Sur une équation diophantienne

Daniel PERRIN

1 Le problème de l'APM

1.1 La question

Le problème abordé ici est posé dans le numéro 543 de *Au fil des maths* (problème 543-3) :

Résoudre dans les entiers relatifs puis dans les entiers naturels :

$$(E_1) \qquad \frac{a}{b+c}+\frac{b}{c+a}+\frac{c}{a+b}=4.$$

Comme souvent avec les problèmes provenant de l'imagination débordante de Vincent Thill, celui-ci est loin d'être évident et je me contenterai ici de donner quelques éléments de solution, renvoyant à la référence [1] pour de plus amples détails. Je démontre ci-dessous que l'équation E_1 admet une infinité de solutions, à la fois dans $\mathbf{Z}$ et dans $\mathbf{N}$, mais c'est au prix de l'utilisation de théorèmes [1] pas du tout triviaux (Mordell, Mazur, Hurwitz). J'ai bien essayé de prouver de manière "élémentaire" l'infinitude des solutions (en exploitant la symétrie de l'équation), mais sans succès. Le seul point non banal de ce qui suit est le calcul explicite d'une solution positive (pas tout à fait triviale) de l'équation.

1.2 Traductions

1.2.1 L'équation E_2

En multipliant par les dénominateurs on obtient l'équation :

$$(E_2) \quad P(a,b,c) := a^3+b^3+c^3-3(b^2c+bc^2+c^2a+ca^2+a^2b+ab^2)-5abc=0.$$

Le polynôme $P(a,b,c)$ est homogène de degré 3 et symétrique en a,b,c. On vérifie que P est un polynôme irréductible sur $\mathbf{Q}$.

1.1 *Remarques.* 1) Les équations étant homogènes, si (a,b,c) est solution de E_1 ou E_2 il en est de même de $(\lambda a,\lambda b,\lambda c)$ où λ est un entier (voire un rationnel). On se contentera donc, dans ce qui suit, de chercher les solutions entières primitives, c'est-à-dire celles qui vérifient $pgcd(a,b,c)=1$. De plus, toute solution rationnelle de l'une des équations fournit une solution entière en multipliant par un dénominateur commun.

1. Mais, après tout, les théorèmes sont faits pour être utilisés !

2) Si (a,b,c) est une solution entière de E_1 c'est aussi une solution de E_2. Inversement, si (a,b,c) est solution de E_2, c'est une solution de E_1, sauf si l'une des sommes $b+c$, $c+a$ ou $a+b$ est nulle.

3) Il est facile de déterminer les solutions de E_2 qui vérifient $b+c=0$, $c+a=0$ ou $a+b=0$. À un scalaire près on trouve seulement $(0,-1,1)$, $(1,0,-1)$, $(-1,1,0)$, $(1,-1,1)$, $(1,1,-1)$ et $(-1,1,1)$.

1.2.2 La courbe elliptique

Vu l'homogénéité de l'équation, ce qu'il est pertinent de considérer ici, ce ne sont pas les solutions de l'équation E_2 dans $\mathbf{Q}^3$, mais, en identifiant les solutions proportionnelles, de les déterminer dans le plan projectif $\mathbf{P}^2(\mathbf{Q})$. L'ensemble des zéros de P dans ce plan est une courbe projective $\mathscr{C}$ de degré 3 et nous allons voir qu'elle est lisse (sans points singuliers). C'est donc une **courbe elliptique**. À ces mots le corbeau ne se sent plus de joie, et le mathématicien non plus ...

1.2 Proposition. *La courbe $\mathscr{C}$ est lisse.*

Démonstration. On calcule :

$$\frac{\partial P(a,b,c)}{\partial a} = 3(a^2-b^2-c^2) - 5bc - 6ca - 6ab = 6a^2 + bc - 3s^2$$

en posant $s=a+b+c$. On a de même $\frac{\partial P(a,b,c)}{\partial b} = 6b^2+ca-3s^2$ et $\frac{\partial P(a,b,c)}{\partial c} = 6c^2+ab-3s^2$. Si (a,b,c) est singulier il annule les dérivées partielles. On vérifie d'abord que les points avec une coordonnée nulle ou deux égales ne sont pas singuliers. Ensuite, par différence on voit que si (a,b,c) est singulier on a $(a-b)(6a+6b-c)=0$ et les équations analogues obtenues par permutation. Mais en ajoutant les équations du type $6a+6b=c$ on obtient $a+b+c=0$, puis $c=0$ et on a gagné.

1.2.3 Un changement de variables

Le changement de variable suivant est innocent (on obtient une courbe isomorphe à $\mathscr{C}$). Je trouve simplement les calculs un peu plus simples avec cette version.

On pose $x=b+c$, $y=c+a$, $z=a+b$ d'où $a=\frac{1}{2}(y+z-x)$, $b=\frac{1}{2}(z+x-y)$ et $c=\frac{1}{2}(x+y-z)$. En projectif on peut même écrire $a=y+z-x$, $b=z+x-y$ et $c=x+y-z$, de sorte que l'on passe aisément d'une forme à l'autre. L'équation en x,y,z est alors :

$$(E_3) \qquad f(x,y,z) := y^2z + yz^2 + z^2x + zx^2 + x^2y + xy^2 - 11xyz = 0$$

ou encore $(yz + zx + xy)(x + y + z) = 14xyz$. Le polynôme f est encore homogène de degré 3 et symétrique. On note Γ la courbe $V(f)$, ensemble des zéros de f dans $\mathbf{P}^2(\mathbf{Q})$. Comme f est symétrique, la courbe Γ est invariante par les permutations du groupe $\mathfrak{S}_3$.

1.3 *Remarque.* Les six points de $\mathscr{C}$ vus ci-dessus correspondent aux points $(0, 1, -1)$, $(-1, 0, 1)$, $(1, -1, 0)$, $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$ de Γ. Ils correspondent aux orbites particulières sous le groupe $\mathfrak{S}_3$ en vertu de la proposition suivante.

1.4 Proposition. *Les orbites des points $(a, b, c) \in \Gamma(\mathbf{Q})$ sous l'action de $\mathfrak{S}_3$ ont toutes six éléments à l'exception des deux orbites à trois éléments suivantes :*

$$\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\} \text{ et } \{(0, 1, -1), (-1, 0, 1), (1, -1, 0)\}.$$

Démonstration. Les orbites exceptionnelles sont celles qui correspondent à des points dont le stabilisateur n'est pas réduit à l'identité. On cherche donc les points (a, b, c) tels que $(\sigma(a), \sigma(b), \sigma(c)) = (a, b, c)$ pour $\sigma \in \mathfrak{S}_3$. Attention, il s'agit d'une égalité dans le plan projectif sur $\mathbf{Q}$ qui s'écrit donc $(\sigma(a), \sigma(b), \sigma(c)) = \lambda(a, b, c)$ avec $\lambda \in \mathbf{Q}^*$. On vérifie aisément que les seuls λ possibles sont ± 1 et que les points en question ont une coordonnée nulle ou deux égales ou deux opposées. Le cas $a = b$ n'a pas de solution rationnelle non nulle et il reste seulement les points annoncés.

1.5 *Remarque.* Si (a, b, c) est un point de $\Gamma(\mathbf{Q})$, il en est de même de $\big(\frac{1}{a}, \frac{1}{b}, \frac{1}{c}\big)$, c'est-à-dire encore de (bc, ca, ab). C'est un autre avantage de cette version.

2 Étude de la courbe Γ

2.1 La théorie

La courbe Γ, comme la courbe $\mathscr{C}$, est une cubique lisse, donc une courbe elliptique. On renvoie à [3] pour les bases de la théorie. On choisit un point d'inflexion de Γ (c'est-à-dire un point qui est tel que la tangente en ce point ne recoupe pas Γ). C'est le cas, par exemple, de $\omega = (1, -1, 0)$, avec la tangente $-x - y + 13z = 0$. On obtient alors une loi de groupe sur Γ de la manière suivante : si m, n sont deux points distincts de Γ on considère le point $m \vee n$ où la droite (mn) recoupe Γ et le point $m + n$ est la troisième intersection de la droite qui joint ω et $m \vee n$ avec Γ. On vérifie que si $m \vee n = (a, b, c)$ on a $m + n = (b, a, c)$. Si m est égal à n on remplace (mn) par la tangente en

m et on obtient ainsi le point $m \vee m$ puis le double $2m$ en échangeant a et b. On verra que ces deux procédures permettent de construire de nouveaux points à partir de points déjà connus.

Dans cette procédure, le point ω est élément neutre de la loi et l'opposé de (a, b, c) est (b, a, c). La loi est évidemment commutative, on montre qu'elle est associative, de sorte qu'on a un groupe abélien. Ce groupe est de type fini (théorème de Mordell), donc isomorphe à $\mathbf{Z}^r \oplus T$ où r est ce qu'on appelle le rang de la courbe et où T (le sous-groupe de torsion) est fini. De plus, un théorème (non trivial) de Mazur assure que T est de cardinal ≤ 16 (voir [3] th. 7.5). On en déduit le résultat suivant :

2.1 Théorème. *Les points de* Γ *sur* $\mathbf{Q}$ *sont en nombre infini. Il en est de même de ceux de* $\mathscr{C}$*. L'équation* E_1 *a une infinité de solutions entières non deux à deux proportionnelles.*

Démonstration. Il suffit de montrer que r est ≥ 1 et pour cela que $|\Gamma|$ n'est pas réduit à son sous-groupe de torsion, donc de cardinal > 16. Or, outre les six points vus ci-dessus on a aussi $(2, 3, 10)$ et ses six permutés et $(3, 10, 15)$ et ses six permutés, ce qui donne au moins 18 points [2].

2.2 Corollaire. *L'équation* E_1 *a une infinité de solutions entières positives non deux à deux proportionnelles.*

Démonstration. Cela résulte d'un résultat d'Hurwitz ([2] Satz 13) : si une courbe elliptique Γ a une infinité de points rationnels, ces points sont partout denses dans chaque composante connexe de Γ. Or, les solutions (a, b, c) de E_1 ou E_2 rationnelles positives correspondent aux points $(x, y, 1)$ de Γ qui vérifient les trois conditions $y - 1 < x < y + 1$ et $x + y > 1$ (il s'agit de la zone grisée sur la figure 1) et cet ouvert coupe la courbe réelle Γ (par exemple au point $x = y = \dfrac{9 + \sqrt{65}}{4}$) de sorte qu'il y a bien une infinité de solutions rationnelles de Γ vérifiant ces conditions.

2.3 *Remarque.* Il y a une infinité de solutions positives mais il n'est pas évident d'en exhiber une, comme on va le voir ci-dessous.

2. Attention, les points $(2, 3, 10)$ et $(3, 10, 15)$ sont à coefficients positifs, mais ce sont des points de Γ, pas de $\mathscr{C}$. Les points correspondants de $\mathscr{C}$ sont $(11, 9, -5)$ et $(11, 4, -1)$.

2.2 Calcul du double d'un point et de la somme de deux points

2.2.1 Le double

Soit $m = (a, b, c)$ un point de la courbe $\Gamma = V(f)$. On va calculer son double $2m = (x, y, z)$.

Pour cela on calcule les dérivées partielles en m :

$$A = \frac{\partial f}{\partial x}(a, b, c) = b^2 + c^2 + 2ca + 2ab - 11bc$$

$$B = \frac{\partial f}{\partial y}(a, b, c) = c^2 + a^2 + 2ab + 2bc - 11ca$$

$$C = \frac{\partial f}{\partial z}(a, b, c) = a^2 + b^2 + 2bc + 2ca - 11ab$$

La tangente T à Γ en m a pour équation $Ax + By + Cz = 0$ que l'on résout en $z = -\frac{A}{C}x - \frac{B}{C}y$. On coupe Γ par T. On obtient, en remplaçant z par son expression en x, y un polynôme homogène de degré 3 en x, y : $\alpha x^3 + \beta x^2 y + \gamma x y^2 + \delta y^3$. Ce polynôme admet (a, b) comme racine double et la dernière racine (x, y) se calcule avec les fonctions symétriques : $(x, y) = (-b^2\delta, a^2\alpha)$. Il reste à calculer α et δ. On trouve $\alpha = -AC + A^2$, $\delta = -BC + B^2$. On obtient ainsi (en n'oubliant pas d'échanger x et y) :

2.4 Proposition. *Si $m = (a, b, c)$ est un point de Γ le point $2m = (x, y, z)$ est donné par les formules :*

$$x = a^2AC(A - C),\ y = b^2BC(C - B),\ z = -b^2AB(C - B) - a^2AB(A - C)$$

2.2.2 L'addition

L'addition de deux points $m = (a, b, c)$ et $m' = (a', b', c')$ se calcule comme ci-dessus, on trouve la sécante $Ux + Vy + Wz = 0$ avec $U = bc' - b'c$, $V = ca' - c'a$ et $W = ab' - a'b$, puis le troisième point comme $x = VW(W - V)bb'$, $y = WU(U - W)aa'$ et $z = -bb'UV(W - V) - aa'UV(U - W)$. On obtient ainsi :

2.5 Proposition. *Soient $m = (a, b, c)$ et $m' = (a', b', c')$ deux points distincts de Γ. Avec les notations ci-dessus, le point $m + m' = (x, y, z)$ est donné par les formules :*

$$x = WU(U-W)aa',\ y = VW(W-V)bb',\ z = -bb'UV(W-V)-aa'UV(U-W).$$

2.6 *Remarques.* 1) Attention, les calculs ci-dessus ne sont valables que si les coordonnées des points sont non nulles. Sinon, il faut être plus soigneux et éviter les divisions par 0, voir ci-dessous pour des précisions.

2) On suppose que $m = (2, 3, 10)$. On trouve alors $A = -169$, $B = -44$ et $C = 47$ et on obtient, après simplifications, $2m = (x, y, z) = (2^3 \times 3 \times 13 \times 47, -7 \times 11 \times 47, 5 \times 11 \times 13) = (14664, -3619, 715)$.

3) Attention, on obtient ainsi de nouveaux points, mais pour en déduire l'infinitude de $\Gamma(\mathbf{Q})$ il faut prouver qu'ils sont distincts.

2.2.3 Des points de torsion

Les points avec une coordonnée nulle forment un sous-groupe de Γ :

2.7 Proposition. *On pose $e = (1, 0, 0)$. On a alors les formules suivantes : $2e = (1, 0, -1)$, $3e = (0, 0, 1)$, $4e = (0, 1, -1)$, $5e = (0, 1, 0)$ et $6e = \omega = (1, -1, 0)$ (l'élément neutre du groupe). Les six points considérés forment un sous-groupe de Γ, isomorphe à $\mathbf{Z}/6\mathbf{Z}$.*

2.8 *Remarques.* 1) Si a, b, c sont non nuls, on notera les formules $(1, 0, 0) + (a, b, c) = (ab, bc, ca)$, $(0, 1, 0) + (a, b, c) = (ca, ab, bc)$ et $(0, 0, 1) + (a, b, c) = (bc, ca, ab)$.

2) On a aussi, avec $m = (a, b, c)$, $2e + m = (b, c, a)$ et $4e + m = (c, a, b)$.

3) On a enfin avec $m = (2, 3, 10)$, $e + m = (30, 6, 20) = (15, 3, 10)$. À permutation près on retrouve l'autre point rencontré ci-dessus.

2.2.4 Les résultats de Bremner et Macleod

La courbe $\mathscr{C}$ est étudiée dans l'article [1]. Bremner et Macleod passent par la forme "canonique" de l'équation $y^2 = x^3 + 109x^2 + 224x$. Voici leur résultat :

2.9 Théorème. *1) Le groupe de torsion de $\mathscr{C}$ ou Γ est le groupe isomorphe à $\mathbf{Z}/6\mathbf{Z}$ vu en 2.7.*

2) Le rang de $\mathscr{C}$ ou Γ est égal à 1.

Démonstration. 1) Le groupe Γ contient le sous-groupe isomorphe à $\mathbf{Z}/6\mathbf{Z}$ vu ci-dessus, qui est contenu dans le groupe de torsion T. Le théorème de Mazur (voir [3] *loc. cit.*) ne laisse que trois possibilités : $T \simeq \mathbf{Z}/6\mathbf{Z}$ ou $T \simeq \mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ ou $T \simeq \mathbf{Z}/12\mathbf{Z}$. Dans le deuxième cas on aurait plusieurs éléments d'ordre 2, dans le troisième un élément d'ordre 4. On conclut alors avec le lemme suivant :

2.10 Lemme. *Le groupe Γ n'a pas d'autre élément d'ordre 2 que $(0, 0, 1)$ et il n'a pas d'éléments d'ordre 4.*

Démonstration. Si m est d'ordre 2 on a $2m = \omega = (1, -1, 0)$ et cela signifie que la tangente en m a pour direction $x + y = 0$. Elle est donc invariante par la symétrie $(x, y, z) \mapsto (y, x, z)$, comme Γ, de sorte que m est fixe par cette symétrie. Mais on a vu dans la preuve de 1.4 que l'unique point rationnel de Γ avec $x = y$ est $(0, 0, 1)$.

Si m était un élément d'ordre 4, la tangente en m recouperait Γ à l'origine, donc serait (en affine) de la forme $y = \lambda x$. En coupant Γ par cette droite et en éliminant la solution $x = 0$ on obtient l'équation du second degré

$$\lambda(\lambda + 1)x^2 + (\lambda^2 - 11\lambda + 1)x + \lambda + 1$$

et dire que la droite est tangente signifie que cette équation a une racine double, donc que son discriminant est nul. On aurait donc $\lambda^4 - 26\lambda^3 + 115\lambda^2 - 26\lambda + 1 = 0$ mais on vérifie que cette équation n'a pas de solution rationnelle (elle serait entière et nécessairement égale à ± 1).

2) Je ne vais pas montrer ici l'assertion sur le rang qui nous entraînerait trop loin. Il suffit de vérifier que la fonction L associée à la courbe a un zéro d'ordre 1 au point $s = 1$ (le logiciel *Pari* fait ça très bien), ce qui assure que la courbe est de rang 1. (C'est la conjecture de Birch et Swinnerton-Dyer, qui, dans le cas du rang 1, est vraie en vertu des résultats de Kolyvagin.)

2.2.5 Les itérés d'un générateur

Bremner et Macleod donnent un générateur de la partie libre de Γ : sous la forme canonique il s'agit de $(-4, 28)$, pour $\mathscr{C}$ cela donne $p = (11, 4, -1)$ et pour Γ, $m = (3, 10, 15)$. Ils affirment aussi que $9p$ un point de $\mathscr{C}$ est à coefficients positifs. Grâce aux formules ci-dessus on le vérifie aisément, en calculant d'abord $9m$ avec le logiciel SAGE :

2.11 Proposition. *À partir du point* $m = (3, 10, 15)$ *de* Γ *on obtient* $2m = (14664, 715, -3619)$,

$$4m = (-164522506539145, 196932807438576, -13030716467024711),$$

$$x(8m) = -24540189524859611982582644591490410981079061033251771148236682 56$$

$$y(8m) = 17109594007255635975548181369786884042165267252213492451045039 85$$

$$z(8m) = -56542945251126914281095352993207832740799500248513925316036689$$

$$x(9m) = 41248744472058697085059064167596864978309517527133584614904575465 0$$

$$15648101827615$$

$$y(9m) = 15885041478667486369981256762229122763848086322772704531864807289163$$

$$z(9m) = 191351933902876166269149126585145312311157305638537402696309772369890426669333578.$$

On retourne ensuite à $\mathscr{C}$ pour calculer $9p$. On obtient ainsi :

2.12 Théorème. *Si p est le point de $\mathscr{C}$ donné par $p = (11, 4, -1)$, $9p$ est le point (a, b, c) avec*

$$a = 154476802108746166441951315019919837485664325669565431700026634898253202035277999$$

$$b = 3687513179412999982719781156522547482549297996897197099628313747163722463405557 9$$

$$c = 437361267792869725786125260237139015281653755816161361862143799337842346777203 6$$

Le point (a, b, c) est une solution de E_1 dans $\mathbf{N}^3$.

2.13 *Remarque.* Voir ci-dessous la sortie SAGE attestant qu'on a bien une solution de E_1. On notera que la plus petite des coordonnées, c, a tout de même 79 chiffres. D'après [1] c'est le minimum pour les points de $\mathscr{C}$ à coordonnées positives.

```
Entrée [110]: xe
Out[110]: 154476802108746166441951315019919837485664325669565431700026634898253
          202035277999

Entrée [111]: ye
Out[111]: 368751317941299998271978115652254748254929799689719709962831374716372
          24634055579

Entrée [112]: ze
Out[112]: 437361267792869725786125260237139015281653755816161361862143799337842
          3467772036

Entrée [113]: xe/(ye+ze)+ye/(ze+xe)+ze/(xe+ye)
Out[113]: 4
```

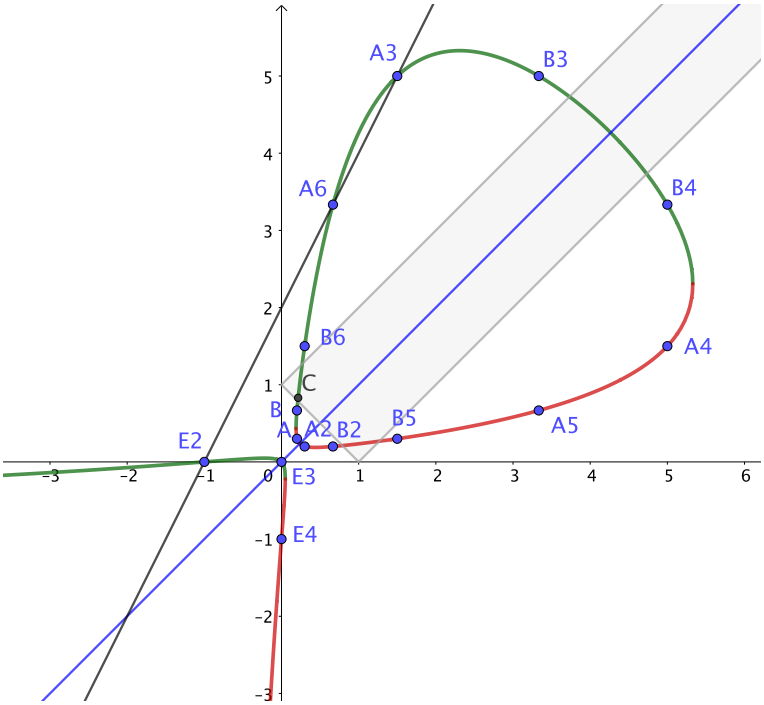

FIGURE 1 – La courbe Γ

2.3 La courbe Γ

Sur la figure 1, les points $E2$, $E3$, $E4$ correspondent à $2e$, $3e$ et $4e$, le point A est le point $(0.2, 0.3)$ qui correspond en projectif à $(2, 3, 10)$ et les Ai sont ses permutés, le point B correspond à $m = (3, 10, 15)$ et les Bi à ses permutés. La zone grisée correspond à la zone des points à coordonnées positives de la courbe $\mathscr{C}$. Le point C est (approximativement) le point $9m$ qui est dans cette zone.

Références

[1] A. Bremner & A. Macleod, *An unusual cubic representation problem*, Annales Mathematicae et Informaticae, 43 (2014), 29-41.

[2] A. Hurwitz, *Über ternäre diophantische Gleichungen dritten Grades*, Vierteljahrschrift der Naturforschenden Gesellschaft in Zürich, Vol. 62 (1917), 207-229.

[3] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 2009.

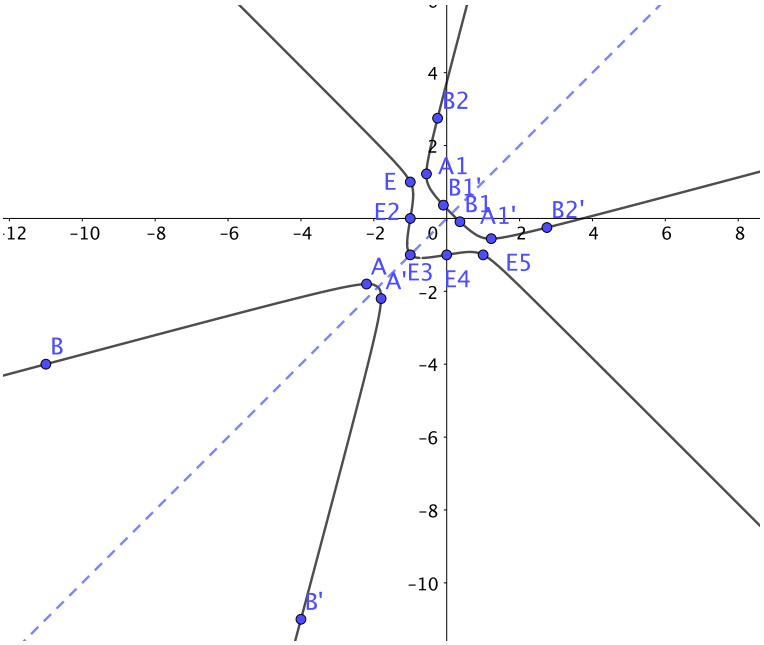

FIGURE 2 – La courbe $\mathscr{C}$