Now choosing c_1 and c_2 as in the following table we see that this is impossible therefore providing us with the final contradiction that proves the theorem.

c_1	c_2	a_1	b_1^2	$\frac{1}{4}g(a_1)$
.87	.88	.74	.014	.22
.88	.89	.72	.011	.24
.89	.9	.705	.0146	.242
.9	.91	.694	.017	.242
.91	.92	.683	.02	.243
.92	.93	.671	.023	.245
.93	.94	.66	.027	.242
.94	.95	.65	.032	.24
.95	.96	.64	.038	.23
.96	.97	.63	.045	.22
.97	.98	.62	.054	.2
.98	.99	.61	.067	.16
.99	1	.6	.086	.11

References

[1] R. P. Bambah, *On lattice coverings by spheres*, Proc. Nat. Inst. Sci. India, 20 (1954), pp. 25–52.
[2] E. S. Barnes, *The covering of space by spheres*, Canad. J. Math. 8 (1956), pp. 293–304.
[3] L. Few, *Covering space by spheres*, Mathematika 3 (1956), pp. 136–139.

Received on 20. 3. 1970

ACTA ARITHMETICA
XVIII (1971)

Euclid's algorithm in algebraic function fields, II

by

J. V. Armitage (London)

In memory of Harold Davenpor

1. Introduction. The theorem that there are only a finite number of Euclidean algebraic number fields with one fundamental unit is a corollary of Davenport's work on the inhomogeneous minima of certain quadratic, cubic and quartic forms ([6], [7], [8]).

In [1], I imitated his arguments and obtained analogues of his theorems for the case of function fields of transcendence degree 1 over finite constant fields. Subsequently, I reformulated the question of the existence of a Euclidean algorithm, in function fields over arbitrary constant fields, in terms of the Riemann–Roch Theorem, [2]. The reformulation led to the solution of the problem (with no restriction on the units) for fields of genus 0 over arbitrary constant fields and later, [3](1), for fields of genus > 0 over infinite constant fields. In this paper, I show that there are only a finite number (in a sense which is made precise in § 3) of function fields, of given genus, over finite constant fields in which Euclid's algorithm holds.

The statement of the main theorem is given in § 3, after the notation has been established in § 2. It is both appropriate and convenient to express part of the argument in the language of the geometry of numbers and the necessary vocabulary is set out in § 4, together with an outline of the proof. The preliminary lemmas are proved in § 5 and the proof of the theorem is completed in § 6.

The results proved below are expressed in terms of the Euclidean algorithm problem, though they can be extended to the case of the inhomogeneous minima of certain forms. The methods are the same as those used here. One replaces a $k[x]$-basis of the ring I defined in § 2 by a set of linear forms with coefficients in the field $k\{x\}$ defined in (17).

(1) There is a mis-print in the displayed formula on p. 5 of the Appendix. The first part should read $\nu_{\mathfrak{p}_1}(\lambda_2^{(1)}-\lambda_1^{(1)}) > \nu_{\mathfrak{p}_1}(\lambda_1^{(1)})$.

The determinant of these forms provides the 'genus' condition (6) and one uses the version of the Riemann–Roch Theorem given in [4].

The problem discussed here involves non-convex regions and, to that extent at least, has some similarity with an interpretation of the Riemann Hypothesis for curves in terms of the product of linear forms([2]). Davenport's work on the product of three linear forms led to major developments in the classical geometry of numbers and it may be that rich rewards would attend similar progress in this field.

Finally, it may be possible to use the ideas of this paper to throw some light on the number field case. Indeed, such a hope partly inspired this most recent work. So far, I have not succeeded, but I hope to be able to return to the question in the future.

2. Recollection of notation and earlier results. Let k be a finite field and let K be a finite algebraic extension, of degree n and genus g, of the transcendental field $k(x)$. Let $\mathfrak{p}$ be the place of $k(x)$ corresponding to x^{-1} (the infinite place) and denote by S the set $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_h\}$ of places of K which lie above $\mathfrak{p}$. We suppose, without loss of generality, that $\deg\mathfrak{P}_1 \leqslant \ldots \leqslant \deg\mathfrak{P}_h$.

Let I denote the ring of S-integers of K. Thus I may be regarded as the integral closure of $k[x]$ in K, or as the intersection of the local rings of the places at finite distance.

If $\mathfrak{b}$ is a divisor of K based on S,

$$\mathfrak{b} = \mathfrak{P}_1^{\nu_1(\mathfrak{b})} \ldots \mathfrak{P}_h^{\nu_h(\mathfrak{b})} \tag{1}$$

where ν_i denotes the order function at $\mathfrak{P}_i$, then, following Chevalley [5], we define

$$L(\mathfrak{b}, S) = \{\beta \in K \mid \nu_i(\beta) \geqslant \nu_i(\mathfrak{b}),\ \mathfrak{P}_i \in S\}. \tag{2}$$

It was shown in [2] that I is Euclidean if and only if

$$K = \bigcup L(\mathfrak{b}, S) + I \tag{3}$$

where the union is taken over all divisors $\mathfrak{b}$ based on S such that

$$\deg\mathfrak{b} = \sum_{i=1}^{h} \nu_i(\mathfrak{b}) \deg\mathfrak{P}_i \geqslant 1. \tag{4}$$

Moreover, for any divisor $\mathfrak{a}$ based on S, we have

$$\dim_k K/\big(L(\mathfrak{b}, S) + I\big) = \delta(\mathfrak{a}^{-1}) \tag{5}$$

where $\delta(\mathfrak{a}^{-1})$ is the dimension of the space of differentials $\equiv 0 \pmod{\mathfrak{a}^{-1}}$.

([2]) See my lecture, to be reproduced in the Proceedings of the Bordeaux Number Theory Conference, 1969 and published in an Appendix to Bull. Soc. Math. de France.

3. Statement of the main theorem.

THEOREM. *There exists a constant $c = c(K, S)$, depending only on g and $\deg\mathfrak{P}_1, \ldots, \deg\mathfrak{P}_h$, such that if $q = \mathrm{Card}(k) > c$, then I is Euclidean if and only if*

$$g + d = 1. \tag{6}$$

It follows that, for a given g and a fixed rational function field $k(x)$, there are only a finite number of extensions $K/k(x)$ whose rings of integers are Euclidean.

No attempt is made to obtain the precise value of c, though it could be done. For example, in a 'totally real cubic field' $(n = h = 3)$, $c = (2g+1)(g+1)+1$. In general, c involves sums of the coefficients in the expansion of

$$(1-t^{\deg\mathfrak{P}_1})^{-1} \ldots (1-t^{\deg\mathfrak{P}_h})^{-1}. \tag{7}$$

Now the ideal-class number h_S of the ring I is given by

$$h_S = r(K, S) L_S(1) \tag{8}$$

where $r(K, S)$ depends on K and S (it is essentially the regulator) and

$$(1-u^{\deg\mathfrak{P}_1}) \ldots (1-u^{\deg\mathfrak{P}_h}) L_S(u) = (1-u)(1-qu) Z(u). \tag{9}$$

Here, $Z(u)$ is the zeta function of the field K (or of the associated curve). The condition on q and the relation between (7) and (9) suggest that one might be able to prove that $h_S > 1$ if q is large enough, but so far I have not been able to make significant progress on those lines.

4. Geometrical language and outline of the proof. The sufficiency part of the theorem has already been proved in [2]. So we may, and we shall, suppose that $g > 1$.

Write

$$d = \text{g.c.d.}(\deg\mathfrak{P}_1, \ldots, \deg\mathfrak{P}_h), \qquad m = \text{l.c.m.}(\deg\mathfrak{P}_1, \ldots, \deg\mathfrak{P}_h) \tag{10}$$

and let a be the integer defined by $(a-1)d < 2g-1 \leqslant ad$. Let $\mathfrak{a}_0$ be a fixed divisor based on S of degree $-ad$ and write $\nu_i(\mathfrak{a}_0) = a_i$. Thus

$$a_1 \deg\mathfrak{P}_1 + \ldots + a_h \deg\mathfrak{P}_h = -ad \leqslant -2g+1. \tag{11}$$

It follows from (5) and the fact that $\deg\mathfrak{a}_0^{-1} \geqslant 2g-1$, that

$$\dim_k K/\big(L(\mathfrak{a}_0, S) + I\big) = 0. \tag{12}$$

So the neighbourhood $L(\mathfrak{a}_0, S)$ when translated along the integer lattice I covers K.

We regard K as being embedded in the locally compact space $\hat{E} = \hat{K}_1 \times \ldots \times \hat{K}_h$, where K_i denotes the completion of K at $\mathfrak{P}_i$ with respect to the valuation

$$(13)\qquad |\alpha|_{\mathfrak{P}_i} = q^{-\nu_i(\alpha)}, \quad \alpha \in K.$$

We denote elements of $\hat{E}$ by $\mathfrak{x}$ and we write

$$(14)\qquad \hat{L}(\mathfrak{a}, S) = \Big\{\mathfrak{x} \in \prod_{1\leqslant i\leqslant h} \hat{K}_i \mid \nu_i(\mathfrak{x}) \geqslant \nu_i(\mathfrak{a})\Big\}.$$

Evidently

$$(15)\qquad L(\mathfrak{a}, S) = K \cap \hat{L}(\mathfrak{a}, S)$$

and we write

$$(16)\qquad L(\mathfrak{a}) = I \cap L(\mathfrak{a}, S).$$

Let $k\{x\}$ denote the completion of $k(x)$ with respect to the valuation

$$(17)\qquad \left|\frac{a}{b}\right| = q^{\deg a - \deg b} = q^{-\nu_\infty(a/b)}, \quad a, b \in k[x].$$

Then there is a $k\{x\}$-linear isomorphism(3)

$$(18)\qquad \eta:\ \hat{E} = \prod_{1\leqslant i\leqslant h} \hat{K}_i \to k\{x\}^n = P_n.$$

The space P_n is a locally compact, ultrametric space with respect to the distance

$$(19)\qquad \|\boldsymbol{x}\| = \max(|x_1|, \ldots, |x_n|), \quad \boldsymbol{x} \in P_n.$$

In the isomorphism (18), the space $L(\mathfrak{a}, S)$ corresponds to a convex body $C(\mathfrak{a})$ of volume $V\big(C(\mathfrak{a})\big) = q^{-\deg \mathfrak{a}}$ (cf. [4], Lemma 1, p. 388). The notion of volume in P_n can be extended to non-convex regions and we shall suppose that done in the sequel(4); we denote the volume of the region R by $V(R)$.

We can now outline the proof of the theorem.

By (12), the condition (3) may be replaced by

$$(20)\qquad L(\mathfrak{a}_0, S) \subseteq \bigcup_{\deg \mathfrak{b}\geqslant 1} L(\mathfrak{b}, S) + I.$$

It follows from the approximation theorem (see Chevalley, op. cit., p. 11, Theorem 3) and the fact that $\hat{E}$ is locally compact, that (20) holds if and only if

$$(21)\qquad \hat{L}(\mathfrak{a}_0, S) \subseteq \bigcup_{\deg \mathfrak{b}\geqslant 1} \hat{L}(\mathfrak{b}, S) + I.$$

---

(3) The details of the computation are given in [4], (21). The reader who is prepared to argue by analogy with algebraic number theory may think in terms of imbedding a number field in $\boldsymbol{R}^n$ via r real infinite primes and s complex ones.

(4) The volume is analogous to Jordan measure. Its essential properties are consequences of general theorems on Haar measure. An elementary discussion, with proofs of all results used here and in [4], is given in the author's London Ph. D. dissertation, 1956, unpublished.

Using the isomorphism η, this is equivalent to

$$(22)\qquad C_0 \subseteq \bigcup_{\deg \mathfrak{b}\geqslant 1} C(\mathfrak{b}) + \eta(I),$$

where $C(\mathfrak{b}) = \eta\big(L(\mathfrak{b}, S)\big)$, $C_0 = \eta\big(L(\mathfrak{a}_0, S)\big)$.

We now introduce an indexing set for the divisors $\mathfrak{a}$ which divide $\mathfrak{a}_0$. Let $t = (t_1, \ldots, t_h) \in \boldsymbol{Z}^h$, with $t_1 \geqslant 0, \ldots, t_h \geqslant 0$, and define

$$(23)\qquad \mathfrak{a}_t = \mathfrak{a}(t_1, \ldots, t_h) = \mathfrak{P}_1^{a_1 - t_1} \ldots \mathfrak{P}_h^{a_h - t_h}.$$

For a given t, we define

$$(24)\qquad \mathscr{B}_t = \bigcup \hat{L}(\mathfrak{b}, S)$$

where the union is taken over all divisors $\mathfrak{b}$ based on S, with $\deg \mathfrak{b} \geqslant 1$, and such that $\nu_i(\mathfrak{b}) = a_i - t_i$ if $t_i > 0$ and $\nu_i(\mathfrak{b}) \geqslant a_i$ otherwise.

Clearly, (21) may be replaced by

$$(25)\qquad \hat{L}(\mathfrak{a}_0, S) \subseteq \bigcup_t \mathscr{B}_t + I.$$

Starting from the hypothesis $g + d > 1$, we shall construct a family, $\mathscr{C}$, of cosets of linear spaces in $\hat{L}(\mathfrak{a}_0, S)$, which have no point in common with any of the cosets $\hat{L}(\mathfrak{b}, S) + \xi$, $\mathfrak{a}_0 | \mathfrak{b}$ and $\xi \in L(\mathfrak{a}_0)$.

Now, if a covering of the kind (25) exists, it must be equivalent to a finite subcovering, since $\hat{L}(\mathfrak{a}_0, S)$ is compact and the sets $\hat{L}(\mathfrak{b}, S)$ are open. Hence, there exists $s \in \boldsymbol{Z}^h$ and a corresponding $\mathfrak{a}_s$, defined as in (23), such that

$$(26)\qquad \hat{L}(\mathfrak{a}_0, S) + L(\mathfrak{a}_s) \subseteq \bigcup \hat{L}(\mathfrak{b}, S) + L(\mathfrak{a}_s),$$

where the union is taken over all divisors $\mathfrak{b}$ with $\deg \mathfrak{b} \geqslant 1$ and $\mathfrak{a}_s | \mathfrak{b}$. In particular we must have

$$(27)\qquad \mathscr{C} + L(\mathfrak{a}_s) \subseteq \bigcup \hat{L}(\mathfrak{b}, S) + L(\mathfrak{a}_s)$$

where the union is taken over all $L(\mathfrak{b}, S) \in \mathscr{B}_t$, with $t \neq (0, \ldots, 0)$.

So, in order to show that (25) cannot hold, it suffices to prove that

$$V\big(\eta\mathscr{C} + L(\mathfrak{a}_s)\big) \cap \Big(\eta\big(\bigcup \hat{L}(\mathfrak{b}, S) + L(\mathfrak{a}_s)\big)\Big) < V\Big(\eta\big(\mathscr{C} + L(\mathfrak{a}_s)\big)\Big).$$

It follows from Lemmas 3, 4 and 5, below, that this last is equivalent to

$$(28)\qquad \sum_{\mathfrak{b}} V\big(\eta\mathscr{C} \cap \eta\hat{L}(\mathfrak{b}, S)\big) < V(\eta\mathscr{C})$$

where the sum is taken over all divisors $\mathfrak{b}$ as in (27). Indeed, we shall show in Lemma 5 that, if $q > c_1$, then $V(\eta\mathscr{C}) \geqslant 1$. So, in order to prove the theorem, it suffices to prove that

$$\sum V\big(\eta\hat{L}(\mathfrak{b}, S) \cap \eta\hat{L}(\mathfrak{a}_0, S)\big) < 1.$$

The details of this computation are given in § 6.

5. Preliminary lemmas.

LEMMA 1. *Let T be an integer $\geqslant 0$. Then*

$$\bigcup_{a+T\leqslant \deg\mathfrak{b}} L(\mathfrak{b}, S) = \bigcup_{d+T\leqslant \deg\mathfrak{b}\leqslant m+T} L(\mathfrak{b}, S). \tag{29}$$

The number of such divisors $\mathfrak{b}$ satisfying $d+T\leqslant \deg\mathfrak{b}\leqslant m+T$ and $\mathfrak{a}_0|\mathfrak{b}$ is equal to the number, $N(T)$, of solutions of

$$x_1\deg\mathfrak{P}_1+\ldots+x_h\deg\mathfrak{P}_h = (\mu+a)d+T, \qquad a\leqslant \mu d\leqslant m. \tag{30}$$

Proof. Suppose $\deg\mathfrak{b} > d+T+m$. Then we can find a divisor $\mathfrak{b}'$ such that $d+T\leqslant \deg\mathfrak{b}' < \deg\mathfrak{b}$ and $\mathfrak{b}'|\mathfrak{b}$. Clearly,

$$\bigcup_{d+T\leqslant\deg\mathfrak{b}} \hat{L}(\mathfrak{b}, S) = \bigcup_{d+T\leqslant\deg\mathfrak{b}\leqslant d+T+m} \hat{L}(\mathfrak{b}', S).$$

If $\mathfrak{a}_0|\mathfrak{b}$ (that is, if $\nu_i(\mathfrak{b})\geqslant\nu_i(\mathfrak{a}_0)$, $1\leqslant i\leqslant h$) then

$$\mathfrak{b} = \mathfrak{P}_1^{x_1+a_1}\ldots\mathfrak{P}_h^{x_h+a_h}$$

where

$$x_1\deg\mathfrak{P}_1+\ldots+x_h\deg\mathfrak{P}_h = \mu d+T-\deg\mathfrak{a}_0 = (\mu+a)d+T.$$

But $d+T = \deg\mathfrak{b}$ and $x_1\geqslant 0, \ldots, x_h\geqslant 0$. Thus the number of such divisors is $N(T)$.

LEMMA 2. *Let $\mathfrak{a}_t$ be a divisor of the type introduced in* (23) *and write $T = t_1\deg\mathfrak{P}_1+\ldots+t_h\deg\mathfrak{P}_h$. Let $\mathscr{B}_t$ denote the union of linear spaces defined in* (24). *Then*

$$\hat{L}(\mathfrak{a}_0, S)\cap\mathscr{B}_t = \bigcup\hat{L}(\mathfrak{b}, S) \tag{31}$$

where the union on the right-hand side is taken over all divisors $\mathfrak{b}$ such that $d+T\leqslant\deg\mathfrak{b}\leqslant d+T+M$ and $\nu_i(\mathfrak{b}) = a_i$ at places where $t_i>0$.

Proof. Let $\mathfrak{b}'$ be a divisor contributing to (24). Consider the divisor $\mathfrak{b}$ such that $\nu_i(\mathfrak{b}) = \nu_i(\mathfrak{b}')$ if $\nu_i(\mathfrak{b}')\geqslant a_i$ and $\nu_i(\mathfrak{b}) = a_i$ if $\nu_i(\mathfrak{b}')<a_i$. Then, in the notation of (23) and (24)

$$\deg\mathfrak{b} = \deg\mathfrak{b}'+t_1\deg\mathfrak{P}_1+\ldots+t_h\deg\mathfrak{P}_h = \deg\mathfrak{b}'+T.$$

Obviously,

$$\hat{L}(\mathfrak{a}_0, S)\cap\hat{L}(\mathfrak{b}', S) = \hat{L}(\mathfrak{b}, S)$$

and the desired result now follows from Lemma 1.

LEMMA 3. *Let $\xi, \xi'\in I$. Then if the intersections are non-empty,*

$$\begin{aligned} V\big(\eta\hat{L}(\mathfrak{a}_0, S)\cap\eta\hat{L}(\mathfrak{b}, S)\big) &= V\Big(\eta\hat{L}(\mathfrak{a}_0, S)\cap\eta\big(\hat{L}(\mathfrak{b}, S)+\xi\big)\Big) \\ &= V\Big(\eta\big(\hat{L}(\mathfrak{a}_0, S)+\xi'\big)\cap\eta\big(\hat{L}(\mathfrak{b}, S)+\xi+\xi'\big)\Big). \end{aligned}$$

Proof. The notion of volume referred to above is the analogue of Jordan measure. It is additive and invariant under translations and those are the properties which we use.

Choose $\alpha\in\big(\hat{L}(\mathfrak{b}, S)+\xi\big)\cap\hat{L}(\mathfrak{a}_0, S)$. Then if $\beta\in\hat{L}(\mathfrak{b}, S)\cap\hat{L}(\mathfrak{a}_0, S)$,

$$\alpha+\beta\in\big(\hat{L}(\mathfrak{b}, S)+\xi\big)\cap\hat{L}(\mathfrak{a}_0, S).$$

So

$$V\Big(\eta\hat{L}(\mathfrak{a}_0, S)\cap\eta\big(\hat{L}(\mathfrak{b}, S)+\xi\big)\Big) = V\big(\eta\hat{L}(\mathfrak{a}_0, S)\cap\eta\hat{L}(\mathfrak{b}, S)\big),$$

since the volume is invariant under translation.

Again,

$$V\Big(\eta\big(\hat{L}(\mathfrak{a}_0, S)+\xi'\big)\cap\eta\big(\hat{L}(\mathfrak{b}, S)+\xi+\xi'\big)\Big) = V\big(\eta\hat{L}(\mathfrak{a}_0, S)\cap\eta\hat{L}(\mathfrak{b}, S)\big),$$

and so the lemma is proved.

LEMMA 4. *Let $g\geqslant 1$ and write $G = ad+1-g\geqslant g$* (cf. (10)). *Let*

$$M = q^{-G}\left(1-\frac{1}{q}\right)^h\prod_{1\leqslant i\leqslant h} q^{\deg\mathfrak{P}_i+(\deg\mathfrak{P}_i-1)[G/\deg\mathfrak{P}_i]}(q-N_{i,1}-1)\times \times\prod_{2\leqslant j\leqslant[G/\deg\mathfrak{P}_i]}(q-N_{i,j}), \tag{32}$$

where, for given i, $N_{i,j}$ denotes the number of solutions of

$$\begin{gathered} x_1\deg\mathfrak{P}_1+\ldots+x_{i-1}\deg\mathfrak{P}_{i-1}\leqslant G, \\ x_1\deg\mathfrak{P}_1+\ldots+x_{i-1}\deg\mathfrak{P}_{i-1}+j\deg\mathfrak{P}_i > G, \end{gathered} \tag{33}$$

subject to the condition $1\leqslant j\leqslant[G/\deg\mathfrak{P}_i]$ (the integer part of $G/\deg\mathfrak{P}_i$).

Then, there exist M elements $\mathfrak{x}^{(j)}$ $(1\leqslant j\leqslant M)$ in $\hat{L}(\mathfrak{a}_0, S)$ such that:

(a) *For all $\xi\in L(\mathfrak{a}_0)$,*

$$\nu_i(\mathfrak{x}_i^{(j)}-\xi)\leqslant\nu_i(\mathfrak{a}_0)+[G/\deg\mathfrak{P}_i], \qquad 1\leqslant i\leqslant h. \tag{34}$$

(b) *For all $\xi\in L(\mathfrak{a}_0)$,*

$$\sum_{1\leqslant i\leqslant h}\nu_i(\mathfrak{x}_i^{(j)}-\xi)\deg\mathfrak{P}_i\leqslant 0. \tag{35}$$

(c) *For all r, s with $1\leqslant r, s\leqslant M$,*

$$\mathfrak{x}^{(r)}-\mathfrak{x}^{(s)}\notin I. \tag{36}$$

Proof. It follows from the Riemann–Roch Theorem that there are exactly G k-independent points of I in $L(\mathfrak{a}_0, S)$; we denote them by $\xi^{(1)}, \ldots, \xi^{(G)}$. For $\xi^{(l)}$, considered as an element of $\hat{K}_i$, write

$$\xi^{(l)} = \sum_r c_{i,r}^{(l)}\pi_i^r, \qquad r\geqslant a_i,\ 1\leqslant l\leqslant G,\ 1\leqslant i\leqslant h, \tag{37}$$

where π_i is a prime element at $\mathfrak{P}_i$ and the $c_{i,r}$ are elements of the residue field at $\mathfrak{P}_i$, possibly 0. Any element of $L(\mathfrak{a}_0)$, considered as an element of $\hat{K}_i$, may accordingly be written in the form

$$\sum_l \sum_r \lambda_l c_{i,r}^{(l)} \pi_i^r, \qquad \lambda_l \in k,\ r \geqslant a_i,\ 1 \leqslant l \leqslant G. \tag{38}$$

We now construct $\mathfrak{x}^{(j)} \in \hat{L}(\mathfrak{a}_0, S)$, $1 \leqslant j \leqslant M$, by considering the local expansions at $\mathfrak{P}_i$ and choosing the coefficients so as to ensure that the conditions of the lemma are satisfied.

We write the ith component $\mathfrak{x}_i^{(j)}$ of $\mathfrak{x}^{(j)}$ in the form

$$\mathfrak{x}_i^{(j)} = \sum_r d_{i,r}\pi_i^r, \qquad a_i \leqslant r \leqslant a_i + [G/\deg\mathfrak{P}_i], \tag{39}$$

and we consider systems of equations of the form

$$\lambda_1 c_{i,r}^{(1)} + \ldots + \lambda_G c_{i,r}^{(G)} = d_{i,r}, \qquad \lambda_l \in k. \tag{40}$$

Each of these equations may be thought of as $\deg\mathfrak{P}_i$ equations with coefficients in k.

In order to satisfy condition (a) we may lose not more than $[G/\deg\mathfrak{P}_i]$ exponents at $\mathfrak{P}_i$. In order to satisfy (b) it is sufficient to ensure that $d_{i,a_i} \neq 0$ and that if x_i exponents are lost at $\mathfrak{P}_i$, then

$$x_1 \deg\mathfrak{P}_1 + \ldots + x_h \deg\mathfrak{P}_h \leqslant G.$$

For then,

$$\sum_{1\leqslant i\leqslant h} \nu_i(\mathfrak{x}_i^{(j)} - \xi)\deg\mathfrak{P}_i = \sum_{1\leqslant i\leqslant h} a_i + G = -ad + G = 1 - g \leqslant 0.$$

By starting at $\mathfrak{P}_1$ and working with $\mathfrak{P}_2, \mathfrak{P}_3$, etc., successively, it is now straightforward, although tedious, to verify that the number of such choices is $q^G M$, where M is defined by (32).

In order to satisfy condition (c), it suffices to observe that to each of the $\mathfrak{x}^{(j)}$ just constructed, there correspond q^G points $\mathfrak{x}^{(j)} + \xi$, $\xi \in L(\mathfrak{a}_0)$. But the difference of any two $\mathfrak{x}^{(r)} - \mathfrak{x}^{(s)}$ must lie in $L(\mathfrak{a}_0)$ and so, a fortiori, there are at most q^G distinct $\mathfrak{x}^{(j)} + \xi$ in $L(\mathfrak{a}_0)$, with $\xi \in I$.

Hence there are M points $\mathfrak{x}$ satisfying (a), (b) and (c).

LEMMA 5. *With the assumptions of Lemma 4, let $\mathfrak{x}$ be one of the M points constructed and let $\mathscr{C}$ be the family of cosets defined by*

$$\nu_i(\mathfrak{x} - \mathfrak{x}^{(j)}) \geqslant a_i + [G/\deg\mathfrak{P}_i] + 1, \qquad 1 \leqslant j \leqslant M. \tag{41}$$

Then:

(a) *No two members of the family $\mathscr{C} + I$ overlap.*

(b) *If $\nu_i(\mathfrak{x} - \mathfrak{x}^{(j)}) \geqslant a_i + [G/\deg\mathfrak{P}_i] + 1$, then for all $\xi \in L(\mathfrak{a}_0)$,*

$$\sum_{1\leqslant i\leqslant h} \nu_i(\mathfrak{x} - \xi)\deg\mathfrak{P}_i \leqslant 0. \tag{42}$$

(c) *In the space P_n the volume of $\eta\mathscr{C}$ satisfies*

$$V(\eta\mathscr{C}) > q^{G-1}\left(1 - \frac{1}{q}\right)^h \prod_{1\leqslant i\leqslant h}\left\{\prod_{1\leqslant j\leqslant[G/\deg\mathfrak{P}_i]}\left(1 - \frac{N_{i,j}+1}{q}\right)\right\}. \tag{43}$$

(d) *There exists a constant $c_1(K, S)$ such that if $q > c_1$, then $V(\eta\mathscr{C}) \geqslant 1$.*

Proof. (a). Suppose there exists $\mathfrak{x} \in \hat{L}(\mathfrak{a}_0, S)$ such that

$$\nu_i(\mathfrak{x} - \mathfrak{x}^{(r)}) \geqslant a_i + [G/\deg\mathfrak{P}_i] + 1$$

and for some $\xi \in L(\mathfrak{a}_0)$

$$\nu_i(\mathfrak{x} - \mathfrak{x}^{(s)} - \xi) \geqslant a_i + [G/\deg\mathfrak{P}_i] + 1.$$

Then

$$\nu_i(\mathfrak{x}^{(r)} - \mathfrak{x}^{(s)} + \xi) \geqslant a_i + [G/\deg\mathfrak{P}_i] + 1.$$

Now it follows from (39) that $\mathfrak{x}^{(r)} - \mathfrak{x}^{(s)} \in I$, a contradiction to Lemma 4 (c).

(b) We have

$$\sum_{1\leqslant i\leqslant h} \nu_i(\mathfrak{x} - \xi)\deg\mathfrak{P}_i = \sum_{1\leqslant i\leqslant h} \nu_i\big((\mathfrak{x} - \mathfrak{x}^{(j)}) + (\mathfrak{x}^{(j)} - \xi)\big)\deg\mathfrak{P}_i$$
$$= \sum_{1\leqslant i\leqslant h} \nu_i(\mathfrak{x}^{(j)} - \xi)\deg\mathfrak{P}_i \leqslant 0,$$

by (41) and Lemma 4 (b).

(c). Since the bodies do not overlap and the volume is additive, we have

$$V(\eta\mathscr{C}) = M \prod_{1\leqslant i\leqslant h} q^{-(a_i + [G/\deg\mathfrak{P}_i] + 1)\deg\mathfrak{P}_i}$$
$$= q^{G-1}\left(1 - \frac{1}{q}\right)^h \prod_{1\leqslant i\leqslant h}\left(1 - \frac{N_{i,1}+1}{q}\right) \prod_{2\leqslant j\leqslant[G/\deg\mathfrak{P}_i]}\left(1 - \frac{N_{i,j}}{q}\right)$$
$$> q^{G-1}\left(1 - \frac{1}{q}\right)^h \prod_{1\leqslant i\leqslant h}\left\{\prod_{1\leqslant j\leqslant[G/\deg\mathfrak{P}_i]}\left(1 - \frac{N_{i,j}+1}{q}\right)\right\}.$$

(d) Choose $q > c_1$ in order that

$$\left(1 - \frac{1}{q}\right)^h \prod_{1\leqslant i\leqslant h}\left\{\prod_{1\leqslant j\leqslant[G/\deg\mathfrak{P}_i]}\left(1 - \frac{N_{i,j}+1}{q}\right)\right\} \geqslant \frac{1}{q},$$

(for example, take $c_1 = \max\big(2^{2h}, 2(N_{i,j}+1)\big)$). Then, for $G > 1$, (d) holds. The case $G = 1$ occurs if and only if $g = 1$ and $d = 1$. If $\deg\mathfrak{P}_1 = \ldots = \deg\mathfrak{P}_h = 1$, then by a modification of the argument used in the proof of Lemma 4 we see that the exponent q^{G-1} in (c) may be replaced by q^G.

A similar observation is true if at least one of $\deg\mathfrak{P}_i > 1$. This completes the proof of (d).

6. Proof of the theorem. As already remarked in § 4, the cases $g+d = 1$ and $g = 0$, $d \geqslant 2$ have already been dealt with; so we are left with the cases in which $g \geqslant 1$.

We refer to the outline of the proof given in § 4. We take the family $\mathscr{C}$ to be that constructed in Lemmas 4 and 5 and we note that, by Lemma 5 (d), $V(\eta\mathscr{C}) \geqslant 1$, provided that $q > c_1(K, S)$. Consequently, in order to complete the proof of the theorem, it suffices to prove that if $q > \max(c_1, c_2)$, where the constant c_2 is defined below, after (46), then

$$\sum_{\mathfrak{b}} V\big(\eta\hat{L}(\mathfrak{b}, S) \cap \eta\hat{L}(\mathfrak{a}_0, S)\big) < 1,$$

where $\bigcup \hat{L}(\mathfrak{b}, S)$ is defined in (26). (Cf. (28).)

Let $t = (t_1, \ldots, t_h)$ be a vector $0 \leqslant t_1 \leqslant s_1, \ldots, 0 \leqslant t_h \leqslant s_h$, and let $\mathscr{B}_t$ be the family of spaces defined by (24). To fix ideas, suppose that $t_i \neq 0$, $1 \leqslant i \leqslant r \leqslant h$. Then it follows from Lemmas 1 and 2, that

$$(43)\qquad \sum_{\mathfrak{b}} V\big(\eta\hat{L}(\mathfrak{b}, S) \cap \eta\hat{L}(\mathfrak{a}_0, S)\big) \leqslant N(t_1\deg\mathfrak{P}_1+\ldots+t_r\deg\mathfrak{P}_r)\, q^{-d-(t_1\deg\mathfrak{P}_1+\ldots+t_r\deg\mathfrak{P}_r)}, \qquad \hat{L}(\mathfrak{b}, S) \in \mathscr{B}_t,$$

where $N(t_1\deg\mathfrak{P}_1+\ldots+t_r\deg\mathfrak{P}_r)$ is the number of solutions of the equations

$$a_1\deg\mathfrak{P}_1+\ldots+a_r\deg\mathfrak{P}_r+x_{r+1}\deg\mathfrak{P}_{r+1}+\ldots+x_h\deg\mathfrak{P}_h = (\mu+a)\,d+\sum_{1\leqslant i\leqslant h} t_i\deg\mathfrak{P}_i,$$

with $x_{r+1} \geqslant 0, \ldots, x_h \geqslant 0$ and $d \leqslant \mu d \leqslant m$. Hence, for vectors t in which there are exactly r non-zero components t_i,

$$(44)\qquad \sum_{t\geqslant 0}\sum_{\mathfrak{b}} V\big(\eta\hat{L}(\mathfrak{b}, S) \cap \eta\hat{L}(\mathfrak{a}_0, S)\big) \leqslant q^{-d}\sum_{t} N(T)\, q^{-T}, \qquad \hat{L}(\mathfrak{b}, S) \in \mathscr{B}_t,$$

where T stands for the various expressions of the type $t_1\deg\mathfrak{P}_1+\ldots+$ $+t_r\deg\mathfrak{P}_r$.

Let us consider the right-hand side of (44) in the case when t has exactly one non-zero component. The contribution of such terms to the sum in (44) is

$$(45)\qquad q^{-d}\sum_{1\leqslant i\leqslant h}\sum_{1\leqslant t_i} N(t_i\deg\mathfrak{P}_i)\, q^{-t_i\deg\mathfrak{P}_i} \leqslant q^{-d}\sum_{1\leqslant i\leqslant h}\sum_{0\leqslant n} N\big((n+1)\deg\mathfrak{P}_i\big)\, q^{-n\deg\mathfrak{P}_i}.$$

For the number $N\big((n+1)\deg\mathfrak{P}_i\big)$ we have an estimate of the form

$$N\big((n+1)\deg\mathfrak{P}_i\big) \leqslant A_i(n)$$

where A_i is a polynomial of degree $h-2$ in n whose coefficients depend only on $\deg\mathfrak{P}_1, \ldots, \deg\mathfrak{P}_h$ (and which is, of course, related to (7)).

It follows that the series in (45) involving such t is dominated by a recurring series in q^{-1} whose scale of relation is $(1-q^{-1})^{h-1}$. Hence its sum is less than $D_i^{(1)}$, where $D_i^{(1)}$ is a rational function in q^{-1}, of degree 1, with coefficients depending only on $\deg\mathfrak{P}_1, \ldots, \deg\mathfrak{P}_h$.

Similarly, the more general sums, in which exactly r components in t have non-zero entries, are less than $D_{i_1,\ldots,i_r}^{(r)}$, where the D's are rational functions in q^{-1} of degree 1, with coefficients depending only on the degrees of the places in S.

Hence

$$(46)\qquad \sum_{\mathfrak{a}_S|\mathfrak{b}} V\big(\eta\hat{L}(\mathfrak{a}_0, S) \cap \eta\hat{L}(\mathfrak{b}, S)\big) < q^{-d}\Big(\sum_i D_i^{(1)} q^{-\deg\mathfrak{P}_i}+\sum_{i,j} D_{i,j}^{(2)} q^{-\deg\mathfrak{P}_i-\deg\mathfrak{P}_j}+\text{etc.}\Big).$$

Since $d \geqslant 1$, it follows from (46) that there exists a constant $c_2(S, K)$ (which can be determined in terms of the coefficients in the L-series (7)) such that, if $q > c_2(S, K)$, then the left-hand side is < 1. As already remarked, this proves the theorem.

7. Postlude on the case $h = 2$. The analogues of Davenport's theorems in the case $h = 2$ (that is, when there is just one fundamental unit of infinite order) may be derived easily from Lemma 4.

Since $\hat{E}$ is locally compact, there exists an $\mathfrak{a}_t$, with $\mathfrak{a}_0|\mathfrak{a}_t$, such that, if (3) holds, then

$$(47)\qquad L(\mathfrak{a}_t, S) \subseteq \bigcup L(\mathfrak{b}, S)+L(\mathfrak{a}_t).$$

As in the proof of Lemma 4, we now construct a badly approximable $\mathfrak{x}$, with

$$(48)\qquad G = \deg\mathfrak{a}_0+t_1\deg\mathfrak{P}_1+\ldots+t_h\deg\mathfrak{P}_h.$$

Note that such a construction is always possible, since $h = 2$. If $h > 2$, then the construction works only if $q > N_{3,t}$, which depends on t.

By the approximation theorem, there exists $a \in K$, such that $v_i(\mathfrak{x}-a)$ is arbitrarily large. Whence, by (35), with $\mathfrak{a}_t$ in place of $\mathfrak{a}_0$, we obtain a contradiction to (47).

References

[1] J. V. Armitage, *Euclid's algorithm in certain algebraic function fields*, Proc. London Math. Soc. (3) 7 (1957), pp. 498–509.

[2] — *Euclid's algorithm in algebraic function fields*, J. London Math. Soc. 38 (1963), pp. 55–59. *Addendum*, J. London Math. Soc. 43 (1968), pp. 171–172.

[3] — *On unique factorization in algebraic function fields*, Illinois J. Math. 11 (1967), pp. 280–283. *Appendix*, Illinois J. Math. 12 (1968), pp. 5–6.

[4] — *Algebraic functions and an analogue of the geometry of numbers: the Riemann-Roch theorem*, Archiv der Mathematik, 17 (1967), pp. 383–393.
[5] C. Chevalley, *Algebraic functions of one variable*, American Math. Soc. Surveys No. 6, New York 1951.
[6] H. Davenport, *Indefinite binary quadratic forms, and Euclid's algorithm in real quadratic fields*, Quart. J. of Math. (Oxford) (2) 1 (1950), pp. 54–62.
[7] — *Euclid's algorithm in cubic fields of negative discriminant*, Acta Mathematica 84 (1950), pp. 159–179.
[8] — *Euclid's algorithm in certain quartic fields*, Trans. Amer. Math. Soc. 68 (1950), pp. 508–532.

KING'S COLLEGE LONDON
London, England

Received on 25. 3. 1970

ACTA ARITHMETICA
XVIII (1971)

Cyclotomy and complementary difference sets

by

G. SZEKERES (Kensington, New South Wales)

In memory of H. Davenport

1. Let $(\boldsymbol{G}, +)$ be an additive abelian group of order n, $\boldsymbol{A}, \boldsymbol{B}, \ldots, \boldsymbol{C}$ k non-empty subsets of $\boldsymbol{G}$, each containing m elements. The sets $\boldsymbol{A}, \boldsymbol{B}, \ldots, \boldsymbol{C}$ are said to form a *k-ary difference system* in $\boldsymbol{G}$ if for each non-zero $\delta \in \boldsymbol{G}$ the total number of solutions of the k equations

$$(1)\qquad \begin{aligned} \delta &= \alpha_1 - \alpha_2, \quad \alpha_1, \alpha_2 \in \boldsymbol{A},\\ \delta &= \beta_1 - \beta_2, \quad \beta_1, \beta_2 \in \boldsymbol{B},\\ &\ldots\ldots\ldots\ldots\ldots\\ \delta &= \gamma_1 - \gamma_2, \quad \gamma_1, \gamma_2 \in \boldsymbol{C} \end{aligned}$$

is the same number N, independent of δ. Clearly we must have

$$(2)\qquad (n-1)N = km(m-1).$$

For instance, if $\boldsymbol{G}$ is the group of residues mod 5 then $\boldsymbol{A} = \{0, 1\}$, $\boldsymbol{B} = \{0, 2\}$ is a binary difference system, with $N = 1$. The number of solutions of the individual equations (1) is of no interest, only the total number of solutions of all k equations. Ordinary difference sets correspond to the case $k = 1$.

Of particular interest are binary difference sets $\boldsymbol{A}, \boldsymbol{B}$ in a group $\boldsymbol{G}$ of order $n = 2m+1$; in this case we say that $\boldsymbol{A}, \boldsymbol{B}$ are *complementary difference sets*, provided that at least one of the sets, say $\boldsymbol{A}$, has the property that

$$(3)\qquad \alpha \in \boldsymbol{A} \Rightarrow -\alpha \notin \boldsymbol{A}.$$

The number of solutions of (1) in a complementary difference system is $N = m-1$. Interest in complementary difference sets stems from the fact that if they exist in some $\boldsymbol{G}$ of order $2m+1$, then there also exists a skew Hadamard matrix of order $4(m+1)$ (see [5], Theorem 2).