Séminaire Delange-Pisot-Poitou.
Théorie des nombres

William G. Ellison

Variations sur un thème de Carl Runge

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 13, n° 1 (1971-1972), exp. n° 9, p. 1-4

<http://www.numdam.org/item?id=SDPP_1971-1972__13_1_A8_0>

© Séminaire Delange-Pisot-Poitou. Théorie des nombres
(Secrétariat mathématique, Paris), 1971-1972, tous droits réservés.

L'accès aux archives de la collection « Séminaire Delange-Pisot-Poitou. Théorie des nombres » implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

Numdam
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
13e année, 1971/72, n° 9, 4 p.

10 janvier 1972

VARIATIONS SUR UN THÈME DE CARL RUNGE

par William G. ELLISON

Soit $f(x , y) \in \underset{\sim}{Z}[x , y]$. Je voudrais considérer l'équation $f(x , y) = 0$ avec $x , y \in \underset{\sim}{Z}$. La théorie qualitative de l'équation est connue. Nous avons en effet le théorème suivant de SIEGEL :

THÉORÈME. - Soit $f(x , y) \in \underset{\sim}{Z}[x , y]$ un polynôme irréductible. L'équation $f(x , y) = 0$ a, au plus, un nombre fini de solutions avec $x , y \in \underset{\sim}{Z}$, à moins qu'il y ait une solution paramétrique de la forme

$$x = \frac{A(t)}{L^n(t)} , \quad y = \frac{B(t)}{L^n(t)} \tag{1}$$

où

$$x = \frac{C(t)}{Q^n(t)} , \quad y = \frac{D(t)}{Q^n(t)} , \tag{2}$$

où $A(t) , \dots , D(t) , L(t) , Q(t) \in \underset{\sim}{Z}[t]$, et $L(t)$ est un polynôme linéaire, $Q(t)$ est un polynôme quadratique avec discriminant positif. Dans ce cas, il peut y avoir une infinité de solutions entières.

Il est possible, dans un cas numérique, de décider si l'équation a une solution paramétrique de la forme (1) ou (2) .

COROLLAIRE. - Si le genre, g , de la courbe $f(x , y) = 0$ est plus grand que zéro, l'équation $f(x , y) = 0$ a seulement un nombre fini de solutions avec $x , y \in \underset{\sim}{Z}$.

Quand l'équation $f(x , y) = 0$ a un nombre fini de solutions entières, la théorie de SIEGEL ne permet pas de trouver les solutions, ni même une borne pour la plus grande solution.

C'est un problème difficile de majorer les solutions entières de l'équation $f(x , y) = 0$. Avec le travail de BAKER, on peut donner une borne quand le genre de la courbe est 1 ou 0 (dans le cas où il y a un nombre fini des solutions).

Dans le livre "Diophantine equations" de MORDELL, le théorème suivant est démontré :

THÉORÈME (RUNGE). - Soit $f(x , y) \in \underset{\sim}{Z}[x , y]$ irréductible sur $\underset{\sim}{Q}$. Si

$$f(x , y) = \Sigma_i f_i(x , y) , \quad 1 \leqslant i \leqslant r ,$$

où $f_i(x , y)$ est une forme homogène de degré i , et $f_n(x , y)$ est réductible sur $\underset{\sim}{Q}$, différent de la forme $a_0\{q(x , y)\}^t$, où $a_0 \in \underset{\sim}{Z}$, $q(x , y) \in \underset{\sim}{Z}[x , y]$ irréductible sur $\underset{\sim}{Q}$, alors l'équation $f(x , y) = 0$ a, au plus, un nombre fini de

solutions entières, et on peut les trouver dans chaque cas numérique.

Aujourd'hui, je voudrais donner une variation de ce théorème. Il y a quelques autres variations dans mon cours à Bordeaux (il paraîtra ultérieurement une édition polycopiée de ce cours).

THÉORÈME. - Soit $f(x , y) = A_0(x)y^n + \dots + A_n(x)$, où $A_i(x) \in \mathbb{Z}[x]$, le degré de $A_0(x) = \mu > 0$, et $f(x , y)$ est irréductible sur $\mathbb{Q}$.

Pour chaque $\delta > 0$, il y a au plus un nombre fini de rationels y' et d'entiers x' avec les propriétés suivantes :

(a) $f(x' , y') = 0$,

(b) si $y' = u/v$, où $u , v \in \mathbb{Z}$, $|v| \leq |x'|^{(\mu-\delta)/n}$.

Dans un cas numérique, on peut effectivement trouver les nombres (x' , y') .

COROLLAIRE. - Si les hypothèses du théorème sont vraies pour $f(x , y)$, l'équation $f(x , y) = 0$ a, au plus, un nombre fini de solutions en entiers x' , y' , et on peut les trouver.

Le théorème est faux quand $\delta = 0$.

Exemple. - Considérons l'équation $xy^2 - 2x - 1 = 0$. Si $y = u/v$ avec $(u , v) = 1$, nous avons $xu^2 - 2v^2 x - v^2 = 0$. Par suite, x/v^2 et v^2/x , donc $x = v^2$ et $u^2 - 2v^2 = 1$.

Donc il existe une infinité de solutions $(x' , y') = (v^2 , u/v)$ avec $|v| = |x'|^{\frac{1}{2}}$.

Pour démontrer le théorème, nous avons besoin d'un lemme facile.

LEMME. - Nous supposons que x , y vérifient l'équation

$$f(x , y) = A_0(x)y^n + \dots + A_n(x) = 0 , \tag{1}$$

où $A_i(X) \in \mathbb{Z}[X]$, $\partial A_0(X) = \mu > 0$, et les $A_j(X)$ n'ont pas de facteurs commun dans $\mathbb{Q}[X]$. Supposons le polynôme $f(X , Y)$ irréductible sur $\mathbb{Q}$.

(a) On peut écrire chaque élément de l'anneau $\mathbb{Q}[x , y]$ sous la forme

$$\varphi_0(x) + \varphi_1(x)y + \dots + \varphi_{n-1}(x)y^{n-1} + \Psi_0(x)y^n + \dots + \Psi_m(x)y^{n+m} , \tag{2}$$

où $\varphi_i(x)$, $\Psi_j(x) \in \mathbb{Q}[x]$ et $\delta\Psi_j(x) < \mu$ pour $0 \leq j \leq m$.

La représentation dans cette forme est unique.

(b) Pour chaque entier $\nu \geq 0$, nous avons

$$y^{n+\nu} = \frac{B_1^{(\nu)}(x)}{A_0^{\nu+1}(x)}y^{n-1} + \dots + \frac{B_n^{(\nu)}(x)}{A_0^{\nu+1}(x)} , \tag{3}$$

où $B_i^{(\nu)}(x) \in \mathbb{Z}[x]$ pour $1 \leq i \leq n$, $\nu = 0 , 1 \dots$

(c) Si $|x| \geqslant C_0$, on peut écrire les coefficients de y^{n-r} dans $(3)_\nu$ sous la forme

$$B_r^{(\nu)}(x)/A_0^{\nu+1}(x) = P_r^{(\nu)}(x) + a_{r1}^{(\nu)}/x + a_{r2}^{(\nu)}/x^2 + \dots ,$$

où $P_r^{(\nu)}(x) \in \underset{\sim}{Q}[x]$ et les $\{a_{rs}\} \in \underset{\sim}{Q}$.

Démonstration du théorème. - On peut écrire chaque développement en série de Puiseux à l'infini, de la courbe $f(x , y) = 0$, sous la forme

$$y = a(x) = \alpha_0 x^{p/q} + \alpha_1 x^{(p-1)/q} + \dots ,$$

où $|x| \geqslant C_1$ et $\{\alpha_i\} \in K$ avec $[K : \underset{\sim}{Q}] < \infty$.

Nous démontrerons qu'il y a, au plus, un nombre fini d'entiers x' et rationels y' avec :

(a) $|x'| \geqslant C_1$,
(b) $y' = \varphi(x')$,
(c) $y' = u/v$ avec $|v| \leqslant |x'|^{(\mu-\delta)/n}$.

Ceci suffira, parce qu'il y a, au plus, un nombre fini d'entiers x' et de rationels y' avec $|x'| \leqslant C_1$ et $f(x' , y') = 0$.

L'idée de la démonstration est facile. Avec chaque développement en série de Puiseux, nous construirons un polynôme $H(X , Y) \in \underset{\sim}{Z}[X , Y]$ et une fonction $R(X)$ avec les propriétés suivantes :

Si $f(x , y) = 0$ et $|x| \geqslant C_1$, nous avons
(a) $H(x , y) = R(x)$,
(b) $|R(x)| \dashrightarrow 0$ comme $|x| \longrightarrow \infty$,
(c) $|H(x , y)| \neq 0$ et $H(x , y)$ est presque un entier.

Donc, si $|x|$ est grand, nous aurons une contradiction.

Soit $h(X , Y) = \sum_{r=0}^{\mu-1} \sum_{\nu=0}^{m} C_{r\nu} X^r Y^{n+\nu}$, où m et les $C_{r\nu}$ sont des entiers que nous déterminerons ultérieurement.

Si x , y vérifient l'équation $f(x , y) = 0$, par $(3)_\nu$, nous avons

$$h(x , y) = \sum_{r=0}^{\mu-1} \sum_{\nu=0}^{m} \sum_{i=1}^{n} C_{r\nu} x^r B_i^{(\nu)}(x)/A_0^{\nu+1}(x) y^{n-i} .$$

Par les équations $(4)_\nu$, nous avons

$$h(x , y) = \sum_{r,\nu,i} C_{r\nu} x^r P_i^{(\nu)}(x) y^{n-i} + \sum_{r,\nu,i} \sum_{j=1}^{\infty} C_{r\nu} a_{ij}^{(\nu)} y^{n-i}/x^{j-r}$$

$$= P(x , y) + \sum_{t=0}^{n+1} \sum_{s=0}^{\infty} L_{ts}(c) y^t/x^s ;$$

où $P(x , y)$, considéré comme polynôme en y , a ses coefficients dans $\underset{\sim}{Q}[x , \{C_{r\nu}\}]$ et son dégré égal à $(n - 1)$, et les $L_{ts}(c)$ sont des formes linéaires des $C_{r\nu}$ à coefficients rationels.

Nous choisirons les $\{C_{r\nu}\} \in \underset{\sim}{Z}$, non tous nuls, de telle sorte que $L_{ts}(c) = 0$ pour tout (t , s) , avec $0 \leqslant t \leqslant (n - 1)$ et $0 \leqslant s \leqslant pt/q + (n + m)(\mu - \delta)/n$.

C'est possible, parce que nous avons $\mu(m + 1)$ variables, $C_{r\nu}$ et au plus $(\mu - \delta)(m + n) + pn(n + 1)/2q$ équations $L_{ts}(c) = 0$, si m est grand, nous avons

$$\mu(m+1) > (\mu-\delta)(m+n) + pn(n+1)/2q ,$$

et les équations $L_{ts}(c) = 0$ ont une solution non triviale avec $C_{r\nu} \in \underset{\sim}{Z}$.

Nous avons

$$h(x , y) - P(x , y) = \sum_{t=0}^{n-1} \sum_{s=0}^{\infty} L_{ts}\, y^t/x^s .$$

Ecrivons $y = \varphi(x) = \sum_{r=0}^{\infty} \alpha_r\, x^{(p-r)/q}$ dans le second membre de l'équation précédente, et multiplions par le dénominateur commun des coefficients de $P(x , y)$

$$dh(x , y) - dP(x , y) = R(x) = \sum_{i=0}^{\infty} \beta_i/x^{(\gamma+i)/q} ,$$

pour $|x| \geqslant c_1$, où les $\{\beta_i\} \in K$ et $\gamma > (n+m)(\mu-\delta)q/n$.

Observations.

1° $R(x) \not\equiv 0$, parce que, si $R(x) \equiv 0$, on a

$$0 = dh(x , y) - dP(x , y) = -P(x , y) + \Psi_0(x)y^n + \ldots + \Psi_m(x)y^{n+m} ,$$

et, comme $\partial_y P(x , y) \leqslant (n-1)$, nous déduisons par le lemme (a),

$$\Psi_0(x) = \ldots = \Psi_m(x) = 0 .$$

Par suite, tous les $C_{r\nu} = 0$, d'où une contradiction.

2° Si $R(x) \not\equiv 0$, il existe c_2 avec la propriété $|R(x)| \neq 0$, $\forall\, x$, avec $|x| \geqslant c_2$, parce que $R(x) = \beta_0/x^{\gamma/q} + \beta_1/x^{(\gamma+1)/q} + \ldots$ et, comme $|x| \longrightarrow \infty$, nous avons

$$|\beta_0/x^{\gamma/q}| \geqslant |\beta_1/x^{\gamma+2/q} + \ldots| .$$

3° Il existe c_3 avec la propriété $0 < |R(x)\cdot x^{(n+m)(\mu-\delta)/n}| < 1$ si $|x| > c_3$.

Donc, si $|x| \geqslant c_4 = \max\{c_0 , c_1 , c_2 , c_3\}$, nous avons

$$0 < |R(x)| = |dh(x , y) - dP(x , y)| < |x|^{-(n+m)(\mu-\delta)/n} ,$$

si $x' \in \underset{\sim}{Z}$, $y' = u/\nu$, $|x'| \geqslant c_4$ et $f(x' , y') = 0$, nous avons

$$0 < 1/|\nu|^{m+n} \leqslant |h(x' , u/\nu) - P(x' , u/\nu)| < |x'|^{-(m+n)(\mu-\delta)/n}) ,$$

donc, $|\nu| > |x'|^{(\mu-\delta)/n}$.

Par suite, il y a un nombre fini d'entiers x' et de rationels y' , avec $f(x' , y') = 0$ et $y' = u/\nu$ avec $|\nu| \leqslant |x'|^{(\mu-\delta)/n}$. Ils remplissent la condition $|x'| \leqslant c_4$.

Il est possible d'écrire c_4 en fonction des coefficients du polynôme $f(x , y)$.

(Texte reçu le 24 janvier 1972)

William J. ELLISON
Université de Bordeaux-I
Département de Mathématiques
351 cours de la Libération
33405 TALENCE