Triangles : aire, périmètre et isométries

Daniel PERRIN

Le point de départ de ce texte est une question posée dans le numéro 152 des *Chantiers de pédagogie mathématique* de l'APMEP : *Deux triangles ayant la même aire et le même périmètre sont-ils forcément isométriques ?*

On verra dans ce qui suit que cette question en apparence anodine est reliée à de nombreux domaines : topologie, calcul différentiel, algèbre, théorie des nombres, algorithmique et, bien entendu, géométrie. On verra aussi qu'elle mène à des questions dont la solution n'est pas triviale. Il y a d'ailleurs un aspect fascinant quand on aborde naïvement un tel problème. En effet, on s'aperçoit rapidement (avec l'aide d'Internet) que la littérature regorge de questions très liées à celle qu'on étudie, mais jamais totalement équivalentes [1]. Cela laisse donc un espace où chacun peut s'adonner au plaisir de la recherche.

Un mot sur une utilisation éventuelle de ce thème dans l'enseignement secondaire. Il présente à mon avis plusieurs charmes :

• Il montre ce qu'est vraiment une **activité mathématique** : poser des problèmes, explorer, expérimenter, conjecturer, formuler, prouver, etc.

• Il montre tout l'intérêt des logiciels de géométrie et de l'algorithmique.

• Il fait le lien avec les mathématiques vivantes et actuelles.

Nul doute cependant qu'une utilisation pertinente de cette situation dans une classe nécessite de dominer largement le sujet. Cela ne fait que confirmer l'importance de la culture pour la formation des professeurs.

1 Réponse à la question : non, évidemment

C'est la réponse qui m'est venue aussitôt en lisant l'énoncé de la question posée.

1.1 Pourquoi est-ce évident ?

L'idée intuitive est très simple : l'espace des triangles modulo isométries est de dimension [2] trois, autrement dit, modulo isométries, un triangle dépend de trois paramètres, donc un élément de cet espace ne peut certainement pas être déterminé par deux seulement (ici l'aire et le périmètre) : deux

1. C'est le cas ici du problème des triangles de Héron.

2. Cette idée de dimension, au sens des variétés, mais que l'on peut comprendre intuitivement au sens de décompte des paramètres, me semble importante pour la formation en géométrie des futurs professeurs.

paramètres déterminent en général une famille de dimension 1 de triangles, autrement dit, une "courbe de triangles", voir Figure 4.

Pour les plus vieux d'entre nous, cette idée est reliée aux cas d'isométrie des triangles qui, tous, affirment justement qu'un triangle est déterminé, à isométrie près, par trois paramètres indépendants (deux longueurs et un angle ou deux angles et une longueur, ou trois longueurs). D'ailleurs, un exercice classique qu'on proposait encore dans les années 1950 consistait à "résoudre" un triangle, autrement dit à le déterminer [3] à isométrie près (en calculant les longueurs de ses côtés ou en le construisant) à partir de trois données (indépendantes), par exemple les longueurs des hauteurs, ou deux angles et une médiane, ou toute autre combinaison que l'on imaginera (une véritable mine pour les professeurs de l'époque !).

On trouvera des détails sur ce thème de l'espace des triangles dans la Partie V de mon livre en préparation *Géométrie projective et applications aux géométries non euclidiennes et euclidienne*. Voir sur ma page web :

`http://www.math.u-psud.fr/~perrin/`.

1.2 Dimension

Bien entendu, tel que je l'ai dit, l'argument n'est pas dans le bon sens : les cas d'isométrie disent que trois paramètres suffisent à assurer l'isométrie de deux triangles, mais pas que deux sont insuffisants, même si l'exemple de deux longueurs nous en convainc aisément. Pour conclure, il faut montrer que l'espace des triangles est vraiment de dimension 3. Voilà comment je propose de voir les choses, de manière intuitive toujours.

On considère l'espace $\mathcal{T}$ de tous les triangles. Un triangle c'est trois points A, B, C, que l'on peut voir comme des points de $\mathbf{R}^2$, $A = (a_1, a_2)$, etc. L'espace $\mathcal{T}$ est donc $(\mathbf{R}^2)^3$, qui est de dimension 6. Plus précisément, si l'on se limite aux vrais triangles, il faut supposer que les points A, B, C ne sont pas alignés (cela écarte aussi le cas où deux d'entre eux coïncident). L'espace $\mathcal{T}$ est donc un ouvert de $\mathbf{R}^6$, défini en coordonnées par $\begin{vmatrix} a_1 & a_2 & 1 \\ b_1 & b_2 & 1 \\ c_1 & c_2 & 1 \end{vmatrix} \neq 0$.

Le groupe G^+ des déplacements du plan, lui, est de dimension 3. Intuitivement c'est clair car on peut voir ses éléments comme composés d'une translation (déterminée par un vecteur, donc de dimension deux) et d'une rotation de centre fixé (déterminée par son angle, donc de dimension 1). En

3. Dans certains cas il peut y avoir plusieurs solutions, mais toujours en nombre fini. Un bel exemple : résoudre un triangle connaissant son périmètre et les rayons de ses cercles inscrit et circonscrit.

multipliant les déplacements par une réflexion fixée, on voit que les isométries négatives ne constituent qu'une copie de G^+ et la dimension du groupe G de toutes les isométries est encore égale à 3. L'espace qui nous intéresse est le quotient $\mathcal{Q}$ de $\mathcal{T}$ par la relation d'équivalence associée à l'opération de G : deux triangles sont considérés comme égaux dans le quotient s'il existe une isométrie qui passe de l'un à l'autre. On a alors une projection naturelle $p : \mathcal{T} \to \mathcal{T}/G$, dont les fibres $p^{-1}(t)$ sont essentiellement isomorphes à G. En effet, $p^{-1}(t)$ est l'ensemble des triangles isométriques à un triangle donné T d'image t, et il est formé des $g(T)$ pour $g \in G$. L'idée intuitive qu'il faut avoir dans cette situation, commune aux géomètres différentiels, algébriques ou autres, c'est qu'on a une formule $\dim \mathcal{T} = \dim G + \dim(\mathcal{T}/G)$. On a donc ici $\dim \mathcal{T}/G = 6 - 3 = 3$.

Un mot sur cette formule de dimension : elle ressemble beaucoup au théorème noyau-image : $\dim E = \dim f(E) + \dim \operatorname{Ker} f$ pour une application linéaire f. Elle y ressemble trop pour que ce soit un hasard. De fait, si les objets considérés sont des variétés, on va pouvoir, grâce au calcul différentiel, passer des applications à leurs différentielles, qui sont linéaires, et se ramener à ce théorème.

Bien entendu, comme toujours en mathématiques, pour avoir un théorème il faut des hypothèses, mais cette formule doit être notre guide. Pour le reste, l'intendance suivra, comme disent les militaires.

En vérité, le quotient $\mathcal{Q}$ n'est pas tout à fait l'espace qui nous intéresse. En effet, il faut encore considérer comme équivalents deux triangles obtenus par permutation comme ABC et ACB, autrement dit considérer le quotient de $\mathcal{Q}$ par le groupe symétrique $\mathfrak{S}_3$. Mais comme ce groupe est fini, cela ne change pas la dimension.

1.3 La topologie seulement ?

Tout de même, la mise au point de cet argument n'est pas si facile. Si l'on est un peu paresseux, et qu'on ne veut pas rentrer dans la problématique des dimensions des variétés et du calcul différentiel, on peut tenter de rester au niveau topologique. On commence par montrer que l'espace quotient $\mathcal{Q} = \mathcal{T}/G$, muni de la topologie quotient, est homéomorphe à un ouvert de $\mathbf{R}^3$. Pour cela on part de $\mathcal{T}$, partie de $\mathbf{R}^6$ formée des "vrais" triangles, et on considère l'application Φ qui associe au triangle ABC le triplet des longueurs $a = BC$, $b = CA$, $c = AB$. L'image de Φ est l'ouvert $\mathbf{R}^3$ des (a, b, c) qui sont > 0 et vérifient les inégalités triangulaires $|b - c| < a < b + c$. Il mérite qu'on lui donne un nom :

1.1 Définition. *On note $\mathcal{U}$ l'ouvert de $\mathbf{R}^3$ formé des triplets (a,b,c) vérifiant :*

$$a,b,c>0 \quad \text{et} \quad |b-c|<a<b+c.$$

L'application Φ "passe au quotient" en $\overline{\Phi}:\mathcal{T}/G\to\mathcal{U}$, qui est continue par définition même de la topologie quotient. Pour voir que c'est un homéomorphisme il suffit d'exhiber la réciproque, donc de fabriquer un triangle de côtés a,b,c donnés. On associe [4] à (a,b,c) le triangle ABC avec $B=(0,0)$, $C=(a,0)$ et $A=(x,y)$ avec $x=\dfrac{c^2+a^2-b^2}{2a}$ et $y=\sqrt{c^2-x^2}$. Cette application étant évidemment continue, on voit que $\mathcal{Q}$ est homéomorphe à $\mathcal{U}$.

On a, par ailleurs, l'application continue $\Psi:\mathcal{U}\simeq\mathcal{Q}\to\mathbf{R}^2$, qui à un triangle modulo isométrie associe son aire et son périmètre et une réponse positive à la question initiale signifierait que cette application est **injective**. On sent bien qu'une telle application ne peut exister (car $\mathcal{U}$ est un ouvert de $\mathbf{R}^3$, donc plus gros que $\mathbf{R}^2$), mais ce résultat si intuitif n'est pas trivial [5], c'est le théorème dit *d'invariance du domaine* de Brouwer qui affirme qu'il n'y a pas d'application continue injective d'un ouvert non vide de $\mathbf{R}^n$ dans $\mathbf{R}^p$ avec $p<n$ (voir par exemple Greenberg *Lectures on algebraic topology*, Benjamin, 1967). La preuve de ce résultat nécessite des techniques de topologie algébrique qui nous entraîneraient trop loin et il vaut mieux aborder les choses d'une autre manière.

1.2 *Remarque.* La description de $\mathcal{Q}$ grâce aux longueurs va nous servir tout au long de ce texte. On notera qu'elle permet aussi de montrer qu'on ne perd pas de dimension en passant au quotient par les permutations. En effet, celles-ci opèrent aussi sur $\mathcal{U}$ en permutant les longueurs et le quotient $\mathcal{Q}/\mathfrak{S}_3$ est homéomorphe à $\mathcal{U}/\mathfrak{S}_3$. Mais, si dans l'ouvert $\mathcal{U}$ on considère l'ouvert $\mathcal{U}'$ formé des (a,b,c) avec $a<b<c$, il est clair que cet ouvert s'injecte dans $\mathcal{U}/\mathfrak{S}_3$ et on voit facilement qu'il est homéomorphe à son image, de sorte que le quotient est bien de dimension 3. Dans la suite nous oublierons donc les passages au quotient par les permutations pour nous intéresser essentiellement aux espaces [6] $\mathcal{Q}$ ou $\mathcal{U}$.

4. Le lecteur vérifiera les détails.

5. C'est souvent le cas en topologie, penser au théorème de Jordan et cela montre que les paresseux sont toujours punis...

6. Au passage, le lecteur pourra résoudre trois questions naturelles, mais pas forcément très intéressantes : Que se passe-t-il si l'on utilise deux longueurs et un angle au lieu de trois longueurs ? La propriété est-elle vraie modulo similitude (cette fois le quotient est bien de dimension 2) ? Et dans les géométries non euclidiennes ?

2 Une preuve par le calcul différentiel

2.1 Un peu d'algèbre pour calculer les paramètres

Avant d'aller plus loin, il faut écrire les deux paramètres considérés, aire et périmètre, de manière efficace. Cela va d'ailleurs permettre de prendre en compte les permutations des sommets du triangle.

On considère un triangle ABC on note a, b, c les longueurs de ses côtés ($a = BC$, $b = CA$, $c = AB$) et p son périmètre, $p = a + b + c$. Pour l'aire, on rappelle la formule de Héron [7], voir 8.3.1 pour une preuve :

$$\mathcal{A} = \sqrt{p'(p'-a)(p'-b)(p'-c)} \tag{1}$$

où p' est le **demi-périmètre** de ABC. Cette formule s'écrit encore [8] :

$$16\mathcal{A}^2 = (a+b+c)(b+c-a)(c+a-b)(a+b-c) = p(p-2a)(p-2b)(p-2c)$$

ou encore, en développant le tout :

$$16\mathcal{A}^2/p = -p^3 + 4(bc+ca+ab)p - 8abc.$$

Se donner $\mathcal{A}$ et p revient donc à se donner p et s :

$$s := (bc+ca+ab)p - 2abc = bc^2 + b^2c + ca^2 + c^2a + ab^2 + a^2b + abc,$$

avec la formule $16\mathcal{A}^2 = 4sp - p^4$. On voit apparaître ici les deux autres fonctions symétriques élémentaires de a, b, c : $q = bc + ca + ab$ et $r = abc$ et on a $s = qp - 2r$. Rappelons qu'alors a, b, c sont les trois racines de l'équation $(X-a)(X-b)(X-c) = X^3 - pX^2 + qX - r = 0$.

2.1 *Remarque.* La formule suivante nous sera plusieurs fois utile :

$$4s - p^3 = (b+c-a)(c+a-b)(a+b-c).$$

À partir de maintenant, on pourra remplacer l'aire, si besoin est, par la fonction s. On peut préciser l'objet de nos investigations :

7. Il s'agit de Héron d'Alexandrie, qui vivait au premier siècle après J.-C. et qui a donné le premier exemple de triangle à côtés entiers $13, 14, 15$, dont l'aire 84 est aussi entière. C'est ce qu'on appelle maintenant les triangles de Héron, voir 8.3.2.

8. Cette formule suggère le changement de variables $\alpha = b + c - a$, $\beta = c + a - b$ et $\gamma = a + b - c$. Nous y reviendrons.

2.2 Définition. *Soient p, s deux nombres réels. On note $\mathcal{Q}_{p,s}$ l'ensemble des triangles de périmètre p et d'invariant s (i.e. d'aire donnée par $16\mathcal{A}^2 = 4sp - p^4$), modulo isométries. Cet espace est en bijection avec l'ensemble $\mathcal{U}_{p,s}$ des triplets $(x, y, z) \in \mathbf{R}^3$ vérifiant :*

$$x, y, z > 0, \quad |y-z| < x < y+z, \quad x+y+z = p \quad \text{et} \quad (yz+zx+xy)p-2xyz = s.$$

On notera $\mathcal{U}_{p,s}(k)$ la partie de $\mathcal{U}_{p,s}$ formée des $(x, y, z) \in k^3$ où k désigne un sous-corps ou un sous-anneau[9] *de $\mathbf{R}$.*

Commentaire. Notre objectif est maintenant l'étude de $\mathcal{Q}_{p,s}$ ou de son avatar $\mathcal{U}_{p,s}$. Voici quelques-unes des questions que nous aborderons (il y en a bien d'autres) :

0) La question initiale (APM) est de savoir s'il y a plusieurs éléments dans $\mathcal{Q}_{p,s}$ (qui ne soient pas permutés les uns des autres).

1) En fait, il y a une première question bien naturelle : pour quels p, s existe-t-il des triangles de périmètre p et d'aire $(4sp - p^4)/16$, autrement dit, quand $\mathcal{Q}_{p,s}$ est-il non vide ? La réponse sera donnée en 5.5.

2) Une deuxième question, qui donne évidemment la réponse à (APM) : l'ensemble $\mathcal{Q}_{p,s}$, s'il est non vide, est-il infini ? La réponse est positive, voir 2.4, et nous décrirons précisément cet ensemble comme une composante d'une courbe elliptique, voir 5.5.

3) Nous nous demanderons aussi s'il y a des triangles isocèles dans $\mathcal{Q}_{p,s}$ et combien, voir 4.1.

4) Enfin, nous pourrons aussi chercher s'il y a des triangles d'invariants p, s dont les côtés sont rationnels, voire entiers. Cette question nous entraînera dans l'univers magique des courbes elliptiques et nous verrons qu'il reste quelques questions ouvertes (en tous cas pour moi) sur ce sujet.

2.2 Une preuve *via* les fonctions implicites

Donnons d'abord une définition :

2.3 Définition. *Deux triangles non isométriques sont dits* **frères**[10] *s'ils ont même aire et même périmètre.*

Le but de ce paragraphe est de montrer le résultat suivant :

2.4 Théorème. *Soit $T = ABC$ un triangle non équilatéral. Il existe une infinité de triangles frères de T. Autrement dit, avec les notations du paragraphe précédent, si p, s sont les invariants de T, l'ensemble $\mathcal{Q}_{p,s}$ associé est infini.*

9. On s'intéressera essentiellement aux cas $k = \mathbf{Q}$ ou $k = \mathbf{Z}$.

10. Normal puisqu'ils ont même pér(imètre) et même mère, je veux dire même aire.

Démonstration. Par rapport à la tentative purement topologique de 1.3, on utilise ici un outil supplémentaire, le calcul différentiel, essentiellement le théorème des fonctions implicites ou d'inversion locale. Pour des preuves plus élémentaires, patience.

On note a, b, c les longueurs des côtés de T. Comme il n'est pas équilatéral, on peut supposer, par exemple, qu'on a $b \neq c$. On paramètre les (vrais) triangles XYZ par l'ouvert $\mathcal{U}$ de $\mathbf{R}^3$ formé des longueurs de leurs côtés :

$$\mathcal{U} = \{(x, y, z) \in \mathbf{R}^3 \ \mid \ x, y, z > 0 \quad \text{et} \quad |y - z| < x < y + z \ \}.$$

Intuitivement, comme $\mathcal{U}$ est de dimension 3, on doit pouvoir trouver des triangles en imposant non seulement p et s (périmètre et aire), mais une des longueurs. Ici, on va imposer x.

On considère donc l'application $\Psi : \mathcal{U} \subset \mathbf{R}^3 \to \mathbf{R}^3$ qui à (x, y, z) associe (x, p, s). Cette application est polynomiale, donc C^∞, et son déterminant jacobien est égal à :

$$\begin{vmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ y^2+z^2+yz+2x(y+z) & z^2+x^2+zx+2y(z+x) & x^2+y^2+xy+2z(x+y) \end{vmatrix},$$

c'est-à-dire à $(y - z)(y + z - x)$. Au point (a, b, c) il est donc non nul. Le théorème des fonctions implicites montre alors que l'image de $\mathcal{U}$ contient un voisinage de $\Psi(a, b, c) = (a, p, s)$. Elle contient donc tous les points (x, p, s) pour x assez voisin [11] de a. Cela signifie qu'il existe $(x, y, z) \in \mathcal{U}$ avec $\Psi(x, y, z) = (x, p, s)$, autrement dit des triangles T avec même périmètre et même aire que T, mais pas le même x. Comme il y a une infinité de x possibles, il y a une infinité de tels triangles non isométriques.

2.5 *Remarques.* 1) Nous rencontrerons beaucoup d'autres preuves de ce théorème dans la suite. Certaines, comme celles-ci, se contenteront de donner un résultat d'existence, d'autres seront explicites en donnant des moyens de calculer les longueurs des côtés de triangles frères, voir par exemple 5.5 ou 6.11.

2) Nous verrons en 5.4 que le triangle équilatéral doit être écarté car c'est le seul [12] qui n'admet pas de triangle frère.

2.6 *Exercice.* Montrer l'existence de triangles frères sans utiliser les fonctions implicites (ni un calcul explicite !). (En tirant $z = p - x - y$ on se ramènera à montrer qu'une fonction f, disons de classe C^1, définie sur un ouvert non

11. Voir Figure 4 avec $x = BC'$.
12. Trop fier, le triangle équilatéral.

vide de $\mathbf{R}^2$ et à valeurs dans $\mathbf{R}$ ne peut être injective. Pour cela on étudiera les fonctions $x \mapsto f(a,x)$ et $y \mapsto f(b,y)$ au voisinage d'un point où la dérivée par rapport à x est non nulle et on montrera qu'elles atteignent toutes deux certaines valeurs.)

2.3 Variante : apparition d'une cubique plane

Cette variante est très voisine, mais peut sembler plus simple car on n'y utilise pas directement les fonctions implicites. Partons pour simplifier d'un triangle de côtés a, b, c avec $0 < a < b < c$ et $c < a+b$ et cherchons un triangle de côtés x, y, z, vérifiant les mêmes inégalités, tels que $a+b+c = p = x+y+z$ et $(bc + ca + ab)p - 2abc = s = (yz + zx + xy)p - 2xyz$, mais distincts des précédents (i.e. $(x,y,z) \neq (a,b,c)$). Dans ce cas les deux triangles de côtés a, b, c et x, y, z auront même périmètre p et même aire $\mathcal{A}$ (donnée par $16\mathcal{A}^2 = 4sp - p^4$) mais ne seront pas isométriques.

Géométriquement, il s'agit de trouver sur la courbe [13] $\mathcal{G}_{p,s}$ de $\mathbf{R}^3$ d'équations

$$x + y + z = p \quad \text{et} \quad 2xyz - (yz + zx + xy)p + s = 0$$

un point (x,y,z) assez voisin de (a,b,c) pour vérifier les mêmes inégalités, mais distinct. La courbe $\mathcal{G}_{p,s}$ est la section d'une surface cubique par un plan, donc une cubique plane. On peut d'ailleurs se ramener au cas d'une cubique $\Gamma_{p,s}$ dans le plan des (x,y) en éliminant $z = p - x - y$ et on obtient :

$$(*) \qquad F(x,y) := 2xy(x+y) - p(x^2 + y^2 + 3xy) + p^2(x+y) - s = 0.$$

Il s'agit donc de montrer qu'il y a des points $n = (x,y)$ au voisinage de $m = (a,b)$ sur cette courbe. Cela semble presque évident, en vérité, si la courbe est bien digne de ce nom. Il faut tout de même être prudent, car il peut y avoir des points isolés sur une cubique (par exemple, sur la courbe d'équation $x^3 + x^2 + y^2 = 0$, le point $(0,0)$ est isolé, voir aussi 5.2 ci-dessous). Pour éliminer ce cas, il faut savoir qu'un tel point isolé est nécessairement un point singulier de la courbe $F(x,y) = 0$, c'est-à-dire un point vérifiant $\dfrac{\partial F}{\partial x}(m) = \dfrac{\partial F}{\partial y}(m) = 0$. C'est d'ailleurs ce que dit le théorème des fonctions implicites, encore lui, qui affirme que si l'une des dérivées partielles est non nulle on peut tirer une variable en fonction de l'autre et avoir ainsi une vraie courbe. Dans le cas de la courbe $F = 0$, on obtient les équations $4ab + 2b^2 - 2pa - 3pb + p^2 = 4ab + 2a^2 - 2pb - 3pa + p^2 = 0$. Par différence, on trouve soit $a = b$, soit $a + b = c$ et ces deux cas sont exclus car le triangle n'est ni aplati, ni isocèle.

13. Comme son nom l'indique, cette courbe nous servira de guide dans la suite.

Si l'on répugne décidément au calcul différentiel, on peut aussi voir $(*)$ comme une équation du second degré en y, avec x comme paramètre, et résoudre cette équation [14]. Notons $\Delta(x)$ son discriminant. Pour $x = a$, cette équation admet la solution b, de sorte que l'on a $\Delta(a) \geq 0$. Si le discriminant est > 0, il l'est encore pour x voisin de a et on a des solutions y. Le seul problème est donc le cas où $\Delta(a)$ est nul. On peut calculer ce discriminant [15] et on trouve $\Delta(a) = (b-c)^2(a-b-c)^2$: il est bien non nul avec les hypothèses faites sur a, b, c (ni aplati, ni isocèle).

Pour conclure sur ce point, on voit qu'il y a une sorte de morale : quelle que soit la méthode envisagée, elle conduit à montrer qu'on est dans un cas assez générique (déterminant jacobien non nul, point de la cubique non singulier, discriminant de l'équation du second degré non nul) et que cela provient des hypothèses faites sur a, b, c.

3 Des preuves élémentaires

Les preuves ci-dessus font appel au théorème des fonctions implicites ou requièrent un calcul un peu délicat. Elles ne sont donc pas faciles, même pour des étudiants de licence [16]. Nous donnons ci-dessous d'autres approches plus élémentaires que l'on peut proposer à des lycéens. Dans un premier temps nous montrons simplement l'existence de paires de triangles non isométriques admettant même aire et même périmètre. Dans un second temps nous donnons une preuve élémentaire du théorème 2.4.

3.1 Aire constante et valeurs intermédiaires

L'idée est de disposer d'une famille continue de triangles de même aire. On utilise pour cela la formule $2\mathcal{A} = base \times hauteur$. On part d'un triangle A_0BC, avec $BC = a$ et on appelle h la hauteur issue de A_0. On a donc $2\mathcal{A}(A_0BC) = a \times h$. Notons que si l'on suppose $h > a$ on est sûr que a est le plus petit côté de A_0BC. Pour faire bonne mesure, on supposera $h > 2a$. À partir de ce triangle on en a toute une famille qui ont la même aire en gardant $[BC]$ fixe et en faisant varier A sur la parallèle à (BC) passant par A_0.

On construit ensuite d'autres triangles de même aire en changeant C en C', aligné avec B et C avec $BC' = a' > a$ et avec un sommet A' qui décrit la

14. Cela revient à transformer les fonctions implicites en fonctions explicites grâce à l'algèbre !

15. Mais ce n'est pas si facile, sauf avec un logiciel approprié.

16. Sans compter qu'il faut connaître la formule de Héron.

parallèle à (BC) située à la distance h' avec $a \times h = a' \times h'$. (Il est facile de construire cette droite à la règle et au compas grâce à Thalès.) On suppose que a' n'est pas trop grand : $a < a' < a\sqrt{2}$. Alors, on a $h' = \dfrac{ah}{a'} > a'$ (car $a'^2 < 2a^2 < ah$). Cette précaution assure que pour cette deuxième famille de triangles aussi, c'est a' le plus petit côté.

On a donc ainsi deux familles de triangles : les ABC (la famille du haut) et les $A'BC'$ (celle du bas), tous de même aire. On va montrer qu'il y a un triangle de la famille du haut et un de la famille du bas qui ont même périmètre (et toujours même aire). Cela donnera la réponse négative à la question, puisque leurs petits côtés sont différents.

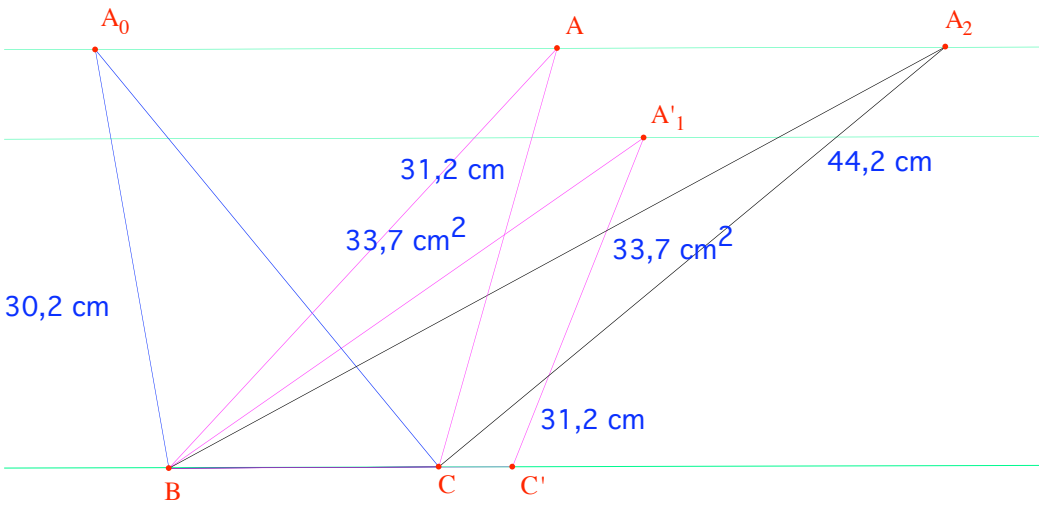

FIGURE 1 – Les deux familles de triangles de même aire

Pour cela, la remarque de base est que, si l'on déplace le point A ou A' sur la parallèle à (BC) et si l'on s'éloigne, le périmètre tend vers l'infini. On part donc d'un triangle du haut, par exemple A_0BC. Il a un périmètre p_0. On peut trouver un triangle du bas, disons A'_1BC' qui a un périmètre plus grand, disons $p_1 > p_0$. Mais on peut trouver un triangle A_2BC du haut avec un périmètre encore plus grand, disons $p_2 > p_1 > p_0$.

Maintenant, quand A varie entre A_0 et A_2, le périmètre de ABC est une fonction continue [17] de A (ou de son abscisse), qui passe nécessairement par p_1 en vertu du théorème des valeurs intermédiaires. Le triangle ABC ainsi

17. Que l'on peut l'expliciter à la demande d'un professeur ou d'un élève em...bêtant.

obtenu a même aire et même périmètre que A'_1BC', mais il ne lui est pas isométrique.

3.2 Variante avec une ellipse

Dans la méthode précédente, on peut éviter l'argument de valeurs intermédiaires, qui fait appel à l'analyse, en utilisant une ellipse[18], donc un peu plus de géométrie. On reprend la situation précédente, en partant, pour simplifier, d'un triangle isocèle ABC, avec $BC = a$ et $h = 2a$ (un triangle du haut). Le théorème de Pythagore donne $AB = AC = \dfrac{a\sqrt{17}}{2}$. On choisit alors C' sur (BC) avec $BC' = a' = 2a$ et on considère des triangles $A'BC'$ de hauteur $h' = a$ qui ont donc même aire que ABC (triangles du bas). Pour trouver un triangle du bas de même périmètre que ABC, il faut trouver A' tel que $A'B + A'C' + BC' = AB + AC + BC$, donc $A'B + A'C' = a(\sqrt{17} - 1)$.

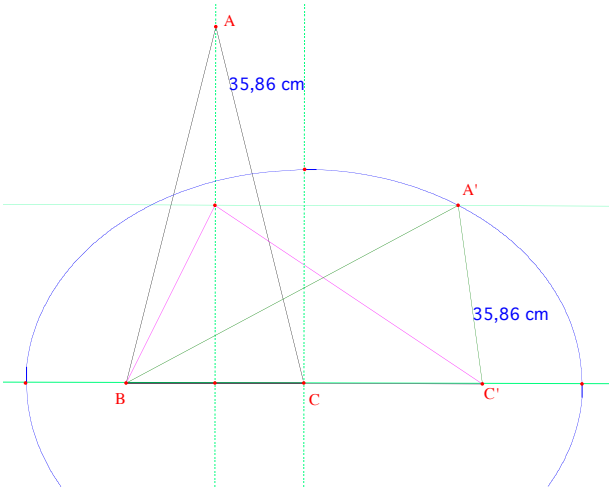

FIGURE 2 – Avec une ellipse

On trouve A' à l'intersection de la parallèle à (BC) à la distance a et de l'ellipse de foyers B, C' et de grand axe $a(\sqrt{17} - 1)$. Avec les choix effectués, cette intersection existe. (Le petit axe de l'ellipse est égal à $\sqrt{\dfrac{7 - \sqrt{17}}{2}}\, a$ et il est plus grand que a.) Le triangle obtenu n'est pas isométrique à ABC car il a un côté de longueur $2a$ alors que ABC a des côtés de longueurs a et $a\sqrt{17}/2$.

18. Cette variante m'a été soufflée par M.-J. Perrin-Glorian.

Bien entendu, la méthode s'applique avec un triangle quelconque et on peut aussi faire varier la position de C', les choix effectués ci-dessus n'ont d'autre but que de simplifier les calculs.

3.3 Variante à périmètre constant

Au lieu d'utiliser une famille de triangles d'aire constante, on peut considérer une famille de triangles de périmètre constant. Pour cela on part d'un segment $I = [A_0A_1]$, de longueur p, que l'on partage en trois morceaux de longueurs c, a, b par des points B et C et on considère le triangle ABC obtenu en prenant pour A un point d'intersection (s'il en existe) des cercles de centre B (resp. C) et rayon c (resp. b). Tous les triangles ainsi obtenus à partir de I en faisant varier B, C ont pour périmètre p.

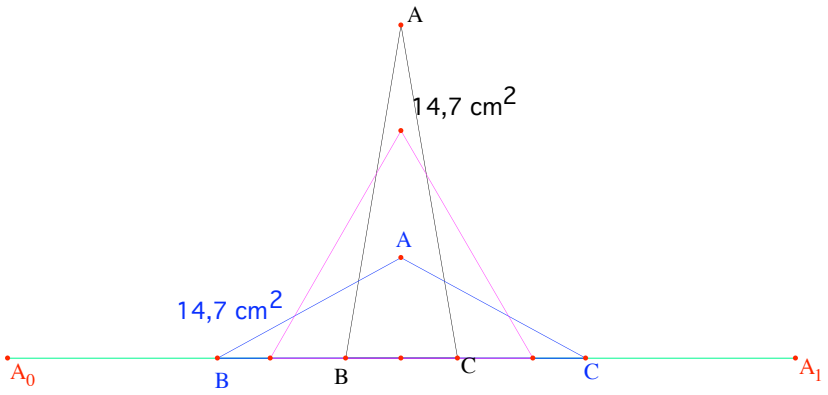

FIGURE 3 – À périmètre constant

Prenons pour simplifier le cas des triangles isocèles[19] en A (donc avec $b = c = \frac{p-a}{2}$). Pour avoir un triangle, éventuellement aplati, il faut imposer la condition $0 \leq a \leq p/2$. On voit immédiatement que l'aire de ABC va varier entre deux minima égaux à 0 dans le cas $a = 0$ où B et C sont tous deux au milieu de I et dans le cas $a = p/2$ où B et C sont au quart de I respectivement du côté de A_0 et de A_1. Entre temps, l'aire passe par un maximum dans le cas équilatéral pour $a = p/3$. On voit sur le tableau de variation de l'aire (ou sur la figure) que chaque valeur de l'aire est prise deux fois, l'une par un triangle grand et mince avec $a < p/3$, l'autre par un triangle petit et gros avec $a > p/3$, voir figure ci-dessus.

19. Là encore, ce n'est que par paresse.

Voici le calcul précis. La hauteur du triangle est $\frac{1}{2}\sqrt{4b^2 - a^2}$ et sa base est a. En tenant compte de $b = \frac{p-a}{2}$ on en déduit l'aire par la formule[20] $16\mathcal{A}^2 = a^2p^2 - 2a^3p$. L'étude de la fonction $a \mapsto 16\mathcal{A}^2(a)$ donne le résultat.

3.4 Une preuve élémentaire de 2.4

Dans ce paragraphe nous donnons une preuve complète de 2.4 : si T est un triangle non équilatéral, il existe une infinité de triangles, non isométriques à T qui ont même aire et même périmètre que T. La preuve proposée ici reprend les idées précédentes (et notamment l'usage des valeurs intermédiaires) et dissimule les idées géométriques derrière l'étude de fonctions. Pour une variante géométrique, voir 8.5.

Soit T un triangle non équilatéral. Il y a un unique triangle équilatéral d'aire $\mathcal{A} := \mathcal{A}(T)$, dont le côté d est donné par $d^2 = \frac{4\mathcal{A}}{\sqrt{3}}$. Comme T n'est pas équilatéral, l'un des côtés de T est différent de d. Appelons a ce côté et considérons le triangle isocèle T' de base a et de même hauteur que T. On a donc $\mathcal{A}(T) = \mathcal{A}(T')$ et T' n'est pas équilatéral non plus (car $a \neq d$). De plus, on a $p(T') \leq p(T)$ en vertu du lemme suivant :

3.1 Lemme. *Soit T un triangle de base a et de hauteur h et T' le triangle isocèle de même base et même hauteur. Alors on a $p(T') \leq p(T)$.*

Démonstration. À défaut de connaître les propriétés de l'ellipse, on peut prouver le résultat par le calcul. On appelle $[AB]$ la base des triangles et on utilise un repère orthonormé d'origine le milieu O de $[AB]$ et d'axe des x porté par (AB). On a $A = (e, 0)$ et $B = (-e, 0)$ avec $e = a/2$. On considère les triangles ABE et ABM avec $E = (0, h)$ et $M = (x, h)$ et il s'agit de montrer qu'on a $EA + EB \leq MA + MB$. Cela s'écrit :

$$f(x) := \sqrt{(x-e)^2 + h^2} + \sqrt{(x+e)^2 + h^2} \geq f(0) = 2\sqrt{e^2 + h^2}.$$

Il y a deux méthodes, de difficultés comparables. L'une, algébrique, consiste à élever au carré deux fois et à prouver l'inégalité directement. L'autre, analytique, consiste à montrer que la fonction $f(x)$ atteint son minimum en $x = 0$. Le lecteur choisira selon ses convictions.

Ce lemme étant établi, on considère un nombre x voisin de a et un triangle isocèle $S(x)$ de base x et de hauteur ah/x, de sorte qu'on a $\mathcal{A}(S(x)) = \mathcal{A}(T)$. Soit $p(x)$ le périmètre de $S(x)$. On a le lemme suivant :

20. Bien entendu, la formule de Héron donne aussitôt ce résultat, mais on a préféré l'éviter ici.

3.2 Lemme. *La fonction $x \mapsto p(x)$ est dérivable au voisinage de a et a n'est pas un minimum relatif pour p.*

Démonstration. On calcule $p(x) = x + \sqrt{x^2 + \dfrac{4a^2h^2}{x^2}}$. On voit que p est dérivable pour $x > 0$ et on a :

$$p'(x) = 1 + \frac{x^4 - 4a^2h^2}{x^3\sqrt{x^2 + \frac{4a^2h^2}{x^2}}}.$$

Il suffit de voir que $p'(a)$ est non nul, ce qui s'écrit $a\sqrt{a^2+4h^2}+a^2-4h^2 \neq 0$, ou encore $h \neq a\frac{\sqrt{3}}{2}$ et c'est le fait que T' n'est pas équilatéral.

Maintenant qu'on a vu que a n'est pas un minimum de p, il y a une infinité de valeurs de x, voisines de a, mais distinctes de a et des autres côtés de T, telles que l'on ait $p(x) = p(S(x)) < p(T') = p(a) \leq p(T)$. Pour un tel x, on dispose d'un triangle $S(x)$ de même aire que T et de périmètre plus petit, mais aussi, en déplaçant le sommet sur une parallèle à la base comme en 3.1, d'un triangle $U(x)$ de base x et de hauteur ah/x et de périmètre arbitrairement grand et notamment $> p(T)$. On peut alors appliquer les valeurs intermédiaires comme dans 3.1 et on obtient, entre $S(x)$ et $U(x)$, un triangle de côté x, de même aire et de même périmètre que T. Comme x n'est pas un côté de T, ce triangle n'est pas isométrique à T.

4 Les triangles isocèles

4.1 Les faux jumeaux

Puisqu'ils sont apparus plusieurs fois ci-dessus, il est temps de faire un sort aux triangles isocèles. Cette fois, l'argument de dimension indique que l'espace des triangles isocèles est de dimension 2, un triangle étant déterminé par sa base et l'un de ses côtés égaux. Il n'est donc plus absurde de penser le déterminer à partir de deux invariants comme l'aire et le périmètre et, en tous cas, on s'attend à n'avoir qu'un nombre fini de solutions. De fait, on a le résultat suivant :

4.1 Proposition. *Soit ABC un triangle isocèle non équilatéral. Il admet exactement un frère isocèle.*

Démonstration. On suppose ABC isocèle en A et on conserve les notations du paragraphe 2.1. On a donc $b = c$, avec $a, b > 0$ et $a < 2b$ et les données deviennent $p = a + 2b$ et $s = 2b^3 + 3ab^2 + 2a^2b$.

Soit XYZ un triangle isocèle en X avec $x = YZ$, $y = XY$ et les mêmes valeurs de p et s que ABC : $p = x + 2y$ et $s = 2y^3 + 3xy^2 + 2x^2y$. On élimine x entre ces équations : $x = p - 2y$. Il reste une équation en y :

$$4y^3 - 5py^2 + 2p^2y - s = 0$$

qui admet la racine $y = b$. On peut donc mettre $y - b$ en facteur et il reste :

$$(**) \qquad 4y^2 - (5a + 6b)y + 2b^2 + 3ab + 2a^2 = 0.$$

Le discriminant de cette équation est $\Delta = 4b^2 + 12ab - 7a^2 = (2b+7a)(2b-a)$, il est positif à cause de $a < 2b$. Cela montre qu'il y a bien deux solutions y_1 et y_2 à $(**)$. Celle munie du signe + est à rejeter car on a alors $x = p - 2y < 0$. En revanche, l'autre donne une solution x, y acceptable, que voici :

$$(2) \qquad x = \frac{2b - a + \sqrt{\Delta}}{4}, \quad y = \frac{5a + 6b - \sqrt{\Delta}}{8}.$$

(La relation $x < 2y$ équivaut à $\sqrt{\Delta} < 3a + 2b$ et elle est trivialement vérifiée.) On vérifie que la relation $y = b$ implique $a = b$, ce qui correspond au cas équilatéral. Sinon, on a bien un triangle isocèle non isométrique au précédent.

4.2 *Remarque.* On notera qu'il y a deux équations de degré 3 qui définissent les triangles isocèles. La relation $4y^3 - 5py^2 + 2p^2y - s = 0$ vue ci-dessus et obtenue en éliminant x grâce à $x = p - 2y$ signifie qu'il existe un triangle isocèle, d'invariants p, s et de côtés $y, y, x = p-2y$. L'élimination de y conduit elle à la relation $2x^3 - px^2 + 4s - p^3 = 0$ qui signifie qu'il existe un triangle isocèle d'invariants p, s et de **base** x. Nous reverrons ces deux équations dans la suite.

4.3 *Exercice.* Construire à la règle et au compas le deuxième triangle isocèle à partir du premier (c'est possible car les formules sont quadratiques).

4.4 *Exercice.* Soit T un triangle non équilatéral. Montrer que T admet exactement deux frères isocèles. (Étudier le nombre de solutions de l'équation $4y^3 - 5py^2 + 2p^2y - s = 0$.)

4.5 *Exercice.* Montrer qu'à isométrie près il n'y a qu'un triangle rectangle de périmètre et d'aire donnés.

4.2 En nombres entiers

Dans le cas des triangles isocèles, les calculs précédents permettent de préciser les triangles de $\mathcal{Q}_{p,s}$ à côtés entiers (on traitera plus loin du problème analogue pour les triangles quelconques).

La version la plus ambitieuse consiste à déterminer tous les entiers positifs a, b, vérifiant la condition $a < 2b$, donc côtés d'un triangle isocèle a, b, b, tels que le triangle isocèle frère ait lui aussi des côtés x, y (donnés par les formules (2)) qui soient entiers. Il suffit pour cela que y soit un entier positif car x est aussi entier à cause de la formule $x = p - 2y$. Une condition nécessaire [21] est que le discriminant soit le carré d'un entier : $\Delta = (2b + 7a)(2b - a) = \delta^2$.

Dans toute cette étude, on peut supposer a et b premiers entre eux (sinon, on a une solution plus petite en les divisant par leur *pgcd*).

4.2.1 Une version élémentaire mais incomplète

Dans ce paragraphe on montre déjà qu'il y a une infinité de triangles isocèles frères à côtés entiers, sans essayer de trouver toutes les solutions.

4.6 Proposition. *Il existe une infinité de paires de triangles isocèles non isométriques, à côtés entiers, ayant même aire et même périmètre.*

Démonstration. On utilise le fait que Δ est factorisé et il suffit de trouver des entiers α, β positifs, avec :

$$\begin{cases} 2b + 7a = \alpha^2 \\ 2b - a = \beta^2, \end{cases}$$

ce qui donne :

$$\begin{cases} 8a = \alpha^2 - \beta^2 \\ 16b = \alpha^2 + 7\beta^2 \end{cases}$$

et on cherche donc α, β tels que $\alpha^2 + 7\beta^2 \equiv 0 \pmod{16}$ (ce qui implique aussi $\alpha^2 - \beta^2 \equiv 0 \pmod 8$). Comme on a $-7 \equiv 9 \pmod{16}$, il suffit de prendre $\alpha \equiv 3\beta \pmod 8$. Pour que y soit entier, il faut aussi que 8 divise $5a + 6b - \alpha\beta$, ce qui équivaut à $\alpha^2 + 2\beta^2 - \alpha\beta \equiv 0 \pmod 8$. On vérifie que $\alpha \equiv 3\beta \pmod 8$ réalise aussi cette condition [22] et x est alors entier lui aussi.

Pour trouver des solutions, on choisit un entier $\beta > 0$ quelconque, puis $\alpha = 3\beta + 8k$ avec $k \in \mathbf{Z}$, $k \neq 0$ (sinon le triangle est équilatéral) de telle sorte que α soit positif. On prend a, b donnés par les formules ci-dessus et on a une solution entière du problème posé. Précisément, on obtient :

$$a = \beta^2 + 6\beta k + 8k^2 \quad \text{et} \quad b = \beta^2 + 3\beta k + 4k^2,$$

21. Mais pas suffisante comme le montre l'exemple $a = 20$, $b = 11$, $\Delta = 18^2$ mais $y = 37/2$.

22. Il y a d'autres solutions que celles qui vérifient $\alpha - 3\beta$ multiple de 8, par exemple $\alpha = 8$, $\beta = 4$ qui donne les triangles isocèles de côtés $(6, 11, 11)$ et $(12, 8, 8)$. Le lecteur pourra les déterminer facilement en notant que les congruences ci-dessus s'écrivent $(\alpha - 3\beta)(\alpha + 3\beta) \equiv 0 \pmod{16}$ et $(\alpha + 2\beta)(\alpha - 3\beta) \equiv 0 \pmod 8$.

$$x = \beta^2 + 2\beta k \quad \text{et} \quad y = \beta^2 + 5\beta k + 8k^2.$$

Il est très facile d'écrire un programme permettant de tabuler les valeurs obtenues. Par exemple, avec $\beta, k \leq 10$ on trouve une quarantaine de solutions $(a, b; x, y)$. En voici quelques-unes : $(15, 8; 3, 14)$, $(35, 22; 15, 32)$, $(45, 23; 5, 43)$, $(91, 46; 7, 88)$, $(153, 77; 9, 149)$, etc.

4.2.2 Recherche de toutes les solutions

On voit aisément que certaines solutions échappent à la liste précédente. Par exemple $a = 4$, $b = 11$ qui donne $\Delta = 900 = 30^2$ et $x = 12$, $y = 7$. Dans ce paragraphe on va déterminer tous les triangles isocèles à côtés entiers qui ont un frère isocèle à côtés entiers. On verra que le résultat n'est ni évident à trouver, ni trivial à démontrer.

4.7 Théorème. *Les triangles isocèles frères à côtés entiers positifs a, b, b et x, y, y avec a, b (resp. x, y) premiers entre eux sont donnés par les formules suivantes :*

- **Solutions du premier type :**

$$a = 8uv + 12v^2, \ b = 4u^2 + 7v^2, \tag{3}$$

$$x = 4v^2 - 8uv, \quad y = 4u^2 + 8uv + 11v^2.$$

avec u, v entiers premiers entre eux, v impair et > 0, $2u+3v > 0$ et $v-2u > 0$,

- **Solutions du deuxième type :**

$$a = 2^{\alpha+1}w(u + 3.2^{\alpha-1}w), \quad b = u^2 + 7.2^{2(\alpha-1)}w^2, \tag{4}$$

$$x = 2^{2\alpha}w^2 - 2^{\alpha+1}uw, \quad y = u^2 + 2^{\alpha+1}uw + 11.2^{2\alpha-2}w^2.$$

avec u, w entiers impairs, premiers entre eux, $\alpha > 1$, $w > 0$, $u+3.2^{\alpha-1}w > 0$ et $u < 2^{\alpha-1}w$.

- **Solutions du troisième type :**

$$a = \frac{uw + 3w^2}{2}, \quad b = \frac{u^2 + 7w^2}{8}, \tag{5}$$

$$x = \frac{w^2 - uw}{2}, \quad y = \frac{u^2 + 4uw + 11w^2}{8},$$

avec avec u, w entiers impairs, premiers entre eux, $w > 0$, $w > u$, $u+3w > 0$ et $u \not\equiv w + 4 \pmod 8$.

4.8 *Remarque.* Si l'on pose $\Delta = (2b + 7a)(2b - a) = \delta^2$ on a respectivement $\delta = 14v^2 - 24uv - 8u^2$, $\delta = 7 \times 2^{2\alpha-1}w^2 - 6 \times 2^{\alpha}uw - 2u^2$ et $\delta = \frac{(w-u)(u+7w)}{4}$.

4.9 *Remarque.* On retrouve les solutions particulières rencontrées en 4.6 comme solutions du troisième type en posant $u = 2k - \beta$ et $w = 2k + \beta$ (pour trouver cela, calculer le fameux paramètre t de 4.10) et on retrouve $a = 8k^2 + 6\beta k + \beta^2$, $b = \beta^2 + 3\beta k + 4k^2$, etc.

Démonstration. On cherche les solutions entières de l'équation $(2b+7a)(2b-a) = \delta^2$ qui vérifient $a > 0$, $b > 0$, $\delta > 0$, $a < 2b$ et a, b premiers entre eux. L'équation $(2b + 7a)(2b - a) = \delta^2$ est l'équation d'une conique projective. On passe à la conique affine en posant $\xi = a/\delta$ et $\eta = b/\delta$ qui vérifient $(2\eta + 7\xi)(2\eta - \xi) = 1$. On commence par déterminer les points rationnels de cette courbe :

4.10 Lemme. *1) Les points rationnels (ξ, η) de la courbe C d'équation $(2\eta+7\xi)(2\eta-\xi) = 1$ sont le point $(0, -1/2)$ et les points donnés par les formules :*

$$\xi = \frac{-4t - 6}{4t^2 + 12t - 7}, \quad \eta = \frac{-4t^2 - 7}{8t^2 + 24t - 14} \quad \text{avec } t \in \mathbf{Q}.$$

2) Les points rationnels (ξ, η) de la courbe C qui vérifient $\xi > 0$, $\eta > 0$ et $\xi < 2\eta$ sont donnés par les formules :

$$\xi = \frac{4t + 6}{7 - 12t - 4t^2}, \quad \eta = \frac{4t^2 + 7}{14 - 24t - 8t^2}$$

avec $t \in \mathbf{Q}$ et $-\frac{3}{2} < t < \frac{1}{2}$.

Démonstration. On a un point rationnel évident qui est $m_0 = (0, 1/2)$. Pour trouver les autres, on coupe C par une droite variable passant par m_0 et de pente $t \in \mathbf{Q}$: $\eta - \frac{1}{2} = t\xi$. On trouve l'équation :

$$\xi\big((4t^2 + 12t - 7)\xi + 4t + 6\big) = 0$$

qui donne $\xi = 0$ (le point m_0) et les solutions annoncées. (Le point $(0, -1/2)$ correspond à la valeur infinie du paramètre.) Pour avoir des solutions positives, il faut que la quantité $7 - 12t - 4t^2$ soit positive donc qu'on soit entre $-7/2$ et $1/2$. Pour que ξ soit > 0 il faut de plus que t soit $> -3/2$. La condition $\xi < 2\eta$ est automatique.

Revenons à 4.7 en posant $\xi = a/\delta$ et $\eta = b/\delta$. On applique le lemme précédent en posant $t = u/v$, avec $u \in \mathbf{Z}$, $v \in \mathbf{N}^*$, u, v premiers entre eux et $-3v < 2u < v$. On a alors :

$$\frac{a}{\delta} = \frac{4uv + 6v^2}{7v^2 - 12uv - 4u^2} \quad \text{et} \quad \frac{b}{\delta} = \frac{4u^2 + 7v^2}{14v^2 - 24uv - 8u^2},$$

d'où $\dfrac{a}{b} = \dfrac{8uv + 12v^2}{4u^2 + 7v^2}$. Comme a et b sont premiers entre eux, on obtient, par Gauss :

$$\lambda a = 4v(2u + 3v), \quad \lambda b = 4u^2 + 7v^2 \quad \text{et} \quad \lambda\delta = 14v^2 - 24uv - 8u^2$$

avec $\lambda \in \mathbf{N}^*$. On en déduit aussi les valeurs de x et y par les formules (2) :

$$x = \frac{2b - a + \delta}{4} = \frac{4v^2 - 8uv}{\lambda} \quad \text{et} \quad y = \frac{5a + 6b - \delta}{8} = \frac{4u^2 + 8uv + 11v^2}{\lambda}.$$

Soit p un facteur premier de λ. On voit que p divise 2 ou v ou $2u + 3v$. Dans tous les cas, on a $p = 2$. C'est évident si $p = 2$, facile si p divise v (car il divise alors $4u^2$ et pas u) et s'il divise $2u + 3v$ on a $2u \equiv -3v \pmod p$, donc $4u^2 \equiv 9v^2 \pmod p$ et p divise $16v^2$, de sorte qu'on est ramené aux cas précédents. On voit ainsi que λ est une puissance de 2, $\lambda = 2^m$.

• **Premier cas : $m = 0$, donc $\lambda = 1$** On obtient les formules $a = 8uv + 12v^2$ et $b = 4u^2 + 7v^2$ avec u, v entiers premiers entre eux, $v > 0$, $2u + 3v > 0$ et $v - 2u > 0$. De plus, comme a est pair, b est impair donc v impair. On vérifie qu'alors a et b sont premiers [23] entre eux. On obtient les solutions du premier type données par les formules (3). Exemple : $u = -1$, $v = 1$ donne $a = 4$, $b = 11$, $\delta = 30$, $x = 12$, $y = 7$.

Si on a $m = 1$, donc $\lambda = 2$, on voit que v est pair, donc a et b le sont aussi ce qui est absurde car a, b sont premiers entre eux : ce cas est impossible.

• **Deuxième cas $m = 2$ donc $\lambda = 4$** On voit que v est pair, $v = 2^\alpha w$ avec $\alpha \geq 1$ et w impair. On a alors $a = 2^{\alpha+1}w(u+3.2^{\alpha-1}w)$ et $b = u^2+7.2^{2(\alpha-1)}w^2$. Comme a est pair, b doit être impair et cela impose $\alpha > 1$. On trouve le second type de solutions données par les formules (4). Exemple : $\alpha = 2$, $u = w = 1$ donne $a = 56$, $b = 29$, $x = 8$ et $y = 53$.

On pose désormais $\lambda = 2^m$ avec $m \geq 3$, v est pair et on pose $v = 2^\alpha w$ avec $\alpha \geq 1$ et w impair. La relation $2^m b = 4(u^2 + 2^{2(\alpha-1)}.7.w^2)$ montre que α est nécessairement égal à 1 (sinon, le second membre, divisé par 4, est impair). On a alors les relations :

$$(6)\ \ 2^{m-4}a = w(u+3w), \quad 2^{m-2}b = u^2+7w^2 \quad \text{et} \quad 2^{m-3}\delta = 7w^2-6uw-u^2,$$

$$2^{m-4}x = w(w-u), \quad 2^{m-2}y = u^2 + 4uw + 11w^2.$$

On a le lemme suivant :

4.11 Lemme. *Si u est impair on a $u^2 \equiv 1 \pmod 8$. Si u et w sont impairs, $u^2 + 7w^2$ est multiple de 8.*

23. Mais pas nécessairement x et y comme le montre l'exemple $u = 1$, $v = 201$.

Il résulte de ce lemme que, si m est égal à 3 ou 4, a et b sont tous deux pairs, et c'est exclu.

• **Troisième cas** $m = 5$, $\lambda = 32$ On trouve $2a = uw + 3w^2$ et $8b = u^2 + 7w^2$. On voit que a et b sont bien entiers (pour b c'est le lemme 4.11). On vérifie qu'ils sont premiers entre eux, sauf si l'on a $u \equiv w + 4 \pmod 8$. On a alors $x = \dfrac{w^2 - uw}{2}$ et $y = \dfrac{u^2 + 4uw + 11w^2}{8}$. On vérifie que x et y sont entiers. Pour y, le numérateur est congru à $12 + 4uw = 4(3 + uw)$ modulo 8 et $3 + uw$ est pair.

Exemple : $u = 1$, $w = 7$, $a = 77$, $b = 43$, $\delta = 75$, $x = 21$, $y = 71$.

Pour aller plus loin, on élimine d'abord le cas $m > 7$:

4.12 Lemme. *Pour $m \geq 7$ les relations (6) n'ont pas de solutions avec a, b, δ, x, y entiers et u, w impairs.*

Démonstration. On suppose $m > 5$. On a $2^{m-4}a = w(u + 3w)$. Comme w est impair, c'est que 2^{m-4} divise $u + 3w$ et on pose $u = -3w + 2^{m-4}z$ avec z entier. On obtient alors $2^{m-6}x = w^2 - 2^{m-6}zw$. Si m est > 6, cette relation est impossible puisque w est impair.

Il reste à éliminer le cas $m = 6$. On raisonne comme ci-dessus pour montrer qu'on a $u = -3w + 4z$. On obtient d'abord $2b = 2w^2 - 3wz + 2z^2$ ce qui montre que z est pair. On obtient ensuite $2y = w^2 - wz + 2z^2$, ce qui contredit le fait que w est impair.

5 La courbe elliptique associée au problème : la courbe réelle

5.1 Les équations

Revenons à la situation inaugurée au paragraphe 2.3. On a vu que si on a un (vrai) triangle de côtés a, b, c, en trouver un autre de côtés x, y, z avec même périmètre $p = a + b + c$ et même aire $\mathcal{A}$, ou encore même invariant $s = (bc + ca + ab)p - 2abc$, revient à résoudre le système de deux équations :

$$x + y + z = p \quad \text{et} \quad 2xyz - (yz + zx + xy)p + s = 0.$$

On définit ainsi une courbe $\mathcal{G}_{p,s}$ de l'espace affine $\mathbf{R}^3$, située dans le plan $x + y + z = p$ que l'on peut encore écrire comme une courbe $\Gamma_{p,s}$ du plan des (x, y) en éliminant $z = p - x - y$:

$$(*) \qquad F(x, y) := 2xy(x + y) - p(x^2 + y^2 + 3xy) + p^2(x + y) - s = 0.$$

Il est essentiel pour étudier ces courbes de considérer aussi leurs complétions projectives obtenues en homogénéisant les équations au moyen d'une variable t. On obtient ainsi dans $\mathbf{P}^3$ les équations de la courbe $\widehat{\mathcal{G}}_{p,s}$:

$$x+y+z-pt=0 \quad \text{et} \quad 2xyz-(yz+zx+xy)pt+st^3=0.$$

À l'infini, donné par $t=0$, on a les trois points $O=(0,1,-1,0)$, $I=(-1,0,1,0)$ et $J=(1,-1,0,0)$. Dans le plan $\mathbf{P}^2$ on a l'équation de la courbe projective $\widehat{\Gamma}_{p,s}$:

$$\widehat{F}(x,y,t) := 2xy(x+y)-p(x^2+y^2+3xy)t+p^2(x+y)t^2-st^3=0.$$

Les points O,I,J deviennent $O=(0,1,0)$, $I=(1,0,0)$ et $J=(1,-1,0)$. Nous interpréterons plus loin ces points en termes de directions asymptotiques.

Le passage de la version de l'espace à la version plane étant donné par l'application linéaire $X=x$, $Y=y$, $Z=pt-x-y$, $T=t$, les deux courbes sont isomorphes. On notera parfois ces courbes $\mathcal{G}$, $\widehat{\mathcal{G}}$, Γ ou $\widehat{\Gamma}$ s'il n'y a pas d'ambiguïté.

5.2 Lissité de la courbe et cas équilatéral

La première question à se poser sur la courbe ci-dessus est celle de sa lissité :

5.1 Proposition. *La courbe $\widehat{\Gamma}_{p,s}$ donnée par les équations ci-dessus est lisse, sauf si l'on a l'une des égalités $4s-p^3=0$ ou $27s-7p^3=0$. Si p,s sont les invariants d'un triangle de côtés a,b,c, le premier cas correspond à un triangle aplati et le second à un triangle équilatéral.*

Démonstration. Pour une courbe projective plane d'équation $\widehat{F}$, les éventuels points singuliers sont ceux où les dérivées partielles de $\widehat{F}$ s'annulent simultanément sur la courbe. On vérifie d'abord que les points à l'infini ne sont pas singuliers. On est donc ramené au cas affine et l'on vérifie qu'on a $\dfrac{\partial F}{\partial x}-\dfrac{\partial F}{\partial x}=(y-x)(2x+2y-p)$. On étudie les deux cas $x=y$ et $x+y=\frac{p}{2}$ qui donnent, au prix d'un calcul facile, les deux relations ci-dessus. On a vu en 2.1 l'égalité $4s-p^3=(b+c-a)(c+a-b)(a+b-c)$ de sorte que la nullité de cette quantité correspond bien au cas d'un triangle aplati. Pour voir que $27s-7p^3=0$ correspond au cas équilatéral, voir 5.3 ci-dessous.

5.2 *Remarques.* 1) Si la courbe $\Gamma_{p,s}$ (ou plutôt $\widehat{\Gamma}_{p,s}$) est lisse, c'est ce qu'on appelle une **courbe elliptique**.

2) Dans le cas équilatéral, le point singulier est le point $(x, y) = (p/3, p/3)$: c'est le triangle équilatéral lui-même qui est singulier (c'est un point isolé de la courbe).

5.3 Proposition. (Inégalité isopérimétrique) *Soit T un triangle, p son périmètre, $\mathcal{A}$ son aire. Alors, on a $\mathcal{A} \leq \dfrac{p^2}{12\sqrt{3}}$ avec égalité si et seulement si le triangle est équilatéral. L'inégalité (resp. l'égalité) est équivalente à $27s \leq 7p^3$ (resp. $27s - 7p^3 = 0$).*

Démonstration. On sait qu'on a $16\mathcal{A}^2 = p(b+c-a)(c+a-b)(a+b-c)$ et il faut montrer que cette quantité est $\leq \dfrac{p^4}{27}$ ou encore qu'on a :

$$27(b+c-a)(c+a-b)(a+b-c) \leq (a+b+c)^3.$$

Si on pose $\alpha = b+c-a$, $\beta = c+a-b$ et $\gamma = a+b-c$, il s'agit de montrer que, si α, β, γ sont > 0 et $\alpha+\beta+\gamma = p$ on a $27\alpha\beta\gamma \leq p^3$. Il y a de multiples façons de faire (voir l'annexe 8.4 pour une variante élémentaire), mais le mieux est d'utiliser les extrema liés qui montrent que le maximum est atteint lorsque α, β, γ sont égaux à $p/3$.

Comme on a vu ci-dessus l'égalité $\alpha\beta\gamma = 4s - p^3$, on en déduit que la relation $27\alpha\beta\gamma \leq p^3$ est bien équivalente à $27s \leq 7p^3$ et de même pour l'égalité.

L'inégalité isopérimétrique permet de montrer que le cas équilatéral est le seul pour lequel la question initiale admet une réponse positive :

5.4 Corollaire. *Soit T un triangle équilatéral. Si un triangle T' a même aire et même périmètre que T, il lui est isométrique.*

Démonstration. Il suffit de montrer que T' est équilatéral lui aussi. Notons p et $\mathcal{A}$ le périmètre et l'aire de T. On a $\mathcal{A}^2 = \frac{p^2}{12\sqrt{3}}$ alors que, si T' n'est pas équilatéral, on a $\mathcal{A}(T') < \dfrac{p(T')^2}{12\sqrt{3}}$ en vertu de 5.3.

Dans toute la suite on supposera que les triangles ne sont pas équilatéraux.

5.3 Description de $\mathcal{Q}_{p,s}$ ou $\mathcal{U}_{p,s}$

Rappelons que nous avons désigné par $\mathcal{Q}_{p,s}$ l'ensemble des triangles de périmètre p et d'invariant s (ou d'aire $\mathcal{A}$ avec $16\mathcal{A}^2 = 4ps - p^4$), modulo isométries et que cet espace est isomorphe à l'espace $\mathcal{U}_{p,s}$ des triplets

$(x, y, z) \in \mathbf{R}^3$ vérifiant $x, y, z > 0$, $|y - z| < x < y + z$, $x + y + z = p$ et $(yz + zx + xy)p - 2xyz = s$. La question initiale est essentiellement de décrire cet ensemble. C'est ce que réalise le théorème suivant :

5.5 Théorème. *Soient p, s deux réels.*

1) L'ensemble $\mathcal{U}_{p,s}$ est non vide si et seulement si p et s vérifient $p > 0$ et $\dfrac{27s}{7} \leq p^3 < 4s$. Dans le cas $27s - 7p^3 = 0$, il est réduit au triplet $(p/3, p/3, p/3)$ qui correspond au triangle équilatéral.

2) On suppose $0 < \dfrac{27s}{7} < p^3 < 4s$. L'ensemble $\mathcal{U}_{p,s}$ est exactement la composante connexe[24] *bornée de la courbe elliptique $\Gamma_{p,s}$. Il est infini.*

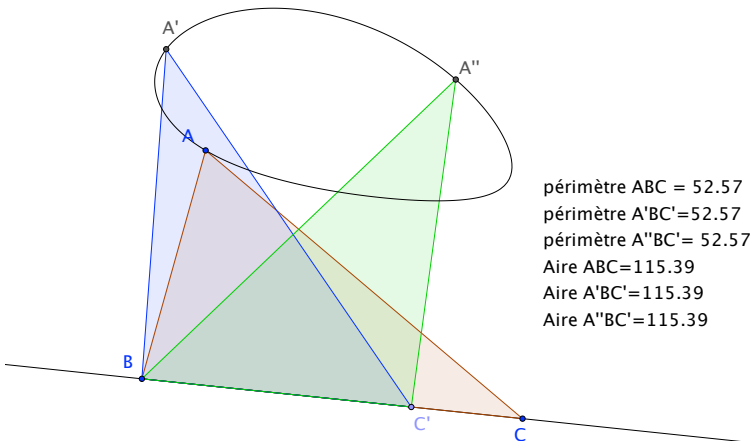

FIGURE 4 – La courbe des triangles frères de ABC

Démonstration. On a vu ci-dessus que les conditions de 1) sont nécessaires (le périmètre p est > 0, la formule $16\mathcal{A}^2 = 4sp - p^3 > 0$ montre que $4s - p^3$ est > 0 et la dernière inégalité est l'inégalité isopérimétrique). Le cas du triangle équilatéral étant acquis, il suffit de prouver le point 2).

Soit $(x, y, z) \in \mathbf{R}^3$. Outre les inégalités, dire qu'il est dans $\mathcal{U}_{p,s}$ signifie que z est égal à $p - x - y$, et que x, y vérifient la relation $(*)$:

$$F(x, y) = (2x - p)y^2 + (2x^2 - 3px + p^2)y + p^2x - px^2 - s = 0,$$

que l'on regarde comme une équation de degré 2 en y. On note qu'on a $2x^2 - 3px + p^2 = (2x - p)(x - p)$. Cela montre que la somme des racines est

24. Donc non vide.

$p-x$ donc que, pour un côté x fixé, les racines sont les deux autres côtés y et $z = p - x - y$. Le discriminant de cette équation est :

$$\Delta(x) = (2x - p)(2x^3 - px^2 + 4s - p^3).$$

On pose $f(x) = 2x^3 - px^2 + 4s - p^3$. On a $f'(x) = 2x(3x - p)$, négatif entre 0 et $p/3$. Comme on a $f(0) = f(p/2) = 4s - p^3 > 0$ et $f(p/3) = \frac{4}{27}(27s - 7p^3) < 0$, on voit que f a trois racines α, β, γ avec $\alpha < 0 < \beta < p/3 < \gamma < p/2$. On en déduit que $\Delta(x)$ est ≥ 0 sur les intervalles $]-\infty, \alpha]$, $[\beta, \gamma]$ et $[p/2, +\infty[$. La courbe Γ n'a donc de points (x, y) que si x est dans l'un de ces intervalles. La partie de Γ correspondant à $[\beta, \gamma]$ est bornée (x l'est et y en est fonction continue, avec deux signes possibles, voir ci-dessous). Les autres intervalles correspondent à trois [25] parties connexes non bornées de Γ.

Cela montre déjà que si x, y, z correspond à un triangle, le point (x, y) est dans la composante bornée. En effet, les autres vérifient soit $x < 0$, soit $x \geq p/2$ (et même $> p/2$ car il n'y a pas de solution avec $p/2$ à cause du dénominateur) et c'est impossible (on a $y + z = p - x > x$).

Montrons la réciproque. Soit donc $x \in [\beta, \gamma]$. Un calcul immédiat donne les deux racines de l'équation $(*)$:

$$y = \frac{p-x}{2} + \frac{\sqrt{\Delta(x)}}{2(p-2x)} \quad \text{et} \quad z = \frac{p-x}{2} - \frac{\sqrt{\Delta(x)}}{2(p-2x)}.$$

Alors, (x, y, z) est dans $\mathcal{U}_{p,s}$, ainsi que (x, z, y). En effet, on a bien $F(x, y) = 0$ et $z = p - x - y$. Il reste à vérifier les inégalités imposées. Pour $x > 0$ et $y > 0$ c'est clair, ainsi que pour $x < y + z = p - x$. La condition $z > 0$ s'écrit $(p - x)(p - 2x) > \sqrt{\Delta(x)}$ soit $(p - x)^2(p - 2x)^2 > \Delta(x) = (p - 2x)(-2x^3 + px^2 - 4s + p^3)$, ou encore $s > px(p - x)$. Comme la quantité $x(p - x)$ est maximum pour $x = p/2$, c'est encore la condition $4s > p^3$. Enfin, il reste à voir $y - z < x$, qui se ramène à $\Delta(x) < x^2(p-2x)^2$ et c'est encore $4s - p^3 > 0$.

Pour terminer, il reste à montrer que $\mathcal{U}_{p,s}$ est infini, mais, comme on a $\beta < \gamma$, c'est clair car on a pour chaque $x \in]\beta, \gamma[$ deux valeurs y, z convenables.

5.6 *Remarques.* 1) On notera que la composante bornée de Γ peut être définie par les inégalités $\beta \leq x \leq \gamma$.

25. En projectif, ces trois parties se recollent en les trois points à l'infini : on a $y(x) \geq z(x)$ et la courbe $y(x)$ (resp. $z(x)$) a une asymptote $y = -x + p/2$ en $-\infty$ (resp. en $+\infty$) qui correspond au point J, la courbe z (resp. y) une asymptote $z = p/2$ en $-\infty$ (resp. $+\infty$), qui correspond à I et les deux courbes y et z une asymptote $x = p/2$ correspondant à O, voir figure 5.

2) On vérifie [26] que la fonction z (resp. y) est convexe (resp. concave). Cela montre que la composante bornée est "convexe" (on entend par là qu'elle est toute entière du même côté de ses tangentes).

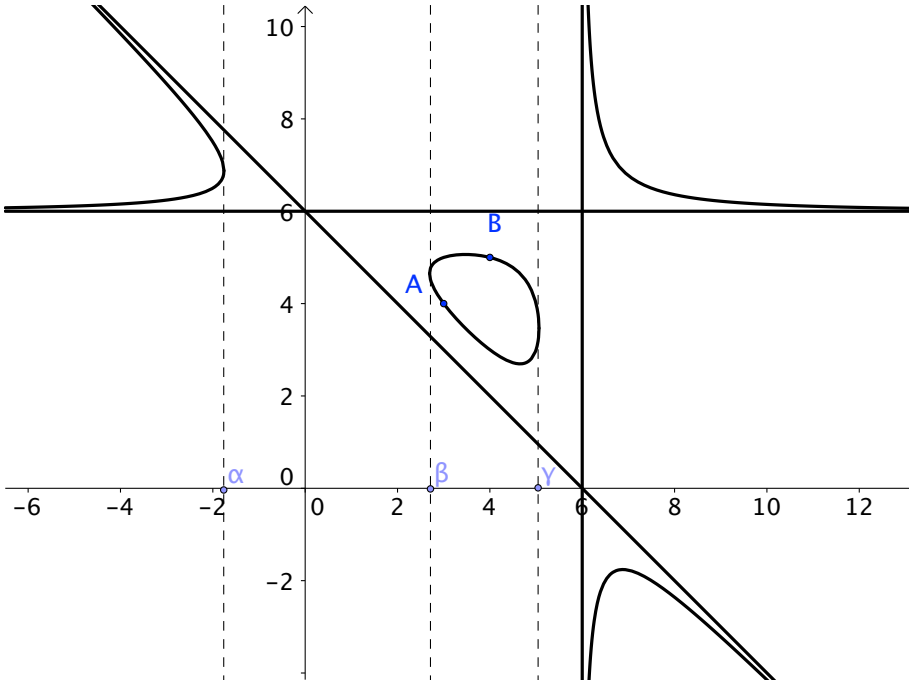

FIGURE 5 – La courbe elliptique du triangle $3, 4, 5$, ici on a $p = 12$

6 La courbe elliptique sur Q

6.1 La loi de groupe

Maintenant que nous avons identifié l'espace des triangles de périmètre p et d'invariant s comme la composante bornée de la courbe elliptique $\Gamma = \Gamma_{p,s}$, nous allons en chercher des points à coefficients rationnels, voire entiers. Cela nous donnera des exemples de triangles à côtés rationnels ou entiers avec même aire et même périmètre. Bien entendu, pour qu'il existe $a, b, c \in \mathbf{Q}$ tels que $p = a + b + c$ et $s = (bc + ca + ab)p - 2abc$, il faut que p et s soient rationnels. **Attention**, la réciproque n'est pas vraie, voir 6.21.1 ci-dessous.

26. Le calcul est plus facile si l'on utilise la forme de Weierstrass $y^2 = x^3 + Ax + B$, $A < 0$, $B > 0$, voir Annexe 1.

Nous supposerons désormais que p et s sont rationnels.

On est maintenant en terrain connu, l'arithmétique des courbes elliptiques étant l'une des branches les plus développées des mathématiques, et nous allons en utiliser librement les résultats, même s'ils sont difficiles. On note $\Gamma(\mathbf{Q})$ l'ensemble des points de Γ à coefficients dans $\mathbf{Q}$. Commençons par une remarque évidente :

6.1 *Remarque.* Sur une courbe elliptique donnée il n'y a qu'un nombre fini de points à coordonnées entières en vertu d'un théorème (non trivial [27]) de Siegel. Cependant, si l'on a deux triangles non isométriques, de même aire et même périmètre, à côtés rationnels, on en a aussi à côtés entiers en multipliant les longueurs par un dénominateur commun k (mais la courbe $\Gamma_{p,s}$ est devenue Γ_{kp,k^3s}) . Par exemple, les triangles de côtés $3, 4, 5$ et $\frac{41}{15}, \frac{101}{21}, \frac{156}{35}$ ayant même aire et même périmètre, on en obtient à coefficients entiers [28] en multipliant par 105 : $315, 420, 525$ et $287, 505, 468$.

On est donc essentiellement ramené à étudier les points rationnels de Γ. La remarque fondamentale, sans doute très ancienne [29], c'est qu'à partir de deux points de $\Gamma(\mathbf{Q})$, voire d'un seul, on sait en construire d'autres par la méthode de la sécante et celle de la tangente. L'idée est simple. Comme on a une courbe de degré 3, si l'on dispose de deux points de $\Gamma(\mathbf{Q})$ et qu'on trace la droite qui les joint, elle recoupe Γ en un troisième point, lui aussi à coefficients dans $\mathbf{Q}$ (c'est le théorème de Bézout, mais on peut faire le calcul explicitement). Si l'on ne détient qu'un point de $\Gamma(\mathbf{Q})$, on en obtient un autre en coupant Γ par la tangente en ce point.

Cette remarque permet de munir $\widehat{\Gamma}(\mathbf{Q})$ d'une structure de groupe abélien de la manière suivante. On choisit une origine O (en général un point d'inflexion de $\widehat{\Gamma}$). Ensuite, si P, Q sont deux points distincts de $\widehat{\Gamma}$, on leur asso-

27. Dans le cas présent, il est clair qu'il n'y a qu'un nombre fini de triangles à côtés entiers de périmètre donné. Pour voir qu'il n'y a qu'un nombre fini de points entiers sur la courbe voir 6.21.2.

28. D'une certaine façon, c'est triché, et nous donnerons plus loin des exemples avec des triplets d'entiers **premiers entre eux**.

29. En tous cas, Newton, au XVII-ième siècle, savait faire cela et plus tard Sylvester et Poincaré ont beaucoup utilisé cette méthode. Si l'on lit entre les lignes avec nos connaissances actuelles, on peut même reconnaître cette procédure chez Fermat, Bachet, voire Diophante, voir le très intéressant article de [Schappacher].

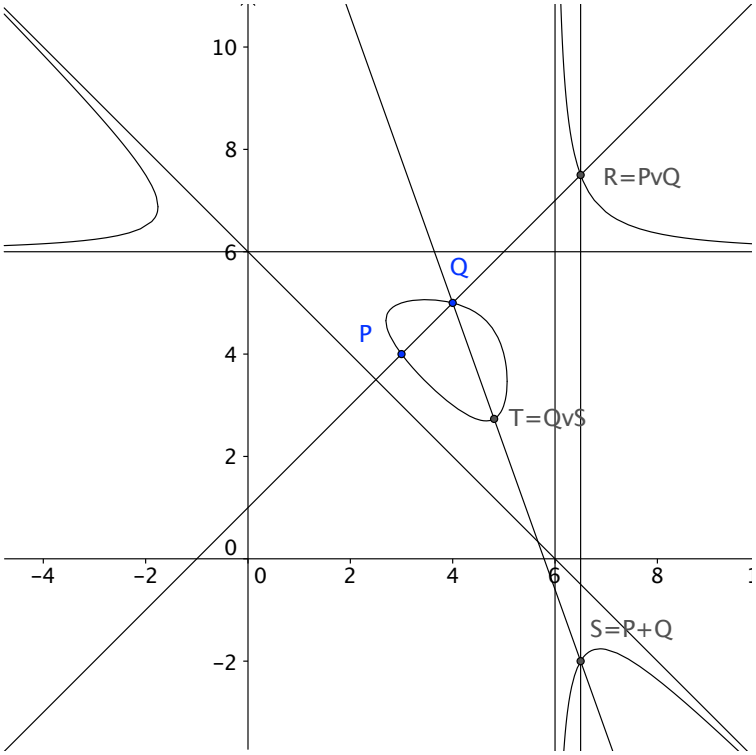

FIGURE 6 – La loi de groupe sur la courbe elliptique

cie [30] le point $R = P \vee Q$ où la droite (PQ) recoupe [31] $\widehat{\Gamma}$, puis le point $P+Q$ où la droite (OR) recoupe $\widehat{\Gamma}$. On montre que l'on définit ainsi sur $\widehat{\Gamma}(\mathbf{Q})$ une structure de groupe abélien [32] et le théorème de Mordell (1922) affirme que le groupe $\widehat{\Gamma}(\mathbf{Q})$ est **de type fini**, donc produit d'un groupe abélien libre $\mathbf{Z}^r$ par un groupe fini T. C'est là que les difficultés commencent car il n'est pas facile de déterminer [33] T ni surtout r. Le calcul de r est d'ailleurs l'objet de

30. On peut se demander pourquoi l'on ne définit pas l'addition simplement comme $A \vee B$. Une raison décisive est qu'elle n'est pas associative. On comprend bien mieux cette loi un peu bizarre si l'on pense en termes de diviseurs, voir par exemple R. Hartshorne, *Algebraic Geometry* Partie II, Ch. 6.

31. Avec des conventions évidentes dans le cas tangent.

32. On attribue souvent la paternité de cette notion à Poincaré – on ne prête qu'aux riches –. Schappacher, avec des arguments qui me semblent convaincants, le conteste. Deux choses sont sûres : le mot groupe n'est pas dans le travail de Mordell, mais il est dans celui de Weil (1929).

33. Le logiciel Pari permet de faire beaucoup de calculs sur les courbes elliptiques et je l'ai largement utilisé dans ce qui suit. Attention, lorsque je donnerai la valeur du rang dans les exemples ci-dessous, il s'agira le plus souvent du rang "analytique" qui n'est égal au rang que si la conjecture de Birch et Swinnerton-Dyer est vraie (c'est le cas en rang 0 ou 1).

la fameuse conjecture de Birch et Swinnerton-Dyer, l'un des sept problèmes du millenium.

6.2 Le résultat principal

6.2.1 L'énoncé

Dans la suite de ce texte, nous allons essentiellement prouver que la courbe Γ associée à un triangle à côtés rationnels, non isocèle, contient une infinité de points rationnels, sauf dans un cas particulier :

6.2 Théorème. *Soit ABC un triangle non isocèle à côtés rationnels, $a, b, c \in \mathbf{Q}$ ses côtés, $p = a + b + c$, $s = (bc + ca + ab)p - 2abc$ et $\Gamma = \Gamma_{p,s}$ la courbe elliptique associée. Alors, si ABC n'est pas un douzain (voir 6.14), le rang de $\widehat{\Gamma}(\mathbf{Q})$ est ≥ 1 (en particulier $\Gamma(\mathbf{Q})$ est infini).*

6.2.2 Principe de la démonstration

En vertu du théorème de Mordell, on sait que $\widehat{\Gamma}(\mathbf{Q})$ est un groupe abélien de type fini, donc isomorphe à $\mathbf{Z}^r \times T$ où T est fini. Si le rang est 0, $\widehat{\Gamma}(\mathbf{Q})$ est donc réduite à son sous-groupe de torsion. Or, on dispose du théorème [34] suivant :

6.3 Théorème. (Mazur) *Les sous-groupes de torsion possibles pour une courbe elliptique sur $\mathbf{Q}$ sont les suivants :*

- $T = \mathbf{Z}/n\mathbf{Z}$ *avec* $n = 1, 2, \ldots, 10, 12$,
- *ou* $T = \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ *avec* $n = 2, 4, 6, 8$.

De plus, nous verrons en 6.4 ci-dessous que $\widehat{\Gamma}(\mathbf{Q})$ contient des éléments d'ordre 3, ce qui ne laisse subsister, dans la liste de Mazur, que les cas $\mathbf{Z}/3\mathbf{Z}$, $\mathbf{Z}/6\mathbf{Z}$, $\mathbf{Z}/9\mathbf{Z}$, $\mathbf{Z}/12\mathbf{Z}$ et $\mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, tous de cardinal ≤ 12. Il suffira donc de montrer que la courbe contient strictement plus que 12 points pour être sûr qu'elle est infinie.

6.3 Inflexions et points d'ordre 3

Rappelons l'équation de Γ vue comme une cubique plane :

$$F(x, y) := 2xy(x + y) - p(x^2 + y^2 + 3xy) + p^2(x + y) - s = 0,$$

et sa variante projective $\widehat{\Gamma}$:

$$\widehat{F}(x, y, t) := 2xy(x + y) - p(x^2 + y^2 + 3xy)t + p^2(x + y)t^2 - st^3 = 0.$$

34. Qui date de 1976 et n'est pas du tout trivial, voir [Mazur].

6.3.1 Les inflexions

6.4 Proposition-Définition. *0) Les points $O = (0, 1, 0)$, $I = (1, 0, 0)$ et $J = (1, -1, 0)$ sont des points d'inflexion de $\widehat{\Gamma}$.* **On choisit désormais O comme origine de $\widehat{\Gamma}$.** *On a alors les faits suivants :*

1) L'opposé d'un point P est le point $-P$ aligné avec O et P. En particulier P est d'ordre 2 si et seulement si la tangente en P passe par O. Le point $P \vee Q$ est l'opposé de $P + Q$.

2) Les points I, J sont des points d'ordre 3 de $\widehat{\Gamma}$, avec $I = -J$. Il en résulte que le sous-groupe de torsion T de $\widehat{\Gamma}$ est de cardinal multiple de 3.

Démonstration. En revenant dans $\mathbf{P}^3$, il suffit, par permutation, de montrer par exemple que I est un point d'inflexion. Mais la tangente en I est la droite $2Y - pT = 0$ et on vérifie qu'elle ne coupe $\widehat{\Gamma}$ qu'en I qui est donc un point d'inflexion. Sur la figure 5, cela correspond au fait que les asymptotes à la courbe ne la recoupent pas. Pour le point 1), si P, Q sont alignés avec O on a $P \vee Q = O$ et, comme O est une inflexion, $P + Q = O$. Pour 2), un point P est d'ordre 3 si et seulement si $P \vee P = -2P = P$, donc si la tangente en P recoupe $\widehat{\Gamma}$ en P autrement dit si P est un point d'inflexion. Dans le cas présent, I et J sont donc des points d'ordre 3, opposés car la droite (IJ) est la droite à l'infini $t = 0$ qui recoupe $\widehat{\Gamma}$ en O.

6.5 *Remarques.* 1) Soit (a, b, c) un triangle et (a, b) le point correspondant de Γ dans le plan. Comme on a pris pour origine $O = (0, 1, 0)$, l'opposé de P a même abscisse que P. Mais, comme (a, c, b) est un autre triangle de même périmètre et même aire, le point (a, c) est sur Γ, et c'est donc $-P$. En particulier P et $-P$ sont tous deux dans la composante bornée ou tous deux extérieurs (donc en même temps des vrais triangles ou non). On voit qu'un point n'est d'ordre 2 que si deux de ses coordonnées coïncident.

2) Il résulte du théorème de Mazur qu'il n'y a pas d'autres inflexions rationnelles sur $\widehat{\Gamma}$ que O, I, J.

6.3.2 La loi de groupe et les composantes

Revenons un instant à la courbe projective réelle $\widehat{\Gamma}(\mathbf{R})$. On a dit plus haut qu'elle contient deux composantes connexes, la composante bornée B et la composante non bornée N (qui contient les points O, I, J). Par ailleurs, on peut définir la loi de groupe sur $\widehat{\Gamma}(\mathbf{R})$ comme on l'a fait sur $\mathbf{Q}$. Le comportement des composantes par la loi de groupe est décrit par le lemme suivant :

6.6 Lemme. *On a les formules $N + N \subset N$, $2B \subset B + B \subset N$, $B + N = N + B \subset B$, $B + B + B \subset B$. En particulier, le double d'un point P n'est jamais dans la composante bornée.*

Démonstration. Comme la loi de composition est continue (voir ci-dessous 6.11 pour en avoir confirmation) et que le produit de deux connexes l'est, l'image par la loi du produit cartésien de deux composantes est contenue dans une composante. Pour décider de laquelle il s'agit, il suffit de regarder un point particulier, par exemple l'élément neutre. Cela donne le résultat (pour le cas de $B+B$, on note que si P est dans B il en est de même de son opposé).

6.4 Permutations et passage à neuf points

6.4.1 Dans l'espace

Rappelons que, dans l'espace, la courbe $\mathcal{G}_{p,s}$ est définie par les équations :

$$x+y+z=p \quad \text{et} \quad 2xyz-(yz+zx+xy)p+s=0,$$

ou, en projectif :

$$x+y+z-pt=0 \quad \text{et} \quad 2xyz-(yz+zx+xy)pt+st^3=0.$$

À l'infini, i.e. pour $t=0$, on a les points $O=(0,1,-1,0)$, $I=(-1,0,1,0)$ et $J=(1,-1,0,0)$.

Comme les équations de $\mathcal{G}$ sont des polynômes symétriques en x,y,z la courbe est invariante par le groupe des homographies de $\mathbf{P}^2$ qui permutent x,y,z et fixent t, groupe isomorphe au groupe symétrique $\mathfrak{S}_3$. Les orbites de ce groupe sur $\mathcal{G}$ ont en général 6 éléments, à l'exception des orbites des points $m=(x,y,z;t)$ fixés par certaines permutations. Rappelons que σ fixe m, en projectif, si l'on a $(\sigma(x,y,z);t)=\lambda(x,y,z;t)$ avec $\lambda\neq 0$. À l'infini, on voit que O,I,J sont chacun fixés par une transposition et constituent une orbite. À distance finie on a $t\neq 0$, donc nécessairement $\lambda=1$. Par les permutations circulaires, le seul point fixe est (x,x,x) avec $x=p/3$, qui n'existe que si l'on a $27s=7p^3$ (le cas d'un triangle équilatéral, qui a été écarté). Par les transpositions, les points fixes sont les points[35] "isocèles" correspondant au cas où deux des x,y,z sont égaux. Nous étudierons le cas où il y a des points isocèles au paragraphe 7.3.

L'opération de $\mathfrak{S}_3$ implique que dès qu'on dispose d'un point rationnel (non isocèle) de $\mathcal{G}$ ou Γ on en a 6.

6.7 *Remarque.* Attention, à l'exception de l'identité et de la transposition (y,z), les automorphismes ci-dessus ne sont pas des automorphismes de groupe (car ils transforment l'origine O en I ou J).

35. On convient de parler de points isocèles de $\mathcal{G}$ pour les points (x,y,z) de la version spatiale dont deux coordonnées sont égales. Parmi ces points, seuls ceux qui sont dans la composante bornée correspondent à de vrais triangles isocèles.

6.4.2 Dans le plan

On suppose qu'on dispose d'un point $(a, b, c) \in \mathcal{G}(\mathbf{Q})$ non isocèle, avec $a+b+c = p$. On a alors six transformés distincts de ce point par permutations. Dans la variante plane Γ on pose $A = (b, c)$ (ou $(b, c, 1)$ en projectif), $B = (c, a)$ et $C = (a, b)$ et on a aussi les points $A' = (b, a)$, $B' = (c, b)$ et $C' = (a, c)$. Avec en plus O, I, J, on a donc déjà trouvé 9 points distincts de $\widehat{\Gamma}$. Bien entendu, on peut en construire d'autres par la méthode de la sécante ou de la tangente, mais pas autant qu'on pourrait le penser :

6.8 Lemme. *1) Les points A, A' (resp. B, B', resp. C, C') sont opposés.*
2) On a $B - C = C - A = A - B = I = -J$.
3) On a $2A = B + C$, $2B = C + A$, $2C = A + B$.

Démonstration. 1) Cela résulte de 6.5 puisque A, A', par exemple, ont même abscisse.

2) Dire qu'on a $B - C = I$ s'écrit encore $B = C + I$, ou $B' = C \vee I$ et cela vient du fait que ces points sont alignés sur la droite $y = b$ (de direction I). La situation est analogue pour les autres.

3) C'est une conséquence de 2).

6.5 Atteindre et franchir les douze points

6.5.1 Le lemme du cardinal ≥ 12

6.9 Lemme. *Soit ABC un triangle non isocèle, a, b, c ses côtés, $p = a+b+c$, $s = (bc + ca + ab)p - 2abc$ et $\widehat{\Gamma} = \widehat{\Gamma}_{p,s}$ la courbe elliptique associée. Alors, l'ensemble $\widehat{\Gamma}(\mathbf{Q})$ est de cardinal ≥ 12.*

Démonstration. Avec les notations du paragraphe précédent on a déjà les 9 points O, I, J et A, A', B, B', C, C'. Par ailleurs, on a construit aussi les doubles $2A, 2B, 2C$. Comme ces points sont dans la composante non bornée en vertu de 6.6, ils sont différents de A, B, C, A', B', C' et les formules de 6.8 montrent qu'ils sont aussi différents de O, I, J.

6.10 *Remarque.* Bien entendu, on a aussi les points $2A', 2B', 2C'$ et ces points sont en général différents des douze premiers, comme le montre la figure 7 ci-dessous. Cependant, il peut arriver qu'on ait des coïncidences, par exemple $2A = 2A'$. Pour examiner ce point nous aurons besoin d'expliciter la loi de composition sur Γ.

6.5.2 Calcul du double d'un point

6.11 Lemme. *On reprend les notations de 6.8, en particulier $A = (b, c)$, $B = (c, a)$ et $C = (a, b)$. Le point $A \vee A = B \vee C$ (opposé de $2A = B + C$) a pour coordonnées (x, y, z) (dans la courbe $\mathcal{G}$ de l'espace) :*

$$x = \frac{a^3 + b^3 + c^3 - 2a^2b - 2bc^2 + abc}{2(a-b)(c-b)},$$

$$y = \frac{a^3 + b^3 + c^3 - 2a^2c - 2b^2c + abc}{2(b-c)(a-c)}, \quad z = \frac{a^3 + b^3 + c^3 - 2ac^2 - 2ab^2 + abc}{2(a-b)(a-c)}.$$

Démonstration. On écrit soit la sécante (CA), soit la tangente en B et on coupe la courbe en tenant compte du fait qu'on connait déjà deux racines. Le calcul est sans difficulté, mais pénible, et on peut utiliser un logiciel de calcul formel (par exemple *xcas*) pour le faire.

6.12 *Remarques.* 1) Le calcul précédent vaut si a, b, c sont distincts et l'on a alors $t = 1$. On peut encore écrire $A \vee A$ dans le plan projectif :

$$x = (a^3+b^3+c^3-2a^2b-2bc^2+abc)(a-c),\ y = (a^3+b^3+c^3-2a^2c-2b^2c+abc)(b-a),$$

$$t = 2(a-b)(c-a)(b-c)$$

et le principe de prolongement des identités algébriques montre que ces formules valent encore quand certains des nombres a, b, c coïncident.

2) On retrouve ainsi le fait que, sauf si deux des nombres a, b, c sont égaux, le point n'est pas d'ordre 2 (dire qu'il est d'ordre 2 signifie que $2A = O$ donc $t = 2(a-b)(c-a)(b-c) = 0$).

6.5.3 Les douzains et la fin de la preuve de 6.2

6.13 Lemme. *Soit ABC un triangle non isocèle. On suppose que a, b, c vérifient la condition :*

$$(b + c - a)(b - c)^3 \neq (a + b - c)(a - b)^3$$

et les deux conditions analogues obtenues par permutation circulaire sur a, b, c. Alors, le cardinal de $\widehat{\Gamma}(\mathbf{Q})$ est > 12.

Démonstration. Une première remarque : la relation $2A = 2A'$, i.e. $B + C = -B - C$ équivaut à $2B' = 2C$ et $2C' = 2B$ et de même par permutation. Autrement dit, si on a une coïncidence entre des points $2A, 2B, 2C$ et $2A', 2B', 2C'$ l'un d'eux est nécessairement égal à son opposé.

Avec la condition de l'énoncé, montrons que $2A$ et $2A'$ sont distincts. On passe de A à A' en échangeant a et c. Dans l'expression de $2A$ on voit que cela revient à échanger y et z. Dire que $2A = 2A'$ signifie donc qu'on a $y = z$ et on vérifie que cette relation est équivalente à celle de l'énoncé. La conclusion est identique pour les autres cas et cela montre que les trois points $2A', 2B', 2C'$ sont distincts des douze premiers.

6.14 Définition. *Un triangle qui vérifie :*

$$(b + c - a)(c - b)^3 = (c + a - b)(a - c)^3$$

ou l'une des deux conditions analogues obtenues par permutation circulaire sur a, b, c est appelé[36] *un* **douzain**.

On obtient ainsi le résultat annoncé en 6.2 :

6.15 Théorème. *Soit ABC un triangle non isocèle, $a, b, c \in \mathbf{Q}$ ses côtés, $p = a + b + c$, $s = (bc + ca + ab)p - 2abc$ et $\Gamma = \Gamma_{p,s}$ la courbe elliptique associée. Alors, si ABC n'est pas un douzain, le rang de $\widehat{\Gamma}(\mathbf{Q})$ est ≥ 1 (en particulier $\Gamma(\mathbf{Q})$ est infini).*

6.16 Corollaire. *Un triangle ABC à côtés rationnels, non isocèle et non douzain, étant donné, il existe une infinité de triangles à côtés rationnels, non isométriques à ABC, ayant même aire et même périmètre.*

Démonstration. Attention, contrairement aux apparences, ce résultat n'est pas tout à fait évident. En effet, il y a bien une infinité de points rationnels sur la courbe elliptique Γ, mais encore faut-il qu'il y en ait une infinité dans composante bornée, celle qui correspond aux vrais triangles. Cela résulte essentiellement de 6.6. En effet, une conséquence de ce résultat c'est que si P est dans la composante bornée B, ses multiples pairs sont dans la composante non bornée et ses multiples impairs dans la composante bornée. Il reste à montrer le lemme suivant :

6.17 Lemme. *Si ABC n'est ni isocèle ni un douzain, l'un au moins des points A, B, C, A', B', C' est d'ordre infini.*

Démonstration. (du lemme) Comme on a $A \neq A'$, A n'est pas d'ordre 2, et de même pour les autres. Les seuls points d'ordre 3 sont I, J. Si A était d'ordre 4, on aurait $2A = 2A'$ et cela a été exclu. Si A était d'ordre 6, son double serait d'ordre 3, donc à l'infini, et le calcul ci-dessus montre que ce n'est pas le cas. Comme les puissances impaires de A sont dans la composante

36. Cela correspond au fait que le groupe de torsion est égal à $\mathbf{Z}/12\mathbf{Z}$, voir §7.1.

bornée en vertu de 6.6, cela exclut que A soit d'ordre 9. Enfin, il reste la possibilité pour les points A, B, C, A', B', C' d'être d'ordre 12. Le groupe de torsion serait alors $\mathbf{Z}/12\mathbf{Z}$ et comme il contient seulement 4 éléments d'ordre 12 ils ne le sont pas tous.

6.18 *Remarque.* Le raisonnement [37] ci-dessus permet de montrer que si E est une courbe elliptique à coefficients rationnels et si $E(\mathbf{Q})$ est infini il est dense dans les composantes connexes de $E(\mathbf{R})$ qu'il rencontre. Voir aussi [Waldschmidt] page 104. Attention, il existe des courbes elliptiques de rang > 0 où les points rationnels sont denses dans la composante non bornée mais où la composante bornée n'en contient pas. C'est assez facile à voir dans le cas de la courbe de Bremner : $y^2 = x^3 + 6x^2 + 2x$.

6.19 Corollaire. *Il existe une infinité de paires de triangles à côtés entiers, non isocèles, de même aire et même périmètre (a, b, c) et (x, y, z), avec par exemple x, y, z premiers entre eux.*

Démonstration. Prenons $a = 4k - 1$, $b = 4k$ et $c = 4k + 1$ avec k entier ≥ 1. Montrons que le triangle n'est pas un douzain. Si l'on a par exemple $(b + c - a)(c - b)^3 = (c + a - b)(a - c)^3$, cela signifie $2k + 1 = 16k$ ce qui est impossible. Les deux autres sont analogues et la courbe Γ est donc de rang > 0 et il y a une infinité de triangles frères de a, b, c à côtés rationnels. On en prend un différent de a, b, c, que l'on écrit, par réduction au même dénominateur, $a' = x/d$, $b' = y/d$ et $c' = z/d$ avec x, y, z premiers entre eux. Mais alors, les triangles da, db, dc et x, y, z sont frères et le second est bien formé d'entiers premiers entre eux.

Pour conclure, il faut être sûr qu'on ne retrouve pas plusieurs fois les mêmes triangles. Pour réaliser cela, on commence par prendre pour a_1 un nombre premier de la forme $4k - 1$ (il y en a une infinité). On obtient un triangle commençant par da_1. On prend ensuite pour a_2 un nombre premier de la forme $4k - 1$ plus grand que da_1, etc.

6.20 *Remarque.* Nous verrons en 7.10 qu'il existe une infinité de triplets a, b, c et x, y, z, entiers, donnant même aire et même périmètre, avec à la fois a, b, c et x, y, z premiers entre eux comme $5, 17, 18$; $10, 11, 19$.

6.6 Variante : le changement de variables des différences

6.6.1 Le changement de variables

Le changement de variable suivant m'a été inspiré par la lecture de l'article *Le conte des deux triangles : triangles de Héron et courbes elliptiques* du

37. Merci à Jean-François Mestre de me l'avoir soufflé.

Projet Klein écrit par William Mc Callum, voir Annexe 2, mais il est aussi très naturel à partir de la formule de Héron.

On part d'un triangle ABC de côtés a, b, c et on pose simplement $\alpha = b+c-a$, $\beta = c+a-b$ et $\gamma = a+b-c$, ou encore $a = \dfrac{\beta+\gamma}{2}$, $b = \dfrac{\gamma+\alpha}{2}$ et $a = \dfrac{\alpha+\beta}{2}$. On note aussi les formules $\alpha = p-2a$, $\beta = p-2b$ et $\gamma = p-2c$. On voit que les nombres a, b, c et α, β, γ sont rationnels en même temps et – presque – entiers en même temps (attention à la parité). On voit aussi que α, β, γ correspondent à un vrai triangle si et seulement si ils sont > 0 et que le triangle est isocèle si et seulement si deux des nombres α, β, γ sont égaux.

Les équations liant α, β, γ sont $\alpha+\beta+\gamma = a+b+c = p$ et $\alpha\beta\gamma = \dfrac{16\mathcal{A}^2}{p} = 4s-p^3 := m$. (La dernière relation est évidente avec Héron qui s'écrit $16\mathcal{A}^2 = p\alpha\beta\gamma$, voir ci-dessus §2.1.) Inversement, le théorème 5.5 montre qu'il existe des réels $\alpha, \beta, \gamma > 0$ vérifiant $p = \alpha+\beta+\gamma$ et $m = \alpha\beta\gamma$ si et seulement si p et m sont positifs et vérifient $27m < p^3$.

Trouver un triangle de même aire et même périmètre que ABC revient donc à résoudre les équations $x+y+z = p$ et $xyz = m$ et si l'on élimine z entre ces équations et il reste la courbe elliptique $\Lambda_{p,m}$ d'équation :

$$xy(x+y) - pxy + m = 0,$$

dont les points à l'infini sont encore O, I, J, voir §5.1. On peut mettre cette courbe sous une forme canonique (pas tout à fait celle de Weierstrass, mais acceptée par Pari). Pour cela on passe à la version projective $xy(x+y) - pxyt + mt^3 = 0$. On pose $X_1 = t$, $Y_1 = y$ et $T_1 = x$. On obtient $T_1^2Y_1 + T_1Y_1^2 - pX_1Y_1T_1 + mX_1^3$. On multiplie par m^2 et on pose $X = -mX_1$, $Y = mY_1$ et $T = T_1$ et on trouve : $Y^2T + pXYT + mYT^2 = X^3$, soit en affine $y^2 + pxy + my = x^3$.

6.21 *Remarques.* 1) Cette écriture permet de répondre par la négative à la question posée ci-dessus : si p, s (ou p, m) sont rationnels, existe-t-il toujours des a, b, c rationnels correspondant à p, s. En effet, si l'on prend $p = 4$ et $m = 1$ (ou $s = 65/4$, ou encore $\mathcal{A} = 1/2$), la courbe elliptique Λ associée est $y^2 + 4xy + y = x^3$ et Pari montre qu'elle ne contient aucun point rationnel autre que les trois points à l'infini. Voici un exemple de triangle (isocèle) de périmètre 4 et d'aire $1/2$: on prend $B = (0,0)$, $C = (a,0)$ avec a racine du polynôme irréductible $2a^3 - 4a^2 + 1 = 0$ (par exemple $a \simeq 0.597$) et $A = (a/2, 1/a)$.

2) Elle permet aussi de montrer le théorème de Siegel dans ce cas particulier. En effet, les points entiers de la courbe vérifient $\alpha\beta\gamma = m$ et il n'y a qu'un nombre fini de α, β, γ possibles.

6.6.2 Calcul de solutions réelles

On peut écrire l'équation ci-dessus comme une équation du second degré en y avec x comme paramètre :

$$xy^2 + x(x-p)y + m = 0.$$

Le discriminant de cette équation est $\Delta(x) = xf(x)$ avec $f(x) = x^3 - 2px^2 + p^2x - 4m$. On étudie la fonction $f(x)$ et on voit qu'elle admet trois racines réelles α, β, γ avec $0 < \alpha < p/3 < \beta < p < \gamma$ et l'équation admet des solutions y réelles si et seulement si on a $x \leq 0$ ou $\alpha \leq x \leq \beta$ ou $x \geq \gamma$. Les intervalles extrêmes doivent être écartés car ils donnent des $x < 0$ ou $> p$. Il reste donc une infinité de solutions avec $x \in [\alpha, \beta]$, données par

$$y = \frac{p-x}{2} + \frac{\sqrt{\Delta(x)}}{2x} \quad \text{et} \quad z = \frac{p-x}{2} - \frac{\sqrt{\Delta(x)}}{2x}.$$

On retrouve ainsi une démonstration de 2.4.

6.6.3 Calculs de la somme et du double avec le changement de variables des différences

Pour ces calculs, le changement de variables des différences conduit à des résultats plutôt plus simples :

6.22 Proposition. *Soit $\Lambda := \Lambda_{p,m}$ la courbe de l'espace affine définie par les équations $x + y + z = p$ et $xyz = m$ et soit $P = (x, y, z) \in \Lambda$. Le point $P \vee P = (X, Y, Z)$ a pour coordonnées :*

$$X = \frac{x(y-z)^2}{(z-x)(x-y)}, \quad Y = \frac{y(z-x)^2}{(x-y)(y-z)}, \quad Z = \frac{z(x-y)^2}{(y-z)(z-x)}.$$

Démonstration. On coupe la courbe par la droite D d'équations paramétriques $X = x + \lambda u$, $Y = y + \lambda v$, $Z = z + \lambda w$ qui passe par P. On trouve aussitôt $u + v + w = 0$ et une équation en λ :

$$uvw\lambda^3 + (xvw + ywu + zuv)\lambda^2 + (uyz + vzx + wxy)\lambda = 0.$$

On écrit que D est tangente à Λ, c'est-à-dire que $\lambda = 0$ est racine double, ce qui donne (à un scalaire près) les valeurs de u, v, w :

$$u = x(z-y), \quad v = y(x-z), \quad w = z(y-x)$$

et en reportant dans X, Y, Z on obtient les formules annoncées.

6.23 *Remarque.* En revenant à la courbe de $\mathbf{P}^3$, on obtient les formules :

$$X = x(y-z)^3, \quad Y = y(z-x)^3, \quad Z = z(x-y)^3, \quad T = t(y-z)(z-x)(x-y).$$

On peut aussi calculer $P = P_1 \vee P_2 = (x, y, z)$ avec $P_i = (x_i, y_i, z_i)$:

$$x = \frac{(x_2 - x_1)(y_1 z_1 - y_2 z_2)}{(y_2 - y_1)(z_2 - z_1)}, \; y = \frac{(y_2 - y_1)(z_1 x_1 - z_2 x_2)}{(z_2 - z_1)(x_2 - x_1)}, \; z = \frac{(z_2 - z_1)(x_1 y_1 - x_2 y_2)}{(x_2 - x_1)(y_2 - y_1)}.$$

6.6.4 Utilisation

Le lecteur fera lui-même l'expérience de l'utilisation de ce changement de variables et constatera qu'il donne lieu à des calculs plutôt plus simples. Par exemple, la condition définissant les douzains devient $\alpha(\beta-\gamma)^3 = \beta(\gamma-\alpha)^3$ ou l'une des deux conditions analogues obtenues par permutation circulaire.

7 Compléments

7.1 Les douzains

On a vu que la preuve du théorème 6.15 est en défaut si le triangle est un douzain. Cela pose trois questions :

1) Existe-t-il des douzains et comment peut-on en construire ?

2) Quel est le groupe de torsion correspondant à un douzain ?

3) Les douzains donnent-ils obligatoirement des courbes de rang 0 ?

Pour répondre à la première question, utilisons le changement de variables des différences. Il est facile de construire des exemples de triangles non isocèles de paramètres α, β, γ rationnels vérifiant $\alpha(\beta-\gamma)^3 = \beta(\gamma-\alpha)^3$. Si l'on pose $\dfrac{\beta}{\alpha} = \lambda$ et $\dfrac{\gamma}{\alpha} = \mu$, cette équation devient $(\lambda-\mu)^3 = \lambda(\mu-1)^3$ et on voit que λ doit être un cube : $\lambda = q^3$, avec $q \in \mathbf{Q}$ et on trouve $\mu = \dfrac{q(q^2+1)}{q+1}$. En prenant $\alpha = q+1$ avec $q > 0$ on obtient une infinité de solutions qui donnent de vrais triangles :

$$\alpha = q+1, \quad \beta = q^3(q+1), \quad \gamma = q(q^2+1).$$

La réponse à la question 2) est immédiate : si le triangle est un douzain, le groupe de torsion de $\widehat{\Gamma}(\mathbf{Q})$ est $T = \mathbf{Z}/12\mathbf{Z}$. En effet, on a vu que T contient alors un élément d'ordre 4 (si on a $2A = 2A'$, on a $4A = 0$) et comme il contient I qui est d'ordre 3, il contient un élément d'ordre 12 qui l'engendre par Mazur.

La troisième question est plus délicate :

7.1 *Exemple.* Si l'on prend $q = 2$ dans les formules précédentes, on obtient $\alpha = 3$, $\beta = 24$, $\gamma = 10$ ou, si l'on veut des nombres entiers pairs, $6, 48, 20$. On vérifie avec le logiciel Pari que, dans ce cas, $\widehat{\Gamma}$ est de rang 0 avec un groupe de torsion isomorphe à $\mathbf{Z}/12\mathbf{Z}$. Cette solution correspond au triangle de côtés $34, 13, 27$ qui est donc un des (rares) triangles à côtés rationnels qui n'a pas de frère rationnel. En effet, les douze points de $\widehat{\Gamma}$ sont alors, dans le paramétrage des différences, O, I, J, puis $A = (6, 48, 20)$ et ses cinq permutés qui correspondent au triangle initial et $2A = (-8, -8, 90)$ et ses deux permutés, mais ces trois points isocèles ne correspondent pas à des triangles.

Bien entendu, le triangle $34, 13, 27$ a des frères irrationnels, par exemple celui rencontré en 5.5 :

$$\frac{74}{3}, \frac{74}{3} + \frac{98\sqrt{481}}{222}, \frac{74}{3} - \frac{98\sqrt{481}}{222}.$$

7.2 *Remarque.* Cette situation est générale : si p, s sont les invariants d'un vrai triangle A qui est un douzain, la courbe Γ ne contient pas de (vrai) triangle isocèle. En effet, le groupe de torsion de Γ est $\mathbf{Z}/12\mathbf{Z}$ qui ne contient qu'un point d'ordre 2. Il n'y a donc qu'un point isocèle sur Γ, c'est donc $2A$ ou un de ses permutés et comme A est dans la composante bornée, $2A$ n'y est pas (voir 6.6).

Sur la figure 8 ci-dessous, les points A, B, C ont respectivement pour coordonnées $(27, 13)$, $(13, 34)$, $(34, 27)$. Le groupe $\widehat{\Gamma}(\mathbf{Q})$ est isomorphe à $\mathbf{Z}/12\mathbf{Z}$ avec la correspondance suivante : le point à l'infini O dans la direction de l'axe des y est l'élément neutre 0, le point I à l'infini dans la direction de l'axe des x vaut 4, le point J (direction de $y = -x$) vaut -4. Un générateur du groupe est $C = 1$ et les autres sont $D = 2$, $A' = 3$, $B = 5$, $F = 6$, $B' = -5$, $A = -3$, $E = -2$ et $C' = -1$. On note que la partie du groupe située dans les [38] composantes non bornées (qui contiennent l'élément neutre) constitue le sous-groupe $\mathbf{Z}/6\mathbf{Z}$.

7.3 *Exemple.* **Attention**, si le triangle est un douzain, la preuve de 6.15 ne fonctionne plus, mais ce n'est pas pour autant que le rang de $\widehat{\Gamma}$ est nul. Par exemple, on vérifie que le triangle qui correspond à $q = 3$ et qui, à un scalaire près, est de paramètres $\alpha = 4$, $\beta = 108$, $\gamma = 30$ (donc de côtés $69, 17, 56$) est bien un douzain, et pourtant la courbe associée est de rang 1. Avec l'aide de Pari [39] on trouve un triangle frère, avec $(\alpha', \beta', \gamma') = (\frac{27}{10}, \frac{384}{5}, \frac{125}{2})$ et les

38. La composante en projectif.
39. Et du programme *ratpoints* de Michaël Stoll.

côtés $\frac{1393}{20}$, $\frac{163}{5}$ et $\frac{159}{4}$. Avec le paramétrage $\alpha = q+1, \beta = q^3(q+1), \gamma = q(q^2+1)$ on trouve que le rang est nul pour $q = 2$, $q = 4$, $q = 8$ (mais pas $q = 16$) ou encore $q = 1/2$, $q = 3/5$, etc. mais, le plus souvent le rang est 1 et parfois 2 comme pour $q = 12$ ou $q = 7/8$. La question de savoir s'il existe une infinité de douzain "isolés" (c'est-à-dire correspondant à une courbe de rang 0) reste donc posée.

7.2 Points et triangles isocèles, le cas réel

Nous revenons maintenant sur les triangles isocèles, un peu délaissés ci-dessus. Précisons d'abord les notions :

7.4 Définition. *Soit $P = (x, y, z)$ un point de $\mathcal{G}_{p,s}(\mathbf{R})$ (dans la version de l'espace). On dit que P est un* **point isocèle** *si deux de ses coordonnées sont égales. Plus précisément, on dit que P est un point isocèle* **de première espèce** *(resp. de seconde, resp. de troisième) s'il est de la forme (x, y, y) (resp. (x, y, x), resp. (x, x, y)). Sur la courbe plane Γ ces points correspondent respectivement aux points (x, y) vérifiant $y = \frac{p-x}{2}$, $y = p - 2x$, $y = x$.*

Ces points correspondent à des triangles isocèles si et seulement si ils sont dans la composante bornée de Γ.

Le théorème suivant rassemble les résultats utiles sur les points isocèles :

7.5 Théorème. *1) Le point (x, y) de $\Gamma_{p,s}$ est isocèle de première espèce si et seulement si x et y vérifient les équations :*

$$(*) \quad f(x) := 2x^3 - px^2 + 4s - p^3 = 0, \qquad (**) \quad 4y^3 - 5py^2 + 2p^2y - s = 0.$$

Il est de seconde espèce si x vérifie $(**)$ et y vérifie $(*)$ et de troisième espèce si x, y vérifient tous deux $(**)$.

2) Le point P est isocèle de première espèce (resp. de seconde, resp. de troisième) si et seulement si la tangente en P est parallèle à l'axe des y (resp. à l'axe des x, resp. à la droite $x + y = 0$).

3) Le point P est isocèle de première espèce si et seulement si c'est un élément d'ordre 2 du groupe $\widehat{\Gamma}(\mathbf{R})$. C'est un point de seconde espèce (resp. de troisième) si et seulement si l'on a $2P = J$ (resp. $2P = I$) ; un tel point est d'ordre 6 dans le groupe.

Démonstration. 1) Ces équations ont déjà été rencontrées plus haut. On les obtient en remplaçant y par $\frac{p-x}{2}$ ou x par $p - 2y$ dans l'équation $F(x, y) = 0$. L'équation en x provient aussi du calcul de y, z en fonction de x effectué dans la preuve de 5.5 (dire qu'on a $y = z$ signifie que le discriminant $\Delta(x)$ est nul).

2) Si x est un réel, la droite $X = x$ coupe $\widehat{\Gamma}$ en O (à l'infini) et en au plus deux points (x, y) et (x, z) avec y, z donnés par les formules de 5.5. Dire que cette droite est tangente à $\widehat{\Gamma}$ en (x, y) signifie exactement qu'on a $y = z$ donc un point isocèle. Les deux autres cas s'obtiennent en permutant circulairement les coordonnées (x, y, z).

3) Le point précédent signifie qu'on a $P \vee P = O$ (resp. I, resp. J), donc $2P = O$ (resp. J, resp. I). Comme I, J sont d'ordre 3 on voit que les points de seconde et troisième espèce sont d'ordre 6.

7.6 *Remarques.* 1) Reprenons les notations de la preuve de 5.5. On suppose qu'on a les conditions $0 < \frac{27s}{7} < p^3 < 4s$. On peut préciser la localisation des points isocèles de première espèce sur la courbe réelle $\widehat{\Gamma}(\mathbf{R})$. Leurs abscisses sont les réels α, β, γ, racines de $f(x) = 0$, avec $\alpha < 0 < \beta < \gamma$ et le point d'abscisse α est dans la composante non bornée, tandis que les autres sont dans la composante bornée. Par permutation circulaire on voit que deux des points isocèles de seconde et troisième espèce sont dans la composante bornée et un dans la composante non bornée. On voit qu'il y a deux (vrais) triangles isocèles réels, ainsi que leurs permutés, soit six points de la composante bornée, et trois points isocèles ne correspondant pas à des triangles, voir figure 9.

2) Bien entendu, il se peut qu'aucun des points précédents ne soit à coordonnées rationnelles, voir ci-dessous pour une discussion.

3) On vérifie aussitôt que si P est isocèle de type 1, $P + I$ est isocèle de type 2 et $P + J$ de type 3, tandis que si P est isocèle de type 2 (resp. 3), $P + J$ (resp. $P + I$) est isocèle de type 1.

7.3 Points et triangles isocèles, groupe de torsion, le cas rationnel

Soit ABC un triangle à côtés rationnels a, b, c, et soient p et s ses invariants. Nous allons préciser le rang et le groupe de torsion de $\widehat{\Gamma}(\mathbf{Q})$ selon qu'il existe ou non des points isocèles.

7.3.1 En l'absence de points isocèles

Le corollaire suivant précise à la fois le rang et le groupe de torsion :

7.7 Corollaire. *On suppose que $\widehat{\Gamma}(\mathbf{Q})$ ne contient pas de points isocèles (ce qui signifie que le polynôme $4x^3 - 5px^2 + 2p^2x - s$ ou son acolyte $2x^3 - px^2 +$*

$4s - p^3$ *n'a pas de racine rationnelle). Alors le rang de* $\widehat{\Gamma}(\mathbf{Q})$ *est* ≥ 1 *et son groupe de torsion est* $\mathbf{Z}/3\mathbf{Z}$ *ou* $\mathbf{Z}/9\mathbf{Z}$.

Démonstration. En effet, il n'y a pas de points d'ordre 2, ce qui exclut tous les groupes de torsion d'ordre pair et notamment 12 et empêche ABC d'être un douzain, de sorte que le rang est ≥ 1.

7.8 *Remarque.* On trouve facilement des exemples avec $T = \mathbf{Z}/3\mathbf{Z}$ (par exemple le triangle de côtés $3, 4, 5$). Il est beaucoup plus difficile d'en trouver avec $T = \mathbf{Z}/9\mathbf{Z}$. C'est l'objet du paragraphe suivant.

7.3.2 Le cas $T = \mathbf{Z}/9\mathbf{Z}$

7.9 Théorème. *Il existe des triangles à côtés rationnels tels que le groupe de torsion de* $\widehat{\Gamma}$ *soit* $\mathbf{Z}/9\mathbf{Z}$*, par exemple le triangle de côtés* $\dfrac{8621}{19800}$, $\dfrac{739}{1980}$ *et* $\dfrac{159}{2200}$.

Démonstration. On utilise le changement de variables des différences. Il suffit de disposer d'un point[40] C d'ordre 9, donc vérifiant $3C = I$, ou encore $2C = I - C$. Ce point n'est pas isocèle, de sorte qu'on peut supposer qu'il s'écrit $C = (x, y, z)$ avec x, y, z distincts. Posons $A = (y, z, x)$. Les calculs vus en 6.8 donnent $I = C - A$ et la relation cherchée est donc équivalente à $2C = -A$ ou encore $C \vee C = A$. En utilisant 6.22 on trouve la relation $y^2z+z^2x+x^2y-3xyz = 0$. On a de nouveau affaire à une cubique plane, mais celle-ci est singulière au point $(1, 1, 1)$ (en affine x, y si on pose $X = x - 1$ et $Y = y-1$, la courbe devient $X^2Y + X^2 - XY + Y^2 = 0$). On paramètre cette courbe en coupant par une droite $Y = tX$ qui passe par le point singulier. On obtient les points $x = -\dfrac{(t-1)^2}{t}$, $y = t(1-t)$, $z = 1$. Ces points sont sur la courbe $\Gamma_{p,m}$ avec $p = \dfrac{-t^3+3t-1}{t}$ et $m = (t-1)^3$. Pour que cette courbe soit associée à un vrai triangle il faut avoir $p > 0$, $m > 0$ et $\dfrac{p^3}{27} < m$. Cette condition est réalisée $t > 1$, assez voisin de 1. Attention, même avec cette condition, il se peut que la courbe soit de rang 0 (par exemple pour $t = 6/5$, $p = \dfrac{109}{150}$ et $m = \dfrac{1}{125}$, Pari *dixit*), auquel cas elle ne correspond pas à un triangle. Prenons $t = 11/10$, $p = \dfrac{969}{1100}$ et $m = \dfrac{1}{1000}$. Pari affirme que la courbe est de rang 1, mais encore faut-il exhiber des points dans la composante bornée. Il suffit pour cela de trouver des entiers positifs u, v, w, k

40. La difficulté est que ce point ne saurait être dans la composante bornée de Γ.

vérifiant $969k = u + v + w$ et $11^3 \times 10^3 \times k^3 = uvw$, car alors $x = \dfrac{u}{1100k}$, $y = \dfrac{v}{1100k}$, et $z = \dfrac{w}{1100k}$ conviennent. Une recherche systématique avec *xcas* donne $k = 9$, $u = 100$, $v = 1331$, $w = 7290$, qui donnent $x = \dfrac{1}{99}$, $y = \dfrac{121}{900}$ et $z = \dfrac{81}{110}$ et les longueurs des côtés annoncées.

7.3.3 En présence de points isocèles

On suppose toujours qu'on a un triangle ABC à côtés rationnels a, b, c, d'invariants p, s, on étudie $\widehat{\Gamma}(\mathbf{Q})$ et on suppose que cette courbe contient un point isocèle rationnel.

On a vu qu'elle contient des points d'ordre 2, et donc aussi des points d'ordre 6 en utilisant les inflexions I, J. Le groupe de torsion est donc égal à $\mathbf{Z}/6\mathbf{Z}$, $\mathbf{Z}/12\mathbf{Z}$ ou $\mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Plusieurs questions se posent alors :

1) Tous ces cas sont-ils possibles ?

2) Existe-t-il de telles courbes de rang nul, de rang positif ?

3) Les points isocèles sont-ils nécessairement des triangles, ou encore, le sous groupe de torsion peut-il être inclus dans la composante non bornée ?

Nous allons donner des exemples des divers types possibles. La plupart d'entre eux sont calculés grâce à la procédure expliquée en 4.6 et à quelques lignes de programme sur *xcas*.

7.3.4 Le cas $T = \mathbf{Z}/6\mathbf{Z}$

Le groupe contient un unique point isocèle et il y a trois situations possibles :

• Le point isocèle est un vrai triangle isocèle rationnel admettant un frère rationnel non isocèle, par exemple $(3, 18, 18)$ et $(6, 14, 19)$. La courbe est de rang 1.

• Le point isocèle est un vrai triangle isocèle rationnel sans frère rationnel non isocèle, comme $(1, 4, 4)$. La courbe est de rang 0.

• Le point isocèle n'est pas un triangle, mais il admet un frère qui est un triangle rationnel. C'est le cas de $(-2, 9, 9)$ qui admet le frère $(7, 6, 3)$ ($p = 16$, $s = 1044$). Le rang est 1 en vertu de 6.15 (le triangle ABC n'est pas un douzain). Dans ce cas, le groupe de torsion est tout entier dans la composante non bornée. (Expliquons comment on trouve cet exemple. On part de l'équation des points isocèles $2x^3 - px^2 + 4s - p^3 = 0$, on impose la racine négative -2. Il reste $m := 4s - p^3 = 16 + 4p$. On utilise le changement de variable des différences : $p = \alpha + \beta + \gamma$, $m = \alpha\beta\gamma$ et on tire $\gamma = \dfrac{16 + 4(\alpha + \beta)}{\alpha\beta - 4}$,

dont on cherche une solution positive. En prenant $\alpha = 2, \beta = 4$ on a $\gamma = 10$ donc $a = 7$, $b = 6$, $c = 3$.)

7.3.5 Le cas $T = \mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$

Le groupe contient trois points isocèles dont deux sont des vrais triangles en vertu de 7.6. Il y a deux cas :

• La courbe est de rang 0, donc ses points rationnels sont réduits au groupe de torsion. C'est le cas[41] des triangles isocèles rationnels $(3, 14, 14)$ et $(8, 8, 15)$.

• La courbe est de rang 1. C'est le cas des deux triangles isocèles rationnels $(15, 32, 32)$ et $(22, 22, 35)$ (ou en variante différence $49, 15, 15$ et $35, 35, 9$ avec $p = 79$, $m = 11025$).

7.3.6 Le cas $T = \mathbf{Z}/12\mathbf{Z}$

Le point isocèle est l'unique élément d'ordre 2 de T, qui est le double des éléments d'ordre 4. Il est donc dans la composante non bornée en vertu de 6.6 (comme d'ailleurs tout le sous-groupe $\mathbf{Z}/6\mathbf{Z}$). Il n'y a donc pas de vrai triangle isocèle. Deux cas sont possibles *a priori* :

• Le groupe de torsion T contient un vrai triangle. Dans ce cas, il en contient 6 (les éléments d'ordre 4 ou 12 de T) et on est dans le cas d'un douzain, le rang peut être nul ou positif, voir paragraphe précédent.

• Le groupe de torsion est entièrement contenu dans la composante non bornée. J'ignore si ce cas est possible en présence d'un vrai triangle ABC.

7.4 Les vrais triangles à côtés entiers

Nous reprenons ici la problématique des triangles à côtés entiers, de manière plus sérieuse, c'est-à-dire en refusant les exemples non primitifs (i.e. avec des côtés non premiers entre eux).

7.10 Théorème. *Il existe une infinité de triangles non isocèles à côtés entiers a, b, c et x, y, z, de même aire et même périmètre, avec à la fois a, b, c et x, y, z premiers entre eux.*

Démonstration. On commence par montrer le lemme suivant, inspiré par le changement de variables des différences :

41. Pour les petites valeurs, ce cas semble plus fréquent. Ainsi, on a la même situation pour $(4, 11, 11)$ et $(7, 7, 12)$ ou encore $(6, 11, 11)$, $(8, 8, 12)$.

7.11 Lemme. *Il existe une infinité de paires de triplets distincts $\alpha, \beta, \gamma \in \mathbf{N}^*$ et $\xi, \eta, \zeta \in \mathbf{N}^*$ avec $\alpha < \beta < \gamma$ et $\xi < \eta < \zeta$ tels que l'on ait $\alpha + \beta + \gamma = \xi + \eta + \zeta$ et $\alpha\beta\gamma = \xi\eta\zeta$. On peut supposer, de plus, que les nombres en question sont tous impairs.*

Démonstration. (du lemme) On cherche les entiers sous la forme suivante [42] : $\alpha = uv$, $\beta = w$, $\gamma = t$ et $\xi = wt$, $\eta = u$, $\zeta = v$ avec u, v, w, t entiers > 0. Cette écriture assure que la condition $\alpha\beta\gamma = \xi\eta\zeta$ est réalisée et il reste celle sur la somme, qui s'écrit $uv+w+t = wt+u+v$, soit encore $uv-u-v = wt-w-t$. En ajoutant 1 aux deux membres on est ramené à $(u-1)(v-1) = (w-1)(t-1)$ que l'on résout en posant $u = pq + 1$, $v = rs + 1$, $w = pr + 1$ et $t = qs + 1$, avec pour p, q, r, s des entiers > 0. Pour avoir $\alpha, \ldots, \zeta$ impairs, il suffit de prendre p, q, r, s pairs et on obtient une infinité d'exemples en prenant $p = 2$, $q = 4$, $r = 6$ et $s = 2k$, $k \geq 4$.

7.12 *Remarques.* 1) La question analogue avec deux entiers α, β est évidente : ils sont déterminés par leur somme et leur produit. Bien entendu, avec trois entiers α, β, γ la somme $p = \alpha+\beta+\gamma$ et le produit $m = \alpha\beta\gamma$ ne suffisent plus (il faudrait se donner aussi la troisième fonction symétrique $\beta\gamma + \gamma\alpha + \alpha\beta$).

2) La plus petite solution [43] obtenue par ce procédé est $(2, 16, 24\,; 4, 6, 32)$ qui donne des triangles de côtés $(20, 13, 9)$ et $(19, 18, 5)$. Un programme rudimentaire sur *xcas* donne 35 solutions avec tous les entiers ≤ 40 en un peu plus d'une heure.

Revenons au théorème. On trouve les côtés a, b, c du triangle associé à α, β, γ en en prenant les demi-sommes (qui sont des entiers si α, β, γ sont impairs) et de même pour x, y, z à partir de ξ, η, ζ. Ensuite, il faut s'assurer que les a, b, c obtenus sont premiers entre eux. Si un nombre premier l divise a, b, c ou x, y, z, il divise aussi $a + b - c$, etc. donc α, β, γ ou ξ, η, ζ. On aura gagné si l'on s'assure que ces nombres sont premiers entre eux. Une méthode pour construire une infinité de tels exemples est la suivante. On prend $p = r = 2$ (donc $w = 5$), puis pour q un nombre pair tel que $u = pq+1$ soit premier et > 5 (il en existe une infinité, puisqu'il y a une infinité de nombres premiers congrus à 1 modulo 4). Ensuite on prend s pair tel que $v = rs + 1$ soit premier et $> u$. Alors, il est clair que ξ, η, ζ sont premiers entre eux (à cause de $\eta = u$ et $\zeta = v$). Mais α, β, γ le sont aussi, car le seul diviseur premier de $\beta = w = 5$ est 5, qui ne divise pas $\alpha = uv$.

On vérifie aisément que les triangles obtenus ne sont pas isocèles. De plus, ils ne sont pas isométriques car β est égal à 5 et qu'aucun des ξ, η, ζ ne vaut 5 (on note que $\xi = wt = 5t$ est au moins égal à 25 car q et s sont ≥ 2).

42. On les remet dans l'ordre ensuite.

43. Avec des entiers de même signe, mais pas nécessairement impairs.

7.13 *Remarque.* Le premier exemple ainsi obtenu l'est pour $q = 6$ et $s = 8$, on trouve $u = 13$, $v = 17$, $w = 5$, $t = 49$ et les triangles $113, 135, 27$ et $129, 131, 15$.

7.5 Questions et conjectures

L'étude précédente a laissé un certain nombre de points dans l'ombre sur lesquels on peut poser des questions et hasarder des conjectures. Rappelons les notations : on se donne a, b, c trois nombres rationnels positifs vérifiant $|b - c| < a < b + c$ et on pose $p = a + b + c$ et $s = (bc + ca + ab)p - 2abc$. On note Γ la courbe elliptique $\Gamma_{p,s}$. Commençons par la question du rang de la courbe $\widehat{\Gamma}$.

7.14 Question. *On a vu ci-dessus des exemples de courbes $\widehat{\Gamma}$ de rang 0 et 1. La question est de savoir quels rangs sont possibles.*

Sur ce sujet, l'expérience semble mener à une conjecture :

7.15 Conjecture. *S'il existe deux triangles, de même aire et même périmètre, avec deux triplets de côtés entiers premiers entre eux et distincts, le rang de la courbe est toujours ≥ 2.*

Rappelons qu'on dispose d'une infinité de tels triangles (voir 7.10). L'expérience faite avec Pari sur de nombreux exemples semble corroborer cette conjecture. On trouve d'ailleurs parfois des courbes de rang 3 comme avec les triplets $6, 22, 23$ et $8, 19, 24$ ($p = 51$, $m = 1365$, $s = 33504$).

Il reste aussi la question des vrais douzains :

7.16 Question. *Existe-t-il une infinité de triangles qui soient des douzains isolés, c'est-à-dire tels que la courbe elliptique associée soit de rang 0, ou encore tels que $\widehat{\Gamma}(\mathbf{Q})$ soit réduite à son groupe de torsion $\mathbf{Z}/12\mathbf{Z}$?*

En ce qui concerne le sous-groupe de torsion, il reste une seule question :

7.17 Question. *Existe-t-il des vrais triangles rationnels avec un groupe de torsion $\mathbf{Z}/12\mathbf{Z}$ entièrement contenu dans la composante non bornée ?*

8 Annexes

8.1 Annexe 1 : Γ écrite sous forme de Weierstrass

Il est commode, notamment pour utiliser les logiciels de calcul, d'écrire la courbe Γ sous forme canonique $Y^2T = X^3 + AXT^2 + BT^3$.

Pour cela, à partir de la variante projective plane en x, y, t :

$$\widehat{F}(x,y,t) := 2xy(x+y) - p(x^2+y^2+3xy)t + p^2(x+y)t^2 - st^3 = 0.$$

on effectue successivement les changements de variables suivants :

1) On pose $X_1 = t$, $Y_1 = y$ et $T_1 = 2x - pt$.

2) On pose $X_2 = X_1$, $Y_2 = Y_1 + \dfrac{T_1 - pX_1}{4}$, $T_2 = T_1$.

3) On pose $X_3 = X_2 + \dfrac{p^2 T_2}{12(4s-p^3)}$, $Y_3 = Y_2$, $T_3 = T_2$.

4) Enfin, on pose $X = \dfrac{4s-p^3}{4} X_3$, $Y = \dfrac{4s-p^3}{4} Y_3$ et $T = T_3$. On obtient une expression de la forme annoncée avec :

$$A = \frac{p}{32}\left(4s - \frac{25p^3}{24}\right),$$

$$B = \frac{p^6}{16 \times 3456} - \frac{p^3(4s-p^3)}{16 \times 96} + \frac{(4s-p^3)^2}{256}.$$

8.2 Annexe 2 : l'article de Mc Callum

Dans l'article *Le conte des deux triangles : triangles de Héron et courbes elliptiques* du Projet Klein écrit par William Mc Callum, il propose une autre paramétrisation pour étudier le problème des triangles d'aire et périmètre donnés. Le principe est le suivant. Soit ABC un triangle, I le centre du cercle inscrit, r son rayon, A', B', C' les projetés orthogonaux de I sur $[BC]$, $[CA]$ et $[AB]$ respectivement. On note $\alpha = \widehat{BIC}$, $\beta = \widehat{CIA}$ et $\gamma = \widehat{AIB}$ et on pose $x = \tan\frac{\alpha}{2}$, $y = \tan\frac{\beta}{2}$ et $z = \tan\frac{\gamma}{2}$. Avec ces paramètres, on calcule le périmètre du triangle qui vaut $p = r(x+y+z)$ et son aire qui est égale égale à $rp/2$. Par ailleurs, on a $\alpha + \beta + \gamma = 2\pi$, ce qui en passant aux tangentes fournit la relation $xyz = x+y+z$. En définitive, pour les triangles de périmètre p et d'aire $\mathcal{A}$ on a les deux équations $x+y+z = xyz = \dfrac{p^2}{2\mathcal{A}}$. On trouve une courbe elliptique et en éliminant z on en a une version plane :

$$xy(x+y) - kxy - k = 0$$

avec $k = \dfrac{p^2}{4\mathcal{A}}$. De plus, on calcule aisément les côtés à partir des paramètres x, y, z. Par exemple, on a $a = BC = BA' + A'C = r\tan\frac{\alpha}{2} + r\tan\frac{\gamma}{2} = r(y+z)$ et de même pour les autres ou, à l'envers, $x = \dfrac{p}{4\mathcal{A}}(b+c-a)$ etc.

En fait, le défaut de cette méthode est qu'on perd la rationalité (par exemple, si a, b, c sont rationnels, x, y, z ne le sont pas nécessairement car

l'aire n'est pas nécessairement le carré d'un rationnel, sauf pour les triangles de Héron, voir ci-dessous). C'est ce qui m'a conduit à adapter cette méthode en introduisant le changement de variable vu en 6.6.1.

8.3 Annexe 3 : Héron d'Alexandrie

8.3.1 La formule de Héron

On considère un triangle ABC de côtés a, b, c et son aire $\mathcal{A}$. Une conséquence immédiate de la formule donnant le double de l'aire comme base multipliée par hauteur est $2\mathcal{A} = bc \sin \widehat{A}$. Par ailleurs, on sait calculer $\cos \widehat{A}$ par la formule d'Al-Kashi : $a^2 = b^2 + c^2 - 2bc \cos \widehat{A}$. On en déduit le carré de l'aire grâce à la formule $\cos^2 \widehat{A} + \sin^2 \widehat{A} = 1$:

$$16\mathcal{A}^2 = 4b^2c^2 - (b^2 + c^2 - a^2)^2$$

et il n'y a plus qu'à utiliser les identités remarquables [44] :

$$16\mathcal{A}^2 = (2bc + b^2 + c^2 - a^2)\,(2bc - b^2 - c^2 + a^2) = ((b+c)^2 - a^2)\,(a^2 - (b-c)^2)$$

$$= (a+b+c)(b+c-a)(c+a-b)(a+b-c).$$

Voici une autre manière de faire, qui évite la trigonométrie. Soit H le projeté orthogonal de A sur (BC). Quitte à changer de côté, on peut le supposer dans $[BC]$. Posons $x = BH$. En appliquant Pythagore dans ABH et ACH on calcule $x = \dfrac{a^2 + c^2 - b^2}{2a}$, puis $AH^2 = \dfrac{4a^2c^2 - (a^2 + c^2 - b^2)^2}{4a^2}$ et on finit le calcul comme ci-dessus.

8.3.2 Les triangles de Héron

Il s'agit de triangles dont les côtés a, b, c sont entiers, ainsi que l'aire, dont Héron a donné le premier exemple avec $13, 14, 15$, d'aire 84. Ils ont été abondamment étudiés depuis l'Antiquité et le sont encore de nos jours, voir L. Dickson *History of Number Theory* vol. II, p. 191. Le mathématicien indien Brahmagupta (598-668) en a donné une famille infinie $a = (y+z)(x^2 - yz)$, $b = y(x^2 + z^2)$, $c = z(x^2 + y^2)$ avec x, y, z entiers. L'idée est toute simple : on accole deux triangles rectangles à côtés entiers par l'un de leurs côtés de l'angle droit (les côtés et la hauteur du triangle obtenu sont alors entiers). Pour Héron, il s'agit des triangles $5, 12, 13$ et $9, 12, 15$, pour Brahmagupta, c'est facile à partir des triangles pythagoriciens de côtés $x^2 + z^2$, $x^2 - z^2$, $2xz$

44. Dont c'est une superbe application.

et x^2+y^2, x^2-y^2, $2xy$ en multipliant le premier par y et le second par z et en les accolant le long du côté $2xyz$.

La question de savoir s'il existe plusieurs paires de triangles de Héron ayant même aire et même périmètre est évidemment plus difficile que celle que nous avons abordée. La réponse est positive, on en a même une infinité d'exemples, mais pas – à ma connaissance – avec des solutions primitives (i.e. a, b, c et x, y, z premiers entre eux). Voir l'article de Kramer et Luca : *Some remarks on Heron triangles*, Acta Acad. Paed. Agriensis, Sectio Mathematicae 27 (2000) 25–38.

8.4 Annexe 4 : l'inégalité isopérimétrique

On prouve ici, de manière élémentaire, le lemme suivant, pas décisif vers l'inégalité isopérimétrique 5.3 :

8.1 Théorème. *Soient α, β, γ des réels ≥ 0.*

On a l'inégalité $27\alpha\beta\gamma \leq (\alpha+\beta+\gamma)^3$, l'égalité n'ayant lieu que si α, β et γ sont égaux.

Démonstration. On note qu'on peut supposer que α, β, γ sont non nuls. On montre d'abord le cas particulier du "triangle" isocèle :

8.2 Lemme. *Soient α, γ des nombres ≥ 0. On a $27\alpha^2\gamma \leq (2\alpha+\gamma)^3$, avec égalité si et seulement si $\alpha = \gamma$.*

Démonstration. En développant le cube, on voit que l'inégalité équivaut à :

$$8\alpha^3 - 15\alpha^2\gamma + 6\alpha\gamma^2 + \gamma^3 \geq 0,$$

ce qui s'écrit encore :

$$8\alpha^3 - 16\alpha^2\gamma + 8\alpha\gamma^2 + \alpha^2\gamma - 2\alpha\gamma^2 + \gamma^3 \geq 0$$

c'est-à-dire :

$$8\alpha(\alpha^2 - 2\alpha\gamma + \gamma^2) + \gamma(\alpha^2 - 2\alpha\gamma + \gamma^2) \geq 0$$

et on a le résultat.

Pour conclure, il reste à se ramener au cas du "triangle" isocèle :

8.3 Lemme. *Soient α, β, γ trois nombres positifs non tous égaux et supposons par exemple $\alpha \neq \beta$. Alors, si l'on pose $\alpha' = \dfrac{\alpha+\beta}{2}$, on a $\alpha\beta\gamma < \alpha'^2\gamma$ et $\alpha+\beta+\gamma = 2\alpha'+\gamma$.*

Démonstration. C'est clair car on a $\alpha\beta < \alpha'^2$ en vertu de l'inégalité $(\alpha+\beta)^2 > 4\alpha\beta$, équivalente à $(\alpha-\beta)^2 > 0$.

8.4 *Remarque.* En fait, le lemme 8.3 suffit presque à prouver le théorème, à condition de disposer de connaissances de topologie. En effet, soient α, β, γ trois réels ≥ 0, posons $p = \alpha + \beta + \gamma$ et considérons :

$$K = \{(x, y, z) \in \mathbf{R}^3 \mid x \geq 0, y \geq 0, z \geq 0 \text{ et } x + y + z = p\}.$$

Il est clair que K est un compact, de sorte que la fonction $f(x, y, z) = 27xyz$ admet un maximum M sur K. Le lemme montre qu'il ne peut être atteint que lorsque les trois nombres x, y, z sont égaux et qu'il vaut donc p^3, ce qui établit le théorème.

8.5 Annexe 5 : prouver géométriquement les lemmes sur les triangles isocèles

Dans ce paragraphe, on montre les lemmes vus en 3.4, mais par des arguments géométriques. La formule de Héron en est l'ingrédient essentiel.

On commence par le lemme suivant :

8.5 Lemme. *Soit $T = ABC$ un triangle.*

1) Soit $A'BC$ le triangle isocèle de même base $[BC]$ et même périmètre que T. Alors, l'aire de T' est supérieure ou égale à celle de T.

2) Soit $T'' = A''BC$ le triangle isocèle de même base $[BC]$ et même hauteur que T. Alors, le périmètre de T'' est inférieur ou égal à celui de T.

Démonstration. 1) Notons a, b, c les longueurs des côtés de T et p son périmètre. Ceux de T' sont alors a, b', b' avec $b' = \frac{b+c}{2}$. La formule de Héron donne $16\mathcal{A}(T)^2 = p(p-2a)(p-2b)(p-2c)$ et $16\mathcal{A}(T')^2 = p(p-2a)(p-2b')(p-2b')$. Il suffit donc de montrer qu'on a $(p-2b)(p-2c) \leq (p-2b')^2$, mais comme on a $b+c = 2b'$, il reste à voir $bc \leq b'^2$, ce qui est n'est autre que $(b-c)^2 \geq 0$.

2) Considérons maintenant T' et T''. Comme on a $\mathcal{A}(T'') = \mathcal{A}(T) \leq \mathcal{A}(T')$, on voit que la hauteur de T' est plus grande que celle de T'', donc aussi, comme ils ont même base, les côtés (par Pythagore) et le périmètre.

8.6 Lemme. *Soit $T = ABC$ un triangle isocèle de base $BC = a$ et de côté $AB = AC = b$. On suppose $a < b$ (resp. $a > b$) et on choisit une longueur x vérifiant $a < x < b$ (resp. $a > x > b$).*

1) Soit $T' = A'BC'$ le triangle isocèle de base $BC' = x$ et de même périmètre que T. Alors on a $\mathcal{A}(T') > \mathcal{A}(T)$.

2) Soit $T'' = A''BC'$ le triangle isocèle de base $BC' = x$ et de même aire que T. Alors, on a $p(T'') < p(T)$.

Démonstration. 1) Supposons par exemple $a < b$, l'autre cas est analogue. On note b' l'autre côté de T'. Grâce à la formule de Héron, il suffit de prouver $(2b-a)a^2 < (2b'-x)x^2$. Mais, comme on a $p = 2b+a = 2b'+x$, il reste $pa^2 - 2a^3 < px^2 - 2x^3$ soit encore $2(x-a)(x^2+ax+a^2) < p(x-a)(x+a)$. Comme $x-a$ est positif, on obtient, en remplaçant p par $2b+a$, $2x^2+ax+a^2 < 2bx+2ab$, ce qui est clair car on a $2x^2 < 2bx$ et $a(x+a) < a(2b)$.

2) Le raisonnement est identique à celui du point 2) de 8.5.

8.6 Annexe 6 : côtés rationnels ou coordonnées rationnelles ?

Dans ce qui précède nous avons abondamment étudié les triangles dont les côtés sont rationnels, mais il y a en fait deux notions :

8.7 Définition. *Soit $T = ABC$ un triangle du plan réel muni d'un repère orthonormé.*

1) On dit que T est **à côtés rationnels** *si les nombres $a = BC$, $b = CA$ et $c = AB$ sont rationnels.*

2) On dit que T est **à coordonnées rationnelles** *s'il existe un triangle $A'B'C'$ isométrique à T tel que les points A', B', C' soient à coordonnées rationnelles dans le repère donné.*

8.8 Lemme. *1) Si T est à côtés rationnels son périmètre est rationnel.*

2) Si T est à coordonnées rationnelles, son aire est rationnelle.

Démonstration. 1) est évident et 2) se voit en utilisant l'expression de l'aire comme $\frac{1}{2}\det(\overrightarrow{AB}, \overrightarrow{AC})$.

Ce lemme permet de montrer que les deux notions ne sont pas équivalentes :

8.9 *Exemples.* 1) Le triangle équilatéral de côté unité n'est pas à coordonnées rationnelles.

2) Le triangle isocèle rectangle bâti sur le repère n'est pas à côtés rationnels.

Le résultat suivant montre que la rationalité de l'aire et du périmètre est la seule obstruction à l'équivalence :

8.10 Théorème. *Soit ABC un triangle dont l'aire et le périmètre sont rationnels. Alors, il est à côtés rationnels si et seulement si il est à coordonnées rationnelles.*

Démonstration. 1) Supposons a, b, c rationnels et prenons $B = (0, 0)$, $C = (a, 0)$ et $A = (x, y)$. Il s'agit de voir que x et y sont rationnels. On a $\mathcal{A}(ABC) = \frac{1}{2}ay$, de sorte que y est rationnel. Par ailleurs, comme b^2 et c^2 sont rationnels, $x^2 + y^2$ et $(x - a)^2 + y^2$ le sont aussi, donc x^2, puis ax et enfin x et ABC est bien à coordonnées rationnelles.

2) Inversement, supposons ABC à coordonnées rationnelles. Par Pythagore, a^2, b^2 et c^2 sont rationnels. Comme $p = a+b+c$ l'est aussi, il en résulte que p^2 l'est, donc aussi $bc + ca + ab$. Enfin, l'aire étant rationnelle, on voit que $4sp - p^4$ est rationnel, donc aussi s et donc abc. Autrement dit, les trois fonctions symétriques de a, b, c sont rationnelles. Soit $P(X)$ le polynôme de $\mathbf{Q}[X]$ dont les racines sont a, b, c. Comme a^2 est rationnel, ce polynôme a une racine dans une extension quadratique de $\mathbf{Q}$, donc n'est pas irréductible. Il a donc une racine rationnelle, disons a. Mais alors, b, c sont tels que leur somme, leur produit et leurs carrés soient rationnels. Si d est le discriminant de l'équation du second degré dont b, c sont racines, on a $b = \alpha + \beta\sqrt{d}$ et $c = \alpha - \beta\sqrt{d}$ avec d, α, β rationnels. Si $\sqrt{d}$ n'est pas rationnel, comme b^2 l'est c'est que α ou β est nul. Si c'est β, on voit que b, c sont rationnels, si c'est α, ils sont opposés et c'est impossible car ils sont > 0.

8.11 *Exemple.* Ce théorème montre que le triangle rectangle de côtés $3, 4, 5$ a des frères à coordonnées rationnelles, par exemple le triangle ABC avec $B = (0, 0)$, $C = (41/15, 0)$ et $A = (1691/861, 180/41)$.

8.12 *Remarque.* Ce théorème permet de voir qu'un triangle, même d'aire et de périmètre rationnels, n'a pas toujours de frère à coordonnées rationnelles. Il suffit de reprendre l'exemple 6.21.1 : $p = 4$, $s = \frac{65}{4}$ ou encore $\mathcal{A} = \frac{1}{4}$ et, comme on a vu qu'il n'y a pas de triangle à côtés rationnels dans la fratrie, il n'y en a pas non plus à coordonnées rationnelles.

9 Références

[Mazur] **Mazur Barry** *Modular curves and the Eisenstein ideal*, Publications mathématiques de l'IHÉS, tome 47 (1977), p. 33-186.

[Schappacher] **Schappacher Norbert** *Développement de la loi de groupe sur une cubique*, Séminaire de Théorie des Nombres Paris 1988/89, Progress in Mathematics 91 (Birkhäuser) 1991, 159–184.

[Waldchmidt] **Waldschmidt Michel**, *Topologie des points rationnels*, Cours de troisième cycle, 1994/95, Université Pierre et Marie Curie (disponible sur Internet)

Remerciements

Je remercie Bernadette Perrin-Riou pour m'avoir installé *Pari* et m'avoir initié à son fonctionnement et Marie-Claude David pour sa lecture attentive et ses remarques.

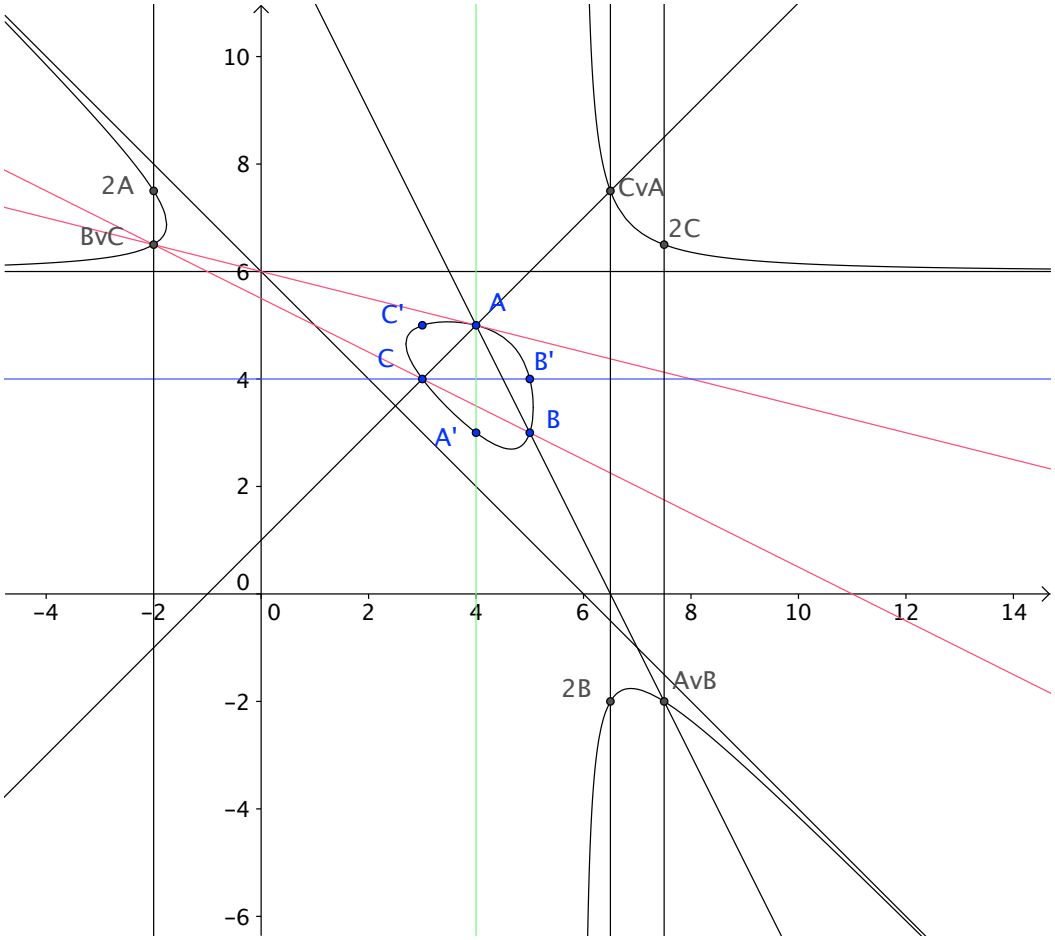

FIGURE 7 – La figure correspond au cas $3, 4, 5$. On y voit les douze points $A, B, C, A', B', C', 2A, 2B, 2C$ et O, I, J (les trois directions asymptotiques). Ici les points $2A' = B \vee C$, etc. sont distincts des précédents.

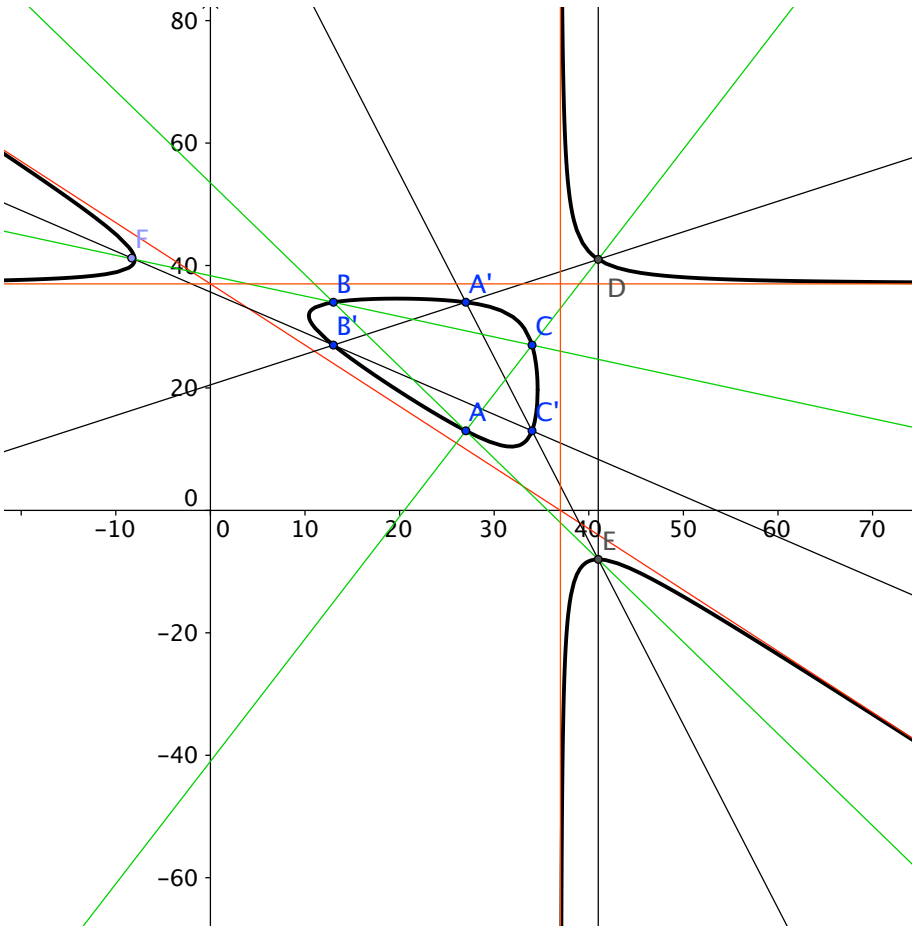

FIGURE 8 – Le douzain $(34, 27, 13)$

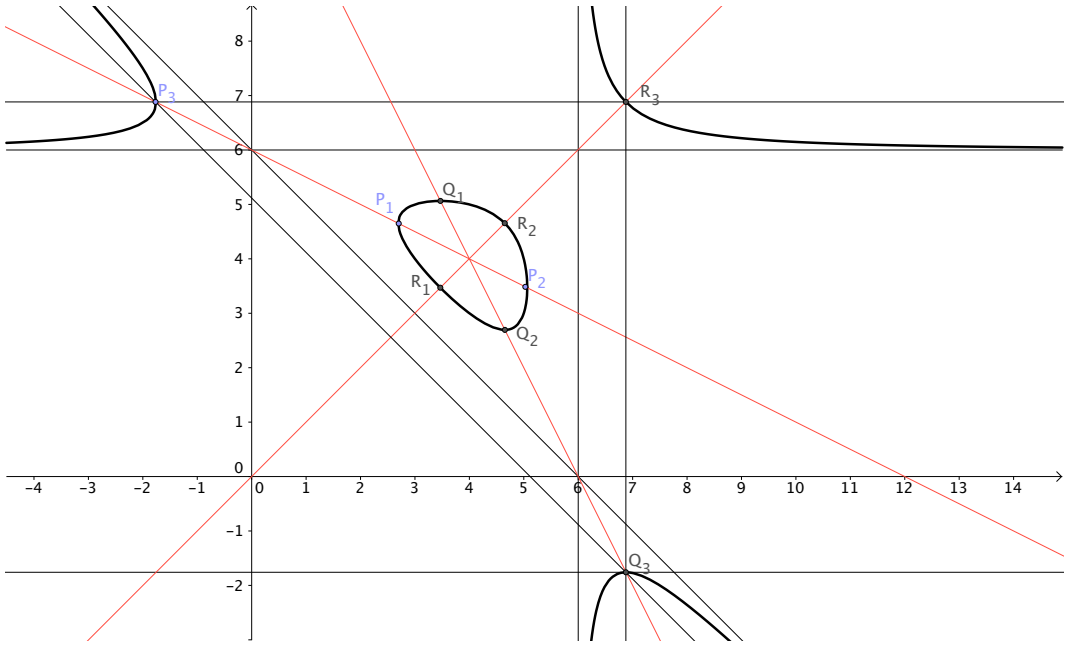

FIGURE 9 – Les points isocèles sur la courbe elliptique. Les points P, Q, R sont d'espèce $1, 2, 3$ respectivement.