SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

TENA AYUSO

Sur l'existence d'un point rationnel d'ordre n sur une courbe elliptique

Séminaire de théorie des nombres de Grenoble, tome 1 (1971-1972), p. 20-27

<http://www.numdam.org/item?id=STNG_1971-1972__1__20_0>

SUR L'EXISTENCE D'UN POINT RATIONNEL D'ORDRE n SUR UNE COURBE ELLIPTIQUE

par TENA AYUSO les 15.12.71 et 5.1.72

A - INTRODUCTION.

Soit $\mathcal{C}$ une cubique plane $F(x,y) = 0$ à coefficients rationnels et ayant un point rationnel. On sait que, quitte à faire une transformation birationnelle, on peut mettre $\mathcal{C}$ sous la forme canonique :

$$y^2 = x^3 - Ax - B \qquad (1)$$

laquelle admet la paramétrisation

$$x = p(u) \qquad y = 1/2\ p'(u) \qquad (2)$$

où $p(u)$ est la fonction de Weierstrass correspondant au réseau Γ de $\mathbb{C}$ déterminé par les invariants :

$$g_2 = 4A \qquad g_3 = 4B \quad . \qquad (3)$$

Définition 1.

Un point $P(u) \in \mathcal{C}$ est d'ordre n si et seulement si :

$$nu \equiv 0 \pmod{\Gamma} \quad \text{et} \quad n'u \not\equiv 0 \pmod{\Gamma} \quad \text{pour} \quad 0 < n' < n \ .$$

Problème : Pour quelles valeurs de n existe-t-il une courbe elliptique ayant un point rationnel P d'ordre n ?

Dem'janenko [4] a montré que n est borné. En fait les valeurs $n = 1$ 10 et 12 sont réalisées, et on peut conjecturer l'impossibilité de valeurs autres que celles-ci.

B - CONSTRUCTION.

Soient donnés dans le plan projectif les points P_o, P_1, P_2, P_3 non alignés (et à coordonnées rationnelles).

Question : Quelles conditions doivent satisfaire les coordonnées d'un autre point P_4 différent de ceux-ci pour qu'ils fassent partie d'un groupe exceptionnel cyclique à n éléments ? (Plus précisément pour qu'ils correspondent aux arguments elliptiques 0 , u , $2u$, $3u$, $4u$).

Note 1 : Les conditions imposées impliquent $n \geq 5$. Si on désire en outre (ce qui sera le cas en général) que jamais trois des cinq points $P_o, \ldots, P_4$ ne soient alignés, alors on aura $n > 9$.

On peut alors construire d'autres points, $P_{-1}, P_{-2}, \ldots, P_5, P_{-5}, \ldots, P_n, P_{-n} \ldots$ $n \in \mathbb{N}$, sur le plan vérifiant la condition suivante :

Condition 1. Trois points $P_{n_1}, P_{n_2}, P_{n_3}$ sont alignés, si et seulement si, ses indices n_1 , n_2 , n_3 vérifient (en tant que nombres entiers) la relation :

$$n_1 + n_2 + n_3 = 0 \quad . \qquad (4)$$

Ainsi, par exemple, le point P_{-4} doit être aligné avec P_o et P_4 et avec P_1 et P_3 , et donc il est déterminé comme le point d'intersection des droites passant par P_o et P_4 ; P_1 et P_3 (que nous noterons (P_o, P_4) et (P_1, P_3) respectivement) .

Note 2 : Pour que cette construction ait un sens, il faut en outre que pour chaque n , toutes les droites qui, en vertu de la condition 1, contiennent le point P_n se rencontrent en un point. La proposition ci-dessous nous dit que cette condition se trouve heureusement vérifiée dans le cas $n > 9$ (et pour le cas $n \leq 9$ on le vérifie également sans peine).

Commençons par construire de façon rigoureuse, pour $n > 9$:

Construction - définition 2.

Le point P_m $(m \geq 5)$ est déterminé comme le point d'intersection des droites

$$(P_{m_1-m}, P_{m_1}) \qquad (0 \leq m_1 < 1/2\ m) \qquad (5)$$

Le point P_{-m} $(m \geq 6)$ comme le point d'intersection des droites

$$(P_{m_1}, P_{m-m_1}) \qquad (1 \leq m_1 < 1/2\ m) \quad . \qquad (6)$$

Proposition 1.

Pour $n > 9$ les 9 points P_o , $P_{\pm 1}$, P_2 , $P_{\pm 3}$, $P_{\pm 4}$, P_{-5} sont différents et il existe une seule cubique qui passe par eux. Les points P_m , P_{-m} , pour toute valeur de m (entier naturel) sont bien déterminés (unicité), ils sont sur la cubique ci-dessus, et la tangente à la cubique en P_m passe par le point P_{-2m} .

Le cas $n = 5,6$ étant sans intérêt on suppose donc $n \geq 7$. Dans ce cas on sait qu'il est impossible que trois des points P_o, P_1, P_2, P_3 soient alignés. On peut donc les prendre comme sommets d'un système de coordonnées projectives dans le plan. Soient donc

$$P_o = (1,1,1) \ , \ P_1 = (1,0,0) \ , P_2 = (0,1,0) \ , \ P_3 = (0,0,1) \quad .$$

Si dans cette base P_4 a les coordonnées $P_4 = (x_1, x_2, x_3)$ on peut obtenir les coordonnées des autres points comme des expressions rationnelles en x_1 , x_2 , x_3 .

Ainsi :

$$\begin{aligned}
P_{-1} &= (x_1 - x_2 + x_3, x_3, x_3) \\
P_{-2} &= (x_1 - x_2 + x_3, x_3, x_1 - x_2 + x_3) \\
P_{-3} &= (1,1,0) \qquad (7) \\
P_{-4} &= (x_1 - x_2, 0, x_3 - x_2) \\
P_{-5} &= (0, x_2, x_3) \\
P_5 &= (x_1x_2 + x_1x_3 - x_2^2, x_1x_3, x_2(x_1 - x_2 + x_3))
\end{aligned}$$

etc...

Alors pour n fixé on aura : P_{n_1} , P_{n_2} , P_{n_3} sont alignés, si et seulement si,

a) $n_1 + n_2 + n_3 \equiv 0 \pmod{n}$

b) il n'existe pas trois points $P_{n'_1}$, $P_{n'_2}$, $P_{n'_3}$ alignés avec

$$|n'_1 + n'_2 + n'_3| < n \quad . \tag{8}$$

Ce qui donne des conditions à satisfaire par x_1 , x_2 , x_3 .

C - CAS D'EXISTENCE - EXEMPLES.

Pour $n = 7,8,9$ on sait que le point P_4 est aligné avec deux des points P_o , P_1 , P_2 , P_3 . En effet on obtient

$$n = 7 : \quad x_1 - x_2 = 0 \quad \text{et} \quad x_3 = 0 \tag{9}$$

$$n = 8 : \quad x_2 = 0 \tag{10}$$

$$n = 9 : \quad x_1 = 0 \tag{11}$$

Exemples de cubiques ayant un sous-groupe cyclique rationnel d'ordre $n = 7,8,9$:

$n = 7 : 16y^2 = 2x^3 + 15x^2 + 16x + 19 \qquad P_1 = (-1,1)$

$n = 8 : 16y^2 = 27x^3 + 414x^2 + 243x \qquad P_1 = (-1,3)$

$n = 9 : \quad y^2 = 8x^3 + 33x^2 + 18x + 9 \qquad P_1 = (-3,6)$

Pour $n = 10,12$ on obtient respectivement

$$n = 10 : x_1x_2 + x_1x_3 - x_2^2 = 0 \tag{12}$$

$$n = 12 : x_2^2 - x_1x_3 = 0 \tag{13}$$

Ces cubiques ont chacune une infinité de points rationnels. Il suffit de prendre comme P_4 un d'eux, non aligné avec deux des points de base. Exemples :

$n = 10 : \quad 9y^2 = 8x^3 + 25x^2 - 64x \qquad P_1 = (-1,3)$

$n = 12 : \quad y^2 = x^3 - 122x^2 + 9^3.7^2x \qquad P_1 = (21,840)$

D - CAS D'IMPOSSIBILITE.

On obtient :

$n = 11$: $x_1^2x_2 - x_1x_2^2 - x_1x_3^2 + x_2^3x_3 = 0$

$n = 13$: $x_1^2x_2^2 - x_1x_2^3 - x_1x_2x_3^2 + x_1x_3^3 + x_2^3x_3 - x_2^2x_3^2 = 0$

$n = 14$: $x_1^3x_2 - x_1^2x_2^2 - x_1^2x_2x_0 - x_1^2x_3^2 - x_1x_2^3 + x_1x_2x_3^2 + x_2^4 - x_2^3x_3 = 0$

$n = 15$: $x_1^2x_2^2 + x_1^2x_2x_3 + x_1^2x_3^2 - x_1x_2^3 - x_1x_2^2x_3 - x_1x_2x_3^2 + x_2^3x_3 = 0$

$n = 17$: $x_2x_3^2(x_3-x_1)^2 - (x_1x_3-x_1x_2+x_2x_3)(x_3-x_1+x_2)(x_3(x_3-x_1)^2 + x_1x_2(x_2-x_1)) = 0$.

Le cas $n = 13$ n'est pas encore résolu. Le cas $n = 11$ a été étudié par Billing et Mahler [2] . Les cas $n = 14, 15$ sont analogues au cas $n = 11$ (courbes de genre 1) : le procédé de Billing et Mahler est donc en principe applicable. Nous étudions par la suite le cas $n = 17$ selon Ogg [3] .

$n = 17$: Faisant $x_3 = 1$ et le changement de variables,

$$x_1 = x \qquad y = \frac{x_2+(x_1-1)}{x_2} \tag{14}$$

l'équation correspondante devient :

$$x(1-x)y^2 = x[x^2+(1-x)^2]y + (1-x-x^2+x^3-x^4) = 0 \quad . \tag{15}$$

Comme x et y doivent être rationnels le discriminant de cette équation en y doit être un carré. Et donc

$$z^2 = x^2[x^2+(1-x)^2]^2 - 4x(1-x)(1-x-x^2+x^3-x^4) = -4x^3 + 9x^2 - 4x \tag{16}$$

Points exceptionnels.

La courbe possède les points exceptionnels $(0,0)$ $(1,\pm1)$ (∞) . Elle n'en possède pas d'autres (car il n'existe pas de point d'inflexion rationnel, et on peut appliquer le théorème de l'Appendice). Mais ces quatres points sont alignés avec deux des points P_0 , P_1 , P_2 , P_3 .

Points ordinaires.

Mettons l'équation sous la forme $y^2 = x^3 + 9x + 16x$. En faisant la division par 2 (voir Appendice) on trouve la courbe : $y^2 = x(x-1)(x-17)$.

Soit $P = (x,y)$ point ordinaire générateur. Sans perte de généralité on peut supposer (voir [3]) :

$$x > 17 \quad \text{et} \quad 17 \nmid \text{Numérateur de } x .$$

Soit alors $x = A/B^2$, $y = C/B^3$ (17)

$$(A,B) = (A,C) = (B,C) = 1 \quad , \quad 17 \nmid A .$$

et $$C^2 = A(A-B^2)(A-17B^2) \quad . \tag{18}$$

Et on a la factorisation

$$\left.\begin{array}{l} A = d_1 C_1^2 \\ A-B^2 = d_2 C_2^2 \\ A-17B^2 = d_3 C_3^2 \end{array}\right| \quad \left.\begin{array}{l} d_1 = 1,17 \Rightarrow d_1 = 1 \\ d_2 = 1,2 \\ d_3 = 1,2,17 \Rightarrow d_3 = 1,2 \end{array}\right\} \; d_1 d_2 d_3 = C^2 \tag{19}$$

Le cas $d_2 = d_3 = 2$ conduit à une contradiction.

Alors $d_2 = d_3 = 1$. Mais dans ce cas $P = 2P'$, contradiction avec le caractère générateur de P . Le rang de la cubique est donc 0 .

NOTE.

L'équation reliant les coordonnées x_1 , x_2 , x_3 du point P_4 peut être interprétée en termes du groupe modulaire comme équation de la surface de Riemann $X_1(n)$ obtenue par compactification de $H/\Gamma_1(n)$, avec :

H demi-plan de Poincaré

$$\Gamma_1(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \begin{array}{l} a,b,c,d \in Z \\ a \equiv d \equiv 1 \pmod n \end{array} \quad ab - cd = \pm 1 \right\}$$

$X_1(n)$ est une paramétrisation de l'espace de courbes elliptiques ayant un point rationnel fixé d'ordre n .

En effet, à tout point de $X_1(n)$ rationnel non "parabolique" (c'est-à-dire à tout point P_4 non aligné avec deux des points P_o, P_1, P_2, P_3) correspond une courbe elliptique ayant un point rationnel d'ordre n .

APPENDICE.

Division par un sous-groupe d'ordre 2 d'une courbe elliptique.

Soit $\mathcal{C}$ une courbe ayant un point rationnel d'ordre 2 , laquelle peut donc être mise sous la forme

$$\mathcal{C} : y^2 = x^3 + Mx^2 + Nx \quad .$$

Soit $\Gamma = Z\omega_1 \oplus Z\omega_2$ le réseau correspondant à $\mathcal{C}$ et $\Gamma' = Z(\omega_1/2) \oplus Z\omega_2$, ω_1 réel.

Considérons les 2 variétés abéliennes

$$\mathcal{C} = \mathbb{C}/\Gamma \qquad \mathcal{C}' = \mathbb{C}/\Gamma' \quad .$$

L'application $\mathbb{C} \xrightarrow{id} \mathbb{C}$ induit l'application

$$\varphi : \mathcal{C} \to \mathcal{C}' \quad , \quad \varphi : \underset{\text{mod } \Gamma}{Z} \to \underset{\text{mod } \Gamma'}{Z} \quad .$$

On peut montrer que la cubique $\mathcal{C}'$ peut s'écrire

$$y'^2 = x'^3 - 2Mx'^2 + (M^2-4N)x'$$

(Il suffit de calculer les valeurs g'_2 et g'_3 correspondent au réseau Γ') et que les coordonnées

$$(x',y') = \varphi(x,y)$$

sont exprimées comme fonctions de x,y par

$$x' = \frac{x^2+Mx+N}{x} \qquad y' = \frac{y(x^2-N)}{x^2} \quad .$$

L'application φ est une isogénie de $\mathcal{C}$ sur $\mathcal{C}'$ de degré 2 qui peut être interprétée comme le passage au quotient de $\mathbb{C}/\Gamma$ par $(0,\omega_1/2)$

ou encore comme le passage au quotient de $\mathcal{C}$ par le sous-groupe d'ordre 2 $\{(0,0),\infty\}$.

En réalisant 2 fois successivement cette division par 2 on peut démontrer (voir [1]) le

Théorème.

Soit $\mathcal{C} : y^2 = x^3 + Mx^2 + Nx$. Si $P(x,y) \in \mathcal{C}$ est un point rationnel, il est divisible par 2 , si et seulement si un des nombres

$$M + 2x \pm 2\sqrt{x^2+Mx+N}$$

est un carré rationnel.

BIBLIOGRAPHIE

[1] - C.E. LIND - "Untersuchungen über die Rationalen Punkte der ebenen..." (Uppsala 1940).

[2] - BILLING et MAHLER - "On exceptional points on cubic curves". (J. London Math. Soc. 1940).

[3] - OGG - "Rational points of finite order on elliptic curves" (Inventiones math. 1971).

[4] - DEM'JANENKO - "Sur la torsion des courbes elliptiques". (en russe), Izvestiia Akademii Nauk SSSR (1971).