Passerelle vers l'Agrégation Interne (Algèbre/Géométrie) – Feuille 5c

La paramétrisation rationnelle de l'ellipse

$$x^2 + y^2 - xy = 1$$

utilisée précédemment :

$$x = \frac{4 - 4t - 3t^2}{4 + 3t^2}, \qquad y = \frac{4 + 4t - 3t^2}{4 + 3t^2}$$
$$t = 2\frac{y - x}{x + y + 2},$$

a compliqué inutilement la discussion des solutions entières à l'équation $b^2 + c^2 - bc = d^2$. Il était dans la nature des choses que 3 vienne nous enquiquiner un peu, mais en ce qui concerne le nombre premier 2, il n'y avait aucune raison qu'il le fasse avec autant de détermination. On aurait réduit un peu les soucis en utilisant $u = \frac{1}{2}t$ plutôt que t mais ça ne règle pas tout.

Non, en fait, on a voulu trop bien faire en projetant du point $(-1, -1)$ vers la tangente au point $(1, 1)$: a posteriori (pour moi…) il est plus simple de prendre par exemple le point d'intersection entre la droite qui est définie par les deux points $(-1, -1)$ et (x, y), et l'axe des x ! Je vous laisse faire les calculs qui mènent (on note $(-t, 0)$ le point d'intersection) aux formules suivantes :

$$x = \frac{1 - 2t}{1 - t + t^2}, \qquad y = \frac{1 - t^2}{1 - t + t^2}$$
$$t = \frac{y - x}{1 + y}.$$

Le point $(-1, -1)$ correspond à $t = +2$, le point $(1, 1)$ à $t = 0$, et le point $(0, -1)$ à $t = \infty$. La partie de l'ellipse avec $0 < x < y$ correspond à $0 < t < \frac{1}{2}$. Lorsque l'on écrit $t = \frac{p}{q}$ sous forme irréductible ($q \geqslant 1$), cela nous donne les entiers :

$$B = q(q - 2p), \quad C = q^2 - p^2, \quad D = q^2 - qp + p^2,$$

Il est maintenant un peu plus facile de déterminer $\delta = \mathrm{pgcd}(B, C, D)$:

1. Trouver une identité de Bezout dans $\mathbb{Q}[X]$ entre les polynômes $X(X-2)$ et $X^2 - 1$,

2. en déduire l'identité magique $(2q+p)(q^2-2pq)-(2q-3p)(q^2-p^2) = -3p^3$,
3. et démontrer en conséquence que si un entier positif δ divise à la fois B et C il vaut 1 ou 3 (ici, p et q sont premiers entre eux).

Si $\delta = 3$, c'est donc que $q + p \equiv 0 \bmod 3$ (puisque $\delta \mid B$) et la réciproque vaut puisque $C = (q - p)(q + p)$. Ainsi, c'est particulièrement simple :

$$\delta\left(\frac{p}{q}\right) = \begin{cases} 1 & (3 \nmid p + q) \\ 3 & (3 \mid p + q) \end{cases}$$

On peut faire la remarque que si $3 \nmid p + q$ alors $3 \nmid D$: en effet $D \equiv (p + q)^2 \bmod 3$. Et on peut aussi ajouter que si $3 \mid p + q$ alors en fait 3 ne divise D qu'une seule fois. En effet avec $q = 3k - p$, $D = 9k^2 - 9kp + 3p^2$, puis $\frac{1}{3}D \equiv p^2 \bmod 3$ et 3 ne peut pas diviser p sinon il diviserait aussi q. Or p et q sont premiers entre eux. En résumé $\delta^{-1}(q^2 - qp + p^2)$ n'est jamais divisible par 3.

On déduit de toute cette discussion (et de ce qui avait déjà été établi dans la fiche 5) que les polynômes $P = X(X - b)(X - c)$ avec $0 < b < c$ entiers, tels que P' a des racines entières, sont paramétrés exactement par les formules :

$$b = 3k\frac{q(q - 2p)}{\delta}$$
$$c = 3k\frac{q^2 - p^2}{\delta},$$

avec $0 < 2p < q$, p et q premiers entre eux, $\delta = 1$ si 3 ne divise pas $p + q$ et $\delta = 3$ si 3 divise $p + q$. De plus k est un entier au moins 1.

La semi-distance entre les deux racines de P' est $\Delta = k\delta^{-1}(q^2 - qp + p^2)$, et il est maintenant extrêmement facile de montrer que sa valeur minimale est 7 et de déterminer quand elle est atteinte. On impose bien sûr pour cela $k = 1$. En général on a $q^2 - qp + p^2 = (q - \frac{p}{2})^2 + \frac{3}{4}p^2 > \frac{9}{4}p^2 + \frac{3}{4}p^2 = 3p^2$. Donc Δ ne peut être inférieur ou égal à 7 que si $\delta = 1$ et $p = 1$ ou $\delta = 3$ et $p = 1$ ou $p = 2$. Pour $p = 2$, la valeur minimale de $q > 2p = 4$ qui donnera $\delta = 3$ est $q = 7$, et on a alors $\Delta = \frac{1}{3}(49 - 14 + 4) = 13 > 7$. Ne subsiste comme possibilité que $p = 1$. On doit avoir $q > 2$. La première valeur autorisée est $q = 3$, elle donne $\delta = 1$ et $\Delta = 9 - 3 + 1 = 7$. La plus petite valeur de $q \equiv 2 \bmod 3$ qui donne $\delta = 3$ est $q = 5$ et alors $\Delta = \frac{1}{3}(25 - 5 + 1) = 7$.

Donc 7 est la valeur minimale, et elle n'est atteinte parmi les couples (p, q), $0 < 2p < q$, $(p, q) = 1$ que pour $(p = 1, q = 3)$ et $(p = 1, q = 5)$. Ce qui correspond à $(b, c) = (9, 24)$ et $(b, c) = (15, 24)$.