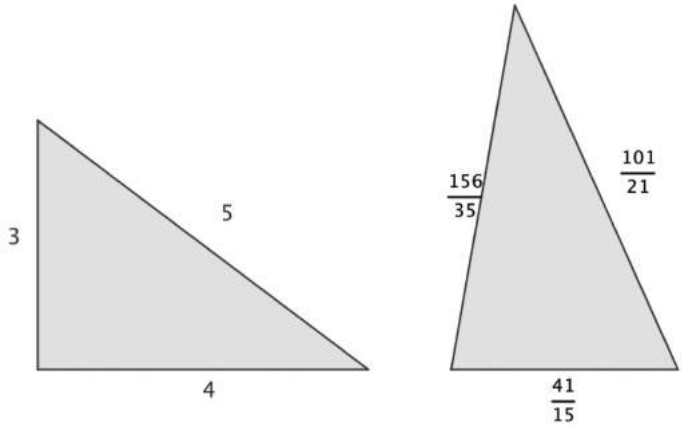
Formule de Héron et courbes elliptiques

William Gordon McCallum, Université de l'Arizona
Traduction de Catherine Combelles

Ce texte est une « vignette » du projet Klein. Le texte d'origine, en anglais, se trouve à l'adresse : http://wikis.zum.de/dmuw/Heron_Triangles_and_Elliptic_Curves

Histoire d'une paire de triangles



La question suivante est apparue dans un groupe de travail entre enseignants et mathématiciens, aux États-Unis, dans le cadre du « Focus on Math project. »(1) :
Si deux triangles ont la même aire et le même périmètre, sont-ils nécessairement isométriques ?
Il s'avère que la réponse est non. Par exemple, le triangle de côtés 3, 4, 5 a la même aire et le même périmètre que le triangle de côtés 41/15, 101/21, et 156/35.
En effet , pour les périmètres :

$$\frac{41}{15}+\frac{101}{21}+\frac{156}{35}=\frac{287+505+468}{105}=\frac{1260}{105}=12=3+4+5.$$

L'aire du triangle de côtés 3, 4, 5 est : $\frac{1}{2}4\cdot 3=6.$

(1) On trouvera à l'adresse http://www.focusonmath.org/ le site de ce projet qui fournit aux professeurs de Mathématiques ressources et formation.
Pour voir le travail du groupe sur cette question, voir : Steven Rosenberg, Michael Spillane, and Daniel~B. Wulf, *Delving deeper: Heron triangles and moduli spaces*, Mathematics Teacher 101 (2008), nº.~9, 656

Pour trouver l'aire du deuxième triangle, utilisons la formule de Héron, qui fournit l'aire d'un triangle à partir des longueurs des côtés, notées a, b, c. Elle est donnée par :

$$\begin{aligned} \mathrm{A} &= \frac{1}{4}\sqrt{(a+b+c)(-a+b+c)(a-b+c)(a+b-c)} \\ &= \sqrt{p(p-a)(p-b)(p-c)} \end{aligned}$$

où $p = \frac{1}{2}(a+b+c)$ est le demi-périmètre du triangle. Un rapide calcul utilisant cette formule montre que l'aire du deuxième triangle est, elle aussi, 6.

L'espace des triangles

Comment trouver des exemples tels que celui-ci ? Le secret est de trouver la bonne façon de représenter l'espace des triangles. Il y a de nombreuses façons de le faire ! Par exemple, on peut considérer l'espace des triangles comme un sous-ensemble de l'ensemble $\mathbb{R}^3$ des triplets (a, b, c). Tous les points de $\mathbb{R}^3$ ne correspondent pas à un triangle. Par exemple, toutes les coordonnées doivent être positives. Voyez-vous d'autres restrictions ?

Il y a une autre façon de mettre des coordonnées sur l'espace des triangles, en utilisant des angles plutôt que des longueurs. Tout triangle possède un cercle inscrit, et il existe une relation simple entre le rayon r de ce cercle, l'aire A du triangle, et son demi-périmètre p :

$$\mathrm{A} = rp \qquad (1)$$

Pour le prouver, traçons les perpendiculaires aux côtés du triangle passant par le centre du cercle inscrit. Ces perpendiculaires sont les hauteurs de trois petits triangles ayant pour bases les côtés du grand triangle et pour sommet le centre du cercle inscrit. En additionnant les aires de ces triangles, on obtient l'équation (1).

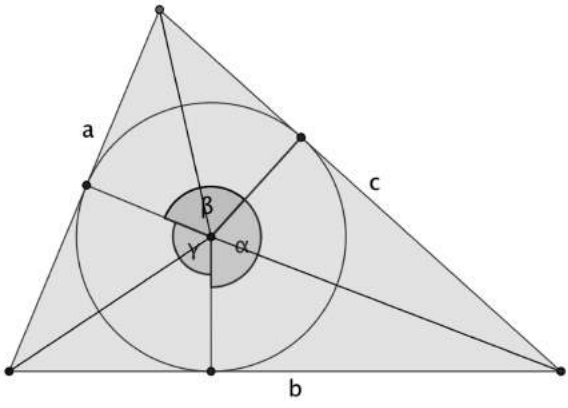


Figure 1: les trois angles α, β, γ

L'équation (1) nous apprend que si deux triangles ont la même aire et le même demi-périmètre, alors les rayons de leurs cercles inscrits sont aussi les mêmes. Ainsi, si nous cherchons deux tels triangles, nous les trouverons dans l'ensemble des triangles dont les côtés sont tangents à un cercle fixe. Au lieu d'utiliser les longueurs des côtés pour paramétrer cet ensemble, nous allons utiliser les angles α, β et γ formés par les trois rayons, de sommet le centre du cercle inscrit, comme indiqué sur la figure 1.

Une courbe des triangles d'aire et de périmètre constants

À l'intérieur de cet espace, nous pouvons trouver des courbes représentant les familles de tous les triangles d'aire A et de demi-périmètre p identiques.
Exprimons d'abord p en fonction des angles α, β et γ et du rayon r du cercle inscrit. Les rayons et les segments qui joignent les sommets du triangle au centre du cercle inscrit découpent le grand triangle en six triangles rectangles. Les droites joignant le centre du cercle inscrit à chacun des sommets sont les bissectrices du grand triangle, ces triangles rectangles se présentent donc par paires de triangles isométriques. En calculant un seul côté par paire et en ajoutant, nous obtenons :

$$p = r\left(\tan\frac{\alpha}{2} + \tan\frac{\beta}{2} + \tan\frac{\gamma}{2}\right) \qquad (2)$$

Les équations (1) et (2) nous apprennent que si l'aire A et le demi-périmètre p sont fixés, il en est de même de la somme des tangentes :

$$\tan\frac{\alpha}{2} + \tan\frac{\beta}{2} + \tan\frac{\gamma}{2} = \frac{p^2}{\mathrm{A}} \qquad (3)$$

Ensuite, nous traduisons cette condition en une équation définissant une courbe dans le plan.

Posons : $x = \tan\dfrac{\alpha}{2}$, $y = \tan\dfrac{\beta}{2}$, $z = \tan\dfrac{\gamma}{2}$.

Puisque $\alpha + \beta + \gamma = 2\pi$, nous avons : $\dfrac{\gamma}{2} = \pi - \dfrac{\alpha}{2} - \dfrac{\beta}{2}$.

Donc :

$$z = \tan\left(\frac{\gamma}{2}\right) = \tan\left(\pi - \frac{\alpha}{2} - \frac{\beta}{2}\right) = -\tan\left(\frac{\alpha}{2} + \frac{\beta}{2}\right) = \frac{x+y}{1-xy}.$$

Alors, si on appelle k la constante $\dfrac{p^2}{\mathrm{A}}$, l'équation (3) devient, pour k fixé :

$$x + y - \frac{x+y}{1-xy} = k,$$

que nous pouvons écrire sous la forme :

$$x^2y + xy^2 = kxy - k.$$

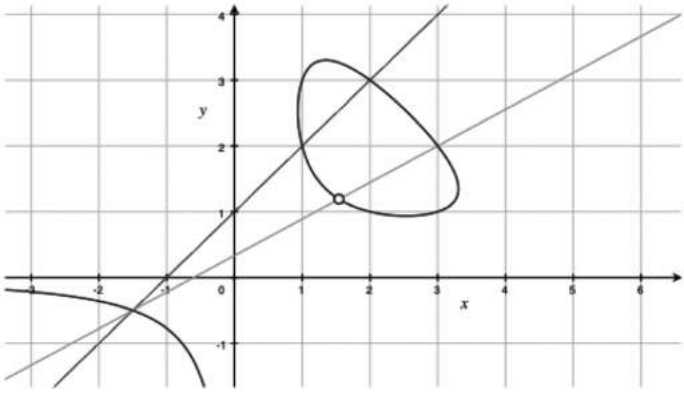


Figure 2 : la courbe des triangles

Tout triangle d'aire A et de demi-périmètre p définit un point de cette courbe, et tout point de la courbe, dans une certaine région du plan, correspond à un triangle. La région correspond aux angles en jeu dans la figure 1, c'est-à-dire les angles vérifiant : $\alpha + \beta + \gamma = 2\pi$, $0 < \alpha < \pi$, $0 < \beta < \pi$, $0 < \gamma < \pi$, ce qui correspond à la région : $x > 0$, $y > 0$ et $xy > 1$ (puisque $z > 0$).
La figure 2 montre cette courbe pour $k = 6$, valeur correspondant au triangle de côtés 3, 4 , 5. Tout point de la composante de cette courbe qui se trouve dans le premier quadrant ($x > 0$, $y > 0$) correspond à un triangle. Les longueurs des côtés de ce triangle sont : $a = x + y$, $b = y + z$, $c = z + x$ puisque $r = 1$[(2)]. En particulier, les points de coordonnées (1,2), (2,1), (2,3), (3,2), (1,3), (3,1) correspondent tous au triangle de côtés 3, 4 et 5, les côtés étant pris dans des ordres différents.

Trouver des points de la courbe

La courbe de la figure 2 étant définie par une équation de degré 3, on peut trouver des points de cette courbe en utilisant la méthode de la sécante. Deux points de la courbe définissent une sécante qui coupe la courbe en un troisième point. Trouver ce point revient à résoudre une équation du troisième degré en x dont on connaît déjà deux racines. Comme nous avons déjà six points sur cette courbe, nous avons de nombreuses possibilités de sécantes, et plus on construit de points, plus on crée de possibilités. En fait, la courbe a une infinité de points de coordonnées rationnelles.

(2) Plus généralement, si on se donne deux rationnels positifs p et A, la connaissance d'un point rationnel (x,y) sur la courbe d'équation $x^2y + xy^2 = kxy - k,$, où $k\dfrac{p^2}{\mathrm{A}}$, permet de trouver un triangle d'aire A et de demi-périmètre p dont les côtés aient des longueurs a, b, c rationnelles.

Il suffit d'utiliser les formules $x + y - \dfrac{x+y}{1-xy} = k$, $r = \dfrac{\mathrm{A}}{p}$, puis (se reporter à la figure 1) :

$c = r\left(\tan\dfrac{\alpha}{2} + \tan\dfrac{\beta}{2}\right) = r(x+y)$ et de même $b = r(z+x)$, $a = r(y+z)$ avec $z = \dfrac{x+y}{1-xy}$.

La procédure à deux sécantes illustrée sur la figure 2 conduit au point de coordonnées (54/35, 25/21) qui correspond au triangle de côtés 41/15,101/21 et 156/35.
La méthode de la sécante fonctionne pour toute cubique dans le plan.

Les courbes telles que celle-ci sont appelées courbes elliptiques non parce qu'elles sont des ellipses, mais parce qu'elles apparaissent dans l'étude d'une certaine classe de fonctions complexes appelées fonctions elliptiques. La procédure de la sécante permet de définir une structure de groupe sur l'ensemble des points rationnels d'une courbe elliptique (c'est-à-dire des points de coordonnées rationnelles).

La morale mathématique

L'étude des courbes elliptiques est un sujet central de la recherche en théorie des nombres, avec des applications aux systèmes de cryptographie qui sont utilisés pour sécuriser les transactions financières sur Internet ; les courbes elliptiques jouent un rôle central dans la démonstration du dernier théorème de Fermat.
L'histoire racontée dans cet article témoigne de la remarquable unité des mathématiques en commençant, comme il se doit, au lycée, et en finissant au niveau de la recherche. En chemin, nous avons rencontré une idée fondamentale dans les mathématiques d'aujourd'hui : l'idée de résoudre un problème sur un objet particulier (les triangles d'aire 6 et de périmètre 12, par exemple) en situant cet objet dans un espace plus général (l'espace des triangles) et en trouvant la bonne façon de paramétrer cet espace.

Pour prolonger cette lecture :

- On trouvera des compléments intéressants sur le problème des triangles d'aire et de périmètre donnés dans un article de Henry Bottomley :
  http://www.btinternet.com/~se16/hgb/trianglearea perimeter.htm
  Il y donne des exemples à côtés entiers et démontre plusieurs résultats .
- Le numéro de janvier 2012 de la « gazette des mathématiciens » publie un article de Antoine Chambert-Loir intitulé « De Galois aux corps finis » qui mentionne en particulier le rôle des courbes elliptiques en cryptographie et donne une définition claire de l'addition sur les courbes elliptiques. En voici l'adresse :
  http://smf4.emath.fr/Publications/Gazette/2012/131/smf_gazette_131_58-68.pdf
- Nous donnons en annexe sur le site de l'APMEP d'autres liens en rapport avec cet article.