Géométrie et arithmétique

Jean Fresnel(*)

Résumé. L'objet de cet article est de présenter quelques problèmes à l'énoncé compréhensible par des professeurs de lycées et collèges dont les solutions, lorsqu'elles existent, nécessitent des résultats mathématiques contemporains. Il s'agit de problèmes en apparence de nature géométrique pour lesquels l'arithmétique intervient de façon profonde.

0. Introduction

Les quelques pages qui suivent sont extraites d'une conférence grand public donnée le 29 janvier 2005 dans le cadre de la journée annuelle de l'APMEP d'Aquitaine organisée à l'Université Bordeaux 1, par Éric Barbazo, Président de la Régionale APMEP d'Aquitaine.

Son objectif était de présenter quelques problèmes à l'énoncé compréhensible par des professeurs de lycées et collèges dont les solutions, lorsqu'elles existent, nécessitent des résultats mathématiques contemporains.

Dans cette voie, le plus célèbre est certainement le « grand théorème de Fermat », à l'énoncé le plus élémentaire possible, qui a maintenu en haleine la communauté mathématique pendant 300 ans et demandé pour sa solution l'utilisation de mathématiques élaborées du demi-siècle passé.

En résumé, quelques problèmes d'énoncés simples qu'Euclide aurait pu formuler et dont la solution utilise les développements récents de la géométrie arithmétique.

En ce qui concerne notre exposé, les énoncés appartiennent à la géométrie euclidienne, le plus souvent plane. Pour ce qui est du premier, vite dit, il s'agit de décrire si possible les configurations de n points du plan euclidien pour lesquelles il existe un point à distance rationnelle des dits points. C'est a priori un problème qui semble actuellement inaccessible. Sachant que pour $n = 2$ la réponse est sans difficulté, curieusement $n = 3$ oblige déjà à un exercice. À titre indicatif le début de ce problème a été traité par deux classes de collèges dans le cadre de *Maths en Jeans*. Il est donc assez facile, connaissant les formules reliant les cosinus, les sinus des angles d'un triangle aux longueurs de leurs côtés, de montrer un certain nombre de résultats sur les triangles dont les côtés sont de longueur rationnelle. La première difficulté est de trouver un triangle pour lequel il n'existe pas de point dont toutes les distances aux sommets du triangle sont rationnelles.

Prenons par exemple le cas d'un triangle aux côtés rationnels, existe-t-il une famille dense du plan euclidien dont les distances aux trois sommets sont rationnelles ? Facilement la mise en équation conduit à une cubique plane et là on est naturellement confronté à la célèbre théorie des courbes elliptiques dont l'ensemble des points rationnels sur $\mathbf{Q}$ constitue un groupe commutatif pour lequel de grands mystères ont été résolus, entre autres par J. L. Mordell, A. Weil et A. Wiles et pour

(*) Laboratoire de Théorie des nombres et Algorithmique Arithmétique. 351 cours de la libération, 33405 Talence France. fresnel@math.u-bordeaux1.fr

lequel la célèbre conjecture de Birch et Swinnerton-Dyer reste encore une énigme qui « vaut » un million de dollars.

Parmi les problèmes d'énoncés géométriques simples, il reste des mystères étonnants. Par exemple existe-t-il un point à distance rationnelle des sommets d'un carré de côté 1 ? Existe-t-il un parallélépipède rectangle dont les arêtes, les diagonales de surface et les diagonales de solides sont entières ?

Nous terminons cet exposé par la recherche des nombres congruents ; i.e. des nombres entiers qui sont l'aire d'un triangle rectangle dont les trois côtés sont rationnels. Là encore la mise en équation conduit à savoir si une cubique plane admet pour la structure de groupe un point d'ordre infini. Cette question est intimement reliée à la célèbre conjecture de Birch et Swinnerton-Dyer, énoncée il y a 40 ans, disant que l'existence d'un point d'ordre infini est équivalent au fait qu'une fonction associée à la courbe elliptique, analogue à la fonction zêta de Riemann, s'annule en 1. C'est en reliant cette valeur au point 1 de la fonction, au nombre de représentations de l'entier N par certaines formes quadratiques que Tunnell (1983) a permis véritablement de progresser dans la connaissance des N qui sont congruents. À l'époque, il a su déterminer tous les nombres congruents inférieurs à 1 000, et maintenant on connaît ceux inférieurs à 40 000. Toutefois la description d'un triangle rectangle associé à un nombre congruent semble inaccessible ; par exemple, N = 157 est l'aire d'un triangle rectangle à côtés rationnels, chacun d'eux nécessitant au numérateur et au dénominateur environ vingt chiffres en base 10.

1. Les triangles rationnels, les quadrilatères rationnels, le problème des distances rationnelles à un ensemble fini du plan

1.0. Le problème « inaccessible »

Soit $\{a_1, a_2, \ldots, a_n\}$ un ensemble fini de points du plan euclidien. Existe-t-il un point m du plan tel que les distances de m à chaque point a_i soient des nombres rationnels ? Ou encore, trouver les ensembles finis du plan $\{a_1, a_2, \ldots, a_n\}$ tels que les distances de a_i et a_j soient entières pour tout i et j.

1.1. Le cas de trois points ; les outils

1.1.1. Relations entre les angles et les longueurs des côtés d'un triangle (fig.1 ; [Fr] p. 180)

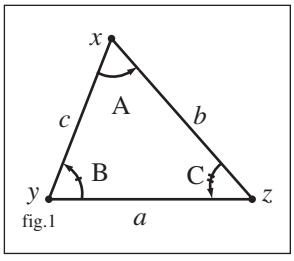

fig.1

Selon les notations de la figure 1, ci-contre, on a la loi des sinus :

$$\frac{\sin A}{a} = \frac{\sin B}{b} = \frac{\sin C}{c}$$

et les formules reliant cosinus et longueurs des côtés :

$$\cos A = \frac{b^2 + c^2 - a^2}{2bc}, \cos B = \frac{c^2 + a^2 - b^2}{2ca}, \cos C = \frac{a^2 + b^2 - c^2}{2ab}.$$

1.1.2. Les formules trigonométriques d'addition seront en permanence utilisées :

$$\cos(A+B)=\cos A\cos B-\sin A\sin B,\ \sin(A+B)=\sin A\cos B+\cos A\sin B.$$

1.1.3. La paramétrisation du cercle unité et d'une ellipse

Soient **Q** (resp. **R**) le corps des nombres rationnels (resp. réels), K = **Q** ou **R**,

$$A(K)=\left\{(x,y)\in K^2 \mid x^2+y^2=1,(x,y)\neq(0,1)\right\},$$

et si D ∈ **Q**, soit

$$A_D(K)=\left\{(x,y)\in K^2 \mid Dx^2+y^2=1,(x,y)\neq(0,1)\right\}.$$

Alors $\rho_K : K \to A(K)$ (resp. $\rho_{D,K} : K \to A_D(K)$) définie par

$$\rho_K(t)\coloneqq\left(\frac{2t}{t^2+1},\frac{t^2-1}{t^2+1}\right)$$

$$\left(\text{resp. } \rho_{D,K}(t)\coloneqq\left(\frac{2t}{t^2+D},\frac{t^2-D}{t^2+D}\right)\right)$$

est une bijection. De plus $\rho_{\mathbf{R}}$ (resp. $\rho_{D,\mathbf{R}}$) est bicontinu. Il suit de cela que A(**Q**) (resp. A_D(**Q**)) est dense dans A(**R**) (resp. A_D(**R**)).

Il est facile de montrer que ρ_K (resp. $\rho_{D,K}$) est injectif. Montrons que ρ_K est surjectif. Soit (x,y) ∈ A(K), comme $x \neq 0$, on a $\left(\frac{1}{x}\right)^2-\left(\frac{y}{x}\right)^2=1$, et donc $\left(\frac{1}{x}+\frac{y}{x}\right)\left(\frac{1}{x}-\frac{y}{x}\right)=1$; soit alors $t\coloneqq\frac{1}{x}+\frac{y}{x}$, on a t ∈ K et $\frac{1}{x}-\frac{y}{x}=\frac{1}{t}$. Il suit facilement de ces relations que $x=\frac{2t}{t^2+1}$, $y=\frac{t^2-1}{t^2+1}$. Le cas de $\rho_{D,K}$ se traite de façon analogue avec la relation $\left(\frac{1}{x}\right)^2-\left(\frac{y}{x}\right)^2=D$.

1.2. Conséquences sur les triangles à longueur des côtés rationnels

1.2.1. Un triangle à côtés rationnels

Soit (x,y,z) un triangle dont les longueurs de côtés sont rationnelles, alors il suit de 1.1.1. que cos A, cos B, cos C ∈ **Q** et que $(\sin A)^2$, $(\sin B)^2$, $(\sin C)^2$ ∈ **Q**. En plus si sin A ∈ **Q**, alors 1.1.1. dit que sin B, sin C ∈ **Q** ; si sin A = $\sqrt{D}$ où D ∈ **Q**, alors on a sin B ∈ **Q** $\sqrt{D}$, sin C ∈ **Q** $\sqrt{D}$.

1.2.2. Les types d'angles

Définition. Un nombre réel A sera dit *de type I*, si cos A ∈ **Q** et sin A ∈ **Q**. Si D ∈ **Q**, un nombre réel A sera dit *de type II associé à* $\sqrt{D}$, si cos A ∈ **Q** et

$\sin A \in \mathbf{Q}\sqrt{D}$.

Ainsi un nombre réel A qui est de type I, est aussi de type II ; en revanche un nombre réel A de type II associé à $\sqrt{D}$, est aussi de type I si et seulement si D est un carré de **Q**.

Il suit donc de 1.1.2. que si A et B sont de type I (resp. de type II associé à $\sqrt{D}$), alors A + B est de type I (resp. de type II associé à $\sqrt{D}$). En particulier si A, B, C sont des mesures d'angles d'un triangle, alors si A et B sont de type I (resp. de type II associé à $\sqrt{D}$), alors C est de type I (resp. de type II associé à $\sqrt{D}$).

Il suit de 1.2.1. que si (x,y,z) est un triangle à côtés rationnels, alors les trois angles sont de type I , ou les trois angles sont de type II associés au même $\sqrt{D}$ avec $D \in \mathbf{Q}$.

1.2.3. Sur la densité des angles

Soit $\theta :]0,2\pi[\to A(\mathbf{R})$ (resp. $\theta_D :]0,2\pi[\to A_D(\mathbf{R})$) défini par :

$$\theta(\alpha) \coloneqq (\sin\alpha, \cos\alpha)\left(\text{resp. } \theta_D(\alpha) \coloneqq \left(\frac{\sin\alpha}{\sqrt{D}}, \cos\alpha\right)\right).$$

Alors θ (resp. θ_D) est bicontinu. Sachant par 1.1.3. que $A(\mathbf{Q})$ (resp. $A_D(\mathbf{Q})$) est dense dans $A(\mathbf{R})$ (resp. $A_D(\mathbf{R})$) , il suit par θ^{-1} que $\left\{\alpha \in]0,2\pi[\,\middle|\, (\sin\alpha, \cos\alpha) \in \mathbf{Q}^2\right\}$

$\left(\text{resp. } \left\{\alpha \in]0,2\pi[\,\middle|\, \left(\frac{\sin\alpha}{\sqrt{D}}, \cos\alpha\right) \in \mathbf{Q}^2\right\}\right)$ est dense dans $]0,2\pi[$; en particulier ces ensembles sont infinis.

1.3. Les résultats avec trois points (x, y, z)

1.3.0. Les triangles à côtés et hauteurs rationnels

Il existe une infinité de triangles du plan euclidien, non semblables, de façon que les longueurs des côtés soient des nombres rationnels et que les longueurs des hauteurs soient des nombres rationnels.

Soient y, z deux points du plan euclidien avec $\|y-z\| = 1$, B, C $\in [0,\pi[$ avec B, C de type I et B + C < π.

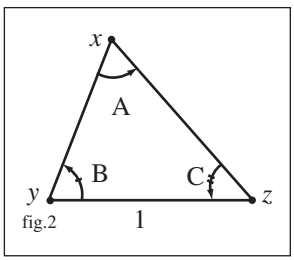

fig.2

Alors il existe x tel que les angles du triangle aient pour mesures respectives A = π − (B + C), B, C. Il suit de 1.2.2. que A est aussi de type I et de la loi des sinus que les longueurs des côtés du triangle (x, y, z) sont rationnelles. Sachant que les angles sont du type I et les côtés rationnels, il suit facilement que les hauteurs sont

rationnelles. Enfin il résulte de 1.2.3. qu'il y a une infinité de tels triangles non semblables.

1.3.1. Les points sur les côtés d'un triangle

Soit (x, y, z) un triangle du plan euclidien, dont les longueurs des côtés sont des nombres rationnels. Alors sur la droite passant par y et z, il existe une famille dense de points m dont les distances à x, y, z sont des nombres rationnels.

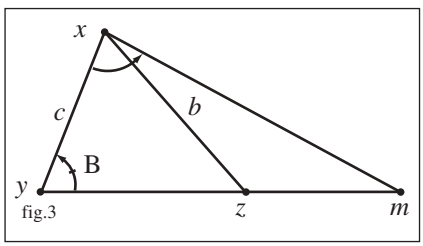

fig.3

Soit m un point de la droite V(y, z) de façon que la mesure α de l'angle en x du triangle (x, y, m) soit de type I, si B est de type I (resp. de type II associé à $\sqrt{D}$, si B est de type II associé à $\sqrt{D}$). Il suit alors de 1.2.2. que l'angle en m du triangle (x, y, m) sera de type I (resp. de type II associé à $\sqrt{D}$). Ici encore la loi des sinus implique que $\|x-m\|$ et $\|y-m\|$ sont rationnels et donc $\|z-m\|$ est aussi rationnel. La densité résulte de 1.2.3.

1.3.2. Les points sur le cercle circonscrit à un triangle

Soit (x, y, z) un triangle du plan euclidien, dont les longueurs des côtés sont des nombres rationnels. Alors sur le cercle C *passant par x, y, z, il existe une famille dense de points m dont les distances à x, y, z sont des nombres rationnels.*

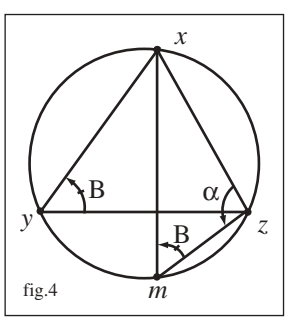

fig.4

Soit m un point de C de façon que la mesure α de l'angle en z du triangle (x, y, m) soit de type I, si B est de type I (resp. de type II associé à $\sqrt{D}$, si B est de type II associé à $\sqrt{D}$). Sachant par l'arc capable que B est une mesure de l'angle en m du triangle (x, y, m), il suit alors de 1.2.2. et de la loi des sinus que $\|x-m\|$ et $\|z-m\|$ sont rationnels. Par la même méthode en utilisant le triangle (x, y, m), on montre que $\|y-m\|$ est rationnel. La densité résulte de 1.2.3.

1.3.3. Un exemple irrationnel

Il existe un triangle (x, y, z) du plan euclidien tel que pour tout point m du plan, l'une au moins des distances de m à l'un des sommets ne soit pas un nombre rationnel.

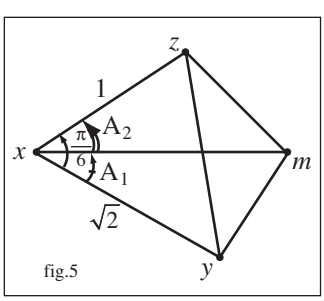

fig.5

On considère le triangle (x, y, z) avec les données numériques consignées dans la figure 5. On suppose

qu'il existe un point m tel que $\|x-m\|$, $\|y-m\|$, $\|z-m\|$ soient rationnels. Il suit de 1.2.1. que cos $A_2 \in \mathbf{Q}$, sin $A_2 = \sqrt{D}$, $D \in \mathbf{Q}$, de 1.1.1. que cos $A_1 = s\sqrt{2}$, $s \in \mathbf{Q}$, sin $A_1 = \sqrt{E}$, $E \in \mathbf{Q}$, parce que $\cos^2 A_1 + \sin^2 A_1 = 1$. Il suit des formules d'addition 1.1.2. que

$$\frac{\sqrt{3}}{2} = \cos\frac{\pi}{6} = \cos(A_1 + A_2) = s'\sqrt{2} - \sqrt{D}\sqrt{E},\ s' \in \mathbf{Q}.$$

Il suit, en élevant $\left(\frac{\sqrt{3}}{2} - s'\sqrt{2}\right)$ au carré que $\sqrt{6} = r \in \mathbf{Q}$. C'est donc impossible.

1.3.4. Le résultat fondamental

Théorème. *Soit (x, y, z) un triangle du plan euclidien dont l'angle en x est de cosinus rationnel et tel que $\|x-y\|$ et $\|x-z\|$ soient rationnels. Alors il existe une famille dense de points m du plan telle que $\|x-m\|$, $\|y-m\|$, $\|z-m\|$ soient rationnels.*

Corollaire 1. *Soit (x, y, z) un triangle du plan euclidien dont les longueurs des côtés sont rationnelles. Alors il existe une famille dense de points m du plan tels que les distances de m à x, y et z soient rationnelles.*

Corollaire 2. *Soit (x, y, z, t) les sommets d'un carré de longueurs de côté* 1. *Alors il existe une famille dense de points m du plan tels que les distances de m à x, y et z soient rationnelles.*

Démonstration du théorème

1.3.4.1. Soient (x, y, z) un triangle dont l'angle en x, de mesure A, est de cosinus rationnel et tel que $\|x-y\|$ et $\|x-z\|$ soient rationnels. Soit Δ une droite passant par x, notons α_1, α_2 les mesures des angles selon la figure 6. Comme cos $A \in \mathbf{Q}$, on a sin $A = \sqrt{D}$, avec $D \in \mathbf{Q}$. Par 1.2.3. il existe une famille dense de réels α_1 de façon que cos $\alpha_1 \in \mathbf{Q}$, et sin $\alpha_1 \in \mathbf{Q}\sqrt{D}$; en plus on choisit α_1 de façon que les projections orthogonales de y et z sur Δ soient distinctes. Il suit alors des formules d'addition 1.1.2. que cos $\alpha_2 = \cos(A - \alpha_1) \in \mathbf{Q}$ et même que sin $\alpha_2 \in \mathbf{Q}\sqrt{D}$.

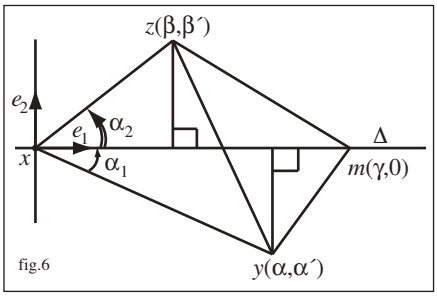

fig.6

Soit $(x\ ;\ e_1,\ e_2)$ un repère orthonormé de façon que $\Delta = x + \mathbf{R}e_1$. Soient (α, α') (resp. (β, β')) les coordonnées de y (resp. z) dans ce repère. On a donc $\alpha \in \mathbf{Q}$ (resp. $\beta \in \mathbf{Q}$) et $\alpha'^2 = 4a \in \mathbf{Q}$ (resp. $\beta'^2 = 4b \in \mathbf{Q}$). Soit m un point de Δ de coordonnées $(\gamma, 0)$. On a donc

$$\|m-y\|^2=(\gamma-\alpha)^2+4a\,,\quad \|m-z\|^2=(\gamma-\beta)^2+4b\,.$$

Il suit facilement, en imitant 1.1.3., qu'il existe $u\in\mathbf{R}$ (resp. $v\in\mathbf{R}$) tels que

$$(\gamma-\alpha)=u-\frac{a}{u},\ (\gamma-\beta)=v-\frac{b}{v}\ ; \tag{1}$$

soit $c:=\beta-\alpha$, alors (1) donne

$$u-\frac{a}{u}=v-\frac{b}{v}+c\,. \tag{1′}$$

Si $u,\ v\in\mathbf{Q}-\{0\}$ et satisfont (1′) , on aura alors

$$\|m-y\|^2=\left(u-\frac{a}{u}\right)^2+4a=\left(u+\frac{a}{u}\right)^2,$$

de même

$$\|m-z\|^2=\left(v+\frac{b}{v}\right)^2.$$

Il suit de cela $\|m-y\|$ et $\|m-z\|$ sont rationnels. Par ailleurs $\|m-x\|=|\gamma|=\left|u-\frac{a}{u}+\alpha\right|$ est rationnel.

Ainsi donc, tout point m de coordonnées $(\gamma,0)$ satisfaisant (1) et (1′) avec $u,\ v\in\mathbf{Q}$ est à distance rationnelle de (x,y,z).

Une solution facile de (1′) est donnée par $u=v=\frac{b-a}{c}\in\mathbf{Q}-\{0\}$ si $a\neq b$.

Notre souhait est de montrer que (1′) admet une infinité de solutions dans $\mathbf{Q}$ où les u (resp. v) constituent une partie dense de $\mathbf{R}$.

1.3.4.2. L'équation (1′) est une cubique plane. Il est assez facile de montrer la suite des égalités ci-après.

$$\left(x-\frac{a}{x}\right)-\left(y-\frac{b}{y}\right)=c\,, \tag{2}$$

en élevant au carré, on obtient

$$\left(x^2+\frac{a^2}{x^2}\right)+\left(y^2+\frac{b^2}{y^2}\right)+2\left(b\frac{x}{y}+a\frac{y}{x}\right)-2xy-2\frac{ab}{xy}-2(a+b)=c^2\,, \tag{3}$$

$$\left(x^2+\frac{a^2}{x^2}\right)+\left(y^2+\frac{b^2}{y^2}\right)+2\left(b\frac{x}{y}+a\frac{y}{x}\right)=c^2+2(a+b)+2xy+2\frac{ab}{xy}\,. \tag{4}$$

Soit $\mathrm{X}:=xy,\ \mathrm{Y}:=\mathrm{X}\left(\left(x+\frac{a}{x}\right)\left(y+\frac{b}{y}\right)\right)$. On a donc

$$\mathrm{Y}^2=\mathrm{X}^2\left(\left(x^2+\frac{a^2}{x^2}\right)+\left(y^2+\frac{b^2}{y^2}\right)+2\left(b\frac{x}{y}+a\frac{y}{x}\right)+2(a+b)+2xy+2\frac{ab}{xy}\right), \tag{5}$$

$$Y^2 = X^2\left(c^2 + 4(a+b) + 4xy + 4\frac{ab}{xy}\right), \qquad (6)$$

$$Y^2 = 4X^2 + \left(c^2 + 4(a+b)\right)X^2 + 4ab\,X. \qquad (7)$$

En particulier, X = 0, Y = 0 et $X = \frac{(b-a)^2}{c^2}$, $Y = 2\frac{(b-a)^3}{c^3} + \frac{(b-a)}{c}(a+b)$ sont solutions de (7).

1.3.4.3. L'équivalence entre (2) et (7) sur **Q**.

Soit $(\alpha, \beta) \in \mathbf{Q}^2$ une solution de (7) avec $\alpha\beta \neq 0$, alors il existe $(u, v) \in \mathbf{R}^2$ avec $uv = \alpha$ et $\beta = \alpha\left(\left(u + \frac{a}{u}\right) + \left(v + \frac{b}{v}\right)\right) \in \mathbf{Q}$. On déduit de cela que

$$\left(\left(u - \frac{a}{u}\right) - \left(v - \frac{b}{v}\right)\right)^2 = c^2.$$

Ainsi, quitte à changer (α, β) en $(\alpha, -\beta)$, on peut supposer que $\left(u - \frac{a}{u}\right) - \left(v - \frac{b}{v}\right) = c$. Comme $\left(u + \frac{a}{u}\right) + \left(v + \frac{b}{v}\right) \in \mathbf{Q}$, on déduit que $2u + 2\frac{b}{v} \in \mathbf{Q}$. Alors de $uv \in \mathbf{Q}$, on conclut que $u \in \mathbf{Q}$ et donc que $v \in \mathbf{Q}$. En conclusion, si $(\alpha, \beta) \in \mathbf{Q}^2$ satisfait (7) avec $\alpha\beta \neq 0$, alors quitte à changer (α, β) en $(\alpha, -\beta)$, il existe $u, v \in \mathbf{Q}$ satisfaisant (2) avec $uv = \alpha$ et $\beta = \alpha\left(\left(u + \frac{a}{u}\right) + \left(v + \frac{b}{v}\right)\right) \in \mathbf{Q}$. On est donc ramené à trouver une famille dense de (α, β) satisfaisant (7) ; c'est pourquoi un détour par les courbes elliptiques est nécessaire.

1.3.4.4. Le groupe associé à une cubique plane.

Soit P(X, Y) := $Y^2 - H(X)$ où $H(X) \in \mathbf{Q}[X]$, degré H = 3, 1 = pgcd(H, H′) où H′ est le polynôme dérivé de H . Soit

$$E(\mathbf{Q}) := \left\{(\alpha, \beta) \in \mathbf{Q}^2 \mid P(\alpha, \beta) = 0\right\} \cup \{\infty\}.$$

Alors l'ensemble E(**Q**) peut être muni d'une structure de groupe commutatif où ∞ est l'élément neutre de la façon qui suit. Si $p, q \in E(\mathbf{Q})$, la droite passant par p et q coupe E(**Q**) en un troisième point r'. Ensuite la droite passant par r' et parallèle à l'axe des « y » coupe E(**Q**) en un point noté $p + q$. Alors l'application $(p, q) \mapsto p + q$ définit sur E(**Q**) une loi de groupe commutatif (en fait cet énoncé est approximatif pour deux raisons, la première est qu'il faudrait considérer le cas où $p = \infty$, la seconde est que

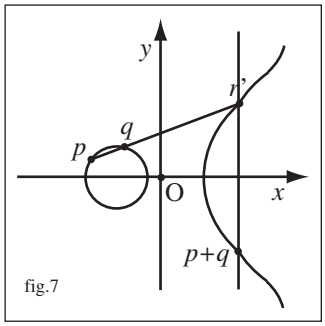

fig.7

le troisième point demande à être précisé si $p = q$; enfin le fait que la loi soit associative n'est pas évident).

Pour ceux qui sont familiers avec les espaces projectifs, on peut interpréter de façon plus agréable E(**Q**). Si

$$H(X) = q_0 + q_1X + q_2X^2 + q_3X^3$$

et si

$$P^{\#}(X,Y,T) := Y^2T - (q_0\ T^3 + q_1T^2X + q_2TX^2 + q_3X^3)$$

est l'homogénéisé de P, alors E(**Q**) s'identifie à la partie suivante de $P^2(\mathbf{Q})$:

$$\left\{(\alpha:\beta:\gamma)\in P^2(\mathbf{Q}) \mid P^{\#}(\alpha,\beta,\gamma)=0\right\},$$

les (α,β) étant $(\alpha : \beta : 1)$ et ∞ étant $(0 : 1 : 0)$. Par ailleurs on définit E(**R**) par

$$E(\mathbf{R})=\left\{(\alpha,\beta)\in\mathbf{R}^2 \mid P(\alpha,\beta)=0\right\}\cup\{\infty\}$$

et si **C** est le corps des nombres complexes, on définit E(**C**) par

$$E(\mathbf{C})=\left\{(\alpha,\beta)\in\mathbf{C}^2 \mid P(\alpha,\beta)=0\right\}\cup\{\infty\}.$$

On peut montrer qu'il existe $\tau\in\mathbf{C}$ de partie imaginaire strictement positive et un isomorphisme de groupe de E(**C**) sur $\dfrac{\mathbf{C}}{\mathbf{Z}1\oplus\mathbf{Z}\tau}$, où **Z** est le groupe additif des entiers. On lit en particulier que les éléments d'ordre fini de E(**C**) sont les éléments de $\dfrac{\mathbf{Q}}{\mathbf{Z}}\times\dfrac{\mathbf{Q}}{\mathbf{Z}}$.

La structure du groupe E(**Q**) méritera ultérieurement de plus amples commentaires. Ici le polynôme issu de (7) définit un groupe E(**Q**) , on souhaite trouver un point $(\alpha,\beta)\in$ E(**Q**) d'ordre infini parce que le sous-groupe engendré par un tel point est dense dans E(**R**) . La conséquence de cette situation est que l'équation (1′) admettra une famille $\left((u_i,v_i)\right)_i$ de solutions avec $\left((u_i)\right)_i$ (resp. $\left((v_i)\right)_i$) dense dans **R**. Il suivra que la famille $(m_i)_i$ de points de coordonnées $\left(\alpha+u_i-\dfrac{a}{u_i},0\right)$ sera dense dans Δ.

1.3.4.5. L'existence d'un point $(\alpha,\beta)\in$ E(**Q**) qui est d'ordre infini résultera du théorème ci-après :

Le théorème de Nagell-Lutz. *Soit la courbe* $y^2 = x^3 + ax + b$ *avec* $a, b \in \mathbf{Z}$. *Soit* (α,β) *un point rationnel de la courbe qui est d'ordre fini. Alors* $\alpha,\beta\in\mathbf{Z}$ *et soit* $\beta=0$ *soit* $\beta^2 \mid 4a^3+27b^2$ *dans* **Z**.

Il restera donc à montrer qu'il existe une famille dense d'angles α_1 de façon que le point $\left(\dfrac{(b-a)^2}{c^2}, 2\dfrac{(b-a)^3}{c^3}+\dfrac{(b-a)}{c}(a+b)\right)$ soit d'ordre infini (c'est l'article [Al]).

2. Le cas de quatre points et des problèmes ouverts

2.1. Le problème du carré

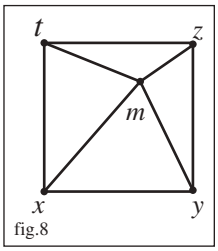

fig.8

Soit (*x, y, z,* t) un carré de longueur de côté 1. Existe-t-il un point *m* dont les distances à *x*, *y*, *z*, *t* soient des nombres rationnels ?

2.2. Le problème des médianes

Existe-t-il un triangle dont les longueurs des côtés, les hauteurs et les médianes sont des nombres rationnels ?

2.3. Le problème du parallélépipède

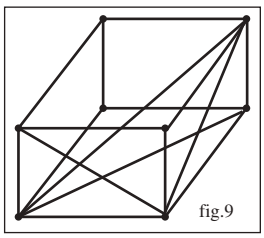
fig.9

Existe-t-il un parallélépipède rectangle dont les arêtes sont entières, dont les diagonales de surface sont entières, et dont les diagonales de solide sont entières ?

3. Les nombres congruents

3.1. La définition d'un nombre congruent

Un entier $N \geq 1$ est dit *congruent* s'il satisfait une des propriétés équivalentes suivantes.

i) *L'entier* N *est l'aire d'un triangle rectangle à côtés rationnels,*

ii) *il existe un nombre rationnel x tel que* $x^2 - N$ *et* $x^2 + N$ *soient tous deux des carrés de nombres rationnels,*

iii) *il existe* $x, y \in \mathbf{Q}, y \neq 0$ *tels que* $y^2 = x\left(x^2 - N^2\right)$,

iv) *il existe* $s, t \in \mathbf{Q}, st \neq 0$ *tels que* $s^4 - N^2 = t^2$.

Démonstration

iv) *implique* iii) De la relation $s^4 - N^2 = t^2$ il suit $s^2\left(\left(s^2\right)^2 - N^2\right) = (st)^2$, ce qui montre iii) en posant $x = s^2$ et $y = st$.

iii) *implique* i) De la relation $y^2 = x\left(x^2 - N^2\right)$, on pose $a := \left|\frac{N^2 - x^2}{y}\right|$, $b := \left|\frac{2Nx}{y}\right|$, $c := \left|\frac{N^2 + x^2}{y}\right|$. Il suit de cela que $ab = 2N$ et $a^2 + b^2 = c^2$, ce qui est bien i).

i) *implique* ii) De la relation $2N = ab$, $a^2 + b^2 = c^2$ avec $a, b, c \in \mathbf{Q}$, on déduit $c^2 + 4N = (a + b)^2$, $c^2 - 4N = (a - b)^2$, ce qui est ii).

ii) *implique* iv) De $x^2 - N = u^2$, $x^2 + N = v^2$, on déduit $x^4 - N^2 = (uv)^2$, ce qui est iv) .

Remarque 1. Soient les entiers $N \geq 1$, $\alpha \geq 1$. Alors N est congruent si et seulement si $\alpha^2 N$ est congruent. Il suit de cela qu'il suffit de connaître les nombres congruents sans facteurs carrés.

Remarque 2. La propriété iii) dit que N est congruent si la cubique définie par $Y^2 - X(X^2 - N^2)$ admet un point $(\alpha, \beta) \in \mathbf{Q}^2$ avec $\beta \neq 0$; c'est cette propriété qui sera abondamment utilisée.

3.2. Quelques exemples

3.2.0. Deux équations diophantiennes classiques

3.2.0.1. L'équation diophantienne $x^2 + y^2 = z^2$

Soient

$$\mathrm{F}_2 \coloneqq \left\{(x,y,z) \in \mathbf{Z}^3 \mid x^2 + y^2 = z^2,\ x > 0,\ y > 0,\ z > 0, 2 \mid x \text{ et } \operatorname{pgcd}(x,y) = 1\right\},$$

$$\mathrm{E} \coloneqq \left\{(a,b) \in \mathbf{Z}^2 \mid a > 0, b > 0, \operatorname{pgcd}(a,b) = 1, a + b \equiv 1 \bmod 2\right\}.$$

Alors l'application $\rho : \mathrm{E} \to \mathrm{F}_2$ définie par $\rho(a,b) = \left(2ab, a^2 - b^2, a^2 + b^2\right)$ est une bijection.

Démonstration Soient $(a,b) \in \mathrm{E}$, facilement $\rho(a,b) \in \mathrm{F}_2$ et ρ est injectif. Soit maintenant $(x,y,z) \in \mathrm{F}_2$, il suit que $1 = \operatorname{pgcd}(y,z)$, 2 ne divise pas y et 2 ne divise pas z ; ainsi $\frac{z-y}{2}$, $\frac{z+y}{2}$, $\frac{x}{2} \in \mathbf{Z}$ avec $\left(\frac{x}{2}\right)^2 = \left(\frac{z-y}{2}\right)\left(\frac{z+y}{2}\right)$ et $1 = \operatorname{pgcd}\left(\frac{z+y}{2}, \frac{z-y}{2}\right)$. On déduit de cela qu'il existe $a,\ b \in \mathbf{Z}$ avec $\frac{z+y}{2} = a^2$, $\frac{z-y}{2} = b^2$, $a > 0$, $b > 0$, $a > b$, et $1 = \operatorname{pgcd}(a,b)$. On conclut que $x = 2ab$, $y = a^2 - b^2$, $z = a^2 + b^2$. En utilisant $a^2 + b^2 \equiv z \equiv 1 \mod 2$, on a bien

$$a + b \equiv 1 \mod 2\,.$$

3.2.0.2. L'équation diophantienne $x^2 = y^4 - z^4$

Il n'existe pas de triplet $(x,y,z) \in \mathbf{Z}^3$ avec $x^2 = y^4 - z^4$ et $xyz \neq 0$.

(*) On suppose qu'il existe $(x',y',z') \in \mathbf{Z}^3$ avec $x'^2 = y'^4 - z'^4$ et $x'y'z' \neq 0$.
Alors en considérant le pgcd de y' et z', il suit qu'il existe $(x,y,z) \in \mathbf{Z}^3$ avec $1 = \operatorname{pgcd}(y,z)$, $x > 0$, $y > z > 0$ et $x^2 = y^4 - z^4$.

(**) Soient $(x,y,z) \in \mathbf{Z}^3$ avec $1 = \operatorname{pgcd}(y,z)$, $x > 0$, $y > z > 0$ et $x^2 = y^4 - z^4$ et y minimal satisfaisant ce qui précède.

Soient $(x,y,z) \in \mathbf{Z}^3$ satisfaisant (**), alors l'examen de (**) modulo 8 montre que $2 \mid y$ est impossible.

Soient $(x,y,z) \in \mathbf{Z}^3$ satisfaisant (**), avec 2 ne divise pas y et 2 ne divise pas z. Conclure que $2 \mid x$ et $1 = \operatorname{pgcd}(x, z^2)$. En utilisant 3.2.0.1. avec $x^2 + z^4 = y^4$, on déduit qu'il existe $a > b > 0$ avec $x = 2ab$, $z^2 = a^2 - b^2$, $y^2 = a^2 + b^2$. On a donc $(yz)^2 = a^4 - b^4$ avec $a < y$. Cela contredit la minimalité de (**).

Soient $(x,y,z) \in \mathbf{Z}^3$ satisfaisant (**) , avec 2 ne divise pas y et $2 \mid z$. Alors on a $1 = \text{pgcd}(x,z^2)$. En utilisant 3.2.0.1. avec $x^2 + z^4 = y^4$, on déduit qu'il existe $a > 0$, $b > 0$ avec $z^2 = 2ab$, $y^2 = a^2 + b^2$, $1 = \text{pgcd}(a,b)$. Quitte à permuter a et b, on peut supposer que $2 \mid a$. Il suit que $a = 2p^2$, $b = q^2$ avec 2 ne divise pas q, $1 = \text{pgcd}(p,q)$; ainsi $y^2 = 4p^4 + q^4$ avec $1 = \text{pgcd}(2p^2, q^2)$. Toujours en utilisant 3.2.0.1. avec $y^2 = 4p^4 + q^4$ on déduit qu'il existe $r > 0, s > 0$, avec $1 = \text{pgcd}(r,s)$, $2p^2 = 2rs$, $q^2 = r^2 - s^2$. Ainsi $r = u^2$, $s = v^2$, $1 = \text{pgcd}(u,v)$, et $q^2 = u^4 - v^4$. Comme $u < y$, cela contredit la minimalité de (**).

3.2.1. Proposition (Fermat). *Le nombre* 1 *n'est pas congruent.*

Démonstration. Supposons le contraire, i.e. que 1 soit congruent. On déduit de iii) qu'il existe $\alpha, \beta, a, b \in \mathbf{Z}$ avec $\alpha \neq 0$, $\beta > 0$, $a \neq 0$, $b > 0$, $1 = \text{pgcd}(\alpha,\beta)$, $1 = \text{pgcd}(a,b)$ et $\left(\frac{\alpha}{\beta}\right)^2 = \frac{a}{b}\left(\frac{a^2}{b^2} - 1\right)$ et donc que $b^3\alpha^2 = a\left(a^2 - b^2\right)\beta^2$. Il suit de cela et de la factorisation en premiers que $\alpha^2 = \alpha_1^2 a$, que a est un carré, que $b^3\alpha_1^2 = \left(a^2 - b^2\right)\beta^2$ et $1 = \text{pgcd}(\alpha_1,\beta)$. Toujours en utilisant $1 = \text{pgcd}(a,b)$, $1 = \text{pgcd}(\alpha_1,\beta)$ et la factorisation en premiers que $b^3 = \beta^2$, donc que b est un carré et que $\alpha_1^2 = a^2 - b^2$. En posant $a = a'^2$, $b = b'^2$, on déduit que $\alpha_1^2 = a'^4 - b'^4$. On sait alors par 3.2.0.2. que $\alpha_1 = 0$ ou que $b' = 0$; ce qui est contraire à notre hypothèse. Ainsi donc 1 n'est pas congruent.

3.2.2. Proposition. *Le nombre* 5 *est congruent.*

Démonstration. Il suffit de vérifier que $(x,y) = (3^2 \times 5, 2^2 \times 3 \times 5^2)$ satisfait $y^2 = x(x^2 - 5^2)$.

3.2.3. L'exemple des triangles pythagoriciens

Ce sont les triangles rectangles à côtés entiers. Il suffit de considérer $x, y, z \in \mathbf{N}$ avec $x^2 + y^2 = z^2$, $1 = \text{pgcd}(x,y,z)$, $2 \mid x$. Alors on sait par 3.2.0.1. qu'on peut les écrire sous la forme $x = 2ab$, $y = a^2 - b^2$, $z = a^2 + b^2$, $1 = \text{pgcd}(a,b)$. Ainsi donc les $N = ab(a^2 - b^2)$ pour $1 \leq b < a$, $1 = \text{pgcd}(a,b)$ sont congruents.

$N = ab(a^2 - b^2)$	a	b
6	2	1
$3 \times 8 = 6 \times 2^2$	3	1
6×5	3	2

3.3. Les courbes elliptiques E_N

3.3.1. Le groupe des points rationnels

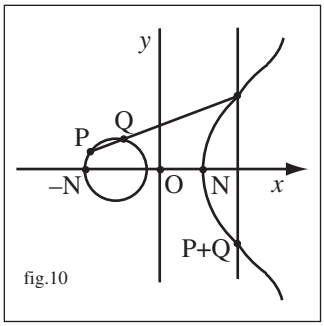

fig.10

Soient N un entier sans facteur carré, E_N la courbe définie par l'équation $y^2 = x(x^2 - N^2)$. Alors l'ensemble $E_N(\mathbf{Q})$ défini par

$$E_N(\mathbf{Q}) := \left\{(\alpha,\beta) \in \mathbf{N^2} \mid \beta^2 = \alpha\left(\alpha^2 - N^2\right)\right\} \cup \{\infty\}$$

peut être muni d'une structure de groupe commutatif selon 1.3.4.4. Soient $a := (-N, 0)$, $b := (0, 0)$, $c := (N, 0)$; on a facilement $a + a = \infty, b + b = \infty$, $c + c = \infty$ et $c = a + b$.

Il suit de cela que $G := \{\infty, a, b, c\}$ est un sous-groupe de $E_N(\mathbf{Q})$ isomorphe à $\frac{\mathbf{Z}}{2\mathbf{Z}} \times \frac{\mathbf{Z}}{2\mathbf{Z}}$. On peut montrer que $G := E_N(\mathbf{Q})_{tors}$, i.e. le sous-groupe des points d'ordre fini de $E_N(\mathbf{Q})$. Il résulte de cela que les points de $E_N(\mathbf{Q})$ d'ordre infini sont exactement les $(\alpha, \beta) \in E_N(\mathbf{Q})$ avec $\beta \neq 0$.

3.3.2. Les beaux résultats

Deux noms sont historiquement attachés aux courbes elliptiques, ce sont L. J. Mordell ([Mo],1922) et A. Weil ([We],1928). Soit $E(\mathbf{Q})$ le groupe commutatif défini comme en 1.3.4.4., alors $E(\mathbf{Q})$ est de type fini , i.e. $E(\mathbf{Q}) \approx F \times \mathbf{Z}^{r_E}$ où F est un groupe commutatif fini, $r_E \geq 0$ est entier. En 1978, B. Mazur ([Ma1]) montre que le groupe F, i.e. le sous-groupe $E(\mathbf{Q})_{tors}$ de torsion de $E(\mathbf{Q})$ est d'ordre borné indépendamment de E. Plus précisément on a $E(\mathbf{Q})_{tors}$ est isomorphe à $\frac{\mathbf{Z}}{n\mathbf{Z}}$ avec $1 \leq n \leq 10$ ou $n = 12$, ou bien isomorphe à $\frac{\mathbf{Z}}{2\mathbf{Z}} \times \frac{\mathbf{Z}}{2m\mathbf{Z}}$ avec $1 \leq m \leq 4$.

3.3.3. Le rang des courbes elliptiques sur $\mathbf{Q}$

Ainsi donc la description de $E(\mathbf{Q})_{tors}$ est réglée par le résultat de Mazur. En ce qui concerne le rang, la conjecture folklorique est que celui-ci peut être aussi grand qu'on veut. Voici les résultats depuis 60 ans.

rang ≥	année	auteur	rang ≥	année	auteur
3	1938	Billing	15	1992	Mestre
4	1945	Wiman	17	1992	Nagao
6	1974	Penney-Pomerance	19	1992	Fermigier
7	1975	Penney-Pomerance	20	1993	Nagao
8	1977	Grunewald-Zimmert	21	1994	Nagao-Kouya
9	1977	Brumer-Kramer	22	1997	Fermigier
12	1982	Mestre	23	1998	Martin-McMillen
14 =	1986	Mestre	24	2000	Martin-McMillen

En 2002 A. Dujella construit une courbe elliptique de rang exactement 15.
L'exemple de Roland Martin et William Mc Millen est de la forme suivante :

$$y^2 + xy + y = x^3 - ax + b$$

où a (resp. b) s'écrit avec environ 40 chiffres (resp. 50 chiffres) en base 10 .

Bien entendu, on est loin des grandes valeurs ; toutefois cette conjecture est confortée par le fait que le résultat est vérifié pour les courbes elliptiques sur un corps de fractions rationnelles à une variable sur un corps fini.

3.4. Les résultats sur les nombres congruents

3.4.1. Remarque.

Caractériser un nombre congruent avec la propriété i) ou ii) de 3.1. semble inaccessible. On peut s'en rendre compte avec les exemples suivants.

Si N = 157, on a $N = \frac{uv}{2}$, $u^2 + v^2 = w^2$, $u,\ v,\ w \in \mathbf{Q}$ et $u,\ v,\ w$ s'écrivent sous la forme $\frac{A}{B}$, A et B nécessitant une vingtaine de chiffres en base 10.

Si N = 101, on a $x^2 + Ny^2 = z^2, x^2 - Ny^2 = t^2, x,\ y,\ z,\ t \in \mathbf{Z}$ avec une vingtaine de chiffres en base 10 .

3.4.2. Les records

En 1983 Tunnell a déterminé tous les nombres congruents ≤ 1 000.
En 1993 Kazunari Noda & Hideo Wada ont déterminé tous les nombres congruents ≤ 10 000.
En 1998 Fidel Ronquillo Nemenzo a déterminé tous les nombres congruents ≤ 40 000.

Bibliographie

[Al] **Almering J. H.** J. *Rational quadrilaleterals*, Indagationes Math. 25 (1963), 192-199, 27 (1965), 290-304.
[Au] **Audin M.** *Arcs en ciel, soucoupes volantes, toupies, courbes elliptiques et tout ça*, dans *La place des mathématiques vivantes dans l'éducation secondaire*, Brochure APMEP nº 168.
[Be] **Berry T. G.** *Points at rational distance from the corners of a unit square*, Ann. Scuola Norm. Sup. Pisa Cl Sci. (4) 17 (1990), 505-529.
Points at rational distance from the vertices of a triangle, Acta Arith. 62 (1992) 391-398.
[BSD] **Birch B.J. and Swinnerton-Dyer H.P.F.** *Notes on elliptic curves I and II,* J. reine.u.ang.Math. 212 (1963), 7-25 et 218 (1965), 79-108.
[CW] **Coates J. and Wiles A.** *On the conjecture of Birch and Swinnerton-Dyer*, Inv. Math. 39 (1977), 223-251.
[Fr] **Fresnel J.** *Méthodes modernes en géométrie*, Hermann (1998) ; *Anneaux*, Hermann (2000).

[Go] **Goldstein C.** *Un théorème de Fermat et ses lecteurs*, Presses universitaires de Vincennes, 1995.
[G] **Guy R. K.** *Unsolved problems in number theory*, Springer Verlag (2004).
[GZ] **Gross B. H. and Zagier D.** *Heegner points and derivatives of L-series*, Inv. Math. 84 (1986) 225-320.
[H] **Henniart Guy** *Nombres congruents, courbes elliptiques et formes modulaires,* Journée annuelle de la SMF 1987.
[Ko] **Koblitz N.** *Introduction to elliptic curves and modular forms*, Springer Verlag (1984).
[Li] **Liu Q.** *Algebraic geometry and arithmetic curves*, Oxford University Press (2002).
[Ma1] **Mazur B.** *Modular curves and the Eisenstein ideal*, Publ. Math. I.H.E.S. 47 (1977) 33-186.
[Mo] **Mordell L. J.** *On the rational solutions of the indeterminate equations of the 3rd an 4th degrees*, Proc. Camb. Phil. Soc., 21 (1922), 179-192.
[Sa] **du Sautoy M.** *La symphonie des nombres premiers*, Éd. Héloïse d'Ormesson (2005).
[Se] **Serre J.-P**. *Cours d'arithmétique*, P.U.F. (1970).
[Si] **Singh S.** *Le dernier théorème de Fermat*, J.-C. Lattès (1998).
[Sil] **Silverberg A.** *Open Questions in Arithmetic Algebraic Geometry*, pre-print IAS/Park City Mathematics Series Volume 00, 0000 (2004 ?).
[Si] **Silverman J.H.** *The arithmetic of elliptic curves*, Springer Verlag (1986).
[Tu] **Tunnell J. B.** *A classical diophantine problem and modular forms of weight 3/2*, Inv. Math. 72 (1983), 323-334.
[T,W] **Taylor R. Wiles A. J.** *Ring-theoretic properties of certain Hecke algebras*, Annals of Math 142 (1995), 553-572.
[We] **Weil A.** *Sur un théorème de Mordell*, Bull. Sci. Math., (2) 54 (1930) 182-191.
[Wi] **Wiles A.** J. *Modular elliptic curves and Fermat's Last Theorem*, Annals of Maths. 142 (1995), 443-551.

un site pour le calcul : http://megrez.math.u-bordeaux.fr/pub/pari/

Triangle pour rire

« Peut-on considérer que le triangle est un tétragone décadent, voire un carré sans envergure ou un cercle qui a mal tourné ? ».

H.S. Tangente nº 24 recensé page 742.