Or si $u \in O_K$, on vérifie que:

$$\begin{cases}(x+2u)^4 - c_4 \equiv 8(x+2u)z' \bmod 16,\\ P(x+2u) \equiv 16(z')^2 \bmod 64,\end{cases}$$

où $z' = z + ux^2 + u^2x$.

Cela démontre l'assertion. Par conséquent, la solution x du système peut être recherchée modulo 2.

D. Conséquences.

1. Considérons E une courbe elliptique définie sur K. Soit (W) un modèle de E entier, et π une uniformisante de K. (W) est un modèle minimal pour E si et seulement si $c_4(W)/\pi^4$ et $c_6(W)/\pi^6$ ne sont pas les invariants $c_4(W')$ et $c_6(W')$ d'une équation de Weierstrass (W') définie sur O_K. Les résultats précédents permettent donc de déterminer si un modèle donné de E est minimal.

2. Désignons par $v_p(a)$ la valuation p-adique d'un entier relatif a.

PROPOSITION 2. *Soient c_4, c_6, Δ des éléments de $\mathbf{Z}$ tels que $c_4^3 - c_6^2 = 1728\,\Delta$ et $\Delta \neq 0$. Pour qu'il existe une équation de Weierstrass (W) à coefficients dans $\mathbf{Z}$ avec $c_4 = c_4(W)$, $c_6 = c_6(W)$ il faut et il suffit que l'on ait $v_3(c_6) \neq 2$ et*

$$\begin{cases} c_6 \equiv -1 \bmod 4\\ \textit{ou}\\ v_2(c_4) \geqslant 4 \quad \textit{et} \quad c_6 \equiv 0 \textit{ ou } 8 \bmod 32.\end{cases}$$

On a $c_4 = c_4(W)$, $c_6 = c_6(W)$ avec (W) une équation de Weierstrass définie sur $\mathbf{Z}$ si et seulement si il en est de même sur $\mathbf{Z}_2$ et $\mathbf{Z}_3$. Il suffit alors de récrire les corollaires des deux théorèmes pour obtenir le résultat.

Remarque. J. F. Mestre m'a communiqué l'énoncé de la proposition 2 qu'il avait obtenu auparavant mais qu'il n'a pas publié.

Bibliographie

[1] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*; in: *Modular Functions of One Variable IV*, Lecture Notes in Math. 476, Springer-Verlag, 1975, 33–52.

Reçu le 1.3.1988 (1795)

ACTA ARITHMETICA
LIV (1989)

Sur un théorème de M. Langevin

par

MAURICE MIGNOTTE (Strasbourg)

1. Introduction. Dans [4], Michel Langevin a démontré le résultat suivant.

THÉORÈME A. *Soit V un voisinage d'un point du cercle unité. Alors il existe une constante $C > 1$, effectivement calculable, telle que tout polynôme à coefficients entiers, irréductible et qui ne possède pas de zéro dans V a une mesure qui vérifie $M(P) \geqslant C^d$ lorsque le degré d du polynôme P est assez grand.*

La démonstration utilise la notion de diamètre transfini. L'étape principale consistant à prouver que le diamètre transfini du disque unité privé des points de V est < 1.

Nous allons donner une démonstration très différente de ce résultat. Cette démonstration s'effectue en deux étapes:

1°, construction d'un multiple du polynôme P de petite hauteur,

2°, application d'un théorème d'Erdős–Turán sur la répartition des racines d'un polynôme à coefficients complexes.

Par cette méthode nous obtenons un résultat général dont le théorème A est un corollaire (voir la remarque à la suite du corollaire 3).

Soit

$$F = \sum_{i=0}^{n} a_i X^i, \quad a_n \neq 0,$$

un polynôme à coefficients complexes. Rappelons les définitions suivantes: on pose

$$H(F) = \max_{0 \leqslant i \leqslant n} |a_i|, \quad \text{la hauteur de } F,$$

$$L(F) = \sum_{i=0}^{n} |a_i|, \quad \text{la longueur de } F.$$

Enfin, la mesure de F, notion très importante introduite par K. Mahler, est définie par

$$M(F) = |a_n| \prod_{j=1}^{n} \max\{1, |z_j|\},$$

où $z_1, \ldots, z_n$ sont les racines complexes de F.

2. Construction d'un multiple de P de petite hauteur.

THÉORÈME B. *Soit P un polynôme à coefficients entiers, irréductible, de degré égal à d. Soit D un entier, $D \geqslant d$. Alors il existe un polynôme G non nul, à coefficients entiers, divisible par P, de degré au plus D et qui vérifie*

$$H(G) \leqslant \left((D+1)^{d/2} M^D\right)^{1/(D+1-d)},$$

où M est la mesure de P.

> C'est une application directe du raffinement du lemme de Siegel obtenu par Bombieri et Vaaler, [1]. Mais, comme me l'a fait remarquer P. Bundschuh, une application directe du théorème de Minkowski suffit pour obtenir la borne

$$H(G) \leqslant \left(2^d (D+1)^{d/2} M^D\right)^{1/(D+1-d)}. <$$

3. Le théorème d'Erdős–Turán. Le théorème d'Erdős–Turán dont il s'agit ici est le suivant:

THÉORÈME C. *Soit Q un polynôme non nul à coefficients complexes, de degré D, de coefficients extrêmes a et b, et de longueur L. Soit S un secteur du plan complexe centré à l'origine et d'ouverture α, $0 \leqslant \alpha \leqslant 2\pi$. Alors le nombre $N(S)$ de racines du polynôme Q qui appartiennent à S vérifie*

$$|N(S) - \alpha D/2\pi| \leqslant c\left(D \operatorname{Log}(L/\sqrt{|ab|})\right)^{1/2},$$

où c vaut

$$c = (2\pi/0.916\ldots)^{1/2} < 2.62.$$

Voir [2] pour une démonstration (dans l'énoncé du théorème de cet article figure la constante $c = 16$, mais une lecture rapide de la démonstration donne le résultat avec la valeur $c = 4$). Une autre démonstration a été donnée par Ganelius, [3]; ce dernier obtient le théorème avec la constante qui figure ici.

Remarque. Dans l'énoncé du théorème C, nous n'avons pas précisé si le secteur S est ouvert ou fermé (ou semi-fermé), en fait le théorème est vrai dans tous les cas.

4. Sur la répartition des racines des polynômes irréductibles à coefficients entiers. A partir des théorèmes B et C on obtient le résultat général suivant.

THÉORÈME. *Soit P un polynôme irréductible à coefficients entiers de degré d. Soit S un secteur (ouvert ou fermé) du plan complexe, centré à l'origine et d'ouverture $2\pi\theta$, où $0 \leqslant \theta \leqslant 1$. Alors le nombre $N(S)$ de racines du polynôme P qui appartiennent à S vérifie toujours*

(i)
$$N(S) \leqslant 2\theta d + c\sqrt{2d\left(\tfrac{3}{2}\operatorname{Log}(2d) + 2\operatorname{Log} M\right)},$$

où M désigne la mesure du polynôme P.

De plus, si pour un certain nombre ε, $0 < \varepsilon < 1$, la condition

(*)
$$\operatorname{Log}\left((2d+1)M\right) \leqslant 2\varepsilon^3 d(\theta/c)^2$$

a lieu alors on a

(ii)
$$N(S) \leqslant \theta d + c_1 \sqrt[3]{d^2 \operatorname{Log}\left((2d+1)M\right)} \cdot \theta^{1/3},$$

où

$$c_1 = c^{2/3}\left(2^{-1/3} + 2^{1/6}\sqrt{1+3\varepsilon}\right).$$

> Soit D un entier qui sera fixé plus loin, $D \geqslant d$. Considérons le polynôme G, multiple de P, obtenu grâce au théorème B. Si on lui applique le théorème C, il vient

$$N_G(S) \leqslant \theta D + c(D \operatorname{Log} L)^{1/2},$$

où L, la longueur de G, vérifie

$$L(G) \leqslant \left((D+1)^{d/2} M^D\right)^{1/(D+1-d)} \cdot (D+1).$$

De plus, trivialement,

$$N(S) = N_P(S) \leqslant N_G(S).$$

En regroupant toutes ces inégalités on trouve

$$N(S) \leqslant \theta D + c\sqrt{D \cdot \left(\operatorname{Log}(D+1) + \frac{1}{D+1-d} \operatorname{Log}\left((D+1)^{d/2} M^D\right)\right)}.$$

D'où (i) en choisissant $D = 2d-1$.

Passons maintenant à la démonstration de (ii). Nous supposons donc la condition (*) satisfaite. Si x est un nombre réel quelconque compris entre $D-d$ et $D-d+1$, la majoration précédente de $N(S)$ implique

$$N(S) \leqslant \theta d + \theta x + c\sqrt{(d+x)\left(\operatorname{Log}(d+x+1) + \frac{1}{x} \operatorname{Log}\left((d+x+1)^{d/2} M^{d+x}\right)\right)}.$$

Prenons

$$x = \left(\frac{c^2 d^2 \mu}{2\theta^2}\right)^{1/3},$$

où, pour simplifier, on a posé

$$\mu = \mathrm{Log}((2d+1)M).$$

La condition (*) implique $x \leqslant \varepsilon d$, et donc

$$N(S) \leqslant \theta d + \theta x + c\sqrt{(d+x)\left(1+\frac{d}{x}\right)\mu} \leqslant \theta d + \theta x + c\sqrt{\frac{d^2(1+3\varepsilon)\mu}{x}}.$$

D'où l'inégalité (ii). <

On en déduit aussitôt le résultat suivant déjà démontré dans [5].

COROLLAIRE 1. *Soit P un polynôme irréductible à coefficients entiers de degré d et de mesure M. Alors le nombre r de racines réelles positives de P vérifie*

$$r \leqslant 2c\sqrt{2d\left(\tfrac{3}{2}\mathrm{Log}(2d) + 2\mathrm{Log}M\right)},$$

en particulier pour $M \leqslant 2d$ on a

$$r \leqslant 14\sqrt{d\,\mathrm{Log}(2d)}.$$

COROLLAIRE 2. *Soient S et P comme dans l'énoncé du théorème. On a toujours*

(i') $$N(S) \geqslant 2\theta d - d - c\sqrt{2d\left(\tfrac{3}{2}\mathrm{Log}(2d) + 2\mathrm{Log}M\right)}.$$

De plus, si (*) a lieu alors on a

(ii') $$N(S) \geqslant \theta d - c_1(1-\theta)^{1/3}\left(d^2\,\mathrm{Log}((2d+1)M)\right)^{1/3}.$$

> Appliquer le théorème au secteur S' complémentaire de S ainsi que la relation évidente $N(S)+N(S') = d$. <

COROLLAIRE 3. *Soit P un polynôme à coefficients entiers, irréductible et de degré d. Soit S un secteur centré à l'origine et d'ouverture $2\pi\theta$, $0 \leqslant \theta \leqslant 1/2$. On suppose que le polynôme P ne possède pas de racine dans l'ensemble*

$$D(S, \lambda) = \{z \in S;\ \lambda^{-1} \leqslant |z| \leqslant \lambda\},$$

où λ est un réel fixé > 1. Alors la mesure du polynôme P vérifie

$$\mathrm{Log}(M) \geqslant \mathrm{Inf}\{\tfrac{1}{16}d\theta^3 - \tfrac{11}{2}\mathrm{Log}2d,\ \tfrac{1}{8}d\theta\,\mathrm{Log}\lambda\}.$$

> Soit P un polynôme vérifiant les conditions de l'énoncé.

Supposons d'abord que P possède au moins $d\theta/4$ racines dans S, alors ou bien, P a au moins $d\theta/8$ zéros de module $\geqslant \lambda$ et on a donc

$$\mathrm{Log}M \geqslant (d\theta/8)\,\mathrm{Log}\lambda,$$

ou bien, P a au moins $d\theta/8$ zéros de module $\leqslant \lambda^{-1}$ et, si $z_1, \ldots, z_k$ sont ces zéros, l'inégalité $M|z_1 \ldots z_k| \geqslant 1$ montre que la minoration précédente a encore lieu.

Le corollaire est donc vrai dans ce cas.

Supposons maintenant que le polynôme P possède au plus $d\theta/4$ racines dans S. Appliquons alors au complémentaire S' de S la seconde majoration de $N(S')$ obtenue dans la démonstration du théorème. En choisissant $x = \theta' d$, où $\theta' = \theta/(4(1-\theta))$, il vient

$$d - \theta d/4 \leqslant (1-\theta)(d+x) + c\left((d+x)(1+1/(2\theta'))\,\mathrm{Log}\,2d + ((1+\theta')/\theta')\mu\right)^{1/2},$$

ce qui implique

$$\frac{\theta d}{2} \leqslant c\left(\frac{5d}{4}\left(\frac{2-\theta}{\theta}\mathrm{Log}\,2d\right) + \left(\frac{(4-3\theta)^2}{4\theta(1-\theta)}\right)d\mu\right)^{1/2}.$$

On a donc

$$\mu \geqslant \frac{4\theta(1-\theta)}{(4-3\theta)^2}\left(\frac{\theta^2 d}{4} - \frac{5c^2}{4\theta}(2-\theta)\,\mathrm{Log}\,2d\right),$$

ou encore

$$\mu \geqslant \frac{(1-\theta)\theta^3}{(4-3\theta)^2}d - \frac{5c^2(1-\theta)(2-\theta)}{(4-3\theta)^2}\mathrm{Log}\,2d.$$

Compte tenu de l'encadrement $0 \leqslant \theta \leqslant 1/2$, on en déduit la minoration

$$\mu \geqslant \theta^3 d/16 - (11/2)\,\mathrm{Log}\,2d. <$$

Remarque. Le corollaire 3 entraîne le théorème A. En effet, il existe S et $\lambda > 1$ tels que V contienne un domaine de la forme $D(S, \lambda)$ avec $\theta > 0$. Par conséquent, sous les hypothèses du théorème A, pour tout $\eta > 0$ fixé, la mesure M du polynôme P vérifie $M > C^d$ pour $d > d(\eta)$, avec

$$C = \exp(\min\{(1/17)\theta^3, (\theta/8)\,\mathrm{Log}\,\lambda\}).$$

Notons aussi que ce corollaire (donc aussi le théorème) n'est plus vrai si on suppose seulement P à coefficients entiers (exemple: $P = (X-1)^n$), ou P quadratfrei à coefficients réels (exemple: $P = (X-x_1)\ldots(X-x_n)$, où les x_i sont des nombres réels distincts très proches de 1).

Remerciements. Je remercie vivement Peter Bundschuh et Michel Langevin pour leurs conseils et pour m'avoir signalé quelques erreurs dans une version antérieure de cet article.

Références

[1] E. Bombieri and J. D. Vaaler, *On Siegel's lemma*, Invent. Math. 73(1983), 539–560.
[2] P. Erdős and P. Turán, *On the distribution of roots of polynomials*, Annals of Math. 51(1950), 105–119.
[3] T. Ganelius, *Sequences of analytic functions and their zeros*, Arkiv för Math. 3(1958), 1–50.

[4] M. Langevin, *Minoration de la maison et de la mesure de Mahler de certains entiers algébriques*, C. R. Acad. Sc. Paris 303 (1986), 241.

[5] M. Mignotte, *Sur la répartition des racines des polynômes*, Journées arithmétiques de Caen, septembre 1980.

UNIVERSITÉ LOUIS PASTEUR
MATHÉMATIQUE
67087 Strasbourg
France

Reçu le 23.3.1988
et dans la forme modifiée le 3.8.1988 (1801)