Astérisque

ROGER APERY

Points rationnels sur certaines courbes algébriques

Astérisque, tome 24-25 (1975), p. 229-236

<http://www.numdam.org/item?id=AST_1975__24-25__229_0>

Société Mathématique de France
Astérisque 24-25 (1975)

POINTS RATIONNELS SUR CERTAINES COURBES ALGÉBRIQUES

par

Roger APÉRY

-:-:-:-

PRÉLIMINAIRES. - Le problème général est l'étude des points d'une courbe C à coordonnées dans une extension finie K de $\mathbb{Q}$.

Les problèmes sont les suivants :

(A) Existe-t-il un point (ou une place si la courbe admet des singularités) sur la courbe ?

(B) En supposant qu'il existe une place, étudier la structure de l'ensemble des places de C.

Les courbes sont classées par le genre.

PREMIER CAS : GENRE 0. - On sait répondre complètement.

(A) Pour presque toutes les localisations du corps K, il y a une place ; selon le principe de Hasse, pour qu'il y ait une place sur le corps K, il suffit

qu'il y en ait une sur chaque localisé. On ne doit examiner qu'un nombre fini de corps localisés et pour chacun d'eux on a des algorithmes.

(B) Si la courbe admet une place, elle est birationnellement équivalente à une droite projective.

DEUXIÈME CAS : GENRE ≥ 2 . - Une conjecture de Mordell encore en suspens dit que l'ensemble des points est fini.

TROISIÈME CAS : GENRE 1

(A) Le principe de Hasse n'est pas valable et on ne connait pas de critère général d'existence d'un point.

(B) Si l'ensemble des points n'est pas vide, en en fixant un comme origine les points acquièrent une structure de groupe abélien A (Poincaré).

Ce groupe A est de type fini (Mordell-Weil), c'est-à-dire qu'il contient un groupe fini A_o et le groupe quotient A/A_o est un groupe libre de dimension finie r , appelé rang de la courbe.

Des méthodes régulières permettent de déterminer le groupe fini.

La méthode de descente de Fermat permet de majorer r ; par contre une minoration de r ne peut être obtenue qu'à partir des points effectivement nommés.

Nous voulons examiner la conjecture émise par Mordell au congrès de Debrecen (1968) selon laquelle la courbe

$$y^2 = px^4 + 1 \qquad (1)$$

admet pour p premier $\equiv 5 \bmod 8$ des solutions rationnelles non triviales.

Sous forme homogène, avec un léger changement de notation, l'équation s'écrit

$$y^2 = px^4 + z^4 \qquad (2)$$

La réduction mod 8 donne : y impair, x pair, z impair.

Une décomposition facile donne l'un des deux cas suivants :

Premier cas :

$$\left(\frac{y + \varepsilon z^2}{2} , \frac{y - \varepsilon z^2}{2}\right) = (Y^4 , 4pX^4) \quad \text{et} \quad x = 2XY$$

d'où $Y^4 - 4pX^4 = \varepsilon z^2$. La réduction mod (4) donne $\varepsilon = \pm 1$

$$\left(\frac{Y^2 + z}{2} , \frac{Y^2 - z}{2}\right) = (z'^4 , px'^4)$$

$$Y^2 = px'^4 + z'^4 .$$

Deuxième cas :

$$\left(\frac{y + \varepsilon z^2}{2} , \frac{y - \varepsilon z^2}{2}\right) = (pX^4 , 4Y^4) .$$

La réduction mod (4) donne $\varepsilon = \pm 1$

$$pX^4 - 4Y^4 = Z^2 \qquad (3)$$

X , Y , Z impair.

Un argument classique de descente montre que : ou bien l'équation (3) est possible avec $X , Y , Z \neq 0$ et la courbe (1) est de rang 1 ; ou bien l'équation (3) est impossible et la courbe (1) est de rang 0 .

p est de la forme $\alpha^2 + \beta^2 = \alpha^2 + 4\beta'^2$. Les entiers α , β sont déterminés au signe près qui est fixé dans la suite.

Par décomposition dans l'anneau $\mathbb{Z}[i]$, l'équation (3) devient

$$Z^2 + 2iY^2 = (\alpha + i\beta)\ (\xi + i\eta)^4$$

à condition que $\beta' \equiv 1 \mod 4$, ce qui fixe le signe de β.

On fixe le signe de α en imposant $\alpha \equiv 1 \mod 4$. On obtient le système :

$$X^2 = \xi^2 + \eta^2 \qquad (4)$$

$$Y^2 = \beta'(\xi^4 - 6\xi^2\eta^2 + \eta^4) + 2\alpha\eta(\xi^2 - \eta^2)\ . \qquad (5)$$

Pour continuer la descente, on utilise les propriétés du corps $K = \mathbb{Q}(\sqrt{p}, i)$ qui est galoisien sur $\mathbb{Q}$, admet comme groupe de Galois le groupe de Klein et pour anneau des entiers l'anneau A dont le $\mathbb{Z}$ module sous-jacent a pour base

$$\left(1\ ,\ \frac{1+\sqrt{p}}{2}\ ,\ i\ ,\ \frac{i+\sqrt{p}}{2}\right)\ .$$

LEMME. - L'entier p est la norme d'un élément de A.

De façon précise, en appelant ε l'unité fondamentale (de norme -1) de l'anneau $B = \mathbb{Z}\left(\frac{1+\sqrt{p}}{2}\right)$, il y a exactement un couple $\{\theta, \theta'\}$ d'éléments de B tels que

$$\varepsilon\sqrt{p} = \theta^2 + \theta'^2 \qquad (6)$$

où ce qui est équivalent

$$\sqrt{p} = \varepsilon\varphi^2 - \bar{\varepsilon}\bar{\varphi}^2$$

où le surlignage désigne la conjugaison

$$\theta' = \pm\varepsilon\overline{\theta}$$

La norme relative de $\theta + i\theta'$ par rapport à $\mathbb{Z}[i]$ est le produit de $(\alpha \pm i\beta)$ par une unité de $\mathbb{Z}[i]$.

On en déduit :

$$\beta'(x^2 - y^2) + \alpha x y = \left(\frac{\lambda x + \mu y}{2}\right)^2 - p\left(\frac{\lambda' x + \mu' y}{2}\right)^2$$

où

$$\left(\frac{\lambda + \lambda'\sqrt{p}}{2}, \frac{\mu + \mu'\sqrt{p}}{2}\right) = (\theta, \theta')$$

$$\lambda\mu' - \mu\lambda' = -2 \quad .$$

En posant, après changement de notation

$$x = \xi^2 - \eta^2$$

$$y = 2\xi\eta$$

on obtient le système

$$X^2 = x^2 + y^2$$

$$Y^2 = \left(\frac{\lambda x + \mu y}{2}\right)^2 - p\left(\frac{\lambda' x + \mu' y}{2}\right)^2 \qquad (7)$$

Comme le nombre de classes d'idéaux de $\mathbb{Q}(\sqrt{p})$ est impair, l'équation (7) donne

$$\frac{\lambda x + \mu y}{2} + \sqrt{p}\,\frac{\lambda' x + \mu' y}{2} = \left(\frac{u + v\sqrt{p}}{2}\right)^2$$

$$X = x^2 + y^2$$

$$Y^2 = \left(\frac{\lambda x + \mu y}{2}\right)^2 - p\left(\frac{\lambda' x + \mu' y}{2}\right)^2 \qquad (8)$$

où

$$\left(\frac{\lambda + \lambda'\sqrt{p}}{2}, \frac{\mu + \mu'\sqrt{p}}{2}\right) = (\theta, \theta')$$

$$\lambda\mu' - \mu\lambda' = -2 \quad .$$

Comme le nombre de classes d'idéaux de $\mathbb{Q}(\sqrt{p})$ est impair, l'équation (8) donne

$$\frac{\lambda x + \mu y}{2} + \sqrt{p}\,\frac{\lambda' x + \mu' y}{2} = \left(\frac{u + v\sqrt{p}}{2}\right)^2$$

$$\lambda x + \mu y = \frac{u^2 + pv^2}{2}$$

$$\lambda' x + \mu' y = uv$$

d'où la combinaison $(-\mu' + \lambda i\ ,\ \mu - \lambda i)$ l'équation

$$F(u,v) = 4(\xi + i\eta)^2 \qquad (9)$$

où $$F(u,v) = (\lambda' i - \mu')(u^2 + pv^2) - 2(\lambda i - \mu)uv \qquad (10)$$

Le discriminant de la forme quadratique $F(u,v)$ est

$$\Delta = (\lambda i - \mu)^2 - p(\lambda' i - \mu')^2 = -4(\beta + \alpha i)$$

LEMME 2. - La forme $F(u,v)$ peut s'écrire

$$(\gamma_1 u + \delta_1 v)^2 - (\beta + \alpha i)(\gamma_2 u + \delta_2 v)^2 \quad .$$

Remarquons d'abord que

$$(\lambda + \mu i) = (\beta + \alpha i)(\mu' + \lambda' i) \quad .$$

Appelons γ_1, γ_2 des éléments de $Z(i)$ tels que

$$\gamma_1^2 - (\beta + \alpha i)\gamma_2^2 = \lambda' i - \mu' \quad .$$

Comme les coefficients de uv et v^2 dans F sont divisibles par $\beta + \alpha i$, on peut poser

$$\delta_1 = (\beta + \alpha i)\delta_o \quad .$$

On trouve

$$(\beta + \alpha i)\gamma_2 \delta_o - \gamma_1 \delta_2 = \pm 2$$

ce qui permet de déterminer δ_o, δ_2 .

On sait pour toute extension quadratique $L \to K$, où L est un corps de nombres algébriques dont le nombre de classes d'idéaux est impair, que le nombre de classes d'idéaux de K est impair dès que $\rho = 1 + \rho'$, où ρ désigne le nombre de places qui se ramifient dans l'extension et $2\rho'$ est l'indice dans le groupe des unités normes d'éléments de K .

Dans le cas de l'extension définie par $L = Q(i)$ et $K = L(\sqrt{\beta} + \alpha i)$, $2i$ est un carré, 2 n'est pas une norme, i n'est pas une norme, donc $\rho' = 1$; il y a exactement deux places qui se ramifient : les places définies par $(1+i)$ et $(\beta+\alpha i)$, donc $\rho = 2$; le nombre de classes de K est impair.

Comme $\beta - \alpha i$ est une norme relative d'un entier de L, on en déduit la même propriété pour $(\lambda' i - \mu')$.

On détermine ainsi δ_o, δ_2 d'où l'équation

$$(\gamma_1 u + \delta_1 v)^2 - (\beta + \alpha i)(\gamma_2 u + \delta_2 v)^2 = 4(\xi + i\eta)^2$$

ce qui permet de continuer la descente.

L'utilisation de calculateurs de bureau permet de calculer effectivement les solutions de l'équation (3).

-:-:-:-

Roger APÉRY
Université de Caen
Département de Mathématiques
U. E. R. de Sciences
Esplanade de la Paix
14000 CAEN

$$pX^4 - 4Y^4 = Z^2$$

p	α	β'	ξ	η	X	Y	Z
5	1	1			1	1	1
13	3	1			1	1	3
29	5	1			1	1	5
37	1	-3			5	3	151
53	7	1			1	1	7
61	5	-3			5	9	109
101	1	5			29	25	8359
109	3	5			5	1	261
149	7	5			5	7	289
157	11	-3	6	7	85	93	88861
173	13	1			1	1	13
181	9	5	19	10	461	715	2670111
197	1	-7	37	56	4505	9541	219078991
229	15	1			1	1	15
269	13	5	2	1	5	11	331
277	9	-7	43	16	2105	3901	67173561
293	17	1			1	1	17
317	11	-7	263	64	73265	48869	95450823979
349	5	9			1	3	5
373	7	9			1	3	7
389	17	5	2	1	5	13	359
397	19	-3	181	38	34205	76227	20208571931
421	15	-7	11	8	185	587	135009
461	19	5	79	10	6341	18985	475038539
509	5	-11	5	6	61	187	46435
541	21	5	5	2	29	95	7539
557	19	-7	8	11	185	59	807709
613	17	9			1	3	17
653	13	-11	2	3	13	23	4187
661	25	-3	7	6	85	219	159071
677	1	13	9	2	85	251	139511
701	5	13	53	174	33085	53407	28415544861
709	15	-11	3	2	13	47	855
733	27	1			1	1	27
757	9	13	87	34	8725	20521	1917696399
773	17	-11	2	3	13	17	4663
797	11	13	1462	771	2731885	1773371	210600981540301
821	25	-7	8	-11	185	667	412279
829	27	5	2	1	5	17	429
853	23	9			1	3	23