References

[1] З. И. Боревич, И. Р. Шафаревич, *Теория чисел*, Москва 1972.

[2] И. М. Виноградов, *Верхняя граница модуля тригонометрической суммы*, И. А. Н. СССР, серия матем., 14 (1950), pp. 199–214.

[3] -- *Метод тригонометрической суммы в теории чисел*, Москва 1971.

[4] А. В. Соколовский, *Теорема о нулях дзета функции Дедекинда и расстояние между „соседними" простыми идеалами*, Acta Arith. 13 (1968), pp. 321–334.

[5] E. Landau, *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale*, Leipzig und Berlin 1927.

[6] J. S. Luthar, *A note on a result of Mahler*, J. Austral. Math. Soc. 6 (1966), pp. 399–401.

[7] K. Mahler, *Inequalities for ideal bases in algebraic number fields*. ibid. 4 (1964), pp. 425–448.

[8] T. Mitsui, *On the prime ideal theorem*, J. Math. Soc. Japan 20 (1–2) (1968), pp. 233–247.

[9] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Warszawa 1974.

[10] К. Прахар, *Распределение простых чисел*. Москва 1967.

[11] R. Remak, *Elementare Abschätzungen von Fundamentaleinheiten und des Regulator's eines algebraischen Zahlkörpres*, J. Reine Angew. Math. 165 (1931), pp. 159–180.

[12] C. L. Siegel, *Abschätzung von Einheiten*, Nachr. Akad. Wiss. Göttingen (1969), pp. 71–86.

[13] Vera T. Sós and P. Turán, *On some new theorems in the theory of diophantine approximations*, Acta Math. Hung. 6 (1965), pp. 241–257.

[14] W. Staś, *Über eine Anwendung der Methode von Turán auf die Theorie des Restgliedes im Primidealsatz*, Acta Arith. 5 (1959), pp. 179–195.

[15] P. Turán, *Eine neue Methode in der Analysis und deren Anwendungen*, Budapest 1953.

INSTITUTE OF MATHEMATICS OF THE ADAM MICKIEWICZ UNIVERSITY
Poznań, Poland

Received on 26. 4. 1976 (846)

ACTA ARITHMETICA
XXXIV (1978)

Sur la dimension diophantienne des corps p-adiques

par

GUY TERJANIAN (Toulouse)

1. La notion de dimension diophantienne. Soient A un anneau intègre et p un élément de $A[X_i]_{i\in I}$, nous dirons que p est anisotrope, ou anisotrope sur A, si I est fini, si p est sans terme constant et si le seul zéro de p dans A est le zéro banal; sous ces hypothèses, si p est de degré $d>1$ on appelle ordre de p le nombre $\log_d n$, où n est le nombre des indéterminées de p. Soit K un corps commutatif, on appelle dimension diophantienne de K et on note $\mathrm{dd}(K)$ la borne supérieure, finie ou non, des ordres des polynômes à coefficients dans K, de degrés strictement supérieurs à un, homogènes et anisotropes.

Nous nous proposons de montrer que, si K est une extension finie du corps des nombres p-adiques, on a $\mathrm{dd}(K)\geqslant 3$. Nous généraliserons ainsi le résultat que J. Browkin avait obtenu dans le cas du corps des nombres p-adiques; pour cela, nous nous servons, outre les travaux déjà cités de Browkin [1], d'une idée que nous avons remarquée dans des travaux non publiés de S. Schanuel.

2. Le polynôme de Browkin–Schanuel. Rappelons et précisons quelques définitions de Browkin [1]. On désigne par p un nombre premier et par r un entier $\geqslant 0$. On suppose $r\geqslant 3$ lorsque p vaut 2. On a $p^r\geqslant 2r+1$ et on note n la partie entière de $p^r/(2r+1)$. Pour i entier compris entre 1 et $r+1$, on note a_i le nombre

$$(-1)^{i+1}\binom{r+i-1}{i-1}\binom{2r+1}{r+i}.$$

Si $s_1,\dots,s_j$ sont des entiers $\geqslant 0$ et $X_1,\dots,X_j$ des indéterminées, on note $d(s_1,\dots,s_j)$ l'opérateur $\dfrac{\partial^{s_1+\dots+s_j}}{\partial X_1^{s_1}\dots\partial X_j^{s_j}}$. Pour k entier tel que $1\leqslant k\leqslant n$, on définit les éléments ψ_k et φ_k de $\boldsymbol{Z}[X_1,\dots,X_n]$ par:

$$\psi_k=\sum_{i=1}^{r+1}a_iX_1^{p^r-(r+i)(k-1)}\prod_{2\leqslant j\leqslant k}X_j^{r+i},$$

$$\varphi_k=\sum_{1\leqslant i_1<\dots<i_k\leqslant n}\psi_k(X_{i_1},\dots,X_{i_k}).$$

On pose enfin:

$$f = \sum_{k=1}^{n} (-1)^{k+1} \varphi_k.$$

PROPOSITION 1. *Soit a un élément non nul de $\mathbf{Z}^n$ dont les coordonnées valent 0 ou 1, on a $f(a) = 1$; de plus, si les entiers $s_1, \ldots, s_n$ sont $\geqslant 0$ tels que $1 \leqslant s_1 + \ldots + s_n \leqslant r$, on a*

$$d(s_1, \ldots, s_n)(f)(a) \equiv 0 \bmod p^r.$$

Voir [1] pour la démonstration.

Soit K une extension finie du corps $\mathbf{Q}_p$ des nombres p-adiques. Nous noterons A l'anneau des entiers de K, π une uniformisante, e l'indice de ramification et $q = p^f$ le nombre des éléments du corps résiduel. De plus, l'entier $d = ef$ sera le degré de K sur $\mathbf{Q}_p$, $\omega_1, \ldots, \omega_d$ sera une base de A sur $\mathbf{Z}$ et γ le plus petit entier strictement positif, tel que, pour tout élément inversible x de A, on ait $x^\gamma \equiv 1 \bmod p$.

PROPOSITION 2. *On a $\gamma = p^k(q-1)$ où k est le plus petit entier tel qu'on ait $e \leqslant p^k$.*

Le nombre des éléments inversibles de l'anneau $A/(p)$ est $q^{e-1}(q-1)$; donc γ divise $q^{e-1}(q-1)$. D'autre part, le groupe multiplicatif du corps résiduel est cyclique d'ordre $q-1$; donc γ est un multiple de $q-1$. Il résulte de ceci que γ est de la forme $p^l(q-1)$.

On a $(1+\pi)^\gamma \equiv 1 \bmod p$; d'où $(1+\pi^{p^l})^{q-1} \equiv 1 \bmod p$; d'où $p^l \geqslant e$. Inversement, si $p^m \geqslant e$ et si x est un élément inversible de A, on a $x^{q-1} = 1 + a\pi$ avec $a \in A$; d'où $x^{(q-1)p^m} \equiv 1 + (a\pi)^{p^m} \bmod p$; d'où $x^{(q-1)p^m} \equiv 1 \bmod p$.

PROPOSITION 3. *Soit x un élément de A^n dont les coordonnées sont congrues à zéro ou 1 mod p, sans être toutes congrues à zéro, on a*

$$f(x) \equiv 1 \bmod p^{r+1}.$$

Soient y et z les éléments de A^n tels qu'on ait $x = y + pz$ et que les coordonnées de y soient 0 ou 1; on a, par la formule de Taylor

$$f(x) = \sum_{(s_1, \ldots, s_n)} \frac{p^{s_1+\ldots+s_n}}{s_1! \ldots s_n!} z_1^{s_1} \ldots z_n^{s_n} d(s_1, \ldots, s_n)(f)(y).$$

Puisque $\dfrac{d(s_1, \ldots, s_n)(f)}{s_1! \ldots s_n!}$ est un polynôme à coefficients entiers, les termes pour lesquels $s_1 + \ldots + s_n \geqslant r+1$ sont divisibles par p^{r+1}. De plus, si les entiers $s_1, \ldots, s_n$ sont tels que $1 \leqslant s_1 + \ldots + s_n \leqslant r$, alors $\dfrac{p^{s_1+\ldots+s_n}}{s_1! \ldots s_n!}$ est divisible par p, tandis qu'en vertu de la proposition 1, $d(s_1, \ldots, s_n)(f)(y)$ est divisible par p^r, de sorte que le terme correspondant de la formule de Taylor est divisible par p^{r+1}. On a donc $f(x) \equiv f(y) \bmod p^{r+1}$ et la proposition 1 permet de conclure.

Définissons maintenant les polynômes g, h, H et G. Le polynôme g est l'élément de $\mathbf{Z}[X_1, \ldots, X_n]$ tel que $g = f(X_1^\gamma, \ldots, X_n^\gamma)$.

Posant $s = p^{r+1} - 1$ et $t = ns$, le polynôme h est l'élément de $\mathbf{Z}[X_1, \ldots, X_t]$ défini par

$$h = \sum_{i=0}^{s-1} g(X_{in+1}, \ldots, X_{(i+1)n}).$$

Posant $u = dt$, le polynôme H est l'élément de $A[X_1, \ldots, X_u]$ tel que

$$H = \sum_{i=1}^{d} \omega_i h(X_{(i-1)t+1}, \ldots, X_{it}).$$

Enfin, nous posons $v = \left[\dfrac{\gamma p^r}{e(r+1)}\right]$ et $w = vu$, nous définissons G comme l'élément de $A[X_1, \ldots, X_w]$ tel que

$$G = \sum_{i=0}^{v-1} p^{i(r+1)} H(X_{iu+1}, \ldots, X_{(i+1)u})$$

et nous dirons que G est le polynôme de Browkin–Schanuel du corps K.

On voit aisément que:

PROPOSITION 4. (i) *Soit x un élément de A^n; si les coordonnées de x sont toutes divisibles par π, on a $g(x) \equiv 0 \bmod p^{r+1}$; sinon on a $g(x) \equiv 1 \bmod p^{r+1}$.*

(ii) *Soit x un élément de A^l; si les coordonnées de x sont toutes divisibles par π, on a $h(x) \equiv 0 \bmod p^{r+1}$; sinon, $h(x)$ est congru modulo p^{r+1} à un entier compris entre 1 et $p^{r+1}-1$.*

(iii) *Si x est un élément de A^u tel qu'on ait $H(x) \equiv 0 \bmod p^{r+1}$, alors toutes les coordonnées de x sont divisibles par π.*

THÉORÈME 1. *Le polynôme G est anisotrope sur K.*

Nous raisonnerons par l'absurde en supposant G isotrope. Puisque G est homogène, il possède un zéro non banal x dans A et on peut supposer que l'une des coordonnées de x n'est pas divisible par π. Soit l le plus grand entier tel que les coordonnées de x d'indice $\leqslant lu$ soient multiples de π. Pour i entier tel que $0 \leqslant i \leqslant l$, les quantités $p^{i(r+1)} H(x_{iu+1}, \ldots, x_{(i+1)u})$ sont divisibles par π^{rp^r}, donc par $p^{v(r+1)}$ et par $p^{(l+1)(r+1)}$. Il en résulte que $p^{l(r+1)} H(x_{lu+1}, \ldots, x_{(l+1)u})$ est divisible par $p^{(l+1)(r+1)}$ et, en vertu de la proposition 4, que les éléments $x_{lu+1}, \ldots, x_{(l+1)u}$ sont divisibles par π, ce qui est absurde.

Le degré de G est γp^r, c'est donc un multiple de $(q-1)p^r$ et en particulier de $(p-1)p^r$. Le nombre des indéterminées de G est w et on a

$$w = d(p^{r+1}-1)\left[\frac{p^r}{2r+1}\right]\left[\frac{\gamma p^r}{e(r+1)}\right].$$

On prouve aisément que l'on a

$$\frac{w}{(\gamma p^r)^3} \leqslant \frac{fp}{\gamma^2(r+1)(2r+1)}.$$

En particulier, le rapport $w/(\gamma p^r)^3$ est inférieur ou égal au rapport $fp/(p^f-1)^2(r+1)(2r+1)$. On en déduit, en considérant d'abord le cas $p = 2$, que l'ordre de G est strictement inférieur à 3. D'autre part, l'ordre de G est

$$\log_{\gamma p^r} d(p^{r+1}-1) + \log_{\gamma p^r}\left[\frac{p^r}{2r+1}\right] + \log_{\gamma p^r}\left[\frac{\gamma p^r}{e(r+1)}\right].$$

Lorsque r tend vers l'infini, chacun des trois logarithmes tend vers 1 et on a prouvé:

THÉORÈME 2. *La dimension diophantienne de K est supérieure ou égale à trois.*

Je crois que, si K est une extension finie du corps des nombres p-adiques, on a $\mathrm{dd}(K) = 3$; une preuve de ceci ne constituerait qu'un premier pas dans l'étude des propriétés diophantiennes des corps p-adiques, car une étude plus approfondie se devrait de déterminer les fonctions $\varphi(K, s)$ et $\varphi_n(K, s)$ que j'ai définies dans [4].

Bibliographie

[1] J. Browkin, *On forms over p-adic fields*, Bull. Acad. Polon. Sci., Ser. Sci. Math. 14 (1966), p. 489–492.

[2] S. Schanuel, *Extensions of Terjanian's counter-example*, Notices Amer. Math. Soc. 14 (1967), p. 125–126.

[3] G. Terjanian, *Un contre-exemple à une conjecture d'Artin*, C.R.A.S. Paris 262A (1966), p. 612.

[4] — *Dimension arithmétique d'un corps*, J. of Algebra 22 (1972), p. 517–545.

UNIVERSITÉ PAUL SABATIER
Toulouse, France

Reçu le 5. 5. 1976
et dans la forme modifiée le 10. 7. 1976 (847)

ACTA ARITHMETICA
XXXIV (1978)

Формулы для числа представлений чисел некоторыми регулярными и полурегулярными тернарными квадратичными формами, принадлежащими двухклассным родам

Г. А. Ломадзе (Тбилиси)

1. Джонс и Полл [3] доказали, что существует лишь 20 *регулярных* примитивных положительных квадратичных форм вида

$$f = \{a_1, a_2, a_3\} = a_1x_1^2 + a_2x_2^2 + a_3x_3^2,$$

принадлежащих многоклассным родам. Они также нашли связанные с родами этих форм арифметические прогрессии, все числа которых и только они непредставимы соответствующей формой f. Далее, в [3] приведены и формы всех других классов упомянутых многоклассных родов. Эти формы являются *полурегулярными* примитивными квадратичными формами вида

$$g = \{c_{11}, c_{22}, c_{33}, c_{23}, c_{13}, c_{12}\} = \\ = c_{11}x_1^2 + c_{22}x_2^2 + c_{33}x_3^2 + 2c_{23}x_2x_3 + 2c_{13}x_1x_3 + 2c_{12}x_1x_2;$$

для некоторых из них в [3] найдены числа, которые вместе с числами упомянутых арифметических прогрессий также непредставимы соответствующей формой g.

В следующей ниже таблице приведены 6 из имеющихся 20 регулярных примитивных квадратичных форм f, принадлежащих двухклассным родам (первый столбец) и им соответствующие полурегулярные примитивные квадратичные формы g из другого класса того же рода (третий столбец); во втором столбце помещены арифметические прогрессии, все числа которых и только они непредставимы формами f (все числа этих прогрессий непредставимы и формами g); в четвертом столбце помещены множества чисел n, которые вместе с числами указанных арифметических прогрессий также непредставимы формами g.

Впервые Полл [10] получил формулы для числа представлений произвольных натуральных чисел формой $\{1, 1, 16\}$. Эти формулы выражаются через число представлений натурального числа суммой трех квадратов. Затем Л. Коган ([5], [6]) получил формулы для числа