}{3t^2+2}$.

Ainsi, pour tout point courant de l'ellipse $M(X,Y)$ avec $X\neq 1$, il existe un réel t tel que $X=\dfrac{3t^2-6t-2}{3t^2+2}, Y=\dfrac{-3t^2-4t+2}{3t^2+2}$.

Est-il possible d'étendre ces expressions au cas où M coïncide avec A ? Pour cela, il suffit de déterminer s'il existe un réel t tel que $\dfrac{3t^2-6t-2}{3t^2+2}=1$ et $\dfrac{-3t^2-4t+2}{3t^2+2}=1$. Le réel $t=-\dfrac{2}{3}$ convient et c'est le seul. On montre de même qu'on ne peut pas étendre ces expressions au cas où M coïncide avec $M_\infty(1;-1)$. La notation parle d'elle-même : ce point est atteint pour t tendant vers $\pm\infty$.

Au final, pour tout point courant de l'ellipse $M(X,Y)$ distinct du point $M_\infty(1;-1)$, il existe un réel t tel que $X=\dfrac{3t^2-6t-2}{3t^2+2}, Y=\dfrac{-3t^2-4t+2}{3t^2+2}$.

Un même point courant de l'ellipse $M(X,Y)$ peut-il être obtenu avec deux valeurs distinctes de t ? Pour cela, il faudrait avoir simultanément $f(t_1)=f(t_2)$ et $g(t_1)=g(t_2)$ avec $t_1\neq t_2$ et $f(t)=\dfrac{3t^2-6t-2}{3t^2+2}, g(t)=\dfrac{-3t^2-4t+2}{3t^2+2}$. L'étude des variations de f et g montre que c'est impossible. À chaque point courant de l'ellipse $M(X,Y)$ distinct du point $M_\infty(1;-1)$ correspond donc un unique réel t tel que $X=f(t), Y=g(t)$.

t	$-\infty$		$-\frac{\sqrt{10}+2}{3}$		$-\frac{2}{3}$		$\frac{3-\sqrt{15}}{3}$		$\frac{\sqrt{10}-2}{3}$		1		$\frac{3+\sqrt{15}}{3}$		$+\infty$
f	1	↗		↘	1	↘		↗		↗		↗	1		
g	-1	↗	1	↗		↘	0	↘		↘	-1	↗		↗	-1

Réciproquement, pour tout réel t, on vérifie que $2\times\left(\dfrac{3t^2-6t-2}{3t^2+2}\right)^2+3\times\left(\dfrac{-3t^2-4t+2}{3t^2+2}\right)^2=5$, autrement dit $(f(t),g(t))$ est un point de l'ellipse.

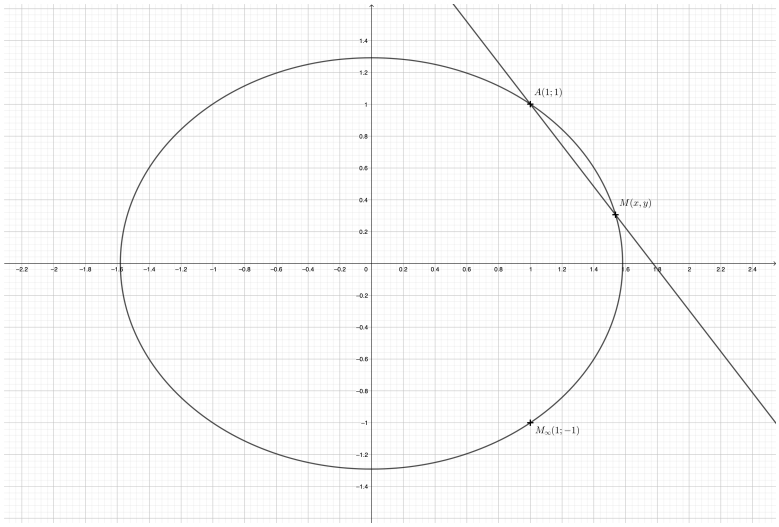
Ainsi, les points de l'ellipse distincts de $M_\infty(1;-1)$ sont exactement les points $M(X,Y)$ de coordonnées $X=\dfrac{3t^2-6t-2}{3t^2+2}, Y=\dfrac{-3t^2-4t+2}{3t^2+2}$, où t parcourt $\mathbb{R}$, et cette correspondance est biunivoque.

Si $t\in\mathbb{Q}$, alors il est évident d'après ces expressions que $X\in\mathbb{Q}, Y\in\mathbb{Q}$.

Réciproquement, nous avons vu que si $X = 1 \in \mathbb{Q}, Y = 1 \in \mathbb{Q}$, alors $t = -\dfrac{2}{3} \in \mathbb{Q}$. Si $X \neq 1$, puisque $t = \dfrac{Y-1}{X-1}$, si $X \in \mathbb{Q}, Y \in \mathbb{Q}$, alors $t \in \mathbb{Q}$.

Ainsi, les points de l'ellipse à coordonnées rationnelles sont exactement $M_\infty(1;-1)$ et les points $M(X,Y)$ de coordonnées $X = \dfrac{3t^2-6t-2}{3t^2+2}, Y = \dfrac{-3t^2-4t+2}{3t^2+2}$, où t décrit $\mathbb{Q}$, et cette correspondance est biunivoque.

Un point de détail sur l'aspect biunivoque : $t = \dfrac{1}{2}$ et $t = \dfrac{2}{4}$ renvoient le même point de la conique car $\dfrac{1}{2} = \dfrac{2}{4}$. Pour chaque rationnel t, on peut donc se restreindre à son unique représentant irréductible : ainsi, à chaque point à coordonnées rationnelles de la conique correspond un représentant irréductible $\dfrac{a}{b}$ du paramètre, de façon biunivoque.



2.2 Résolution de $(**)$

Écrivons alors X, Y sous forme de fractions (numérateurs et dénominateurs entiers) en écrivant $t = \dfrac{a}{b}, (a,b) \in \mathbb{Z}^2, b \neq 0, a \wedge b = 1$. Il vient $X = \dfrac{3a^2-6ab-2b^2}{3a^2+2b^2}, Y = \dfrac{-3a^2-4ab+2b^2}{3a^2+2b^2}$. Les dénominateurs sont bien non nuls.

Est-il possible d'étendre ces expressions au cas où M coïncide avec M_∞ ? Oui, il suffit de prendre $a = 1$ et $b = 0$ (on a bien $a \wedge b = 1$) et on peut vérifier que c'est le seul couple (a,b) possible.

Pour conclure, les points de l'ellipse à coordonnées rationnelles sont exactement les points $M(X,Y)$ de coordonnées $X = \dfrac{3a^2-6ab-2b^2}{3a^2+2b^2}, Y = \dfrac{-3a^2-4ab+2b^2}{3a^2+2b^2}$, où $(a,b) \in \mathbb{Z}^2, (a,b) \neq (0;0), a \wedge b = 1$ et la correspon-

dance entre les points à coordonnées rationnelles et de tels couples (a, b) est biunivoque.

3 Résolution de $(*)$

3.1 Détermination de E

Nous venons de résoudre $(**)$. D'après ce que nous avons vu précédemment, nous pouvons en déduire les éléments de E, puisque chaque élément de E est associé de façon biunivoque à un point à coordonnées rationnelles de l'ellipse.

$\forall (a, b) \in \mathbb{Z}^2, (a, b) \neq (0; 0), a \wedge b = 1$, posons $k \coloneqq \text{PGCD}(3a^2 - 6ab - 2b^2, -3a^2 - 4ab + 2b^2, 3a^2 + 2b^2)$.

Les éléments de E sont donc exactement les triplets $\frac{1}{k}(3a^2 - 6ab - 2b^2, -3a^2 - 4ab + 2b^2, 3a^2 + 2b^2)$. À chaque couple (a, b) convenable est associé un élément de E, de façon biunivoque.

3.2 Détermination de S

D'après la structure des solutions, les solutions de $(*)$ sont exactement les triplets $\frac{n}{k}(3a^2 - 6ab - 2b^2, -3a^2 - 4ab + 2b^2, 3a^2 + 2b^2)$, où n décrit $\mathbb{Z}$ et d'après tout ce qui a été vu, chaque couple (a, b) convenable et chaque n donnent une solution distincte.

3.3 Précisions sur k

k divise $-(3a^2 - 6ab - 2b^2) - (-3a^2 - 4ab + 2b^2) = 10ab$.

Donc k divise $-b \times 10ab + 5a(3a^2 + 2b^2) = 15a^3$.

k divise $-3a^2 - 4ab + 2b^2 + 3a^2 + 2b^2 = 4b^2 - 4ab$.

Donc k divise $2 \times 10ab + 5 \times (4b^2 - 4ab) = 20b^2$.

k divise $60a^3$ et $60b^2$ donc k divise $\text{PGCD}(60a^3, 60b^2) = 60 = 2^2 \times 3 \times 5$.

Donc $k = 2^\alpha \times 3^\beta \times 5^\gamma$, où α, β, γ sont des entiers naturels inférieurs ou égaux respectivement à $2, 1, 1$.

Supposons que 4 divise k.

Par transitivité, 4 divise $3a^2 + 2b^2$.

Or, il suffit d'examiner les congruences modulo 4 pour constater que c'est impossible.

Donc 4 ne divise pas k.

Donc $\alpha \leq 1$.

Donc k divise 30.