Gentilles fonctions polynomiales de degré 3

Jacques MAROT

14 décembre 2019

Résumé

Lors de l'initiation à l'étude des variations d'une fonction f à l'aide du signe de sa fonction dérivée, il serait bienvenu que les deux fonctions f et f' s'annulent pour des valeurs exclusivement dans $\mathbb{Z}$. Walter Mesnier, enseignant au lycée du Bois d'Amour à Poitiers qui nous avait soumis ce problème dans la défunte rubrique : « Problème de la quinzaine [1] » du site de l'Académie de Poitiers, avait qualifié de gentilles, ces fonctions f définies et dérivables sur $\mathbb{R}$, telle que les solutions des équations $f(x)=0$ et $f'(x)=0$ soient toutes entières. Il est très simple de proposer à nos élèves de gentilles fonctions polynomiales de degré 2, si $f(x)=a(x-x_1)(x-x_2)$, il faut et il suffit que x_1 et x_2 soient des entiers de même parité pour que f soit gentille. Mais si nous recherchons la forme générale d'un polynôme de degré 3 scindé dans $\mathbb{Z}$, tel que son polynôme dérivé soit lui aussi scindé dans $\mathbb{Z}$, on tombe sur un problème moins trivial à résoudre, puisqu'il s'agit de déterminer les solutions dans $\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$ de l'équation diophantienne $12n^2=3p^2+q^2$. La résolution de ce problème aboutit à un module GEOGEBRA permettant de construire toute gentille fonction polynomiale de degré 3, il est disponible sur GEOGEBRA-TUBE à cet URL : https://www.geogebra.org/m/ckdjctak

Au passage, on évoquera les méthodes de résolution d'une équation de degré 3 et le fameux « Casus irreducibilis [2] », qui montre que l'utilisation de radicaux réels n'est pas suffisante pour exprimer les trois racines réelles d'une équation aussi simple que $8x^3-6x-1=0$, et fait donc de la fonction g telle que $g(x)=8x^3-6x-1$, une fonction extrêmement méchante, dont la dérivée est pourtant extrêmement gentille.

Sommaire

1 Solutions d'une équation de degré 3 exprimées à l'aide de la fonction cos

Étant donné $(b,c,d)\in\mathbb{R}\times\mathbb{R}\times\mathbb{R}$ et $f: \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^3+bx^2+cx+d \end{array}$, nous allons rechercher les conditions pour que la courbe $\mathscr{C}_f$ représentative de la fonction f, coupe l'axe des abscisses en trois points distincts.

1. http://ww2.ac-poitiers.fr/math/spip.php?article645
2. Voir Wikipedia : https://en.wikipedia.org/wiki/Casus_irreducibilis

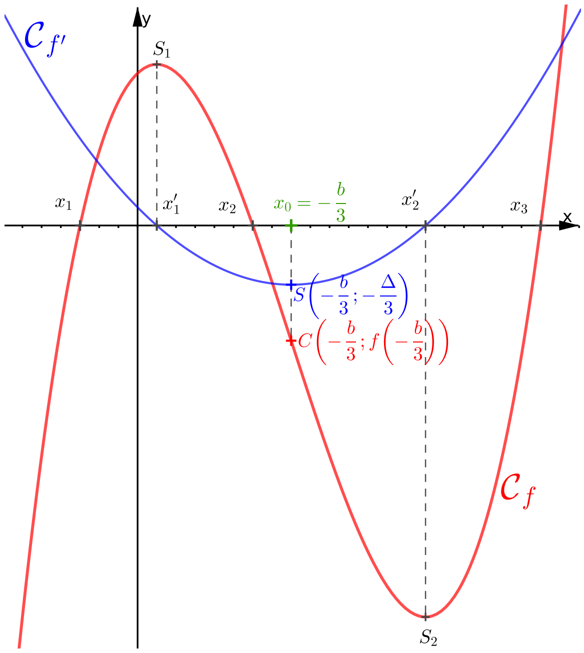


FIGURE 1 – Courbes représentatives de f et f' telles que $f(x)=x^3+bx^2+cx+d$ avec $b^2-3c>0$

1.1 Paramétrisation d'une partie de la cubique $\mathscr{C}_f$ à l'aide de la fonction cos

La fonction dérivée de f est la fonction du second degré f', telle que $f'(x)=3x^2+2bx+c=3\left(x+\frac{b}{3}\right)^2-\frac{\Delta}{3}$, où Δ est le discriminant réduit b^2-3c. Cette dérivée est représentée par une parabole $\mathscr{C}_{f'}$ qui admet pour sommet le point $\mathrm{S}\left(-\frac{b}{3};-\frac{\Delta}{3}\right)$, ce point a même abscisse que le point d'inflexion de $\mathscr{C}_f$, car c'est pour cette valeur que la dérivée seconde f'' s'annule. On en déduit le développement de Taylor suivant de f en $x_0=\frac{-b}{3}$:

$$f(x_0+h)=f(x_0)+f'(x_0)h+f''(x_0)\frac{h^2}{2}+f'''(x_0)\frac{h^3}{6}=f\left(-\frac{b}{3}\right)-\frac{\Delta}{3}h+h^3$$

Cette expression de f met en évidence que $\mathrm{C}\big(x_0; f(x_0)\big)$ est aussi centre de symétrie de $\mathscr{C}_f$, car lorsque h est changé en son opposé, il en est de même de l'écart entre $f(x_0+h)$ et $f(x_0)$.

Si on souhaite que l'équation $f(x)=0$ admette trois solutions réelles distinctes, alors $f'(x)$ doit nécessairement changer deux fois de signe, on doit donc avoir $\Delta>0$, mais cela ne suffit pas. Pour parvenir à une condition suffisante, exprimons notre développement de Taylor avec $h=r.\cos\alpha$, où $r=\frac{2\sqrt{\Delta}}{3}$ est l'écart entre les abscisses $\frac{-b\pm\sqrt{\Delta}}{3}$ des sommets de la cubique $\mathscr{C}_f$:

$$f\left(-\frac{b}{3}+r.\cos\alpha\right)=f\left(-\frac{b}{3}\right)-\frac{\Delta}{3}\times\frac{2\sqrt{\Delta}}{3}\cos(\alpha)+\frac{8\sqrt{\Delta}^3}{27}\cos^3(\alpha)=f\left(-\frac{b}{3}\right)+\frac{8\sqrt{\Delta^3}}{27}\left(\cos^3(\alpha)-\frac{3}{4}\cos\alpha\right)$$

À l'aide de l'identité $\cos^3(\alpha)=\left(\frac{e^{i\alpha}+e^{-i\alpha}}{2}\right)^3=\frac{e^{3i\alpha}+e^{-3i\alpha}}{8}+3\frac{e^{i\alpha}+e^{-i\alpha}}{8}=\frac{1}{4}\cos(3\alpha)+\frac{3}{4}\cos\alpha$, on en déduit :

$$f\left(-\frac{b}{3}+r.\cos\alpha\right)=f\left(-\frac{b}{3}\right)+\frac{r^3}{4}.\cos(3\alpha)$$

Lorsqu'une fonction polynomiale f de degré 3 admet un maximum et un minimum local, comme celles représentées en figure 1 ou 2, par des courbes qui admettent deux sommets S_1 et S_2, une partie de la courbe est assimilable à une courbe de Lissajous. C'est ce qui est détaillé avec plus de précision, sur la partie de la courbe comprise dans le rectangle bleu de la figure 2.

L'équation $f(x)=0$ admet trois solutions réelles distinctes, si et seulement si $\mathscr{C}_f$ coupe trois fois l'axe des abscisses, cet axe doit donc être sécant avec le cercle de centre C et rayon $\frac{r^3}{4}$. Pour que notre équation ait trois solutions distinctes, il faut donc adjoindre à l'inégalité $\Delta>0$ cette autre condition : $\left|f\left(-\frac{b}{3}\right)\right|<\frac{r^3}{4}$.

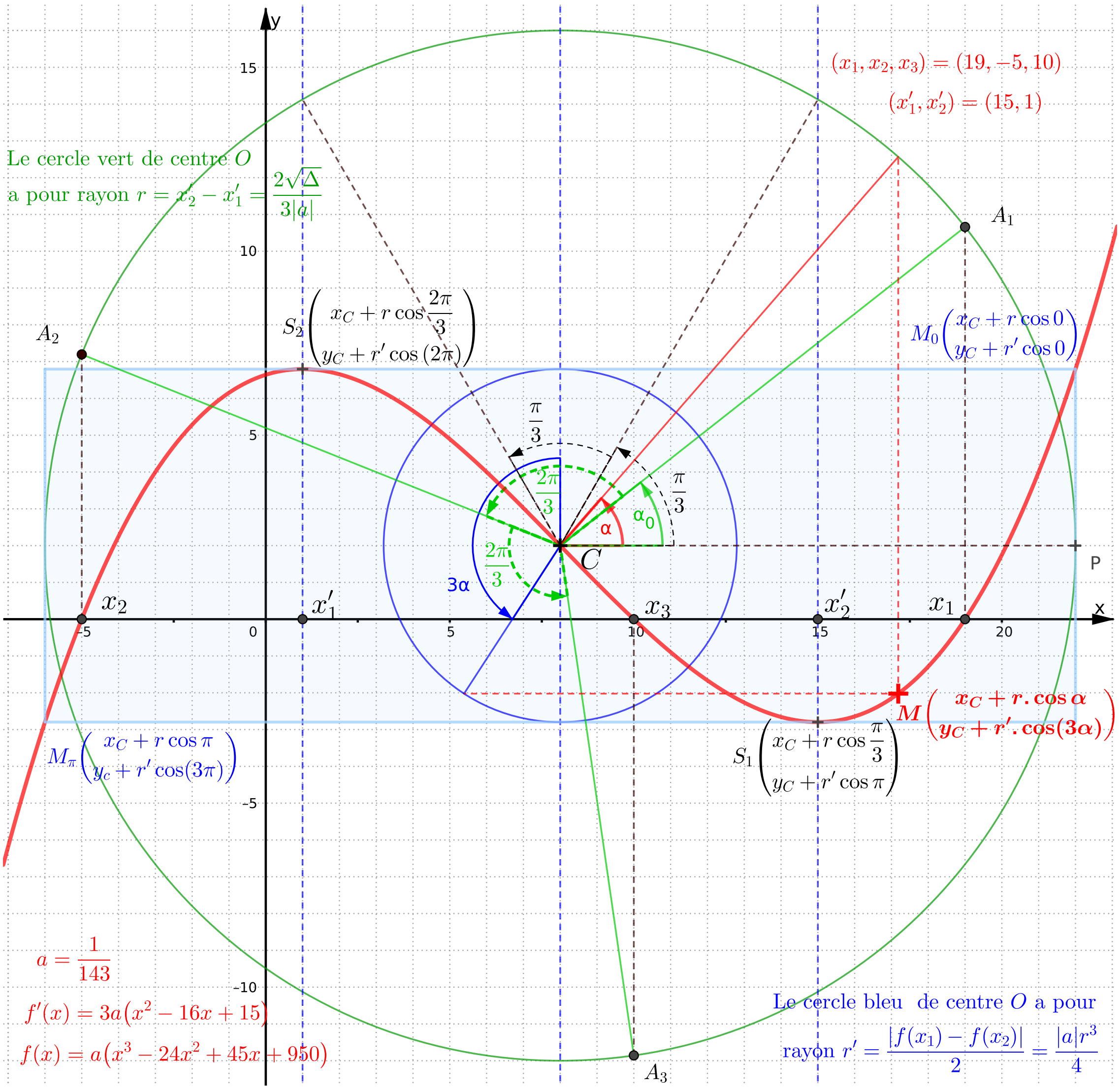


FIGURE 2 – gentille fonction f telle que $f(x)=a(x+5)(x-10)(x-19)$ et $f'(x)=3a(x-1)(x-15)$

Les solutions x_1, x_2 et x_3 de l'équation $f(x)=0$, et les solutions x'_1 et x'_2 de l'équation $f'(x)=0$ peuvent alors s'exprimer à l'aide de $\alpha_0 = \arccos\left(-\dfrac{4}{r^3} f\left(-\dfrac{b}{3}\right)\right)$ et $r = \dfrac{2\sqrt{\Delta}}{3}$:

$$\begin{cases} x'_1 = -\dfrac{b}{3} - \dfrac{r}{2} \\ x'_2 = -\dfrac{b}{3} + \dfrac{r}{2} \end{cases} \qquad \begin{cases} x_1 = -\dfrac{b}{3} + r.\cos\dfrac{\alpha_0}{3} \\ x_2 = -\dfrac{b}{3} + r.\cos\dfrac{\alpha_0 - 2\pi}{3} \\ x_3 = -\dfrac{b}{3} + r.\cos\dfrac{\alpha_0 + 2\pi}{3} \end{cases}$$

Il sera révélé à la fin du paragraphe 2.4, comment a été fabriquée la gentille fonction de cette figure, dont une version animée est consultable sur geogebra-tube à l'adresse indiquée en préambule.

1.2 Remarques générales sur les équations du troisième degré

On a pris l'habitude de dire que les équations algébriques de degré inférieur ou égal à 4 sont résolubles par radicaux, mais il faut bien s'entendre sur la signification de l'expression « résoluble par radicaux », car lorsque qu'un polynôme de $\mathbb{R}[X]$ de degré 3 admet 3 racines réelles distinctes, il nous faut déterminer $\cos\alpha$ pour lequel le réel $\cos(3\alpha)$ s'exprime par des opérations élémentaires sur les coefficients du polynôme. Chercher $\cos\alpha$ tel que $\cos 3\alpha = A$ se ramène au problème de la trisection d'un angle dont $A \in [-1\,;1]$ est le cosinus, pour exprimer la partie réelle de la racine cubique du nombre complexe $A \pm i\sqrt{1-A^2}$. Peut-on parler d'une résolution par radicaux, lorsqu'il s'agit de calculer les racines cubiques d'un nombre complexe non réel tel que $A + iB$? Sauf cas particulier aucune des 3 racines cubiques de $A + iB$ n'est exprimable à l'aide de radicaux, au sens où il s'agirait de racines carrées ou cubiques de nombres réels exprimables par des opérations élémentaires sur les réels A et B. Il serait judicieux de remplacer l'expression « résoluble par radicaux » par « extractions de racines », car les racines cubiques d'un complexe non réel ne sont généralement pas évaluables par des procédés algébriques, c'est ce qui est expliqué en annexe C, en montrant l'impasse dans laquelle on se trouve pour exprimer $\cos\frac{\pi}{9}$ à l'aide de radicaux où n'interviendraient que des nombre réels, ce réel est pourtant solution de $8x^3 - 6x - 1 = 0$.

Par contre, si un polynôme de degré 3 à coefficients réels n'admet que deux racines réelles distinctes dont une de multiplicité 2, ou bien une seule racine réelle et deux autres complexes conjuguées non réelles, il devient possible d'exprimer les racines à l'aide de racines carrées et cubiques, de nombres réels exprimables par des opérations élémentaires sur les coefficients réels du polynôme, on utilise à cet effet les fonctions hyperboliques ch ou sh restreintes à $\mathbb{R}$, à la place de la fonction cos. Le fait que les réciproques de $\mathrm{sh}_{/\mathbb{R}}$ et $\mathrm{ch}_{/[1;+\infty[}$ soient exprimables à l'aide de la fonction logarithme sur $]0;+\infty[$, permet d'exprimer les solutions par radicaux réels, des explications plus détaillées sont fournies en annexe B.

On remarquera aussi que, contrairement aux bruits qui courent dans la littérature mathématique qui ne jure que par la méthode de Cardan, il n'y a nulle nécessité à faire intervenir le corps $\mathbb{C}$ pour calculer les solutions d'une équation de degré 3, lorsqu'elles sont toutes les trois réelles. Les calculs dans $\mathbb{C}$ sont bien entendu dissimulés derrière l'identité d'Euler : $\left(e^{ix}+e^{-ix}\right)^n = 2^n\cos^n(x)$, mais pour $n=3$ l'identité $4\cos^3 x = \cos 3x + 3\cos x$ est aisément vérifiable sans intervention de nombres complexes.

2 Recherche de gentilles fonctions polynomiales de degré 3

2.1 Ramenons le problème à l'équation diophantienne $12n^2 = 3p^2 + q^2$

Nous allons chercher quelle forme doit prendre le triplet $(x_1, x_2, x_3) \in \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$, pour que le polynôme dérivé de $\mathrm{P(X)} = (\mathrm{X}-x_1)(\mathrm{X}-x_2)(\mathrm{X}-x_3)$ n'admette lui aussi que des racines entières. Toute gentille fonction $f : \mathbb{R} \longrightarrow \mathbb{R}$ polynomiale de degré 3 pourra être obtenue à partir d'un polynôme tel que P, en posant $f(x) = a\mathrm{P}(x)$ avec $a \in \mathbb{R}^*$ quelconque.

Étant donné que $\mathrm{P'(X)} = 3\mathrm{X}^2 - 2(x_1+x_2+x_3)\mathrm{X} + (x_1x_2+x_2x_3+x_3x_1)$, nous voudrions qu'il existe un couple $(x'_1, x'_2) \in \mathbb{Z}\times\mathbb{Z}$ tel que : $x'_1 + x'_2 = \dfrac{2(x_1+x_2+x_3)}{3}$ et $x'_1x'_2 = \dfrac{x_1x_2+x_2x_3+x_3x_1}{3}$. Posons $x_\mathrm{C} = \dfrac{x_1+x_2+x_3}{3} = \dfrac{x'_1+x'_2}{2}$, l'hypothèse $\{x'_1, x'_2, x_1, x_2, x_3\} \subset \mathbb{Z}$ implique que $x_\mathrm{C} = (x_1+x_2+x_3)-(x'_1+x'_2)$ est aussi élément de $\mathbb{Z}$, cet entier est l'abscisse du centre de symétrie de la courbe $\mathscr{C}_f$ représentative d'une fonction polynomiale f telle que $f(x) = a.\mathrm{P}(x)$. Soit l'entier naturel $n = \left|x'_2 - x_\mathrm{C}\right| = \left|x_\mathrm{C} - x'_1\right|$, si $a=1$ on peut appliquer les résultats du paragraphe 1.1 avec $r = 2n$, ils permettent de paramétrer une partie de la cubique $\mathscr{C}_f$ de la manière suivante :

$$\left\{\begin{array}{rclcl} x(t) & = & x_\mathrm{C} & + & 2n.\cos t \\ y(t) & = & f(x_\mathrm{C}) & + & 2n^3.\cos(3t) \end{array}\right. \qquad \text{avec } t \in [0;\pi]$$

En permutant éventuellement les indices 1, 2 et 3, et en posant $\alpha = \dfrac{1}{3}\arccos\dfrac{-f(x_\mathrm{C})}{2n^3}$, cette paramétrisation d'une partie de $\mathscr{C}_f$ permet d'exprimer les solutions de $f(x)=0$ et $f'(x)=0$ sous la forme suivante :

$$\left\{\begin{array}{rclclcl} x_1 & = & x_\mathrm{C} & + & 2n.\cos\alpha & & \\ x_2 & = & x_\mathrm{C} & - & n.\cos\alpha & - & n.\sqrt{3}\sin\alpha \\ x_3 & = & x_\mathrm{C} & - & n.\cos\alpha & + & n\sqrt{3}\sin\alpha \end{array}\right. \qquad \left\{\begin{array}{rcl} x'_1 & = & x_\mathrm{C} - n \\ x'_2 & = & x_\mathrm{C} + n \end{array}\right.$$

L'entier x_C peut être choisi arbitrairement, cela se traduit par le fait que toute gentille fonction est dans une classe d'équivalence de fonctions, dont les courbes représentatives dans un repère $\left(\mathrm{O};\vec{\imath},\vec{\jmath}\right)$ sont les translatées les unes des autres, par un vecteur $k\vec{\imath}$ avec $k \in \mathbb{Z}$. Mais on doit rechercher un réel α et des entiers p et q tels que $p = x_1 - x_\mathrm{C} = 2n\cos\alpha$ et $q = x_3 - x_2 = 2n\sqrt{3}\sin\alpha$, qui permettent d'exprimer les racines de la manière suivante :

$$x_1 = x_\mathrm{C} + p \qquad ; \qquad x_2 = x_\mathrm{C} - \frac{1}{2}(p+q) \qquad ; \qquad x_3 = x_\mathrm{C} - \frac{1}{2}(p-q)$$

Ces expressions permettent tout à fait d'envisager les situations avec racine triple ou double :

- on a $x_1 = x_2 = x_3 = x_\mathrm{C}$ si et seulement si $p = q = n = 0$,
- on a $x_3 = x_2 = x_\mathrm{C} \pm n$ si et seulement si $\alpha = 0$ ou $\alpha = \pi$, on a alors $q = 0$, $p = \pm 2n$ et $x_1 = x_\mathrm{C} \pm 2n$,
- on a $x_1 = x_3 = x_\mathrm{C} + n$ si et seulement si $\alpha = \frac{\pi}{3}$, on a alors $p = n$, $q = 3n$ et $x_1 = x_\mathrm{C} - 2n$,
- on a $x_1 = x_2 = x_\mathrm{C} - n$ si et seulement si $\alpha = \frac{2\pi}{3}$, on a alors $p = -n$, $q = 3n$ et $x_3 = x_\mathrm{C} + 2n$.

En toute situation, y compris les quatre cas particuliers que nous venons d'évoquer, (n, p, q) doit toujours vérifier $\left(\dfrac{p}{2n}\right)^2 + \left(\dfrac{q}{2n\sqrt{3}}\right)^2 = 1$, ce qui équivaut à l'équation diophantienne $12n^2 = 3p^2 + q^2$. Il apparait des solutions évidentes de cette équation, déduites des situations avec racines doubles : si $p = \pm 2n$ on obtient $q = 0$, si $p = \pm n$ on obtient $q = \pm 3n$. Les triplets solutions de l'équation diophantienne qui fournissent des polynômes avec racines multiples, sont donc uniquement de la forme $(n, \pm 2n, 0)$ ou $(n, \pm n, \pm 3n)$. Ils permettent d'exprimer à l'aide d'un entier quelconque n dans $\mathbb{Z}$, des polynômes tels que : $\mathrm{P(X)} = (\mathrm{X} - x_\mathrm{C} - 2n)(\mathrm{X} - x_\mathrm{C} + n)^2$ et $\mathrm{P'(X)} = 3(\mathrm{X} - x_\mathrm{C} + n)(\mathrm{X} - x_\mathrm{C} - n)$; le réel x_C peut être racine triple de P et double de P′ si et seulement si $n = 0$.
Les calculs ci-dessous, permettent de vérifier que tout autre solution de l'équation diophantienne qui permet d'exprimer les racines entières d'un polynôme P, est telle que P′ admette lui aussi des racines entières distinctes.

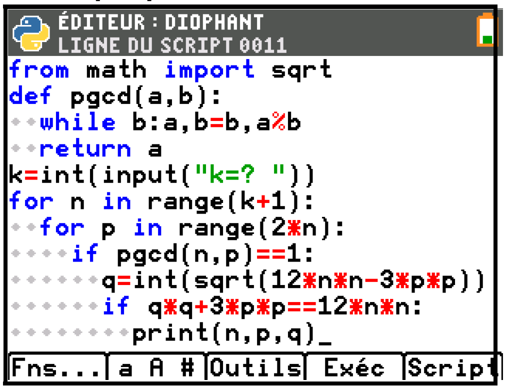
$$x_1x_2 + x_1x_3 = (x_\mathrm{C}+p)(2x_\mathrm{C}-p) = 2x_\mathrm{C}^2 + px_\mathrm{C} - p^2 \quad \text{et} \quad x_2x_3 = x_\mathrm{C}^2 - px_\mathrm{C} + \frac{p^2-q^2}{4} = x_\mathrm{C}^2 - px_\mathrm{C} + p^2 - 3n^2$$

Donc : $\mathrm{P'(X)} = 3\mathrm{X}^2 - 2(x_1+x_2+x_3)\mathrm{X} + x_1x_2 + x_2x_3 + x_3x_1 = 3\mathrm{X}^2 - 6x_\mathrm{C}\mathrm{X} + 3x_\mathrm{C}^2 - 3n^2 = 3(\mathrm{X} - x_\mathrm{C} - n)(\mathrm{X} - x_\mathrm{C} + n)$

2.2 Recherche des premières solutions de l'équation diophantienne sur TI-83-python

Toute solution dans $\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$ de l'équation diophantienne $12n^2=3p^2+q^2$ pourra s'écrire $(dn\,;\,d'p\,;\,d''q)$, avec trois entiers relatifs d, d' et d'' de même valeurs absolues et un triplet $(n,p,q)\in\mathbb{N}\times\mathbb{N}\times\mathbb{N}$ que nous qualifierons de primitif lorsque n, p et q sont premiers entre eux. Pour plus d'efficacité nous allons donc rechercher les seules solutions dans $\mathbb{N}\times\mathbb{N}\times\mathbb{N}$, pour lesquelles on aura $\text{pgcd}(n,p,q)=1$. Avec $n>1$ on ne pourra obtenir que des polynômes avec trois racines distinctes, car nous avons vu que seuls les triplets de la forme $(n,\pm 2n,0)$ ou $(n,\pm n,\pm 3n)$, permettent de former des polynômes avec une racine double, voire triple si $n=0$. Étant donné un entier naturel k à choisir lors de l'exécution sur calculatrice TI-83 du script python ci-dessous, on recherche de manière exhaustive les solutions primitives pour tout $n\in[1\,;\,k]$.

On teste seulement les entiers $p\in[1\,;2n[$ pour lesquels $\text{pgcd}(n,p)=1$, car si trois entiers n, p et q premiers entre eux sont liés par la relation $12n^2=3p^2+q^2$, alors tout facteur premier commun à n et p est aussi nécessairement facteur premier de q. Les deux seuls entiers n et p sont donc premiers entre eux si et seulement si $\text{pgcd}(n,p,q)=1$. On doit ensuite rechercher des couples d'entiers naturels, (n,p) tels que $12n^2-3p^2$ soit le carré parfait d'un entier q, on sélectionne pour cela tous les entiers $p\in[1\,;2n[$ premiers avec n, tels que $\sqrt{12n^2-3p^2}$ soit un entier. Pour $n<7$, ce script affiche pour unique solution $(1;1;3)$, c'est le seul triplet primitif avec $q\neq 0$ qui peut générer des polynômes qui ont une racine double.



Dès que qu'un entier $n\geqslant 7$ permet d'obtenir des solutions, on en voit apparaitre au moins trois distinctes avec ce même entier n. Cela vient du fait que si (n,p,q) est une première solution primitive, l'entier p est la distance entre la racine désignée arbitrairement par x_1 et la moyenne x_C des trois racines, on doit donc pouvoir exprimer au moins deux autres triplets solutions de l'équation diophantienne en remplaçant p par les distances entre x_C et l'une des deux autres racines : $p'=\left|x_2-x_C\right|=\dfrac{|p-q|}{2}$ ou $p''=\left|x_3-x_C\right|=\dfrac{p+q}{2}$. On vérifie ainsi que $\left(n,p',q'\right)=\left(n,\dfrac{|p-q|}{2},\dfrac{3p+q}{2}\right)$ et $\left(n,p'',q''\right)=\left(n,\dfrac{p+q}{2},\dfrac{|3p-q|}{2}\right)$ sont aussi deux autres solutions de l'équation diophantienne : $3\left(\dfrac{p-q}{2}\right)^2+\left(\dfrac{3p+q}{2}\right)^2=3\left(\dfrac{p+q}{2}\right)^2+\left(\dfrac{3p-q}{2}\right)^2=3p^2+q^2=12n^2$.

Nous reviendrons sur ce fait au paragraphe 2.4, on vérifiera que si (n,p,q) est une solution primitive, alors (n,p',q') et (n,p'',q'') sont aussi des solutions primitives qui engendrent une même famille de gentilles fonctions polynomiales du troisième degré. On montrera aussi que parmi ces trois triplets, il y en existe toujours un et un seul dont la dernière composante q, q' ou q'' est multiple de 24, cela permettra d'exprimer plus simplement toute gentille fonction polynomiale de degré 3. Pour $n<60$, il faut $n\in\{7;13;19;31;37;43;49\}$ pour obtenir des solutions, cela nous fournit une première liste de 7 ensembles de 3 triplets primitifs qui permettent d'engendrer chacun, toute une famille de gentilles fonctions obtenues en faisant varier (a,x_C,d) dans $\mathbb{R}\times\mathbb{Z}\times\mathbb{Z}$.

1. $\mathrm{E}_7=\{(7,2,24),(7,11,15),(7,13,9)\}$ fournit les fonctions f telles que :
$$f(x)=a(x-x_C-2d)(x-x_C-11d)(x-x_C+13d)\quad\text{et}\quad f'(x)=3a(x-x_C+7d)(x-x_C-7d)$$
2. $\mathrm{E}_{13}=\{(13,1,45),(13,22,24),(13,23,21)\}$ fournit les fonctions f telles que :
$$f(x)=a(x-x_C-d)(x-x_C-22d)(x-x_C+23d)\quad\text{et}\quad f'(x)=3a(x-x_C+13d)(x-x_C-13d)$$
3. $\mathrm{E}_{19}=\{(19,11,63),(19,26,48),(19,37,15)\}$ fournit les fonctions f telles que :
$$f(x)=a(x-x_C-11d)(x-x_C-26d)(x-x_C+37d)\quad\text{et}\quad f'(x)=3a(x-x_C+19d)(x-x_C-19d)$$
4. $\mathrm{E}_{31}=\{(31,13,105),(31,46,72),(31,59,33)\}$ fournit les fonctions f telles que :
$$f(x)=a(x-x_C-13d)(x-x_C-46d)(x-x_C+59d)\quad\text{et}\quad f'(x)=3a(x-x_C+31d)(x-x_C-31d)$$
5. $\mathrm{E}_{37}=(\{37,26,120),(37,47,99),(37,73,21)\}$ fournit les fonctions f telles que :
$$f(x)=a(x-x_C-26d)(x-x_C-47d)(x-x_C+73d)\quad\text{et}\quad f'(x)=3a(x-x_C+37d)(x-x_C-37d)$$
6. $\mathrm{E}_{43}=\{(43,22,144),(43,61,105),(43,83,39)\}$ fournit les fonctions f telles que :
$$f(x)=a(x-x_C-22d)(x-x_C-61d)(x-x_C+83d)\quad\text{et}\quad f'(x)=3a(x-x_C+43d)(x-x_C-43d)$$
7. $\mathrm{E}_{49}=\{(49,23,165),(49,71,117),(49,94,48)\}$ fournit les fonctions f telles que :
$$f(x)=a(x-x_C-23d)(x-x_C-71d)(x+x_C-94d)\quad\text{et}\quad f'(x)=3a(x-x_C+49d)(x-x_C-49d)$$

Pour une même valeur de n, notre équation diophantienne peut avoir plus de trois solutions, mais toujours en nombre multiple de 3. Pour qu'il y en ait six il faut au minimum $n = 91$, les solutions obtenues sont $(91, 61, 297)$, $(91, 74, 288)$, $(91, 107, 255)$, $(91, 118, 240)$, $(91, 179, 57)$, $(91, 181, 33)$, elles permettent d'exprimer deux fonctions :

$$f_1(x) = a(x - x_C + 179d)(x - x_C - 61d)(x - x_C - 118d)$$

$$f_2(x) = a(x - x_C + 181d)(x - x_C - 74d)(x - x_C - 107d)$$

Ces deux fonctions ont la même fonction dérivée f' telle que : $f'(x) = 3a(x - x_C + 91d)(x - x_C - 91d)$. on peut vérifier que f_1 et f_2 ont bien les mêmes coefficients de degré 3, 2 et 1, qui sont respectivement a, $-3ax_c$ et $a(3x_C^2 - 24843d^3)$, mais leurs coefficients de degré 0 sont nécessairement différents étant donné que f_1 et f_2 sont différentes, sinon leurs décompositions en facteurs irréductibles ci dessus seraient identiques.

Le plus petit entier n qui fournit plus de 6 solutions est 1729 pour lequel il y a 12 solutions, le plus petit entier pour lequel on obtient plus de 12 solutions est $n = 53\,599$, pour lequel il y en a 24. Cette progression géométrique du nombre de solutions : 3 ; 6 ; 12 ; 24 est assez étonnante, d'autant plus que plusieurs heures de calcul n'ont pas permis de trouver un entier n, pour lequel on ait un nombre de solutions égal à 9 ; 15 ; 18 ou 21. Pour parvenir à ces résultats donnés en annexe A, il est proposé un algorithme plus efficace que celui utilisé ci-dessus, car il est inadapté pour de très grands entiers. La méthode utilisée qui consiste à tester tous les termes d'une suite arithmétique, même si celle-ci est bien choisie, demande des temps de calculs extrêmement longs sur calculatrice. Sur ordinateur les temps de calculs sont considérablement raccourcis, mais la méthode utilisée devient quand même inopérante pour les grands entiers, car bien que python soit censé effectuer des calculs arithmétiques exacts sans borne supérieure pour les entiers, il n'en est pas de même avec les nombres réels obligatoirement limités en précision. On tombe alors dans un piège inhérent à tout calcul automatisé dès que n devient trop grand, on constate des inégalités $\mathrm{sqrt}\left(n^2\right) \neq |n|$ arithmétiquement fausses, car la fonction «sqrt» retourne des résultats de type «réels flottants» limités en précision ; il faudra donc prévoir une procédure spéciale pour reconnaitre un carré parfait très grand. Après avoir résolu l'équation diophantienne dans le paragraphe suivant, nous proposons en annexe A un script python optimisé tenant compte de ces remarques, les temps de calcul sont considérablement améliorés et nous découvrirons ainsi, qu'avec $n = 3\,591\,133$ il y a 48 solutions.

2.3 Solution générale de l'équation diophantienne $12n^2 = 3p^2 + q^2$

On a déjà vu que notre équation admet comme solutions évidentes dans $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$, tous les triplets de la forme $(n, n, 3n)$ ou $(n, 2n; 0)$ avec $n \in \mathbb{N}$, et que ces solutions ne permettaient d'obtenir que des polynômes ayant une racine double, voire triple si $n = 0$. Pour obtenir des polynômes avec trois racines entières distinctes, il faut et il suffit que les entiers naturels p et q vérifient $q \neq 0$ et $3p \neq q$, toute solution avec $n > 1$ telle que $\mathrm{pgcd}(n, p, q) = 1$ fournira donc des polynômes avec trois racines simples.

Si (n, p, q) est une telle solution dans $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ de l'équation $3p^2 + q^2 = 12n^2$, alors $n \neq 0$ et $\left(\frac{q}{n} ; \frac{p}{n}\right)$ est solution dans $\mathbb{Q} \times \mathbb{Q}$ de l'équation en (x, y) : $x^2 + 3y^2 = 12$. Réciproquement toute solution dans $\mathbb{Q} \times \mathbb{Q}$ de cette équation exprimée sous la forme $(x, y) = \left(\frac{q}{n}, \frac{p}{n}\right)$, à l'aide de $(n, p, q) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$, fournit ce triplet comme solution de notre équation diophantienne. Le point $A(0; 2)$ sur l'ellipse $\mathscr{E}$ d'équation $x^2 + 3y^2 = 12$ tracée en figure 3, va nous servir de point de départ pour déterminer tous les autres points de coordonnées rationnelles sur $\mathscr{E}$.

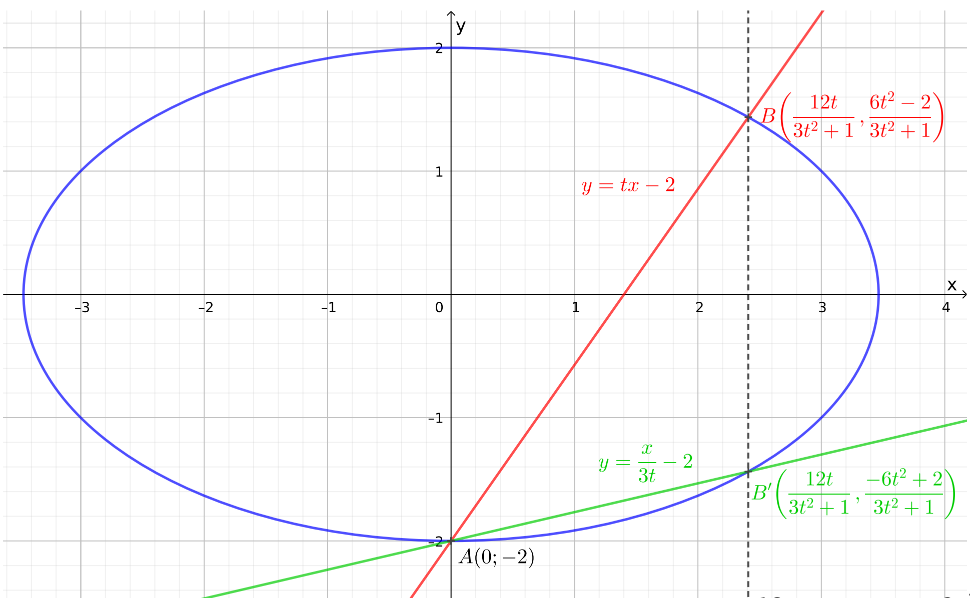


FIGURE 3 – Ellipse admettant les équations paramétriques $x(t) = \dfrac{12t}{3t^2+1}$ et $y(t) = \dfrac{6t^2-2}{3t^2+1}$.

Si un autre point B sur cette ellipse a des coordonnées rationnelles, le coefficient directeur de la droite (AB) qui est $\dfrac{y_B+2}{x_B}$ est lui aussi rationnel. Réciproquement, considérons une droite d passant par A de coefficient directeur rationnel t, elle admet pour équation $y = tx - 2$; en substituant $tx-2$ à y dans l'équation de $\mathscr{E}$ ci-dessus, on peut vérifier que d recoupe $\mathscr{E}$ en un point B à coordonnées rationnelles, car on doit résoudre cette équation de degré 2 $x^2+3(t^2x^2-4tx+4)=12$ équivalente à $x\big((3t^2+1)x-12t\big)=0$. L'abscisse de B est donc $\dfrac{12t}{3t^2+1}$ et son ordonnée est $\dfrac{12t^2}{3t^2+1}-2=\dfrac{6t^2-2}{3t^2+1}$. Si on suppose que t est rationnel, il existe des entiers u et v premiers entre eux, qui permettent d'écrire t et les coordonnées de B sous forme de fractions : $t=\dfrac{u}{v} \Rightarrow x_B=\dfrac{12uv}{3u^2+v^2}$ et $y_B=\dfrac{6u^2-2v^2}{3u^2+v^2}$. Nous n'avons besoin que des seules solutions de l'équation diophantienne dans $\mathbb{N}\times\mathbb{N}\times\mathbb{N}$, on posera donc $(n,p,q)=\big(3u^2+v^2,\left|6u^2-2v^2\right|,12uv\big)$ en utilisant exclusivement des entiers u et v positifs. Pour parvenir à exprimer finalement une solution primitive, il nous faudra diviser ce triplet par pgcd(n,p,q). Si on suppose que u et v sont premiers entre eux, les seuls facteurs premiers communs que peuvent avoir $12uv$ et $3u^2+v^2$ sont 2 lorsque u et v sont impairs, et 3 lorsque celui ci est diviseur de v. Si $v=3v'$ avec $v'\in\mathbb{N}$, après simplification par 3 on obtient la solution : $\big(u^2+3v'^2,\left|6v'^2-2u^2\right|,12v'u\big)$; qui aurait pu être obtenue directement à l'aide de $t=\dfrac{v'}{u}$, on en comprend mieux les raisons sur la figure 3 où l'on a tracé deux droites de coefficients directeurs $t=\dfrac{u}{v}$ et $\dfrac{1}{3t}=\dfrac{v'}{u}$. Toute solution primitive de $12n^2=3p^2+q^2$ peut donc être exprimée en partant d'un couple (u,v) d'entiers premiers entre eux, tel que v ne soit pas multiple de 3. Pour parvenir à exprimer toute solution primitive, il ne nous reste donc à envisager que deux autres possibilités :

- si u et v sont tels que l'un soit pair et l'autre impair, aucun facteur premier de $12uv$ ne peut diviser $3u^2+v^2$, on obtient d'emblée la solution primitive :
$$(n,p,q)=\big(3u^2+v^2\,,\left|6u^2-2v^2\right|\,,12uv\big)$$
- si u et v sont impairs, $6u^2-2v^2$ et $3u^2+v^2$ sont multiples de 4, on peut alors effectuer une simplification par 4, et puisqu' aucun facteur premier de $3uv$ ne peut être diviseur de $3u^2\pm v^2$, on obtient cette solution primitive :
$$(n,p,q)=\left(\frac{3u^2+v^2}{4}\,,\frac{\left|3u^2-v^2\right|}{2}\,,3uv\right)$$

Même les triplets qui engendrent des polynômes avec une racine double peuvent s'exprimer sous l'une de ces deux formes, le triplet $(1,2,0)$ est obtenu avec $(u,v)=(0,1)$ et $(1,1,3)$ est obtenu avec $(u,v)=(1,1)$.

2.4 Conclusion : forme générale des gentilles fonctions polynomiales de degré 3

Nous sommes parvenus à exprimer toutes les solutions primitives de notre équation diophantienne selon deux formes possibles, mais pour engendrer l'ensemble des racines de tout gentil polynôme du troisième degré, nous allons voir qu'il est possible de n'en utiliser qu'une seule. Lorsqu'on utilise des entiers u et v impairs, on obtient des triplets dont la dernière composante $3uv$ est impaire, pourtant dans la liste des solutions du paragraphe 2.2, parmi les trois triplets qui permettent d'engendrer une même famille de gentilles fonctions, il en apparait toujours un dont la troisième composante est multiple de 24. Ceci est une propriété générale, qui va nous permettre d'ignorer cette deuxième forme possible des solutions de l'équation diophantienne.

Éclaircissons d'abord les raisons pour lesquelles les racines d'un gentil polynôme du troisième degré, peuvent être obtenues à partir de plusieurs solutions distinctes de l'équation diophantienne. Si on considère un premier triplet $(n,p,q)\in\mathbb{N}\times\mathbb{N}\times\mathbb{N}$ tel que pgcd$(n,p,q)=1$ et $12n^2=3p^2+q^2$ nous avons déjà constater en 2.2, que $(n,p',q')=\left(n,\dfrac{p-q}{2},\dfrac{3p+q}{2}\right)$ et $(n,p'',q'')=\left(n,\dfrac{p+q}{2},\dfrac{3p-q}{2}\right)$ étaient aussi des solutions dans $\mathbb{N}\times\mathbb{Z}\times\mathbb{Z}$ de l'équation diophantienne, et nous pouvons vérifier que les racines qu'elles engendrent sont les symétriques par rapport à x_C de celles engendrées par (n,p,q). car :

$$x_C+p'=x_C+\frac{p-q}{2}\quad,\quad x_C-\frac{p'+q'}{2}=x_C-p\quad,\quad x_C-\frac{p'-q'}{2}=x_C+\frac{p+q}{2}$$
$$x_C+p''=x_C+\frac{p+q}{2}\quad,\quad x_C-\frac{p''+q''}{2}=x_C-p\quad,\quad x_C-\frac{p''-q''}{2}=x_C+\frac{p-q}{2}$$

Il apparait encore plus de solutions de l'équation diophantienne par changement de signe de n, p, p', p'', q, q' et q'', mais l'ensemble des racines engendrées est insensible aux signes de q, q' et q'', et encore moins au signe de n qui n'intervient que pour exprimer les racines $x_C\pm n$ du polynôme dérivé. Par contre, avec $(n,-p,q)$, on obtient un ensemble de racines symétrique par rapport à x_C de celui obtenu avec (n,p,q), le changement de signe de p' ou p'' permet donc de retrouver les mêmes racines qu'avec (n,p,q).

On peut de plus vérifier que si $\big(n,p,q\big)$ est une solution primitive alors $\big(n,\left|p'\right|,q'\big)$ et $\big(n,p'',\left|q''\right|\big)$ sont aussi des solutions primitives, car si d est un diviseur premier de pgcd(n,p',q') ou de pgcd(n,p'',q''), il doit aussi diviser

$p'+q'=p''+q'''=2p$ et $q'-3p'=3p''-q''=2q$. Mais, puisque $\text{pgcd}(n,p,q)=1$, le seul facteur premier que pourraient avoir en commun n, $2p$ et $2q$ est nécessairement 2, pourtant n ne peut pas être pair, sinon p et q qui doivent être nécessairement de même parité seraient tous les deux impairs. Or dans $\mathbb{Z}/8\mathbb{Z}$ on a $\overline{1}^2\equiv\overline{3}^2\equiv\overline{5}^2\equiv\overline{7}^2$, on aboutirait alors à une contradiction, car avec n pair, la projection dans $\mathbb{Z}/8\mathbb{Z}$ de l'égalité $12n^2=3p^2+q^2$ donnerait $\overline{0}=\overline{4}$.

Finalement nous allons vérifier que parmi les trois solutions primitives (n,p,q), $(n,|p'|,|q'|)$ ou $(n',p'',|q''|)$, il y en a toujours une et une seule dont la dernière composante est paire. En observant les deux formes possibles des solutions de l'équation diophantienne à la fin du paragraphe précédent, on voit que l'un des trois entiers q, q' ou q'' doit de plus être multiple de 24 ; ce qui fournit un excellent moyen d'accélérer la recherche de nos gentilles fonctions à l'aide de moyens numériques. Cela apparait immédiatement si on utilise des entiers u et v de parités différentes, dans cette situation on a du poser $q=12uv$ qui est évidemment multiple de 24 puisque u ou v est pair, et de plus q' et q'' ne peuvent pas être pairs, car par projection de q' et q'' dans $\mathbb{Z}/2\mathbb{Z}$ on obtient $\overline{q'}=\overline{q''}=\overline{3(u^2-v^2)\pm6uv}=\overline{u-v}=\overline{1}$.

Par contre si on utilise des entiers u et v impairs et que l'on doive poser $(p,q)=\left(\dfrac{|3u^2-v^2|}{2},3uv\right)$, il est évident que $q=3uv$ et impair et on a $\{q',q''\}=\left\{\dfrac{3}{4}\left|3u^2-v^2-2uv\right|,\dfrac{3}{4}\left|3u^2-v^2+2uv\right|\right\}$. Si u et v impairs on vérifie alors qu'un et un seul des deux nombres $3(3u^2-v^2\pm2uv)$ est divisible par 8. car en arithmétique modulo 8 les entiers impairs u, v et uv sont nécessairement équivalents à 1, 3, 5 ou 7, on a donc les congruences modulo 8 suivantes : $u^2\equiv v^2\equiv1$. Il ne nous reste donc que quatre cas à envisager :

- si $uv\equiv1$ alors $3u^2-v^2-2uv\equiv3-1-2\equiv0$ et $3u^2-v^2+2uv\equiv3-1+2\equiv4$,
- si $uv\equiv3$ alors $3u^2-v^2-2uv\equiv3-1-6\equiv4$ et $3u^2-v^2+2uv\equiv3-1+6\equiv0$,
- si $uv\equiv5$ alors $3u^2-v^2-2uv\equiv3-1-10\equiv0$ et $3u^2-v^2+2uv\equiv3-1+10\equiv4$,
- si $uv\equiv7$ alors $3u^2-v^2-2uv\equiv3-1-14\equiv4$ et $3u^2-v^2+2uv\equiv3-1+14\equiv0$.

Dans les quatre cas on voit que les deux entiers $\dfrac{3}{4}\left(3u^2-v^2-2uv\right)$ et $\dfrac{3}{4}\left(3u^2-v^2+2uv\right)$ sont bien, de parités différentes, on arrive donc à la conclusion suivante :

> Pour toute gentille fonction polynomiale $f:\mathbb{R}\longrightarrow\mathbb{R}$ de degré 3 il existe :
>
> - deux entiers naturels de parité différentes u et v premiers entre eux tels que 3 ne divise pas v,
> - un couple d'entiers relatifs (x_C,d),
> - un nombre réel a non nul,
>
> qui permettent d'exprimer f sous la forme suivante :
>
> $$f(x)=a\left(x-x_C+d(6u^2-2v^2)\right)\left(x-x_C-d(3u^2-v^2+6uv)\right)\left(x-x_C-d(3u^2-v^2-6uv)\right)$$

On aurait pu dès le départ exhiber le polynôme P unitaire de degré 3 dont les racines entières sont :

$$x_1=x_C-d(6u^2-2v^2)\quad,\quad x_2=x_C+d(3u^2-v^2+6uv)\quad,\quad x_3=x_C+d(3u^2-v^2-6uv),$$

puis vérifier par un simple calcul que $x_1'=x_C+d(3u^2+v^2)$ et $x_2'=x_C-d(3u^2+v^2)$, sont bien les racines de $\mathrm{P}'(\mathrm{X})=3\mathrm{X}^2-2(x_1+x_2+x_3)\mathrm{X}+x_1x_2+x_2x_3+x_3x_1$ en constatant que :

$$x_1'+x_2'=2x_C=\frac{2(x_1+x_2+x_3)}{3}\quad\text{et}\quad x_1'x_2'=x_C^2-d^2(3u^2+v^2)^2=\frac{(x_2+x_3)x_1+x_2x_3}{3}$$

Mais notre étude en dit plus, en affirmant que toutes les fonctions que nous cherchions peuvent s'exprimer sans exception comme nous venons de le faire ci-dessus, même les cas particuliers avec une racine double s'obtiennent en posant $(u,v)=(0,1)$, et ceux avec une racine triple peuvent s'obtenir en posant $d=0$.

Dans l'expression générale d'une gentille fonction polynomiale de degré 3 ci-dessus, le réel a non nul peut être quelconque, cela permet de fixer le centre de symétrie de la courbe représentative de la gentille fonction que l'on souhaite créer, à condition qu'il ait une ordonnée $y_C$non nulle. L'abscisse de ce centre de symétrie est x_C, on doit donc avoir $f(x_C)=y_C$. En posant $p=d(3u^2-v^2)$ et $q=6duv$ on obtient $f(x_C)=2ap(p^2-q^2)$, avec trois racines distinctes on a $p(p^2-q^2)\neq0$, il suffit alors de poser $a=\dfrac{y_C}{2p\left(p^2-q^2\right)}$ pour obtenir $f(x_C)=y_C$.

À titre d'exemple, revenons sur la manière avec laquelle a été choisie l'illustration du paragraphe 1.1 :

(a) On a choisi de placer arbitrairement le centre de symétrie en $C(8;2)$, d'où $x_C=8$.

(b) On a été au plus simple en choisissant $(u,v)=(1,2)$ et $d=1$, on obtient $(n,p,q)=(7,2,24)$ et les racines :
$x_1=x_C+p=10\quad,\quad x_2=x_C-\dfrac{p-q}{2}=19\quad,\quad x_3=x_C-\dfrac{p+q}{2}=-5$

(c) Étant donné le polynôme P tel que $\mathrm{P}(\mathrm{X})=(\mathrm{X}-10)(\mathrm{X}-19)(\mathrm{X}+5)=\mathrm{X}^3-24\mathrm{X}^2+45\mathrm{X}+950$, son polynôme dérivé P′ tel que $\mathrm{P}'(\mathrm{X})=3\left(\mathrm{X}^2-16\mathrm{X}+15\right)$ admet bien pour racines $x_1'=x_C-n=1$ et $x_2'=x_C+n=15$.

(d) On a $\mathrm{P}(8)=286$, on a donc posé $a=\dfrac{2}{286}$ et nous avons représenté la fonction f telle que :

$$f(x)=\frac{1}{143}\left(x^3-24x^2+45x+950\right)\quad\text{et}\quad f'(x)=\frac{3}{143}\left(x^2-16x+15\right)$$

A Recherche des solutions de $12n^2 = 3p^2 + q^2$ avec python

Le script suivant permet d'afficher les solutions pour tous les entiers n compris entre deux bornes qu'il faut entrer à son lancement, Il s'arrête dès que pour un même entier n, on a obtenu un nombre de solutions supérieurs ou égal à s qui est le troisième paramètre demandé. En demandant l'arrêt pour au moins 4 solutions on en obtient 6, cela ne peut pas nous étonner car on sait qu'elles sont en nombre multiple de 3. En demandant l'arrêt pour au moins 9 solutions, on en obtient 12, jamais 9 ; en demandant au moins 15 solutions, le plus petit entier n obtenu est 53 599 pour lequel il y a 24 solutions, et pire encore dès que l'on en demande au moins 25, après un long temps de calcul on obtient 48 solutions pour $n = 3\,591\,133$. On peut aussi vérifier qu'il n' y a aucun entier inférieur à 3 591 133, pour lequel il y aurait un nombre de solutions différent de 3, 6, 12, 24, 48.

On peut donc conjecturer que le nombre de solutions serait toujours de la forme 3×2^a avec $a \in \mathbb{N}$, plusieurs heures de calcul sur ordinateur avec le script ci-dessous légèrement modifié pour ne tester que les entiers écrits sous la forme $n = 3u^2 + v^2$ avec u et v premiers entre eux, de parité différente et tel que 3 ne divise pas v, n'ont pas pu remettre en cause cette hypothèse, mon ordinateur tourne encore pour trouver un nombre de solutions au moins égal à 51.

diophante2.py

```python
from math import *
def sol(n):
  b,c=int(2*n/sqrt(3))+1,0
  for q in range(8,b,8) :
    if gcd(n,q)==1: #"gcd=Greatest Commun Divisor" est à programmer si nécessaire.
      p=int(sqrt(4*n**2-3*q**2))
      while p**2<4*n**2-3*q**2 : p=p+1
      if 4*n**2==p**2+3*q**2:
        c=c+1
        print(c,":(", n ,",", p          , "," , 3*q           ,")",
              "(", n ,",", abs(p-3*q)//2, "," , (3*p+3*q)//2   ,")",
              "(", n ,",", (p+3*q)//2   , "," , abs(3*p-3*q)//2 ,")")
  return 3*c
n=int(input("pour quel entier n minimum cherche-t-on des solutions ? min="))
n=n+1-n%2 #n doit être impair
k=int(input("pour quel entier n maximum cherche-t-on des solutions ? max="))
s=int(input("Combien de solutions au moins  veut-on pour un même entier n ? "))
c=0
while c<=s and n<= k :
  c=sol(n)
  if c:print("Avec n =", n," ,il y a",c,"solutions")
  n=n+2
```

Shell

```
>>> %Run diophante2.py
 pour quel entier n minimum cherche-t-on des solutions ? min=3591133
 pour quel entier n maximum cherche-t-on des solutions ? max=4000000
 Combien de solutions au moins  veut-on pour un même entier n ? 25
 1 :( 3591133 , 7181834 , 136440 ) ( 3591133 , 3522697 , 10840971 ) ( 3591133 , 3659137 , 10704531 )
 2 :( 3591133 , 7179766 , 328200 ) ( 3591133 , 3425783 , 10933749 ) ( 3591133 , 3753983 , 10605549 )
 3 :( 3591133 , 6940298 , 3201816 ) ( 3591133 , 1869241 , 12011355 ) ( 3591133 , 5071057 , 8809539 )
 4 :( 3591133 , 6866422 , 3648504 ) ( 3591133 , 1608959 , 12123885 ) ( 3591133 , 5257463 , 8475381 )
 5 :( 3591133 , 6730634 , 4341720 ) ( 3591133 , 1194457 , 12266811 ) ( 3591133 , 5536177 , 7925091 )
 6 :( 3591133 , 6227978 , 6196104 ) ( 3591133 , 15937 , 12440019 ) ( 3591133 , 6212041 , 6243915 )
 7 :( 3591133 , 5747062 , 7461144 ) ( 3591133 , 857041 , 12351165 ) ( 3591133 , 6604103 , 4890021 )
 8 :( 3591133 , 4962166 , 8993640 ) ( 3591133 , 2015737 , 11940069 ) ( 3591133 , 6977903 , 2946429 )
 9 :( 3591133 , 4865782 , 9150264 ) ( 3591133 , 2142241 , 11873805 ) ( 3591133 , 7008023 , 2723541 )
 10 :( 3591133 , 4665098 , 9458616 ) ( 3591133 , 2396759 , 11726955 ) ( 3591133 , 7061857 , 2268339 )
 11 :( 3591133 , 3173258 , 11160024 ) ( 3591133 , 3993383 , 10339899 ) ( 3591133 , 7166641 , 820125 )
 12 :( 3591133 , 2930422 , 11357496 ) ( 3591133 , 4213537 , 10074381 ) ( 3591133 , 7143959 , 1283115 )
 13 :( 3591133 , 2539658 , 11636376 ) ( 3591133 , 4548359 , 9627675 ) ( 3591133 , 7088017 , 2008701 )
 14 :( 3591133 , 1402634 , 12200520 ) ( 3591133 , 5398943 , 8204211 ) ( 3591133 , 6801577 , 3996309 )
 15 :( 3591133 , 646538 , 12389544 ) ( 3591133 , 5871503 , 7164579 ) ( 3591133 , 6518041 , 5224965 )
 16 :( 3591133 , 536182 , 12405336 ) ( 3591133 , 5934577 , 7006941 ) ( 3591133 , 6470759 , 5398395 )
 Avec n = 3591133  ,il y a 48 solutions

>>>
```

B Équations de degré 3 qui n'ont qu'une ou deux solutions dans $\mathbb{R}$

Il s'agit toujours de résoudre $f(x) = 0$ où f est la fonction polynomiale de degré trois à coefficients réels telle que $f(x) = x^3 + bx^2 + cx + d$. Lorsque le discriminant réduit $\Delta = b^2 - 3c$ est positif, on pourra considérer le cercle $\mathscr{C}$ de rayon $r = \dfrac{4\sqrt{\Delta}^3}{27}$, et centre $\mathrm{C}\left(-\dfrac{b}{3}\,;\, f\left(-\dfrac{b}{3}\right)\right)$. Les situations où notre équation du troisième degré n'admet plus trois solutions réelles distinctes sont les suivantes :

B.1 Le cercle $\mathscr{C}$ est tangent à l'axe des abscisses

Lorsque $f\left(-\dfrac{b}{3}\right)=\pm\dfrac{r^3}{4}$, le cercle $\mathscr{C}$ de la figure 2 n'est plus sécant avec l'axe des abscisses, mais lui est seulement tangent. Il y a un doublon dans les expressions des solutions de $f(x)=0$ du paragraphe 1.1, il n'y a donc que deux solutions qui s'expriment très simplement à l'aide de radicaux :

- lorsque $f\left(-\dfrac{b}{3}\right)>0$, on a $x_1=x_3=\dfrac{-b}{3}+\dfrac{r}{2}$ avec $\alpha_0=-\dfrac{\pi}{3}$;
- lorsque $f\left(-\dfrac{b}{3}\right)<0$, on a $x_2=x_3=\dfrac{-b}{3}-\dfrac{r}{2}$ avec $\alpha_0=0$.

B.2 Le cercle $\mathscr{C}$ ne rencontre plus l'axe des abscisses

On observe sur les graphiques de la figure 4 que le cercle $\mathscr{C}$ ne rencontre plus l'axe des abscisses, lorsque $f\left(-\dfrac{b}{3}\right)\notin\left[-\dfrac{r^3}{4};\dfrac{r^3}{4}\right]$, l'équation $f(x)=0$ n'admet donc plus qu'une seule solution réelle. La fonction arccos définie seulement sur $[-1;1]$ ne peut plus être utilisée, mais on pourra avoir recours à la fonction cosinus hyperbolique $\mathrm{ch}: \begin{array}{ccc}\mathbb{R} & \longrightarrow & \mathbb{R}\\ x & \longmapsto & \dfrac{e^x+e^{-x}}{2}\end{array}$, et l'identité :

$$\mathrm{ch}^3(x)=\left(\frac{e^x+e^{-x}}{2}\right)^3=\frac{e^{3x}+e^{-3x}}{8}+3\frac{e^x+e^{-x}}{8}=\frac{1}{4}\mathrm{ch}(3x)+\frac{3}{4}\mathrm{ch}(x)$$

Pour mettre en évidence l'unique solution de $f(x)=0$, on continuera à poser $r=\dfrac{2\sqrt{\Delta}}{3}$, mais il faudra tenir compte du fait que Argch est définie seulement sur $[1;+\infty[$. On posera alors $\alpha_0=\dfrac{1}{3}\mathrm{Argch}\left(\dfrac{4}{r^3}\left|f\left(\dfrac{-b}{3}\right)\right|\right)$, puis selon le signe de $f\left(\dfrac{-b}{3}\right)$, on utilisera le développement de Taylor vu en 1.1 avec $h=r\,\mathrm{ch}(\alpha)$ ou bien $h=-r\,\mathrm{ch}(\alpha)$:

$$f\left(-\frac{b}{3}+r.\mathrm{ch}(\alpha)\right)=f\left(-\frac{b}{3}\right)+\frac{r^3}{4}\mathrm{ch}(3\alpha)\qquad f\left(-\frac{b}{3}-r.\mathrm{ch}(\alpha)\right)=f\left(-\frac{b}{3}\right)-\frac{r^3}{4}\mathrm{ch}(3\alpha)$$

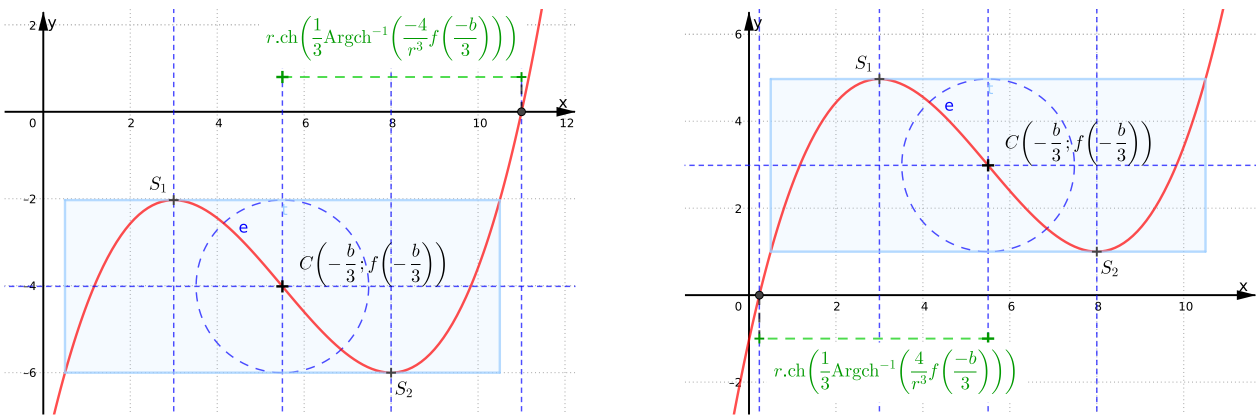


FIGURE 4 – Cubiques sécantes avec l'axe des abscisses en un seul point

- si $f\left(-\frac{b}{3}\right)<0$ avec la première égalité on obtient la solution $-\dfrac{b}{3}+r.\mathrm{ch}(\alpha_0)$, (graphique à gauche en figure 4).
- si $f\left(-\frac{b}{3a}\right)>0$ avec la deuxième égalité on obtient la solution $-\dfrac{b}{3}-r.\mathrm{ch}(\alpha_0)$, (graphique à droite en figure 4).

Dans les deux cas, la solution est exprimable par radicaux réels et ne nécessite plus l'utilisation des fonctions ch et Argch, car on peut montrer que la restriction de ch à $\mathbb{R}^+$ est injective et que sa fonction réciproque est :

$$\mathrm{Argch}: \begin{array}{ccc}[1;+\infty[& \longrightarrow & \mathbb{R}^+\\ y & \longmapsto & \ln\left(y+\sqrt{y^2-1}\right)\end{array}$$

En posant $y=\left|\dfrac{4}{r^3}f\left(\dfrac{-b}{3}\right)\right|$, on a :

$$\mathrm{ch}\left(\frac{1}{3}\mathrm{Argch(y)}\right)=\frac{e^{\frac{1}{3}\mathrm{Argch(y)}}+e^{-\frac{1}{3}\mathrm{Argch(y)}}}{2}=\frac{e^{\frac{1}{3}\ln\left(y+\sqrt{y^2-1}\right)}+e^{-\frac{1}{3}\ln\left(y+\sqrt{y^2-1}\right)}}{2}=\frac{\sqrt[3]{y+\sqrt{y^2-1}}+\sqrt[3]{y-\sqrt{y^2-1}}}{2}$$

B.3 f est strictement monotone sur $\mathbb{R}$

Nous distinguerons les deux cas $\Delta = 0$ et $\Delta < 0$. Lorsque $\Delta = 0$, bien que f' s'annule en $\dfrac{b}{3}$, f est strictement monotone car f' ne change pas de signe. Le développement de Taylor de f en $\dfrac{-b}{3}$ prend alors la forme très simple $f\left(-\dfrac{b}{3}+h\right)=f\left(-\dfrac{b}{3}\right)+h^3$, la seule racine réelle de l'équation $f(x)=0$ est $x_0=-\dfrac{b}{3}+\sqrt[3]{-f\left(-\dfrac{b}{3}\right)}$.

Lorsque Δ est strictement négatif, comme précédemment f' ne change pas de signe et f est strictement monotone. Dans cette situation, le calcul de l'unique solution réelle de l'équation $f(x)=0$ est plus complexe, nous aurons recours à la fonction sinus hyperbolique $\mathrm{sh}: \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \frac{\mathrm{e}^x-\mathrm{e}^{-x}}{2} \end{array}$, qui vérifie l'identité :

$$\mathrm{sh}^3(x)=\left(\frac{\mathrm{e}^x-\mathrm{e}^{-x}}{2}\right)^3=\frac{\mathrm{e}^{3x}-\mathrm{e}^{-3x}}{8}-3\frac{\mathrm{e}^x-\mathrm{e}^{-x}}{8}=\frac{1}{4}\,\mathrm{sh}(3x)-\frac{3}{4}\,\mathrm{sh}(x)$$

Avec $r=\dfrac{2\sqrt{|\Delta|}}{3}$, le développement de Taylor de f en $\dfrac{-b}{3}$ permet les calculs successifs suivants :

$$f\left(-\frac{b}{3}+r.\mathrm{sh}(\alpha)\right)=f\left(-\frac{b}{3}\right)+\frac{r^3}{4}\left(3\,\mathrm{sh}(\alpha)+4\,\mathrm{sh}^3(\alpha)\right)=f\left(-\frac{b}{3}\right)+\frac{r^3}{4}\,\mathrm{sh}(3\alpha)$$

En posant $\alpha_0=\dfrac{1}{3}\mathrm{Argsh}\left(\dfrac{-4}{\mathrm{r}^3}\mathrm{f}\left(\dfrac{-\mathrm{b}}{3}\right)\right)$ on voit que $-\dfrac{b}{3}+r.\mathrm{sh}(\alpha_0)$ est l'unique solution réelle de l'équation $f(x)=0$. Si on pose $y=\dfrac{-4}{r^3}f\left(\dfrac{-b}{3}\right)$, il apparait encore que cette solution réelle s'exprime par radicaux, car on montre que la réciproque de sh est $\mathrm{Argsh}: \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ y & \longmapsto & \ln\left(y+\sqrt{y^2+1}\right) \end{array}$. On obtient donc cette écriture avec radicaux :

$$\mathrm{sh}\left(\frac{1}{3}\mathrm{Argsh(y)}\right)=\frac{\mathrm{e}^{\frac{1}{3}\mathrm{Argsh(y)}}-\mathrm{e}^{-\frac{1}{3}\mathrm{Argsh(y)}}}{2}=\frac{\mathrm{e}^{\frac{1}{3}\ln\left(y+\sqrt{y^2+1}\right)}-\mathrm{e}^{-\frac{1}{3}\ln\left(1+\sqrt{y^2+1}\right)}}{2}=\frac{\sqrt[3]{\sqrt{y^2+1}+y}-\sqrt[3]{\sqrt{y^2+1}-y}}{2}$$

C Casus irreducibilis

On remarque que lorsqu'une équation du troisième degré à coefficients réels n'admet qu'une solution réelle et une ou deux autres complexes conjuguées, ou bien seulement deux solutions réelles mais aucune autre même complexe, elles peuvent s'exprimer à l'aide de racines carrées et cubiques de nombres réels calculables par des opérations élémentaires sur les coefficients de l'équation, l'expression « résoluble par radicaux » prend alors tout son sens. Par contre, il me semblerait préférable de dire que les équations algébriques de degré inférieur ou égal à 4, sont résolubles par extractions de racines, étant entendu que l'extraction de racines doit s'étendre au corps $\mathbb{C}$, même lorsque les coefficients de l'équation sont tous réels, car comme nous l'avons vu, pour les équations du troisième degré à coefficients réels qui admettent trois solutions dans $\mathbb{R}$, il faut faire appel aux fonctions trigonométriques et leurs réciproques pour extraire ces racines!

Les formules de Cardan et l'utilisation de $\mathrm{j}=-\dfrac{1}{2}+\mathrm{i}\dfrac{\sqrt{3}}{2}$ qui est l'une des racines cubiques de l'unité habituellement notée ainsi, nous sont d'aucune aide pour pouvoir exprimer par exemple $\cos\dfrac{\pi}{9}$ par radicaux de nombres réels, ce réel est pourtant solution de l'équation $8x^3-6x-1=0$, (voir figure 5). Pour résoudre cette équation, Jérôme Cardan[3] poserait $x=u+v$ pour écrire l'équation de la façon suivante :

$$8(u+v)^3-6(u+v)-1=0 \qquad ; \qquad 8(u^3+v^3)+24uv(u+v)-6(u+v)-1=0$$

En imposant $4uv=1=(2u)^3\times(2v)^3$, l'équation prend la forme simplifiée $(2u)^3+(2v)^3=1$, tout le génie créateur de Cardan a été alors d'imaginer, que $(2u)^3$ et $(2v)^3$ étaient effectivement d'hypothétiques racines du polynôme $\mathrm{X}^2-\mathrm{X}+1$. C'est ainsi qu'on peut se permettre d'écrire cinq siècles plus tard $\left\{(2u)^3\,;\,(2v)^3\right\}=\left\{\frac{1+\mathrm{i}\sqrt{3}}{2}\,;\,\frac{1-\mathrm{i}\sqrt{3}}{2}\right\}$.

Mais nous sommes confrontés à un « casus irreducibilis » ainsi nommé par les anciens, dit d'une manière plus triviale on tourne en rond. Même si aujourd'hui on sait écrire $\frac{1+\mathrm{i}\sqrt{3}}{2}$ sous la forme $\mathrm{e}^{\mathrm{i}\frac{\pi}{3}}$ et ses trois racines cubiques sous la forme $\mathrm{e}^{\mathrm{i}\frac{(6k+1)\pi}{9}}$, on n'a pas fait avancer la question posée en posant $\{2u\,;\,2v\}=\left\{\mathrm{e}^{\mathrm{i}\frac{(6k+1)\pi}{9}}\,;\,\mathrm{e}^{\mathrm{i}\frac{-(6k+1)\pi}{9}}\right\}$ et $x=u+v=\mathscr{R}e\left(\mathrm{e}^{\mathrm{i}\frac{(6k+1)\pi}{9}}\right)$. On sait tout simplement que $\cos\dfrac{\pi}{9}$ est un réel positif qui est la partie réelle d'une racine cubique de $\frac{1+\mathrm{i}\sqrt{3}}{2}$, qu'on ne sait pas extraire et évaluer sans les moyens de l'analyse numérique.

3. Nom francisé du mathématicien Girolamo Cardano né à Pavie en 1501 : https://fr.wikipedia.org/wiki/Jérôme_Cardan

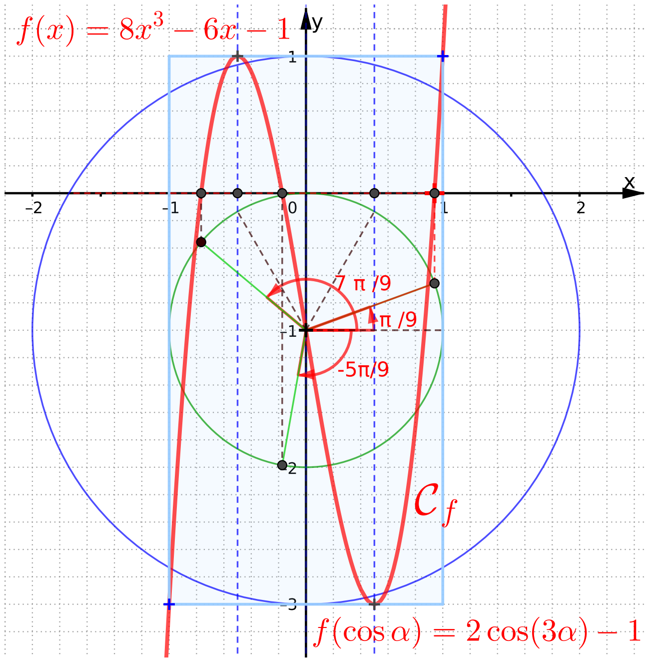


FIGURE 5 – Cubique qui coupe l'axe des x en $x_1 = \cos\frac{\pi}{9}$, $x_2 = \cos\frac{5\pi}{9}$ et $x_3 = \cos\frac{7\pi}{9}$

Serait-il possible d'écrire $\cos\frac{\pi}{9}$ en utilisant les seuls coefficients du polynôme $8X^3-6X-1$, et les opérations du corps $(\mathbb{R},+,\times)$ en y ajoutant le symbole $\sqrt[n]{}$ pour exprimer dans $\mathbb{R}$ des racines carrées, cubiques, quadratiques... ? On sait aujourd'hui qu'il faut répondre à cette question par la négative, c'est confronté à ce type de problème que Jérôme Cardan fit faire un pas de géant aux mathématiques, en introduisant des nombres qu'on qualifiait d'imaginaires au XVIe siècle, et qui sont à l'origine des nombres complexes qui n'ont plus rien de mystérieux aujourd'hui.