Conspectus materiae tomi XXXI, fasciculi 4

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange — Address of the Editorial Board and of the exchange — Die Adresse der Schriftleitung und des Austausches — Адрес редакции и книгообмена

ACTA ARITHMETICA

ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

PRINTED IN POLAND

W R O C Ł A W S K A   D R U K A R N I A   N A U K O W A

ACTA ARITHMETICA
XXXI (1976)

Homogeneous approximation in completions of A-fields of non-zero characteristic

by

I. S. Luthar and Meenakshi Duggal (Chandigarh, India)

In 1941 Mahler [4] developed an analogue of Minkowski's Geometry of Numbers in fields of formal power series over finite fields; using the results of this paper, Aggarwal [1] obtained certain results on homogeneous approximation in fields of series. Recently, the authors [3] have been able to extend Mahler's results to the situation when $F_q(T)$, $F_q\{T\}$ and $F_q[T]$ are replaced by k, k_u and $\mathfrak{o}_u$, where k is an arbitrary A-field of characteristic $p \neq 0$, k_u is the completion of k at an arbitrary place u of k and $\mathfrak{o}_u$ is the ring of u-exceptional integers of k, i.e., those x in k such that $\operatorname{ord}_v(x) \geqslant 0$ for all places $v \neq u$ of k. It is the object of this paper to prove the results of Aggarwal [1] in the more general situation described above; in fact, we are able to improve upon one of his theorem by removing the rather severe condition that $q \geqslant m+n-1$.

Thus, let k be an A-field of characteristic $p \neq 0$ and genus g; let F_q denote the field of constants of k. Let u be a place of k of degree d and let $\mathfrak{o}_u$ be the ring of u-exceptional integers; let k_u denote the completion of k at u. For any element a of k_u, $\|a\|_u$ means $\inf_{a\in\mathfrak{o}_u} |a-a|_u$.

Theorem 1. *Let $L_j(x) = L_j(x_1, \ldots, x_m)$, $1 \leqslant j \leqslant n$, be n linear forms in m variables; then for each integer*

$$t > \frac{n}{m} + \frac{(m+n)(g-1)}{md},$$

the inequalities

$$|x_i|_u \leqslant q_u^t, \quad \|L_j(x)\|_u \leqslant q_u^{t'} \quad (1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n)$$

can be solved for a non-zero vector x in $\mathfrak{o}_u^m$; here

$$t' = \left[\frac{(m+n)(g-1)}{nd} - \frac{m}{n} t\right] + 1$$

(notice that, in view of the inequality for t, $t' < 0$).

Proof. Consider the k_u-lattice in the $(m+n)$-dimensional space k_u^{m+n} of vectors $(x_1, \ldots, x_m, y_1, \ldots, y_n)$ defined by

$$(1) \qquad |x_i|_u \leqslant q_u^t, \quad |L_j(x)-y_j|_u \leqslant q_u^{t'} \quad (1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n);$$

the volume of this lattice is $q_u^{mt+nt'} > q^{(m+n)(g-1)}$. Consequently, by Theorem 1 of [3], there exists (x, y) in $\mathfrak{o}_u^{m+n}$, not zero, such that the inequalities (1) are satisfied. If $x = 0$, then $|y_j|_u \leqslant q_u^{t'} < 1$; as y_j is in $\mathfrak{o}_u$, it follows that each y_j is zero; this gives the contradiction $(x, y) = 0$.

In particular, taking $m = 1$, we see that

$$|x|_u^{1/n} \max_{1\leqslant j\leqslant n} \|\theta_j x\|_u \leqslant q^{(1+1/n)(g-1)+d}$$

has infinitely many solution x in $\mathfrak{o}_u$.

Theorem 1 is best possible in the following sense.

THEOREM 2. *For each pair of positive integers m and n, there exists a constant γ and linear forms $L_j(x)$, $1 \leqslant j \leqslant n$, in m variables over k_u, such that for each non-zero x in $\mathfrak{o}_u^m$,*

$$(\max_i |x_i|_u)^m (\max_j \|L_j(x)\|_u)^n \geqslant q_u^{\gamma}.$$

The proof of a theorem like this depends upon the existence of a monic polynomial in $\mathfrak{o}_u[x]$ of degree $l = m+n$ which is irreducible over k, but has l distinct roots in k_u. Aggarwal [1] used the polynomial constructed by Armitage in [2] under the condition that $q \geqslant l-1$; the polynomial constructed by Armitage had an extra property regarding the absolute value of the discriminant which we do not need in this context. We construct below a monic polynomial of arbitrary degree $l \geqslant 1$ having coefficients in $\mathfrak{o}_u$, irreducible over k, and having l distinct roots in k_u. The proof of Theorem 2 then proceeds as usual and will not be reproduced here.

Suppose K is a p-field with maximal compact ring R; let $f(X)$ be a polynomial in $R[X]$ of degree $l \geqslant 1$ and let a be an element of R such that $f'(a) \neq 0$ and

$$\mathrm{ord}_K f'(a) = \delta, \qquad \mathrm{ord}_K f(a) = 2\delta + \varrho, \qquad \varrho \geqslant 1.$$

By Hensel's lemma, there exists in K one and only one root ξ of $f(X)$ such that

$$\mathrm{ord}_K(\xi - a) \geqslant \delta + 1;$$

for this ξ, we have, in fact,

$$\mathrm{ord}_K(\xi - a) \geqslant \delta + \varrho.$$

We now take

$$(2) \qquad f(X) = (X - a_1 z) \ldots (X - a_l z) - 1,$$

where $a_1, \ldots, a_l$ are fixed distinct non-zero elements of $\mathfrak{o}_u$, and z is some non-zero element of $\mathfrak{o}_u$ such that $t = -\mathrm{ord}_u z$ is very large. The roots of $f(X)$ are reciprocals of the roots of

$$(3) \qquad g(X) = (b_1 w - X) \ldots (b_l w - X) - b w^l X^l$$

where

$$b_i = a_i^{-1}, \; 1 \leqslant i \leqslant l, \qquad w = z^{-1}, \qquad b = \prod_i b_i.$$

As $|a_i|_u \geqslant 1$, $|z|_u \geqslant 1$, therefore $|b_i|_u \leqslant 1$, $|w|_u \leqslant 1$ and hence $g(X)$ has coefficients in the maximal compact subring r_u of k_u. Now

$$g'(b_i w) = -\prod_{j\neq i}(b_j w - b_i w) - l b b_i^{l-1} w^{2l-1}$$

and therefore, for large enough t

$$(4) \qquad \mathrm{ord}_u g'(b_i w) = (l-1)t + t_i,$$

where

$$t_i = \mathrm{ord}_u \prod_{j \neq i}(b_j - b_i)$$

is independent of z; moreover $g(b_i w) = -b b_i^l w^{2l}$ so that

$$(5) \qquad \mathrm{ord}_u g(b_i w) = 2lt + t_i' = 2(l-1)t + 2t_i + (2t - 2t_i + t_i'),$$

where $t_i' = \mathrm{ord}_u(b b_i^l)$ is again independent of z. For large t, $2t - 2t_i + t_i' \geqslant 1$ and hence, by Hensel's lemma, there exists a unique root η_i of $g(X)$ in k_u such that

$$(6) \qquad \mathrm{ord}_u(\eta_i - b_i w) \geqslant (l+1)t - t_i + t_i'$$

so that for large t

$$(7) \qquad \mathrm{ord}_u(\eta_i) = \mathrm{ord}_u(b_i w).$$

If $\eta_i = \eta_j$ for $i \neq j$, then by (6), we get

$$\mathrm{ord}_u\big((b_i - b_j)w\big) \geqslant (l+1)t + \min(t_i' - t_i, t_j' - t_j);$$

this is impossible if t is large. Thus, for large t, $g(X)$ has l distinct roots in k_u. Now, let $\xi_i = \eta_i^{-1}$; then ξ_i is a root of $f(X)$, and by (6) and (7), we have:

$$(8) \qquad \mathrm{ord}_u(\xi_i - a_i z) \geqslant (l+1)t + t_i' - t_i - 2\,\mathrm{ord}_u(b_i w) = (l-1)t + t_i'',$$

where t_i'' does not depend upon z. In case $f(X)$ is not irreducible over k, there is a proper subset, say $\xi_1, \ldots, \xi_L$ with $L < l$, of the roots of $f(X)$ which are conjugate to each other over k. As $f(a_1 z) = -1$, $a_1 z$ is not a root of $f(X)$, and hence

$$\xi = \prod_{\lambda=1}^{L} (a_1 z - \xi_\lambda) \neq 0;$$

now ξ is a polynomial in $a_1 z$ with coefficients which are $\pm$ (elementary symmetric functions of $\xi_1, \ldots, \xi_L$) and hence elements of k; these coefficients are integral over $\mathfrak{o}_u$ and hence they are in $\mathfrak{o}_u$ because $\mathfrak{o}_u$ is integrally closed. Consequently ξ is a non-zero member of $\mathfrak{o}_u$ and hence $\mathrm{ord}_u(\xi) \leqslant 0$. On the other hand, we have, by (8):

$$\mathrm{ord}_u(a_1 z - \xi_1) \geqslant (l-1)t + t_1''$$

and for $2 \leqslant \lambda \leqslant L$,

$$\mathrm{ord}_u(a_1 z - \xi_\lambda) = -t + \mathrm{ord}_u(a_1 - a_\lambda)$$

so that

$$\mathrm{ord}_u(\xi) \geqslant (l-L)t + c,$$

where c depends only on $a_1, \ldots, a_l$, and not on t. Taking t large, $\mathrm{ord}_u(\xi) > 0$, giving us the desired contradiction. This concludes the construction of a polynomial of the desired kind, which in turn, leads to a proof of Theorem 2.

Let again $L_j(x)$, $1 \leqslant j \leqslant n$, be n independent linear forms in m variables $x_1, \ldots, x_m$, of matrix $A = (a_{ij})_{n\times m}$. Define

$$q_u^{\delta} = \max_N |\det(N)|_u, \tag{9}$$

where N runs through all non-singular $n \times n$ submatrices of A, and

$$q_u^{\varrho} = \max_S \min_{S'} |\det(SS'^{-1})|_u, \tag{10}$$

where S runs through all $s \times s$ submatrices of A with $s \leqslant n-1$, and for a given S of this kind, S' runs through all non-singular $(s+1)\times(s+1)$ submatrices of A which "contain" S. Let $\varrho_1, \ldots, \varrho_n, \sigma$ be integers such that $\varrho_j \geqslant \varrho$, $1 \leqslant j \leqslant n$, and $\sigma \geqslant 0$. Proceeding exactly as in Aggarwal [1], we see that the inequalities

$$|x_i|_u \leqslant q_u^{\sigma}, \quad |L_j(x)|_u \leqslant q_u^{-\varrho_j} \quad (1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n) \tag{11}$$

define a k_u-lattice of volume $q_u^{(m-n)\sigma-(\delta+\varrho_1+\ldots+\varrho_n)}$. Consequently, by Theorem 1 of [3], we have

THEOREM 3. *Let $L_1, \ldots, L_n$ be n independent linear forms over k_u in m variables $x_1, \ldots, x_m$, of matrix $A = (a_{ij})_{n\times m}$. Let δ and ϱ be defined by* (9) *and* (10), *and let $\varrho_1, \ldots, \varrho_n, \sigma$ be integers such that $\varrho_j \geqslant \varrho$ for $1 \leqslant j \leqslant n$, and $\sigma \geqslant 0$. Suppose that*

$$(m-n)\sigma > \frac{m(g-1)}{d} + (\delta + \varrho_1 + \ldots + \varrho_n);$$

then the inequalities (11) *can be solved for a non-zero x in $\mathfrak{o}_u^m$.*

Using this theorem, we easily deduce

THEOREM 4. *Let $L_1, \ldots, L_n$ be as above and let $m > n$. Suppose there is no non-zero x in $\mathfrak{o}_u^m$ at which all of L_j vanish. Then the inequality*

$$\big(\max_j |L_j(x)|_u\big)^n \big(\max_i |x_i|_u\big)^{m-n} \leqslant q^{m(g-1)} q_u^{\delta+m-n}$$

has infinitely many solutions in $\mathfrak{o}_u^m$.

References

[1] S. K. Aggarwal, *Homogeneous approximation in the field of formal power series*, Proc. Nat. Inst. Sci. India, A, 34 (5) (1968), pp. 242–249.

[2] J. V. Armitage, *The product of n linear forms in a field of series*, Mathematika 4 (1957), pp. 132–137.

[3] I. S. Luthar and Meenakshi Vinyard, *Minkowski's theorems in completions of A-fields of non-zero characteristic*, submitted.

[4] Kurt Mahler, *An analogue to Minkowski's Geometry of Numbers in a field of series*, Ann. of Math. 42 (1941), pp. 488–522.

[5] André Weil, *Basic Numbers Theory*, New York 1967.

MATHEMATICS DEPARTMENT
PANJAB UNIVERSITY
Chandigarh, India

Received on 17. 2. 1975 (680)