COLLOQUIA MATHEMATICA
SOCIETATIS JÁNOS BOLYAI, 51

NUMBER THEORY

Vol. II.

Diophantine and Algebraic

Edited by

K. GYŐRY and G. HALÁSZ

NORTH-HOLLAND

COLLOQUIA MATHEMATICA
SOCIETATIS JÁNOS BOLYAI, 51

NUMBER THEORY

Vol. II.

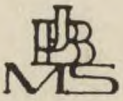
Diophantine and Algebraic

Edited by

K. GYŐRY and G. HALÁSZ

NORTH-HOLLAND PUBLISHING COMPANY
AMSTERDAM - OXFORD - NEW YORK

Budapest, Hungary, 1990



ISBN North-Holland: 0444 70476 0 VOL. I. – II.
0444 70475 2 VOL. II.

ISBN Bolyai: 963 8022 42 6 VOL. I. – II.
963 8022 46 9 VOL. II.

ISSN Bolyai: 0 139 3383

Joint edition published by

JÁNOS BOLYAI MATHEMATICAL SOCIETY

and

ELSEVIER SCIENCE PUBLISHERS B. V.

Saraburgerhartstraat 25, P. O. Box 103

1000 AC, Amsterdam, The Netherlands

In the U.S.A. and Canada:

ELSEVIER SCIENCE PUBLISHING COMPANY INC.

655 Avenue of Americas

New York, N. Y. 10010

U.S.A.

Assistant editor: A. BALOG and J. PINTZ

Printed in Hungary
Franklin Nyomda
Budapest

CONTENTS

Volume I.

Volume II.

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

WEAK HASSE PRINCIPLE FOR SYSTEMS OF BILINEAR FORMS

BAYER-FLUCKIGER E.*

INTRODUCTION

Let F be a field, and let V be a finite dimensional F-vector space. Let I be a set, and let $S = \{b_i\}$ where $b_i : V \times V \to F$ are F-bilinear forms for all i in I. The systems S and $S' = \{b'_i\}$ are said to be *isomorphic* if there exists an isomorphism $f : V \to V$ such that $b'_i(fx,fy) = b_i(x,y)$ for all x,y in V and for all i. If F is a *global field*, se say that the *weak Hasse principle* holds for a system S if every system S' of F-bilinear forms which becomes isomorphic to S over every completion of F is already isomorphic to S over F.

* Supported by the "Fonds national suisse de la recherche scientifique"

To every system S one associates a ring with involution R_S such that the norm-one-group of R_S is canonically identified with the group of isomorphisms of the system S. If F is a global field of characteristic $\neq 2$, the properties of R_S determine whether the weak Hasse principle holds for S (see Section 3). It is therefore useful to know which rings with involution arise in this way. Theorem 2.1 gives a necessary condition for this to be the case. The proof of this result is constructive, and is used in Section 4 to obtain counter-examples to the weak Hasse principle for systems of 3 quadratic forms (see also [1] and [2]), pairs of bilinear forms and systems of 6 alternating forms. Section 5 contains counter-examples to the weak Hasse principle for the similitude of systems of bilinear forms.

1. THE RING WITH INVOLUTION OF A SYSTEM OF BILINEAR FORMS

Let S be a system of bilinear forms, and set

$R_S = \{(f,g) \in End(V) \times End(V) \mid b(fx,y) = b(x,gy)$ and $b(x,fy) = b(gx,y)$ for all x,y in V and for all b in S$\}$.

We view R_S as a sub F-algebra of $End(V) \times End(V)^o$, so the multiplication is defined by $(f,g).(f',g') = (ff',g'g)$. Setting $(f,g)^* = (g,f)$ defines an F-linear involution of R_S.

The *norm-one-group* of a ring R with involution * is by definition $U(R) = \{r \in R \mid rr^* = 1\}$.

If f is an automorphism of S, then (f,f^{-1}) is in $U(R_S)$. Conversely, if $r = (f,g)$ is in $U(R_S)$ then $g = f^{-1}$ and f is an automorphism of S. Therefore we may *identify the group of automorphisms of the system* S *with the norm-one-group of* R_S.

This implies (cf. [2], (1.6)) that

1.1 PROPOSITION: *The group of automorphisms of a system of bilinear forms is an extension of a product of classical groups by a split unipotent group.* □

Let J be the radical of R_S, and set $\bar{R} = R_S/J$. Then $\bar{R} = R_1 \times \ldots \times R_r \times (R_{r+1} \times R_{r+1}^*) \times \ldots \times (R_k \times R_k^*)$, where the R_i's are simple F-algebras, $R_i^* = R_i$ if $i=1,\ldots,r$ and $R_j \neq R_j^*$ if $j=r+1,\ldots,k$. We have $R_i = M_{n_i}(D_i)$ for some skew field D_i.

Let R be a finite dimensional simple F-algebra. Recall that an involution $^*: R \to R$ is said to be of the *first kind* if the restriction of * to the center of R is the identity, and of the *second kind* otherwise. Let K be the center of R, and let n^2 be the dimension of R over K. Set $R^+ = \{r \in R \mid r^* = r\}$. Assume that * is of the first kind. Then the involution * is *called of orthogonal type if* $\dim_K(R^+) = \frac{1}{2} n(n+1)$, and of *symplectic type* if $\dim_K(R^+) = \frac{1}{2} n(n-1)$.

The set of skew fields $D_1,\ldots,D_r$ and the kind and

type of the involutions $*: R_i \to R_i$ are invariants of the system S. If F is a global field of characteristic $\neq 2$, then these invariants determine whether the weak Hasse principle holds for S (see (3.1)).

2. SYSTEMS OF BILINEAR FORMS HAVING A GIVEN RING WITH INVOLUTION

Let R be a finite dimensional F-algebra, and let $*: R \to R$ be an F-linear involution. Does there exist a system of F-bilinear forms S such that $R_S = R$? It will be useful to consider a stronger question, namely ask for a system of *symmetric* F-bilinear forms.

The algebra R is said to have *property* (P) if there exists an F-linear form $t : R \to F$ such that:

(a) $t(xy) = t(yx)$ for all x,y in R

(b) $t(x^*) = t(x)$ for all x in R

(c) the F-bilinear form $R \times R \to F$ defined by $(x,y) \mapsto t(xy)$ is non-degenerate.

For instance, this property is satisfied if char(F)=0 and R is semi-simple: one can then take t to be the trace of the regular representation of R.

2.1 THEOREM: *If* R *has property* (P), *then there exists a system of symmetric* F-*bilinear forms with algebra* R.

Let m be a positive integer and let $V = R^m$. Let S be

the set of all symmetric F-bilinear forms $b: V \times V \to F$ such that $b(rx,y) = b(x,r^*y)$ for all r in R and for all x,y in V. Then clearly R is contained in R_S. Moreover, we have:

2.2 LEMMA: *If* $m \geq 2$, *then* $R = R_S$.

PROOF: If $h : V \times V \to R$ is a hermitian form, then the F-bilinear form $b : V \times V \to F$ defined by $b(x,y) = t(h(x,y))$ belongs to S. Conversely, it is easy to check that all elements of S have this form : if b is in S, then there exists a hermitian form $h: V \times V \to R$ such that $b(x,y) = t(h(x,y))$ for all x and y in V.

Let $V' = \mathrm{Hom}_F(V,F)$ be the dual of V, and let $G: V \to V'$ be the isomorphism defined by $G(x)(y) = t(xy^*)$. If b is in S, denote by $B : V \to V'$ the adjoint homomorphism of b. It is easy to check that (f,g) is in R_S if and only if $f(G^{-1}B) = (G^{-1}B)f$ for all B as above, and $g = G^{-1}f'G$ where f' is the transpose of f. The above discussion shows that the endomorphisms of V of the form $G^{-1}B$ are exactly those given by $x \mapsto Ax$, where A is a hermitian mxm-matrix with entries in R.

Therefore the lemma is proved provided we show that the hermitian matrices generate the algebra $M_m(R)$. Let us prove this for m = 2 : the general case is similar. Let M be the subalgebra of $M_2(R)$ generated by the hermitian matrices.

Then

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & r^* \\ r & 0 \end{pmatrix}$$

are in M. Therefore so are

$$\begin{pmatrix} 0 & r \\ 0 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 0 \\ r & 0 \end{pmatrix}$$

By multiplying with $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, we get $\begin{pmatrix} r & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 0 & r \end{pmatrix}$

Therefore $M = M_2(R)$. □

2.3 REMARK: if $m = 1$, then R_S and R are not always equal. For instance, let R be a quaternion algebra with center F. The reduced trace $t : R \to F$ satisfies the conditions (a), (b) and (c). Let $R^+ = \{r \in R \mid r^* = r\}$. If * is the canonical involution of R (i.e. if * is of symplectic type) then $R^+ = F$, and S consists of the scalar multiples of $t(xy^*)$. In this case, $R_S = M_4(F)$. On the other hand, if * is a non canonical involution of R, then $\dim_F(R^+) = 3$ and $R_S = R$.

3. THE WEAK HASSE PRINCIPLE FOR SYSTEMS OF BILINEAR FORMS

Assume that F is a global field of characteristic $\neq 2$. We denote by F_v the completion of F at the place v. Let K be a finite extension of F, and let D be a quaternion field of center K. We say that D is *ramified*

at a place v of K if $D \otimes_K K_v$ is a skew field.

Let S be a system of F-bilinear forms. Recall that in Section 1 we have associated to S a finite number of skew fields $D_1,\ldots,D_r$ and involutions $*:R_i \to R_i$, $i=1,\ldots,r$.

3.1 THEOREM: *The following are equivalent:*

(i) The weak Hasse principle does not hold for S

(ii) There exists an index i $(1 \leq i \leq r)$ *such that* D_i *is a quaternion algebra on its center* K_i *which is ramified at least at 4 places of* K_i *and that the involution* $*: R_i \to R_i$ *is of the first kind and orthogonal type.*

This can be deduced from (1.1) and Kneser's results [3] as in [2], Section 2. □

4. COUNTER-EXAMPLES TO THE WEAK HASSE PRINCIPLE

4.1 Let us keep the notations of Section 3. Let a and b be two non-zero elements of F. Let us consider the following systems of F-bilinear forms:

Three quadratic forms

$$\begin{cases} X_1^2 - aX_2^2 + bX_3^2 - abX_4^2 \\ X_2X_3 - X_1X_4 \\ X_1X_3 - a\,X_2X_4 \end{cases}$$

Two bilinear forms

$$B_1 = \begin{pmatrix} 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & -a \\ 1 & 0 & 0 & b \\ 0 & -a & -b & 0 \end{pmatrix}$$

$$B_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -a & 0 & 0 \\ 0 & 0 & b & 0 \\ 0 & 0 & 0 & -ab \end{pmatrix}$$

Six alternating forms

Let $D = (a,b)$ be a quaternion algebra over F. Let i,j and k be elements of D such that $i^2 = a$, $j^2 = b$ and $k = ij = -ji$. Let $*: D \to D$ be the F-linear involution of D such that $i^* = -i$ and $j^* = j$. Set $V = D^2$, and let $h_r : V \times V \to D$ be the skew hermitian forms defined by the following matrices:

$$h_1 = \begin{pmatrix} i & 0 \\ 0 & 0 \end{pmatrix} \quad h_2 = \begin{pmatrix} 0 & 0 \\ 0 & i \end{pmatrix} \quad h_3 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

$$h_4 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad h_5 = \begin{pmatrix} 0 & ij \\ -ij & 0 \end{pmatrix} \quad h_6 = \begin{pmatrix} 0 & j \\ -j & 0 \end{pmatrix}$$

Let $t : D \to F$ be the reduced trace. Let $A_r : V \times V \to F$ be the F-bilinear form defined by $A_r(x,y) = t(h_r(x,y))$. It is easy to check that the A_r's are alternating.

4.2 If v is a valuation of F, let us denote by F_v the completion of F at v, and let $(\ ,\ )_v$ be the Hilbert symbol. Let T be the set places v of F such that $(a,b)_v = -1$.

If $S = \{b_1,\ldots,b_n\}$ is a system of bilinear forms and $\alpha \in F$, set $\alpha S = \{\alpha b_1,..,\alpha b_n\}$.

Let $\alpha \in F$ *such that* $(a,\alpha)_v = 1$ *for all* $v \notin T$. *Let* S *be one of the systems described in* (4.1). *Then* S and αS *are isomorphic over all completions of* F. *Moreover,* S *and* αS *are isomorphic over* F *if and only if* $(a,\alpha)_v = (a,\alpha)_w$ *for all* $v,w \in T$.

Let us prove this statement in a more general context:

4.3 Let S be a system of bilinear forms such that R_S is $(D,*)$.

The following are equivalent:

(i) S *and* α S *are isomorphic*

(ii) *There exists* $d \in D$ *such that* $dd^* = \alpha$.

This equivalence is easy to prove. Let us outline two methods of proof: One can associate an algebra with involution to the pair S, αS such that the isomorphisms between S and αS are identified with the elements of "norm" α of this algebra. Then one checks that this

algebra is $(D,*)$. Another proof can be obtained by noting that S and αS are isomorphic over $F(\sqrt{\alpha})$, and use Galois cohomology.

4.4 Let $E = F(i) = F(\sqrt{a})$, and let $N : E \to F$ be the norm. *Then* (ii) *is equivalent to*

(iii) $\alpha \in N(E)$ *or* $\alpha b \in N(E)$.

This follows from an argument of Springer, see [3] , p.149 or [4] , Chapter, 10, Lemma 3.4.

It is easy to deduce from (4.3) and (4.4) that (4.2) holds for any system S of bilinear forms with algebra $(D,*)$. It remains to check that this is the case for the systems of (4.1):

4.5 Let $V = D$, and let $D_1 = 1$, $d_2 = ij/ab$, $d_3 = j/b$. Let $Q_r : V \to F$ be the quadratic form defined by $Q_r(x) = t(xd_r x^*)$. By (2.3), the algebra with involution of the system $\{Q_1, Q_2, Q_3\}$ is $(D,*)$. A computation shows that this is the system of three quadratic forms described in (4.1).

Let $d_4 = i/a$, and let $B_r : V \times V \to F$ be the bilinear forms defined by $B_1(x,y) = \frac{1}{2}t(x(d_3+d_4)y^*)$, $B_2(x,y) = t(xy^*)$. Then B_1 and B_2 are the bilinear forms of (4.1). Again by (2.3), the associated algebra is $(D,*)$.

Finally, (2.2) implies that the algebra of the system $A_1, \ldots, A_6$ is also $(D,*)$.

5. A COUNTER-EXAMPLE TO THE WEAK HASSE PRINCIPLE FOR THE SIMILARITY OF SYSTEMS OF QUADRATIC FORMS

Two systems of bilinear forms S and S′ are said to be *similar* if there exists a non-zero element β of F such that S and βS are isomorphic.

Let us keep the notations of the preceding section. Let S be a system of 3 quadratic forms as in (4.1). Let $\alpha \in F$, $\alpha \neq 0$, and set $S' = \alpha S$.

We say that a system is isotropic if there exists a non-zero element of the underlying vector space which is a simultaneous zero of all the forms.

5.1 LEMMA *The following are equivalent:*

(i) $S \boxplus -S$ *and* $S \boxplus -S'$ *are similar*

(ii) $S \boxplus -S'$ *is isotropic*

(iii) S *and* S′ *are isomorphic.*

PROOF: It is clear that (i) implies (ii) and that (iii) implies (i). Suppose that (ii) holds. Then there exist $x,y \in D$, not both zero, such that

$$t(xd_i x^*) = \alpha t(yd_i y^*)$$

for $i = 1,2,3$.

Let d_4 be a non-zero element of D such that $d_4^* = -d_4$. Then $t(z\, d_4\, z^*) = 0$ for all $z \in D$. The set $\{d_1, d_2 \cdot d_3, d_4\}$ is an F-basis of D. Therefore

$t(dx^*x) = t(xdx^*) = \alpha t(ydy^*) = \alpha t(dy^*y)$ for all d in D. As

the reduced trace is non-degenerate, this implies that $x^*x = \alpha y^*y$. So x and y are both non-zero, and $\alpha = uu^*$ with $u = (xy^{-1})^*$. By (4.3) this shows that S and $S' = \alpha S$ are isomorphic. □

Using (4.2) and (5.1) we obtain:

5.2 *Let* $\alpha \in F$ *such that* $(a,\alpha)_v = 1$ *for all* $v \notin T$ *and that* $(a,\alpha)_v \neq (a,\alpha)_w$ *for some* $v,w \in T$. *Then* $S \boxplus -S$ *and* $S \boxplus -\alpha S$ *are similar over every completion of* F, *but are not similar over* F.

In the same way, one obtains counter-examples to the weak Hasse principle for the similarity of systems of 2 bilinear forms and of 6 alternating forms.

REFERENCES

[1] E. BAYER-FLUCKIGER "Intersections de groupes orthogonaux et principe de Hasse faible pour les systèmes de formes quadratiques", *C.R. Acad. Sc. Paris*, t.301, Série I, n°20 (1985), 911-914.

[2] E. BAYER-FLUCKIGER "Principe de Hasse faible pour les systèmes de formes quadratiques", *J. reine angew. Math.* 378 (1987), 53-59.

[3] M. KNESER "Lectures on Galois cohomology of classical groups", (appendix by T.A. Springer), *Tata Lecture Notes, Bombay* (1969).

[4] W. SCHARLAU "Quadratic and Hermitian forms", *Grundlehren der mathematischen Wissenschaffen 270*, *Springer-Verlag* (1985).

BAYER-FLUCKIGER, E.
IHES
35, route de Chartres
91440 Bures-sur-Yvette (France)

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

POWER VALUES OF SUMS $1^k+2^k+\ldots x^k$

BRINDZA B. *

Power values of the sum $S_k(x) = 1^k + 2^k+\ldots+(x-1)^k$ where k and x are positive integers have been studied by several authors. The first general result was obtained by J.J. Schäffer [7]. He showed that for given values of k and $m > 1$ the number of solutions of the equation

$$1^k + 2^k+\ldots+(x-1)^k = y^m \tag{1}$$

in positive rational integers x,y is infinite only in the trivial cases $k = 1$, $m = 2$; $k = 3$, $m\in\{2,4\}$ and $k = 5$, $m = 2$. In all other cases Schäffer proved the existence

* This research was done at Macquarie University and was made possible by a National Research Fellowship.

of an upper bound depending only on k for the number of solutions. Later, using Baker's method, K. Győry, R. Tijdeman and M. Voorhoeve [4], [8] gave some nice effective generalizations of Schäffer's result. B. Brindza [1] extended their theorems to the case of equations $f(S_k(x)) = y^z$ where f is a given polynomial.

It is well-known that the sum $S_k(x)$ can be expressed by Bernoulli polynomials and so the equation (1) can be considered as a hyperelliptic equation. Applying a general result of J.H. Evertse and J. Silverman [3] concerning hyperelliptic equations one may derive the bound $17^k\, m^{2k}$ for the number of solutions.

We shall prove the following result.

THEOREM 1. *For any given* $m \notin \{1,2,4\}$ *the equation* (1) *has at most* e^{7k} *solutions.*

THEOREM 2. *If* $k \leq 60$ *and* $m \notin \{1,2,4\}$ *then it has at most* e^{33} *solutions.*

Our proofs involve several special properties of Bernoulli polynomials and there seems to be no way to extend them to the case of arbitrary hyperelliptic equations.

PRELIMINARIES

For the following known auxiliary results we refer to [6] (pages 4-22).

Let $B_n(X)$ denote the n-th Bernoulli polynomial and $B_n \doteq B_n(0)$, $n = 0,1,2,\ldots$; moreover, let D_n be the denominator of B_n. Then we have

(A) $$B_n(X) = \sum_{i=0}^{n} \binom{n}{i} B_i X^{n-i}, \qquad (B_0 \doteq 1)$$

(B) $$1^k + 2^k + \ldots + (x-1)^k = \frac{1}{k+1} \left(B_{k+1}(x) - B_{k+1}\right),$$

(C) $$B_n(X) = (-1)^n B_n (1 - X),$$

(D) $$B_{2n+1} = 0, \qquad n = 1,2,\ldots,$$

(E) (Staudt-Clausen), $$D_{2n} = \prod_{p-1 \mid 2n} p,$$ p prime;

(F) For any prime number p $p(p^{2n} - 1)B_{2n}$ is an integer, hence $D_{2n} < 2^{2n+1}$,

(G) (Frobenius), The denominator of $B_{2n}/2n$ contains no other primes than the denominator of B_{2n} itself.

(H) $$\frac{2\cdot(2n)!}{(2\pi)^{2n}} < |B_{2n}| < \frac{(2n)!}{12\ (2\pi)^{2n-2}}\ .$$

Moreover, we shall use the following lemmas.

LEMMA 1. *Let* d(n) *denote, as usual, the number of positive divisors of* n. *Then for every positive* ε *and positive integer* n

$$d(n) \le n^{\varepsilon} \prod_{p^{\varepsilon}<2} \frac{2}{\varepsilon \log 2}, \qquad p \text{ prime};$$

(see e.g. [5], page 111).

LEMMA 2. (*Nagell, Ljunggren, Domar*). *Let* A,B *and* n *be positive integers. If* n > 2 *then the equation*

$$|Ax^n - By^n| = 1$$

has at most two solutions in positive integers x *and* y.

PROOF. See e.g. [2], Lemma 14.

PROOF OF THEOREM 1

Let (x,y) be an arbitrary but fixed solution of (1). At first we assume that k is even. Then

$$(k+1)y^m = (k+1)\ S_k(x) = B_{n+1}(x) =$$

$$= x\left[\binom{k+1}{1}B_k + \binom{k+1}{3}x^2B_{k-2} + \ldots + x^k\right].$$

Set the following notation.

N_k is the absolute value of the numerator of B_k.

P_k is the set of prime divisors of $b_k \doteq (k+1)\ N_k\ D_k$,

(At this stage we remark that b_k is not zero because of the point (H)).

$$P_k^{(1)}(x) \doteq \left\{p\in P_k \mid v_p(x) > \left[\frac{1}{2}\ (v_p(b_k)+1)\right]\right\},$$

$$P_k^{(2)}(x) \doteq \left\{p\in P_k \mid 0 < v_p(x) \leq \left[\frac{1}{2}\ (v_p(b_k)+1)\right]\right\},$$

($v_p(x)$ is defined, as usual, by $p^{v_p(x)} \parallel x$).

$$x_i = \prod_{p\in P_k^{(i)}} p^{v_p(x)}, \quad i = 1,2; \qquad x_3 = \prod_{p\notin P_k} p^{v_p(x)}.$$

It is obvious that x_1, x_2 and x_3 are pairwise relatively prime integers and $x = x_1x_2x_3$. For a prime factor p of x_3 we have

$$v_p(k+1) = v_p((k+1)B_k)) = 0,$$

$$v_p(x^i\binom{k+1}{i+1}B_{k-i})) \geq i-1 > 0, \quad i = 2,4,\ldots,k$$

and therefore

$$v_p((k+1)B_k + \binom{k+1}{3}B_{k-2}x^2 + \ldots + x^k) = 0;$$

hence x_3 has to be a perfect m-th power: $x_3 = x_4^m$. From the definition of x_2 we obtain

$$(3) \qquad x_2 \mid \prod_{p \in P_k} p^{\left[\frac{1}{2}(v_p(b_k)+1)\right]} \doteq c_k.$$

Considering the factor x_1 we find for a p from $P_k^{(1)}(x)$

$$v_p(x^i\binom{k+1}{i+1}B_{k-i})) \geq i\, v_p(x) - 1 \geq 2\, v_p(x) - 1 \geq$$

$$\geq 2(1 + \left[\tfrac{1}{2}\, v_p(b_k)+1\right])-1 > v_p(b_k) \geq v_p((k+1)B_k),$$

$$i = 2,4,\ldots,k.$$

It yields

$$(4) \quad v_p((k+1)y^m) = v_p(x) + v_p((k+1)B_k) =$$

$$= v_p(x_1) + v_p((k+1)B_k).$$

If $v_p(B_k) = 0$ then (4) implies $m\, v_p(y) = v_p(x_1)$ that is x_1 can be written in the form

$$x_5^m \prod_{\substack{p \in P_k^{(1)}(x) \\ p \mid N_k D_k}} p^{v_p(x_1)}$$

where x_5 is a positive integer. Furthermore m_p, for every $p \in P_k^{(1)}(x)$ defined by $m_p \equiv -v_p(x_1) \pmod m$ and $0 \le m_p < m$, is the remainder of $v_p(B_k)$ divided by m. It shows that the m-th power-free part of x_1 has the shape

$$\prod_{p \mid N_k D_k} p^{(m-m_p)\delta_p} \tag{5}$$

where $\delta_p \in \{0,1\}$. Summarizing

$$x = A_1 A_2\, u^m$$

where $A_1 \mid c_k$ and $A_2 = \prod_{p \mid N_k D_k} p^{(m-m_p)\delta_p}$.

Now we are goind to derive a similar formula for $(x-1)$ instead of x. From (B) and (C)

$$(k+1)\, S_k(x) = B_{k+1}(x) = -B_{k+1}(1-x).$$

Repeating the above-used argument we get

$$x-1 = B_1 B_2 w^m$$

where $B_1 | c_k$ and $B_2 = \prod_{p | N_k D_k} p^{(m-m_p)\delta_p^*}$, $(\delta_p^* \in \{0,1\})$. Let $S_k^{(m)}$ denote the set of vectors (A_1, B_1, A_2, B_2) under our conditions. It would be enough to give an appropriate upper bound to the cardinality of $S_k^{(m)}$ and that will be an upper bound for the number of equations

$$A_1 A_2 u^m - B_1 B_2 w^m = 1$$

which have at most two solutions in positive integers u,w. Let $\nu(n)$ denote the number of distinct prime divisors of n. It is easy to see that

$$(6) \quad |S_k^{(m)}| \le \Big(\sum_{\substack{ab=c \\ (a,b)=1}} d(a)d(b) \Big) \Big(\sum_{j=0}^{\nu(N_k D_k)} \binom{\nu(N_k D_k)}{j} 2^{\nu(N_k D_k)-j} \Big) =$$

$$= d(c_k)\, 2^{\nu(c_n)}\, 3^{\nu(N_k D_k)} \le [d(c_k)]^2 \, [d(N_k D_k)]^{\frac{\log 3}{\log 2}} .$$

(It is possible to claim some better inequalities but those would not give a much better upper bound in Theorem 1).

We may assume that $k > 60$. Indeed, if $k \le 60$ then the table in the proof of Theorem 2 and Theorem 2 prove Theorem 1. From (E) and (H)

$$c_k \le (h+1)\frac{k!\ 4^{k+1}}{12(2\pi)^{k-2}} < \left(\frac{k}{3}\right)^k; \quad N_k D_k < \frac{1}{k+1}\left(\frac{k}{3}\right)^k, \quad (k > 30)$$

and applying Lemma 1 with the well-known inequality

$\pi(n) < \frac{6n}{\log n}$, $(n > 2)$ we have

$$|S_k^{(m)}| \le \left(\frac{k}{3}\right)^{k\varepsilon\left(2+\frac{\log 3}{\log 2}\right)} \left(\prod_{p^{\varepsilon}<2} \frac{2}{\varepsilon \log 2}\right)^{2+\frac{\log 3}{\log 2}} {}^{(k+1)} - \frac{\varepsilon \log 3}{\log 2} <$$

$$< \left(\frac{k}{3}\right)^{k\varepsilon\left(2+\frac{\log 3}{\log 2}\right)} {}^{(k+1)} - \frac{\varepsilon \log 3}{\log 2} \exp\left\{\left(2+\frac{\log 3}{\log 2}\right)\frac{6.2^{1/\varepsilon}}{\log 2^{1/\varepsilon}} \log \frac{2}{\varepsilon \log 2}\right\}.$$

Taking $\varepsilon = \frac{\log 2}{\log(k/6)}$ and $f(k) =$

$$f(k) = (\log(k/3)\log 2 + \log 2 - 2\log\log 2 + \log\log(k/6))(\log(k/6))^{-1}$$

a simple calculation gives

$$|S_k^{(m)}| < \frac{1}{2} \exp\{(2+\frac{\log 3}{\log 2})kf(k)\}.$$

Since f(k) is monotonically decreasing (k > 17) we obtain

$$2|S_k^{(m)}| < \exp\{(2+\frac{\log 3}{\log 2})kf(60)\} = \exp\{k\cdot 6,8\ldots\} < e^{7k}$$

which proves our theorem in that case when k is even.

In the remaining case k is odd and k > 60. Then

$$(k+1)y^m = (k+1)S_k(x) = (B_{k+1}(x) - B_{k+1}) =$$

$$= x^2\{\binom{k+1}{2}B_{k-1} + x^2\binom{k+1}{4}B_{k-3} + \ldots + x^{k-1}\}$$

and

$$(k+1)y^m = B_{k+1}(1-x) - B_{k+1} =$$

$$= (x-1)^2\{\binom{k+1}{2}B_{k-1} + (x-1)^2\binom{k+1}{4}B_{k-3} + \ldots + (x-1)^{k-1}\}.$$

Let Q_n denote the set of prime divisors of $d_k \doteq k(k+1)N_{k-1}D_{k-1}$. Setting

$$Q_k^{(1)}(x) = \{p \in Q_k \mid v_p(x) > \left[\frac{1}{2}(v_p(d_k) + 1)\right]\},$$

$$Q_k^{(2)}(x) = \{p \in Q_k \mid 0 < v_p(x) \leq \left[\frac{1}{2}(v_p(d_k) + 1)\right]\}$$

we have again the factorization $x = x_1 x_2 x_3$ where

$$x_i = \prod_{p \in Q_k^{(i)}(x)} p^{v_p(x)}, \quad i = 1,2; \quad x_3 = \prod_{p \notin Q_n} p^{v_p(x)}.$$

We distinguish two cases. If m is even then $m = 2m_1$ and $m_1 > 2$. Moreover, x_3 has to be a perfect m_1-th power and

$$x_2 \mid \prod_{p \mid d_k} p^{\left[\frac{1}{2}(v_p(d_k)+1)\right]}.$$

The m_1-th power-free kernel of x_1 can be written in the form

$$\prod_{p \mid k N_{k-1} D_{k-1}} p^{(m_1 - n_p)\delta_p}$$

where $\delta_p \in \{0,1\}$ and $0 \leq n_p < m_1$ is the remainder of $v_p\left(\frac{k\, N_{k-1}}{2\, D_{k-1}}\right)$ divided by m_1 (cf. (5)). Similar observa-

tions can be made on $(x-1)$ instead of x and we have $2\cdot 3^{\nu(k\,N_{k-1}D_{k-1})}d^2(d_k)$ is an upper bound for the number of solutions. Since

$$d_k \le k(k+1)\,\frac{(k-1)!\,4^k}{12(2\pi)^{k-3}} < \left(\frac{k}{3}\right)^k, \quad (k > 30)$$

our above used procedure can be repeated to show that it is less than e^{7k}.

In that case when m is odd x_3 has to be a perfect m-th power and for a p from $Q_k^{(1)}(x)$

$$2\,v_p(x) + v_p(\binom{k+1}{2}B_{k-1}) = v_p(k+1) + m v_p(y).$$

It implies $2\,v_p(x) = m\,v_p(y)$ that is $m \mid v_p(x)$ provided that $p \mid kN_{k-1}D_{k-1}$ and also the m-th power-free kernel of x_1 has the shape

$$\prod_{p \mid kN_{k-1}D_{k-1}} p^{(m-r_p)\varepsilon_p}$$

where $\varepsilon_p \in \{0,1\}$ and $0 \le r_p < m$ is given by

$$2\,r_p \equiv v_p\left(\frac{k\,N_{k-1}}{2\,D_{k-1}}\right) \pmod m.$$

Therefore

$$2\cdot 3^{\nu(k\,N_{k-1}D_{k-1})}\,d^2(d_k) < e^{7k}$$

is an upper bound for the number of solutions again.

PROOF OF THEOREM 2

Set

$$\alpha_k = \begin{cases} N_k\, D_k & \text{if } k \text{ is even} \\ k\, N_{k-1}\, D_{n-1} & \text{if } k \text{ is odd,} \end{cases}$$

$$\beta_k = \begin{cases} (k+1N_k\, D_k & \text{if } k \text{ is even} \\ k(k+1)\, N_{k-1}\, D_{k-1} & \text{if } k \text{ is odd.} \end{cases}$$

In the proof of Theorem 1 we have shown that

$$c_k = 2 \cdot 3^{\nu(\alpha_k)}\, d(\beta_k) \cdot 2^{\nu(\beta_k)}$$

is an upper bound for the number of solutions of the equation (1). Using Wagstaff's table (see [9]) on factorization of Bernoulli numbers we have made another one (see next page) and it shows by (E) that

$$\max_{1 \le k \le 60} \{\nu(\alpha_k),\ \nu(\beta_k)\} \le 11.$$

Hence β_k can be written in the form $2^{\gamma_1} \cdot 3^{\gamma_3} \cdot 5^{\gamma_3} \cdot p_4^{\gamma_4} \cdots p_{11}^{\gamma_{11}}$, $(k \le 60)$ where $0 \le \gamma_1 \le 6$, $0 < \gamma_2 \le 4$, $0 \le \gamma_j \le 2$, $(4 \le j \le 11)$ and a simple calculation gives that

$$c_k < 2 \cdot 3^{10} \cdot 2^{11} \cdot 7 \cdot 5^2 \cdot 3^7 < e^{33}, \quad (k \le 60)$$

which proves Theorem 2.

REMARK. It is interesting that the numbers $N_2,\ldots,N_{60}$ are square-free, except N_{50} $(5^2|N_{50})$ and so $d(\beta_k)$ is relatively small. Otherwise, if $p > 3$ (p is a prime) and n is a positive integer then $p|D_{2p^n}$ and from (G) we have $p^n|N_{2p^n}$ that is $v_p(N_k)$ can be arbitrarily large.

k	$\gamma'(N_k)$	$\gamma'(D_k)$
2	0	2
4	0	3
6	0	3
8	0	2
10	1	3
12	1	4
14	1	2
16	1	3
18	1	3
20	2	4
22	3	2
24	2	5
26	2	2
28	3	3
30	3	4
32	3	4
34	2	2
36	1	6
38	2	2
40	2	4
42	1	3
44	5	3
46	3	2
48	3	6
50	3	3
52	5	3
54	3	4
56	4	4
58	5	3
60	3	8

REFERENCES

[1] BRINDZA, B., On some generalizations of the diophantine equation $1^k+2^k+\ldots+x^k = y^z$, *Acta Arith.* 44 (1984), 99-107.

[2] EVERTSE, H.J., On the equation $ax^n - by^n = c$, *Compositio Math.* 47 (1982), 289-315.

[3] EVERSTE, J.H., SILVERMAN, J.H., Uniform bounds for the number of solutions to $Y^n = f(x)$, *Math. Proc. Camb. Phil. Soc.* 100 (1986), 237-246.

[4] GYÖRY, K., TIJDEMAN, R. and VOORHOEVE, M., On the equation $1^k+2^k+\ldots+x^k = y^z$, *Acta Arith.* 37 (1980), 234-240.

[5] HUA LOO KENG, *Introduction to Number Theory*, Springer-Verlag, 1982.

[6] RADEMACHER, H., *Topics in Analytic Number Theory*, Springer-Verlag, 1973.

[7] SCHÄFFER, J.J., The equation $1^p+2^p+\ldots+n^p = m^q$, *Acta Math.* 95 (1986), 155-189.

[8] VOORHOEVE, M., GYÖRY, K. and TIJDEMAN, R., On the diophantine equation $1^k+2^k+\ldots+x^k+R(x) = y^z$, *Acta Math.* 143 (1979), 1-8. Corr. 159 (1987), 151-152.

[9] WAGSTAFF, S.S., The irregular primes to 125000, *Math. Comp.* 32 (1978), 583-591.

BRINDZA, B.

KLTE Mat.Int.
Debrecen
Egyetem tér 1.
H-4010

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

TYPE NUMBER AND CLASS NUMBER OF HEREDITARY ORDERS IN NON EICHLER (R) -ALGEBRAS OF PRIME INDEX OVER GLOBAL FUNCTION FIELDS

DENERT M.

In [P], A. Pizer uses Selberg's trace formula to obtain an explicit formula for the type number of hereditary orders in totally definite quaternion algebras. We extend these methods to hereditary orders in non Eichler (R)-algebras of prime index over global function fields and we remark that a subtile adaptation also yields a class number formula for these orders.

PRELIMINARIES

Let K be a global function field, i.e. K is the function field of a complete regular curve C defined over $/F_q$ (where $/F_q$ is supposed to be algebraically closed in K.)

A denotes a central simple K-algebra of prime index n (i.e. $[A : K] = n^2$). For $p \in C$ denote with κ_p the *capacity* and e_p the *ramification index* of A at p, then $\kappa_p \cdot e_p = n$. The *reduced norm* on A is denoted *nr*, cf. [R]. We fix an '*affine*' *ring* R in K by choosing a finite set $T \subset C$ and $R = \bigcap_{p \notin T} R_p$.

We always assume that A is a *non Eichler* (R)*-algebra*, i.e. for every $p \in T$ we have $e_p = n$, so $\kappa_p = 1$.

A *hereditary* R-order Θ is determined by its completions $\{\Theta_p \mid p \notin T\}$ where Θ_p, a hereditary R_p-order in A_p, is determined by its *local type* r_p and its *local invariants* $(n_j) = (n_1, \ldots, n_{r_p})$ with $\Sigma n_j = \kappa_p$; namely if $r_p \neq 1$ then $\kappa_p = n$ and θ_p is isomorphic (i.e. conjugated) to $\Theta_{p,s}^{(n_j)}$ given by:

$$\Theta_{p,s}^{(n_j)} = \begin{bmatrix} (R_p) & (R_p) & \ldots & (R_p) \\ (p) & (R_p) & \ldots & (R_p) \\ \cdot & & \cdot & \cdot \\ \cdot & & \cdot & \cdot \\ (p) & (p) & \ldots & (R_p) \end{bmatrix}^{(n_j)} \subset M_n(R_p), \text{ cf. [R],[D 2]}$$

Remark that for $\Theta_p = \Theta_{p,s}^{(n_j)}$ the units are given by:

$$\Theta_p^* = \begin{bmatrix} (R_p)^* & (R_p) & \dots & (R_p) \\ (p) & (R_p)^* & \dots & (R_p) \\ \vdots & & \ddots & \\ (p) & (p) & \dots & (R_p)^* \end{bmatrix}^{(n_j)} \quad \text{where } (R_p)^*_{j,j} = GL_{nj}(R_p).$$

If $r_p = n$ then Θ_p is called a *minimal hereditary* R_p-*order*.

Since Θ_p is maximal a.e. it follows that $r_p = 1$ a.e., we denote $D(\Theta/R) = D_1(\Theta/R)\ D_2(\Theta/R) = D_1D_2$, the *relative discriminant* of Θ, (cf. [R], [DVG 2], [D 2]) and

$$D_2^{\min}(\Theta/R) = \prod_{\substack{p|D_2 \\ r_p=n}} D(\Theta_p/R_p).$$

A genus of hereditary R-orders in A is denoted $G_{D_1D_2}$.

Let $t_{D_1D_2}$ be the *type number*, i.e. the number of non-isomorphic R-orders in $G_{D_1D_2}$ and $h_{D_1D_2}$ the *class number*, i.e. the number of non-isomorphic locally free left Θ-ideals in A, $\Theta \in G_{D_1D_2}$. We use the shorter notation $t = t_{D_1D_2}$, $h = h_{D_1D_2}$ for a fixed genus $G = G_{D_1D_2}$ of hereditary R-orders in A.

It is easy to describe t and h, using idèles. For $K \subset L \subset A$, X = K, L or A let $J(X)$ be the idèle group of X.

Further denote $U(\Theta)$ the unit idèles of Θ and $N(\Theta)$ the normalizer of Θ.

We fix $\Theta_s \in G = G_{D_1 D_2}$ defined by $\Theta_{s,p} = \Theta_{p,s}^{(n_j)}$ then:

$t = \sharp(_{N(\Theta_s)}\backslash J(A)/_{A^*})$ and $h = \sharp(_{U(\Theta_s)}\backslash J(A)/_{A^*})$

A. Pizer's method depends on a modified idèlic description.

1. CALCULATION OF t AND h

We introduce: $\tilde{G} = J(A)/_{J(K)}$ and Ψ: $J(A) \to \tilde{G}$ the canonical map. Further notation: $G = \Psi(A^*) = A^*/_{K^*}$
$\tilde{G}_{\Theta^*} = \Psi(U(\Theta))$, $G_{\Theta^*} = \Psi(\Theta^*)$, $\tilde{G}_{N(\Theta)} = \Psi(N(\Theta))$,
$G_{N(\Theta)} = \Psi(N(\Theta) \cap A^*) = \Psi(N(\Theta))$.
The relation $\Psi(\tilde{\alpha}) = \tilde{a}$ is also denoted $\tilde{\alpha} \equiv \tilde{a}$.
Since $J(K) \subset N(\Theta)$ we obtain directly that $t = \sharp(\tilde{G}_{N(\Theta_s)}\backslash \tilde{G}/G)$.

For the class number we need a subtile adaptation. Remark that the stable class group $C\ell(\Theta)$ of $\Theta \in G_{D_1 D_2}$, can be presented by $\{x_i \mid 1 \leq i \leq h_R\}$ with $x_i \in J(K)$, $h_R = \sharp C\ell(R)$, cf. [R],[DVG 2]. To $\tilde{\alpha} \in \tilde{G}$, $\tilde{\alpha} \equiv \tilde{a}$, we associate the set $\{\Theta_s\ a\ x_i \mid 1 \leq i \leq h_R\}$ of h_R non-isomorphic left Θ_s-ideals. This is well-defined, namely it doesn't depend on the choice of $\tilde{a} \equiv \tilde{\alpha}$. We obtain:

$$\frac{h}{h_R} = \#(\tilde{G}_{\Theta_s^*} \backslash \tilde{G} / G)$$

To calculate t and h, we use Selberg's trace formula to a certain operator, cf. [P] for more detailed definitions. We obtain:

$$\text{(F1)} \quad t = \#(\tilde{G}_{N(\Theta_s)} \backslash \tilde{G} / G) = \sum_{\{\alpha\}} \int_{\tilde{G}/G(\alpha)} F_{N(\Theta_s)}(x\ \alpha\ x^{-1})\ dx$$

$$\text{(F2)} \quad \frac{h}{h_R} = \#(\tilde{G}_{\Theta_s^*} \backslash \tilde{G} / G) = \sum_{\{\alpha\}} \int_{\tilde{G}/G(\alpha)} F_{\Theta_s^*}(x'\ \alpha\ x'^{-1})\ dx'$$

where the sums run over a set of representatives $\{\alpha\}$ for the conjugacy classes $\{\alpha\}$ in G, $G(\alpha) = \{\beta \in G \mid \alpha\beta = \beta\alpha\}$ is the centralizer of α in G; further $F_{N(\Theta_s)}$ (resp. $F_{\Theta_s^*}$) denotes the characteristic function of $\tilde{G}_{N(\Theta_s)}$ (resp. $\tilde{G}_{\Theta_s^*}$) and dx (resp. dx') is a Haar measure on $\tilde{G}$ normalized by

$$\int_{\tilde{G}_{N(\Theta_s)}} dx = 1 \quad \text{(resp. } \int_{\tilde{G}_{\Theta_s^*}} dx' = 1\text{)}.$$

The relation between these two measures is given by $dx' = n^{l+k} dx$, where $l = \#\{p \mid D_1\}$ and $k = \#\{p \mid D_2^{\min}\}$. This is a consequence of the following lemma:

LEMMA 1. *For every* $\Theta \in G(=G_{D_1 D_2})$: $N(\Theta)/J(K)U(\Theta)$ *is represented by* $\{\tilde{\pi}_1^{f_1} \ldots \tilde{\pi}_{l+k}^{f_{l+k}} \mid 0 \leq f_i < n\}$ *where*

$\tilde{\pi}_i = (\ldots,1,\bar{\pi}_i,2\ \ldots)$ *with* $\bar{\pi}_i = \bar{\pi}_{p_i}^{(\Theta)}$ *the uniformizing element of* Θ_{p_i} (*i.e.* $\bar{\pi}_{p_i}^{(\Theta)}$ *is the generator of* rad Θ_{p_i}) and $p_1,\ldots,p_1|D_1$; $p_{1+1},\ldots,p_{1+k}|D_2^{\min}$.

PROOF: cf [DVG 2] //

The contribution of $\alpha\in G$ in (F1), denoted $C_1(\alpha)$ is non-zero iff there exists $\tilde{\rho}\in\tilde{G}$ such that $\tilde{\rho}\ \alpha\ \tilde{\rho}^{-1}\in\tilde{G}_{N(\Theta_s)}$ or equivaluent $\alpha\in G_{N(\Theta)}$ with $\Theta = \tilde{\rho}^{-1}\ \Theta_s\ \tilde{\rho} \in G$.
Analogously, the contribution of $\alpha \in G$ in (F2), denoted $C_2(\alpha)$ is non-zero iff $\alpha \in G_{\Theta^*}$, for $\Theta\in G$ and then $C_2(\alpha) = n^{1+k}C_1(\alpha)$.
The calculation of (F1) and (F2) breaks up in several steps.

STEP 1: Characterization of $G_{N(\Theta)}$ for $\Theta \in G$.

Denote with I the ideal group of R, I^* the subgroup of principal ideals and E the subgroup generated by $\{p_1,\ldots,p_1|D_1\} \cup \{p_{1+1},\ldots,p_{1+k}|D_2^{\min}\}$.
Let $\{d_i|1 \le i \le m\}$ be integral R-ideals representing $E\cdot I^n \pmod{I^{*n}}$.

LEMMA 2: $\alpha\in G_{N(\Theta)}$ *iff there exists* $a\in A^*$, $\alpha \equiv a$ *with* $a = 1$ *or* a *satisfies the following properties:*

i) $a\in\Theta$

ii) $(nr(a)) = d_i$ *for some* $i\in\{1,\ldots,m\}$

iii) *If* $p \notin T$ *denote* $s_p = \left[\frac{v_p(nr(a))}{n} \right]$ *then* $a\, \pi_p^{-s_p} \in \Theta_p$

iv) *If* $p \notin T$ *and* $v_p(nr(a)) \equiv g \bmod n$ *with* $g \neq 0$, *denote* $f_a(Y) = Y^n + a_1 Y^{n-1} + \ldots + (-1)^n nr(a) \in R[Y]$, *the minimal polynomial of* a *then:*

$$p^{i s_p + \left[\frac{i g}{n}\right] + 1} \mid a_i \quad \textit{for } 1 \leq i \leq n-1.$$

The notation $[x]$, $x \in \mathbb{R}$ is defined by $[x] \in \mathbb{Z}$ and $[x] \leq x < [x] + 1$.

PROOF: *cf.* [P] lemma 5, where $n = 2$.

It is sufficient to prove the lemma for $\Theta = \Theta_s$

($\Rightarrow$) Suppose that $\alpha \in G_{N(\Theta)}$; we must show that $\alpha \equiv a$ with $a = 1$ or a satisfies the properties i) to iv).

If $\{\alpha\} = \{1\}$ then we van take $a = 1$, so we can assume that $\{\alpha\} \neq \{1\}$ and the properties i) to iii) follow as in lemma 5 in [P]. The proof of iv) is different.

Fix $p \notin T$ then $\alpha \equiv a \in N(\Theta_p)$ implies that $a = \varepsilon\, \pi^{-g} \cdot \pi_p^{s_p}$ with $\varepsilon \in \Theta_p^*$, $s_p, g \in \mathbb{Z}$ and $0 \leq g < n$ (we denoted $\bar{\pi} = \bar{\pi}_p^{(\Theta)}$).

Denote $a' = a\, \pi_p^{-s_p}$ and $f_{a'}(Y) = Y^n + a_1' Y^{n-1} + \ldots + a_n' \in R[Y]$, then it is sufficient to prove that $v_p(a_i') \geq \left[\frac{ig}{n}\right] + 1$ for $1 \leq i \leq n-1$. Remark that $a' = \varepsilon \cdot \bar{\pi}^g$ and express that $f_{a'}(a') = 0$. Since n is prime and $0 < g < n$ it follows that $n\, v_p(a_i') + (n - i)g > n\, g$ for $1 \leq i \leq n-1$ and

property iv) follows.

(<=) Conversely, suppose that $a = 1$ or a satisfies properties i) to iv); we must show that $\alpha = \Psi(a) \in G_{N(\Theta)}$.

If $a = 1$ this is trivial, so we assume that $a \notin K^*$ satisfies i) to iv). We now prove that $a \in N(\Theta_p)$ for $p \notin T$ then $\alpha \in G_{N(\Theta)}$ follows directly.

Fix $p \notin T$, in short denote $\pi = \pi_p$, $\bar{\pi} = \bar{\pi}_p^{(\Theta)}$. For $p | D_1$: $N(\Theta_p) = A_p^*$ so $a \in N(\Theta_p)$.

For $p \nmid D_1$ and $g = 0$, we find $v_p(nr(a)) = n \cdot s_p$ and thus $nr(a\,\pi^{-s_p}) \in R_p^*$. Since property ii) provides that $a\,\pi^{-s_p} \in \Theta_p$ we conclude $a\,\pi^{-s_p} \in \Theta_p^*$ so $a \in N(\Theta_p)$.

Leaves the case $g \neq 0$ and $p \mid D_2^{min}$; consider $a' = a\pi^{-s_p}$, and $f_{a'}(Y) = Y^n + a_1' Y^{n-1} + \ldots + a_n' \in R_p[Y]$ with $v_p(a_i') > \left[\frac{ig}{n}\right]$ for $1 \leq i \leq n-1$ and $v_p(a_n') = g$.

We now show that $f_{a'}(Y)$ has a root of the form $\varepsilon \bar{\pi}^{-g}$, $\varepsilon \in \Theta_p^*$; then it follows that we can choose $a \in N(\Theta_p)$.

Consider $\varepsilon \in \Theta_p^*$ of the form:

$$\varepsilon = \left[\begin{array}{c|c} I_{n-g,n-g} & 0_{n-g,g} \\ \hline 0 & \begin{matrix} 1 & & 0 \\ & \ddots & \\ & & 1 \end{matrix} \\ \hline b_1 \ldots b_{n-g} & b_{n-g+1} \ldots b_n \end{array}\right]$$

with $b_n \in R_p^*$, $b_i \in R_p$, $v_p(b_i) \geq 1$ for $1 \leq i < n$.

Calculate $f_{\varepsilon\bar{\pi}^g}(Y) = \det(\varepsilon\bar{\pi}^g - I_n Y)$ then it is clear that we can choose b_i, $1 \leq i \leq n$ such that

$f_{\varepsilon\bar{\pi}^g}(Y) = f_{a'}(Y)$. //

STEP 2: A set of representatives for the conjugacy classes in G, which have non-zero contribution in (F1).

The remarks and calculations in [P], §8, extend easily. Let $\{n_\mu \mid 1 \leq \mu \leq k\}$ represent the principal ideals $\{d_i\}$ and let $\{e_\rho \mid 1 \leq \rho \leq s\}$ represent R^*/R^{*n}. It follows directly that for $\alpha \in G$ with $C_1(\alpha) \neq 0$ there exists $a \in A^*$, $\alpha \equiv a$ such that $a = 1$ or the minimal polynomial of a is of the form:

$$(*) \quad f_{\mu,\rho,(a_i)}(Y) = Y^n + a_1 Y^{n-1} + \ldots + a_{n-1} Y + (-1)^n n_\mu e_\rho$$

satisfying the properties i) to iv) of lemma 2.
Introduce the notation:

$$\delta_n = \begin{cases} 1 & \text{if } X^n - 1 = 0 \text{ has only the trivial root 1 in } K. \\ n & \text{if } X^n - 1 = 0 \text{ has a root } \zeta_n \neq 1 \text{ in } K. \end{cases}$$

LEMMA 3: *Two different polynomials* $f_{\mu,\rho,(a_i)}(Y)$ *and* $f_{\mu',\rho',(a_i')}(Y)$ *of the form* (*) *represent the same conjugacy class in G if and only if* $\delta_n = n$ *and* $\mu = \mu'$,

$\rho = \rho'$ *and there exists* $k \in \{0,\ldots,n-1\}$ *such that* $a_i' = \zeta_n^{ki} a_i$ *for* $1 \leq i \leq n-1$.

PROOF: the proof in §8, in [P] extends directly.//

If $\delta_n = n$, then the irreducible polynomials of the form (*) uniquely represent a conjugacy class in G if and only if $a_i = 0$ for $1 \leq i \leq n-1$, i.e. the roots a of this polynomial satisfy the condition $a^n \in K^*$. The classes corresponding to the other polynomials of the form (*) are counted n times, however the contribution will turn out to be n times less, cf. lemma's 4,6.

STEP 3: Determination of $G(\alpha)$.

Recall that $G(\alpha) = \{\beta \in G \mid \alpha\beta = \beta\alpha\}$.

LEMMA 4: $G(\alpha) = G$ *for* $\alpha \equiv 1$ *and for* $\{\alpha\} \neq \{1\}$, $\alpha \equiv a$ *with* $K(a)$ *a separable extension of* K *we find:*

i) *for* $\delta_n = 1$: $G(\alpha) = K(a)^*/K^*$

ii) *for* $\delta_n = n$: $(G(\alpha) : K(a)^*/K^*) = \begin{cases} 1 & \text{if } a^n \notin K^* \\ n & \text{if } a^n \in K^* \end{cases}$

PROOF: an analogue proof as in [P] lemma 9 can be given. //

STEP 4: Calculation of $C_1(\alpha)$ for $\alpha \in G_{N(\Theta)}$.

The calculation of $C_1(\alpha)$ depends on whether $\alpha \equiv 1$ or not.

LEMMA 5: *If* $\alpha \equiv 1$ *then* $C_1(\alpha) = \frac{1}{n^{1+k} \cdot h_R} \cdot \frac{M_\Theta(S)}{n^{n-1}}$

with $M_\Theta(S) = h_R \cdot q^{(n^2-1)(g_k - 1)} \zeta_K(2) \ldots \zeta_K(n) \prod_{p \in C} T_p$

where $\zeta_K(s)$ *is the zeta function of* K *and* g_K *is the genus of* K. *Furthermore the factors* T_p *are given by:*

$$T_p = \begin{cases} \prod_{1 \le j \le n-1} (Np^j - 1) & \text{if } e_p = n \quad (Np = q^{\varphi p} = \#(R_p/p)) \\ \dfrac{\prod_{1 \le j \le n} (Np^j - 1)}{\prod_{1 \le j \le r} \prod_{1 \le i \le n_j} (NP^i - 1)} & \text{if } e_p = 1 \text{ and the local invariants are } (n_j) \end{cases}$$

$M_\Theta(S)$ is the measure of stably free Θ-idelas, cf. [DVG 2-3], [D 1].

PROOF: As in §11 in [P] and using lemma 1, we obtain:

$$C_1(\alpha) = \frac{1}{n^{1+k} \cdot h_R} \sum_{1 \le i \le h} \frac{1}{(\Theta_i^* : R^*)}.$$

In [D 2-3] we showed that $(\Theta_i^* : R^*) = \frac{\hat{w}_i}{(R^* : nr\Theta_i^*)} \cdot \frac{(R^* : R^{*n})}{\hat{w}_R}$

and $M_\Theta(S) = \sum_{1 \le i \le h} \frac{(R^* : nr\,\Theta_i^*)}{\hat{w}_i}$; the result follows directly.

Now we consider $\alpha \equiv a$, $a \notin K^*$ such that $K(a)$ is a separable extension of K.

By lemma 2, we can choose $a \in \Theta$ with $\Theta = \tilde{q}_0^{-1}\, \Theta_s\, \tilde{q}_0$, $\tilde{q}_0 \in J(A)$. This means that $\Psi(\tilde{q}_0)$ is contained in the support of $F_{N(\Theta_s)}(x \alpha x^{-1})$.

Denote $S_a = \Theta \cap K(a)$, an R-order in $K(a)$ containing a, and let $\langle S_a \rangle = \{\tilde{q} \in J(A) \mid \tilde{q}^{-1}\, \Theta_s \tilde{q} \cap K(a) = S_a\}$; then the support of $F_{N(\Theta_s)}(x \alpha x^{-1})$ is a disjoint union of $\Psi(\langle S_a \rangle)$, S_a an R-order in $K(a)$.

For hereditary orders in quaternion algebras, we always have $\langle S_a \rangle = N(\Theta_s)\, \tilde{q}_0\, J(K(a))$. This is no longer true for hereditary orders in algebras of arbitrary index.

We calculate $N(\Theta_s) \backslash \langle S_a \rangle / J(K(a)) = \prod_{p \notin T} N(\Theta_p) \backslash \langle S_p \rangle / K(a)_p^*$ where

$$\langle S_p \rangle = \{q_p \in A_p^* \mid \Theta_p \cap q_p K(a)_p q_p^{-1} = q_p S_p\, q_p^{-1}\}.$$

Then $\#(N(\Theta_p) \backslash \langle S_p \rangle / K(a)_p^*) = m_p(S)$ is the number of non-equivalent embeddings of S_p in Θ_p modulo $N(\Theta_p)$ · (cf. [V], [DVG 2] or [D 3] for detailed definitions).

Since $m_p(S) = 1$ if Θ_p is maximal, cf. [N], we define $m_T(S) = \prod_{p \notin T} m_p(S)$ and fix a set of $m_T(S)$ representatives $\{\tilde{q}_i\}$ for $N(\Theta_s) \backslash \langle S_a \rangle / J(K(a))$.

Denote $\Theta_i = \tilde{q}_i^{-1}\,\Theta_s\,\tilde{q}_i$ then $\langle S_a\rangle = \dot{\bigcup}_{1\le i\le m_T(S_a)} q_i N(\Theta_i) J(K(a))$

is a disjoint union.

From lemma 1, $N(\Theta_i) = \dot{\bigcup}_{0\le f_1,\ldots,f_{1+k}<n} \tilde{\pi}_1^{f_1}\cdots\tilde{\pi}_{1+k}^{f_{1+k}}\, U(\Theta_i) J(K)$

is a disjoint union, but some of the $\tilde{\pi}_i^{f_i}$ may be absorbed in $U(\Theta_i)\ J(K(a))$.

We 'extend' the definition of Pizer, for $E_{D_1D_1}(S)$ as follows:

DEFINITION: For $S = \Theta \cap L$, define $E_{D_1D_2}(S) = \prod_{p|D_1D_2} \min E_p(S)$

where $E_p(S)$ is given by:

$$E_p(S) = \begin{cases} 1 & \text{if } p \text{ is totally ramified in } L \text{ and } S_p \text{ is} \\ & \text{the maximal } R_p\text{-order in } L_p. \\ n & \text{else.} \end{cases}$$

If we add $E_{D_1D_2}(S) = 0$ if $S \not\subset \Theta$ then this definition coincides with Pizer's.

As in [P] it follows now that $\langle S_a\rangle$ consists of $m_T(S)\cdot E_{D_1D_2}(S)$ disjoint copies of $U(\Theta)J(K(a))$ for $K(a)$ a separable extension of K. In short we denote $E_{D_1D_2}(S) = E(S)$.

LEMMA 6: If S is an R-order in $K(a)$, a separable K-extension

then $C_1(\langle S\rangle) = \dfrac{1}{(G(\alpha) : K(a)^*/_{K^*})} \cdot \dfrac{1}{n^{1+k}\cdot h_R} m_T(S)E(S)\dfrac{h_S}{(S^* : R^*)}$

is the contribution of $\langle S\rangle$ in (F1).

PROOF: The proof of lemma 14 in [P] extends immediately. //

Resuming these four steps, we obtain the following procedure to calculate the type number t and the class number h of a given genus $G = G_{D_1D_2}$ in a non Eichler (R)-algebra of prime index n over a global function field K, with (char K,n) = 1:

*Choose a set of representatives $\{e_\rho\}$ for R/R^{*n}. Consider the ideal group I of R and the sub-group E generated by the prime ideals which divide $D_1D_2^{min}$. Let $\{d_i\}$ be a set of integral R-ideals representing $E\cdot I^n$ mod I^{*n} (where I^* is the sub-group of principal ideals in I) and choose a set $\{n_\mu\}$ in R representing the principal ideals $\{d_i\}$.

*Determine all polynomials in $R[Y]$ of the form:

$f_{\mu,\rho,(a_i)}(Y) = Y^n + a_1Y^{n-1}+\ldots+a_{n-1}\,Y + (-1)^n n_\mu e_\rho$, satisfying the properties:

i) For $p \notin T$ and $s_p = \left[\dfrac{v_p(n_\mu)}{n}\right]$ there exists $a \in \Theta$, $\Theta \in G$ such that $a\cdot\pi_p^{-s_p} \in \Theta_p$.

ii) For $p \notin T$ and $n\, s_p - v_p(n_\mu) = g \neq 0$ the $a_i \in R$ satisfy $v_p(a_i) \geq i\, s_p + \left[\frac{i\, g}{n}\right] + 1$, $1 \leq i \leq n-1$

*Remark that $L = K[Y]/f_{\mu,\rho,(a_i)}(Y) = K(a)$ is a separable splitting field in A. We obtain a finite set $V_L = \{L = K(a)\}$ of separable splitting fields in A. For $L \in V_L$ we determine all R-orders S in L such that $S = \Theta \cap L$ for some R-order $\Theta \in G$. We obtain a finite set V_S of R-orders S embedded in Θ, $\Theta \in G$.

Then it follows that:

$$t = \frac{1}{n^{1+k} \cdot h_R} \{\frac{M_\Theta(S)}{n^{k-1}} + \frac{1}{\delta_n} \sum_{S \in V_S} \frac{h_S}{(S^*:R^*)} E_{D_1 D_2}(S)\, m_T(S)\}$$

$$h = \frac{M_\Theta(S)}{n^{k-1}} + \frac{1}{\delta_n} \sum_{S \in V_S^o} \frac{h_S}{(S^*:R^*)} E_{D_1 D_2}(S)\, m_T(S)$$

with $V_L^o = \{L \in V_L \mid L$ corresponds to $f_{\mu,\rho,(a_i)}(Y)$ with $n_\mu = 1\}$

$V_S^o = \{S \in V_S \mid S$ is an R-order in $L \in V_L^o\}$.

REMARK: The condition (char K,n) = 1 is only needed to provide that every $L \in V_L$ is a separable extension

of K. In the last paragraph, where we restrict to $/F_q[t]$-orders, the class number formulas are also correct if (char K,n) $\neq 1$.

2. SOME EXPLICIT EXAMPLES IF $R = /F_q[t]$ (and (char K,n) = 1).

Let A be a non Eichler $(/F_q[t])$-algebra of prime index n over $/F_q(t)$, then t^{-1} ramifies (totally) in A. This yields that for every $L \in V_L$, L doesn't decompose at t^{-1}, cf. [R].

For $L = K(a)$ with $f_a(Y) = Y^n + a_1 Y^{n-1} + \ldots + a_n \in /F_q[t][Y]$ this implies that $a_i = 0$ or $n \cdot \deg a_i \leq i \cdot \deg a_n$ for $1 \leq i \leq n-1$. (Argue on the unique valuation $\bar{v}_{t^{-1}}$ on L, extending $v_{t^{-1}}$).

Since $/F_q[t]$ is a principal ideal domain denote $p_i = (\pi_i)$, then $\{n_\mu\} = \{ \prod_{1 \leq i \leq l+k} \pi_i^{g_i} \mid 0 \leq g_i < n \}$.

LEMMA 7: *The only polynomials* $f_{\mu,\rho,(a_i)}(Y)$ *we must consider to calculate* t *and* h *are of the form:*

$$f_a(Y) = Y^n + (-1)^n e_\rho n_\mu \quad \textit{or} \quad f_a(Y) \in /F_q[Y].$$

PROOF: Fix $n_\mu = \prod_{j \in I} \pi_j^{g_j}$ with $g_j \neq 0$ if $j \in I$.

Then property ii) above implies that $a_i = 0$ or

$$\deg a_i \geq \sum_{j\in I} \deg\pi_j\left(1 + \left[\frac{ig}{n}\right]\right).$$

Assume $a_i \neq 0$, the remark above yields $n\cdot\deg a_i \leq i\cdot\deg a_n$, for $I \neq \emptyset$ we find a contradiction and for $I = \emptyset$ we deduce that $a_i \in /F_q$ for $1 \leq i \leq n-1$. //

Since every $L \in V_L^o$ is a separable extension, the condition (char K,n) = 1 is not needed to calculate h. However if $V_L \neq V_L^o$ then the condition is necessary to calculate t.

In order to make the formulas more explicit, we must calculate $m_T(S)$ for $S \in V_S$. For maximal orders $m_p(S) = 0$ or 1, cf. [N], Satz 4,4. Now we calculate $m_p(S), p|D_2$ in a special case:
Fix $f_a(Y) \in R[Y]$ an irreducible polynomial of degree n and $p|D_2$ with $p \nmid \mathrm{disc}(a)$. Remark that p doesn't ramify in $L = K(a)$. For $S_p = R_p(a)$ the unique R_p-order in L_p containing a, we calculate $m_p(S)$.
The decomposition of $\bar{f}_a(Y)$ in irreducible factors over $\bar{R} = R_p/p$ is $\bar{f}_a(Y) = \overline{g_1}(Y)\ldots\overline{g_s}(Y)$ with $(\overline{g_i},\overline{g_j}) = 1$.

By Hensel's lemma, the decomposition of $f_a(Y)$ in irreducible factors over R_p is $f_a(Y) = g_1(Y)\ldots g_s(Y)$.
We obtain that $\sum_{1\leq i\leq s} m_i = n$ where $m_i = \deg g_i(Y) =$

$= \deg \overline{g_i}(Y)$.

Assume that $a \in \Theta_p = \Theta_{p,s}^{(n_j)}$ then it follows from p 2 that $\overline{f_a}(Y) = \overline{q_1}(Y)\ldots\overline{q_r}(Y)$ with $\deg q_j = n_j$. Since $\overline{g_i}(Y)$ are the irreducible factors of $\overline{f_a}(Y)$ we conclude $\overline{q_j}(Y) = \overline{g_{i_1}}(Y)\ldots\overline{g_{i_k}}(Y)$ and $n_j = \sum_{1\le l\le k} m_{i_l}$.

DEFINITION: i) We say that (m_i) is a *refinement of* (n_j) iff there exists a function k: $\{0,\ldots,r\} \to \{0,\ldots,s\}$ with $0 = k(0) < k(1) <\ldots< k(r) = s$ such that $(m_{k(j-1)+1},\ldots,m_{k(j)})$ is a partition of n_j for $1 \le j \le r$;

ii) Two refinements (m_i), $(m_{\sigma(i)})$ of (n_j) with $\sigma \in S_s$ *are essentially equal* iff $k(j) = \sigma(k(j))$ and the sets $\{k(j-1)+1,\ldots,k(j)\} = \{\sigma(k(j-1)+1,\ldots,\sigma(k(j))\}$ are equal for every $j \in \{1,\ldots,r\}$.

Remark that for $r = 1$ all refinements (m_i) of (n_j) are essentially equal. Furthermore the remarks above provide that every embedding of a in Θ_p yields a refinement (m_i) of (n_j).

Conversely, let (m_i) be a refinement of (n_j), then we define the '*standard embedding*' of a in $\Theta_p = \Theta_{p,s}^{(n_j)}$ corresponding to this refinement as follows:

Fix $(\alpha_i) \in M_{m_i}(R_p)$ with $g_i(\alpha_i) = 0$, then the standard embedding ϕ_s is given by $\phi_s(a) = \begin{bmatrix} (\alpha_1) & & 0 \\ & \ddots & \\ 0 & & (\alpha_s) \end{bmatrix}^{(m_i)}$.

Since (m_i) is a refinement of (n_j), we find $\phi_s(a) \in \Theta_p$.

LEMMA 8: *For* $p|D_2$, *satisfying the property* $p \nmid \mathrm{disc}(a)$ *and* $\alpha \in \Theta_p = \Theta_{p,s}^{(n_j)}$, *denote* $S_p = \Theta_p \cap K_p(a)$, *then the number of essentially different refinements* $(m_{\sigma(i)})$ *of* (n_j) *is equal to* $\delta_{\min} \cdot m_p(S)$ *with* $\delta_{\min} = n$ *if* $r = n$, $\delta_{\min} = 1$ *else.*

PROOF, cf. [D] theorem IV.4.

COROLLARY 9. *Let* Θ *be a hereditary* $/F_q[t]$*-order and* $p|D_2$ *with* $(n_j) = (n_1,\ldots,n_r)$ *the local invariants of* Θ_p; *let* $K = /F_q(t)$.

i) *For* $S = /F_{q^n}[t]$: $m_p(S) \neq 0$ *iff* $\varphi_p \equiv 0 \mod n$ *and in this case* $m_p(S) \cdot \delta_{\min} = \frac{n!}{n_1! \ldots n_r!}$.

ii) *For* $L = /F_q(t)(a)$ *with* $a^n = c \in R$, $p \nmid c$, $(\mathrm{char}\ K, n) = 1$ *and* $S_p = R_p[a]$, *let* f *be the order of* $q^{\varphi}p \mod n$ *then* $m_p(S) \neq 0$ *iff* $c \in (K_p^*)^n$ *and there exist* $s_1,\ldots,s_r \in \mathbb{N}$ *such that* $(n_j) = (s_j)$ *if* $f = 1$ *or* $(n_j) = (1 + s_1 f, s_2 f, \ldots, s_r f)$ *up to a cyclic permuta-*

tion if $f \neq 0$, *and then:*

$$m_p(S)\cdot\delta_{min} = \frac{s!}{s_1!\ldots s_r!} \text{ with } s = \sum_{1\le i\le r} s_i$$

PROOF: The conditions of lemma 8 are satisfied and the degrees of the irreducible components of $f_a(Y)$ over $\bar{R}$ are:

i) $(m_i) = (n)$ if $\varphi_p \not\equiv 0 \bmod n$ and $(m_i) = (1,\ldots,1)$ else.

ii) $(m_i) = (n)$ if $c \notin (K_p^*)^n$ and $(m_i) = (1,f,\ldots,f)$ else.

Applying lemma 8 the result follows. //

In view of lemma 7, all the terms in the formula for t and h can be calculated explicitly.
As an example we simplify the expression to calculate h.
Counting the $/F_q n$ - rational points, it follows that

$$\#V_L^o = \frac{n}{q-1}\cdot\frac{q^n(q^{n-1}-1)}{n} \quad \text{or} \quad V_L^o = \emptyset, \text{ cf. [D 3], and}$$

for each $L \in V_L^o$ there is a unique $/F_q[t]$-order $S = /F_{q^n}[t]$.
For this ring $h_S = 1$, $(S^* : R^*) = \frac{q^n - 1}{q - 1}$, $E_{D_1D_2}(S) = n^{1+k}$

and $m_T(S) = 0$ or $m_T(S) = n^{-k} \prod_{p|D_2} \frac{n!}{n_1!\ldots n_r!}$. We obtain:

$$h = M_\Theta(S) + \delta\left(1 - \frac{q-1}{q^n-1}\right)n^1 \prod_{p|D_2} \frac{n!}{n_1!\ldots n_r!} \quad \text{with}$$

$$\delta = \begin{cases} 0 & \text{if } \varphi_p \equiv 0 \mod n \text{ for } p \in S_{ram} \text{ or} \\ & \varphi_p \not\equiv 0 \mod n \text{ for } p \mid D_2 \\ 1 & \text{else} \end{cases}$$

This formula can be obtained more directly from the Weight formula for stably free Θ-ideals, cf. [DVG 2].

We conclude with some explicit examples.

EXAMPLE 1: $n = 3$, $D_1 = t^6(t+1)^6$, $D_2 = 1$

$$h_{D_1D_2} = \frac{(q^2 - 1)(q - 1)}{q^2 + q + 1} + 3\,\frac{q^2 + q}{q^2 + q + 1} = q + 1$$

$$t_{D_1D_2} \begin{cases} = \frac{q + 1}{3} & \text{if } q \equiv 2 \mod 3 \ (\delta_n = 1) \\ = \frac{q + 5}{3} & \text{if } q \equiv 1 \mod 3 \ (\delta_n = 3) \end{cases}$$

EXAMPLE 2: $n = 3$, $q \neq 2$, $D_1 = t^6(t+1)^6$, $D_2 = (t+2)^{(1,2)}$

$$h_{D_1D_2} = M_\Theta(S) = q^3 - q^2 - q + 1$$

$$t_{D_1D_2} = \frac{q^3 - q^2 + q + 3}{9} \quad \text{if} \quad q \equiv 2 \mod 3$$

If $q \equiv 1 \mod 3$, the calculation of $t_{D_1D_2}$ depends on q, for $q = 7$ we obtain $t_{D_1D_2} = 36$.

EXAMPLE 3: $n = 3$, $q \neq 2$, $D_1 = t^6(t+1)^6$, $D_2 = (t+2)^{(1,1,1)}$

$h_{D_1D_2} = M_\Theta(S) = q^4 - 2q^2 + 1$

The calculation of $t_{D_1D_2}$ depends on q, for q = 5 we obtain $t_{D_1D_2} = 28$ and for q = 7 we find $t_{D_1D_2} = 104$ ...

REFERENCES

[DVG 1] DENERT, M. - VAN GEEL, J., *Cancellation property for orders in Non Eichler division algebras over global function fields*. J. reine angew. Math. 368, p 165-171, 1986.

[DVG 2] DENERT, M. - VAN GEEL, J., *The classnumber of hereditary orders in Non Eichler algebras over global function fields*. Math. Annalen 282, 1988.

[DVG 3] DENERT, M. - VAN GEEL, J., Orders, in quaternion algebras over global function fields, having the cancellation property. J. of Number Theory 30, p.321-333, 1988.

[D 1] DENERT, M., Orders, in Non Eichler (R)-algebras over global function fields, having the cancellation property. To appear in Mathematica Scandinavica.

[D 2] DENERT, M., *The genus zeta function of hereditary orders in central simple algebras over global*

function fields. To appear in Mathematics of Computation.

[D 3] DENERT, M., Affine and projective orders in central simple algebras over global function fields. Thesis Genth, 1987.

[N] HOETHER, E., *Zerfallende verschrankte Produkte und ihre Maximalordnungen*. Actualités Scientif. et indus. 148, p 5-15, 1934.

[P] PIZER, A., *Type numbers of Eichler orders*. J. reine angew. Math 264, p. 76-102, 1973.

[R] REINER, I., *Maximal orders*. Academic Press, New York, 1975.

[V] VIGNERAS, M. F., *Arithmétique des Algèbres de Quaternions*. Springer LNM 800, Berlin-Heidelberg-New York, 1980.

DENERT, M.
Seminary of Algebra and Functional Analysis
Galglaan 2
B-9000 Ghent, B e l g i u m

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

SOME REMARKS ON BEUKERS' INTEGRALS

DVORNICICH, R. and VIOLA, C.

1. INTRODUCTION

1.1. In [3] Beukers gives an elegant proof of Apéry's theorem [2] on the irrationality of $\zeta(2) = \sum_1^\infty n^{-2} = \pi^2/6$ (which is of course known to be transcendental) and $\zeta(3) = \sum_1^\infty n^{-3}$. Beukers considers the integrals

$$(1) \qquad I_n^{(o)} = \int_0^1 \int_0^1 \frac{P_n(x)(1-y)^n}{1 - xy}\, dx\, dy$$

for $\zeta(2)$ and

$$(2) \qquad I_n^{(1)} = \int_0^1 \int_0^1 \frac{-\log xy}{1 - xy} P_n(x)P_n(y)dx\,dy$$

for $\zeta(3)$, where P_n denotes the n-th Legendre polynomial defined by

$$(3) \qquad P_n(x) = \frac{1}{n!} \frac{d^n}{dx^n} \{x^n(1-x)^n\} .$$

It is easy to see that Beukers' method can be generalized to obtain the following conditional statement on the values of the Riemann zeta-function at positive integers:

Let k *be a non-negative integer. If there exist a constant* $\rho = \rho(k) > e^{k+2}$ *and a sequence of polynomials*

$$F_n(x,y) = \sum_{r,s=0}^{n} a_{rs}x^r y^s$$

with integer coefficients a_{rs} *(depending on* n *and* k*) such that*

$$0 \neq \left|I_n^{(k)}\right| \ll_k \rho^{-n} \quad (n\to\infty) ,$$

where

$$I_n^{(k)} = \int_0^1 \int_0^1 \frac{(-\log xy)^k}{k!(1-xy)} F_n(x,y)dx\,dy ,$$

then $\zeta(k+2)$ *is irrational.*

On choosing $F_n(x,y) = P_n(x)(1-y)^n$ for $k = 0$ and $F_n(x,y) = P_n(x)P_n(y)$ for $k = 1$, one sees that $\left|I_n^{(0)}\right| << \left\{\frac{\sqrt{5}+1}{2}\right\}^{-5n}$ and $\left|I_n^{(1)}\right| << (\sqrt{2}+1)^{-4n}$, thereby proving the irrationality of $\zeta(2)$ and $\zeta(3)$, since $\left\{\frac{\sqrt{5}+1}{2}\right\}^5 > e^2$ and $(\sqrt{2}+1)^4 > e^3$. Unfortunately, for every $k \geq 2$ the existence of polynomials $F_n(x,y)$ satisfying the above conditions is undecided.

1.2. The integrals (1) and (2) yield the sequences of rational approximations to $\zeta(2)$ and $\zeta(3)$ previously found by Apéry through a different method, thus giving the same bounds explicitly obtained in [2] for the irrationality measures of these numbers.

We recall the following definition. For an irrational number α, let $M(\alpha)$ denote the set of positive real numbers μ for which there exists $q_o = q_o(\alpha,\mu) > 0$ such that

$$\left|\alpha - \frac{p}{q}\right| > q^{-\mu}$$

for all integers p and q with $q > q_o$. The irrationality measure of α is defined to be the number

$$\mu(\alpha) = \inf M(\alpha) .$$

Clearly $\mu(\alpha) \geq 2$, and $\mu(\alpha) = 2$ for almost all irrational α.

Apéry's results are the following:

$$(4) \qquad \mu(\zeta(2)) = \mu(\pi^2) \leq 11.85078...$$

$$(5) \qquad \mu(\zeta(3)) \leq 13.41782... \qquad .$$

It is perhaps of some interest to remark that Beukers' method, being apparently simpler and more natural, suggests the possibility of improving the inequalities (4) and (5) by introducing suitable linear combinations with integer coefficients of the integrals (1) or (2).

We shall give simple proofs of the following:

THEOREM 1. $\mu(\zeta(2)) \leq 10.02979...$

THEOREM 2. $\mu(\zeta(3)) \leq 12.74359...$.

For $\zeta(2)$, D. and G. Chudnovsky [4] announced $\mu(\zeta(2)) \leq 7.325$ (without proof). G. Rhin [5] kindly informed us that he has independently obtained $\mu(\zeta(2)) \leq 8.367...$ (unpublished) by a method similar to ours in principle, but more elaborate.

We are unaware of any improvement on Apéry's inequality (5) for $\mu(\zeta(3))$.

We remark that the bounds for $\mu(\zeta(2))$ and $\mu(\zeta(3))$ obtained in Theorems 1 and 2 are effective.

1.3. It is natural to remark that the following integrals of Beukers' type:

$$\int_0^1 \cdots \int_0^1 \frac{F_n(x_1,\ldots,x_m)}{1 - x_1 \cdots x_m}\, dx_1 \ldots dx_m ,$$

where $F_n(x_1,\ldots,x_m) \in \mathbf{Z}[x_1,\ldots,x_m]$, give linear combinations of 1, $\zeta(2)$, $\zeta(3),\ldots,\zeta(m)$ with rational coefficients. One then expects that good choices for the polynomials $F_n(x_1,\ldots,x_m)$ might lead to some results on the linear independence of 1, $\zeta(2),\ldots,\zeta(m)$ over $\mathbf{Q}$.

For simplicity, we shall confine ourselves to the case $m = 3$. As an instance, we shall prove:

THEOREM 3. *At least one of the following two statements holds:*

(i) 1, $\zeta(2)$ *and* $\zeta(3)$ *are linearly independent over* $\mathbf{Q}$;

(ii) $\mu(\zeta(2)) = \mu(\zeta(3)) \leq 7.04826\ldots$.

2. A LEMMA

Given an irrational number α, one usually obtains upper bounds for $\mu(\alpha)$ by proving sufficiently good estimates for $\left|q_m\alpha - p_m\right|$, where p_m/q_m is a suitable sequence of rational approximations to α. This well-known principle can be formulated in several ways. The following is appropriate for our purposes.

LEMMA. *Let α be irrational, and let Q_m be a real sequence such that*

$$\lim_{m\to\infty} Q_m = \infty$$

and

$$Q_{m+1} \ll Q_m^{1+\varepsilon} \quad \text{for any} \quad \varepsilon > 0 \ .$$

Further, let p_m/q_m be a sequence of rational numbers satisfying

$$0 < q_m \le Q_m$$

and

$$Q_m^{-\xi-\varepsilon} \ll \left|q_m\alpha - p_m\right| \ll Q_m^{-\xi+\varepsilon}$$

for a suitable ξ such that $0 < \xi \le 1$ and any $\varepsilon > 0$. Then

$$\mu(\alpha) \le \frac{1}{\xi} + 1 \ .$$

We omit the proof of the lemma. A similar proof is given in [1], lemma 3, where the condition $p_m q_{m+1} \neq q_m p_{m+1}$ replaces our lower bound for $|q_m\alpha - p_m|$.

3. PROOF OF THEOREM 1

We recall (see [3]) that, by repeated partial integration, the integral (1) becomes

$$I_n^{(o)} = (-1)^n \int_0^1 \int_0^1 f_o^n(x,y) \frac{dxdy}{1-xy} ,$$

where

$$f_o(x,y) = \frac{x(1-x)y(1-y)}{1 - xy} .$$

Let

$$\beta_o = \max_{0\leq x,y\leq 1} f_o(x,y) .$$

An easy calculation shows that $\beta_o = \left(\frac{\sqrt{5} - 1}{2}\right)^5$.

Defining

$$\alpha_o = \frac{1}{\beta_o} = \left(\frac{\sqrt{5}+1}{2}\right)^5$$

and

$$d_n = \ell.c.m. \{1,2,\ldots,n\} ,$$

we have

$$(6) \qquad d_n^2 I_n^{(o)} = A_n^{(o)} \zeta(2) + B_n^{(o)} \qquad (A_n^{(o)}, B_n^{(o)} \in Z)$$

with

$$A_n^{(o)} = d_n^2 \sum_{r=0}^{n} \binom{n}{r}^2 \binom{n+r}{r} \ll d_n^2 \, \alpha_o^n \,, \tag{7}$$

by a straightforward application of Stirling's formula. Also, by the Prime Number Theorem,

$$d_n = e^{\psi(n)} = e^{n+o(n)} \,.$$

Clearly

$$\beta_o^{(1+\varepsilon)n} \ll_\varepsilon \left| I_n^{(o)} \right| \ll \beta_o^n \,, \tag{8}$$

so that the Lemma is applicable with $Q_n = (e^{2+\varepsilon}\alpha_o)^n$ and ξ given by the equation

$$(e^2 \, \alpha_o)^{-\xi} = e^2 \beta_o = \frac{e^2}{\alpha_o} \,.$$

This yields

$$\mu(\zeta(2)) \leq \frac{2 \log \alpha_o}{\log \alpha_o - 2} \,,$$

i.e. Apéry's result (4).

We improve upon this by choosing suitable polynomials $R(t) \in \mathbf{Z}[t]$, $R(t) = \sum_{h=0}^{N} c_h t^h$, so that the integrals

$$\int_0^1 \int_0^1 R(f_o(x,y)) \frac{dx\,dy}{1-xy} = \sum_{h=0}^{N} c_h \int_0^1 \int_0^1 f_o^h(x,y) \frac{dx\,dy}{1-xy}$$

$$= \sum_{h=0}^{N} (-1)^h c_h I_h^{(o)}$$

give better rational approximations to $\zeta(2)$.

For $R(t) = R_{m,n;p,q}(t) = t^n(p-qt)^m$, we obtain

$$J_{m,n}^{(o)} = J_{m,n;p,q}^{(o)} = (-1)^n \int_0^1 \int_0^1 R(f_o(x,y)) \frac{dx\,dy}{1-xy}$$

$$= \sum_{h=0}^{m} \binom{m}{h} p^{m-h} q^h I_{n+h}^{(o)} .$$

Moreover, by (6),

$$(9) \qquad d_{n+m}^2 J_{m,n}^{(o)} = \sum_{h=0}^{m} \binom{m}{h} p^{m-h} q^h \left(\frac{d_{n+m}}{d_{n+h}}\right)^2 (d_{n+h}^2 I_{n+h}^{(o)})$$

$$= \sum_{h=0}^{m} \binom{m}{h} p^{m-h} q^h \left(\frac{d_{n+m}}{d_{n+h}}\right)^2 (A_{n+h}^{(o)} \zeta(2) + B_{n+h}^{(o)})$$

$$= C_{m,n}^{(o)} \zeta(2) + D_{m,n}^{(o)} ,$$

with $C^{(o)}_{m,n}$, $D^{(o)}_{m,n} \in \mathbf{Z}$.

Let $n = \lambda m$, and let p, q be such that $\beta_o < \frac{p}{q}$. Then $R(f_o(x,y)) \geq 0$, and we have the following analogue of (8):

$$\gamma_o^{(1+\varepsilon)m} \ll_\varepsilon \left|J^{(o)}_{m,\lambda m}\right| \ll \gamma_o^m ,$$

where

$$\gamma_o = \max_{0 \leq f_o \leq \beta_o} f_o^\lambda (p - q f_o) = \left(\frac{\lambda}{q}\right)^\lambda \left(\frac{p}{\lambda+1}\right)^{\lambda+1} .$$

One of course expects γ_o to be small, provided the factor $p - qf_o$ is small for $f_o = \beta_o$, i.e. p/q is a good approximation to β_o.

From (7) and (9) we get

$$C^{(o)}_{m,\lambda m} = d^2_{(\lambda+1)m} \sum_{h=0}^{m} \binom{m}{h} p^{m-h} q^h \frac{A^{(o)}_{\lambda m+h}}{d^2_{\lambda m+h}}$$

$$\ll d^2_{(\lambda+1)m} \alpha_o^{\lambda m} \sum_{h=0}^{m} \binom{m}{h} p^{m-h} q^h \alpha_o^h$$

$$\ll \left\{ e^{(2+\varepsilon)(\lambda+1)} \alpha_o^\lambda (p + q\alpha_o) \right\}^m .$$

Hence we may apply the Lemma with

$$Q_m = \left\{ e^{(2+\varepsilon)(\lambda+1)} \; \alpha_o^{\lambda}(p+q\alpha_o) \right\}^m$$

and ξ defined by

$$\left\{ e^{2(\lambda+1)} \alpha_o^{\lambda}(p+q\alpha_o) \right\}^{-\xi} = e^{2(\lambda+1)} \left(\frac{\lambda}{q}\right)^{\lambda} \left(\frac{p}{\lambda+1}\right)^{\lambda+1} .$$

It is easy to see that, for any fixed λ, the best value of ξ is obtained for $p = 1$, $q = 11$ (note that $1/11$ is the first convergent in the continued fraction for β_o). With these choices, the maximum of $\xi = \xi(\lambda)$ is taken on at $\lambda_o = 14.18764...$. Letting $n = [\lambda_o m]$, we obtain

$$\mu(\zeta(2)) \leq 10.45494... .$$

To prove the stronger inequality of Theorem 1, we choose

$$R(t) = t^{2k} \; (1-11t)^{2n} \; (1-12t)^{2m} ,$$

with

$$k = [\lambda_1 m] , \quad n = [\nu_1 m] ,$$

$$\lambda_1 = 18.53172... , \; \nu_1 = 1.38784... .$$

An argument entirely similar to the above now gives

$$\mu(\zeta(2)) \leq 10.02979... .$$

4. PROOF OF THEOREM 2

We only sketch the proof of Theorem 2, since the arguments are similar to the proof of Theorem 1. As in [3], we have

$$I_n^{(1)} = \int_0^1 \int_0^1 \int_0^1 f_1^n(x,y,z) \, \frac{dx\,dy\,dz}{1-(1-xy)z}$$

where

$$f_1(x,y,z) = \frac{x(1-x)y(1-y)z(1-z)}{1-(1-xy)z} \ ,$$

and

$$\beta_1 = \max_{0\le x,y,z\le 1} f_1(x,y,z) = (\sqrt{2}-1)^4 \ .$$

Also,

$$d_n^3 \, I_n^{(1)} = A_n^{(1)} \zeta(3) + B_n^{(1)} \quad (A_n^{(1)}, \, B_n^{(1)} \in \mathbb{Z})$$

and

$$A_n^{(1)} \ll d_n^3 \, \alpha_1^n \ ,$$

where $\alpha_1 = \frac{1}{\beta_1} = (\sqrt{2}+1)^4$. The second convergent in the continued fraction for β_1 is $1/34$. Defining now

$$R(t) = R_{m,n}(t) = t^{2n}(1-34t)^{2m}$$

and

$$J_{m,n}^{(1)} = \int_0^1 \int_0^1 \int_0^1 R(f_1(x,y,z)) \frac{dx\,dy\,dz}{1-(1-xy)z} ,$$

we have

$$d_{2n+2m}^3 J_{m,n}^{(1)} = C_{m,n}^{(1)} \zeta(3) + D_{m,n}^{(1)} \quad (C_{m,n}^{(1)}, D_{m,n}^{(1)} \in \mathbf{Z}) .$$

Letting $n = \lambda m$, we obtain

$$\gamma_1^{(1+\varepsilon)m} \ll_\varepsilon \left| J_{m,\lambda m}^{(1)} \right| \ll \gamma_1^m ,$$

where

$$\gamma_1 = \left\{ \left(\frac{\lambda}{34}\right)^\lambda \left(\frac{1}{\lambda+1}\right)^{\lambda+1} \right\}^2 ,$$

since

$$\left(\frac{\lambda}{34}\right)^\lambda \left(\frac{1}{\lambda+1}\right)^{\lambda+1} > \beta_1^\lambda (34\ \beta_1 - 1)$$

for $\lambda \leq 100$, say. A crude estimate gives

$$\left| C_{m,\lambda m}^{(1)} \right| \ll \left\{ e^{(3+\varepsilon)(\lambda+1)}\ \alpha_1^\lambda (1+34\alpha_1) \right\}^{2m} .$$

We apply the Lemma with

$$Q_m = \left\{ e^{(3+\varepsilon)(\lambda+1)}\ \alpha_1^\lambda (1+34\alpha_1) \right\}^{2m}$$

and ξ defined by

$$\left\{e^{3(\lambda+1)}\ \alpha_1^{\lambda}(1+34\alpha_1)\right\}^{-\xi} = e^{3(\lambda+1)}\ \left(\frac{\lambda}{34}\right)^{\lambda}\left(\frac{1}{\lambda+1}\right)^{\lambda+1}.$$

For $n = [\lambda_o^{(1)} m]$, $\lambda_o^{(1)} = 45.72151...$, we have

$$\mu(\zeta(3)) \leq 12.90791... \quad .$$

On choosing

$$R(t) = t^{2k}(1-34t)^{2n}(1-35t)^{2m} \quad ,$$

with

$$k = [\lambda_1^{(1)} m] \ , \ n = [\nu_1^{(1)} m] \ ,$$

$$\lambda_1^{(1)} = 56.41... \ , \ \nu_1^{(1)} = 1.342 \quad ,$$

we obtain

$$\mu(\zeta(3)) \leq 12.74359... \quad .$$

5. PROOF OF THEOREM 3

As remarked in the Introduction, an integral of the type

$$\int_0^1 \int_0^1 \int_0^1 \frac{F(x,y,z)}{1 - xyz}\, dx\, dy\, dz \ ,$$

where $F(x,y,z) \in \mathbf{Z}[x,y,z]$, gives a linear combination of 1, $\zeta(2)$ and $\zeta(3)$ with rational coefficients. More precisely, every monomial $x^r y^s z^t$ contributes to the above integral as follows:

$$M_{rst} = \int_0^1 \int_0^1 \int_0^1 \frac{x^r y^s z^t}{1 - xyz}\, dx\, dy\, dz =$$

$$= \int_0^1 \int_0^1 \int_0^1 x^r y^s z^t \sum_{h=0}^{\infty} (xyz)^h\, dx\, dy\, dz$$

$$= \sum_{h=0}^{\infty} \int_0^1 x^{r+h} dx \int_0^1 y^{s+h} dy \int_0^1 z^{t+h} dz$$

$$= \sum_{j=1}^{\infty} \frac{1}{(r+j)(s+j)(t+j)} \quad .$$

We may assume $r \geq s \geq t$. If $r = s = t$, then

$$M_{rrr} = \sum_{\nu=r+1}^{\infty} \frac{1}{\nu^3} = \zeta(3) - \sum_{\nu=1}^{r} \frac{1}{\nu^3} \quad .$$

If $r > s > t$, then

$$M_{rst} = \frac{1}{(r-s)(s-t)} \sum_{j=1}^{\infty} \left(\frac{1}{t+j} - \frac{1}{s+j} \right)$$

$$- \frac{1}{(r-s)(r-t)} \sum_{j=1}^{\infty} \left(\frac{1}{t+j} - \frac{1}{r+j} \right)$$

$$= \frac{1}{(r-s)(s-t)} \sum_{\nu=t+1}^{s} \frac{1}{\nu} - \frac{1}{(r-s)(r-t)} \sum_{\nu=t+1}^{r} \frac{1}{\nu} \ .$$

If $r = s > t$, then

$$M_{rrt} = \frac{1}{(r-t)^2} \sum_{j=1}^{\infty} \left(\frac{1}{t+j} - \frac{1}{r+j} \right) - \frac{1}{r-t} \sum_{j=1}^{\infty} \frac{1}{(r+j)^2}$$

$$= \frac{1}{(r-t)^2} \sum_{\nu=t+1}^{r} \frac{1}{\nu} - \frac{1}{r-t} \left(\zeta(2) - \sum_{\nu=1}^{r} \frac{1}{\nu^2} \right) \ .$$

Similarly, if $r > s = t$, then

$$M_{rtt} = \frac{1}{r-t} \left(\zeta(2) - \sum_{\nu=1}^{t} \frac{1}{\nu^2} \right) - \frac{1}{(r-t)^2} \sum_{\nu=t+1}^{r} \frac{1}{\nu} \ .$$

Therefore, if $F(x,y,z) = \sum_{r,s,t=0}^{n} a_{rst} x^r y^s z^t$, $a_{rst} \in \mathbf{Z}$, then the product

$$d_n^3 \int_0^1 \int_0^1 \int_0^1 \frac{F(x,y,z)}{1 - xyz} \, dx \, dy \, dz$$

is a linear combination of 1, $\zeta(2)$ and $\zeta(3)$ with integer coefficients.

We now choose

$$F(x,y,z) = P_n(x)(1-y)^n(1-z)^n \ ,$$

where $P_n(x)$ is defined by (3). Then

$$H_n = \int_0^1 \int_0^1 \int_0^1 \frac{P_n(x)(1-y)^n(1-z)^n}{1 - xyz}\, dx\, dy\, dz$$

$$= \int_0^1 \int_0^1 \cdot (1-y)^n(1-z)^n dy\, dz \int_0^1 \frac{P_n(x)}{1-xyz}\, dx$$

$$= (-1)^n \int_0^1 \int_0^1 \int_0^1 \frac{x^n(1-x)^n y^n(1-y)^n z^n(1-z)^n}{(1 - xyz)^{n+1}}\, dx\, dy\, dz,$$

by repeated partial integration.

Let

$$g(x,y,z) = \frac{x(1-x)y(1-y)z(1-z)}{1- xyz} ,$$

and

$$\eta = \max_{0\le x,y,z\le 1} g(x,y,z) .$$

It is easy to see that

$$\eta = \frac{x_o^3(1-x_o)^3}{1 - x_o^3} ,$$

where $0 < x_o < 1$, $x_o^3 + x_o^2 + x_o - 1 = 0$. One finds

$\eta = 0.01819...$.

We have

(10) $$\eta^{(1+\varepsilon)n} \ll_\varepsilon \left|H_n\right| \ll \eta^n .$$

Writing, as above,

$$P_n(x)(1-y)^n(1-z)^n = \sum_{r,s,t=0}^{n} a_{rst} x^r y^s z^t$$

and

$$d_n^3 H_n = S_n \zeta(3) + T_n \zeta(2) + U_n \quad , \tag{11}$$

we get

$$a_{rst} = (-1)^{r+s+t} \binom{n}{r}\binom{n}{s}\binom{n}{t}\binom{n+r}{r} \quad ,$$

$$S_n = d_n^3 \sum_{r=0}^{n} (-1)^r \binom{n}{r}^3 \binom{n+r}{r} \quad ,$$

$$T_n = d_n^3 \sum_{r=0}^{n} \sum_{s \neq r} \frac{(-1)^s}{s-r} \binom{n}{r}^2 \binom{n}{s} \left\{ 2\binom{n+r}{r} + \binom{n+s}{s} \right\} \quad .$$

Again by Stirling's formula we obtain

$$|S_n| \ll d_n^3 \, \theta^n \quad , \tag{12}$$

where $\theta = 21.74952...$ is the maximum of

$$\frac{(1+t)^{1+t}}{t^{4t}(1-t)^{3-3t}}$$

for $0 < t < 1$. Similarly, since

$$n^2 \binom{n}{r}^2 \binom{n}{s}\binom{n+r}{r} \ll \left\{ 2\left(\frac{\sqrt{5}+1}{2} \right)^5 \right\}^n$$

and

$$n^2 \binom{n}{r}^2 \binom{n}{s} \binom{n+s}{s} \ll \left\{4(\sqrt{2}+1)^2\right\}^n ,$$

we have

$$|T_n| \ll d_n^3 \Phi^n , \tag{13}$$

where $\Phi = 4(\sqrt{2}+1)^2 = 23.29708\ldots$.

To prove Theorem 3, we now assume that 1, $\zeta(2)$ and $\zeta(3)$ are linearly dependent over $\mathbf{Q}$, so that there exist integers u, v, w ($u \neq 0$, $v \neq 0$) satisfying

$$u\zeta(3) + v\zeta(2) + w = 0 . \tag{14}$$

This clearly implies $\mu(\zeta(2)) = \mu(\zeta(3))$. Let

$$K_n = ud_n^3 H_n = ud_n^3 H_n - S_n(u\zeta(3) + v\zeta(2) + w).$$

We have, by (11),

$$K_n = V_n \zeta(2) + W_n ,$$

where

$$V_n = u T_n - v S_n ,$$

$$W_n = u U_n - w S_n .$$

Since $\Phi > \theta$, we have, by (12) and (13),

$$\left|V_n\right| \ll d_n^3 \, \Phi^n$$

and, since $u \neq 0$,

$$d_n^3 \, \eta^{(1+\varepsilon)n} \ll_\varepsilon \left|K_n\right| \ll d_n^3 \, \eta^n$$

by (10). We apply the Lemma with

$$Q_n = (e^{3+\varepsilon} \, \Phi)^n$$

and ξ defined by the equation

$$(e^3 \, \Phi)^{-\xi} = e^3 \, \eta \ .$$

This yields

$$\mu(\zeta(2)) \leq \frac{1}{\xi} + 1 = 7.10828.... \ .$$

To improve upon this we define

$$R(t) = R_{m,n}(t) = t^{2n}(1 - 55t)^{2m} \ ,$$

and

$$L_{m,n} = \int_0^1 \int_0^1 \int_0^1 R(g(x,y,z)) \, \frac{dx \, dy \, dz}{1 - xyz} \ .$$

Let, as before, $n = \lambda m$. One finds that the maximum of the corresponding function $\xi = \xi(\lambda)$ is taken on at

$\lambda_o = 106.699... \ .$

Assuming again (14), we obtain

$$\mu(\zeta(2)) \leq 7.04826.... \ .$$

This completes the proof of Theorem 3.

REFERENCES

[1] ALLADI, K. and ROBINSON, M.L., Legendre polynomials and irrationality, *J. reine angew. Math.* 318 (1980), 137-155.

[2] APÉRY, R., Irrationalité de $\zeta(2)$ et $\zeta(3)$, *Astérisque* 61 (1979), 11-13.

[3] BEUKERS, F., A note on the irrationality of $\zeta(2)$ and $\zeta(3)$, *Bull. London Math. Soc.* 11 (1979), 268-272.

[4] CHUDNOVSKY, D.V. and CHUDNOVSKY, G.V., Padé and rational approximations to systems of functions and their arithmetic applications, *Lect. Notes in Math.* 1052 (1984), 37-84.

[5] RHIN, G., private communication, May 1987.

Dipartimento di Matematica
Università di Pisa
Via Buonarroti, 2
56100 Pisa, Italy.

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

THE S-UNIT EQUATION AND DIRICHLET SERIES

EVEREST, G.R.

Suppose n is a square free integer. Let ζ_n denote a primitive nth root of unity and $L = \mathbf{Q}(\zeta_n)$. Write $\Gamma = \mathrm{Gal}(L|\mathbf{Q})$ then it is well known that the conjugates of ζ_n under Γ form a $\mathbf{Z}$-basis for o_L-the ring of algebraic integers of L. The set of all such generators is the Galois orbit

$$\zeta_n \cdot \mathbf{Z}\Gamma^x \tag{11}$$

where $\mathbf{Z}\Gamma^x$ denotes the units of the integral group ring $\mathbf{Z}\Gamma$ and $\cdot$ denotes the natural action of $\mathbf{Q}\Gamma$ on L. One knows that $L|\mathbf{Q}$ is a tame, abelain extension and our methods apply to this more general set-up viz.

$$\Gamma \left\{ \begin{array}{ccc} L & - & o_L \\ | & & | \\ Q & - & Z \end{array} \right. \text{ where } \quad o_L = a \cdot Z\Gamma \quad \text{for some } a \in o_L .$$

The orbit $a \cdot Z\Gamma^x$ gives rise to an S-unit equation. A study of these orbits was initiated by Bushnell in ([1], [2], [3]). In [4] we proved that for any $M > 0$, the inequality

$$|N_{L|Q}(a \cdot x)| < M \tag{2}$$

has only finitely many solutions $x \in Z\Gamma^x$. Define

$$l_a(s) = \sum_{x \in Z\Gamma^x} (\log|N_{L|Q}(a \cdot x)|)^{-s}, \quad s \in \mathbf{C}. \tag{3}$$

Note: in this paper it will be assumed that undefined terms have been omitted from any summation. For example, in the above this means only a finite number of terms and does not affect the type of result in which we are interested.

Before we state the theorem, recall Higman's theorem ([8]) which gives the structure of $Z\Gamma^x$,

$$Z\Gamma^x \cong \Gamma \times Z^{r_\Gamma} \tag{4}$$

where r_Γ is a non-negative integer, and $\Gamma = \{\pm\gamma : \gamma \in \Gamma\}$.

THEOREM: Let $\hat{\Gamma} = \mathrm{Hom}(\Gamma, C^x)$ denote the character group of Γ and suppose

$$L \cap \mathbb{Q}(\hat{\Gamma}) = \mathbb{Q}. \tag{5}$$

(i) $l_a(s)$ has half-plane of convergence $\mathrm{Re}(s) > r_\Gamma$

(ii) $l_a(s)$ has analytic continuation to $\mathrm{Re}(s) > r_\Gamma - 2$ where it is analytic apart from simple poles at $s = r_\Gamma$ and $s = r_\Gamma - 1$.

(iii) The residue at $s = r_\Gamma$ is independent of L while that at $s = r_\Gamma - 1$ looks like,

$$\Gamma_1 + \Gamma_2 b_L$$

where b_L depends on L and is defined in §3, Γ_1 and Γ_2 are (messy) group ring constans.

In §1 we will study the geometry of $Z\Gamma^x$ more closely and show how a spectral decomposition enables us to regard this problem as an S-unit equation. In §2 we will demonstrate the link with diophantine approximation, using our geometric results together with, in one case, Baker's theorem, and in another, W. Schmidt's subspace theorem. In §3 we will show how these ingredients are used to give the analytic continuation.

§1. Given $\chi \in \hat{\Gamma} = \mathrm{Hom}(\Gamma, \mathbf{C}^x)$ and $x = \Sigma\, x_\gamma\, \gamma \in \mathbf{C}\Gamma$, let

$$1_\chi(x) = \sum_{\gamma\in\Gamma} \chi(\gamma) x_\gamma$$

and

$$|x| = \max_{\chi\in\hat{\Gamma}} \{|1_\chi(x)|\}. \tag{6}$$

Also, write e_χ for the standard idempotent

$$e_\chi = |\Gamma|^{-1} \sum_{\gamma\in\Gamma} \bar{\chi}(\gamma)\gamma.$$

We say $\chi \in \hat{\Gamma}$ is *non-degenerate* if $\mathbf{Q}(x)$- the field generated by the values of χ - is not $\mathbf{Q}$ or an imaginary quadratic extension of $\mathbf{Q}$.

Let

$$E = \{\pm\delta(e_\chi + e_{\bar{\chi}}): \ \chi \text{ non-degenerate}, \ \delta \in \Gamma\}. \tag{7}$$

Also, write c_1 for the $|\ |$-unit ball,

$$c_1 = \{x \in \mathbf{C}\Gamma : |x| = 1\}. \tag{8}$$

Given $e_i \neq e_j \in E$ let

$$1_{ij} = e_i + te_j, \quad 0 \leq t \leq 1,$$

and let G denote the set of all l_{ij}. Suppose W is any open subset of c_1. Define,

$$l(s) = \sum_{x \in \mathbb{Z}\Gamma^x} (\log|x|)^{-s}, \tag{9}$$

$$l_w(s) = \sum_{\substack{x \in \mathbb{Z}\Gamma^x \\ x' \in W}} (\log|x|)^{-s}, \quad (\text{so } l(s) = l_{c_1}(s))$$

where $x' = x|x|^{-1}$ denotes the central projection of x into c_1.

PROPOSITION A. (i) $l_W(s)$ has half-plane of convergence $Re(s) > r_\Gamma$,

(ii) $l_W(s)$ has analytic continuation to $Re(s) > r_\Gamma - 2$

(iii) If $E \subset W$ then $l(s) - l_W(s)$ is analytic in $Re(s) > r_\Gamma - 1$

(iv) If $G \subset W$ then $l(s) - l_W(s)$ is analytic in $Re(s) > r_\Gamma - 2$

(These will appear in [6]).

Our aim is to use inequalities from diophantine approximation to compare $l_a(s)$ with the series above.

To obtain a spectral decompositisn define the *resolvent*

$$(a|\chi) = \sum_{\gamma \in \Gamma} a^{\gamma}\, \bar{\chi}(\gamma). \tag{10}$$

The orthogonality relations yield

$$a \cdot x = |\Gamma|^{-1} \sum_{\gamma \in \hat{\Gamma}} (a|\chi) 1_{\chi}(x) \quad \text{and therefore}$$

$$N_{L|Q}(a \cdot x) = \prod_{\delta \in \Gamma} (|\Gamma|^{-1} \sum_{\chi \in \hat{\Gamma}} (a|\chi) 1_{\chi}(x)). \tag{11}$$

Now it is easy to prove that for $x \in Z\Gamma$,

$$x \in Z\Gamma^{x} \text{ if and only if } \prod_{\chi \in \hat{\Gamma}} 1_{\chi}(x) = \pm 1. \tag{12}$$

Thus, by (11), (12), we are studying a special case of the S-unit equation.

Evertse's paper [7] discusses the general S-unit equation but his results are not applicable to our problem. We replace his bound by three separate bounds, two of which are superior for 'most' of the units (in the sense of the proposition). The third is inferior but it does not rely upon the non-vanishing sub-sum condition which, in this case, seems difficult to verify.

§2. There are three types of bound which are important here

PROPOSITION B: There exist open subsets of C_1, V and W where $E \subset V$, $G \subset W$ such that

(i) $\log|N_{L|Q}(a\cdot x)| = |\Gamma|\log|x| + b_{L,e} + 0(1/\log|x|)$

$\forall x \in Z\Gamma^x,$

$x' \in V \cap b_e,\ e \in E,$

and b_e denotes a sufficiently small ball about e.

(ii) $\log|N_{L|Q}(a\cdot x)| = |\Gamma|\log|x| + 0(\log\log|x|)$

$\forall\ x \in Z\Gamma^x,\ x' \in W$

(iii) $\log|N_{L|Q}(a\cdot x)| > \kappa\log|x| \quad \forall\ x \in Z\Gamma^x,$ where $\kappa > 0$.

No details are given here. In essence (i) follows by insisting that in each of the factors of $N_{L|Q}(a\cdot x)$ one term is very much larger than the others. In (ii) one allows two large terms but one can apply Baker's theorem. Part (iii) uses W. Schmidt's subspace theorem (see [5] for details).

§3. The proof is easier to describe in the case where $|\Gamma|$ is a prime so we make that assumption.

Given that

$$U = Z\Gamma^x \cong T \times Z^{r_\Gamma},$$

tensor with the reals,

$$U_R = U \otimes R.$$

Then the l_χ can be viewed as being defined on R^{r_Γ},

(and no longer on $R^{|\Gamma|}$!). Write

$$H(y) = \max_{\chi \in \hat{\Gamma}} \{|1_{\chi}(y)|\}, \quad y \in R^{r_\Gamma}. \tag{13}$$

Let 0 denote any open ball about the origin in R^{r_Γ}. Then one can prove([5]) that the function

$$I(s) = \int_{T=R^{r_\Gamma}-0} (\log H(y))^{-s}\, dy, \quad s \in \mathbf{C}, \tag{14}$$

is meromorphic in C with simple poles at $s = 1,\ldots,r_\Gamma$. Also, the residues of the poles at $s = r_\Gamma$, $r_\Gamma - 1$ are independent of the choice of 0. The function $I(s)$, (14), is used to give the analytic continuation of $1_a(s)$. It is clear that $T = \bigcup_{x \in Z^{r_\Gamma}} c_x \cap T$, where c_x denotes the (closed) unit cube with centre x. Now, for all $x \in Z\Gamma^x$ with $x' \in V$ one can use the mean value theorem to obtain

$$\int_{c_x \cap T} (\log H(y))^{-s}\, dy = (\log H(x))^{-s} + b_\gamma + 0\left\{\frac{1}{\log H(x)}\right\} \tag{15}$$

where the 0 means a function f which satisfies

$|f| \leq \frac{|g(s)|}{\log H(x)}$ where $g(s)$ is an analytic function.

Break the sum for $l_a(s)$ into three sums according as $x \in Z\Gamma^x$ satisfies:

$x' \in V$, $x' \in W - V$, $x' \notin W$, respectively S_1, S_2, S_3.

Then

$$S_1 - \sum_{\substack{x \in Z\Gamma^x \\ x' \in V}} \int (|\Gamma| \log H(y))^{-s} = C_x$$

$$= \sum_{\substack{x \in Z\Gamma^x \\ x' \in W-V}} (|\Gamma| \log |x|)^{-s} \{ 0\left[\frac{\log\log|x|}{\log|x|}\right] + 0\left[\frac{}{\log|x|^2}\right] \}$$

using Prop B.

Given any $\epsilon > 0$, this expands out to

$$\sum_{\substack{x \in Z\Gamma^x \\ x' \in W-V}} \frac{0(1)}{(\log|x|)^{s+1-\epsilon}}$$

and this is analytic in $\mathrm{Re}(s) > r_\Gamma - 2 + \epsilon$, by Prop A.

Finally, use Prop B to majorise S_3 by

$$\sum_{\substack{x \in Z\Gamma x \\ x' \in W}} \frac{0(1)}{(\log|x|)^s}$$

which is analytic for $\mathrm{Re}(s) > r_\Gamma - 2$, again by Prop A.

Thus, we have obtained the analytic continuation to $\mathrm{Re}(s) > r_\Gamma - 2$. It is straighforward to read off the singular behaviour at $s = r_\Gamma - 1$. The constant b_L is defined in the following way,

$$\exp(b_L) = \prod_{\chi n \cdot d} \{(a|\chi) + (a|\bar{\chi})\}^{1/2} \qquad (16)$$

where the product is over all non-degenerate $\chi \in \hat{\Gamma}$. The linear disjointness condition ensures that this expression does not vanish.

We have made two calculations of the number on the right hand side of (16).

1. $Q(\zeta_{11})$ — Here Γ is cyclic of order 5 and the number is $11^3 \cdot 109$

$L = Q(\cos\frac{2\pi}{11})$

Γ | Q

2. $Q(\zeta_{13})$ — Here Δ is the unique subgroup of order 6 of the Galois Group of $Q(\zeta_{31})/Q$. So again, L/Q is a quintic. This time the number is

Δ | L | Q

$$31^3 \cdot 719$$

In both cases, the first factor can be predicted using the Stickelberger relations. The second factor is not so easy to interpret.

REFERENCES

[1] BUSHNELL, C.J., Norms of normal integral generators, *J. London Math. Soc.* (2) 15 (1977), 199-209.

[2] BUSHNELL, C.J., Norm distribution in Galois orbits, *J. reine angew. Math.* 310 (1979), 81-99.

[3] BUSHNELL, C.J., Diophantine approximation and norm distribution in Galois orbits, *Illinois J. Math.* 27 (1983), 145-157.

[4] EVEREST, G.R., Diophantine approximation and the distribution of normal integral generators, *J. London Math. Soc.* (2) 28 (1983), 227-237.

[5] EVEREST, G.R., Angular distribution of units in abelian group rings - an application to Galois module theory, *J. reine angew. Math.* 375 (1987), 24-41.

[6] *Units in abelian group rings and meromorphic functions*, to appear in *Illinois J.Math.* (1989).

[7] EVERTSE, J.-H., On sums of S-units and linear recurrences, *Compositio Math.* 53 (1984), 225-244.

[8] SEHGAL, S., Topics in group rings, New York, 1978.

EVEREST. G.R..
School of Mathematics and Physics, University of East Anglia
Norwich NR4 7TJ

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, (HUNGARY), 1987

ON THE NUMBERS OF SOLUTIONS OF UNIT EQUATIONS AND DECOMPOSABLE POLYNOMIAL EQUATIONS

EVERTSE J.H.* (Amsterdam)*** and GYŐRY K.** (Debrecen)

§ 1. INTRODUCTION

The unit equations and decomposable form equations play an important role in several branches of number theory. The theory of unit equations and the theory of decomposable form equations are in fact equivalent. In 1986, Evertse, Győry, Stewart and Tijdeman [13] and Evertse and Győry [10] gave general surveys on unit equations and decomposable form equations, respectively, as

*) Research supported by the Netherlands Organization for the Advancement of Pure Research (Z.W.O.).

**) Research supported in part by Grant 273 from the Hungarian National Foundation for Scientific Research.

***) Current address: Mathematisch Instituut, R.U. Leiden, 2300 RA Leiden, The Netherlands

well as on their applications. The purpose of this paper is to present some recent results on the numbers of solutions of unit equations and decomposable form equations.

For the equations in question there exist general finiteness criteria. Further, in case of equations in two unknowns (and for certain restricted classes of decomposable form equations in more unknowns), there are explicit upper bounds for the numbers of solutions which are independent of the coefficients of the form involved. In Evertse and Győry [11] (for unit equations) and Evertse, Gaál and Győry [7] (for decomposable form equations) similar (but not explicitely given) upper bounds have been recently established in full generality, under the most general finiteness conditions. The papers [11] and [7] are closely related, [11] furnishes the basic tool for the proof of the main result of [7] . The results of [7] have also been extended to the "inhomogeneous" case, that is to decomposable polynomial equations. In §§ 2 and 3 of this paper we present the most important results of [11] and [7], respectively. Further, we outline the basic ideas of the proofs of the main results.

§ 2. ON THE NUMBERS OF SOLUTIONS OF UNIT EQUATIONS

Let K be an algebraic number field of degree d ,

and let Γ be a finitely generated subgroup of the multiplicative group[1] K^*. We shall deal with the number of solutions of the equation

$$(1) \qquad \alpha_1 x_1 + \ldots + \alpha_n x_n = 1 \quad \text{in } x_1, \ldots, x_n \in \Gamma ,$$

where $n \geq 2$ is an integer and $\alpha_1, \ldots, \alpha_n \in K^*$. Of particular importance is the special case when Γ is the unit group of K or, more generally, the group of S-units U_S of K for some finite set S of (pairwise inequivalent) additive valuations on K. Further, every finitely generated subgroup of K^* is contained in some group of S-units of K. Hence equations of the type (1) are called *unit equations* and, for $\Gamma = U_S$, *S-unit equations*.

There is an extensive literature of unit equations and their applications (cf. [13]). A solution $(x_1, \ldots, x_n)$ of (1) is called *non-degenerate* if $\sum_{j \in \sigma} \alpha_j x_j \neq 0$ for each non-empty subset σ of $\{1,2,\ldots,n\}$ and *degenerate* otherwise. It is clear that if Γ is infinite and if (1) has a degenerate solution then (1) has infinitely many degenerate solutions. Using the p-adic analogue of the Thue-Siegel-Roth-Schmidt method, van der Poorten and

---

1) K^* denotes the set of non-zero elements of K. In general, for any integral domain R, R^* will denote the unit group (i.e. the multiplicative group of invertible elements) of R.

Schlickewei [25] and Evertse [5] proved independently of each other that (1) has only finitely many non-degenerate solutions. For n=2, more precise results are known. By combining a method of Thue and Siegel involving hypergeometric functions with some ideas of Mahler on p-adic approximations, Evertse [6] derived in case n=2, $\Gamma = U_S$ the upper bound $3 \times 7^{3d+2s}$ for the number of solutions of (1), where s denotes the cardinality of S. Two tuples $(\alpha_1,\ldots,\alpha_n)$, $(\beta_1,\ldots,\beta_n)$ with non-zero entries in K* are said to be Γ-*equivalent* if there are $\varepsilon_1,\ldots,\varepsilon_n \in \Gamma$ such that $\beta_i = \alpha_i \varepsilon_i$ for $i=1,\ldots,n$. Obviously, the number of (non-degenerate) solutions of (1) does not change when $(\alpha_1,\ldots,\alpha_n)$ is replaced by an equivalent tuple. Evertse, Győry, Stewart and Tijdeman [14] showed that in case n=2 (1) has at most two solutions for all but finitely many Γ-equivalent classes of pairs $(\alpha_1,\alpha_2) \in (K^*)^2$, and here the bound "two" is already sharp.

Recently, in [11], we have partly generalized the above-mentioned results of [6] and [14] to the case $n \geq 2$. We shall now present some of these generalizations. In what follows, $C_1(\ )$, $C_2(\ )$, ... will denote numbers which depend only on the parameters occurring between the parentheses.

THEOREM 1. ([11], Thm. 1). *The number of non-degenerate solutions of* (1) *is at most* $C_1(n,\Gamma)$.

This is a refinement of the theorem quoted above of van der Poorten and Schlickewei [25] and Evertse [5]. From the point of view of applications it is a remarkable fact that the bound $C_1(n,\Gamma)$ is independent of the coefficients $\alpha_1,..,\alpha_n$ of (1). We note that in [11] we extended Theorem 1 also to systems of unit equations.

By Theorem 1, the set of non-degenerate solutions of (1) is contained in at most $C_1(n,\Gamma)$ (n-1)-dimensional K-linear subspaces of K^n. Further, the degenerate solutions of (1) belong to the union of fewer than 2^n (n-1)-dimensional K-linear subspaces of K^n. Hence Theorem 1 implies the following result.

THEOREM 2. ([11] , Thm. 3). *All solutions of* (1) *are contained in the union of at most* $C_2(n,\Gamma)$ (n-1)-*dimensional* K-*linear subspaces of* K^n.

On can show in an elementary way (by induction on n; cf. [11]) that Theorem 2 implies Theorem 1. Theorems 1 and 2 are therefore equivalent.

We are not able to make explicit C_1 and C_2 in Theorems 1, 2 by our method. For an expected explicit expression for C_1, see our conjecture formulated at the end of this section.

We have two ways to prove Theorem 2. In the first

method one shows that the solutions of (1) with large "heights" satisfy some diophantine inequality which is independent of the coefficients $\alpha_1,\ldots,\alpha_n$ of equation (1). This diophantine inequality is of such a form that the p-adic subspace theorem of Schlickewei [27] can be applied to it, and thus it follows that the solutions of (1) with large heights are contained in the union of a finite number of (n-1)-dimensional K-linear subspaces of K^n that does not depend on the coefficients $\alpha_1,\ldots,\alpha_n$. Using a "higher dimensional gap principle" (cf. [11], Lemma 6) it can be proved that also the solutions of (1) with small heights are contained in the union of a finite number of (n-1)-dimensional K-linear subspaces of K^n independent of the coefficients of (1).

The second method is an extension to the case $n \geq 2$ of the method used in [14] for the case n=2. This second method enables one to prove the following refinement of Theorem 2.

THEOREM 3 ([11], Thm. 4). *For all but finitely many Γ-equivalence classes of tuples $(\alpha_1,\ldots,\alpha_n)\in(K^*)^n$, the set of solutions of* (1) *is contained in the union of fewer than $2^{(n+1)!}$ (n-1)-dimensional K-linear subspaces of K^n.*

Note that the minimal number of (n-1)-dimensional linear subspaces of K^n containing all solutions of (1)

does not change when $(\alpha_1,\ldots,\alpha_n)$ is replaced by a Γ-equivalent tuple. Hence Theorem 2 is an immediate consequence of Theorem 3 (cf. also [11]).

We shall now outline the basic idea of the proof of Theorem 3. We reduce the problem to (homogeneous) unit equations in (n+1)! unknowns all coefficients of which are equal to 1. Any n+1 solutions $\underline{x}_i=(x_{i1},\ldots,x_{im})$, $i=0,\ldots,n$, of (1) satisfy the equation

$$\Delta(\underline{x}_o,\ldots,\underline{x}_{n-1},\underline{x}_n) = \begin{vmatrix} x_{o1} & \cdots & x_{on} & 1 \\ \vdots & & & \\ x_{n-1,1} & \cdots & x_{n-1,n} & 1 \\ x_{n1} & \cdots & x_{nn} & 1 \end{vmatrix} = 0.$$

One can show that if the set of solutions of (1) is not contained in the union of fewer than $2^{(n+1)!}$ proper linear subspaces of K^n, then there are a subsum $\Sigma = \Sigma_o + \Sigma_1 X_{n1} + \ldots + \Sigma_n X_{nn}$ of the polynomial Δ, solutions $\underline{x}_o,\ldots,\underline{x}_{n-1}$ of (1) with $\tilde{\Sigma}_k := \Sigma_k(\underline{x}_o,\ldots,\underline{x}_{n-1}) \neq 0$ $(k=0,\ldots,n)$, and n linearly independent solutions $\underline{u}_o,\ldots,\underline{u}_{n-1}$ of (1) such that $\ell_\Sigma(\underline{u}_i) = 0$ and $\ell_{\Sigma'}(\underline{u}_i)\neq 0$ for each proper non-empty subset Σ' of Σ for $i=0,\ldots,n-1$, where $\ell_\Sigma = \tilde{\Sigma}_o + \tilde{\Sigma}_1 X_{n1} + \ldots + \tilde{\Sigma}_n X_{nn}$ and $\ell_{\Sigma'}$ is defined in a similar way. But $\ell_\Sigma(\underline{u}_i)$ is the sum of at most (n+1)! elements from Γ. Hence the result of [25] and [5] quoted above can be applied with $i=0,\ldots,n-1$ to prove that u_{ij}/u_{oj} $(i=0,\ldots,n-1;\ j=1,\ldots,n)$ belong to a finite

subset of K^* which depends only on n and Γ. The tuples $(u_{i1}/u_{o1},\ldots,u_{in}/u_{on})$ for i=0,...,n-1 are, however, linearly independent and, in view of (1),

$$\sum_{i=1}^{n} (\alpha_j u_{oj})(u_{ij}/u_{oj}) = 1 \text{ for } i=0,\ldots,n-1.$$

This implies that the numbers $\alpha_j u_{oj}$ (j=1,...,n) belong to a finite subset of K^* depending only on n and Γ whence the assertion of Theorem 3 follows.

For n=2, Theorem 3 implies that equation (1) has fewer than $2^{3!}$ solutions for all but finitely many Γ-equivalence classes of pairs $(\alpha_1,\alpha_2)\in(K^*)^2$. This is a weaker version of the above-mentioned theorem of Evertse, Győry, Stewart and Tijdeman [14]. For n=3, a similar result can be deduced from Theorem 3. Suppose that $\Gamma=U_S$ for some finite set S of additive valuations on K. Theorem 3 implies that apart from finitely many U_S-equivalence classes of $\underline{\alpha}=(\alpha_1,\alpha_2,\alpha_3)\in(K^*)^3$, the solutions of the equation

$$(2) \quad \alpha_1 x_1+\alpha_2 x_2+\alpha_3 x_3 = 1 \quad \text{in} \quad x_1,x_2,x_3\in U_S$$

are contained in the union of at most $2^{4!}$ proper linear subspaces of K^3. However, the non-degenerate solutions contained in such a subspace satisfy an S-unit equation in two unknowns. Hence the theorem of Evertse [6] quoted above gives the following.

COROLLARY 1. ([11], Thm. 5). *For all but finitely many* U_S*- equivalence classes of* $\underline{\alpha} = (\alpha_1, \alpha_2, \alpha_3) \in (K^*)^3$, *equation* (2) *has fewer than* $3 \times 2^{24} \times 7^{3d+2s}$ *non-degenerate solutions.*

An example given in [14], §§ 0,5, shows that the bound occurring in Corollary 1 cannot be replaced by a bound which is polynomial in terms of s.

The results quoted and presented above suggest the following.

CONJECTURE (cf. [11]). *Suppose that* $\Gamma \subseteq U_S$ *for some finite set* S *of additive valuations on* K *with cardinality* s. *It is possible to give an explicit expression* C(n), *in terms of* n *only, such that the number of non-degenerate solutions of* (1) *is at most* $C(n)^{d+s}$.

For a possible approach to prove this conjecture, see Remark 1 at the end of § 3.

REMARK. Our results formulated above are stated and proved in [11] in the more general case when K is an arbitrary finitely generated (not necessarily algebraic) extension field of $\mathbb{Q}$ and Γ is an arbitrary finitely generated subgroup of K^*. Further, we established in [11] an analogue of Theorem 3 above for the function field case.

§ 3. ON THE NUMBERS OF SOLUTIONS OF DECOMPOSABLE POLYNOMIAL EQUATIONS

Let again K be an algebraic number field, and let G be a finite, normal extension of K. We recall (cf.[9]) that if M is a finite set of linear forms in $G[X_1,\ldots,X_t]$ $(t \geq 2)$ then a non-zero K-linear subspace V of K^t is said to be *M-non-degenerate* or *M-degenerate* according as M does or does not contain a subset of at least three linear forms whose restrictions to V are linearly dependent, but pairwise linearly independent. Further, V is called *M-admissible* if no form in M vanishes identically on V.

Let $F(\underline{X}) = F(X_1,\ldots,X_m) \in K[X_1,\ldots,X_m]$ be a *decomposable polynomial* in $m \geq 2$ variables with splitting field contained in G, that is

$$F(\underline{X}) = \prod_{i=1}^{n} \ell_i(\underline{X})$$

where the $\ell_i(\underline{X})$ are linear polynomials (possibly with a non-zero constant term) with coefficients in G. Next we shall deal with the *decomposable polynomial equation*

(3) $F(\underline{x}) = b$ in $\underline{x} = (x_1,..,x_m) \in R^m$ with $\ell(\underline{x}) \neq 0$ for all ℓ in L,

where R is a subring of K which is finitely generated over $\mathbb{Z}$, b is a non-zero element of K, and L is a finite (possibly empty) set of linear polynomials in

$G[X_1,..,X_m]$. If in particular $F(\underline{X})$ and the linear polynomials in L are homogeneous, then $F(\underline{X})$ is called a *decomposable form* and (3) a *decomposable form equation*.

Important classes of decomposable form equations are Thue-equations (when m=2), norm form equations, discriminant form equations and index form equations. A great number of finiteness results have been established for various restricted classes of decomposable form equations and decomposable polynomial equations; for references see e.g.[29],[26],[1],[30],[18[,[19],[4],[15],[31],[16]and [10]. In [9], we gave a general finiteness criterion for decomposable form equations and pointed out that the theory of decomposable form equations is equivalent to the theory of unit equations. In a recent joint work with Gaál (cf.[7]) we have extended this criterion to the "inhomogeneous" case, i.e. to decomposable polynomial equations. In order to formulate this criterion we have to introduce some further notation.

Let L_o be a maximal subset of pairwise linearly independent polynomials in $\{l_1,..,l_n\}$ over G. Put

$$L_o^* = \{X_{m+1}\} \cup \{X_{m+1} \times l(\frac{X_1}{X_{m+1}},\ldots,\frac{X_m}{X_{m+1}}): l \in L_o\}$$

and

$$L^* = \{X_{m+1} \times l(\frac{X_1}{X_{m+1}},\ldots,\frac{X_m}{X_{m+1}}) : l \in L\}.$$

Then L_o^* and L^* consist of linear forms in $G[X_1,\ldots,X_{m+1}]$.

THEOREM 4([7], Thm. 1). *The following two statements are equivalent:*

(i) *The forms in* L_o^* *have rank* $m+1$ *over* G, *and every* $L_o^* \cup L^*$ *-admissible linear subspace of* K^{m+1} *of dimension* ≥ 3 *is* L_o^**-non-degenerate;*

(ii) *For every* b *in* K^* *and every subring* R *of* K *which is finitely generated over* $\mathbb{Z}$, *equation* (3) *has at most finitely many solutions.*

For several restricted classes of decomposable form equations, there are explicit upper bounds for the numbers of solutions which are independent of the coefficients of the decomposable form involved; see [4],[32], [22], [6], [8], [3], [10], [23], [2], [12], [33] and the references given there. Recently, we showed with Gaál (cf. [7]) in full generality that under the finiteness condition (i) of Theorem 4, the number of solutions of (3) is bounded above by a number which is independent of the coefficients of F and the linear polynomials in L. We shall now formulate this statement in a more precise form. Assume that R contains b and the coefficients of F. Put $\hat{R} = R[b^{-1}]$ and denote by $\hat{R}_G$ the integral closure of $\hat{R}$ in G. Both $\hat{R}_G$ and $\hat{R}_G^*$ are finitely generated (cf. [24],[20]). The following theorem is a refinement of the implication (i)=>(ii) of Theorem 4.

THEOREM 5([7], Thm. 2). *Let* $b \in R \setminus \{0\}$ *and suppose that the decomposable polynomial* F *has all its coefficients in* R. *If condition* (i) *of Theorem* 4 *holds then equation* (3) *has at most* $nC_3(m,\hat{R}_G^*)$ *solutions where*

$$C_3(m,\hat{R}_G^*) = \prod_{r=3}^{m+1} C_2(r,\hat{R}_G^*)$$

with the $C_2(,)$ *defined in Theorem 2.*

It is clear that the bound $nC_3(m,\hat{R}_G^*)$ depends only on n,m,b,R and G, but not on L and the coefficients of F.

The proof of Theorem 5 is based on Theorem 2. We give now a sketch of the proof. Put

$$\ell_{n+1}^*(\underline{X}^*) = X_{m+1} \text{ and } \ell_i(\underline{X}^*) = X_{m+1}\ell_i\left(\frac{X_1}{X_{m+1}},\ldots,\frac{X_m}{X_{m+1}}\right) \text{ for}$$

i=1,...,n. It is more convenient to consider equations (3) in the form

(3') $F^*(\underline{x}^*)=b$ in $\underline{x}^* = (x_1,\ldots,x_{m+1}) \in R^{m+1}$ with $x_{m+1}=1$

and $\ell^*(\underline{x}^*) \neq 0$

for all ℓ^* in L^*.

One can show (cf. [7]) that the factorization of F over G into linear factors can be chosen to satisfy

(4) $\ell_i^*(\underline{x}^*) \in \hat{R}_G^*$ (i=1,...,n+1) for every solution $\underline{x}^* = (x_1,\ldots,x_{m+1})$ of (3').

Further, it is easily seen that every two dimensional $L_o^* \cup L^*$-admissible subspace V of K^{m+1} contains at most

n solutions of (3'). Then, one can prove that *if* V *is any* $L_o^* \cup L^*$*-admissible,* L_o^**-non-degenerate subspace of* K^{m+1} *of dimension* $r \geq 3$, *then the solutions in* V *of* (3') *are contained in at most* $C_2(r, \hat{R}_G^*)$ (r-1)*-dimensional* $L_o^* \cup L_o^*$*-admissible subspaces of* V. This implies at once that the total number of solutions of (3') is at most $nC_3(m, \hat{R}_G^*)$.

To prove the above assertion, consider the smallest integer t for which there are t linear forms among $\ell_1^*, \ldots, \ell_{n+1}^*$, say $\ell_1^*, \ldots, \ell_t^*$, such that

$$(5) \qquad \sum_{i=1}^{t} c_i \ell_i^*(\underline{x}^*) = 0 \quad \text{for all } \underline{x}^* \text{ in } V$$

for some $c_1, \ldots, c_t \in G^*$. Then $t \leq r+1$. Further, by (i), $t \geq 3$. From (5) it follows that

$$\sum_{i=1}^{t-1} - \frac{c_i}{c_t} \cdot \frac{\ell_i^*(x^*)}{\ell_t^*(\underline{x}^*)} = 1 \text{ for all solutions } \underline{x}^* \text{ of (3')}$$

in V. Since $\hat{R}_G^*$ is finitely generated, Theorem 2 tohether with (4) implies that the tuples

$(\ell_1^*(x^*)/\ell_t^*(x^*), \ldots,$

$\ldots \ell_{t-1}^*(\underline{x}^*)/\ell_t^*(\underline{x}^*))$, with $\underline{x}^* \in V$ being a solution of (3'), are contained in at most $C_2(r, \hat{\hat{R}}_G^*)$ (t-2)-dimensional

subspaces of G^{t-1}. For each of these subspaces of G^{t-1}, there are $\beta_1,\ldots,\beta_{t-1}\in G$, not all zero, such that

$$(6)\qquad \sum_{i=1}^{t-1} \beta_i \frac{\ell_i^*(\underline{x}^*)}{\ell_t^*(\underline{x}^*)} = 0, \text{ i.e. } \sum_{i=1}^{t-1} \beta_i \ell_i^*(\underline{x}^*)=0$$

for the corresponding solutions $\underline{x}^*$ of (3′) in V. By the minimality of t, (6) cannot hold for all $\underline{x}^*\in$ V. Therefore, the $\underline{x}^*\in$ V satisfying (6) lie in an (r-1)-dimensional subspace of V which is obviously $L_o^*\cup L^*$-admissible. This proves the above assertion and hence Theorem 5.

It is a consequence of the non-explicit character of Theorem 2 that we are not able to make explicit the upper bound $C_3(m,\hat{R}_G^*)$ in Theorem 5. An explicit version of Theorem 2 or Theorem 1 would enable one to compute explicitely all upper bounds occurring in this section. For an expected explicit version of Theorem 1, see our conjecture in § 2 and Remark 1 at the end of this section.

We now present a consequence of Theorems 4 and 5 for decomposable form equations. Let $F_o(\underline{X})=F_o(X_1,\ldots,X_m)\in K[X_1,..,X_m]$ be a decomposable form which factorizes into linear forms $\ell_1(\underline{X}),\ldots,\ell_n(\underline{X})$ over G, let L_o be a maximal subset of pairwise linearly independent linear forms in $\{\ell_1,\ldots,\ell_n\}$ over G, and let L be a finite (possibly empty) set of linear forms in $G[X_1,\ldots,X_m]$.

COROLLARY 2 ([7], Cor. 1). *The following two statements are equivalent:*

(i) *Every* $L_0 \cup L$*- admissible linear subspace of* K^m *of dimension* ≥ 2 *is* L_0*-non-degenerate;*

(ii) *For every* $b \in K^*$ *and every subring* R *of* K *which is finitely generated over* $\mathbb{Z}$, *the equation*

(7) $F_0(\underline{x}) = b$ *in* $\underline{x} \in R^m$ *with* $\ell(\underline{x}) \neq 0$ *for all* ℓ *in* L *has only finitely many solutions.*

Moreover, if (i) *holds and if* R *is a finitely generated subring of* K *containing* $b \neq 0$ *and the coefficients of* F_0 *then equation* (7) *has at most* $nC_3(m, \hat{R}_G^*)$ *solutions.*

The equivalence of statements (i) and (ii) of Corollary 2 was earlier proved in our joint paper [9]. Further, under a condition stronger than (i), we derived in [8] a completely explicit upper bound (independent of the coefficients of F_0) for the number of solutions of (7).

Next we state another consequence of Theorem 4. Let $\ell_1, \ldots, \ell_n, L_0$ have the same meaning as in Corollary 2, and let $L = \{\ell_{n+1}, \ldots, \ell_{n+k}\}$ be a (possibly empty) set of linear forms in $G[X_1, \ldots, X_m]$. Let Λ be the set of tuples $\underline{\lambda} = (\lambda_1, \ldots, \lambda_{n+k}) \in G^{n+k}$ for which the decomposable polynomial

$$F_{\underline{\lambda}}(\underline{X}) := \prod_{i=1}^{n} (\ell_i(\underline{X}) + \lambda_i)$$

has its coefficients in K. Obviously $\underline{0} \in \Lambda$.

COROLLARY 3 ([7], Cor. 2). *The following two statements are equivalent:*

(i) *Every subspace of* K^m *of dimension* ≥ 2 *is* L_o *non-degenerate;*

(ii) *For every* $b \in K^*$, *every* $\underline{\lambda} \in \Lambda$ *and every finitely generated subring* R *of* K, *the equation*

(8) $F_{\underline{\lambda}}(\underline{x}) = b$ *in* $\underline{x} \in R^m$ *with* $\ell_i(\underline{x}) + \lambda_i \neq 0$ *for all* ℓ_i *in* L *has only finitely many solutions.*

It can happen (cf. [7]) that equation (7) has finitely many solutions for every $b \in K^*$ and every finitely generated subring R of K, while, for suitable $\underline{\lambda}$, b and R, the corresponding inhomogeneous equation (8) has infinitely many solutions.

We formulate now some further consequences of Theorems 4 and 5 for Thue equations, discriminant polynomial equations and norm polynomial equations. First consider the case $m=2$. Let $F(X_1, X_2) \in K[X_1, X_2]$ be a decomposable polynomial of degree n which factorizes into linear polynomials $\ell_i(X_1, X_2) + \lambda_i$, $i = 1, \ldots, n$, over G where the ℓ_i are linear forms in X_1, X_2 and $\lambda_i \in G$. Let L_o be a maximal subset of pairwise linearly independent polynomials among $\ell_i + \lambda_i$, $i = 1, .., n$, and put

$$L_o^* = \{X_3\} \cup \{\ell_i(X_1,X_2) + \lambda_i X_3 : \ell_i \in L_o\}$$

COROLLARY 4 ([7], Cor. 3). *The following two statements are equivalent:*

(i) *The forms in* L_o^* *have* rank 3 *over* G, *and there are at least three linear forms in* L_o^* *which are linearly dependent, but pairwise linearly independent;*

(ii) *For every* $b \in K^*$ *and every subring* R *of* K *which is finitely generated over* $\mathbb{Z}$, *the equation*

$$F(x_1,x_2)=b \text{ in } x_1,x_2 \in R \tag{9}$$

has only finitely many solutions.

Moreover, if (i) holds and if R *is a finitely generated subring of* K *containing* $b \neq 0$ *and the coefficients of* F, *then* (9) *has at most* $nC_4(\hat{R}_G^*)$ *solutions where* $C_4(\hat{R}_G^*) = C_3(2,\hat{R}_G^*)$.

From Corollary 3 one can also deduce a finiteness criterion for equations of the type (9). For m=2, condition (i) of Corollary 3 reduces to the following statement (cf. [7]):

(i') *There are at least three pairwise linearly independent forms among* $\ell_1,\ldots,\ell_n$.

When $F(X_1,X_2)$ is a homogeneous polynomial (i.e. $\lambda_i=0$ for i=1,...,n), equation (9) is called a *Thue equation*. Then (i') and condition (i) of Corollary 4 coincide (cf.[9], Corollary to Theorem 1). In case of Thue equations, for

explicit expressions for $C_4(\hat{R}_G^*)$ see Evertse [6], Evertse and Győry [8] and Bombieri [2].

Let M be a finite extension field of K of degree $n \geq 3$, and suppose that G contains M as a subfield. Let $\alpha_1,\ldots,\alpha_m$ ($m \geq 2$) be elements of M such that $M=K(\alpha_1,\ldots,\alpha_m)$ and that $1,\alpha_1,\ldots,\alpha_m$ are linearly independent over K. Let λ be an arbitrary element of M, and consider the *discriminant polynomial equation*

$$(10) \quad a_o D_{M/K}(\alpha_1 x_1+\ldots+\alpha_m x_m+\lambda) = b \text{ in } x_1,\ldots,x_m \in R,$$

where R is a finitely generated subring of K having K as its quotient field and $a_o, b \in R\setminus\{0\}$. If in particular $\lambda=0$, (10) is called a *discriminant form equation*. For discriminant form equations, discriminant polynomial equations and their applications to index form equations and algebraic number theory, see [17], [18], [19], [8], [16], [10] and the references given there. The element a_o can be chosen so that $a_o D_{M/K}(\alpha_1 X_1+\ldots+\alpha_m X_m+\lambda) \in R[X_1,\ldots,X_m]$. Theorems 4 and 5 imply

COROLLARY 5 ([7], Cor. 4). *The number of solutions of* (10) *is at most* $nC_3(m,\hat{R}_G^*)$.

For discriminant form equations, the corresponding result was proved in [8] with an explicitely given C_3.

Let now $\alpha_1,\ldots,\alpha_m$ ($m\geq 2$) be elements of M which are linearly independent over K, and let $a_o,b\in K^*$. Consider the *norm form equation*

$$(11)\qquad a_o N_{M/K}(\alpha_1 x_1+\ldots+\alpha_m x_m)=b \text{ in } x_1,\ldots,x_m\in R,$$

where R is a finitely generated subring of K. We assume that $\alpha_1=1$ and $M=K(\alpha_2,\ldots,\alpha_m)$ which is no restriction. Let V denote the K-vector space generated by $\alpha_1,\ldots,\alpha_m$ in M. V is called *degenerate* or *non-degenerate* according as it does or does not contain any subspace of the form $\mu M'$ where $\mu\in M^*$ and M' is a subfield of M with $K\subsetneq M'\subseteq M$. As is known, equation (11) has only finitely many solutions for every $b\in K^*$ and every finitely generated subring R of K if and only if V is non-degenerate. This criterion is due to Schmidt [28] (see also [30]) and Schlickewei [26] in the case $K=\mathbb{Q}$, and to Laurent [21] in the general case. In [9] we showed that this finiteness result is a consequence of our criterion concerning decomposable form equations of general type (i.e. of the equivalence of statements (i), (ii) of Corollary 2 of the present paper). As a consequence of Theorem 4 presented above, we have recently extended in [7] the above-mentioned result of Schmidt, Schlickewei and Laurent to the "inhomogeneous" case, to norm polynomial equations. Further, in [7] we proved that Theorem 5 stated above implies an

upper bound for the number of solutions which is independent of the coefficients of the norm polynomial involved. Namely, we established with Gaál the following.

COROLLARY 6 ([7], Cor. 5). *The following two statements are equivalent:*

(i) *V is non-degenerate;*

(ii) *For every $\lambda \in M$, every subring R of K which is finitely generated over $\mathbb{Z}$ and every $b \in K^*$, the norm polynomial equation*

$$a_o N_{M/K}(\alpha_1 x_1 + \ldots + \alpha_m x_m + \lambda) = b \quad \text{in } x_1, \ldots, x_m \in R \tag{12}$$

has only finitely many solutions.

Moreover, if a_o, $b \in K^*$, $\lambda \in M$ and R is a finitely generated subring of K containing b and the coefficients of the norm polynomial occurring in (12), then (12) has at most $n\, C_3(m, \hat{R}_G^*)$ solutions.

In the particular case when $\lambda = 0$ and α_{i+1} has degree at least 3 over $K(\alpha_1, \ldots, \alpha_i)$ for $i = 1, \ldots, m-1$, an explicit expression for C_3 can be found in Evertse and Győry [8].

REMARK 1. In his lecture given at the Number Theory Conference of Budapest (July 20-25, 1987), W.M. Schmidt* announced that in the case $K = \mathbb{Q}$, $R = \mathbb{Z}$, $\lambda = 0$, he had derived an explicit upper bound for the number

*Added in proof. See Schmidt's paper in these Proceedings.

of solutions of (12) which depends only on b,n and m. Schmidt's approach is different from ours, he deduced the upper bound from his recent quantitative version of the subspace theorem over $\mathbb{Z}$. We note that a p-adic generalization over algebraic number fields of Schmidt's quantitative subspace theorem together with the "higher dimensional gap principle" (cf. [11]) quoted in §2 would enable one to make explicit the bounds in Theorems 1 and 2 of the present paper.*) As was remarked above, this would make it possible to give explicitely the upper bounds in Theorem 5 and in its corollaries above.

REMARK 2. Our results presented in this section were formulated and proved in [7] in the more general situation when K is an arbitrary finitely generated (not necessarily algebraic) extension field of $\mathbb{Q}$ and R is an arbitrary finitely generated subring of K over $\mathbb{Z}$. Further, it was shown in [7] that the finiteness conditions in our results are decidable, provided that the ground field and the decomposable polynomial involved have appropriate effective representations.

REFERENCES

[1] A. BAKER, Transcendental number theory, 2nd ed., Cambridge, 1979.

[2] E. BOMBIERI, On the Thue-Mahler equation, Springer Lecture Notes in Math., 1290, pp. 213-243.

*) Added in proof. Recently Schlickewei announced (Oberwolfach, March 13-18, 1988) that, in the special case $K = \mathbb{Q}$, he could derive explicit expressions for the bounds C_1 and C_2 in our Theorems 1 and 2.

[3] E. BOMBIERI and W.M. SCHMIDT, On Thue's equation, *Invent. Math.* 88(1987), 69-81.

[4] J.H. EVERTSE, Upper bounds for the numbers of solutions of diophantine equations, *MC-tract 168*. Amsterdam, 1983.

[5] J.H. EVERTSE, On sums of S-units and linear recurrences, *Compositio Math.* 53(1984), 225-244.

[6] J.H. EVERTSE, On equations in S-units and the Thue-Mahler equation, *Invent.Math.* 75(1984), 561-584.

[7] J.H. EVERTSE, I. GAÁL and K. GYŐRY, On the numbers of solutions of decomposable polynomial equations, *Archiv der Math.*,52(1989), 337-353.

[8] J.H. EVERTSE and K. GYŐRY, On unit equations and decomposable form equations, *J.Reine Angew. Math.* 358(1985), 6-19.

[9] J.H. EVERTSE and K. GYŐRY, Finiteness criteria for decomposable form equations, *Acta Arith.*, 50(1988) 357-379.

[10] J.H. EVERTSE and K. GYŐRY, Decomposable form equations, *New Advances in Transcendence Theory*, Cambridge, 1988,pp. 175-202.

[11] J.H. EVERTSE and K. GYŐRY, On the numbers of solutions of weighted unit equations, *Compositio Math.*, 66(1988),329-354.

[12] J.H. EVERTSE and K. GYŐRY, Thue-Mahler equations with a small number of solutions, J. Reine Angew. Math. 399(1989), 60-80.

[13] J.H. EVERTSE, K. GYŐRY, C.L. STEWART and R. TIJDEMAN, S-unit equations and their applications, *New Advances in Transcendence Theory*, Cambridge, 1988, pp. 110-174.

[14] J.H. EVERTSE, K. GYŐRY, C.L. STEWART and R. TIJDEMAN, On S-unit equations in two unknowns, *Invent. Math.*, 92(1988), 461-477.

[15] I. GAÁL, Norm form equations with several dominating variables and explicit lower bounds for inhomogeneous linear forms with algebraic coefficients II, *Studia Sci. Math. Hungar.* 20(1985), 333-344.

[16] I. GAÁL, Inhomogeneous discriminant form equations and integral elements with given discriminant over finitely generated integral domains, *Publ. Math. Debrecen* 34(1987), 109-122.

[17] K. GYŐRY, Sur les polynômes à coefficients entries et de discriminant donné III, *Publ. Math. Debrecen* 23(1976), 141-165.

[18] K. GYŐRY, Résultats effectifs sur la représentation des entiers par des formes décomposables, *Queen's Papers in Pure and Applied Math.*, No. 56, Kingston, Canada, 1980.

[19] K. GYŐRY, On norm form, discriminant form and index form equations, Coll.Math.Soc.J. Bolyai 34. Topics in Classical Number Theory, Budapest, 1981. *North-Holland Publ. Comp.*, 1984, pp. 617-676.

[20] S. LANG, *Fundamentals of diophantine geometry*, Springer Verlag, Berlin-Heidelberg-New York, 1983.

[21] M. LAURENT, Equations diophantiennes exponentielles, *Invent. Math.* 78(1984), 299-327.

[22] K. MAHLER, On Thue's equation, *Math. Scand.* 55(1984), 188-200.

[23] J. MUELLER and W.M. SCHMIDT, Thue's equation and a conjecture of Siegel, *Acta Math.* 160(1988), 207-247.

[24] M. NAGATA, A general theory of algebraic geometry over Dedekind domains I, *Amer.J.Math.* 78(1956), 78-116.

[25] A.J. van der POORTEN and H.P. SCHLICKEWEI, The growth conditions for recurrence sequences, *Macquarie Univ. Math. Rep.* 82-0041, North Ryde, Australia, 1982.

[26] H.P. SCHLICKEWEI, On norm form equations, *J. Number Theory* 9 (1977), 370-380.

[27] H.P. SCHLICKEWEI, The p-adic Thue-Siegel-Roth-Schmidt theorem, *Archiv der Math.* 29(1977), 267-270.

[28] W.M. SCHMIDT, Linearformen mit algebraischen Koeffizienten II, *Math. Ann.* 191(1971), 1-20.

[29] W.M. SCHMIDT, Approximation to algebraic numbers, *Enseign. Math.* 17(1971), 187-253.

[30] W.M. SCHMIDT, *Diophantine approximation*, Lecture Notes in Math. 785, Springer Verlag, 1980.

[31] T.N. SHOREY and R. TIJDEMAN, *Exponential diophantine equations*, Cambridge, 1986.

[32] J.H. SILVERMAN, Representations of integers by binary forms and the rank of the Mordell-Weil group, *Invent. Math.* 74(1983), 281-292.

[33] R. TIJDEMAN, The number of solutions of diophantine equations, these *Proceedings*, to appear.

EVERTSE, J.H.

University of Leiden
Department of Mathematics
and Computer Science
P.O. Box 9512
2300 RA Leiden

GYŐRY, K.

Kossuth Lajos University
Mathematical Institute
4010 Debrecen
Hungary

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

A BOUNDEDNESS THEOREM FOR THE TORSION OF ELLIPTIC CURVES OVER ALGEBRAIC NUMBER FIELDS

HELMUT G. FOLZ and HORST G. ZIMMER

1. INTRODUCTION

Let

$$E : y^2 = x(x^2 + a_2x + a_4)$$

be an *elliptic curve* over an *algebraic number field* K with ring of integers O_K.

$$\Delta = 2^4a_4^2(a_2^2 - 4a_4) \neq 0$$

is the *discriminant* and

$$j = 2^8 \frac{(a_2^2 - 3a_4)^3}{a_4^2(a_2^2 - 4a_4)}$$

the *absolute invariant* of E.

Suppose that $a_2, a_4 \in O_K$ and $j \neq 0, 12^3$.

We call E over K

2-*deficient* if (see [8])

$$a_4 \cong A^2, \ (a_2^2 - 4a_4) \cong B^2$$

and 3-*deficient* if

$$a_4 \cong A^3, \ (a_2^2 - 4a_4) \cong B^2$$

for some integral divisors A, B of K.

Kubert (cf. [21]) defined

E over K to be ℓ-*deficient* for a prime $\ell \geq 5$

if the denominator of j is in ℓ-th power of an integral divisor of K. Hence the above definition amounts to a modification of Kubert's notion.

For the class of ℓ-deficient elliptic curves E over K, where $\ell \geq 2$ is a prime, it is possible to prove the so-called *boundedness conjecture*. To state this conjecture we introduce the *group*

$$E(K) := \{P = (x,y) \in K^2 \mid y^2 = x(x^2 + a_2x + a_4) \text{ or } P = 0 = (\infty\ \infty)\}$$

of *rational points* of E over K and recall the famous

THEOREM (Mordell-Weil, 1922-1928)

$$E(K) \cong E(K)_{tor} \oplus \mathbb{Z}^r$$

where $E(K)_{tor}$ is the finite *torsion group* of points of finite order, and r is the *rank* of E over K.

BOUNDEDNESS CONJECTURE (e.g. Cassels, [2])

For the order of the torsion group, we have

$$\#E(K)_{tor} \leq N(K)$$

with a real positive bound $N(K)$ depending only on K.

A strengthened version of this conjecture asserts that $N(K)$ depends only on the field degree $n = [K:\mathbb{Q}]$.

In 1979 Kubert [21] proved: The conjecture is true for ℓ-deficient elliptic curves, $\ell \geq 5$ a prime, the bound depending on K and ℓ.

In 1985 Folz [8] proved: The conjecture is true for 2-deficient elliptic curves E over K.

In this lecture we first report on some known boundedness results, then outline the proof of the boundedness theorem of the first author for 2-deficient curves and indicate its possible generalization to 3-deficient curves, and finally exhibit some "explicit"

bounds. The method of proof is based on ideas of Demjanenko ([3] - [6]). The details of proof in the 3-deficient case have not been carried out yet.

REMARK: If $\mathbb{Z}/_{2\mathbb{Z}} \oplus \mathbb{Z}/_{4\mathbb{Z}} \subseteq E(K)_{\mathrm{tor}}$, then E over K is 2-deficient; if $\mathbb{Z}/_{2\mathbb{Z}} \oplus \mathbb{Z}/_{6\mathbb{Z}} \subseteq E(K)_{\mathrm{tor}}$, then E over K is 3-deficient.

Hence 2-deficient should possibly be called 2-4-*deficient* and 3-deficient 2-6-*deficient*. This concept generalizes to 2-ℓ-*deficient* for primes $\ell \geq 5$.

2. SOME KNOWN RESULTS

THEOREM (Manin, [22])

For a prime p, the order of the *p-primary part* of $E(K)_{\mathrm{tor}}$ satisfies

$$\sharp E^{(p)}(K)_{\mathrm{tor}} \leq M(K,p)$$

with a real positive bound $M(K,p)$ depending only on K and p.

THEOREM (Kubert, [21])

For a prime $\ell \geq 5$, every ℓ-deficient elliptic curve E over K satisfies

$$\#E(K)_{tor} \leq N(K,\ell)$$

with a real positive bound $N(K,\ell)$ depending only on K and ℓ.

Demjanenko ([3] - [6]) claims to have proved the boundedness conjecture. However, his proofs contain gaps though the basic ideas are useful.

a) Results about the Manin-bound

THEOREM (Kenku, [16] - [20])

Suppose K is a quadratic field. Then

$$M(K,p) \begin{cases} \leq 4 \text{ if } p = 2 \\ = 2 \text{ if } p = 3 \\ = 1 \text{ if } p = 5,\ 7 \\ = 0 \text{ if } p = 17,\ 19,\ 23 \end{cases}$$

and

$$M(K,p) = 0 \quad \text{if} \quad p \geq 181,\ p \neq 191\ ,$$

provided that

$$\|J_0^-(p) = J_0(p)/(1 + w_p)J_0(p)$$

is defined in terms of the fundamental involution w_p of E.

THEOREM (Momose, [24])

(i) Suppose K is a quadratic field. Then

$$M(K,p) \leq 1 \quad if \quad p = 11, 13$$

and

$$M(K,p) = 0 \quad if \quad p \geq 17$$

provided that

$$\#J_0^-(p)(\mathbb{Q}) < \infty.$$

(ii) Suppose K is a cubic field. Then

$$M(K,p) \begin{cases} \leq 5 \ if \ p = 2 \\ = 2 \ if \ p = 3 \\ \leq 1 \ if \ p = 17 \\ = 0 \ if \ p = 19, 23, 41, 47, 59, 71 \end{cases}$$

and

$$M(K,p) = 0 \ if \ p > 79, \ p \neq 109$$

provided that

$$\#J_0^-(p)(\mathbb{Q}) < \infty.$$

THEOREM (Kamienny, [12])

Suppose K is a quadratic field. Then

$$M(K,p) = 0 \ if \ p = 17, 19, 23, 29, 31, 41, 47, 59, 71.$$

b) Some special results on the torsion

THEOREM (Mazur, [23])

Suppose $K := \mathbb{Q}$. Then

$$E(\mathbb{Q})_{tor} \cong \left\{ \begin{matrix} \mathbb{Z}/m\mathbb{Z} \text{ for } 1 \leq m \leq 10 \text{ or } m = 12 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} \text{ for } 1 \leq m \leq 4 \end{matrix} \right\}$$

Kamienny (cf. [13]) calls E *balanced* over K if, for each finite prime p of K and corresponding normalized additive valuation v_p,

$$\left\{ \begin{matrix} v_p(j) < 0 \text{ for } \textit{all } \mathfrak{p} \mid p \text{ whenever} \\ v_p(j) < 0 \text{ for } \textit{one } \mathfrak{p} \mid p \end{matrix} \right\}$$

and Frey [7] calls E *I-balanced at infinity* over K if, for the infinite primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of K and corresponding multiplicative absolute values $||_1, \ldots, ||_r$,

$$| |j|_\mu - |j|_\nu | \leq I \qquad (1 \leq \mu, \nu \leq r)$$

for some real positive I.

THEOREM (Kamienny, [13])

Suppose K is a totally real number field and E is balanced over K. Then

$$\#E(K)_{tor} \leq M(n),$$

where the real positive constant $M(n)$ depends only on the field degree

$$n = [K:Q].$$

This theorem corroborates, in a special case, the strengthened version of the boundedness conjecture. More generally, we have the

THEOREM (Frey, [7])

Suppose K is an arbitrary number field and E is balanced over K and I-balanced at infinity over K for some real positive I. Then

$$\#E(K)_{tor} \leq N(n, I)$$

where the real positive constant $N(n, I)$ depends only on I and the field degree

$$n = [K:Q] .$$

THEOREM (Silverman, [25])

Let $\ell \geq 5$ be a prime, $E[\ell]$ denote the set of ℓ-torsion points on E, $K_\ell := K(E[\ell])$ be the field of ℓ-torsion points over K, and ρ_ℓ denote the ℓ-rank of the

class group of K_ℓ. Then

$$\#E(K)_{tor} \leq N(n, \ell, \rho_\ell),$$

where the real positive constant $N(n, \ell, \rho_\ell)$ depends only ℓ, ρ_ℓ and the field degree

$$n = [K : Q].$$

3. THE BOUNDEDNESS THEOREM FOR 2-DEFICIENT AND 3-DEFICIENT ELLIPTIC CURVES

MAIN THEOREM. Suppose E is a 2-deficient or 3-deficient elliptic curve over an algebraic number field K. Then

$$p \leq N(K)$$

for the prime order p of any torsion point $P = (x_1, x_1) \in E(K)_{tor}$, where $N(K)$ stands for a real positive constant depending only on K.

REMARK: Combined with Manin's p-boundedness result, this theorem corroborates the boundedness conjecture for 2-deficient and 3-deficient elliptic curves E over algebraic number fields K.

As pointed out above, the details of proof in the 3-deficient case are still to be carried out. This will be done in a subsequent paper. Here, we shall confine ourselves to giving an outline of the proof in [8].

MAIN STEPS OF PROOF:

We apply

(1′) Néron's reduction theory,

(2′) Riemann's hypothesis for function fields,

(3′) the generalized Nagell-Lutz-Cassels theorem

to reduce the proof to the case in which

(1) E has semi-stable reduction at all finite p of K,

(2) E has multiplicative reduction at all finite primes $p|2$ of K,

(3) the given torsion point $P = (x_1, x_1)$ of prime order p on E over K and all its multiples $rP = (x_r, y_r)$ have integral coordinates in K.

REMARK: If one of the conditions (1), (2) or (3) does not apply, (1′), (2′) or (3′) leads to the bound

$$N(K) = max\{\ max\{\ p|p\ -1 \le 6v_p(p)\ \text{for one}\ |p\};\ max\{1 + 2\sqrt{N(p)} + N(p)\,|\,p|2\}\}$$

where N denotes the *norm* of a prime divisor p.

Hence we are left with the case in which (1) - (3) are satisfied. Suppose therefore in what follows that (1) - (3) are valid for E over K.

The proof of the main theorem is composed of four theorems. The first two are essentially due to Basarab [1], Demjanenko ([3] - [6]) and Hellegouarch [10], but proved in a different manner, the last two are independent.

THEOREM 1. There are relatively prime integral divisors $A_1,\ldots,A_{\frac{p-1}{2}}$ and $B_1,\ldots,B_{\frac{p-1}{2}}$ of K such that - up to inessential factors -

$$a_4 \sim \prod_{i=1}^{\frac{p-1}{2}} A_i^p \ , \ a_2^2 - 4a_4 \sim \prod_{i=1}^{\frac{p-1}{2}} B_i^p \ ,$$

$$x_r \sim \prod_{i=1}^{\frac{p-1}{2}} A_i^{2\{ri\}_p} \ , \ \frac{y_r}{x_r} \sim \prod_{i=1}^{\frac{p-1}{2}} B_i^{\{ri\}_p}$$

for $rP = (x_r, y_r) \in E(K)_{\mathrm{tor}}$ of prime order p $(r=1,2,\ldots,p-1)$.

Here, for $a \in \mathbf{R}$, $\{a\}_p$ denotes the *distance* of a to the nearest integer in $p\mathbf{Z}$.

REMARK: In Theorem 1, the 2-isogenous curve

$$\tilde{E} : \tilde{y}^2 = \tilde{x}(\tilde{x}^2 + \tilde{a}_2\tilde{x} + \tilde{a}_4)$$

implicitly occurs, since

$$\tilde{a}_2 = -2a_2, \quad \tilde{a}_4 = a_2^2 - 4a_4$$

and

$$\tilde{P} = \left(\frac{y^2}{x^2}, \; y\,\frac{x^2 - a_4}{x^2}\right)$$

is the 2-isogenous point in $\tilde{E}(K)$ corresponding to

$$P = (x, y)$$

in $E(K)$.

Of course, $\tilde{E}$ is 2-deficient over K since E over K was assumed to have this property.

THEOREM 2. There is a finite field extension L of K, depending only on K, such that the mapping

$$(rP \; sP) \to Q_{r,s} = (x_{r,s}, \; y_{r,s})$$

for $r, \; s \in \{1,2,\ldots, p-1\}$ such that $r \not\equiv \pm s \pmod{p}$ yields rational points $Q_{r,s}$ on the auxiliary elliptic curve

$$E^1 : y^2 = x^3 - x$$

over L given via

$$x_{r,s} \cong \prod_{i=1}^{\frac{p-1}{2}} A_i^{\{(r+s)i\}_p - \{(r-s)i\}_p}$$

in L.

In fact, L is obtained from K by adjoining to the Hilbert class field of K all square roots of the roots of unity and of the fundamental units of K. We call the map appearing in Theorem 2 the *Demjanenko map*. Suppose now that the elliptic curve

$$E^1 : y^2 = x^3 - x$$

over L has

rank R (Theorem of Mordell-Weil)

and

number of integral points G (Theorem of Siegel).

The *crucial idea* of the proof is the following. If E over K possesses a torsion point $P = (x_1, x_1)$ of high prime order p we can construct more than G integer points $Q_{r,s} = (x_{r,s}, y_{r,s})$ on the auxiliary elliptic curve E^1 over L via the Demjanenko map.

THEOREM 3. At most

$$k \ (resp.\ \ell) \leq 2^{R+1} - 1$$

of the divisors $A_1,\ldots,A_{\frac{p-1}{2}}$ $(resp.\ B_1,\ldots,B_{\frac{p-1}{2}})$ of K are different from the unit divisor 1 of K.

Two cases are possible.

CASE 1: All divisors $A_1,\ldots,A_{\frac{p-1}{2}}$ $(resp.\ B_1,\ldots,B_{\frac{p-1}{2}})$ are equal to 1. Then

$$p \leq 2G + 1.$$

CASE 2: Exactly k $(resp.\ \ell)$ divisors, viz. $A_{\alpha_1},\ldots,A_{\alpha_k}$ $(resp.\ B_{\beta_1},\ldots,B_{\beta_\ell})$ are different from 1. Then

$$p \leq 2^2 \cdot 3^{2^{R+1}-1} \cdot G .$$

Here, again the A's are referring to the curve E over K whereas the B's refer to the 2-isogenous curve $\tilde{E}$ over K.

How does one ensure that the points $Q_{r,s} = (x_{r,s}, y_{r,s}) \in E^1(L)$ constructed via the Demjanenko map are all distinct and have integral coordinates?

Theorem 2 yields

$$x_{r,s} \cong \prod_{i=1}^{\frac{p-1}{2}} A_i^{\{(r+s)i\}_p - \{(r-s)i\}_p} .$$

It suffices therefore to find $r,s \in \{1,2,\ldots,p-1\}$, where $r \not\equiv \pm s \pmod p$, such that

$$\{(r+s)\alpha_i\}_p - \{(r-s)\alpha_i\}_p > 0$$

(*resp.* $\{(r+s)\beta_i\}_p - \{(r-s)\beta_i\}_p > 0$)

in case 2, case 1 being trivial.

This is accomplished by a theorem in elementary number theory which generalizes a classical theorem of Thue[1] and Scholz:

THEOREM 4. Let $\xi, \eta \in \mathbf{R}$ and $k, n \in \mathbf{N}$ be numbers such that

$$\xi, \eta > 1 \quad \text{and} \quad n > 2\xi^k\eta$$

and suppose that there are given integers $a_1,\ldots,a_k \in \mathbf{Z}$ such that

$$g.c.d.\ (a_i,n) = 1 \quad \text{for} \quad i = 1,2,\ldots,k.$$

[1] We learned from A. Schinzel that some other generalizations of Thue's theorem were obtained by Rédei [Acta Math. Acad. Sci. Hungar. 2 (1951), 75-82] and by Mordell [Proc. Amer. Math. Soc. 5 (1954), 854-859].

There exist at least

$$N \geq \frac{n}{2\xi^k \eta} > 1$$

distinct $(k + 1)$-tuples

$$(x_1, \ldots, x_k, y) \in \mathbb{N}^{k+1}$$

such that

$$x_1, \ldots, x_k \in \{1, 2, \ldots, \left\lfloor \frac{n}{\xi} \right\rfloor\}, \quad y \in \{1, 2, \ldots, \left\lfloor \frac{n}{\eta} \right\rfloor\}$$

satisfying the system of congruences

$$\begin{aligned} a_1 y &\equiv \pm x_1 \pmod{n}, \\ &\vdots \\ a_k y &\equiv \pm x_k \pmod{n}. \end{aligned}$$

COROLLARY 1. Let $K = Q(\sqrt{-p})$ be the imaginary quadratic field generated by a prime $p > 3$ such that $p \equiv 3 \pmod 4$. Then the torsion group of a 2-deficient elliptic curve E over K is, up to isomorphism, contained in one of the following groups:

$$E(K)_{\text{tor}} \leq \left\{ \begin{array}{l} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} \text{ for } m = 5,7,9 \text{ or } 24 \text{ if } p \equiv 3 \pmod 8 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16m\mathbb{Z} \text{ for } m = 9 \text{ or } 15 \text{ if } p \equiv 7 \pmod 8 \end{array} \right\}.$$

The proofs of these theorems and of Corollary 1 are to be found in [8].

4. EXPLICIT BOUNDS FOR 2-DEFICIENT ELLIPTIC CURVES

COROLLARY 2. Suppose E is a 2-deficient elliptic curve over an algebraic number field K satisfying the conditions (1) - (3) of Section 3. Then the prime order p of the torsion point $P = (x_1, y_1)$ on E over K satisfies

$$p \leq 2^2 \cdot 3^{2^{R+1}-1} \cdot G .$$

Here again R is the rank and G the number of integral points on the auxiliary elliptic curve $E^1: y^2 = x^3 - x$ over the finite extension field L over K depending only on K.

Now let S be the number of infinite primes of L. Then we have the

THEOREM (Silverman, [26]) There is a constant H depending only on K such that

$$G \leq H^{R+S+1} .$$

This is Silverman's recent quantitative version of Siegel's theorem on integral points on elliptic curves.

Hence we obtain the "explicit" bound (cf. [9], [27])

$$p \leq 2^2 \cdot 3^{2^{R+1}-1} \cdot H^{R+S+1} .$$

5. FURTHER IMPROVEMENT VIA ELEMENTARY NUMBER THEORY

The bounds in Theorem 3

$$k \leq 2^{R+1} - 1$$

and in Corollary 2

$$p \leq 2^2 \cdot 3^{2^{R+1}-1} \cdot H^{R+S+1}$$

can be considerably sharpened to (see [8], [9])

$$k \leq R + 1$$

and

$$p \leq 2^2 \cdot (3 \cdot H)^{R+1} \cdot H^S$$

provided the prime p would be known to be *non-exceptional*. This means that the rank of the *Demjanenko matrix* (see [9])

$$D^A = \begin{pmatrix} \varepsilon_1^A(r_1,s_1) & \dots & \varepsilon_k^A(r_1,s_1) \\ \vdots & \ddots & \vdots \\ \varepsilon_1^A(r_t,s_t) & \dots & \varepsilon_k^A(r_t,s_t) \end{pmatrix} \in \mathbf{F}_2^{t,k}$$

is

$$rk(D^A) = k$$

for all subsets

$$A = \{\alpha_1,\ldots,\alpha_k\} \subseteq \{1,2,\ldots,\frac{p-1}{2}\}$$

of cardinality k, where (r_i,s_i) ranges over all pairs of integers $(r,s) \in \mathbf{Z}^2$ such that $r,s \in \{1,2,\ldots,p-1\}$ and $r \not\equiv \pm s \pmod{p}$, and ε_i^A is defined by putting

$$\varepsilon_i^A(r,s) := 1 \ (resp.\ 0)$$

for

$$\{(r+s)\alpha_i\}_p - \{(r-s)\alpha_i\}_p > 0 \ \ (resp.\ < 0)\ .$$

Note that of the first 132 primes $p \geq 5$, at most 21 are exceptional for the choice $A = \{1,2,\ldots,\frac{p-1}{2}\}$. The first three exceptional primes are

$$p = 29,\ 113 \ \text{ and } \ 163$$

where

$$rk(D^A) = 11,\ 53 \text{ and } 79$$

instead of

$$k = \frac{p-1}{2} = 14,\ 56 \text{ and } 81\ ,$$

respectively.

We list the ranks of the Demjanenko matrices for these primes p in the subsequent table.

REMARK: During the congress we learned from E. Reyssat about the very interesting phenomenon that the same Demjanenko matrices D^A and the same exceptional primes p also occur in connection with the real subfield of the cyclotomic field of degree p when one wants to compute the rank of the totally positive cyclotomic units modulo squares.

Table

The rank of the Demjanenko matrix

p	rank	p	rank	p	rank	p	rank
5	2	7	3	11	5	13	6
17	8	19	9	23	11	29	11*
31	15	37	18	41	20	43	21
47	23	53	26	59	29	61	30
67	33	71	35	73	36	79	39
83	41	89	44	97	48	101	50
103	51	107	53	109	54	113	53*
127	63	131	65	137	68	139	69
149	74	151	75	157	78	163	79*
167	83	173	86	179	89	181	98
191	95	193	96	197	95*	199	99
211	105	223	111	227	113	229	114
233	116	239	116*	241	120	251	125
257	128	263	131	269	134	271	135
277	134*	281	140	283	141	293	146
307	153	311	145*	313	156	317	158
331	165	337	162*	347	173	349	170*
353	176	359	179	367	183	373	181*
379	189	183	191	389	194	397	194*
401	200	409	204	419	209	421	206*
431	215	433	216	439	219	443	221
449	224	457	228	461	230	463	228*
467	233	479	239	487	243	491	239*
499	249	503	251	509	254	521	260
523	261	541	270	547	271*	557	278
563	281	569	284	571	285	577	288
587	293	593	296	599	299	601	300
607	301*	613	306	617	308	619	309
631	315	641	320	643	321	647	323
653	326	659	326*	661	330	673	336
677	338	683	336*	691	345	701	347*
709	350*	719	359	727	363	733	366
739	369	743	371	751	371*	757	378

REFERENCES

[1] BASARAB, S.A., Some remarks concerning the torsion points of elliptic curves. *Revue Roum. Math. Pures et Appl.* 27 (1982), 621-642.

[2] CASSELS, J.W.S., Diophantine equations with special reference to elliptic curves. *J. London Math. Soc.* 41 (1966), 293-291.

[3] DEMJANENKO, V.A., On torsion points of elliptic curves. *Math. USSR Izv.* 4 (1970), 765-783.

[4] DEMJANENKO, V.A., Torsion of elliptic curves. *Math. USSR Izv.* 5 (1971), 289-318.

[5] DEMJANENKO, V.A., On the uniform boundedness of the torsion of elliptic curves over algebraic number fields. *Math. USSR Izv.* 6 (1972), 477-490.

[6] DEMJANENKO, V.A., Orders of the torsion of points of curves of genus 1. *J. Soviet Math.* 18 (1982), 843-861.

[7] FREY, G., Families of elliptic curves of bounded torsion. Preprint.

[8] FOLZ, H.G., Ein Beschränktheitssatz für die Torsion von 2-defizienten elliptischen Kurven über algebraischen Zahlkörpern. Dissertation, Saarbrücken 1985.

[9] FOLZ, H.G. and ZIMMER, H.G., What is the rank of the Demjanenko matrix? J. Symb. Comp. 4(1987), 53-67.

[10] HELLEGOUARCH, Y., Étude des points d'ordre fini des variétés abéliennes de dimension un définies sur un anneau principal. *J. reine angew. Math.* 244 (1970), 20-36.

[11] KAMIENNY, S., Points of order p on elliptic curves over $Q(\sqrt{p})$. *Math. Ann.* 261 (1982), 413-424.

[12] KAMIENNY, S., Torsion points on elliptic curves over all quadratic fields. *Duke Math. J.* 53 (1986), 157-162.

[13] KAMIENNY, S., On the torsion of elliptic curves over totally real fields. *Invent. Math.* 83 (1986), 545-551.

[14] KAMIENNY, S., Torsion points on elliptic curves over all quadratic fields II. Bull.Soc.Math.Math.France 114(1986),119-122.

[15] KAMIENNY, S., p-Torsion in elliptic curves over subfields of $Q(\mu_p)$. Math.Ann.280(1988),513-519.

[16] KENKU, M.A., Rational 2^n-torsion points on elliptic curves defined over quadratic fields. *J. London Math. Soc.* (2) 11 (1975), 93.

[17] KENKU, M.A., Certain torsion points on elliptic curves defined over quadratic fields. *J. London Math. Soc.* (2) 19 (1979), 233-240.

[18] KENKU, M.A., The modular curve $X_0(169)$ and rational isogeny. *J. London Math. Soc.* (2) 22 (1980), 239-244.

[19] KENKU, M.A., On the modular curves $X_0(125)$, $X_1(25)$ and $X_1(49)$. *J. London Math. Soc.* (2) 23 (1981), 415-427.

[20] KENKU, M.A., Rational torsion points on elliptic curves defined over quadratic fields. To appear. J.Niger.Math.Soc. 2(1983), 1-16.

[21] KUBERT, D.S., Universal bounds on the torsion of elliptic curves. *Compos. Math.* 38 (1979), 121-128.

[22] MANIN, Ju.I., The p-torsion of elliptic curves is uniformly bounded. *Math. USSR Izv.* 3 (1969), 433-438.

[23] MAZUR, B., Rational points on modular curves. In: *Modular Functions of One Variable V*, Bonn 1976. *Lect. Notes in Math.* 601 (1977), 107-148.

[24] MOMOSE, F., p-torsion points on elliptic curves defined over quadratic fields. *Nagoya Math. J.* 96 (1984), 139-165.

[25] SILVERMAN, J.H., Letter to the second author. Boston, Mass., 1985.

[26] SILVERMAN, J.H., A quantitative version of Siegel's theorem: integral points on elliptic curves and Catalan Curves. *J. reine angew. Math.* 378 (1987), 60-100.

[27] ZIMMER, H.G., Zur Arithmetik der elliptischen Kurven. *Bericht Nr.* 271 (1986) *der Math.-Stat. Sektion in der Forschungsgesellschaft Joanneum*, A-8010 Graz, Österreich, Steyrergasse 17.

HELMUT G. FOLZ and HORST G. ZIMMER
Fachbereich 9 Mathematik
Universität des Saarlandes
D-6600 Saarbrücken
F.R. of Germany

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

ON NON-UNIQUE FACTORIZATIONS INTO IRREDUCIBLE ELEMENTS II

GEROLDINGER A.

1. INTRODUCTION

Let H be a semigroup with divisor theory $\partial: H \to D$ and divisor class group G. Every element $a \in H \setminus H^\times$ has a (not necessarily unique) factorization $a = u_1 \ldots u_k$ into irreducible elements $u_1, \ldots, u_k$; k is called the length of the factorization and $L(a) = \{k / a$ has a factorization of length $k\}$ is called the set of lengths of a. One possibility to study non-unique factorization is to consider the sets L(a) for every $a \in H \setminus H^\times$.

The multiplicative semigroup of the ring of integers R of an algebraic number field K with ideal class group G is a most interesting example of a semigroup H with divisor theory. It is well known that R is factorial if and only if #G = 1. The following results back up the

opinion that R is the farer away from unique factorization the bigger G is, and they show that sets of lengths are a measure for non-uniqueness of factorization.

(i) $\#L(a) = 1$ for every $a \in R \setminus (R^\times \cup \{0\})$ if and only if $\#G \leq 2$ (Carlitz [2]).

(ii) If $\#G \geq 3$, then for every $m \in \mathbb{N}$ there is an element $a \in R$ with $\#L(a) = m$ (Śliwa [6]).

(iii) Let $\partial: H \to D$ be a divisor theory with divisor class group G and let $G_0 \subset G$ be a finite subset. Then there are constants $M(G_0)$ and $D(G_0)$ such that every set of lengths $L \in \mathcal{L}(G_0)$ has the following form:

$$L = \{x_1, \ldots, x_\alpha, y, y+\delta_1, \ldots\ldots\ldots, y+\delta_\mu, y+d,$$
$$y+\delta_1+d, \ldots\ldots\ldots\ldots, y+2d,$$
$$\ldots\ldots$$
$$y+\delta_1+(k-1)d, \ldots\ldots\ldots, y+kd, z_1, \ldots, z_\beta\}$$

with $x_1 < \ldots < x_\alpha < y < y+\delta_1 < \ldots < y+\delta_\mu \leq y+d \leq y+kd < z_1 < \ldots < z_\beta$, $0 \leq \alpha \leq M(G_0)$, $0 \leq \beta \leq M(G_0)$ and $1 \leq d \leq D(G_0)-2$ (Geroldinger [3]).

If μ is minimal such that L has a form as above and if L is sufficiently long, then $[\delta_1, \ldots, \delta_\mu d]$ is the period of L ([3]) and $\mu+1$ is called the length of the period.

In this paper I consider long sets of lengths with length of period 1 and using methods of diophantine approximation I study possible values of d in the case of

cyclic divisor class groups.

Arithmetical problems which arise in a semigroup H with divisor theory may be translated into combinatorial problems on the divisor class group. This idea goes back to Davenport and was further studied by Narkiewicz [4]. In this paper I use the combinatorial diction right from the beginning. But all combinatorial results have arithmetical analogues via the translation which is described in [3] (Proposition 1), and so they may be interpreted as arithmetical results on H.

2. NOTATIONS

Let G be an additively written abelian group and let $G_0 \subset G$ be a subset. Two sequences $b = (g_1,\ldots,g_m)$ and $b' = (g_1',\ldots,g_m')$ of elements of G_0 are called equivalent, if for some permutation $\sigma \in S_m$ $g_i' = g_{\sigma(i)}$ for every $i \in \{1,\ldots,m\}$. An equivalence class of sequences $B = \langle g_1,\ldots,g_m\rangle$ is called a block, if $g_1+\ldots+g_m = 0$. The equivalence class consisting of the empty sequence is called empty block. Let $v_g(B)$ denote the multiplicity of $g \in G_0$ in block B and let $\ell(B) = \sum_{g\in G_0} v_g(B) = m$ denote the length of B. The set $\mathcal{B}(G_0)$ of all blocks has a natural semigroup structure defined as follows:

$$\langle b_1,\ldots,b_m\rangle * \langle c_1,\ldots,c_n\rangle = \langle b_1,\ldots,b_m,c_1,\ldots,c_n\rangle$$

(The empty block is the unit element.) As usual a non-empty block $B \in \mathcal{B}(G_o)$ is called irreducible, if $B=B_1*B_2$ implies that B_1 or B_2 is the empty block. For every block $B \in \mathcal{B}(G_o)$ its set of lengths is defined as $L(B) = \{k/B$ has a factorization into k irreducible blocks$\}$; let $\mathcal{L}(G_o) = \{L(B)/B \in \mathcal{B}(B_o)\}$ denote the system of all sets of lengths corresponding to G_o.

Let $D(G_o) = \sup \{\ell(B)/B \in \mathcal{B}(G_o)$, B irreducible$\} \in \mathbb{N}_+ \cup \{\infty\}$ be the maximal length of an irreducible block. If G_o is a finite abelian group, then $D(G_o)$ is Davenport's constant. For $L = \{r_1,\ldots,r_s\} \in \mathcal{L}(G_o)$ with $r_1<\ldots<r_s$ let $\Delta(L) = \{r_{i+1}-r_i / 1 \leq i \leq s-1\}$ be the set of distances of successive lengths of L; further let $\Delta(G_o) = \bigcup_{L \in \mathcal{L}(G_o)} \Delta(L)$. Due to Proposition 3 in [3] $\Delta(G_o) \subset \{1,\ldots,D(G_o)-2\}$ and by virtue of Proposition 4 in [3] $\min \Delta(G_o) = \gcd \Delta(G_o)$.

3. SET OF LENGTHS $L \in \mathcal{L}(G_o)$ WITH PERIOD d

I investigate the period d (I briefly write d instead of [d]) of long sets of lengths with length of period 1. To do so I define $\Delta_1(G_o) = \{d/$for every $k \in \mathbb{N}$ there is an $L \in \mathcal{L}(G_o)$ with period d and $\#L \geq k\}$. Obviously $\Delta_1(G_o)$ does not depend on sets of lengths L for which #L is smaller than a fixed constant. Therefore it is without influence on $\Delta_1(G_o)$, that in [3] due to various reasons I assigned a period only to those sets of lengths L, for

which $\#L \geq P(G_o)$ holds ($P(G_o)$ is described in [3], see Remark 1 after Theorem 1). In the following also only the existence of the constants $M(G_o)$ and $P(G_o)$ is needed and their explicit numerical values, which I assigned to them in [3] , are without importance.

Now let $G_o \subset G$ be a finite subset. In the following propositions $\Delta_1(G_o)$ is studied. Obviously $\Delta_1(G_o)$ is contained in $\Delta(G_o)$ and hence $\Delta_1(G_o)$ is finite.

PROPOSITION 1. *If* $G_1 \subset G_o$ *with* $\Delta(G_1) \neq \emptyset$, *then* $\gcd\Delta(G_1) \in \Delta_1(G_o)$.

PROOF. Because $d = \gcd\Delta(G_1) \in \Delta(G_1)$ there is a block $C \in \mathcal{B}(G_1) \subset \mathcal{B}(G_o)$ such that $x, x+d \in L(C)$ for some $x \in \mathbb{N}$. For $k \in \mathbb{N}$ with $k \geq \max\{2M(G_o) + D(G_o) - 1, P(G_o)\}$ I consider $L(C^k)$. Since for some $y \in \mathbb{N}$ $\{y, y+d, \ldots, y+kd\} \subset L(C^k)$ and since $d = \min\Delta(G_1)$, $L(C^k)$ has period d. □

PROPOSITION 2. *For every* $d \in \Delta_1(G_o)$ *there is a subset* $G_1 \subset G_o$ *with* $\Delta(G_1) \neq \emptyset$ *such that* $d \mid \gcd\Delta(G_1)$ *In particular this implies* $d \mid \gcd\Delta(G_2)$ *for every* $G_2 \subset G_1$ *with* $\Delta(G_2) \neq \emptyset$.

PROOF. Let $G_1, \ldots, G_\psi$ be all subsets of $G_o = \{g_1, \ldots, g_m\}$ with $\Delta(G_i) \neq \emptyset$; let $d_i = \gcd\Delta(G_i)$ and let $C_i \in \mathcal{B}(G_i) \subset \mathcal{B}(G_o)$ be a block such that $x_i, x_i + d_i \in L(C_i)$ for some $x_i \in \mathbb{N}$.

Let $k=M(G_o)+2$ and let $(v_1,\dots,v_m) =$

$$= (\max_{i=1}^{\psi} v_{g_1}(C_i^k),\dots,\max_{i=1}^{\psi} v_{g_m}(C_i^k)).$$

Now let $d \in \Delta_1(G_o)$ and let $L = L(B)$ be a set of lengths with period d and $\#L > \max\{\frac{1}{2}(\sum_{i=1}^{m} v_i)(D(G_o)+2)(D(G_o)-2)+1,$ $2M(G_o)+2(D(G_o)-2),\ P(G_o)\}$. It has to be proved that $d \mid d_i$ for some $i \in \{1,\dots,\psi\}$.

Without restriction I assume $v_{g_i}(B) \geq v_i$ for $1 \leq i \leq \ell$ and $v_{g_i}(B) < v_i$ for $\ell+1 \leq i \leq m$; let $H_1 = \{g_1,\dots,g_\ell\}$ and $H_2 = \{g_{\ell+1},\dots,g_m\}$. H_1 is non-empty: since $H_1 = \emptyset$ would imply $\ell(B) < \sum_{i=1}^{m} v_i$, and thus by Lemma 3 in [3] it would follow

$$\#L \leq \frac{1}{2D(G_o)}(\sum_{i=1}^{m} v_i)(D(G_o)-2)+1.$$

$\Delta(H_1)$ is non-empty: for by Lemma 5 in [3] B may be written in the form $B = B_1 * B_2$ with $B_1 \in \mathcal{B}(H_1)$ and

$$\ell(B_2) \leq D(G_o) \sum_{g \in H_2} v_g(B) \leq D(G_o) \sum_{i=1}^{m} v_i.$$

If $\Delta(H_1) = \emptyset$, it would follow $\#L(B_1) = 1$ and so Lemma 4 in [3] would imply $\#L \leq \frac{1}{2}(\sum_{i=1}^{m} v_i)(D(G_o)-2)(D(G_o)+2)+1$.

Since $\Delta(H_1) \neq \emptyset$ I may assume without restriction

that $G_1 = H_1$. Then there exists a block $E \in \mathfrak{B}(G_o)$ with $B = C_1^k * E$ and an element $u \in \mathbb{N}$ such that

$\{u, u+d_1, \ldots, u+kd_1\} \subset L(B) = \{x_1, \ldots, x_\alpha, y, y+d, \ldots, y+wd, z_1, \ldots, z_\beta\}$,

where $x_1 < \ldots < x_\alpha < y < y+d < y+wd < z_1 < \ldots < z_\beta$, $\alpha \leq M(G_o)$, $\beta \leq M(G_o)$ and $1 \leq d \leq D(G_o)-2$. Since $k = M(G_o)+2$ and $\#L \geq 2M(G_o)+2(D(G_o)-2)$ there is an $s \in \{0, \ldots, k-1\}$ with $u+sd_1$, $u+(s+1)d_1 \in \{y, \ldots, y+wd\}$, and thus I get $d \mid d_1$. □

Summing up Proposition 1 and Proposition 2 it follows that $\{d/d = \gcd\Delta(G_1)$ with $G_1 \subset G_o$ and $\Delta(G_1) \neq \emptyset\} \subset \Delta_1(G_o) \subset \{d/d \mid \gcd\Delta(G_1)$ with $G_1 \subset G_o$ and $\Delta(G_1) \neq \emptyset\}$. Next I show that $\gcd\Delta(G_1)$ can be determined by solving an optimization problem, if the irreducible blocks in $\mathfrak{B}(G_1)$ are known. Concerning integral optimization see Burkard [1].

PROPOSITION 3. *Let* $G_o = \{g_1, \ldots, g_m\} \subset G$ *be a subset with* $\Delta(G_o) \neq \emptyset$; *let* $B_1, \ldots, B_\psi$ *be the irreducible blocks in* $\mathfrak{B}(G_o)$ *and let* $d = \min\Delta(G_o)$ $(= \gcd\Delta(G_o))$. *Then* d *is the solution of the following linear, integral optimization problem:*

Minimize $\sum_{i=1}^{\psi} x_i$

under the restrictions $\sum_{i=1}^{\psi} v_{g_j}(B_i) \cdot x_i = 0$, *for every* $j \in \{1, \ldots, m\}$

$\sum_{i=1}^{\psi} x_i > 0$

$x_i \in \mathbb{Z}$, *for every* $i \in \{1,\ldots,\psi\}$.

PROOF. According to Proposition 2.2 in [3] the set of irreducible blocks $B \in \mathcal{B}(G_o)$ is finite!

1. Every distance d of lengths of factorizations of a block $B \in \mathcal{B}(G_o)$ corresponds to a tuple $(x_1,\ldots,x_\psi)$ for which $d = \sum_{i=1}^{\psi} x_i$ holds and which satisfies the restrictions above: for let

$$B = B_1^{r_1} * \ldots * B_\psi^{r_\psi} = B_1^{s_1} * \ldots * B_\psi^{s_\psi} \text{ with } d = \sum_{i=1}^{\psi} s_i - \sum_{i=1}^{\psi} r_i ,$$

then $(s_1-r_1,\ldots,s_\psi-r_\psi)$ is a tuple satisfying the required properties.

2. Conversely, if $(x_1,\ldots,x_\psi)$ satisfies the restrictions above, then $\sum_{i=1}^{\psi} x_i$ is the distance of lengths of two factorizations of a block $B \in \mathcal{B}(G_o)$: for without loss of generality let $x_1<0,\ldots,x_{\psi_1}<0$, $x_{\psi_1+1}>0,\ldots x_{\psi_2}>0$ and $x_{\psi+1} = \ldots = x_\psi = 0$ then $B = B_1^{-x_1} * \ldots * B_{\psi_1}^{-x_{\psi_1}} = B_{\psi_1+1}^{x_{\psi_1+1}} * \ldots * B_{\psi_2}^{x_{\psi_2}}$ has the factorizations desired. □

Finishing this section I consider subsets G_o consisting of 2 elements.

PROPOSITION 4. *Let* $\#G_o = 2$ *and* $\Delta(G_o) \neq \emptyset$. *Then* $\Delta_1(G_o) = \{\gcd\Delta(G_o)\}$.

PROOF. Let $G_o = \{g,h\}$, $d = \gcd\Delta(G_o)$ and $C \in \mathcal{B}(G_o)$ such that $x, x+d \in L(C)$ for some $x \in \mathbb{N}$; let $k = \max\{2M(G_o)+D(G_o)-1,\ P(G_o)\}$.

Now let $L = L(B) \in \mathcal{B}(G_o)$; I prove that either L has period d or #L is bounded.

Case 1: $(v_g(B), v_h(B)) \geq (v_g(C^k), v_h(C^k)) = (v_1, v_2)$; then B may be written in the form $B = C^k * B_1$. Since $\{y, y+d, \ldots, y+kd\} \subset L(B)$ for some $y \in \mathbb{N}$ and since $d = \min\Delta(G_o)$, L(B) has period d.

Case 2: $(v_g(B), v_h(B)) \ngeq (v_1, v_2)$; without restriction let $v_g(B) < v_1$.

(i) h has infinite order: then $v_g(E) > 0$ for every block $E \in \mathcal{B}(G_o)$. If $B = B_1 * \ldots * B_k$ with irreducible blocks B_i. then $k \leq v_g(B) < v_1$, and thus $\#L(B) \leq \max L(B) < v_1$.

(ii) h has finite order: let $v_h(B) = \ell.\mathrm{ord}(h)+r$ with $0 \leq r < \mathrm{ord}(h)$; let $B = B_1 * B_2$ with $B_2 \in \mathcal{B}(\{h\})$ and $v_h(B_2) = \ell.\mathrm{ord}(h)$. So $\#L(B_2) = 1$ and $\ell(B_1) = r + v_g(B) < \mathrm{ord}(h) + v_1$. According to Lemma 4 in [3] $\#L(B) \leq$

$$\leq \frac{1}{2D(G_o)}(\mathrm{ord}(h)+v_1)(D(G_o)-2)(D(G_o)+2)+1. \quad \square$$

4. SETS OF LENGTHS L ∈ $\mathcal{L}(C_n)$ WITH PERIOD d

From now on let $G = C_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\} = \{0+n\mathbb{Z}, \ldots, (n-1)+n\mathbb{Z}\}$ be the finite cyclic group of order $n \geq 3$. In the following sections $\Delta_1(C_n)$ will be investigated. According to Proposition 1 $\{\gcd\Delta(G_0)/G_0 \subset C_n, \Delta(G_0) \neq \emptyset\} \subset \Delta_1(C_n)$. I shall determine $\gcd\Delta(G_0)$ of subsets $G_0 \subset C_n$ containing two elements and so I obtain a non-empty subset $M = \{\gcd\Delta(G_0)/G_0 \subset C_n, \#G_0 = 2, \Delta(G_0) \neq \emptyset\}$ of $\Delta_1(C_n)$. If n is a prime power, then M has the following property: for every $d \in \Delta_1(C_n)$ there exists a $\delta \in M$ with $d \mid \delta$ (Corollary 1).

Let $\overline{a}, \overline{b} \in C_n$ and $G_0 = \{\overline{a}, \overline{b}\}$; if $\Delta(G_0) \neq \emptyset$ I put $d(\overline{a}, \overline{b}) = \gcd\Delta(G_0)$. First I show that the investigation of $\mathcal{L}(\{\overline{a}, \overline{b}\})$ may be restricted to the case $\overline{b} = \overline{1}$, and I derive a relationship between the irreducible blocks in $\mathcal{B}(G_0)$ and $\Delta(G_0)$ which is easier to handle than the one described in Proposition 3. In section 6 I determine the irreducible blocks in $\mathcal{B}(G_0)$ and combining these results I obtain a formula for $\gcd\Delta(G_0)$ (Theorem 1, section 7).

PROPOSITION 5. *Let* $n \geq 3$, $a,b \in \{1,\ldots,n-1\}$ *and*

$$n_1 = \frac{n.\gcd(a,b,n)}{\gcd(a,n)\ \gcd(b,n)}.$$

1. *There exists a* $c \in \{1,\ldots,n_1-1\}$ *with* $\gcd(c,n_1)=1$ *such that* $\mathcal{L}(\{a+n\mathbb{Z}, b+n\mathbb{Z}\}) = \mathcal{L}(\{1+n_1\mathbb{Z}, c+n_1\mathbb{Z}\})$. *In*

particular $\Delta(\{a+n\mathbb{Z}, b+n\mathbb{Z}\}) = \Delta(\{1+n_1\mathbb{Z}, c+n_1\mathbb{Z}\})$.

2. $\Delta(\{a+n\mathbb{Z}, b+n\mathbb{Z}\}) = \emptyset$ *if and only if* $n_1 \leq 2$ *or* $\frac{a}{\gcd(a,n)} \equiv \frac{b}{\gcd(b,n)} \ (n_1)$ *holds.*

PROOF. Let $g = \gcd(a,b,n)$, $gg_1 = \gcd(a,n)$, $gh_1 = \gcd(b,n)$; then $n = gg_1h_1n_1$ and there are $a_1, b_1 \in \mathbb{N}$ such that $a = gg_1a_1$ and $b = gh_1b_1$.

1. Let $B \in \mathcal{B}(\{a+n\mathbb{Z}, b+n\mathbb{Z}\})$ with $v_{a+n\mathbb{Z}}(B) = k$ and $v_{b+n\mathbb{Z}}(B) = \ell$. Because of $ka + \ell b \equiv 0 \ (gg_1h_1n_1)$ there are $k_1, \ell_1 \in \mathbb{N}$ with $k = h_1k_1$ and $\ell = g_1\ell_1$. Let $B_1 \in \mathcal{B}(\{a_1+n_1\mathbb{Z}, b_1+n_1\mathbb{Z}\})$ be defined by $v_{a_1+n_1\mathbb{Z}}(B_1) = k_1$ and $v_{b_1+n_1\mathbb{Z}}(B_1) = \ell_1$. Let $c_1, c \in \mathbb{N}$ with $b_1c_1 \equiv 1 \ (n_1)$, $a_1c_1 \equiv c \ (n_1)$ and let $C \in \mathcal{B}(\{1+n_1\mathbb{Z}, c+n_1\mathbb{Z}\})$ with $v_{c+n_1\mathbb{Z}}(C) = k_1$ and $v_{1+n_1\mathbb{Z}}(C) = \ell_1$. Because $\gcd(a_1,n_1) = \gcd(c_1,n_1) = 1$ it follows $\gcd(a_1c_1,n_1) = 1$. I consider the map

$$\psi : \mathcal{B}(\{a+n\mathbb{Z}, b+n\mathbb{Z}\}) \to \mathcal{B}(\{1+n_1\mathbb{Z}, c+n_1\mathbb{Z}\})$$
$$B \mapsto \psi(B) = C.$$

Since B is irreducible if and only if $\psi(B)$ is irreducible, $L(A) = L(\psi(A))$ holds for every block $A \in \mathcal{B}(\{a+n\mathbb{Z}, b+n\mathbb{Z}\})$. The surjectivity of ψ now implies $\mathcal{L}(\{a+n\mathbb{Z}, b+n\mathbb{Z}\}) = \mathcal{L}(\{1+n_1\mathbb{Z}, c+n_1\mathbb{Z}\})$.

2. If $n_1 \leq 2$, then $\Delta(\{1+n_1\mathbb{Z}, c+n_1\mathbb{Z}\}) = \emptyset$; $a_1 \equiv b_1 \ (n_1)$ implies $1 \equiv c \ (n_1)$ and thus $\Delta(\{1+n_1\mathbb{Z}, c+n_1\mathbb{Z}\}) = \emptyset$ again. Now on the other hand let $n_1 \geq 3$ and $a_1 \not\equiv b_1 \ (n_1)$; then it

follows $1 \not\equiv c(n_1)$. I define three irreducible blocks: $A = \langle 1+n_1\mathbb{Z}, \ldots, 1+n_1\mathbb{Z} \rangle$, $B = \langle c+n_1\mathbb{Z} \rangle, \ldots, c+n_1\mathbb{Z}$ and $C = \langle c+n_1\mathbb{Z}, \ldots, c+n_1\mathbb{Z}, 1+n_1\mathbb{Z} \rangle$ with $v_{c+n_1\mathbb{Z}}(C) = k$ where k satisfies $kc+1 \equiv 0(n_1)$. The block $E = C^{n_1} = A^k * B$ has factorizations of different lengths. □

PROPOSITION 6. *Let* $n = p^k$ *with* p *prime and* $k \in \mathbb{N}_+$ *and in the case* $p = 2$ *let* $k \geq 2$. *Let* $G_o \subset C_n$ *with* $\Delta(G_o) \neq \emptyset$. *Then there exists a subset* $G_1 \subset G_o$ *with* $\Delta(G_1) \neq \emptyset$ *and* $\#G_o = 2$.

PROOF. I do the proof by induction on k.

(i) Let $p \geq 3$ and $k = 1$: because $\Delta(G_o) \neq \emptyset$ there are elements $a_1, a_2 \in \{1, \ldots, p-1\}$ with $a_1+p\mathbb{Z}, a_2+p\mathbb{Z} \in G_o$. According to Proposition 5.2 $\Delta(\{a_1+p\mathbb{Z}, a_2+p\mathbb{Z}\}) \neq \emptyset$.

(ii) Let $p = 2$ and $k = 2$: then $n = 4$ and the assertion is correct.

Now let $k \geq 2$ in the case $p \geq 3$ and let $k \geq 3$ in the case $p = 2$. Let $a_1, \ldots, a_m \in \{0, \ldots, p^k-1\}$ and let $G_o = \{a_1+p^k\mathbb{Z}, \ldots, a_m+p^k\mathbb{Z}\}$.

Case 1: there are a_i, a_j with $\gcd(a_i, p) = \gcd(a_j, p) = 1$. Then Propositon 5.2 implies $\Delta(\{a_i+p^k\mathbb{Z}, a_j+p^k\mathbb{Z}\}) \neq \emptyset$.

Case 2: $p \mid a_i$ for every $i \in \{1, \ldots, m\}$.

I define a map

$$\psi: (\{a_1+p^k\mathbb{Z}, \ldots, a_m+p^k\mathbb{Z}\}) \to (\{\frac{a_1}{p}+p^{k-1}\mathbb{Z}, \ldots, \frac{a_m}{p}+p^{k-1}\mathbb{Z}\})$$

$$B \mapsto \psi(B)$$

with $v_{\frac{a_i}{p}+p^{k-1}\mathbb{Z}}(\psi(B)) = v_{a_i+p^k\mathbb{Z}}(B)$ for every

$i \in \{1,\dots,m\}$.

Since ψ is an isomorphism and since $\Delta(\{a_1+p^k\mathbb{Z},\dots,a_m+p^k\mathbb{Z}\}) \neq \emptyset$ by assumption, it follows that $\Delta(\{\frac{a_1}{p}+p^{k-1}\mathbb{Z},\dots,\frac{a_m}{p}+p^{k-1}\mathbb{Z}\}) \neq \emptyset$. By induction hypothesis there are a_i, a_j such that $\Delta(\{\frac{a_i}{p}+p^{k-1}\mathbb{Z}, \frac{a_j}{p}+p^{k-1}\mathbb{Z}\}) \neq \emptyset$. This implies $\Delta(\{a_i+p^k\mathbb{Z}, a_j+p^k\mathbb{Z}\}) \neq \emptyset$.

Case 3: there is exactly one index $i \in \{1,\dots,m\}$ with $p \nmid a_i$.

Without restriction I assume $i = 1$. Let $p^j = \min\{\gcd(a_\ell, p^k) / 2 \leq \ell \leq m\}$ and let $G_1 = \{a_1p^j+p^k\mathbb{Z}, a_2+p^k\mathbb{Z}, \dots, a_m+p^k\mathbb{Z}\}$. Now I claim $L(G_0) = L(G_1)$ (Then it is sufficiently to consider $\mathcal{B}(G_1)$, and so Case 3 is reduced to Case 2). I define a map

$$\psi: \mathcal{B}(G_0) \to \mathcal{B}(G_1)$$

$$v_{a_1p^j+p^k\mathbb{Z}}(\psi(B)) = \frac{1}{p^j} v_{a_1+p^k\mathbb{Z}}(B) + v_{a_1p^j+p^k\mathbb{Z}}(B)$$

$$v_{a_i+p^k\mathbb{Z}}(\psi(B)) = v_{a_i+p^k\mathbb{Z}}(B), \text{ for } a_i+p^k\mathbb{Z} \in G_0$$

and

$$a_i+p^k\mathbb{Z} \neq a_1p^j+p^k\mathbb{Z}$$

Since B is irreducible if and only if $\psi(B)$ is irreducible, $L(A) = L(\psi(A))$ holds for every $A \in \mathcal{B}(G_0)$. The

surjectivity of ψ implies $L(G_o) = L(G_1)$. □

REMARK. Proposition 6 does not remain valid if n is not a prime power but an arbitrary integer.

COROLLARY 1. *Let* $n=p^k$ *with* p *prime*, $k \in \mathbb{N}_+$ *and in the case* $p=2$ *let* $k \geq 2$. *Let* $G_o \subset C_n$ *and* $d \in \Delta_1(G_o)$. *Then there exist* $\overline{a},\overline{b} \in G_o$ *with* $d \mid d(\overline{a},\overline{b})$.

PROOF. The assertion follows immediately from Proposition 2 and Proposition 6. □

For every block $B \in \mathcal{B}(C_n)$ I define $S(B)$ (= "sum of the elements in B") by $S(B) = \sum_{i=1}^{n-1} i.v_{\overline{i}}(B)$; of course $S(B) \equiv 0(n)$ holds.

PROPOSITION 7. *Let* $\overline{1} \in G_o \subset C_n$, $\Delta(G_o) \neq \emptyset$ *and* $d = \gcd\Delta(G_o)$. *Then* $d=\gcd\{\frac{1}{n}S(B)-1 / B \in \mathcal{B}(G_o)$ *irreducible*, $B \neq <\overline{0}>\}$.

PROOF.

1. Assertion: if $B \in \mathcal{B}(G_o)$, $B \neq <\overline{0}>$, is an irreducible block, then $d \mid \frac{1}{n}S(B)-1$.

Proof: let $B=<\overline{a_1},\ldots,\overline{a_m}>$ with $a_1,\ldots,a_m \in \{1,\ldots,n-1\}$ and let $\gamma = \frac{1}{n}S(B) = \frac{1}{n}\sum_{i=1}^{m} a_i$. Let $A_1 = <\overline{1},\ldots,\overline{1}>$ with $v_{\overline{1}}(A_1) = n$. I define a block $C \in \mathcal{B}(G_o)$ having the following two factorizations into irreducible blocks:

$$C = B * A_1^{m-\gamma} = \underset{i=1}{\overset{m}{*}} \langle \overline{a_i}, \overline{1}, \ldots, \overline{1} \rangle$$

$$(v_{\overline{1}}(C) = v_{\overline{1}}(B) + n(m-\gamma) = \sum_{i=1}^{m} (n-a_i) + v_{\overline{1}}(B) \ !)$$

Hence C may be written as a product of $(m-\gamma)+1$ and as a product of m irreducible blocks, and therefore $d \mid m-(m-\gamma+1)$.

2. Assertion: let $\{\frac{1}{n}S(B) \ / B \in \mathfrak{B}(B_o)$ irreducible, $B \neq \langle \overline{0} \rangle\} = \{m_1, \ldots, m\}$ and let $\delta \in \Delta(G_o)$. Then $\gcd\{m_i - 1 / 1 \leq i \leq \psi\} \mid \delta$.

Proof: there is a block $B \in \mathfrak{B}(G_o)$ having the following factorizations into irreducible blocks:

$$B = (A_{1,1} * \ldots * A_{1,k_1}) * \ldots * (A_{\psi,1} * \ldots * A_{\psi,k_\psi})$$
$$= (C_{1,1} * \ldots * C_{1,\ell_1}) * \ldots * (C_{\psi,1} * \ldots * C_{\psi,\ell_\psi}),$$

with $\sum_{i=1}^{\psi} \ell_i - \sum_{i=1}^{\psi} k_i = \delta$ and $S(A_{i,r}) = S(C_{i,s}) = n \cdot m_i$.

Because $S(B) = \sum_{i=1}^{\psi} k_i m_i n = \sum_{i=1}^{\psi} \ell_i m_i n$ it follows $\sum_{i=1}^{\psi} (k_i - \ell_i) m_i = 0$ and therefore $\delta = \sum_{i=1}^{\psi} (k_i - \ell_i)(m_i - 1)$; this implies $\gcd\{m_i - 1 / 1 \leq i \leq \psi\} \mid \delta$. □

In the following let $a \in \{1, \ldots, n-1\}$, $\gcd(a,n) = 1$, $\overline{a} = a + n\mathbb{Z}$ and $\overline{1} = 1 + n\mathbb{Z}$. In order to describe all irreducible blocks in $\mathfrak{B}(\{\overline{1}, \overline{a}\})$ I denote for every $m \in \{0, \ldots, n\}$ with B(m) that block in $\mathfrak{B}(\{\overline{1}, \overline{a}\})$ with $v_{\overline{1}}(B(m)) = m$ for which $v_{\overline{a}}(B(m))$ is minimal. Then every

irreducible block $B \in \beta(\{\overline{1},\overline{a}\})$ is of the form $B = B(m)$ for some $m \in \{0,\ldots,n\}$.

For $x \in \mathbb{R}$ let $[x] = \max\{g \in \mathbb{Z} / g \leq x\}$; let $\ell_1 \in \{1,\ldots,n-1\}$ with $a\ell_1+1 \equiv 0 \quad (n)$; for $N \in \mathbb{N}$ let $m_N = [N\frac{n}{\ell_1}] + 1$; then $i < j$ implies $m_i < m_j$ and the following Proposition holds:

PROPOSITION 8.

1. *For* $i \in \{1,\ldots,n-1\}$ *let* $N \in \mathbb{N}$ *be maximal with* $m_N \leq i$. *Then* $v_{\overline{a}}(B(i)) = \ell_1 i - Nn$.
2. *For every irreducible block* $B \in \beta(\{\overline{1},\overline{a}\})$, $B \neq B(0)$, $B \neq B(n)$ *there exists an* $N \in \{0,\ldots,\ell_1-1\}$ *such that* $B = B(m_N)$.

PROOF.

1. $m_N \leq n-1$ implies $N \in \{0,\ldots,\ell_1-1\}$. Because $Nn < m_N\ell_1 \leq i\ell_1 \leq (m_{N+1}-1)\ell_1 \leq (N+1)n$ I obtain $0 < i\ell_1 - Nn \leq n$; and since $(\ell_1 i - Nn)a + i \equiv 0(n)$ I get $\ell_1 i - Nn < n$ and thus $v_{\overline{a}}(B(i)) = \ell_1 i - Nn$.

2. As I noticed above $B = B(i)$ with $i \in \{1,\ldots,n-1\}$; let $N \in \mathbb{N}$ be maximal with $m_N \leq i$. Since $v_{\overline{1}}(B(m_N)) = m_N \leq i = v_{\overline{1}}(B(i))$ and since $B(i)$ is irreducible I obtain $\ell_1 i - Nn = v_{\overline{a}}(B(i)) \leq v_{\overline{a}}(B(m_N)) = \ell_1 m_N - Nn$ and thus $i = m_N$. □

LEMMA 1. *Let* $n \in \{0,\dots,\ell_1-1\}$. *Then the following conditions are equivalent:*

1. $B(m_N)$ *is irreducible.*
2. $m_N - m_{N_1} < \frac{n}{\ell_1}(N-N_1)$ *for every* $N_1 \in \{0,\dots,N-1\}$.
3. $m_N - m_{N_2} < \frac{n}{\ell_1}(N-N_2)$ *with*

$N_2 = \max\{k/k \in \{0,\dots,N-1\},\ B(m_k)$ *irreducible*$\}$.

PROOF.

1. $\Rightarrow$ 2.: $v_{\overline{1}}(B(m_{N_1})) = m_{N_1} < m_N = v_{\overline{1}}(B(m_N))$ for $N_1 < N$; since $B(m_N)$ is irreducible, it follows $m_{N_1}\ell_1 - N_1 n = v_{\overline{a}}(B(m_{N_1})) > v_{\overline{a}}(B(m_N)) = m_N\ell_1 - Nn$.

2. $\Rightarrow$3.: obvious.

3. $\Rightarrow$1.: assume $B(m_N)$ is not irreducible. Then there is an $N_1 < N$ with $B(m_{N_1})$ irreducible and $B(m_N) = B(m_{N_1}) * C$; hence $m_{N_1}\ell_1 - N_1 n = v_{\overline{a}}(B(m_{N_1})) \leq v_{\overline{a}}(B(m_N)) = m_N\ell_1 - Nn$. $(N_1 \leq N_2)$ implies $v_{\overline{1}}(B(m_{N_1})) = m_{N_1} \leq m_{N_2} = v_{\overline{1}}(B(m_{N_2}))$. Since $B(m_{N_2})$ is irreducible it follows $m_{N_2}\ell_1 - N_2 n = v_{\overline{a}}(B(m_{N_2})) \leq v_{\overline{a}}(B(m_{N_1})) = m_{N_1}\ell_1 - N_1 n$. Thus $m_{N_2}\ell_1 - N_2 n \leq m_{N_1}\ell_1 - N_1 n \leq m_N\ell_1 - Nn$, a contradiction. □

COROLLARY 2. *Let* $a \in \{2,\dots,n-1\}$, $\gcd(a,n)=1$, $n = ak+j$ *with* $k \in \mathbb{N}$ *and* $0 < j < a$. *Then*

$$d(\overline{1},\overline{a}) = \gcd\{a-1, \frac{a\ell_1+1}{n} - 1, [N\frac{n}{\ell_1}] - N/N \in \{1,\dots,\ell_1-1\}, B(m_N) \text{ irreducible}\}$$

$$= \gcd\{a-1, \frac{a\ell_1+1}{n} - 1, [N\frac{n}{\ell_1}] - N/m_N \in \{2,\dots,j-1\}, B(m_N) \text{ irreducible}\}.$$

($m_N \leq j-1$ *implies* $N<\ell_1 - 1$).

PROOF. Since $v_{\overline{1}}(B(m_N)) = m_N$ and $v_{\overline{a}}(B(m_N)) = m_N\ell_1 - Nn$ I get $S(B(m_N)) = a(m_N\ell_1 - Nn) + m_N = n(m_N(\frac{a\ell_1+1}{n}) - aN)$. Thus Proposition 6 and Proposition 7 imply

$$d(\overline{1},\overline{a}) = \gcd\{a-1, m_N(\frac{a\ell_1+1}{n}) - aN - 1/$$

$$N \in \{0,\dots,\ell_1-1\}, B(m_N) \text{ irreducible}\}$$

$$= \gcd\{a-1, \frac{a\ell_1+1}{n} - 1, [N\frac{n}{\ell_1}] - N/$$

$$N \in \{1,\dots,\ell_1-1\}, B(m_N) \text{ irreducible}\}.$$

If $B(i)$ with $i \in \{j,\dots,n\}$ is irreducible, then $S(B(i)) = av_{\overline{a}}(B(i)) + i \leq ak+i \leq ak+n < 2n$ implies $S(B(i))=n$; and hence

$$d(\overline{1},\overline{a}) = \gcd\{a-1, \frac{a\ell_1+1}{n} - 1, [N\frac{n}{\ell_1}] - N/m_N \in \{2,\dots,j-1\}, B(m_N) \text{ irreducible}\}.$$

$m_N \leq j-1$ implies $N\frac{n}{\ell_1} < j-1$ and therefore $N < \frac{\ell_1(j-1)}{n} =$

$= \frac{\ell_1(n-ak-1)}{n} = \ell_1 - \frac{\ell_1}{n}(ak+1)$; so it follows

$a\ell_1 k+\ell_1 \geq a\ell_1+1 \geq n$ and thus $N<\ell_1-1$. □

5. DETERMINATION OF [Nα] FOR RATIONAL α

Let $\alpha \in \mathbb{Q}$, $\alpha > 0$, $N \in \mathbb{N}$ and let $\alpha = [a_o;a_1,\ldots,a_m]$ be a continued fraction expansion of α with partial quotients a_i. I shall derive a formula for $[N\alpha]$ involving only the partial quotients a_i. In doing so I rely on a paper of J.Schoissengeier who settled this problem for irrational α (see [5]).

As usual let for $i \in \{1,\ldots,m\}$ $\frac{p_i}{q_i}$ denote the convergents of $\alpha = \frac{p_m}{q_m}$ and let $p_{-2} = 0$, $q_{-2} = 1$, $p_{-1}=1$ and $q_{-1} = 0$.

LEMMA 2. *For* $N \in \{0,\ldots,q_m-1\}$ *there are uniquely determined rational integers* t, $0 \leq t < m$, *and* $b_o,\ldots,b_t$ *having the following properties:*

1. $N = \sum_{i=o}^{t} b_i q_i$.

2. $b_t > 0$ *and* $0 \leq b_i \leq a_{i+1}$ *for every* $i \in \{0,\ldots,t\}$.

3. *If* $0 < i \leq t$ *and* $b_i = a_{i+1}$, *then* $b_{i-1} = 0$.

Furthermore $b_o < a_1$.

PROOF. Let t be determined by $q_t \leq N < q_{t+1}$ and let the integers b_i be determined in the following manner:

$$N = N_t = b_t q_t + N_{t-1} \ , \ 0 \leq N_{t-1} < q_t$$

$$\cdots\cdots\cdots$$

$$N_i = b_i q_i + N_{i-1} \ , \ 0 \leq N_{i-1} < q_i$$

$$\cdots\cdots\cdots$$

$$N_o = b_o q_o \ , \ N_{-1} = 0$$

1. $N_i = \sum_{j=0}^{i} b_j q_j$ for every $i \in \{0,\ldots,t\}$.

2. Obviously $(b_t > 0)$ holds and for every $i \in \{0,\ldots,t\}$ $N_i = b_i q_i + N_{i-1}$ and $q_{i+1} = a_{i+1} q_i + q_{i-1}$ imply

$(a_{i+1}+1) q_i \geq q_{i+1} > N_i$ and thus $b_i \leq a_{i+1}$.

3. Let $b_i = a_{i+1}$ for some $i \in \{1,\ldots,t\}$. Since $N_i = b_i q_i + N_{i-1} < q_{i+1} = a_{i+1} q_i + q_{i-1}$ I obtain $N_{i-1} < q_{i-1}$ and therefore $b_{i-1} = 0$; $N_o < q_1 = a_1$ and $q_o = 1$ imply $b_o < a_1$.

If $j \in \{0,\ldots,m-1\}$ and $b_o,\ldots,b_j$ have the above properties, then $\sum_{i=0}^{j} b_i q_i < q_{j+1}$. This implies the uniqueness of the representation of N. □

LEMMA 3.

1. *Let* $0 \leq 2k \leq t \leq m$. *Then*

$$-(q_{2k}\alpha - p_{2k}) \leq \sum_{2k+2 \leq 2i \leq t} a_{2i}(q_{2i-1}\alpha - p_{2i-1}).$$

2. *Let* $0 \leq 2k+1 \leq t \leq m$. *Then*

$$q_{2k-1}\alpha - p_{2k-1} \leq \sum_{2k+1 \leq 2i+1 \leq t} a_{2i+1}(q_{2i}\alpha - p_{2i}).$$

PROOF.

1. Let $s = [\frac{m}{2}]$; $\sum_{2k+2 \leq 2i \leq t} a_{2i}(q_{2i-1}\alpha - p_{2i-1}) \geq$

$\geq \sum_{i=k+1}^{s} a_{2i}(q_{2i-1}\alpha - p_{2i-1}) = \sum_{i=k+1}^{s} ((q_{2i} - q_{2i-2})\alpha -$

$- (p_{2i} - p_{2i-2})) = (q_{2s} - q_{2k})\alpha - (p_{2s} - p_{2k}) = -(q_{2k}\alpha - p_{2k}) +$

$+ (q_{2s}\alpha - p_{2s})$. If m is even, then $s = \frac{m}{2}$ and $q_{2s}\alpha - p_{2s} =$

$q_m\alpha - p_m = 0$. If m is odd, then $s = \frac{m-1}{2}$ and $q_{2s}\alpha - p_{2s} =$

$q_{m-1}\alpha - p_{m-1} \geq 0$.

2. Similar to 1. □

LEMMA 4. *Let* $N = \sum_{i=0}^{t} b_i q_i$ *with* $0 \leq t < m$. *Then*

1. $-(q_{2k}\alpha - p_{2k}) \leq \sum_{i=2k}^{t} b_i(q_i\alpha - p_i) \leq -(q_{2k-1}\alpha - p_{2k-1})$ *with*

$0 \leq 2k \leq t$.

If $b_{2k} > 0$, *so* $\sum_{i=2k}^{t} b_i(q_i\alpha - p_i) \geq 0$.

2. $q_{2k+1}\alpha - p_{2k+1} < -\sum_{i=2k+1}^{t} b_i(q_i\alpha - p_i) \leq q_{2k}\alpha - p_{2k}$ *with*

$0 \leq 2k+1 \leq t$.

If $b_{2k+1} > 0$, *so* $\sum_{i=2k+1}^{t} b_i(q_i\alpha - p_i) \leq 0$.

PROOF.

1. $-(q_{2k}\alpha - p_{2k}) \leq \sum_{2k+2\leq 2i\leq t+1} a_{2i}(q_{2i-1}\alpha - p_{2i-1}) \leq$

$\leq \sum_{2k+1\leq 2i-1\leq t} b_{2i-1}(q_{2i-1}\alpha\, p_{2i-1}) \leq \sum_{i=2k+1}^{t} b_i(q_i\alpha - p_i) \leq$

$\leq \sum_{i=2k}^{t} b_i(q_i\alpha - p_i) \leq \sum_{2k\leq 2i\leq t} b_{2i}(q_{2i}\alpha - p_{2i}) \leq$

$\leq \sum_{2k\leq 2i\leq t} a_{2i+1}(q_{2i}\alpha - p_{2i}) \leq -(q_{2k-1}\alpha - p_{2k-1})$.

In particular it follows $-(q_{2k}\alpha - p_{2k}) \leq$

$\leq \sum_{i=2k+1}^{t} b_i(q_i\alpha - p_i)$. If $b_{2k} > 0$, then

$0 \leq -(q_{2k}\alpha - p_{2k}) + b_{2k}(q_{2k}\alpha - p_{2k}) \leq \sum_{i=2k}^{t} b_i(q_i\alpha - p_i)$.

2. Similar to 1. □

PROPOSITION 9.

1. *Let* $N = \sum_{i=2k}^{t} b_i q_i$ *with* $0 \leq 2k \leq t < m$ *and* $b_{2k} > 0$.

Then $[N\alpha] = \sum_{i=2k}^{t} b_i p_i$.

2. *Let* $N = \sum_{i=2k+1}^{t} b_i q_i$ *with* $0 \leq 2k+1 \leq t < m$ *and* $b_{2k+1} > 0$.

Then $[N\alpha] = \sum_{i=2k+1}^{t} b_i p_i - 1$.

PROOF.

1. It has to be proved that

$$\sum_{i=2k}^{t} b_i p_i \leq \sum_{i=2k}^{t} b_i q_i \alpha < \sum_{i=2k}^{t} b_i p_i + 1$$

The left inequality follows from Lemma 4.1. Considering the right inequality note that $\sum_{i=2k}^{t} b_i (q_i\alpha - p_i) \leq$

$\leq p_{2k-1} - q_{2k-1}\alpha$.

If $k \geq 1$, then $\frac{p_{2k-1}}{q_{2k-1}} - \alpha < \frac{1}{q_{2k-1}q_{2k}} \leq \frac{1}{q_{2k-1}}$ holds and

thus $p_{2k-1} - q_{2k-1}\alpha < 1$. For $k = 0$ $p_{2k-1} - q_{2k-1}\alpha = 1$ and therefore $\sum_{i=2k}^{t} b_i (q_i\alpha - p_i) \leq 1$; but since $(\sum_{i=2k}^{t} b_i q_i)\alpha \in \mathbb{N}$

equality doesn't hold.

2. Similar to 1. □

6. DETERMINATION OF THE IRREDUCIBLE BLOCKS IN $B(\{1+n\mathbb{Z}, a+n\mathbb{Z}\})$

Let $n \geq 3$, $a, \ell_1 \in \{1,\ldots,n-1\}$, $\gcd(a,n) = 1$, $a\ell_1+1 \equiv 0(n)$. Further let $\alpha = \frac{n}{\ell_1} = [a_o; a_1,\ldots,a_m]$ be a continued fraction expansion of α with convergents $\frac{p_i}{q_i}$ for $i \in \{1,\ldots,m\}$. Proposition 8 states that

$$\{B \in \mathcal{B}(\{1+n\mathbb{Z}, a+n\mathbb{Z}\}) / B \neq B(0), B \neq B(n), B \text{ irreducible}\}$$

$$\subset \{B(m_N)/m_N = [N\alpha]+1, N \in \{0,\ldots,\ell_1-1\}\}.$$

In this section I determine these $N \in \{0,\ldots\ell_1-1\}$ for which $B(m_N)$ is irreducible.

LEMMA 5. *$B(m_N)$ is not irreducible for the following N:*

1. $N = \sum_{i=j}^{t} b_i q_i$ *with* $0 \leq j < t < m$, $b_j > 0$, *and* $b_{2k+1} > 0$ *for some* k *with* $j < 2k+1 \leq t$.

2. $N = \sum_{i=2k+1}^{t} b_i q_i$ *with* $0 < 2k+1 \leq t < m$ *and* $b_{2k+1} \geq 2$.

3. $N = \sum_{i=2k}^{t} b_i q_i$ *with* $2 \leq 2k \leq t < m$ *and* $b_{2k} > 0$.

4. $N = b_o q_o + b_{2k} q_{2k} + \sum_{i=2k+1}^{t} b_i q_i$ *with* $2 \leq 2k \leq t < m$, $b_o > 0$ *and* $b_{2k} > 0$.

5. $N = q_{2k+1}+b_{2\ell}q_{2\ell}+b_{2\ell+2}q_{2\ell+2}+\sum_{i=2\ell+3}^{t} b_i q_i$ *with*

$0 < 2k+1 < 2\ell < 2\ell+2 \leq t < m$, $b_{2\ell} < a_{2\ell+1}$ *and* $b_{2\ell+2} > 0$.

PROOF. In each of the five cases I show the existence of an $N' < N$ with $[N\alpha]-[N'\alpha] > \alpha(N-N')$. Then the assertion follows by Lemma 1.

1. and 2. For $N' = N-q_{2k+1}$ I get $[N\alpha]-[N'\alpha] = p_{2k+1} > \alpha q_{2k+1} = \alpha(N-N')$.

3. For $N' = N+q_{2k-1}-q_{2k}$ I get $[N\alpha]-[N'\alpha] = p_{2k}-p_{2k-1}+1$ and $(N-N') = q_{2k}-q_{2k-1}$. It is well known that $\frac{p_{2k}-p_{2k-1}+1}{q_{2k}-q_{2k-1}} \geq \frac{p_{2k-1}}{q_{2k-1}} > \alpha$, which implies $p_{2k}-p_{2k-1}+1 > \alpha(q_{2k}-q_{2k-1})$.

4. Case 1: $b_o \leq a_1-2$. For $N' = (b_o+1)q_o+(b_{2k}-1)q_{2k}+\sum_{i=2k+1}^{t} b_i q_i$ I obtain $[N\alpha]-[N'\alpha] = p_{2k}-p_o$ and $N-N' = q_{2k}-q_o$. Now for every $\ell \in \{1,\ldots,k\}$ $(q_{2\ell}\alpha-p_{2\ell}) < (q_{2\ell-2}\alpha-p_{2\ell-2})$ holds and therefore it follows

$(q_{2k}\alpha-p_{2k}) < (q_o\alpha-p_o)$.

Case 2: $b_o = a_1-1$. For $N'=q_1+(b_{2k}-1)q_{2k}+\sum_{i=2k+1}^{t} b_iq_i$

I obtain $[N\alpha]-[N'\alpha]=(a_1-1)p_o+p_{2k}-p_1+1=p_{2k}-p_o>\alpha(q_{2k}-q_o)=$

$=\alpha((a_1-1)q_o+q_{2k}-q_1) = \alpha(N-N')$.

5. Case 1: ($b_{2\ell} \leq a_{2\ell+1}-2$) or ($b_{2\ell}=a_{2\ell+1}-1$ and $\ell>k+1$). For $N'=q_{2k+1}+(b_{2\ell}+1)q_{2\ell}+(b_{2\ell+2}-1)q_{2\ell+2}+$

$+\sum_{i=2\ell+3}^{t} b_iq_i$ I get $[N\alpha]-[N'\alpha]= p_{2\ell+2}-p_{2\ell}=a_{2\ell+2}p_{2\ell+1} >$

$>\alpha a_{2\ell+2}q_{2\ell+1} = \alpha(q_{2\ell+2}-q_{2\ell}) = \alpha(N-N')$.

Case 2: $b_{2\ell} = a_{2\ell+1}-1$ and $\ell=k+1$. Then $2\ell-1 =$

$= 2k+1$. For $N' =q_{2\ell+1}+(b_{2\ell+2}-1)q_{2\ell+2}+\sum_{i=2\ell+3}^{t} b_iq_i$ I get

$[N\alpha]-[N'\alpha]= p_{2\ell-1}+(a_{2\ell+1}-1)p_{2\ell}-p_{2\ell+1}+p_{2\ell+2}=p_{2\ell+2}-p_{2\ell}=$

$= a_{2\ell+2}p_{2\ell+1}>\alpha\ a_{2\ell+2}q_{2\ell+1} = \alpha(N-N')$. □

PROPOSITION 10. *Let* $N \in \{1,\ldots,q_m-1\}$. *Then* $B(m_N)$ *is irreducible if and only if* N *has the form* (i) *or* (ii):

(i) $N =q_{t-1}+b_tq_t$ *with* $b_t \in \{1,\ldots,a_{t+1}-1\}$, $t \equiv 0(2)$ *and* $0 \leq t < m$

(ii) $N = q_t$ *with* $t \equiv 1(2)$ *and* $0 \leq t < m$

PROOF.

1. Assertion: if $B(m_N)$ is irreducible, then N has the form (i) or (ii).

Proof: let $B(m_N)$ be irreducible and let $q_t \leq N < q_{t+1}$ with $0 \leq t < m$; then $N = \sum_{i=o}^{t} b_i q_i$ with $b_t > 0$.

Case 1: $t \equiv 0(2)$. Using Lemma 5.1, 5.3 and 5.4 I see that $j = \min\{i/0 \leq i \leq t, b_i > 0\}$ is odd. Let $j=2k+1$. From 5.2 I deduce $b_{2k+1} = 1$; hence $N = q_{2k+1} + \sum_{i=2k+2}^{t} b_i q_i$. By Lemma 5.1 I conclude that $b_i = 0$ for every odd $i \in \{2k+2,\ldots,t\}$. $t > 2k+2$ would imply the existence of an ℓ with $2\ell \in \{2k+2,\ldots,t-2\}$ and $b_{2\ell} < a_{2\ell+1}$, $b_{2\ell+2} > 0$ (for $b_{2k+2} < a_{2k+3}$ and $b_{2t} > 0$) and so N would be of the form 5.5. Thus $2k+2 = t$ and $N = q_{t-1} + b_t q_t$ with $b_t \in \{1,\ldots,a_{t+1}-1\}$.

Case 2: $t \equiv 1(2)$. By 5.1 I get $b_o = \ldots = b_{t-1} = 0$ and by 5.2 I get $b_t = 1$; hence $N = q_t$.

2. Assertion: if N is of the form (i) or (ii), then $B(m_N)$ is irreducible.

Proof: I do the proof by induction on N having a form as above.

Let N=1 ($N = q_{-1}+q_o$ for $a_1 > 1$, $N=q_1$ for $a_1=1$ respectively); $B(m_{N_2})$ is irreducible for $N_2 = 0$ and by

virtue of Lemma 1.3 it has to be proved that $[N\alpha]-[N_2\alpha] < \alpha(N-N_2)$. This holds since $[N\alpha]<\alpha N$ $(0 < m!)$.

Let $N \in \{2,\ldots,q_m-1\}$ having a form as above and let the assertion be proved for all $N_1 < N$. Let $0 \leq N_2 < N$ be maximal such that $B(m_{N_2})$ is irreducible; then according to Lemma 1.3 it has to be proved that $[N\alpha]-[N_2\alpha]<\alpha(N-N_2)$.

Case 1: $N = q_t$ with $t \equiv 1(2)$ and $0 \leq t < m$. Then $N_2 = q_{t-2} + (a_t-1)q_{t-1}$ (and of course this holds in the case $a_t = 1$ and in the case $a_t > 1$) and the inequality $[N\alpha]-[N_2\alpha]<\alpha(N-N_2)$ is fulfilled.

Case 2: $N = q_{t-1}+b_tq_t$ with $t \equiv 0(2)$, $b_t \in \{1,\ldots,a_{t+1}-1\}$ and $0 \leq t < m$. Then $N_2=q_{t-1}+(b_t-1)q_t$ and the inequality $[N\alpha]-[N_2\alpha]<\alpha(N-N_2)$ is fulfilled. □

7. RESULTS ABOUT $\Delta_1(C_n)$

Now I combine Corollary 2 with Proposition 10. In order to give a formula for $d(1+n\mathbb{Z}, a+n\mathbb{Z})$ it remains to determine

$$\gcd\{[N\alpha]-N/N \in \{0,\ldots,\ell_1-1\},\ B(m_N) \text{ irreducible}\}$$

or rather

$$\gcd\{[N\alpha]-N/m_N \in \{2,\ldots,j-1\},\ B(m_N) \text{ irreducible}\}.$$

To do so I define for every $t \in \{0,\ldots,m\}$

$$M(q_t)=\{[N\alpha]-N/0 \leq N < q_t,\ B(m_N) \text{ irreducible}\}$$

$$d_t = \begin{cases} 0 & \text{for} \quad M(q_t) = \{0\} \\ \\ \gcd M(q_t) & \text{else} \end{cases}$$

LEMMA 6.

1. $d_o = 0$;

$$d_1 = \begin{cases} 0, & \textit{for} \quad a_1 = 1 \\ \\ a_o - 1, & \textit{for} \quad a_1 > 1 \end{cases}$$

2. *For* $t \in \{2,\ldots,m\}$

$$d_t = \{\gcd a_o - 1, a_2, a_4, \ldots, a_s\}$$

with

$$s = \begin{cases} t-2, & \textit{for} \quad t \equiv 0(2) \\ t-3, & \textit{for} \quad t \equiv 1(2) \quad \textit{and} \ a_t = 1 \\ t-1, & \textit{for} \quad t \equiv 1(2) \quad \textit{and} \ a_t > 1 \end{cases}$$

If $t \equiv 0(2)$, *so* $d_t \mid (p_{t-1} - q_{t-1} - 1)$ *and* $d_t \mid (p_{t-2} - q_{t-2})$.

If $t \equiv 1(2)$ *and* $a_t > 1$, *so* $d_t \mid (p_{t-1} - q_{t-1})$.

PROOF.

1. $M(q_o) = \{0\}$ and $d_o = 0$. $M(q_1) = M(q_o) \cup \{b_o q_o / 1 \leq b_o \leq a_1 - 1\}$. For $N = b_o q_o$ I get $[N\alpha] - N = b_o(p_o - q_o) = b_o(a_o - 1)$. For $a_1 = 1$ $M(q_1) = M(q_o)$ and hence $d_1 = 0$. For $a_1 > 1$ I obtain $d_1 = a_o - 1$.

2. I use induction on t.

Let $t = 2$. $M(q_2) = M(q_1) \cup \{q_1\}$. For $N = q_1$ $[N\alpha] - N =$

$p_1-q_1-1 = a_1(a_o-1)$. Thus $d_2=a_o-1$ (and this is true in the case $a_1 = 1$ and in the case $a_1 > 1$!) and so $d_2 \mid p_1-q_1-1$ and $d_2 \mid p_o-q_o$.

Let the assertion be proved for $t \geq 2$. $M(q_{t+1}) = M(q_t) \cup R_t$ with $R_t = \{[N\alpha]-N/q_t \leq N < q_{t+1}, B(m_N)$ irreducible$\}$.

Case 1: $t \equiv 1(2)$. Then $R_t=\{[N\alpha]-N/N=q_t\}=\{p_t-q_t-1\}$. If $a_t > 1$, so $p_t-q_t-1=a_t(p_{t-1}-q_{t-1})+(p_{t-2}-q_{t-2}-1)$ and hence $d_t \mid p_t-q_t-1$; from this it is obviously that $d_{t+1}=d_t=\gcd\{a_o-1, a_2,\ldots,a_{t-1}\}$. Now let $a_t=1$. Then $p_t-q_t-1=a_ta_{t-1}(p_{t-2}-q_{t-2})+ a_t(p_{t-3}-q_{t-3})+(p_{t-2}-q_{t-2}-1)$. Since $d_{t-1} \mid p_{t-2}-q_{t-2}-1$ and $d_{t-1} \mid p_{t-3}-q_{t-3}$ I obtain $d_{t+1} \mid a_{t-1}$ and thus $d_{t+1} = \gcd\{a_o-1, a_2,\ldots,a_{t-3},a_{t-1}\}$. In both case d_{t+1} divides (p_t-q_t-1) and $(p_{t-1}-q_{t-1})$.

Case 2: $t \equiv 0(2)$. Then $R_t=\{[N\alpha]-N/N=q_{t-1}+b_tq_t$ with $1 \leq b_t \leq a_{t+1}-1\}$. If $a_{t+1} = 1$, so $R_t = \emptyset$ and hence $d_{t+1}= = d_t = \gcd\{a_o-1, a_2,\ldots,a_{t-2}\}$. Now let $a_{t+1} > 1$. For $N = q_{t-1}+b_tq_t$ I get $[N\alpha]-N = (p_{t-1}-q_{t-1}-1)+b_t(p_t-q_t) = =(p_{t-1}-q_{t-1}-1)+b_ta_t(p_{t-1}-q_{t-1})+b_t(p_{t-2}-q_{t-2})$. Thus $d_{t+1} \mid p_t-q_t$ and $d_{t+1} \mid a_t$ which imply $d_{t+1}=\gcd\{a_o-1, a_2,\ldots,a_t\}$. □

Summing up I obtain the following theorem.

THEOREM 1. *Let* $n \geq 3$, $a \in \{2,\ldots,n-1\}$ *with* $\gcd(a,n)=1$ *and* $\ell_1 \in \{1,\ldots,n-1\}$ *such that* $a\ell_1+1 \equiv 0(n)$. *Let* $\frac{p_i}{q_i}$ *denote the convergents of* $\alpha = \frac{n}{\ell_1}=[a_o; a_1,\ldots,a_m]$. *Further let* $n = ak+j$ *with* $k \in \mathbb{N}$ *and* $0<j<a$, *let* $N_1 = \max(\{N/2\leq m_N\leq j-1,\ B(m_N)\ \textit{irreducible}\}\cup\{0\})$ *and* $\psi = \min\{i/N_1 < q_i\}$. *Then*

$$d(\bar{1},\bar{a}) = \gcd\{a-1,\ \frac{a\ell_1+1}{n}-1,\ d_\psi\}$$

$$= \gcd\{a-1,\ \frac{a\ell_1+1}{n}-1,\ d_m\}$$

For $a_m > 1$ *and* $m \geq 1$ *this means*

$$d(\bar{1},\bar{a}) = \gcd\{a-1,\ \frac{a\ell_1+1}{n}-1,\ a_o-1, a_2,\ldots,a_2\cdot[\frac{m-1}{2}]\}$$

COROLLARY 3.

1. $d(\bar{1},\bar{a})$ *has the form* (i),(ii) *or* (iii):

(i) $d(\bar{1},\bar{a}) = n-2$.

(ii) $d(\bar{1},\bar{a}) = [\frac{n}{i}]-1$ *with* $2\leq i\leq\frac{n}{2}$ *and* $\gcd(i,n) = 1$.

(iii) $d(\bar{1},\bar{a}) = [\frac{n}{i}]$ *with* $4 \leq i \leq n$ *and* $i \nmid n$.

2. *Let* $a,b \in \{1,\ldots,n-1\}$ *with* $\Delta(\{\bar{a},\bar{b}\}) \neq \emptyset$. *Then* $d(\bar{a},\bar{b})$ *has the form* (i), (ii) *or* (iii):

(i) $d(\bar{a},\bar{b}) = [\frac{n}{i}]-2$ *with* $1 \leq i \leq \frac{n}{3}$ *and* $i \mid n$.

(ii) $d(\bar{a},\bar{b}) = [\frac{n}{i}]-1$ *with* $2 \leq i \leq \frac{n}{2}$ *and* $i \mid n$.

(iii) $d(\bar{a},\bar{b}) = [\frac{n}{i}]$ *with* $4 \leq i \leq n$ *and* $i \nmid n$.

3. *Let* $n = p^k$ *with* p *prime and* $k \in \mathbb{N}_+$, *for* $p = 2$ *let* $k \geq 2$.

Then every $d \in \Delta_1(C_n)$ *has the form* (i), (ii), (iii) *or* (iv):

(i) $d = \frac{n}{i} - 2$ *with* $1 \leq i \leq \frac{n}{3}$ *and* $i \mid n$.

(ii) $d = \frac{n}{i} - 1$ *with* $1 \leq i \leq \frac{n}{2}$, $i \mid n$ *and* $i \equiv 0(2)$.

(iii) $d = \frac{n}{i} - 1$ *with* $2 \leq i \leq \frac{n}{2}$ *and* $i \nmid n$.

(iv) $d = [\frac{n}{i}]$ *with* $3 \leq i \leq n$ *and* $i \nmid n$.

PROOF. I use the same notations as in Theorem 1 and assume without restrictions that $a_m > 1$.

1. If $m = 0$, so $\frac{n}{\ell_1} \in \mathbb{N}$. Because of $\gcd(n, \ell_1) = 1$ I get $\ell_1 = 1$ and hence $a = n-1$. Thus $d(\bar{1}, \bar{a}) = d(\bar{1}, \overline{n-1}) = n-2$. If $m \geq 1$, then $\ell_1 > 1$ and $d = d(\bar{1}, \bar{a})$ divides $a_o - 1 = [\frac{n}{\ell_1}] - 1$. Let $n = u\ell_1 + v$ with $0 < v < \ell_1$ and let $dw = u-1$. Then $n = (dw+1)\ell_1 + v$ and $d = \frac{n}{\ell_1 w} - \frac{\ell_1 + v}{\ell_1 w}$. In the case $w = 1$ I get $d = [\frac{n}{\ell_1}] - 1$ and in the case $w > 1$ $\frac{\ell_1 + w}{\ell_1 w} < 1$ implies $d = [\frac{n}{\ell_1 w}]$.

2. According to Proposition 5 for $a+n\mathbb{Z}$, $b+n\mathbb{Z} \in C_n$ there are n_1 and c with $n_1 \mid n$ and $\gcd(c, n_1) = 1$ such that $d(a+n\mathbb{Z}) = d(1+n_1\mathbb{Z}, c+n_1\mathbb{Z})$. So the assertion follows from 1.

3. Corollary 1 states that for every $d \in \Delta_1(C_n)$

there are $\bar{a},\bar{b} \in C_n$ with $d\ d(\bar{a},\bar{b})$ and therefore it remains to show: if $d(\bar{a},\bar{b})$ is of one of the forms in 2, then d is of one of the forms in 3.

Case 1: let $d(\bar{a},\bar{b}) = n_1-2$ with $n_1 | n$ and $d | d(\bar{a},\bar{b})$. Let $dr = n_1-2$ and $n = sn_1 = s(dr+2)$; then $d=\frac{n}{sr} - \frac{2}{r}$. For $r=1$ I get $d = n_1-2$; $r = 2$ implies $d = \frac{n}{2s} - 1$ and for $r \geq 3$ I obtain $d = [\frac{n}{sr}]$ with $sr \nmid n$.

Case 2: let $d(\bar{a},\bar{b}) = [\frac{n}{i}] - 1$ with $2 \leq i \leq \frac{n}{2}$ and $i \nmid n$. Similar computations as in the proof of 1 imply that d has the form (iii) or (iv).

Case 3: let $d(\bar{a},\bar{b}) = [\frac{n}{i}]$ with $4 \leq i \leq n$ $i \nmid n$. Let $n = ui+v$ with $0 < v < i$ and $dw = u$. Then $n = dwi+v$ and $d = \frac{n}{wi} - \frac{v}{wi} = [\frac{n}{wi}]$ $wi \nmid n$. □

COROLLARY 4. *Let* $n \geq 3$, $n = ak+j$ *with* $0 < j < a$ *and let* $a \equiv 1(j)$.
Then $d = \frac{a-1}{j} \in \Delta_1(C_n)$.

REMARK. This implies in particular that $\{\frac{n}{i} - 2 \mid 1 \leq i \leq \frac{n}{3},\ i|n\} \subset \Delta_1(C_n)$. For let $n_1|n$, so $n_1 = (n_1-1)1+1$ and $d = \frac{(n_1-1)-1}{1}$.

PROOF. $\ell_1 = \frac{(j-1)n+k}{j}$ is the unique solution of

$a\ell_1+1 \equiv 0(n)$ with $0< \ell_1 < n$ and hence

$\frac{a\ell_1+1}{n} - 1 = (a-1)+\frac{a-1}{j}$; $\frac{n}{\ell_1} = [a;k]$ for $j = 1$. For $j > 1$ I get $\frac{n}{\ell_1} = [1; j-1, \frac{a-1}{j},k]$. According to Theorem 1 $d(\bar{1},\bar{a}) = \frac{a-1}{j}$. □

If $\frac{n}{i}$ is even, then also $d = \frac{1}{2}(\frac{n}{i} -2) \in \Delta_1(C_n)$. I show this by an explicit construction which also may serve as example for a $d \in \Delta_1(G_o)$ with $\#G_o > 2$ and $d \notin \Delta_1(G_1)$ for a subset $G_1 \subset G_o$ with $\#G_1 = 2$.

PROPOSITION 11. *Let* $n \geq 3$. *Then*

$$\{\frac{n}{i} - 1/1 \leq i \leq \frac{n}{2},\ \ i|n\ ,\ i \equiv 0(2)\} \subset \Delta_1(C_n).$$

PROOF. Let $n_1|n$, $n_1 >2$ and $n_1 \equiv 0(2)$. It is sufficient to show that $\frac{n_1}{2} -1 \in \Delta_1(C_{n_1}) \subset \Delta_1(C_n)$. To do so I define the following five irreducible blocks:

$A_1 = <1+n_1\mathbb{Z} ,\ldots,1+n_1\mathbb{Z} >$, $A_{n_1-1} =$

$= <(n_1-1) + n_1\mathbb{Z} ,\ldots,(n_1-1) + n_1\mathbb{Z} >$,

$B = <1+n_1\mathbb{Z} , (n_1-1)+n_1\mathbb{Z} >$, $C=<\frac{n_1}{2}+n_1\mathbb{Z} , 1+n_1\mathbb{Z},\ldots,1+n_1\mathbb{Z} >$

and $E= <\frac{n_1}{2}+ n_1\mathbb{Z}, (n_1-1)+n_1\mathbb{Z},\ldots,(n_1-1)+n_1\mathbb{Z} >$. For

$k \in \mathbb{N}_+$ let $B_k=A_1^{\,k}*A_{n_1-1}^{\,k} *C*A_{n_1-1}$. Then for every

$\ell \in \{0,\ldots,k\}$ B_k may be written as

$$B_k = A_1^{k-\ell} * A_{n_1-1}^{k-\ell} * B^{n_1\ell} * C * A_{n_1-1} \quad \text{and as}$$

$$B_k = A_1^{k-\ell} * A_{n_1-1}^{k-\ell} * B^{n_1\ell} * B^{n_1/2} * E$$

Hence $L(B_k) = \{2k + \ell(n_1-2) + r \mid \ell \in \{0,\ldots,k\},$

$r \in \{2, \frac{n_1}{2} + 1\}\}$. □

REFERENCES

[1] R.E. BURKARD, Methoden der ganzzahligen Optimierung, *Springer* 1972.

[2] L. CARLITZ, A characterization of algebraic number fields with class number two, *Proc. Amer. Math. Soc.* 11 (1960), 391-392.

[3] A. GEROLDINGER, Über nicht-eindeutige Zerlegungen in irreduzible Elemente, *Math. Z.* 197(1988),505-529.

[4] W. NARKIEWICZ, Finite abelian groups and factorization problems, *Coll. Math.* 42(1979), 319-330.

[5] J. SCHOISSENGEIER, On the discrepancy of $(n\alpha)$, *Acta Arithm.* 44(1984),241-279.

[6] J. ŚLIWA, Remarks on factorizations in algebraic number fields, *Coll. Math.* 46 (1982), 123-130.

GEROLDINGER, A. Institut für Mathematik
Karl-Franzens-Universität Graz
Halbarthgasse 1/1, A-8010 Graz
A u s t r i a

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

PRESENTATIONS OF WEIL GROUPS AND GLOBAL SKEW FIELDS

WOLFRAM JEHNE

1. The fundamental sequence of class field theory

(1) $$L^{\times} \longrightarrow J_L \longrightarrow C_L$$

gives a presentation of the idel class group C_L of a number field L by the idel group J_L with the multiplicative group $L^{\times}$ as kernel. This presentation is of "local type" since J_L is the restricted direct product of the multiplicative groups $L_p^{\times}$ of all local completions of L. For a galois extension $L|K$ of number fields C_L is contained in the Weil group $W_{L|K}$ as a subgroup. The problem we are concerned with is to find a "local type" presentation of the Weil group $W_{L|K}$ which induces (1) as a subsequence.

The solution of this problem has its roots in the theory of noncommutative galois algebras, its local embeddings and previous work of Teichmüller, Nakayama and myself. For a proper treatment, the theory of central separable algebras (Azumaya algebras) has to be refined in various directions. In particular, quite general types of crossed products (over rings) and their formal properties are being studied. More precisely, the solution of the presentation problem of Weil groups, we are going to present, reveals a deeper connection between Weil's class field theory and the structure of central separable algebras over the adel ring of number fields.

However, there is another motivation for looking at a problem of this kind. The sequence (1) has turned out useful for the Grunwald principle, i.e. the construction of characters of C_L of given order with given local components at finitely many places. Can the "local type" presentation, in an analogous way, serve to construct representations of the global Weil groups with given local behaviour at finitely many spots? The solution of this presentation problem can, if of use at all, only be considered as a first modest step in direction of that much deeper representation problem.

The aim of this talk is to report on some work [Je] which appeared recently. The detailed proofs and further references can be found in this paper.

2. Firstly, we need some additional informations on ordinary adel rings which do not seem having been observed so far.

LEMMA 1.

For the adel ring Ad_K of a number field K all finitely generated ideals are principal and projective. Hence: Ad_K is a Bezout ring and a Prüfer ring. The Picard group is trivial:

$$(2) \qquad \mathrm{Pic}\, Ad_K = 1 \ .$$

Here, the adel ring Ad_K is defined as restricted direct product $Ad_K = \prod\!\!\!\!\!\!\prod_p K_p$ of all local completions K_p with respect to the family (R_p) of valuation rings R_p in K_p . In an analoguous way, we introduce the basic definition: An *adel algebra*[1] Γ *to* K is a restricted direct product

$$(3)\ (\alpha) \qquad \Gamma = \prod\!\!\!\!\!\!\prod_p \Gamma_p \quad \text{for} \quad (O_p)$$

---

1) One should notice that in [Je] the notion "adel algebra" is used in a weaker sense, namely without condition (γ).

of central simple K_p -algebras Γ_p with respect to a family (O_p) of maximal orders O_p in Γ_p, subject to the following conditions:

(3)
$$(\beta)\quad \dim_{K_p} \Gamma_p \leq \text{const.} \quad \text{(bounded dimensions)}$$
$$(\gamma)\quad \Gamma_p \sim 1 \text{ split for almost all } p.$$

In (3), p runs over all places of K, finite and infinite ones. The following statements are obvious:

The centre of Γ is the adel ring Ad_K. Different choices of the maximal orders O_p lead to isomorphic Ad_K-algebras.

THEOREM 1. For an Ad_K-algebra Γ the following are equivalent:

(a) Γ is adel algebra to K

(b) Γ is a central separable Ad_K-algebra (Azumaya algebra over Ad_K) .

Since a central separable Ad_K-algebra Γ is, by Theorem 1, uniquely determined by their local components Γ_p one has, via local Hasse invariants, the following

COROLLARY: The Brauer group of the adel ring is determined

$$\mathrm{Br}\ \mathrm{Ad}_K \cong \oplus_p \mathbb{Q}/\mathbb{Z} \oplus \oplus_q \tfrac{1}{2}\mathbb{Z}/\mathbb{Z}$$

here p runs over the finite, q over the real places of K. The classical main theorem on Brauer groups then takes the form:

Brauer-Hasse-Noether:

$$(4) \qquad \mathrm{Br}\ K \xrightarrow[\mathrm{Ad}]{} \mathrm{Br}\ \mathrm{Ad}_L \xrightarrow{\mathrm{inv}_K} \mathbb{Q}/\mathbb{Z}$$

is an exact sequence, where the maps are defined as follows:

The "adel functor" $B \longrightarrow \mathrm{Ad}\ B := \mathrm{Ad}_K \otimes B$ induces the first homomorphism; the second homomorphism in the "global invariant map"

$$\mathrm{inv}_K\ \Gamma := \sum_p \mathrm{inv}_p\ \Gamma_p .$$

This sum over the local Hasse invariants makes sense because of Theorem 1 and (3) (γ).

3. We are now able to formulate the main result. Let us consider a finite galois extension L|K of number fields of degree n and galois group G. Then (4) gives the exact sequence

(4′) $$\mathrm{Br}\ K \xrightarrow[\mathrm{Ad}]{} \mathrm{Br}_n\ \mathrm{Ad}_K \xrightarrow{\mathrm{inv}_K} \frac{1}{n}\,Z/Z \ ,$$

where $\mathrm{Br}_n\ \mathrm{Ad}_K$ denotes the Brauer classes $[\Gamma]$ over Ad_K with $n.\mathrm{inv}_K\ \Gamma = 0$.

We start with a class $[\Gamma] \in \mathrm{Br}_n\ \mathrm{Ad}_K$. Since the global invariant multiplies with the degree n under tensor extension with Ad_L we have

$$\mathrm{inv}_L\ \hat{\Gamma} = 0 \quad \text{for} \quad \hat{\Gamma} := \mathrm{Ad}_L \otimes_{\mathrm{Ad}_K} \Gamma \ .$$

Hence, by (4) for L, there exists exactly one global Brauer class $[B] \in \mathrm{Br}\ L$ such that

$$\Gamma' := \mathrm{Ad}\ B \in [\hat{\Gamma}] \ .$$

So, $[\Gamma]$ determines $[B]$. Keeping this situation fixed, we have

THEOREM 2.

a) Given any $B \in [B]$ there exists a unique $\Gamma \in [\Gamma]$ such that

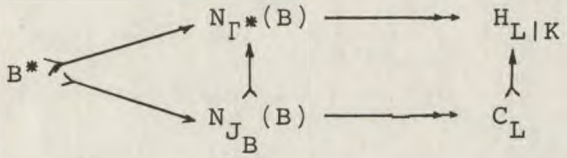
Γ is an "embedding of Ad B" ,

i.e. the centralizer of Ad B in Γ is Ad_L:

(5) $$C_\Gamma(\mathrm{Ad}\ B) = \mathrm{Ad}_L \quad (\text{equiv.: } C_\Gamma(\mathrm{Ad}_L) = \mathrm{Ad}\ B) \ .$$

Such a Γ attached to B is always a free Ad_K-module.

b) The normalizer of B in the idel group $J_B := (\mathrm{Ad}\ B)^{*2)}$ of B is just $B^* J_L$. One has the following commutative diagram

(6)


where $H_{L|K}$ is a certain group extension of C_L with factor group G.

c) The cohomology class [a] which defines $H_{L|K}$ depends only on the Brauer class $[\Gamma]$ of Γ. The map $[\Gamma] \longrightarrow [a]$ is homomorphic and so gives rise to the exact sequence

$$(7) \qquad \mathrm{Br}\ K \rightarrowtail \mathrm{Br}_n \mathrm{Ad}_K \longrightarrow H^2(G, C_L)\ .$$

As an immediate consequence this result (7), together with (4'), gives a definition of an invariant on the 2-cohomology group:

$$\mathrm{inv}_{L|K} : H^2(G, C_L) \xrightarrow{\sim} \frac{1}{n}\ \mathbb{Z}/\mathbb{Z}\ .$$

---

2) The unit group of a ring A is always denoted by A^*

Therefore, if we start with a Brauer class $[\Gamma]$ of invariant $\frac{1}{n} + \mathbf{Z}$, then $[a]$ is the canonical class and $H_{L|K} = W_{L|K}$, The Weil group. Moreover, the procedure at the beginning fixes a unique global skew field $D \in [B]$ attached to $[\Gamma]$. Part a) of Theorem 2, furthermore, fixes a unique $\Gamma \in [\Gamma]$ embedding Ad D in the sense of (5). Now, (6) gives the exact sequence

$$(8) \qquad D^{\times} \rightarrowtail N_{\Gamma^*}(D) \twoheadrightarrow W_{L|K} \quad ,$$

the solution of our presentation problem. (8) can be considered to be of "local type", since $\Gamma^* = \coprod_p \Gamma_p^*$ is restricted direct product of local groups Γ_p^* with respect to the unit groups O_p^* of the maximal orders. Finally, (8) induces sequence (1) as can easily be seen from part b).

However, one observes that the presentation (8) of the Weil group $W_{L|K}$ is not canonical. On the contrary, one can choose infinitely many Brauer classes $[\Gamma]$ over Ad_K of invariant $\frac{1}{n} + \mathbf{Z}$ which give rise to infinitely many global skew fields D. At a first sight this seems a great disadvantage. But it could turn out to be an advantage if applied to the generalized Grunwald problem mentioned in the introduction.

4. I will now give an outline of the proof methods

Theorem 1 is by no means obvious, it requires some nonstandard technics. To make this transparent we start with a characterisation of central separable algebras over an arbitrary commutative ring R, due to *Auslander-Goldman* [A-G] and *Bass*: For a f.g. R-Algebra A to be central separable is necessary and sufficient that the factor algebras A/MA be central simple R/M-algebras for all maximal ideals M of R. So, one needs to know the maximal ideals of the adel ring. Besides the obvious maximal ideals of Ad_K, namely the complements $M_p := \{\alpha \in Ad_K | \alpha_p = 0\}$ of the components K_p, there is a much bigger class of maximal ideals:

$$M_U := \{\alpha \in Ad_K | \{p \in P_K | \alpha_p \in m_p\} \in U\} .$$

Here, U is a nonprincipal ultrafilter on the set P_K of all prime ideals p of K (U is a "superprime" in the sense of [Je-Kl]) and m_p is the maximal ideal of the valuation ring R_p of K_p.

Fortunately (*N. Klingen*):

LEMMA 2: These ideals M_p, M_U are all the maximal ideals of Ad_K.

To prove Theorem 1 one shows

THEOREM 1': The properties (a) and (b) in Theorem 1 are equivalent to the following:

(c) Γ is finitely generated as Ad_K-module,
Γ fulfills (3) (α) and

(9) $\Gamma/M_U\Gamma \cong M_r(k_U)$ is full matrix algebra over the ultraproduct $k_U = \prod_p k_p/U$ of the finite residue class fields $k_p = R_p/m_p$, for all "superprimes" U of K.

For this equivalence one has to use local arithmetic of algebras [H] and *Kanzaki's* double centralizer theorem [Ka].

I now turn to Theorem 2. Some proof ideas involved here are of algebraic nature: a galois theory of central separable algebras over rings, particularly an extensive calculus of generalized crossed products.

We first observe that for a galois extension L|K of number fields with group G the corresponding adel extension $Ad_L|Ad_K$ has automorphism group G and possesses a normal basis (namely a normal basis of L|K). Thus, the adel ring extension is "strict galois" in the following sense: a commutative separable ring extension S|R is called *strict galois with* (the finite automorphism) *group* G if S considered as RG-module is isomorphic to the group ring RG. More generally, a separable R-algebra Λ is called *G-galois* (or G-normal), if its

centre S is strict galois over R with G and all $g \in G$ can be extended to algebra automorphisms of Λ.

Let Λ be G-galois algebra with its strict galois centre S over R. We define: Λ is *embedded* into a central separable R-algebra Γ if

$$(10) \qquad C_\Gamma(\Lambda) = S \qquad \text{(or equiv.: } C_\Gamma(S) = \Lambda) \text{ ;}$$

Γ is then an *embedding of* Λ *for* S|R. If for all such situations for fixed S|R any R-algebra monomorphism $\varphi : \Lambda \longrightarrow \Gamma$ can be extended to an automorphism of Γ I say that the *Noether principle* (NP) holds *for* S|R.

THEOREM 3.

Let S|R be strict galois with G and Pic R = 1, and let us assume (NP) for S|R.

A unitary ring extension Γ of a G-galois algebra Λ with centre S is an embedding for S|R if and only if Γ is a "generalized crossed product" of Λ over R:

$$(11) \qquad \left| \begin{array}{l} \Gamma = \bigoplus_{s \in G} u_s \Lambda =: (\Theta, \sigma, \Lambda | R) \text{ ,} \\ x\, u_s = u_s\, x^{\sigma_s},\ u_s\, u_t = u_{st}\, \Theta_{s,t} \quad (x \in \Lambda,\ \Theta_{s,t} \in \Lambda^*) \\ \Theta_{r,st}\ \Theta_{s,t} = \Theta_{rs,t}\ \Theta_{r,s}^{\sigma_t} \end{array} \right. .$$

Here, σ_s denotes an extension of $s(\in G)$ to Λ.

If S,R are both fields (NP) is just E. Noether's result. If only R is a field an additional condition has to be imposed for (NP) to hold (Teichmüller). That Theorem 3 can be applied to the adel situation is guaranteed by Lemma 1 and the following

THEOREM 4: (NP) holds for adel rings of number fields.

We want to stress one basic consequence of the application of Theorem 3 to Theorem 2. The 2-cocycle a occuring in the latter Theorem can be written as a quotient of two noncommutative 2-cocycles, one of which coming from a crossed product of type (11). Namely, the embedding Γ in part a) of Theorem 2 attached to the global L-central simple algebra B can, by Theorem 3, be written as a generalized crossed product

$$(12) \qquad \Gamma = (\Theta, \sigma, \text{Ad } B | \text{Ad}_K) \ ;$$

here σ is normalised to be an extension section $\sigma: G \longrightarrow \text{Aut}(B|K)$ to automorphisms of B (instead of merely automorphisms of Ad B). It is this 2-cocycle Θ in (12) which is connected with the cocycle a.

Theorem 3 does not provide the full proof of Theorem 2. What is needed to establish the exact sequence (7) is a calculus for generalized crossed products. For instance, the following rules are being used:

Multiplication rule:

(13) $\quad (\Theta,\sigma,\Lambda|R) \otimes_R (\Theta',\sigma',\Lambda'|R) \sim_R (\Theta\Theta', \sigma \otimes_S \sigma', \Lambda \otimes_S \Lambda'|R),$

where Λ,Λ' both have centre S.

Inflation rule:

(14) $\quad (\Theta,\sigma,\Lambda|R) \sim_R (\inf_G^H \Theta\ ,\ \inf_G^H \sigma,\ T \otimes_S \Lambda)\ ;$

here $T|R$ is strict galois algebra with group H containing S with $S = T^N$ where N is the kernel under the restriction $H \longrightarrow\!\!\!\!\!\rightarrow G$. For functorial properties of the presentation (8) is useful the

Restriction rule:

(15) $\quad (\Theta,\sigma,\Lambda|R) \otimes_R S_o \sim_{S_o} (\mathrm{res}_H^G \Theta,\ \sigma|_H,\ \Lambda|S_o)\ ,$

where S_o is the fixed ring of a subgroup H of G in S.

Of course, $\sim_R$ means Brauer equivalence over the commutative ring R in the sense of Auslander-Goldman.

REFERENCES

[A-G] AUSLANDER-GOLDMAN, The Brauer group of a commutative ring, *Trans. AMS* 97 1960 , 367-409.

[Ha] HASSE, H., Über p-adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlsysteme, *Math. Ann.* 104 (1931), 495-534; Werke I, Berlin 1975, 455-494.

[Je] JEHNE, W., Separable adel algebras and a presentation of Weil groups, *J. reine angew. Math.* 375/376 (1987), 211-237.

[Je-Kl] JEHNE, W., KLINGEN, N., Superprimes and a generalized Frobenius symbol, *Acta Arithmetica* 32 (1977), 209-232.

[Ka] KANZAKI, T., On commutor rings and galois theory of separable algebras, *Osaka J. Math.* 1 (1964), 103-115.

[W] WEIL, A., Sur la théorie du corps de classes, *J. Math. Soc. Japan* 3 (1951), 1-35.

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

ON PRIMITIVE PRIME POWER DIVISORS OF LUCAS NUMBERS

PÉTER KISS*

INTRODUCTION

Let $R = \{R_n\}_{n=0}^{\infty}$ be a sequence of Lucas numbers defined by the recursion

$$R_n = A \cdot R_{n-1} + B \cdot R_{n-2} ,$$

where A, B are not zero rational integers and the initial values are $R_0 = 0$ and $R_1 = 1$. We shall denote by α and β the roots of the characteristic polynomial $x^2 - Ax - B$ of R and throughout this paper we assume that $|\alpha| \geq |\beta|$ and R is a non-degenerate Lucas sequence, i.e. α/β is not a root of unity. It is well-known that the terms of a

*Research (partially) supported by Hungarian National Foundation for Scientific Research grant No. 273.

non-degenerate Lucas sequence can be expressed as

$$R_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \qquad (n = 0, 1, 2, \ldots).$$

We say a prime p is a primitive prime divisor of a Lucas number R_n $(n > 0)$ if $p \mid R_n$ but $p \nmid R_m$ for $0 < m < n$. If p is a primitive prime divisor of R_n and p^k $(k \geq 1)$ is the greatest power of p such that $p^k \mid R_n$, then p^k is called a primitive prime power divisor of R_n. We shall denote the product of all distinct primitive prime power divisors of R_n by $\mathcal{R}_n$; i.e.

$$\mathcal{R}_n = \Pi p^k \qquad (n \geq 1)$$

where the product is extended for the distinct primitive prime power factors of R_n. We write $\mathcal{R}_n = 1$ if R_n has no primitive prime divisor. We note that $\mathcal{R}_n > 1$ for large n since it is known that there is an absolute constant C_0 such that in every non-degenerate Lucas sequence the terms R_n have at least one primitive prime divisor for any $n > C_0$ (see, e.g. A. Schnizel [6] and C.L. Stewart [11]).

The aim of this paper is to study the greatest primitive prime and the greatest primitive prime power divisors of Lucas numbers R_n; we shall denote them by $P(\mathcal{R}_n)$ and $PP(\mathcal{R}_n)$, respestively.

RESULTS

The primitive divisors and the greatest prime factors of the terms of linear recurrences were studied by several authors, see e.g. K. Mahler [4], A. Schinzel [5], C.L. Stewart [2], I.E. Shparlinskij [8, 9] and their references. The best results for the greatest prime factors of Lucas numbers have been obtained by T.N. Shorey and C.L. Stewart [7]. Among others they proved that the greatest prime factors (not necessarily primitive ones) of Lucas numbers R_n are greater than

$$\frac{n \cdot \log^2 n}{f(n) \cdot \log \log n}$$

for "almost all" integer n, where f(n) is any real valued function for which $f(n) \to \infty$ as $n \to \infty$ and "almost all" n means the set of natural numbers except perhaps for a set of asymptotic density zero.

For the greatest primitive prime power divisors of Lucas numbers, from results of C.L. Stewart [10], it follows that $PP(R_n) > 0(\varphi(n))^2$, where φ is the Euler's function. But we do not know whether the prime is large or its exponent is greater than 1. In the simple case when R is the Fibonacci sequence we do not know prime for which $p^2 | R_n$ would hold.

In [3] we investigated the average order of the primitive parts of Lucas numbers showing that

$$\sum_{n \le x} \log R_n = \frac{3 \cdot \log |\alpha|}{\pi^2} \cdot x^2 + O(x \cdot \log x).$$

As a consequence of it we can obtain: If λ is a real number, $0 < \lambda < 1$, and $P(R_n) < n^{1+\lambda}$ for almost all natural numbers, then there are infinitely many n such that R_n has a primitive prime power factor with exponent greater than 1; furthermore the set of these n's has positive asymptotic density. Now we show some other connections between the greatest primitive prime and the greatest primitive prime power factors of Lucas numbers. They will show that if we should have only a "few" Lucas numbers with "large" primitive prime divisors, then "many" Lucas numbers would have primitive prime power factors with "large" exponents.

We shall prove the following two theorems:

THEOREM 1. Let γ be a real number with $0 < \gamma < 3/\pi^2$. If

$$\left| \left\{ n : 1 < n \le x,\ P(R_n) > \frac{n^2}{\log n} \right\} \right| < \frac{x}{\log x},$$

then there is a positive real number c such that

$$\left|\left\{n:1<n\le x,\ PP(R_n)>n^{c\cdot\log n}\right\}\right| > \gamma x$$

for any $x>x_0(\gamma,R)$, where $|\{\ \}|$ denotes the cardinality of the set $\{\ \}$.

THEOREM 2. Let δ and ε be real numbers with conditions $0<\delta<1$ and $0<\varepsilon<1-\delta$. Further let N_x and T_x be sets of natural numbers defined by

$$N_x = \left\{n : n\le x,\ P(R_n) > n^{1+\delta}\right\}$$

and

$$T_x = \left\{n : n\le x,\ PP(R_n) > \exp(n^{1-\delta-\varepsilon})\right\} .$$

If for the cardinality of the set N_x we have

$$\left|N_x\right| < x^{\delta} ,$$

then

$$\left|T_x\right| > (1-\varepsilon')x$$

for any $\varepsilon'>0$ and $x>x_0$, where x_0 depends only on δ, ε, ε', and the sequence R.

PRELIMINARY LEMMAS

We need some auxiliary results in the proof.

Let $\Phi_n(\alpha,\beta)$ denote the n^{th} cyclotomic polynomial in α and β for any integer $n > 0$ and any pair α, β of complex numbers, that is

$$\Phi_n(\alpha,\beta) = \prod_{d|n} (\alpha^{n/d} - \beta^{n/d})^{\mu(d)},$$

where μ is the Moebius function.

From some results of C.L. Stewart (Lemma 6 and 7 in [10]) it follows:

LEMMA 1. Let R be a non-degenerate Lucas sequence. Then for $n > 12$ we have

$$R_n = \lambda_n \cdot \Phi_n(\alpha,\beta),$$

where $\lambda_n = 1$ or $\lambda_n = 1/P(n/(3,n))$ and $P(m)$ denotes the greatest prime factor of the integer m.

LEMMA 2. If R is a non-degenerate Lucas sequence, then

$$\exp\{(1-\varepsilon)\varphi(n)\cdot\log|\alpha|\} < R_n < \exp\{(1+\varepsilon)\varphi(n)\cdot\log|\alpha|\}$$

for any $\varepsilon > 0$ and $n > n(\varepsilon)$, where φ denotes the Euler's function.

PROOF. It follows from Lemma 1 using some results on linear forms of logarithms of algebraic numbers e.g. results of A. Baker [1] or A. Baker and C.L. Stewart [2]), but it follows also from results of A. Schinzel (see lemma 1 and formula (5) in [6]).

We prove two other lemmas.

LEMMA 3. If $\omega(m)$ denotes the number of distinct prime divisors of a natural number m, then

$$\omega(R_n) < (1+\varepsilon) \cdot \frac{\varphi(n) \cdot \log|\alpha|}{\log n}$$

for any $\varepsilon > 0$ and $n > n(\varepsilon)$.

PROOF. We know that $p \geq n-1$ for any primitive prime divisor p of a Lucas number R_n. So by Lemma 2

$$(n-1)^{\omega(R_n)} < R_n < \exp\{(1+\frac{\varepsilon}{2}) \cdot \varphi(n) \cdot \log|\alpha|\}$$

and

$$\omega(R_n) < (1+\frac{\varepsilon}{2}) \cdot \frac{\varphi(n) \cdot \log|\alpha|}{\log(n-1)} < (1+\varepsilon) \cdot \frac{\varphi(n) \cdot \log|\alpha|}{\log n}$$

follows for any $\varepsilon > 0$ and $n > n(\varepsilon)$.

LEMMA 4. Let $x > 2$ be a real number. Then

$$\sum_{1<n\le x} \frac{\varphi(n)}{\log^2 n} = \frac{3}{\pi^2} \cdot \frac{x^2}{\log^2 x} + O\left(\frac{x^2}{\log^3 x}\right)$$

PROOF. It is known that

$$\sum_{n\le x} \varphi(n) = \frac{3}{\pi^2} x^2 + O(x \cdot \log x).$$

Therefore, using the partial summation, we get

$$\sum_{1<n\le x} \frac{\varphi(n)}{\log^2 n} = \frac{1}{\log^2 x} \cdot \sum_{n\le x} \varphi(n) +$$

$$+ \int_2^x \left(\sum_{n\le t} \varphi(n)\right) \cdot \frac{2\,dt}{t\cdot\log^3 t} + O(1)$$

$$= \frac{3}{\pi^2} \cdot \frac{x^2}{\log^2 x} + \frac{6}{\pi^2} \cdot \int_2^x \frac{t}{\log^3 t}\,dt +$$

$$+ O\left(\frac{x}{\log^2 x}\right).$$

But

$$\int_2^x \frac{t}{\log^3 t}\,dt = O\left(\frac{x^2}{\log^3 x}\right)$$

and so the required result follows.

PROOFS OF THE THEOREMS

PROOF OF THEOREM 1. Let ε ($< 1/2$) and x be positive real numbers and let L_x be a set of natural numbers defined by

$$L_x = \left\{ n : 1 < n \le x,\ P(R_n) > \frac{n^2}{\log n} \right\} .$$

Suppose that

$$\left| L_x \right| < \frac{x}{\log x} .$$

In this case, using Lemma 3, the prime number theorem and the fact that $\varphi(n) < x$ for any $n \le x$,

$$(1) \qquad \sum_{n \le x} \omega(R_n) < \pi\left(\frac{x^2}{\log x}\right) + \left(1 + \frac{\varepsilon}{2}\right) \cdot \frac{x \cdot \log|\alpha|}{\log x} \cdot \frac{x}{\log x} <$$

$$< \left(\frac{3}{2} + \varepsilon\right) \cdot \frac{x^2 \cdot \log|\alpha|}{\log^2 x}$$

follows for any x sufficiently large.

Let $q > 0$ be a real number and let M_x be a set of integers defined by

$$M_x = \left\{ n : 1 < n \le x,\ \omega(R_n) < \frac{\varphi(n) \cdot \log|\alpha|}{q \cdot \log^2 n} \right\} .$$

If $\left| M_x \right| \le \gamma x$, $\gamma < 3/\pi^2$ and

$$q < \frac{1}{2} \cdot \left(\frac{3}{\pi^2} - \gamma - \varepsilon\right),$$

then by Lemma 4

$$\sum_{n\le x} \omega(R_n) \ge \sum_{n\notin M_x} \omega(R_n) > \sum_{n\notin M_x} \frac{\varphi(n)\cdot\log|\alpha|}{q\cdot\log^2 n} >$$

$$> \sum_{n\le x} \frac{\varphi(n)\cdot\log|\alpha|}{q\cdot\log^2 n} - \frac{x\cdot\log|\alpha|}{q\cdot\log^2 x}\cdot \gamma x =$$

$$= \frac{3\cdot\log|\alpha|}{q\cdot\pi^2}\cdot\frac{x^2}{\log^2 x} - \frac{\gamma}{q}\cdot\frac{x^2\cdot\log|\alpha|}{\log^2 x} +$$

$$+ 0\left(\frac{x^2}{\log^3 x}\right) > \left(\frac{3}{2} + \varepsilon\right)\cdot\frac{x^2\cdot\log|\alpha|}{\log^2 x}$$

would follow. It contradicts to (1), thus we have

$$\left|M_x\right| > \gamma x .$$

It is evident that

$$(PP(R_n))^{\omega(R_n)} \ge R_n$$

for any $n > 1$ therefore if $n \in M_x$, then by Lemma 2

$$PP(R_n) > \exp\left\{(1-\varepsilon)\varphi(n)\cdot\log|\alpha| \cdot \frac{q\cdot\log^2 r}{\varphi(n)\cdot\log|\alpha|}\right\} =$$

$$= n^{(1-\varepsilon)q\cdot\log n}$$

follows which proves the theorem with any $c < q$.

PROOF OF THEOREM 2. If $|N_x| < x^{\delta}$, then by the prime number theorem and Lemma 3, using the fact that $\varphi(n) < x$ for any $n \le x$, we get

$$(2) \qquad \sum_{n\le x} \omega(R_n) < \pi(x^{1+\delta}) + x^{\delta} \cdot \frac{2x \cdot \log|\alpha|}{\log x} < x^{1+\delta}.$$

Let Q_x be a set of positive integers defined by

$$Q_x = \left\{n : n \le x,\ \omega(R_n) < n^{\delta+\varepsilon/2}\right\}.$$

If $|Q_x| \le (1 - \frac{\varepsilon'}{2})x$ for an $\varepsilon' > 0$, then

$$\sum_{n\le x} \omega(R_n) > \sum_{n\notin Q_x} \omega(R_n) \ge \sum_{n\notin Q_x} n^{\delta+\varepsilon/2} \ge$$

$$\ge \sum_{n\le \frac{\varepsilon'}{2} x} n^{\delta+\varepsilon/2} >$$

$$> (1-\varepsilon') \cdot \frac{\left(\frac{\varepsilon'}{2} x\right)^{1+\delta+\varepsilon/2}}{1+\delta+\varepsilon/2} > x^{1+\delta}$$

would follow, which contradicts to (2) and so

$$(3) \qquad |Q_x| > (1 - \frac{\varepsilon'}{2})x$$

for any $\varepsilon' > 0$ and $x > x_0$.

We show that $PP(R_n) > \exp\{n^{1-\delta-\varepsilon}\}$ for any n with $n \in Q_x$ and $n > n_0$. Let $n \in Q_x$. Then

$$R_n \leq (PP(R_n))^{\omega(R_n)} < (PP(R_n))^{n^{\delta+\varepsilon/2}}$$

and so, using Lemma 2 and the known fact that there is a constant c_1 such that $\varphi(m) > c_1 m/\log\log m$ for every integer $m > 9$, it follows that

$$PP(R_n) > \exp\{n^{1-\delta-\varepsilon}\}$$

for any $n \in Q_x$ and $n > n_0$, where n_0 depends only on ε and the sequence R. It implies, using (3), that

$$|T_x| \geq |Q_x| - n_0 > (1 - \varepsilon')x$$

if x is large enough and so the theorem is proved.

REFERENCES

[1] BAKER, A., The theory of linear forms in logarithms, Transcendence theory: advances and applications (ed. by A. Baker and D.W. Masser), *London - New York, Acad. Press*, 1977.

[2] BAKER, A. and STEWART, C.L., Further aspect of transcendence theory, *Astérisque*, 41-42 (1977), 153-163.

[3] KISS, P., Primitive divisors of Lucas numbers, *Proc. second Conf. on Fibonacci Numb. and Their Appl.*, to appear.

[4] MAHLER, K., A remark on recursive sequences, *J. Math. Sci.*, 1 (1966), 12-17.

[5] SCHINZEL, A., On two theorems of Gelfond and some of their applications, *Acta Arithm.*, 13 (1967), 177-236.

[6] SCHINZEL, A., Primitive divisors of the expression A^n-B^n in algebraic number fields, *J. reine agew. Math.*, 268/269 (1974), 27-33.

[7] SHOREY, T.N. and STEWART, C.L., On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers II., *J. London Math. Soc.*, (2) 23 (1981), 17-23.

[8] SHPARLINSKIJ, I.E., Primitive divisors of recurrent sequences (Russian), *Isv. Vyssh. Uchebn. Zaved. Math.*, (4) 215 (1980), 100-103.

[9] SHPARLINSKIJ, I.E., Number of prime divisors of recurrence sequences, *Math. Notes*, 38 (1985), 529-532.

[10] STEWART, C.L., On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers, *Proc. London Math. Soc.*, 35 (1977), 425-447.

[11] STEWART, C.L., Primitive divisors of Lucas and Lehmer numbers, Transcendence theory: advances and applications (ed. by A. Baker and D.W. Masser), *London-New York, Acad. Press,* 1977.

[12] STEWART, C.L., On divisors of terms of linear recurrence sequences, *J. reine angew. Math.,* 333 (1982), 12-31.

PÉTER KISS
Teacher's Training College,
Department of Mathematics
3301. Eger,
Hungary

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

SPECIAL PRODUCT RELATIONS BETWEEN LOCAL GAUSS SUMS

LAKKIS K.

Let p be an odd prime number, K a finite extension of the field $\mathbb{Q}_p$ of p-adic numbers, R the valuation ring of K, P the maximal ideal of R, D the different of the extension $K/\mathbb{Q}_p$, T the inertia field of $K/\mathbb{Q}_p$ and U the group of units of R. For any i=0,1 let $U_i = 1 + P^i$ (thus, U_o=U).

We consider the group G of the multiplicative residue classes mod* P of K (see [1]) and a subgroup H of G of finite index. Let χ be a character of G/H. This character χ leads to a character of G and consequently to a regular character of K^* i.e.to a character of K^* with conductor $f(\chi)=P^i$, where i=0 or i=1.

The local Gauss sum $\tau(\chi)$ is

$$\tau(\chi) = \sum_{\xi} \chi(\tfrac{\xi}{c})\, \psi(\tfrac{\xi}{c}),$$

where c is a generator of the ideal $f(\chi)D$, ψ is the "canonical" character of the additive group K^+, i.e. the composition of the canonical maps:

$$K^+ \xrightarrow{tr_{K/\mathbb{Q}_p}} \mathbb{Q}_p \to \mathbb{Q}_p/\mathbb{Z}_p \overset{\sim}{=} \mathbb{Z}[\tfrac{1}{p}]/\mathbb{Z} \to \mathbb{R}/\mathbb{Z} \xrightarrow{e^{2\pi i}} \mathbb{C}$$

and ξ runs through a set of representatives of U modulo U_i. It is easily verified that $\tau(\chi)$ does not depend on the choice of the representatives of U modulo U_i. Hence, $\tau(\chi)$ does not depend on the choice of c.

In this paper we compute the product

$$\prod_{\chi} \tau(\chi),$$

where χ runs through all the characters of the group G/H.

In order to do this we consider the group G_o of the prime residue classes modulo P of K and we denote by

$$H_o = H \cap G_o,\ G^* = HG_o,\ e=[G_o:H_o] \text{ and } f=[G:G^*].$$

It holds $G_o/H_o \cong G^*/H$. Every character χ of G/H leads (by restriction) to a character χ_o of G_o/H_o.

In the following we choose a fixed generator π of P and a fixed generator δ of D with the following

normalization

$$\mathrm{tr}_{K/T}\left(\frac{1}{\delta\pi}\right) \equiv \frac{1}{p} \mod^{+} 1 .$$

If χ is a character of G/H, then we denote by

$$c(\chi) = \begin{cases} \delta & \text{if } \chi_o = e_o \text{ the principal character of } G_o/H_o \\ \pi\delta & \text{if } \chi_o \neq e_o . \end{cases}$$

From the definition of the local Gauss sum, we have

$$\tau(\chi) = \chi\left(\frac{1}{c(\chi)}\right) \tau(\chi_o) ,$$

where $\tau(\chi_o)$ is the normed Gauss sum in the residue class field mod.p of T corresponding to the character χ_o, i.e.

$$\tau(\chi_o) = \begin{cases} \sum_{x \bmod p} \chi_o(x) e^{2\pi i \mathrm{tr}_{T/\mathbb{Q}_p}\left(\frac{x}{p}\right)} & \text{if } \chi_o \neq e_o \\ 1 & \text{if } \chi_o = e_o \end{cases}$$

(see [2]).

Hence, we have

$$\prod_{\chi} \tau(\chi) = \prod_{\chi} \chi\left(\frac{1}{c(\chi)}\right) . \prod_{\chi} \tau(\chi_o) .$$

But

$$\prod_{\chi} \chi\left(\frac{1}{c(\chi)}\right) = \prod_{\chi_o=e_o} \chi\left(\frac{1}{\delta}\right) \cdot \prod_{\chi_o\neq e_o} \chi\left(\frac{1}{\pi\delta}\right)$$

$$= \frac{\prod_{\chi_o=e_o} \chi\left(\frac{1}{\delta}\right) \cdot \prod_{\chi_o\neq e_o} \chi\left(\frac{1}{\pi\delta}\right) \cdot \prod_{\chi_o=e_o} \chi\left(\frac{1}{\pi}\right)}{\prod_{\chi_o=\varepsilon_o} \chi\left(\frac{1}{\pi}\right)}$$

$$= \frac{\prod_{\chi_o=e_o} \chi(\pi)}{\prod_{\chi} \chi(\delta\pi)}$$

and

$$\prod_{\chi} \tau(\chi_o) = \left(\prod_{\chi_o} \tau(\chi_o)\right)^f,$$

where χ_o runs through all the characters of G_o/H_o. (We mention that for f characters χ we obtain the same Gauss sum $\tau(\chi_o)$).

Hence we have

$$\prod_{\chi} \tau(\chi) = \frac{\prod_{\chi_o=e_o} \chi(\pi)}{\prod_{\chi} \chi(\delta\pi)} \cdot \left(\prod_{\chi_o} \tau(\chi_o)\right)^f.$$

The characters χ of G/H, for which $\chi_o=e_o$, are the characters of the group G/G*. Because this group is cyclic of order f, the following holds

$$\prod_{\chi_o = e_o} \chi(\pi) = (-1)^{f-1}.$$

We are now going to compute the product $\prod_{\chi} \chi(\delta\pi)$. We distinguish the following two cases:

a) G/H has either none quadratic character or it has more that one. This case exists if e,f are both odd or both even and π^f is a square in G*/H.

b) G/H has exactly one quadratic character ω. This is true if e is odd and f is even or if e is even and e is odd or both e and f are even and π^f is not a square in G*/H.

Since for every non-quadratic character $\chi \neq e$ of G/H (e is the principal character of G/H) its inverse character exists, the product $\prod_{\chi} \chi(\delta\pi)$ is reduced to the product $\prod_{\omega} \omega(\delta\pi)$ over all quadratic characters of G/H and this is equal to one if there exist more than one quadratic characters. Hence

$$\prod_{\chi} \chi(\delta\pi) = \begin{cases} 1 & \text{in case a} \\ \\ \omega(\delta\pi) & \text{in case b.} \end{cases}$$

Therefore

$$\prod_{\chi} \tau(\chi) = (-1)^{f-1} \begin{cases} 1 & \text{in case a} \\ \omega(\delta\Pi) & \text{in case b} \end{cases} \left(\prod_{\chi_o} \tau(\chi_o)\right)^f.$$

We are finally going to compute the product $\prod_{\chi_o} \tau(\chi_o)$. To this end we observe that we have: (i) for any pair of inverse characters χ_o, $\chi_o^{-1} \neq e_o$:

$$\tau(\chi_o)\tau(\chi_o^{-1}) = \chi_o(-1)N_K(\mathfrak{p}).$$

(ii) $\tau(e_o) = 1$ and (iii) for the unique quadratic character ω_o, which exists only in the case of an even e, we have

$$\tau(\omega_o) = (-1)^{f-1} \cdot i^{f\frac{p^*-p}{2}} \sqrt{N_K(\mathfrak{p})} \qquad (p^* = (-1)^{\frac{p-1}{2}} p).$$

Hence one can easily verify that

$$\prod_{\chi_o} \tau(\chi_o) = \left\{ \begin{array}{l} 1 \text{ if } e \text{ is odd} \\ (-1)^{(\frac{e}{2}-1)\frac{N(\mathfrak{p})-1}{4}} \cdot (-1)^{f-1} \cdot i^{f\frac{p^*-p}{2}} \end{array} \right\} \sqrt{N_K(\mathfrak{p})^{e-1}}.$$

if e is even.

REFERENCES

[1] H. HASSE, Zahlentheorie, Akademie-Verlag, Berlin, 1949.

[2] H. HASSE, Artinsche Führer, Artinsche L-Funktionen und Gauss'sche Summen über endlich-algebraischen Zahlkörpern, Acta Salmanticensia, Universidad de Salamanca, 1954.

[3] E. LAMPRECHT, Allgemeine Theorie der Gauss'schen Summen in endlichen kommutativen Ringen, Math.Nachr. 9, 1953.

LAKKIS, K.

Department of Mathematics
University of Thessaloniki,
54006-Thessaloniki, G r e e c e

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

INTEGRAL BASES IN FUNCTION AND NUMBER FIELDS

LAMPRECHT, E.

1. INTRODUCTION

We use the following notations:

(1)
$$\begin{aligned} &\nu_K && \text{: integrally closed integral domain,}\\ &K = \frac{\nu_K}{\nu_K} && \text{: field of quotients of } \nu_K,\\ &L && \text{: } \textit{finite} \text{ and } \textit{separable} \text{ extension field of } K \text{ of rank } n = [L:K],\\ &\nu_L && \text{: integral closure of } \nu_K \text{ in } L. \end{aligned}$$

Then ν_L is an ν_K-module and the number of generators is $\geq n$.

DEFINITION. If ν_L is free as an ν_K-module with n generators $\omega_1,\ldots,\omega_n$, $n = [L:K]$, i.e.

(1a)
$$\nu_L = \nu_K \cdot \omega_1 + \ldots + \nu_K \cdot \omega_n ,$$

then $\omega_1, \ldots, \omega_n$ is called a *relative integral basis* of v_L over v_K.

There are some questions concerning this notation.

a) When does a relative integral basis exist?

b) How to calculate this integral basis?

c) When the existence of an integral basis can be excluded?

The general conditions mentioned above cover the following well known special arithmetical cases:

[1] K *number field*, v_K principal order of algebraic integers of K (for instance $K = \mathbb{Q}$, $v_K = \mathbb{Z}$).

[2] K *local field* (with respect to a discrete rank 1 valuation), v_K valuation ring.

[3] K *algebraic function field* of one variable over k, $x \in K$ transcendental over k, v_K integral closure of k[x] in K.

In these cases v_K is a *Dedekind domain*, if L is a finite separable extension of K, v_L is also a Dedekind domain. The following well known result gives an answer to the questions a) and c) for special cases of [1], [3] and the case [2].

RULE. *If* ν_K *is a principal ideal domain and* L *is a finite extension of* K *then there always exists an integral basis for* ν_L *over* ν_K.

In this paper we give a report on more general cases for Dedekind domains and mention some results on *Krull domains*, which cover the following example:

[4] Let k be a field, $R_0 = k[X_1,\ldots,X_n]$ (polynomials in the variables $X_1,\ldots,X_n$), $K_0 = \frac{R_0}{R_0}$, K a finite extension of K_0 and ν_K the integral closure of R_0 in K; R_0 and ν_K are Krull domains and R_0 is also a *factorial ring*.

This report and some supplements are contained in 2. The calculation of integral bases of Kummer extensions of the fields of quotients of Krull domains and factorial domains is given in 3. . Section 4. contains some examples and applications.

2. GENERAL ALGEBRAIC AND ARITHMETIC CONDITIONS

We use some algebraic facts to obtain results for Dedekind or more general domains. Suppose (1); let $\{x_1,\ldots,x_n\}$ be a basis of L over K where $x_\nu \in \nu_L$ $(\nu = 1,\ldots,n)$, $Tr_{L/K}$ the trace of L over K and let

$\delta_\nu(x)$ $(\nu = 1,\ldots,n)$ be the isomorphisms of L into an algebraic closure $\bar{K}$ of K, then the determinant

$$d_{L/K}(x_1,\ldots,x_n) = \det(\mathrm{Tr}_{L/K}(x_\nu x_\mu)) = \det{}^2(\delta_\nu(x_\mu)) \tag{2}$$

is called *discriminant of the basis*. A change of the vector space basis of L/K implies the formula

$$d_{L/K}(y_1,\ldots,y_n) = \det(\alpha_{ij})^2 \cdot d_{L/K}(x_1,\ldots,x_n)$$

$$\text{for} \quad \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = (\alpha_{ij}) \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} . \tag{2a}$$

By use of module-theoretic considerations A. Thome has shown in [9], §2 the *rule of localization*.

PROPOSITION 1. *Suppose* (1) *and let*

$$\begin{cases} (\nu_K)_p = \dfrac{\nu_K}{\nu_K \setminus p} , \ (\nu_L)_p \text{ integral closure of } (\nu_K)_p \text{ in L} \\ \text{for } p \in \mathrm{Spec}(\nu_K) \end{cases} \tag{3}$$

Then $\{x_1,\ldots,x_n\} \subseteq \nu_L$ *is an integral basis for* ν_L *over* ν_K *if and only if*

$\{x_1,\ldots,x_n\}$ *is an integral basis for* $(\nu_L)_p$ *over* $(\nu_K)_p$ *for all* $p \in \mathrm{Spec}(\nu_K)$. (3a)

Now we additionally assume that v_K is a *Krull domain*, i.e.: There exists a family $(v_i)_{i\in I}$ of valuations v_i of K with the following properties ([10], p. 82; [2], p. 1-34):

(KD_1): Every v_i has rank 1 and is discrete.

(KD_2): We have

$$v_K = \bigcap_{i\in I} v_{v_i}, \quad v_{v_i} \text{ valuation ring of } v_i \tag{4}$$

and

$$v_{v_i} = (v_K)_{p_i} \quad \text{localization at the center } p_i \text{ of } v_i \text{ in } v_K. \tag{4a}$$

(KD_3): For every $x \neq 0$, $x \in K$ we have $v_i(x) = 0$ for almost all $i \in I$.

Then $(v_i)_{i\in I}$ is said to be a family of *essential valuations* of v_K. Every v_i of K has at least one and at most $n = [L:K]$ extensions w_{ij} $(j = 1,\ldots,g_i)$ in L; the w_{ij} are discrete valuations of rank 1 and for the corresponding valuation rings holds

$$(v_L)_{p_i} = \bigcap_{j=1}^{g_i} v_{w_{ij}} \tag{5}$$

is the integral closure of $(v_K)_{p_i} = v_{v_i}$ in L. Furthermore, we have

(5a) $$v_L = \bigcap_{i,j} v_{w_{ij}} = \bigcap_i (v_L)_{p_i} ,$$

v_L is a Krull domain in L and $(w_{ij})_{i\in I,j}$ is its family of essential valuations.

PROPOSITION 1a. *Let v_K be a Krull domain and $\{x_1,\dots,x_n\}$ a fieldbasis of L/K of integral elements $x_\nu \in v_L$ ($\nu = 1,\dots,n$). If $\{x_1,\dots,x_n\}$ is a (local) integral basis of $(v_L)_{p_i}$ over $(v_K)_{p_i} = v_{v_i}$ for all v_i, then $\{x_1,\dots,x_n\}$ is an integral basis of v_L/v_K.*

PROOF. We consider

(5b) $$L \ni y = \sum_{\nu=1}^{n} \xi_\nu x_\nu \quad \text{with} \quad \xi_\nu \in K .$$

If $\xi_\nu \in v_K$ ($\nu = 1,\dots,n$) then we have $y \in v_L$.

Now we suppose $y \in v_L$ and that there exists at least one $\xi_\nu \notin v_K$ in (5b); then $\xi_\nu \notin v_{v_i}$ for at least one v_i of K. But $\{x_1,\dots,x_n\}$ is an integral basis of $(v_L)_{p_i}/v_{v_i}$ and $y \in v_L \subseteq (v_L)_{p_i}$. Therefore all the coefficients of y in (5b) must be in v_{v_i}. Thus $\{x_1,\dots,x_n\}$ is an integral basis of v_L/v_K. □

Some further criteria are known in the case of a *Dedekind domain* v_K. Then v_L is a Dedekind domain too (the valuation rings v_{v_i} and $v_{w_{ij}}$ respectively are principal ideal

domains and also Dedekind domains). We consider the ideal

$$(6) \qquad d_{L/K} = \nu_K \cdot \{d_{L/K}(x_1,\ldots,x_n) \mid \{x_1,\ldots,x_n\} \subseteq \nu_L\} \subseteq \nu_K ,$$

generated by the discriminants of bases of integral elements. $d_{L/K}$ is called the *relative discriminant* of ν_L/ν_K.

We mention the well known

PROPOSITION 2. *Suppose* (1) *and* ν_K *to be a Dedekind domain. Then* $\{x_1,\ldots,x_n\} \subseteq \nu_L$ *is an integral basis of* ν_L/ν_K *if and only if*

$$(6a) \qquad (d_{L/K}(x_1,\ldots,x_n)) = d_{L/K} \quad (\textit{principal ideal}).$$

The usual properties of discriminants are valid in this case, especially the multiplicative formula for extensions in towers. This leads to the following

PROPOSITION 2a. *Let* $\nu_{K_0} \subset \nu_K \subset \nu_L$ *be Dedekind domains and* $K_0 \subset K \subset L$ *be the tower of corresponding finite field extensions. Suppose that there exist integral bases for* L/K_0 *and for* K/K_0. *Then the system* $\{x_1,\ldots,x_n\} \subseteq \nu_L$ *is an integral basis for* ν_L/ν_K *if and only if* (N_{K/K_0} : *norm*)

(6b) $$(N_{K/K_0}(d_{L/K}(x_1,\ldots,x_n))) = \frac{d_{L/K_0}}{d^n_{K/K_0}} \; ; \; n = [L:K].$$

If the integral bases of L/K_0 and of K/K_0 are determined, this proposition can be applied for testing the integral basis property of a system $\{x_1,\ldots,x_n\}$ (compare 4., and also Schmal [8], §3).

REMARK. Let $K_0 \subset K \subset L$ be a tower of finite extensions and let integral bases of L/K and of K/K_0 be known, then an integral basis of L/K_0 can easily be calculated.

In the case of Dedekind domains further essential theoretical criteria can be given:

THEOREM I (ARTIN [1]). *Let v_K be a Dedekind domain and $\{x_1,\ldots,x_n\}$ a field basis of the extension L/K. Then there exists a fractional ideal a_x of K such that*

(7) $$(d_{L/K}(x_1,\ldots,x_n)) = a_x^2 \cdot d_{L/K}$$

and we have: There exists an integral basis for L/K if and only if

(7a) a_x *is a principal ideal of* K.

THEOREM II (H.B. MANN [7]). *Let* v_K *be a Dedekind domain which is no principal ideal domain. Then there exists an extension* L *of* K *of degree* $2 = [L:K]$ *without any relative integral basis.*

THEOREM III (A. FRÖHLICH [3]). *Let* K *be an algebraic number field. Then the following is equivalent:*

(i) *The class number* $h(K)$ *of* K *is odd.*

(ii) *Every finite extension* L/K *where* $d_{L/K}$ *is a principal ideal has an integral basis.*

These results can be improved and hold more generally as shown by A. Thome [9a] in the following considerations:

Let $G = \{\sigma_1,\ldots,\sigma_n\}$ be a finite group of order n, S_n the symmetric group of all permutations of the σ_ν and A_n the corresponding alternating group. Then by use of the regular representation ($\sigma \circ \sigma_\nu$, $\nu = 1,\ldots,n$, yields a permutation π_σ of $(\sigma_1,\ldots,\sigma_n)$) we obtain an inclusion map

$$(8) \qquad G \xrightarrow{reg} S_n, \text{ where } G \ni \sigma \longrightarrow \pi_\sigma \in S_n .$$

G is called IB-group, iff $reg(G) \subseteq A_n$.

REMARKS. a) If G is a finite group of odd order, then G is an IB-group. - b) If the order $|G|$ is even, then G is an IB-group if and only if the 2-Sylowgroup is not a cyclic group.

Then Thome's result reads:

THEOREM Ia. *Let* ν_K *be a Dedekind domain,* L *a finite Galois extension with group* $G = G(L/K)$ *and let* $G(L/K)$ *be an IB-group. Then an integral basis for* ν_L/ν_K *exists if and only if there is an element* $b \in \nu_K$ *such that*

$$(8a) \qquad d_{L/K} = (b^2) .$$

If L *is an unramified Galois extension of* K *and* $G(L/K)$ *is an IB-group, then there exists an integral basis.*

Furthermore, Fröhlich's Theorem can be generalized to Galois extensions of the fields of quotients of arbitrary Dedekind domains.

3. INTEGRAL BASES OF KUMMER EXTENSIONS

We calculate integral bases for a class of Galois extensions of a field K by a method which can be applied in very general cases of Krull domains. Let be

$$n \in \mathbb{N},\ K = \frac{\nu_K}{\nu_K^{\times}} \text{ and } \operatorname{char}(K) \nmid n;$$

$$K \ni \varepsilon_n \quad (n\text{-th primitive root of unity});$$

(9)

$$\nu_K\text{: } \textit{Krull domain},\ (v_i)_{i\in I} \text{ family of essential valuations of } \nu_K \quad (v_i(K^{\times}) = \mathbb{Z}).$$

For v_i $(i \in I)$ p_i denotes the corresponding *prime divisor*; the *divisor group* (in additive notation)

$$(\mathrm{Div}(K;(v_i));+) = \{a = \sum_{i\in I} n_i \cdot p_i;\ n_i \in \mathbb{Z},\ \text{almost all } n_i = 0\} \tag{9a}$$

contains the subgroup PDiv(K) of *principal divisors*

$$\mathrm{div}(x) = \sum_{i\in I} v_i(x) \cdot p_i,\ x \neq 0,\ x \in K; \tag{9b}$$

we have $x \neq 0$, $x \in \nu_K$ if and only if div(x) is an integral divisor $(v_i(x) \geq 0,\ i \in I)$.

REMARK 1. These facts hold also in the special cases of a Dedekind domain or of a factorial ring ν_K. - If

$$n^{-1} \in \nu_K, \text{ i.e. n unit in } \nu_K, \tag{9c}$$

then char(K) $\nmid$ n; the property (9c) holds if K is a function field over k, char(k) $\nmid$ n and $\nu_{v_i} \supseteq k$ for all $i \in I$.

L is called a *Kummer extension of* K *of exponent* n, if L/K is a finite Galois extension and $G = G(L/K)$ is abelian of exponent n; if $G = \{\sigma, \sigma^2, \ldots, \sigma^n = id\}$ is cyclic of exponent n, then L is a *cyclic Kummer field over* K *of exponent* n.

In the cyclic case L is generated in the form (compare [4], [5], [5a], [6])

$$\begin{aligned} &L = K(y),\ y^n = B \in K, \\ &B \neq B_o^d, \text{ where } d|n,\ d > 1 \text{ and } B_o \in K; \end{aligned} \tag{10}$$

the generating automorphism σ of L over K can be fixed according to

$$\sigma^\nu(y^\mu) = \varepsilon_n^{\nu\mu} \cdot y^\mu \quad (\nu = 1,\ldots,n;\ \mu \in \mathbb{N}) . \tag{10a}$$

Then all the other Kummer generations of L over K can be obtained in the form

$$\begin{aligned} &L = K(y'),\ y'^n = B' \in K, \text{ where} \\ &y \longmapsto y' = y^\kappa \cdot B_o,\ B \longmapsto B' = B^\kappa \cdot B_o^n, \\ &B_o \neq 0,\ B_o \in K,\ (\kappa,n) = 1; \end{aligned} \tag{10b}$$

Thus the right hand side of (10) can be modified mod. $(K^\times)^n$.

DEFINITION 2. Az element $B \neq 0$, $B \in K$ is said to be *distinguished with respect to* n if it is of the form

$$B = \prod_{\nu=1}^{n-1} b_\nu^\nu, \quad b_\nu \in K,$$

$$\text{(11)} \qquad \operatorname{div}(B) = \sum_{\nu=1}^{n-1} \nu \cdot \operatorname{div}(b_\nu) ,$$

$$\operatorname{div}(b_\nu) = \sum_{i \in I, v_i(B)=\nu} p_i \quad (\nu = 1,\ldots,n-1).$$

REMARK 2. $\operatorname{div}(b_\nu)$ is the sum of all prime divisors p_i with the property $v_i(B) = \nu$ and we suppose that all tnese $\operatorname{div}(b_\nu)$ are given by elements $b_\nu \in K$; and for the greatest common divisor we have

$$\text{(11a)} \qquad \gcd(b_{\nu_1}, b_{\nu_2}) = \operatorname{div}(1) \quad \text{for} \quad \nu_1 \neq \nu_2;$$

furthermore, there holds

$$\text{(11b)} \qquad 0 \leq v_i(B) \leq n-1 \quad \text{for all} \quad i \in I,$$

and $B \in \nu_K$. - If ν_K is a factorial ring or a principal ideal domain, then an arbitrary $B' \neq 0$, $B' \in K$, can be transformed mod $(K^\times)^n$ into a B distinguished with respect to n.

By use of localization at the p_i $(i \in I)$ and transfer of arithmetical considerations for Kummer extensions (compare [4], [5], [5a]) we obtain

LEMMA 1. *Suppose* (9), (9c) *and that* L *according to* (10) *is a cyclic Kummer field of exponent* n *where* B *is distinguished with respect to* n. *Then* $y \in \nu_L$. $\{1,y,\ldots,y^{n-1}\}$ *is a field basis of integral elements and the ramified primes and local discriminant components are obtained by*

$$e(\mathfrak{P}_{ij}/\mathfrak{p}_i) = \frac{n}{(n,v_i(B))} \quad \text{for} \quad v_i(B) \neq 0$$

(11c) $(i \in I)$.

$$v_i(d_{\mathfrak{p}_i}(L/K)) = (n,v_i(B)) \cdot (e(\mathfrak{P}_{ij}/\mathfrak{p}_i)-1)$$

all these $\mathfrak{p}_i$ *are tamely ramified.*

For $\mu = 2,\ldots,n-1$ we have

(11d) $$(y^\mu)^n = B^\mu \in K ;$$

but in general B^μ is not distinguished with respect to n (according to definition 2).

We suppose (11) for B. Then there exist elements

(12) $$g^{(\mu)} \in \nu_K \quad (\mu = 2,\ldots,n-1)$$

such that

(12a) $$\widetilde{B}^{(\mu)} = \frac{B^\mu}{(g^{(\mu)})^n} \in \nu_K \qquad (\mu = 2,\ldots,n-1)$$

are distinghished with respect to n. The elements $g^{(\mu)}$ can be calculated in the following way: For every pair of numbers (ν,μ), $1 \le \nu \le n-1$, $\mu \in \mathbf{N}_o$ there exist numbers $\lambda_{\nu,\mu} \in \mathbf{N}_o$ (uniquely determined), such that

(12b) $\quad 0 \le \nu \cdot \mu - \lambda_{\nu,\mu} \cdot n < n \quad (1 \le \nu \le n-1,\ \mu \in \mathbf{N}_o).$

Let

(12c) $\quad g^{(\mu)} = \prod_{\nu=1}^{n-1} b_\nu^{\lambda_{\nu,\mu}} \in \nu_K$, $\lambda_{\nu,\mu}$ according to (12b),

then the reduced elements $\widetilde{B}^{(\mu)}$ in (12a) are distinghished with respect to n; $g^{(1)} = 1$.

We consider the elements

(13) $\quad \tilde{y}^{(0)} = 1,\ \tilde{y}^{(\mu)} = \dfrac{y^\mu}{g^{(\mu)}} \quad (\mu = 1,\ldots,n-1);$

the elements $\tilde{y}^{(\mu)}$ $(\mu = 0,1,\ldots,n-1)$ give also a field basis of L over K. Because of

(13a) $\quad (\tilde{y}^{(\mu)})^n = \dfrac{y^{n\cdot\mu}}{(g^{(\mu)})^n} = \dfrac{B^\mu}{(g^{(\mu)})^n} = \widetilde{B}^{(\mu)} \in \nu_K$

$(\mu = 1,\ldots,n-1)$

all basis elements $\tilde{y}^{(\mu)}$ are *integral over* ν_K and the n-th powers are distinguished with respect to n.

REMARK 3. The field basis (13) is called the *reduced basis corresponding to* $\{1,y,\ldots,y^{n-1}\}$; the elements $\tilde{y}^{(\mu)}$ are obtained by multiplying the y^{μ} in such a way by factors of K, that $(\tilde{y}^{(\mu)})^n$ are distinguished elements.

In order to calculate the discriminant of the basis (13) we study the trace elements $\mathrm{Tr}_{L/K}(\tilde{y}^{(\mu_1)}\,\tilde{y}^{(\mu_2)})$.
Then by use of (10a), $\mathrm{Tr}_{L/K}(z) = \sum_{\nu=0}^{n-1} \sigma^{\nu}(z)$ and by relations for roots of unity we obtain

$$\text{(13b)}\qquad \mathrm{Tr}_{L/K}(\tilde{y}^{(\mu)}\cdot 1) = \mathrm{Tr}_{L/K}\left[\frac{y^{\mu}}{g^{(\mu)}}\right] = \begin{cases} n \text{ for } \mu = 0, \text{ i.e. } \tilde{y}^{(0)} = 1 \\ 0 \text{ for } \mu = 1,\ldots,n-1 \end{cases}$$

and

$$\mathrm{Tr}_{L/K}(\tilde{y}^{(\mu_1)}\cdot\tilde{y}^{(\mu_2)}) = \mathrm{Tr}_{L/K}\left[\frac{y^{\mu_1+\mu_2}}{g^{(\mu_1)}\cdot g^{(\mu_2)}}\right] =$$

(13c)

$$= \begin{cases} 0 \quad \text{for } \mu_1+\mu_2 \not\equiv 0 \bmod n \ (\mu_1,\mu_2 = 1,\ldots,n-1)\,, \\ \dfrac{n}{g^{(\mu_1)}\cdot g^{(\mu_2)}}\cdot B \quad \text{for } \mu_1+\mu_2 \equiv 0 \bmod n, \text{ i.e. } \mu_2 = n-\mu_1 \end{cases}$$

According to the decompositions (11) and (12c) there holds

$$(13d)\qquad \prod_{\nu=1}^{n-1} b_\nu^{\nu-\lambda_{\nu,\mu_1}-\lambda_{\nu,n-\mu_1}} = \frac{B}{g^{(\mu_1)}\cdot g^{(n-\mu_1)}}$$

$$(\mu_1=1,\ldots,n-1).$$

We discuss the exponents of the b_ν. Then (12b) shows that

$$\lambda_{\nu,\mu_i}\cdot n \le \nu\cdot\mu_i < (\lambda_{\nu,\mu_i}+1)\cdot n,\ (i=1,2),$$

$$(14)\qquad (\lambda_{\nu,\mu_1}+\lambda_{\nu,n-\mu_1})\cdot n \le \nu\cdot(\mu_1+n-\mu_1) < (\lambda_{\nu,\mu_1}+\lambda_{\nu,n-\mu_1}+2)\cdot n.$$

If $\nu\cdot\mu_1 \not\equiv 0 \bmod n$, then $0 < \nu\cdot\mu_1 - \lambda_{\nu,\mu_1}\cdot n$ and we formulate

LEMMA 2. *Let be* $1\le\nu\le n-1$, $1\le\mu_1\le n-1$; *then*

$$(14a)\qquad \lambda_{\nu,\mu_1}+\lambda_{\nu,n-\mu_1} = \begin{cases} \nu-1, \text{ i.e. } b_\nu^{\nu-\lambda_{\nu,\mu_1}-\lambda_{\nu,n-\mu_1}} = b_\nu \\ \quad \textit{for } \nu\cdot\mu_1 \not\equiv 0 \bmod n, \\ \nu, \text{ i.e. } b_\nu^{\nu-\lambda_{\nu,\mu_1}-\lambda_{\nu,n-\mu_1}} = 1 \\ \quad \textit{for } \nu\cdot\mu_1 \equiv 0 \bmod n. \end{cases}$$

Let ν *be fixed and* $\nu_1 = (\nu,n) < n$, *then there are*

$$\nu_1\text{-}1 \text{ values of } \mu_1 \text{ for which } \nu\cdot\mu_1 \equiv 0 \bmod n,$$

(14b)

$$n\text{-}\nu_1 \text{ values of } \mu_1 \text{ for which } \nu\cdot\mu_1 \not\equiv 0 \bmod n.$$

Let μ_1 *be fixed and* $\mu_1' = (\mu_1,n) < n$, *then there are*

$$\mu_1'\text{-}1 \text{ values of } \nu \text{ for which } \nu\cdot\mu_1 \equiv 0 \bmod n,$$

(14c)

$$n\text{-}\mu_1' \text{ values of } \nu \text{ for which } \nu\cdot\mu_1 \not\equiv 0 \bmod n.$$

PROOF. 1) Let $\nu\cdot\mu_i \not\equiv 0 \bmod n$ $(i = 1,2)$; then $\lambda_{\nu,\mu_i}\cdot n < \nu\cdot\mu_i$, $\nu\cdot\mu_1 + \nu(n-\mu_1) \equiv 0 \bmod n$, so $(\lambda_{\nu,\mu_1} + \lambda_{\nu,n-\mu_1})\cdot n < \nu\cdot n < (\lambda_{\nu,\mu_1} + \lambda_{\nu,n-\mu_1} + 2)\cdot n$ and we have (ν being an integer)

$$\lambda_{\nu,\mu_1}+\lambda_{\nu,n-\mu_1} < \nu < \lambda_{\nu,\mu_1} + \lambda_{\nu,n-\mu_1} + 2, \text{ i.e.}$$

$$\nu = \lambda_{\nu,\mu_1} + \lambda_{\nu,n-\mu_1} + 1 .$$

2) Let $\nu\cdot\mu_1 \equiv 0 \bmod n$. Then $\lambda_{\nu,\mu_1}\cdot n = \nu\cdot\mu_1$ and $\lambda_{\nu,n-\mu_1}\cdot n = \nu(n-\mu_1)$. Therefore $(\lambda_{\nu,n-\mu_1}+\lambda_{\nu,\mu_1})\cdot n = \nu\cdot n$ and we obtain the second line of (14a).

3) A simple enumeration of the possible values of μ_1 (and ν respectively) leads to (14b) and (14c). □

By use of lemma 2 the remaining value (13d) reads as follows

$$\frac{B}{g^{(\mu_1)} \cdot g^{(n-\mu_1)}} = \prod_{\nu \cdot \mu_1 \not\equiv 0 \bmod n} b_\nu =$$

(14d)

$$= \begin{cases} \prod_{\nu=1}^{n-1} b_\nu & \text{for } (\mu_1, n) = 1, \\ \prod_{\substack{\nu=1 \\ n \nmid (\nu \cdot \mu_1)}}^{n-1} b_\nu & \text{for } (\mu_1, n) = \mu_1' \neq 1. \end{cases}$$

Now we calculate the basis discriminant

$$d_{L/K}(1, \tilde{y}^{(1)}, \tilde{y}^{(2)}, \ldots, \tilde{y}^{(n-1)}) = \det(\mathrm{Tr}_{L/K}(\tilde{y}^{(\mu_1)} \cdot \tilde{y}^{(\mu_2)})) =$$

$$= n \cdot \prod_{\mu_1=1}^{n-1} \mathrm{Tr}_{L/K}(\tilde{y}^{(\mu_1)} \cdot \tilde{y}^{(n-\mu_1)}) = \pm n^n \cdot \prod_{\mu_1=1}^{n-1} \frac{B}{g^{(\mu_1)} \cdot g^{(n-\mu_1)}}$$

$$= \pm n^n \cdot \prod_{\mu_1=1}^{n-1} b_\nu^{\nu-\lambda_{\nu,\mu_1}-\lambda_{\nu,n-\mu_1}} = \pm n^n \cdot \prod_{\nu=1}^{n-1} b_\nu^{n-(n,\nu)} .$$

By use of (9c) we obtain

$$(15) \qquad \mathrm{div}(d_{L/K}(1, \tilde{y}^{(1)}, \ldots, \tilde{y}^{(n-1)})) = \sum_{\nu=1}^{n-1} (n-(n,\nu)) \cdot \mathrm{div}(b_\nu) .$$

Lemma 1 and especially (11c) show: If $v_i(B) > 0$, i.e. if p_i $(i \in I)$ is ramified in L, then we have

$$(15a) \qquad v_i(d_{L/K}(1,\tilde{y}^{(1)},\ldots,\tilde{y}^{(n-1)})) = n-(n,v_i(B)) = \\ = v_i(d_{p_i}(L/K)) \ ;$$

this is the v_i-value of the local discriminant.

The localization $(v_K)_{p_i}$ is a principal ideal domain and therewith a Dedekind domain; therefore there exists an integral basis $\{\omega_1,\ldots,\omega_n\}$ for the integral closure $(v_L)_{p_i}$ and we have (proposition 2 and rule in 1.)

$$(15b) \qquad d_{L/K}(\omega_1,\ldots,\omega_n) \cong d_{p_i}(L/K) \ .$$

$\{1,\tilde{y}^{(1)},\ldots,\tilde{y}^{(n-1)}\}$ is a field basis of elements integral at p_i. Therefore there exists an $(v_K)_{p_i}$-unimodular basis--transformation from $\{\omega_1,\ldots,\omega_n\}$ to $\{1,\tilde{y}^{(1)},\ldots,\tilde{y}^{(n-1)}\}$ and $\{1,\tilde{y}^{(1)},\ldots,\tilde{y}^{(n-1)}\}$ must be a local integral basis of $(v_L)_{p_i}$ over $(v_K)_{p_i}$. This holds for all p_i of v_K (if p_i is not ramified in L, the result is trivial).
According to proposition 1a $\{1,\tilde{y}^{(1)},\ldots,\tilde{y}^{(n-1)}\}$ is a global integral basis.

THEOREM IV. *Let* K *be the field of quotients of a Krull domain and suppose* (9), (9c); *further, let* $L = K(y)$ *be a cyclic Kummer field of exponent* n *over* K *and* $y^n = B \in K$, *where* B *is distinguished with respect to* n. *Then there exists an integral basis of* v_L *over* v_K: *the reduced basis* $\{1,\tilde{y}^{(1)},\ldots,\tilde{y}^{(n-1)}\}$ *of* (13) *corresponding to* $\{1,y\ldots,y^{n-1}\}$. *If* v_K *is a factorial ring then this is valid for every cyclic Kummer extension of exponent* n.

Consider the case of a general abelian Kummer extension L of exponent n; by use of primary decomposition and the basis theorem for finite abelian groups we may suppose that the Galois group $G = G(L/K)$ is the direct product of cyclic subgroups Z_ρ:

$$G = Z_1 \times Z_2 \times \ldots \times Z_r,$$

$$Z_\rho = [\sigma_\rho],\ \exp(\sigma_\rho) = n(\rho) \text{ for } \rho = 1,\ldots,r, \tag{16}$$

$$n = n(1) \geq n(2) \geq \ldots \geq n(r),\ n(\rho) \mid n(\rho-1),$$

then

$$G = Z_\rho \times Z'_\rho,\ Z_\rho = \bigotimes_{\substack{\nu=1 \\ \nu \neq \rho}}^{r} Z_\nu \quad (\rho = 1,\ldots,r)$$

$$G = \{\sigma = \sigma_1^{x_1} \ldots \sigma_r^{x_r} \mid x_\rho \bmod n(\rho)\}\ . \tag{16a}$$

This implies the following generation of the field extension

$$L = K(y_1,\ldots,y_r) = K_1 \cdot \ldots \cdot K_r,\ K_\rho = K(y_\rho) = L^{z'_\rho},$$

(16b)

$$y_\rho^{n(\rho)} = B_\rho \in \nu_K \text{ (irreducible)};$$

the effect of the automorphisms can be described as follows

$$(\sigma_1^{x_1}\ldots\sigma_r^{x_r})(a\cdot y_1^{\alpha_1}\ldots y_r^{\alpha_r}) =$$

$$(16c) \qquad = a y_1^{\alpha_1}\ldots y_r^{\alpha_r} \cdot \varepsilon^{\sum_{\rho=1}^{r} \frac{n}{n(\rho)} x_\rho \alpha_\rho}$$

for $a \in K$, $0 \le x_\rho,\ \alpha_\rho < n(\rho)$ $(\rho = 1,\ldots,r)$.

The elements

$$(17) \qquad y_1^{\alpha_1}\ldots y_r^{\alpha_r} = z_{\alpha_1,\ldots,\alpha_r} \qquad \begin{matrix}(0 \le \alpha_\rho < n(\rho),\\ \rho = 1,\ldots,r)\end{matrix}$$

yield a field basis of L over K of integral elements. The irreducible equations of these basis elements are

$$(z_{\alpha_1,\ldots,\alpha_r})^{n'} = \prod_{\rho=1}^{r} (B_\rho)^{\alpha_r \cdot \frac{n'}{n(\rho)}} =$$

$$(17a) \qquad = B(\alpha_1,\ldots,\alpha_r)$$

where $n' = n(\alpha_1,\ldots,\alpha_r) = \operatorname{lcm}(\ldots, \frac{n(\rho)}{\gcd(\alpha_\rho, n(\rho))})$.

DEFINITION 3. Suppose that the elements

$$B_\rho = \prod_{\nu=1}^{n(\rho)} b_{\nu,\rho}^{\nu} \qquad (\rho = 1,\dots,r) \tag{17b}$$

are distinguished with respect to $n(\rho)$ respectively and that all the divisors $\gcd(\dots,b_{\nu,\rho},\dots)$ can be given by integral elements of ν_K, then we say: L/K has a *distinguished generation.*

REMARK 4. If ν_K is a factorial ring then every Kummer extension has a distinguished generation. Supposing the situation of definition 3 we are able to find elements $g(\alpha_1,\dots,\alpha_r) \in \nu_K$, such that

$$(\tilde{z}_{\alpha_1,\dots,\alpha_r})^{n(\alpha_1,\dots,\alpha_r)} = \tilde{B}(\alpha_1,\dots,\alpha_r)$$

$$\text{where } \tilde{z}_{\alpha_1,\dots,\alpha_r} = \frac{z_{\alpha_1,\dots,\alpha_r}}{g(\alpha_1,\dots,\alpha_r)} \in \nu_L\,, \tag{18}$$

$$\tilde{B}(\alpha_1,\dots,\alpha_r) = \frac{B(\alpha_1,\dots,\alpha_r)}{g(\alpha_1,\dots,\alpha_r)^{n(\alpha_1,\dots,\alpha_r)}}$$

$$0 \le \alpha_\rho < n(\rho),\ \rho = 1,\dots,r\ .$$

The elements $\tilde{z}_{\alpha_1,\ldots,\alpha_r}$ also yield a basis of integral elements for L over K and the elements $\tilde{B}(\alpha_1,\ldots,\alpha_r)$ are distinguished with respect to $n(\alpha_1,\ldots,\alpha_r)$.

THEOREM IVa. *Let* ν_K *and* K *satisfy the conditions of theorem IV and let* L *be a Kummer extension of* K *of exponent* n *which has a distinguished generation. Then there exists an integral basis of* ν_L/ν_K*: the elements* $\tilde{z}_{\alpha_1,\ldots,\alpha_r}$ *of* (18) *yield this basis; they can be obtained from the basis* $\{\ldots,y_1^{\alpha_1}\ldots y_r^{\alpha_r},\ldots\}$ (17) *by reducing to elements* $\tilde{z}_{\alpha_1,\ldots,\alpha_r}$ *such that the* $\tilde{B}(\alpha_1,\ldots,\alpha_r)$ *on the right hand side of* (18) *are distinguished with respect to* $n(\alpha_1,\ldots,\alpha_r)$*, respectively.*

PROOF. We consider the equation

$$x = \sum_{\substack{\alpha_1,\ldots,\alpha_r \\ \alpha_\rho \bmod n(\rho)}} \xi_{\alpha_1,\ldots,\alpha_r} \cdot \tilde{z}_{\alpha_1,\ldots,\alpha_r} \in L \tag{18a}$$

where $\xi_{\alpha_1,\ldots,\alpha_r} \in K$.

If all the $\xi_{\alpha_1,\ldots,\alpha_r} \in \nu_K$, then $x \in \nu_L$.

Now suppose $x \in \nu_L$. We assert that all the $\xi_{\alpha_1,\ldots,\alpha_r} \in \nu_K$. We use the fact $\tau(x) \in \nu_L$ for all $\tau \in G$. Choose one of

the elements $\tilde{z}_{\alpha_1,\ldots,\alpha_r}$ and consider the field

$$K_{\alpha_1,\ldots,\alpha_r} = K(\tilde{z}_{\alpha_1,\ldots,\alpha_r}) ,$$

(18b)

$$\text{where } [K_{\alpha_1,\ldots,\alpha_r}:K] = n' = n(\alpha_1,\ldots,\alpha_r)$$

and $1,\tilde{z}_{\alpha_1,\ldots,\alpha_r},\ldots,\tilde{z}_{(n'-1)\alpha_1,\ldots,(n'-1)\alpha_r}$ is an integral basis of $K_{\alpha_1,\ldots,\alpha_r}/K$. Let $U_{\alpha_1,\ldots,\alpha_r} = G(L/K_{\alpha_1,\ldots,\alpha_r}) \trianglelefteq G(L/K)$ be the subgroup of $K_{\alpha_1,\ldots,\alpha_r}$, i.e.

$$L^{U_{\alpha_1,\ldots,\alpha_r}} = K_{\alpha_1,\ldots,\alpha_r} , \quad |U_{\alpha_1,\ldots,\alpha_r}| = |G|:n' . \tag{18c}$$

The basis elements of $K_{\alpha_1,\ldots,\alpha_r}$ over K are invariant for every $\sigma \in U_{\alpha_1,\ldots,\alpha_r}$. If $\tilde{z}_{\beta_1,\ldots,\beta_r} \notin K_{\alpha_1,\ldots,\alpha_r}$ then there is at least one $\sigma \in U_{\alpha_1,\ldots,\alpha_r}$ such that $\sigma(\tilde{z}_{\beta_1,\ldots,\beta_r}) = \varepsilon' \cdot \tilde{z}_{\beta_1,\ldots,\beta_r}$, where $\varepsilon' \neq 1$ is a root of unity. Therefore

$$\mathrm{Tr}_{L/K_{\alpha_1,\ldots,\alpha_r}}(\xi\cdot\tilde{z}_{\beta_1,\ldots,\beta_r}) = \sum_{\sigma\in U_{\alpha_1,\ldots,\alpha_r}} (\xi\cdot z_{\beta_1,\ldots,\beta_r})$$

$$= \begin{cases} 0 & \text{for } \tilde{z}_{\beta_1,\ldots,\beta_r} \notin K_{\alpha_1,\ldots,\alpha_r} \\ \frac{|G|}{n} \cdot \xi\cdot\tilde{z}_{\beta_1,\ldots,\beta_r} & \text{for } \tilde{z}_{\beta_1,\ldots,\beta_r} \in K_{\alpha_1,\ldots,\alpha_r},\ \xi \in K \end{cases} . \tag{18d}$$

For x in (18a) this implies

$$\mathrm{Tr}_{L/K_{\alpha_1,\ldots,\alpha_r}}(x) =$$

(18e)

$$= \frac{|G|}{n'} \cdot \sum_{\lambda=0}^{n'-1} \xi_{\lambda\alpha_1,\ldots,\lambda\alpha_r} \cdot \tilde{z}_{\lambda\alpha_1,\ldots,\lambda\alpha_r} \cdot$$

$\frac{|G|}{n'}$ is a unit of ν_K and $\xi_{\lambda\alpha_1,\ldots,\lambda\alpha_r} \in \nu_K$ for $\lambda = 0,1,\ldots,n'-1$. Every $\xi_{\alpha_1,\ldots,\alpha_r}$ in (18a) occurs in at least one field $K_{\alpha_1,\ldots,\alpha_r}$. Therefore all the $\xi_{\alpha_1,\ldots,\alpha_r} \in \nu_L$, and $\{\ldots,\tilde{z}_{\alpha_1,\ldots,\alpha_r},\ldots\}$ must be an integral basis of ν_L/ν_K. □

According to remark 4 this theorem can be applied if ν_K is factorial.

4. APPLICATIONS AND EXAMPLES

Some examples concerning algebraic function fields shall be mentioned. Let

(19)
k: field, $\varepsilon_n \in k$ (n-th primitive root of unity),
$\mathrm{char}(k) \nmid n$,
$\nu_K = k[X_1,\ldots,X_n]$ polynomial ring in n variables,
$K = \frac{\nu_K}{\nu_K}$ field of rational functions;

let

(19a) $$p = \{P_i = P_i(X_1,\ldots,X_n) \mid i \in I\}$$

be a system of irreducible polynomials of v_K (unique up to units) and

(19b) $$(v_i)_{i \in I},\ v_i = v_{P_i}$$

the family of corresponding valuations. Then

(19c) $$v_K = \bigcap_{i \in I} v_{v_i}$$

is a Krull domain and every Kummer extension L of exponent n has a distinguished generation. Therefore L has an integral basis over K, i.e.: *integral bases may exist over Krull domains which are not Dedekind domains.*

REMARK 1. The results of 4. can be applied also for Kummer extensions of L even if v_L is not a factorial ring; it is sufficient to assume that a Kummer extension L_1 of L has a distinguished generation. Thus, integral bases may exist for solvable extensions of the fields of quotients of Krull domains.

REMARK 2. A. Thome ([9], [9a]) has shown that some of the above mentioned results can be proved in the case of extensions with pure equations which are not of Kummer type. - Furthermore, it holds: If ν_K is a principal ideal domain which contains ε_p and p is a unit of ν_K (p ≥ 3 prime number) and L is a Kummer extension of exponent p and degree p^r (r > 1), then there exists an integral basis for $\tilde{L}/\tilde{K}$ for every $K \subset \tilde{K} \subset \tilde{L} \subseteq L$.

We give an illustration by the following example.

[5] Let $k = \mathbb{F}_7$ (field of 7 elements), $K = k(X)$ field of rational functions in X, $\nu_K = k[X]$. K contains the third roots of unity, therefore Kummer extensions of exponent p = 3 are possible. Consider $K_i = K(y_i)$, $y_i^3 = B_i$ (i = 1,2) where $B_1 = (X+1)(X-1)$, $B_2 = X^2+X$; $L = K(y_1,y_2)$ is a Kummer extension of exponent 3 of K. $1, y_i, y_i^2$ is integral basis of K_i/K (i = 1,2); these 5 elements together with $\tilde{z}_{11} = y_1y_2$, $\tilde{z}_{12} = y_1y_2^2 \cdot (X+1)^{-1}$, $\tilde{z}_{21} = y_1^2y_2(X+1)^{-1}$, $\tilde{z}_{22} = y_1^2y_2^2(X+1)^{-1}$ are an integral basis of L over K according to theorem IVa.
The results of Thome mentioned above guarantee that there also exists an integral basis of L over K_1, where $d_{L/K_1} \simeq X^2 \cdot \nu_{K_1}$ (by use of ramification arguments). Furthermore, the elements $\omega_1 = 1$,

$\omega_2 = y_2 \cdot \frac{X-1}{y_1} + y_2^2$ and $\omega_3 = y_2 + \frac{X-1}{y_1^2} \cdot y_2^2$ are integral over $v_{K_1} = v_K[1, y_1, y_1^2]$ and

$$d_{L/K_1}(\omega_1, \omega_2, \omega_3) = |Tr_{L/K_1}(\omega_\nu \omega_\mu)| =$$

$$= 3^3 \cdot B_2^2 \cdot \begin{vmatrix} 2 \cdot \frac{X-1}{y_1} & \frac{2X}{X+1} \\ \frac{2X}{X+1} & 2 \cdot \frac{X-1}{y_1^2} \end{vmatrix} =$$

$$= 3^3 \cdot B_2^2 \frac{(-4)}{(X+1)^2} = -4 \cdot 3^3 \cdot X^2 \cong d_{L/K_1} ;$$

therefore, $\{\omega_1, \omega_2, \omega_3\}$ is an integral basis of v_L / v_{K_1}.

This example can be generalized for the calculations of relative integral bases in Kummer extensions.

REMARK 3. Suppose

(20) $\quad \text{char}(K) \neq 2,\ [L:K] = 2^r,\ \exp(G(L/K)) = 2,$
$\quad K \subset \tilde{K} \subset \tilde{L} \subset L,$

i.e. Kummer extension of exponent 2. Then Schmal [8] showed: If $K = Q$ and $v_{\tilde{L}} / v_{\tilde{K}}$ has no integral basis, then

$[\tilde{L}:\tilde{K}] = 2$. - Thome [9], [9a] has shown: If 2 is invertible in v_K (for instance if $K = k(X)$ is a rational function field), then there exists an integral basis if $[\tilde{L}:\tilde{K}] \geq 4$.

We illustrate the situation by the following example for Kummer extensions of exponent 2 (biquadratic extensions) of function fields.

[6] Let $\mathrm{char}(k) \neq 2$, $K = k(X)$, $v_K = k[X]$; according to theorem IVa and (16b) a biquadratic extension of K can be given by

(20a) $\quad L = K(y_1,y_2)$, $K_i = K(y_i)$ and $y_i^2 = B_i$ $(i = 1,2)$,

where B_i are squarefree polynomials such that

(20b) $\quad B_i = B_{i,o} \cdot G$ $(i = 1,2)$ and $G = \gcd(B_1,B_2)$.

Then we have the integral bases and relative discriminants

(20c)
$$1, y_1, y_2, \frac{y_1 \cdot y_2}{G} \text{ for } L \text{ over } K, \; d_{L/K} \cong B_1^2 \cdot B_{2,o}^2,$$
$$1, y_1 \text{ for } K_1 \text{ over } K, \; d_{K_1/K} \cong B_1 \; .$$

Let $1,z = s+t\cdot y_2 \in \nu_L$ be a basis of L over K_1, then $d_{L/K_1}(1,z) = 4t^2\cdot B_2$. Because of (20c) for $t = x_o + \frac{x_1}{G}\cdot y_1$ and $e \in k^x$ unit in $k[X]$

$$e\cdot N_{K_1/K}(d_{L/K1}(1,z)) = e\cdot 4^2\cdot B_2^2\cdot N_{K_1/K}(t^2) =$$

$$= e\cdot 4^2\cdot B_2^2(x_o^2 - \frac{x_1^2}{G^2}\cdot B_1)^2 = \frac{B_1^2\cdot B_{2,0}^2}{B_1^2} = \frac{d_{L/K}}{d_{K_1/K}^2} = B_{2,0}^2$$

is equivalent to the property that 1,z is an integral basis for ν_L/ν_{K_1} (compare proposition 2a). Therefore, {1,z} is an integral basis iff

$$\text{(20d)} \qquad \tilde{e}\cdot(G\cdot x_o^2 - x_1^2\cdot B_{1,o})^2 = 1, \text{ i.e. } G\cdot x_o^2 - x_1^2\cdot B_{1,o} \cong 1 \in k, \quad \tilde{e} \in k^x,$$

is solvable for $x_o, x_1 \in k[X] = \nu_K$.

Let $\deg(B_1)$ and $\deg(G)$ denote the degrees of B_1 and G respectively (as polynomials of X). If $\deg(B_1) \not\equiv \deg(G) \mod 2$, then (20d) is not solvable. Therefore, we have infinitely many biquadratic extensions of K without an integral basis of ν_L/ν_K (remark that k is an arbitrary field of char(k) $\neq$ 2). This can be used to prove that certain ideals of K_1 cannot be principal ideals.

A. Thome [9] developed conditions for cyclic extensions of prime degree p to exclude the existence of a relative integral basis.

REFERENCES

[1] ARTIN, E., Questions de base minimale dans la théorie des nombres algébriques, *Colloque international du CNRS* 24, 19-20 (1950).

[2] BOURBAKI, N., Algebre commutative, Chap. 7., *Éléments de Mathématique* 31, Paris (1965).

[3] FRÖHLICH, A., The discriminant of relative Extensions and the Existence of Integral Bases, *Mathematika* 7, 15-22 (1960).

[4] HASSE, H., Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper, *J. reine angew. Math.* 172, 37-54 (1934).

[5] LAMPRECHT, E., Zyklische Erweiterungen arithmetischer Funktionenkörper. *Math. Z.* 77, 391-413 (1961).

[5a] LAMPRECHT, E., Zur Charakterisierung zyklischer Erweiterungen rationaler Funktionenkörper I, II, III., *J. reine angew. Math.* 209, 84-95 (1962); *Arch. Math.* 13, 488-497 (1962); *Arch. Math.* 14, 227-237 (1963).

[6] LANG, S., Algebra. New York, 1965.

[7] MANN, H.B., On integral Bases. *Proc. Amer. Math. Soc.* 9, 167-172 (1958).

[8] SCHMAL, B., Diskriminanten, Z-Ganzheitsbasen und relative Ganzheitsbasen bei multiquadratischen Zahlkörpern *Arch. Math.* 52, 245-257 (1989)

[9] THOME, A., Zur Existenz von Ganzheitsbasen bei endlichen separablen Erweiterungen von Dedekindringen. Diss. Saarbrücken, 1986.

[9a] THOME, A., Ganzheitsbasen bei Kummererweiterungen von Dedekindringen und zugehörigen Komposita *Arch.Math.* 51, 523-531 (1988).

[10] ZARISKI, O. and SAMUEL, P., Commutative Algebra II, Princeton, 1966.

LAMPRECHT, E.
Fachbereich 9 Mathematik,
Universität des Saarlandes,
D-6600 Saarbrücken

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

INTEGER-VALUED p-ADIC FUNCTIONS

LAOHAKOSOL, V.[1], LOXTON, J.H., VAN DER POORTEN, A.J.,

INTRODUCTION

A classical theorem of Polya [4] states that among all entire transcendental functions taking integer values at the non-negative integers, the one with least rate of growth is 2^z. There are many extensions of this theorem for entire functions of one or more complex variables taking algebraic values at certain algebraic points. The purpose of this note, however, is to investigate Polya's theorem in the p-adic setting where different problems arise because the functions are only defined locally.

Integer-valued p-adic analytic functions have been investigated by Hilliker and Straus [3] and theirs is the only result of this type that we have found in the literature. They prove a theorem valid in an arbitrary number

number field, but we state it here in the rational case to avoid introducing extra notation. Let p be a finite set of primes and suppose that, for each p in p, $f(z)$ is a p-adic analytic function in the disc $|z|_p \leq R_p$ with $R_p \geq 1$. Further, suppose that $f(n)$ is in $\mathbb{Q}$ for each positive integer n and that

$$\limsup_{n\to\infty} n^{-1} \log \max\{q_n, |f(n)|\} = \gamma_1 < \infty,$$

where q_n is the least common denominator of the numbers $f(1), f(2), \ldots, f(n)$. If

$$\prod_{p \text{ in } p} p^{1/(p-1)} R_p > 2e^{2\gamma_1},$$

then $f(z)$ is a polynomial. The proof relies on the fact that a p-adic function analytic over a domain containing the unit disc can be represented by a convergent Newton series interpolating the function at the positive integers. The hypotheses imply that, from a certain point on, the coefficients of the Newton series vanish and so the function must be a polynomial. Comparison with the classical theorem of Polya suggests that the growth restriction $\gamma_1 < \infty$, or something like it, is essential. Indeed, Hilliker and Straus give an example of an entire p-adic analytic function taking integer values at the positive integers and with $n^{-1}\log|f(n)| \to \infty$ but increasing more slowly than any prescribed rate.

In what follows, we investigate the significance of the condition on the p-adic radius of convergence in the theorem and obtain more precise results. We also show that, as in Polya's theorem, the transcendental functions which take integer values at the positive integers and have the least rate of growth are exponential polynomials. Similar ideas involving the characterisation of exponential polynomials are described in [7].

2. PRELIMINARIES

Throughout, $|\ |$ denotes the usual absolute value on $\mathbb{C}$ and $|\ |_p$ for a rational prime p denotes the p-adic valuation normalised by $|p|_p = p^{-1}$. We denote the completion of the algebraic closure of the p-adic rationals $\mathbb{Q}_p$ by $\mathbb{C}_p$.

Let K be an algebraic number field and set $d = [K:\mathbb{Q}]$. If $\mathfrak{p}$ is a prime ideal of K dividing the rational prime p, we denote by $|\ |_{\mathfrak{p}}$ the corresponding valuation on K which extends $|\ |_p$ and by $d_{\mathfrak{p}} = [K_{\mathfrak{p}}:\mathbb{Q}_p]$ the local degree of the respective completions of K and $\mathbb{Q}$. In this notation, the product formula takes the form

$$\prod_{\mathfrak{p}} |\alpha|_{\mathfrak{p}}^{d_{\mathfrak{p}}} = |N_{K/\mathbb{Q}}\alpha|^{-1}$$

for any non-zero α in K, with the product taken over all

the primes of K.

Let α be a non-zero element of K and let P(X) be the characteristic polynomial of the Q-linear map $\to \alpha x$ on K. If A_0 is the least common denominator of the coefficients of P(X), we can write

$$A_0 P(X) = A_0 X^d + A_1 X^{d-1} + \ldots + A_d = A_0 \prod_{j=1}^{d} (X - \alpha^{(j)}),$$

where $\alpha = \alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(d)}$ are the field conjugates of α and $A_0, A_1, \ldots, A_d$ are relatively prime integers. The absolute height of α is given by

$$h(\alpha) = (|A_0| \prod_{j=1}^{d} \max\{1, |\alpha^{(j)}|\})^{1/d}.$$

Note that $h(\alpha)$ is independent of the field in which we happen to work. We can give an alternative definition of $h(\alpha)$ by using the equations

$$|A_0| = \prod_p \max\{1, |\alpha|_p^{d_p}\}, \quad |A_d| = \prod_p \max\{1, |\alpha|_p^{-d_p}\},$$

which follow from properties of the Newton polygon of P(X). Taken together with the product formula, this shows that $h(\alpha^{-1}) = h(\alpha)$. (For further details on these matters, see [6, pages 205-214].) We record the following fundamental inequality.

LEMMA 1: Let α be a non-zero element of K and p be a finite set of primes of K. Then

$$\prod_{p \text{ in } p} |\alpha|_p^{d_p} \geq h(\alpha)^{-d}.$$

PROOF: From the preceding discussion,

$$h(\alpha)^d = h(\alpha^{-1})^d = |A_d| \prod_{j=1}^{d} \max\{1, |\alpha^{(j)}|^{-1}\} \geq \prod_{p \text{ in } p} |\alpha|_p^{-d_p}.$$

We also need to define heights on the projective space $P^N(K)$, in which we follow [6]. Let $\underset{\sim}{\xi} = (\alpha_0, \ldots, \alpha_N)$ be a point of $P^N(K)$. By working in a bigger field if necessary, we may choose the coordinates α_i to be relatively prime algebraic integers. Then the absolute height of $\underset{\sim}{\xi}$ is given by

$$h(\underset{\sim}{\xi}) = \left(\prod_{j=1}^{d} \max_{0 \leq i \leq N} |\alpha_i^{(j)}| \right)^{1/d}.$$

Alternatively, if $\underset{\sim}{\xi} = (\alpha_0, \ldots, \alpha_N)$ is represented by an arbitrary set of homogeneous coordinates in K, we see from the product formula that

$$h(\underset{\sim}{\xi}) = \left(A_0 \prod_{j=1}^{d} \max_{0 \leq i \leq N} |\alpha_i^{(j)}| \right)^{1/d}$$

with

$$A_0 = \prod_p \max_{0 \le i \le N} |\alpha_i|_p^{d_p}.$$

This formulation makes it clear that $h(\underset{\sim}{\xi})$ does not depend on the field in which we work nor on the choice of coordinates for the point $\underset{\sim}{\xi}$. We can take advantage of this invariance in the following way, familiar from the study of the Thue equation (See, for example, [2], pages 38-39.)

LEMMA 2: Suppose K has r conjugate real fields and s pairs of conjugate complex fields and that the conjugates are numbered so that, for α in K, $\alpha^{(1)},\ldots,\alpha^{(r)}$ are real and $\alpha^{(r+s+j)} = \overline{\alpha^{(r+j)}}$ $(1 \le j \le s)$. There is a constant C_K depending only on K with the following property. If $\beta_1,\ldots,\beta_d$ are non-zero numbers in K with $|\beta_{r+s+j}| = |\beta_{r+j}|$ $(1 \le j \le s)$, then there is a unit η in K such that

$$C_K^{-1}\left\{\prod_{j=1}^{d} |\beta_j|\right\}^{1/d} \le |\eta^{(i)}\beta_i| \le C_K\left\{\prod_{j=1}^{d} |\beta_j|\right\}^{1/d} \quad (1 \le i \le d).$$

In particular, for each $\underset{\sim}{\xi}$ in $P^N(K)$, we can find coordinates $(\alpha_0,\ldots,\alpha_N)$ for $\underset{\sim}{\xi}$ such that

$$C_K^{-1}h(\underset{\sim}{\xi}) \le \max_{0 \le j \le N} |\alpha_j^{(i)}| \le C_k h(\underset{\sim}{\xi}) \quad (1 \le i \le d).$$

PROOF: By Dirichlet's unit theorem, K has a fundamental set of units, $\eta_1,\ldots,\eta_{r+s-1}$, and each point in (r+s-1)-dimensional Euclidean space is within a distance c_0, say, of some point of the lattice with basis $(\log|\eta_j^{(2)}|,\ldots,\log|\eta_j^{(r+s)}|)$ $(1 \le j \le r+s-1)$, for some constant c_0 depending only on K. We deduce that there are rational integers $b_1,\ldots,b_{r+s-1}$ such that

$$\left|\sum_{j=1}^{r+s-1} b_j \log|\eta_j^{(i)}| - \sum_{j=1}^{d}\left\{\frac{1}{d} - \delta_{ij}\right\}\log|\beta_j|\right| \le c_0 \qquad (2 \le i \le r+s).$$

Since $|\beta_{r+s+j}| = |\beta_{r+j}|$, the inequality holds for $2 \le i \le d$. The remaining conjugate appears when we add the d-1 assertions obtained so far and we see that when $j = 1$, the expression on the left-side of the inequality is bounded by $c_0(d-1)$. Thus the unit $\eta = \eta_1^{b_1}\ldots\eta_{r+s-1}^{b_{r+s-1}}$ has the property required in the lemma.

For the final statement of the lemma, we first choose coordinates $\underset{\sim}{\xi} = (\alpha_0\ldots,\alpha_N)$ which are relatively prime algebraic integers, extending the field if necessary. The extension required depends only on K and not on N. We then apply the lemma with $\beta_i = \max_{0\le j\le N}|\alpha_j^{(i)}|$. This yields a unit η such that the coordinate representation

$\underset{\sim}{\xi} = (\eta\alpha_0, , , , .\eta\alpha_N)$ has the required property.

Next we develop a formula for the radius of convergence of a p-adic power series. This involves the forward differences defined by

$$\Delta f(z) = f(z+1) - f(z), \quad \Delta^n f(z) = \Delta(\Delta^{n-1} f(z)).$$

LEMMA 3: Let $f(z) = \sum_{n=0}^{\infty} a_n z^n$ be a power series with coefficients in C_p and radius of convergence $R \geq 1$. Then

$$\limsup_{n\to\infty} \left| \frac{\Delta^n f(0)}{n!} \right|_p^{1/n} = R^{-1}.$$

PROOF: First note that from a standard formula ([1], page 825),

$$\frac{\Delta^m f(0)}{m!} = \sum_{n=m}^{\infty} a_n S(n,m),$$

where the $S(n,m)$ are Stirling numbers of the second kind. The series converges in C_p because the $S(n,m)$ are integers and, by hypothesis, $|a_n|_p \to 0$ as $n \to \infty$. It follows that $|\Delta^m f(0)/m!|_p \to 0$ as $m \to \infty$ and that

$$\limsup_{m\to\infty} \left| \frac{\Delta^m f(0)}{m!} \right|_p^{1/m} \leq \limsup_{m\to\infty} |a_m|_p^{1/m} = R^{-1}.$$

On the other hand, by another standard formula ([1], page 824),

$$a_m = \sum_{n=m}^{\infty} \frac{\Delta^n f(0)}{n!}\, s(n,m),$$

where the $s(n,m)$ are Stirling numbers of the first kind. This series converges in C_p because the $s(n,m)$ are integers and $|\Delta^n f(0)/n!|_p \to 0$ as $n \to \infty$. Consequently,

$$R^{-1} = \limsup_{m\to\infty} |a_m|_p^{1/m} \leq \limsup_{m\to\infty} \left|\frac{\Delta^m f(0)}{m!}\right|_p^{1/m}$$

and the lemma is established.

An exponential polynomial is an expression of the shape

$$f(z) = \sum_{j=1}^{s} P_j(z)\alpha_j^z,$$

where the α_j are distinct non-zero numbers and the P_j are non-zero polynomials with P_j of degree $\nu_j - 1$, say. The order of the exponential polynomial is $\nu = \sum_{j=1}^{s} \nu_j$. The values of f at the non-negative integers satisfy a recurrence relation of order ν. In fact, if E is the translation defined by $Ef(z) = f(z+1)$, then

$$\prod_{j=1}^{s} (E - \alpha_j)^{\nu_j} f(z) = 0.$$

Such a sequence can be characterised by the vanishing of so-called Kronecker-Hankel determinants as follows. (See [5], page 5.)

LEMMA 4: Define the determinants $D_M = \det(f(i+j))_{0 \le i,j \le M}$ Then $D_M = 0$ for $M \ge M_0$ if and only if the numbers $f(n)$ for $n = 0,1,2,\ldots$ are the values of an exponential polynomial $f(z)$ of order at most M_0.

So far, these remarks only involve the values of the exponential polynomial $f(z)$ at the non-negative integers, where the definition of α^z is obvious. As usual, we can interpolate these values by $\alpha^z = e^{z \log \alpha}$. This gives a p-adic analytic function convergent in the disc $|z|_p < R$ if and only if $|\alpha - 1|_p < p^{-1/(p-1)} R^{-1}$.

3. THE MAIN THEOREM

THEOREM. *Let* K *be an algebraic number field of degree* d. *Let* p *be a finite set of primes of* K *and, for each* p *in* p, *let* $\mathfrak{p}$ $(= \mathfrak{p}_p)$ *be the rational prime divisible by* p *and* $d_p = [K_p : \mathbb{Q}_p]$ *be the local degree. Suppose that for each* p *in* p, $f(z)$ *is a* p*-adic analytic function in the* disc $|z|_p \le R_p$ with $R_p \ge 1$. *Further suppose that* $f(n)$ *is in* K *for every non-negative integer* n *and that*

$$\limsup_{n\to\infty} n^{-1}\log h\,(f(0)),f(1),\ldots,f(n)) = \gamma < \infty.$$

(i) If $\prod_{p \text{ in } p} (p^{1/(p-1)} R_p)^{d_p} > e^{\gamma d}$,

then f is an exponential polinomial.

(ii) If $\prod_{p \text{ in } p} (p^{1/(p-1)} R_p)^{d_p} \geq (2e^{\gamma})^d$,

then f is a polynomial.

PROOF: (i) Take $\varepsilon > 0$ and let M be a sufficiently large positive integer to be specified later. Since the data is not affected by multiplying f by a non-zero element of K, we can suppose that the numbers $f(0),f(1),\ldots,f(2M)$ are algebraic integers. If $\xi(n) = (f(0),f(1),\ldots,f(n))$, then

$$h(\underset{\sim}{\xi}(n)) \leq c_1\, e^{n(\gamma+\varepsilon)},$$

where $c_1 = c_1(\varepsilon)$ is independent of n.

Consider the Kronecker-Hankel determinant $D_M = \det(f(m+n))_{0\leq m,n\leq M}$. We will show that $D_M = 0$ if M is sufficiently large; this conclusion also is unaffected by the preliminary normalisation. For each conjugate, we have the estimate

$$|D_M^{(i)}| \le (M+1)!\ \max\ |f(0+n_0)f(1+n_1)\dots f(M+n_M))^{(i)}|,$$

where the maximum is taken over all permutations $\{n_0,\dots,n_M\}$ of $\{0,\dots,M\}$. Let $\{n_0^{(i)},\dots,n_M^{(i)}\}$ be a permutation where this maximum is attained. By lemma 2, we can find units $\eta_0,\dots,\eta_M$ in K such that

$$|(\eta_m f(m+n_m^{(i)}))^{(i)}| \le c_K\left(\prod_{j=1}^{d}|f(m+n_m^{(i)})^{(j)}|\right)^{1/d}$$

$$\le c_K h(\underset{\sim}{\xi}(m+n_m^{(i)})) \le c_K c_1 e^{(m+n_m^{(i)})(\gamma+\varepsilon)}$$

for $1 \le i \le d$. We can now obtain $\eta_0\dots\eta_M D_M$ by multiplying the m-th row of the determinant by η_m and we have the estimate

$$|(\eta_0\dots\eta_M D_M)^{(i)}| \le (M+1)!(c_K c_1)^{M+1}\prod_{m=0}^{M} e^{(m+n_m^{(i)})(\gamma+\varepsilon)}$$

$$= (M+1)!(c_K c_1)^{M+1} e^{M(M+1)(\gamma+\varepsilon)}$$

because $\{n_0^{(i)},\dots,n_M^{(i)}\}$ is a permutation of $\{0,\dots,M\}$.

Thus

$$|N_{K/\mathbb{Q}}D_M| = \prod_{i=1}^{d} |(\eta_0 \ldots \eta_M D_M)^{(i)}| \leq$$

$$\leq (M+1)!^d (c_K c_1)^{d(M+1)} e^{dM(M+1)(\gamma+\varepsilon)}.$$

On the other hand, by adding rows and columns of D_M appropriately, we also have $D_M = \det(\Delta^{m+n} f(0))_{0 \leq m,n \leq M}$. By lemma 3,

$$|\Delta^n f(0)| \leq c_2 |n!|_p (R_p^{-1}+\varepsilon)^m \leq c_2 n p^{1-n/(p-1)} (R_p^{-1}+\varepsilon)^n$$

where $c_2 = c_2(\varepsilon)$ is independent of n. This gives

$$|D_M|_p \leq c_2^{M+1} (2M)! p^{M+1-M(M+1)/(p-1)} (R_p^{-1}+\varepsilon)^{M(M+1)}.$$

Suppose $D_M \neq 0$. Since D_M is an algebraic integer, the product formula of section 2 yields

$$\prod_{p \text{ in } p} |D_M|_p^{d_p} \geq |N_{K/\mathbb{Q}}D_M|^{-1}.$$

If we now use our estimates for $N_{K/\mathbb{Q}}D_M$ and $|D_M|_p$ and take the $M(M+1)$-th root, we obtain

$$\prod_{p \text{ in } p} (p^{1/(p-1)}(R_p + \varepsilon))^{d_p} \leq (1+\varepsilon)e^{d(\gamma+\varepsilon)},$$

whenever $M \geq M_0(\varepsilon)$. This contradicts the hypothesis of the theorem if ε is taken sufficiently small. Consequently, we must have $D_M = 0$ for all sufficiently large M.

By lemma 4, $f(z)$ takes the same values on the non-negative integers as an exponential polynomial, $g(z)$ say. Now $\Delta^k g(0) = \Delta^k f(0)$, so by lemma 3, $g(z)$ is analytic on the disc $|z|_p \leq R_p$ for each p in p and $g^{(k)}(0) = f^{(k)}(0)$ for each k. Thus $f(z)$ is identically equal to $g(z)$.

(ii) After (i), we can take f to be an exponential polynomial of order ν, say

$$f(z) = \sum_{j=1}^{s} P_j(z)\alpha_j^z.$$

The α_j and the coefficients of the polynomials P_j are determined by $f(0), f(1), \ldots, f(\nu-1)$, so we can suppose that they lie in K, after making a finite extension of K if necessary. Denote the degree of P_j by $\nu_j - 1$. If E is the translation defined in section 2, we have

$$(E - \alpha_1)^{\nu_1} \ldots (E - \alpha_{s-1})^{\nu_{s-1}} (E - \alpha_s)^{\nu_s - 1} f(z) = c_3 \alpha_s^z,$$

where c_3 is a non-zero constant in K. On expanding the left-hand side, we obtain

$$\alpha_s^z = \sum_{j=0}^{\nu-1} a_j f(z+j),$$

where the a_j are constants in K. We use this first to estimate the size of α_s^n at each valuation of K and for positive integers n, giving

$$|(\alpha_s^n)^{(i)}| \leq c_4 \max_{0\leq j\leq \nu-1} |f(n+j)^{(i)}|,$$

$$|\alpha_s^n|_p \leq c_p \max_{0\leq j\leq \nu-1} |f(n+j)|_p,$$

where c_4 and c_p are constants independent of n and $c_p = 1$ for all but a finite number of primes p. Since we may assume $f(0) = 1$, we have

$$h(\alpha_s)^n = h(\alpha_s^n) \leq c_5\, h(f(0),\ldots,f(n+\nu-1)),$$

with c_5 independent of n. Taking the n-th root and letting $n \to \infty$ gives

$$h(\alpha_s) \leq e^{\gamma}.$$

Next, since $f(z)$ is analytic in the disc $|z|_p \le R_p$ for each p in p, so is α_s^z. By hypothesis, $R_p \ge 1$, so

$$|\alpha_s - 1|_p = |\log \alpha_s|_p < (p^{1/(p-1)} R_p)^{-1}$$

for each p in p. But $h(\alpha_s - 1) \le 2h(\alpha_s)$. If $\alpha_s \ne 1$, lemma 1 and the preceding estimates yield

$$\prod_{p \text{ in } p} (p^{1/(p-1)} R_p)^{d_p} < (2e^{\gamma})^d,$$

contrary to the hypothesis of the theorem. So $\alpha_s = 1$ and similarly, all $\alpha_j = 1$, that is f is a polynomial.

4. REMARKS

I. The theorem implies the result of Hilliker and Straus [3]. With the notation of the theorem, define

$$\gamma_1 = \limsup_{n \to \infty} n^{-1} \log\{\max q_n, |\overline{f(n)}|\},$$

where q_n is a positive integer making each $q_n f(j)$ an algenraic integer for $0 \le j \le n$ and $|\overline{f(n)}|$ denotes the maximum of the absolute values of the conjugates of $f(n)$. Given $\varepsilon > 0$, there is a constant c_6 such that

$$\max\{q_n, |\overline{f(n)}|\} < c_6 \, e^{n(\gamma_1 + \varepsilon)}$$

for all $n \geq 0$. Thus

$$h(f(0),\ldots,f(n)) = h(q_n f(0),\ldots,q_n f(n)) \leq$$

$$\leq \max_{0\leq j\leq n}\{q, |\overline{f(j)}|\} < c_6 e^{2n(\gamma_1+\varepsilon)}$$

and

$$\gamma = \limsup_{n\to\infty} n^{-1}\log h(f(0),\ldots,f(n)) \leq 2\gamma_1.$$

Assume $\gamma_1 < \infty$. The following two assertions are now immediate from the theorem.

(i) If $\prod_{p \text{ in } \mathcal{P}} (p^{1/(p-1)} R_p)^{d_p} > e^{2\gamma_1 d}$

then f is an exponential polynomial.

(ii) If $\prod_{p \text{ in } \mathcal{P}} (p^{1/(p-1)} R_p)^{d_p} > (2e^{2\gamma_1 d})$

then f is a polynomial.

The second of these is the theorem of Hilliker and Straus. Our theorem using the correct height, is usually much sharper than this, and only reduces to (ii) above in extreme circumstances.

II. The determination between polynomials and exponential polynomials in the theorem is sharp. Take, for example, $K = \mathbb{Q}$ and let $p = 2q-1$ be an odd prime. If

$f(z) = (1-p/q)^z$, then we find $h(f(0),\ldots,f(n)) = q^n$ and $f(z)$ is analytic in the $\mathrm{disc}|z|_p < p^{1-1/(p-1)}$. In the notation of the theorem, $(2e^\gamma)^d = 2q = p+1$ and we can take $p^{1/(p-1)}R_p = p-\varepsilon$ for any $\varepsilon > 0$, so we cannot replace the 2 in part (ii) of the theorem by any smaller constant.

Again, if $K = \mathbb{Q}((1-p/q)^{1/d})$ and $f(z) = (1-p/q)^{z/d}$, with $p = 2q-1$ as before, and $p \nmid d$, then $h(f(0),\ldots,f(n)) = q^{n/d}$ and so $e^{\gamma d}$ and $p^{1/(p-1)}R_p$ have the same values as before and $p^{1/(p-1)}R_p \approx 2e^{\gamma d}$. The appearance of d in part (ii) of the theorem is therefore also essential. (In this example, $(1-p/q)^{1/d}$ is in $\mathbb{Q}_p$, so $d_p = 1$.)

The following less explicit example shows that, in fact, the 2^d of the theorem cannot be replaced by any smaller constant. Let $p = 2^d q-1$ be a prime and choose a polynomial $P(x) = qx^d + \ldots + p$ which is irreducible over $\mathbb{Q}$, splits completely over $\mathbb{Q}_p$ and has all its complex roots near -2. There is just one root, β say, in $\mathbb{Q}_p$ with $|\beta|_p < 1$. Put $f(z) = (1+\beta)^z$. Then $h(f(0),\ldots,f(n)) \approx q^{n/d}$ and $f(z)$ is analytic in the $\mathrm{disc}|z_p| < R_p$ with $R_p = p^{1-1/(p-1)}$. In the notation of theorem, $p^{1/(p-1)}R_p \approx (2e^\gamma)^d$ for this example.

It is, of course, essential that the height used to

measure the rate of growth of the sequence f(n) should take account of the common denominators of $f(0),\ldots,f(n)$. The example $f(z) = (1-p^k z)^{-1}$ shows that we cannot replace $h(f(0),\ldots,f(n))$ by $h(f(n))$ in the definition of γ in the theorem. (For this example, $\limsup_{n\to 0} n^{-1} \log h(f(n)) = 0$ and we can take $R_p = p^{k-\varepsilon}$ for any $\varepsilon > 0$.)

As for part (i) of the theorem, consider the following construction. Let $p_1 = 2$, $p_2 = 3,\ldots$ be the sequence of primes with the prime p omitted and define the sequence u_n by $u_{n^2} = p_n$ and $u_m = 1$ when m is not a square. Set $f(n) = v_n/u_n$, where the integers v_n are chosen successively so that f(n) has denominator u_n in its lowest terms and $\Delta^n f(0) \equiv 0 \bmod p^n$. This can be done with $0 < v_n < 2p^n$. Finally, construct f(z) by interpolating the values f(n) as implied in lemma 3. The resulting function is analytic in $|z_p| \le R_p$ for any $R_p < p^{1-1/(p-1)}$ by lemma 3. Also $h(f(0),\ldots,f(n)) < 2p^n u_n$, so in the notation of the theorem $e^{\gamma} = p$. Thus f just fails to meet the condition in part (i) of the theorem. Clearly, f is not an exponential polynomial because infinitely many primes appear in the denominators of the numbers f(n).

III. It is much easier to prove results about functions whose derivatives at a fixed point are all algebraic. Thus, let K be an algebraic number field of degree d and let p be a finite set of primes of K. Suppose that, for each p in p, $f(z)$ is a p-adic analytic function in the disc $|z|_p \leq R_p$ with $R_p > 0$. Further suppose that $f^{(n)}(0)$ is in K for every non-negative integer n and that

$$\limsup_{n\to\infty} n^{-1} \log h(f^{(n)}(0)) = \gamma_2 < \infty.$$

If

$$\prod_{p \text{ in } p} (p^{1/(p-1)} R_p)^{d_p} > e^{\gamma_2 d},$$

then f is a polynomial. To see this, we need only observe that $|\limsup f^{(n)}(0)/n!|_p^{1/m} = R_p^{-1}$ and use lemma 1 to see that $f^{(n)}(0) = 0$ for all sufficiently large n. The example $f(z) = e^z$ shows that the results is best possible.

REFERENCES

[1] ABRAMOWITZ, M., and STEGUN, A., *Handbook of mathematical functions*. (Dover, 1965).

[2] BAKER, A., *Transcendental number theory*, (Cambridge, 1975).

[3] HILLIKER, D.L. and STRAUS, E.G., Some p-adic versions of Polya's theorem on integer-valued analytic functions. *Proc. Amer. Math. Soc.* 26 (1970), 395-400.

[4] POLYA, G., Über ganzwertige ganze Funktionen. *Rend. Circ. Math. Palermo* 40 (1915), 1-16. (=Collected works, Vol.1. (MIT Press, 1974), 1-16.)

[5] SALEM, R., *Algebraic numbers and Fourier analysis.* (Heath, 1963).

[6] SILVERMAN, J.H., *The arithmetic of elliptic curves.* (Springer, 1986), p. 205-14.

[7] VAN DER POORTEN, A.J., p-adic methods in the study of Taylor coefficients of rational functions. *Bull. Austral. Math. Soc.* 29 (1984), 109-117.

LAOHAKOSOL, V.[1]

[1] This work was completed while the first author was visiting Macquaire University whose support and hospitality are acknowledged.

Department of Mathematics,
Kasetsart University,
Bangkok 10900, T h a i l a n d

LOXTON, J.H.

VAN DER POORTEN, A.J.

School of Mathematics, Physics,
Computing and Electronics,
Macquarie University,
M.S.W. 2109, A u s t r a l i a

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

NORMAL BASES OF UNITS

LORENZ F.

1.

In a previous paper (cf. [1]) we have investigated which normal number fields possess a normal basis consisting of units. These investigations shall now be extended to the relatively normal case. Hereby we hope also to mend some small but irritating deficiences in the presentation of our paper mentioned above.

Our main result will be the following:

THEOREM 1: *A normal extension* K/k *of algebraic number fields possesses a normal basis consisting of units if and only if* K/k *is* <u>not</u> *of the following 'exceptional type':*

(a) K *is imaginary*

(b) k *is real*

(c) *Every unit of* K *is either real or purely imaginary.*

Here and in what follows an algebraic number field K is considered as a *fixed subfield* of the field $\mathbf{C}$ of complex numbers (and we always assume $K/\mathbf{Q}$ to be a *finite* extension). Let then

$$K_0 := K \cap \mathbf{R} \tag{1}$$

be the maximal real subfield of K. If $K \neq K_0$ we say that K is *imaginary*; if $K = K_0$ we call K *real*.

2.

Now let k be a subfield of the algebraic number field K and assume the extension K/k to be *normal* with Galois group $G = \mathrm{Gal}(K/k)$. We denote by

$$\rho : z \mapsto \bar{z} \tag{2}$$

the complex conjugation automorphism of $\mathbf{C}$. The automorphism ρ induces an isomorphism

$$\rho_K : K \mapsto \rho K. \tag{3}$$

We have either $\rho_K \notin G$ or $\rho_K \in G$. The latter case occurs if and only if k is real (and therefore K is

mapped into itself, since K/k is normal).

The proof of Theorem 1 is based on the following

LEMMA 1: *Let* K/k *be a normal extension of algebraic number fields with Galoisgroup* G. *Let* ε *be an element of* K *satisfying*

(4) $|\varepsilon| \geq 1$ *and* $|\varphi\varepsilon| < 1$ *for every* $\varphi \in G \setminus \{id_K, \rho_K\}$.

In case $\rho_K \in G$ *and* $\rho_K \neq id_K$ *we assume furthermore*

(5) $\bar{\varepsilon} \neq \pm\varepsilon$, *i.e.* ε *is neither real nor purely imaginary.*

Under these conditions there exist infinitely many natural numbers n *such that*

$$(6) \qquad \det((\sigma^{-1}\tau\varepsilon^n)_{\sigma,\tau\in G}) \neq 0.$$

PROOF: Let d denote the degree of K/k, so d = G:1. For every $n \in \mathbb{N}$ we consider the d × d-matrix

$$(7) \qquad A_n = \varepsilon^{-n}(\sigma^{-1}\tau\varepsilon^n)_{\sigma,\tau\in G}.$$

It suffices to show that

$$(8) \qquad \det(A_n) \neq 0 \quad \text{for infinitely many } n.$$

Note that the diagonal coefficients of A_n are all equal to 1.

1) We consider now first the case

(9) $\rho_K \notin G$ or $\rho_K = id_K$.

For $\sigma \neq \tau$ and $|\varepsilon| \geq 1$ we have

(10) $|\varepsilon^{-n}\sigma^{-1}\tau(\varepsilon^n)| \leq |\sigma^{-1}\tau(\varepsilon)|^n$.

Therefore by condition (4) the sequence of the matrices A_n converges in case (9) to the $d \times d$-unit matrix:

(11) $$A_n \to \begin{pmatrix} 1 & & 0 \\ & 1 & \\ & \ddots & \\ 0 & & 1 \end{pmatrix} = E_d \quad \text{for} \quad n \to \infty.$$

In particular $\det(A_n) \neq 0$ for sufficiently large n.

2) Now suppose that

(12) $\rho_K \in G$ and $\rho_K \neq id_K$,

i.e. ρ induces a non-trivial automorphism of K/k, which for brevity we shall denote here also by ρ. Let $\sigma_1,\ldots,\sigma_r$ be a system of representatives for the left cosets of G modulo the subgroup $\langle\rho\rangle$ generated by ρ. Then if we write down the elements of G in the following order

(13) $$\sigma_1, \sigma_1\rho, \sigma_2, \sigma_2\rho, \ldots, \sigma_r, \sigma_r\rho,$$

the matrix $A = A_n$ will have the form

(14) $$A = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1r} \\ A_{21} & A_{22} & \cdots & A_{2r} \\ \vdots & & & \vdots \\ A_{r1} & A_{r2} & \cdots & A_{rr} \end{pmatrix}$$

with the 2×2-matrices

(15) $$A_{ij} = \varepsilon^{-n} \begin{pmatrix} \sigma_i^{-1}\sigma_j(\varepsilon^n) & \sigma_i^{-1}(\sigma_j\rho)(\varepsilon^n) \\ (\sigma_i\rho)^{-1}\sigma_j(\varepsilon^n) & (\sigma_i\rho)^{-1}\sigma_j\rho(\varepsilon^n) \end{pmatrix}$$

(which also depend on n). For $i = j$ we have

(16) $$A_{ij} = \begin{pmatrix} 1 & \rho(\varepsilon^n)\varepsilon^{-n} \\ \rho(\varepsilon^n)\varepsilon^{-n} & 1 \end{pmatrix}$$

So if ε has the polar decomposition

(17) $$\varepsilon = re^{it},$$

then we obtain

$$A_{ii} = \begin{pmatrix} 1 & e^{-2int} \\ e^{-2int} & 1 \end{pmatrix} . \tag{18}$$

For $i \neq j$ none of the automorphisms $\sigma_i^{-1}\sigma_j$, $\sigma_i^{-1}\sigma_j\rho$, $\rho\sigma_i^{-1}\sigma_j$, $\rho\sigma_i^{-1}\sigma_j\rho$ occuring in (15) can be equal to either id or ρ. Therefore it follows from condition (4) of the lemma that A_{ij} converges to zero if n tends to infinity:

$$A_{ij} \to \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{for} \quad i \neq j. \tag{19}$$

In order to prove our assertion (8) we observe that the sequence $(e^{int})_n$ certainly contains a convergent subsequence $(e^{in(k)t})_k$. Then the corresponding subsequence $(\det(A_{n(k)})_k$ of $(\det(A_n))_n$ converges to the number

$$(1-z_0^{-4})^r, \quad \text{where} \quad z_0 = \lim_{k\to\infty} e^{in(k)t}, \tag{20}$$

cf. (14), (19) and (18). If $z_0^4 \neq 1$ we are done with the proof since then it follows

$$\det(A_{n(k)}) \neq 0 \tag{21}$$

for all sufficiently large k. If $z_0^4 = 1$ we consider the subsequence

$$(22) \qquad (e^{i(n(k)+1)t})_k.$$

It converges to $z_1 := z_0 e^{it}$ and we now have

$$(23) \qquad z_1^4 = z_0^4 e^{4it} = e^{4it}.$$

But $e^{4it} \neq 1$ since otherwise by (17) we would obtain $\bar{\varepsilon}\varepsilon^{-1} = e^{-2it} = \pm 1$, contradicting our hypothesis (5).

3.

We are now going to prove Theorem 1. So let K/k be a normal extension of algebraic number fields with Galois group G. Let's first depose of the (trivial) necessity part of Theorem 1. If K/k is of exceptional type (as defined in Theorem 1) then $\rho_K \in G \setminus \{id_K\}$ and for every unit ε of K we have $\rho_K \varepsilon = \pm\varepsilon$. Hence for any unit ε of K the system

$$(24) \qquad (\sigma\varepsilon)_{\sigma\in G}$$

is linearly dependent over k and for that reason K/k cannot have a normal basis consisting of units.

Now we shall prove the sufficiency part of Theorem 1. It is well known that there exists a *unit* ε in K for which the condition (4) of lemma 1 is satisfied (cf. [2], page 524). Now, if

$$\rho_K \notin G \quad \text{or} \quad \rho_K = \mathrm{id}_K, \tag{25}$$

by Lemma 1 there exists a natural number n such that for $\alpha := \varepsilon^n$ we have

$$\det((\sigma^{-1}\tau(\alpha))_{\sigma,\tau\in G}) \neq 0. \tag{26}$$

But then it easily follows that the system

$$(\tau\alpha)_{\tau\in G} \tag{27}$$

is linearly independent over k and thus we obtain a normal basis of K/k consisting of units.
So we are left with the case

$$\rho_K \in G \quad \text{and} \quad \rho_K \neq \mathrm{id}_K \tag{28}$$

where ρ induces a non-trivial automorphism of K/k. Then k must be *real* and K *imaginary*. Therefore, if K/k is *not* of 'exceptional type' then K must contain a unit η with

$$\bar{\eta} \neq \pm\eta. \tag{29}$$

We may as well suppose $|\eta| \geq 1$ (otherwise replace η by η^{-1}). Now, if already $\bar{\varepsilon} \neq \pm\varepsilon$ then both conditions (4) and (5) of Lemma 1 are satisfied; thus again for a certain power $\alpha = \varepsilon^n$ of ε, (26) holds and therefore (27) is a normal basis of units for K/k. So assume $\bar{\varepsilon} = \pm\varepsilon$. Then we consider units of the form

$$\varepsilon_m = \varepsilon^m\eta \quad \text{with} \quad m \in \mathbf{N} \tag{30}$$

in K. For them we certainly have $\bar{\varepsilon}_m \neq \pm\varepsilon_m$ by (29). Hence if m is sufficiently large we can apply Lemma 1 to ε_m (instead of our original ε) and again we obtain a normal basis of units for K/k.

4.

We want to give other characterizations of the normal extensions of algebraic number fields which have a normal basis consisting of units. In view of Theorem 1 we may restrict ourself to the case that the groundfield is *real*. For any algebraic number field K we denote by E_K the group of its units and by W_K the group of its roots of unity. We call K *totally real* if all its isomorphic images in $\mathbf{C}$ lie in $\mathbf{R}$ and *totally imaginary* if none of its isomorphic images in $\mathbf{C}$ are

contained in R.

DEFINITION 1: We call an algebraic number field K a 2-*restricted* CM-*field* if the following conditions are satisfied:

(α) K is a CM-*field*, i.e. K is totally imaginary, $K_0 = K \cap R$ is totally real and $[K:K_0] = 2$ (cf. [4]).

(β) The order of W_K is a divisor of 4; i.e. $W_K \subseteq \langle i \rangle$.

(γ) If $W_K = \langle i \rangle$ then $E_K = W_K E_{K_0}$ (i.e. $Q = 1$, where Q denotes the *Hasse unit index* of K, cf. [3]).

To begin with, one has the following characterizations of the imaginary number fields with only real or purely imaginary units:

THEOREM 2 (cf. [1]): *Let* K *be an* imaginary *algebraic number field. Then the following statements are equivalent:*

(i) $E_K \subseteq R \cup i R$

(ii) $K \neq Q(E_K^2)$

(iii) $K \neq Q(\varepsilon^2)$ *for every* $\varepsilon \in E_K$

(iv) K *is a* 2-*restricted* CM-*field* (cf. the preceding Definition 1).

For the convenience of the reader we restate here our proof of Theorem 2 given in [1]:

(i) => (ii): If $E_K \subsetneq \mathbf{R} \cup i\mathbf{R}$ then $E_k^2 = \{\varepsilon^2 | \varepsilon \in E_K\}$ is contained in $\mathbf{R}$, thus $\mathbf{Q}(E_K^2) \subseteq K_0 \neq K$.

(ii) => (iii): trivial.

(iii) => (iv): Let T be the set of all subfields L of K with $L \neq K$. Then the hypothesis implies

$$E_K^2 \subseteq \bigcup_{L \in T} E_L. \tag{31}$$

By tensoring with $\mathbf{Q}$ over $\mathbf{Z}$ it follows

$$E_K \otimes \mathbf{Q} = \bigcup_{L \in T} E_L \otimes \mathbf{Q}. \tag{32}$$

But a finite dimensional vectorspace (over a non finite field) cannot be a finite union of proper subspaces, hence there is a $L \in T$ such that

$$E_K \otimes \mathbf{Q} = E_L \otimes \mathbf{Q}. \tag{33}$$

Now, by *Dirichlet's unit theorem* one easily derives from (33) that L is totally real, K totally imaginary and $[K:L] = 2$. In particular $L = K_0$. So we already know that K is a CM-*field*. Assuming that one of the properties (β) or (γ) of a 2-*restricted* CM-*field* is violated for K,

we are going to construct an unit ε of K satisfying the following three conditions:

(34) $|\varepsilon| \geq 1$

(35) $|\sigma\varepsilon| < 1$ for all embeddings $\sigma : K \to \mathbf{C}$ except the inclusion and the complex conjugation map

(36) $\varepsilon^2 \notin K_0$.

Then ε^2 will have $[K:\mathbf{Q}]$ different conjugates. But then $K = \mathbf{Q}(\varepsilon^2)$, contradicting our hypothesis (iii).

First we choose an unit ε_0 in K_0 satisfying the conditions

(37) $|\varepsilon_0| > 1$

(38) $|\sigma_0\varepsilon_0| < 1$ for all embeddings $\sigma_0 : K_0 \to \mathbf{R}$ except the inclusion map.

It is well known that such an unit ε_0 in K_0 does exist (see again [2], page 524; note that $K_0 \neq \mathbf{Q}$ in the case we consider).

Now, if (β) is violated, i.e. if K contains a root ζ of unity with $\zeta^4 \neq 1$, then the unit $\varepsilon := \zeta\varepsilon_0$ of K satisfies all of the conditions (34), (35), (36).

Finally let us assume that property (γ) is violated,

i.e.

(39) $$W_K = \langle i \rangle \quad \text{and} \quad E_K \neq W_K E_{K_0}.$$

For any CM-field K the endomorphism $1-\rho\colon x \mapsto x/\rho x$ of E_K has image in W_K (a wellknown fact, cf. [4]); so it induces Kummer's exact sequence

(40) $$1 \to W_K E_{K_0} \to E_K \xrightarrow{1-\rho} W_K/W_K^2.$$

Hence (39) implies that there exists an unit $\eta \in E_K$ with $\eta/\bar{\eta} = i$, i.e. $\eta^2 \notin K_0$. It follows that every unit of the form

(41) $$\varepsilon := \varepsilon_0^n \eta$$

satisfies condition (36). But if we choose n sufficiently large then ε will satisfy conditions (34) and (35) as well (since ε_0 satisfies (37) and (38)).

(iv) => (i): So assume that K is a 2-*restricted* CM-*field*. Then by looking at the exact sequence (40) we see that for every $\varepsilon \in E_K$ we have $\varepsilon/\bar{\varepsilon} = \pm 1$. It follows $E_K \subseteq R \cup iR$, i.e. (i).

LEMMA 2: *If an algebraic number field* K *is real then for each* $n \in \mathbb{N}$ *there exists an unit* ε *of* K *such that* $K = \mathbb{Q}(\varepsilon^n)$.

PROOF: We know (cf. [2], page 524) that there exists an unit $\varepsilon \in E_K$ such that $|\varepsilon| \geq 1$ and $|\sigma\varepsilon| < 1$ for all embeddings $\sigma: K \to \mathbf{Q}$ which are different from the inclusion map. The same then holds for ε^n as well. From this we easily conclude that ε^n has $[K:\mathbf{Q}]$ different conjugates. It follows $K = \mathbf{Q}(\varepsilon^n)$.

THEOREM 3: *Let* K/k *be a normal extension of algebraic number fields, and suppose* k *to be real. Then the following statements are equivalent:*

(i) K/k *has a normal basis consisting of units*

(ii) $K = \mathbf{Q}(E_K^2)$

(iii) *There is an* $\varepsilon \in E_K$ *such that* $K = \mathbf{Q}(\varepsilon^2)$

(iv) K *is not a 2-restricted* CM-*field* (cf. Def. 1 above)

(v) *There is an* $\varepsilon \in E_K$ *such that* $K = k(\varepsilon^2)$

(vi) $K = k(E_K^2)$.

PROOF: 1) First we consider the case that K is real. Then all six statements turn out to be true. For (i) this follows by Theorem 1. For (ii), (iii), (v), (vi) it follows by Lemma 2, and for (iv) it is trivial.

2) Now suppose K is imaginary.

(vi) => (i): Assume (i) to be false. Then by Theorem 1 we must have $E_K \subseteq \mathbf{R} \cup i\mathbf{R}$ and consequently $E_K^2 \subseteq K_0$.

It follows

$$k(E_K^2) \subseteq K_0 \neq K \tag{42}$$

and so (vi) does not hold.

(i) => (ii): Suppose (i) holds. Then by Theorem 1 (and our assumptions) we have $E_K \notin \mathbf{R} \cup i\mathbf{R}$. Applying Theorem 2 we get $K = \mathbf{Q}(W_K^2)$, i.e. (ii).
All the rest follows immediately by Theorem 2.

5.

Finally we want to generalize Theorem 2 (and Lemma 2) in the following sense: Given an algebraic number field K and a natural number n. When does there exist an unit ε of K such that $K = \mathbf{Q}(\varepsilon^n)$? The answer to this question given without proof in [1] is not quite correct. This was noticed by S. Krüger, a student of mine, while she was working at her Diplomarbeit in 1986.

We first generalize the notion of a 2-restricted CM-field, in a suitable way, to that of a n-restricted CM-field:

DEFINITION 2: Let K be an algebraic number field and let n be a natural number. We call K a n-*restricted* CM-*field* if the following conditions are

satisfied:

(α) K is a CM-field

(β) The order of W_K is a divisor of 2n

(γ) If $W_K^n \neq 1$ then $E_K = W_K E_{K_0}$

THEOREM 4: *Let* K *be an arbitrary algebraic number field. Then for a given natural number* n *the following two statements are equivalent:*

(i) *There is an unit* ε *of* K *such that* $K = \mathbf{Q}(\varepsilon^n)$.

(ii) K *is not a* n*-restricted* CM*-field* (cf. the preceding Definition 2).

PROOF: (i) => (ii): We assume that K *is* a n-restricted CM-field. In particular, K is a CM-field and so the sequence in (40) is well defined and exact. For any $\varepsilon \in E_K$ we know that $\varepsilon/\bar{\varepsilon}$ is a root of unity in K. In case $W_K^n = 1$ it follows $\varepsilon^n = \bar{\varepsilon}^{-n}$, i.e. ε^n is real, and so for every unit ε of K we have $\mathbf{Q}(\varepsilon^n) \subseteq K_0 \neq K$, contradicting (i).

Therefore we may suppose $W_K^n \neq 1$. By property (γ) of a n-restricted CM-field we have $E_K = W_K E_{K_0}$. Then, by the exactness of the sequence (40), we conclude that $\varepsilon/\bar{\varepsilon} \in W_K^2$ for every $\varepsilon \in E_K$. But $W_K^{2n} = 1$, by property (β). So again $\varepsilon^n \in K_0$ for all $\varepsilon \in E_K$.

(ii) => (i): We assume that $K \neq \mathbf{Q}(\varepsilon^n)$ for every $\varepsilon \in E_K$ and proceed analogously as in the proof of (iii) => (iv) of Theorem 2. By the same method as there we then first can conclude that K is a CM-field. Since in case of an imaginary quadratic numberfield K our assertion is easily seen to be true, we may suppose from now on that $K_0 \neq \mathbf{Q}$.

So again we can choose an unit ε_0 of K_0 which satisfies the conditions (37) and (38) above.
Now, suppose first that property (β) of a n-restricted CM-field is violated for K, i.e. let us assume that K contains a root ζ of unity such that $\zeta^{2n} \neq 1$. Then the unit $\varepsilon := \zeta\varepsilon_0$ of K satisfies the following three conditions:

(43) $\quad |\varepsilon| > 1$

(44) $\quad |\sigma\varepsilon| < 1$ for all embeddings $\sigma: K \to \mathbf{C}$ except the inclusion and the complex conjugation

(45) $\quad \varepsilon^n \notin K_0$.

But then it follows $K = \mathbf{Q}(\varepsilon^n)$, contradicting our initial assumption.
Suppose now that property (γ) is violated for K, i.e.

(46) $\qquad W_K^n \neq 1 \quad \text{and} \quad E_K \neq W_K E_{K_0}$.

The exact sequence (40) tells us then that there is an $\eta \in E_K$ for which the element $\zeta := \eta/\bar{\eta}$ belongs to W_K but not to W_K^2. It follows $\zeta^n \neq 1$ (since we already know that the cyclic grorp W_K has order dividing 2n, and by (46) we have $W_K^n \neq 1$).

But $\zeta^n \neq 1$ implies $\eta^n \notin K_0$. Thus every unit of the form

(47) $\qquad \varepsilon := \varepsilon_0^k \eta \quad \text{with} \quad k \in \mathbf{N}$

satisfies condition (45). If we choose k large enough then ε will satisfy conditions (43) and (44) as well. Thus again we arrive at $K = \mathbf{Q}(\varepsilon^n)$.

REFERENCES

[1] HALTER-KOCH, F. and LORENZ, F., *Ein Normalbasissatz für Einheiten algebraischer Zahlkörper*, Math. Ann. 257, 335-339 (1981).

[2] HASSE, H., *Zahlentheorie*, sec. edit., Akademie-Verlag, Berlin 1963.

[3] HASSE, H., *Über die Klassenzahl algebraischer Zahlkörper*, Akademie-Verlag, Berlin, Reprint 1985.

[4] WASHINGTON, L.C., *Introduction to cyclotomic fields*, Springer Verlag, New York - Heidelberg - Berlin, 1982.

LORENZ F.

Westfälische Wilhelms-Universität
Mathematisches Institut
D-44 Münster/Westf.
Roxeler Strasse 64

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

AN OVERVIEW OF THE SOLUTION TO THE CLASS NUMBER ONE PROBLEM FOR REAL QUADRATIC FIELDS OF RICHAUD-DEGERT TYPE

MOLLIN, R.A.

ABSTRACT

The purpose of this article of to give a survey of the results leading up to the recent solution of the class number one problem for real quadratic fields of Richaud-Degert type (modulo a suitable Riemann hypothesis). Included will be the remarkable connection with prime--producing quadratic polynomials.

1. NOTATION AND PRELIMINARIES

Throughout, D will denote a positive square-free integer. $Q(\sqrt{D})$ (or simply D), is said to be of (wide)

Richaud-Degert type, (or simply of R-D type), whenever $D = \ell^2 + r \neq 5$ where ℓ is a positive integer, r devides 4ℓ, and $-\ell < r \leq \ell$, (see [2] and [16]). If $|r| \in \{1,4\}$ then D is said to be of *narrow* R-D type. Finally h(D) will denote the class number of $Q(\sqrt{D})$.

2. RESULTS

The longest-standing class number one problem for R-D types is that of the narrow R-D type $D = \ell^2 + 1$. In [1] S. Chowla conjectured that if $p = m^2 + 1$ is prime with $m > 26$ then $h(p) > 1$. This remains an open problem. However, in [8] we established the following result.

THEOREM 1. $D = 4\ell^2 + 1$, *then the following are equivalent*

(1) $h(D) = 1$

(2) p *is inert in* $Q(\sqrt{D})$ *for all primes* $p < \ell$.

(3) $f_D(x) = -x^2 + x + \ell^2 \not\equiv 0 \pmod{p}$ *for all integers* x *and primes* p *with* $0 < x < p < \ell$.

(4) $f_D(x)$ *is equal to a prime for all integers* x *with* $1 < x < \ell$.

The case where $D = \ell^2 + 1$ with $\ell > 1$ odd is easily handled by the genus theory of Gauss to yield $h(D) > 1$. In the case where ℓ is even, Gauss's genus theory also

reduces to the case where D is prime. This also follows easily from Theorem 1. Moreover, if ℓ is composite then setting $x = 1$ in (3) of Theorem 1 yields that $h(D) > 1$. Hence the Chowla conjecture reduces to the case where $p = 4q^2 + 1$ where p and q are odd primes. Furthermore observe that the equivalence of (1) and (4) of Theorem is similar to the Rabinovitch result for complex quadratic fields (see [14] and [15]).

Although Theorem 1 appears to exhaust the algebraic techniques for attacking the Chowla conjecture, Mollin and Williams were able to prove the following result in [11]. In what follows GRH means the generalized Riemann hypothesis; i.e., the Riemann hypothesis for the zeta function ζ_K of the field K under consideration.

THEOREM 2. *If* GRH *holds for* $K = Q(\sqrt{p})$ *with* $p = m^2 + 1$ *prime, then* $h(p) > 1$ *for* $m > 26$.

Essentially Theorem 2 was proved by using the GRH to get an effective bound (in this case $p > 10^{13}$) for which the Chowla conjecture holds.

With Theorem 1 and 2 as an inspiration, Mollin and Williams were able to handle all other narrow R-D types in [12]. To discuss this work we need to set some notation. In what follows:

$$f_D(x) = \begin{cases} -x^2 + x + (D-1)/4 & \text{if } D \equiv 1 \pmod 4 \\ -x^2 + D & \text{if } D \not\equiv 1 \pmod 4 \end{cases}$$

and

$$\alpha = \begin{cases} (\sqrt{D-1})/4 & \text{if } D \equiv 1 \pmod 4 \\ \sqrt{D} & \text{if } D \not\equiv 1 \pmod 4 \end{cases}.$$

Moreover we label the following conditions to which we will refer.

(I) p is inert in $\mathbb{Q}(\sqrt{D})$ for all primes $p < \alpha$.

(II) $f_D(x) \not\equiv 0 \pmod p$ for all integers x and primes p such that $0 \le x < p < \alpha$.

(III) $f_D(x)$ is prime for all integers x with $1 < x < \alpha$.

(IV) $h(D) = 1$.

The first result of [12] is the following.

LEMMA 1. (I) $\leftrightarrow$ (II) $\rightarrow$ (III) $\rightarrow$ (IV). *Additionally, if* $D \equiv 1 \pmod 4$ then (III) $\rightarrow$ (II).

Thus Lemma 1 provides three sufficient conditions for $h(D) = 1$, and in the case $D \equiv 1 \pmod 4$ these three conditions are equivalent. At first glance this seems to be quite a general result. However the following result tells a more restrictive story.

LEMMA 2. *If* (III) *holds for* $D > 13$ *then* $D \equiv 1 \pmod 4$ *and* D *is of narrow* R-D *type.*

As an immediate consequence or Lemma 1 and 2 we have the following result.

THEOREM 3. *Let* $D > 13$, *then* (I) $\leftrightarrow$ (II) $\leftrightarrow$ (III) $\leftrightarrow$ $\leftrightarrow$ (IV) *holds if and only if* $D \equiv 1 \pmod 4$ *and* D *is of narrow* R-D *type.*

COROLLARY 1. $h(D) > 1$ if any of the following conditions hold:

(1) $D = m^2 + 1$ with $m > 1$ odd.

(2) $D = 4m^2 + 1$ with m composite or D composite.

(3) $D = m^2 - 1$ with $m > 2$.

(4) $D = m^2 \pm 4$ with $(D-1)/4$ composite.

The cases not covered by Corollary 1 are of interest. As we demonstrated earlier, the case where $D = 4q^2 + 1$ is prime with q prime is the remaining case of the Chowla conjecture. Moreover, Yokoi conjectured in [18] that if $D = \ell^2 + 4$ with $\ell > 17$ then $h(D) > 1$. Thus Corollary 1 reduces this conjecture to the case $D = \ell^2 + 4 = 4p + 1$, p a prime. Furthermore, Mollin conjectured in [9] - [10] that if $D = \ell^2 - 4$ with $\ell > 21$ then $h(D) > 1$. Corollary 1 tells us that, in this case, $(D-1)/4$ must be prime when $h(D) = 1$.

All of the above conjectures are solved (modulo GRH) by Mollin and Williams in [12]. Specifically:

THEOREM 4. *Suppose* $D > 13$ *and the* GRH *holds. Thus,* (I) $\leftrightarrow$ (II) $\leftrightarrow$ (III) $\leftrightarrow$ (IV) *holds if and only if* $D \in \{17, 21, 29, 37, 53, 77, 101, 173, 197, 293, 437, 677\}$.

As an immediate consequence we get the following remarkable Rabinovitch result for real quadratic fields.

THEOREM 5. *If* GRH *holds then* $f_D(x)$ *is prime for all integers* x *with* $1 < x < \alpha$ *if and only if* $D \in \{2, 3, 5, 6, 7, 11, 13, 17, 21, 29, 37, 53, 77, 101, 173, 197, 293, 437, 677\}$.

It is worth observing that Theorem 4 establishes (modulo GRH) that Saski [17] *did* without realizing it, find all real quadratic fields with $h(D) = k(D) = 1$ (where $k(D)$ is the period of the continued fraction expansion of $(1+\sqrt{D})/2$ for $D > 2$). They are $D \in \{2, 5, 13, 29, 53, 173, 293\}$.

Finally, the real quadratic fields of narrow R-D type with $h(D) = 1$ are all determined (modulo GRH) in [12]:

THEOREM 6. *If* GRH *holds then* $h(D) = 1$ *for* D *of narrow* R-D *type implies* $D \in \{2, 3, 17, 21, 29, 37, 53, 77, 101, 173, 197, 293, 437, 677\}$.

Observe that 6, 7 and 11 are of the more general wide R-D typed, whereas 5 and 13 are not R-D types.

The existence of the link between prime-producing polynomials and class number one, as suggested by Theorems 5 and 6, is a fact which has far-reaching implications beyond those established above. It is the investigation of this link which led Mollin and Williams in [13] to discover *all* real quadratic fields of R-D type with class number one (modulo GRH). We now discuss these connections.

The first result in [13] dealt with wide R-D types $D \not\equiv 1 \pmod 4$. In [10] Mollin proved that if $h(D) = 1$ for such D then $D = \ell^2 + r$ with $|r| = 2$. We consider two cases separately, that when t is even and that when t is odd. We deal with the even case first.

THEOREM 7. *Let* $D = 4\ell^2 \pm 2 > 2$. *If* $f_D(x) = -2x^2 + D/2$ *is prime or* 1 *for all integers* x *with* $0 \le x < \sqrt{D}/2$ *then* $h(D) = 1$.

Table 1.

D	$f_D(x) = -2x^2 + D/2$ for $0 \le x < \sqrt{D}/2$
6	3
14	7, 5
38	19, 17, 11, 1
62	31, 29, 23, 13
398	199, 197, 191, 181, 167, 149, 127, 101, 71, 37

Observe that when D = 398 we get the so-called *Karst polynomial* (see [3]). Karst showed that the density of primes in $-2x^2 + 199$ is higher than the celebrated *Euler* polynomial $x^2 + x + 41$. However, no explanation, other than having done a computer search, was given. Theorem 7 indicated *why* this should be the case. Moreover the following conjecture posed by Mollin [13] indicates that D = 398 is at the "top of its class".

CONJECTURE 1. *If* $D = 4\ell^2 + 2$ *then* $h(D) = 1$ *if and only if* D *is an entry in Table* 1.

We will return to this conjecture later. First we deal with the case where ℓ is odd. Mollin and Williams [13] proved:

THEOREM 8. *If* $D = (2m+1)^2 \pm 2$ *with* $m > 0$ *and* $f_D(x) = -2x^2 + 2x + (D-1)/2$ *is prime or* 1 *for all integers* x *with* $0 < x < (\sqrt{D}+1)/2$ *then* $h(D) = 1$.

As an illustration we have:

Table 2.

D	$f_D(x) = -2x^2 + (D-1)/2$ for $0 < x < (\sqrt{D}+1)/2$
7	3
11	5, 1
23	11, 7
47	23, 19, 11
83	41, 37, 29, 17, 1
167	83, 79, 71, 59, 43, 23
227	113, 109, 101, 89, 73, 53, 29, 1

Mollin [13] posed the following:

CONJECTURE 2. *If* $D = (2m+1)^2 \pm 2 > 3$ *then* $h(D) = 1$ *if and only if* D *is an entry in Table 2.*

Again we will return to this conjecture later. First we turn to wide R-D types $D \equiv 1 \pmod 4$. As a first case we consider the situation where r divides 2ℓ. In [10] Mollin proved that if $h(D) = 1$ for such D then $D = 33$ if $D \equiv 1 \pmod 8$ and $D = \ell^2 - p$ where p is an odd prime dividing ℓ if $d \equiv 5 \pmod 8$. Therefore $h(D) = 1$ forces $q = d/p$, prime and $p \equiv q \equiv 3 \pmod 4$.

Mollin [13] posed the following:

CONJECTURE 3. *Suppose* $D = \ell^2 - p$ *where* p *is an odd prime dividing* ℓ *and* $D \equiv 5 \pmod 8$. *If* $|px^2 + px - (D-p^2)/4p|$ *is prime for all integers* x *with* $0 \le x, (\sqrt{d-1})/4 - 1/2$ *then* $h(D) = 1$.

Evidence was given for the conjecture and the following illustrates it.

Table 3.

D	p	q	ℓ	$\lvert px^2+px-(D-p^2)\ 4p\rvert$ for $0 \le x < (\sqrt{d-1})/4 - 1/2$
141	3	147	2	11, 5, 7
573	3	193	24	79, 47, 43, 41, 29, 13
1293	3	431	36	223, 263, 109, 107, 101, 89, 71, 61, 47
1757	7	251	42	1619, 1409, 1213, 1031, 863, 709, 569, 443, 331, 233

This led Mollin [13] to pose:

CONJECTURE 4. *Suppose* $D = \ell^2 - p \equiv 1 \pmod 4$ *where* p *is an odd prime dividing* ℓ. *If* $h(D) = 1$ *then* D *is an entry in Table 3.*

The remaining R-D types are those of the form $D = \ell^2 \pm 4m$ with ℓ odd, $m > 1$ and m dividing ℓ is odd. Therefore if $h(D) = 1$ then $p = m$ must be prime, as must $q = D/m$ and $p \equiv q \equiv 3 \pmod 4$. Certain evidence given in [13] suggests that the following holds.

CONJECTURE 5. *Let* $D = \ell^2 \pm 4p$ *where* ℓ *is an odd prime dividing* ℓ. *If* $|px^2 + px - (D-p^2)/4p|$ *is* 1 *or prime for all integers* x *with* $0 \le x < (\sqrt{D-1})/2 + 1/2$ *then* $h(D) = 1$.

As an illustration we have:

Table 4.

D	p	q	t	$\lvert px^2 + px - (D-p^2)/4p \rvert$ for $0 \le x < \sqrt{D}/2 + 1/2$
213	3	7		1, 11, 17, 18, 3,
237	3	79		1, 13, 29, 71, 127,
413	7	59		1, 19, 23, 31, 37,
453	3	151	21	1, 19, 23, 31, 37, 53, 89, 131, 173, 233, 293, 359
717	3	239	27	23, 31, 37, 41, 53, 59, 67, 109, 157, 233, 271, 337, 409, 487
1077	3	359	33	1, 29, 37, 53, 71, 79, 83, 181, 241, 307, 379, 457, 541, 631, 727, 829, 937
1133	11	103	33	1, 23, 43, 109, 197, 107, 439, 539, 769, 967, 1187,1439,1693,1979,2287,2716,2969,3343
1253	7	179	35	13, 29, 41, 43, 97, 167, 251, 349, 461, 587, 727, 881,1049,1231,1427,1637,1861,2079,2351.

CONJECTURE 6. *Suppose* $D = \ell^2 \pm 4p \equiv 1 \pmod 4$ *where* $p|\ell$, p *an odd prime. If* $h(D) = 1$ *then* D *is an entry in Table 4.*

Using some of the techniques of [11] together with a new approach for the D's of Conjectures 4 and 6 Mollin and Williams [13] proved:

THEOREM 9. *If the* GRH *holds then Conjectures 1, 2, 4 and 6 hold.*

In summary we have the following remarkable result.

THEOREM 10. *If the* GRH *holds then all real quadratic fields of* R-D *type* $\mathbb{Q}(\sqrt{D})$ *with* $h(D) = 1$ *are one of* 39 *values of* D *given in the set* {2, 3, 6, 7, 11, 14, 17, 21, 23, 29, 33, 37, 38, 53, 47, 53, 62, 77, 83, 101, 141, 167, 173, 197, 213, 227, 237, 293, 398, 413, 437, 453, 573, 677, 717, 1077, 1133, 1253, 1293, 1757}. *Of these values* 14 *are of narrow* R-D *type, and the remaining* 25 *are of wide* R-D *type. (Note that* 5 *is not included since it is not generally considered to be of* R-D *type; and* 13, 69 *and* 93 *are excluded since they are of the form* $d = \ell^2 + r$ *with* $|r| > \ell$).

Although Theorem 10 is contingent upon GRH there are other substantial reasons for believing that this result is true, independent of GRH. For example, Theorems 7 and 8 prove that, if any more D exist than are in Tables 1 and 2 then there would have to exist a prime-producing quadratic polynomial with an astronomical density of primes. Conjectures 3 and 5 point in the same direction. In what follows we discuss some data pertaining to these prime densities.

Let $\nu(f,N)$ be the cardinality of the set $\{x \in \mathbb{Z} : 0 \le x \le N;\ |f(x)| = 1 \text{ or prime}\}$ where f is a polynomial.

Table 5.

f(x)	$\nu(f, 8000)$
$3x^2 + 3x - 11$	998
$3x^2 + 3x - 19$	1780
$7x^2 + 7x - 13$	2031
$3x^2 + 3x - 37$	2199
$3x^2 + 3x - 107$	2492
$3x^2 + 3x - 59$	2513
$7x^2 + 7x - 61$	2540
$7x^2 + 7x - 43$	2871
$3x^2 + 3x - 89$	2897
$2x^2 - 199$	3573

We observe that for the Euler polynomials $x^2 + x + 41 = f(x)$, $\nu(f,8000) = 3406$. Thus the Karst polynomial has a higher density for reasons given earlier. Moreover, a search through the literature shows that in the papers dealing with high density prime-producing quadratic polynomials there are no reasons given for the phenomenon other than having done a computer search as in [3]. However on the basis of the work accomplished above and evidence obtained it seems that if $D > 0$ *is any square-free integer, then* $h(D) = 1$ *if and only if there exists some polynomial* $ax^2 + bx + c = f_D(x)$ *whose discriminant* $b^2 - 4ac = v^2D$ *for some integer* $v \geq 1$, *and* $f_D(x)$ *is prime for certain integers* x *depending on* a,b *and* c.

We cannot be sure specific about the bounds on x in terms of a,b and c because they are not yet well understood. Further investigations should yield specifics. Yet, given the R-D class number one solution in this paper, it appears that the answers for the bounds may be quite complicated indeed.

Finally we note that, although R-D types may appear to be very restrictive, they provide a firm basis for a general investigation of arbitrary square-free D. As evidence for this point of view we cite the following. It is clear that there as always an integer $v \geq 1$ such that $v^2 = \ell^2 \pm 4$, since one needs only look at the norm of the fundamental unit of $Q(\sqrt{D})$. Thus, if we choose the *smallest* integer $v \geq 1$ such that $v^2D = \ell^2 + r$ where r divides 4ℓ and $-\ell < r \leq \ell$ then using [4] we may explicitly write down the fundamental unit for $Q(\sqrt{D})$ in terms of v, ℓ and r. Hence R-D types are much more general than they appear. It is on this basis that we are continuing further investigations begun in [5] - [7].

NOTE ADDED IN PROOF: Since the writing of this survey substantial progress has been made. In particular the author and H.C. Williams have been able to remove the GRH assumption in Theorem 10 yielding an unconditional result saying that the values of D in Theorem 10 are *all*

R-D types having $h(D) = I$ *with possibly only one more value*. Moreover we have given evidence to show that it is virtually impossible for this exceptional value to exist. Finally, the author and H.C. Williams have been able to classify certain *non* R-D types with class number one in terms of prime-producing quadratic polynomials.

REFERENCES

[1] CHOWLA, S. and FRIEDLANDER, J., Class numbers and quadratic residues, *Glasgow Math. J.* 17 (1976), 47-52.

[2] DEGERT, G., Über die bestimming der grundeinheit gewisser reell-quadratischer Zaklkorper, *Abh. Math. Sem. Univ. Hamburg* 22 (1958), 92-97.

[3] KARST, E., New quadratic polynomials with high density of primes, *Elem. Math.* 28 (1973), 116-118.

[4] KUTSUNA, M., On the fundamental units of real quadratic fields, *Proc. Japan Acad.* 50 (1974), 580-583.

[5] MOLLIN, R.A., Diophantine equations and class numbers, *J. Number Theory*, 24 (1986), 7-19.

[6] MOLLIN, R.A., On the insolubility of a class of diophantine equations and the nontriviality of the class numbers of related real quadratic fields of Richaud-Degert type, *Nagoya Math. J.*, 105 (1987), 39-47.

[7] MOLLIN, R.A., Lower bounds for class numbers of real quadratic fields, *Proc. Amer. Math. Soc.*, 96 (1986), 545-550.

[8] MOLLIN, R.A., Necessary and sufficient conditions for the class number of a real quadratic field to be one and a conjecture of S. Chowla, *Proc.Amer.Math.Soc.*, 102 (1988), 17-21.

[9] MOLLIN, R.A., Class number one criteria for real quadratic fields I., *Proc. Japan Acad., Ser. A.*, 63 (1987), 121-125.

[10] MOLLIN, R.A., Class number one criteria for real quadratic fields II., *Proc. Japan Acad., Ser. A.*, 63 (1987), 162-164.

[11] MOLLIN, R.A. and WILLIAMS, H.C., A conjecture of S. Chowla via the generalized Riemann hypothesis, *Proc.Amer.Math.Soc.*, 102 (1988), 794-796.

[12] MOLLIN, R.A. and WILLIAMS, H.C., Prime-valued polynomials and class numbers of real quadratic fields, (to appear: *Nagoya Math.J.*).

[13] MOLLIN, R.A. and WILLIAMS, H.C., Prime producing polynomials and real quadratic fields of class number one, (to appear: *Proceedings of Internat. Conf. on number theory at Quebec*, 1987).

[14] RABINOVITCH, G., Eindentigkeit der zerlegung in primzahlfaktoren in quadratischen zahlkörpern, *Proc. Fifth Internat. Congress Math. (Cambridge)* Vol. 1 (1913), 418-421.

[15] RABINOVITCH, G., Eindentigkeit der zerlegung in primalzahlfaktoren in quadratischen zahlkörpern, *J. rein. angew. Math.* 142 (1913), 153-164.

[16] RICHAUD, C., Sur la résolution des équations $x^2 - Ay^2 = \pm 1$, *Alti Acad. Pontif. Nuovi Lincei* (1866), 177-182.

[17] SASAKI, R., A characterization of certain real quadratic fields, *Proc. Japan Acad. Ser. A*, 62 (1986), 97-100.

[18] YOKOI, H., Class-number one problem for certain kind of real quadratic fields, *Proc. Internat. Conf. in Class numbers and fundatmental units of algebraic number fields, Katata, Japan* (1986), 125-137.

MOLLIN, R.A.
Mathematics Department
University of Calgary
Calgary, Alberta
CANADA T2N 1N4

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

A CONSTRUCTION OF QUADRATIC FIELDS WHOSE CLASS NUMBERS ARE DIVISIBLE BY A POWER OF 3

NAKAHARA, T.

1. INTRODUCTION

One aim of ours is to solve a question of T. P. Vaughan as an application of class number problems in Section 3[9], [5].

For the preliminary it is necessary for us to have a series of real quadratic fields whose fundamental units are explicitely known and infinitely many real quadratic fields whose class numbers are divisible by a power of 3 (cf. Section 2).

Our results estiblished in Section 3, are closely related to works of G. Gras, P.J. Weinberger and D. Shanks (cf. [3], [10], [8]).

In Section 4, we shall give some experimental data concerning the 3-Sylow group of the class groups of real quadratic fields whose odd (resp. even) discriminants

are smaller than or equal to 999,869 (resp. 4,000,008). H. Cohen discribed some asymptotic distribution of class groups of quadratic fields [1]. We hope that our experiments support a part of his heuristic statements. Recently F. Diaz y Diaz, P. Llorente and J. Qver found several examples of 3-rank equal to 4 of the class groups in the real case [2].

2. KNOWN RESULTS

From the following Proposition 1, Theorem 1 and Lemma our new results will be deduced succinctly in the next Section.

PROPOSITION 1[5]. *Put* $f^2 d = 1 + 4(cx)^{2n}$, *where* $n > 1$, $c \geq 1$ *are arbitrary fixed rational integers. Then*

$$\varepsilon_f = 2(cx)^n + f\sqrt{d}$$

is the fundamental unit of a real quadratic field $Q(\sqrt{d})$, *where* x *takes any prime number except for at most a finite number of primes.*

We proved this Proposition by a slight modification of Lemma 4[10], using the Thue-Siegel-Roth theorem [4, pp. 121-160].

From the above result we obtained the following

THEOREM 1[5]. *For* $D = 1 + 4x^{2n}$, *let the* x *take all of the prime numbers except for a finite number of primes, where* $n = 3^e m$, $(3, m) = 1$ *and* $e \geq 1$ *hold. Then the class numbers of real quadratic fields* $Q(\sqrt{D})$ *are divisible by* 3^e. *Therefore there exist infinitely many real quadratic fields whose ideal class groups have a* 3*-subgroup.*

The following lemma is known as the 'Spiegelungssatz' of Scholz.

LEMMA [7]. *For an integer* $d > 1$ *whose square-free part* > 1 *is prime to* 3 , *let* r *and* s *be the* 3*-rank of the class groups of an imaginary quadratic field* $Q(\sqrt{-3d})$ *and of a real quadratic field* $Q(\sqrt{d})$ *respectively. Then*

$$s \leq r \leq s + 1.$$

3. SEMI-CUBE FUNDAMENTAL UNITS

In [9], T.P. Vaughan proposed an interesting question: For what integer $D > 0$ do we have $3 \mid h(-3D)$ while the fundamental unit of $Q(\sqrt{D})$ is not a semi-cube? Are there any such D?

Let $F = Q(\sqrt{D})$ be a quadratic field. Define the ideal T in F by

$$T = \begin{cases} (3)^2 & \text{if 3 is not ramified in } F, \\ \\ p^3 & \text{if 3 is ramified in } F;\ (3) = p^2. \end{cases}$$

Then a number $\gamma \in F$ is called a semi-cube in F provided

(0) γ is an integer and γ is not a perfect cube,

(i) the principal ideal (γ) is an ideal cube,

(ii) γ is a cubic residue modulo T; $\gamma \equiv \xi^3 \bmod T$ for some integer $\xi \in F$,

(iii) $N(\gamma)$ is not divisible by 3.

By [7] it is known that if the fundamental unit of $Q(\sqrt{D})$ is a semi-cube, then the class number $h(-3D)$ is divisible by 3. However, we can see that its converse does not hold in general. In Theorem 2 we will give that there is an infinite class for which the converse does not hold.

PROPOSITION 2. *For $m \equiv 0 \bmod 3$ let $f^2 d = 1 + 4(3p)^{2m}$ or $f^2 d = p^{2m} + 4$, where d is square-free. Then the fundamental unit of $Q(\sqrt{d})$ is not a semi-cube for any prime $p > 3$ up to a finite number of primes p.*

PROOF. From Proposition 1 and Lemma 4 in [10] we can see that the units $\epsilon = 2(3p)^m + f\sqrt{d}$ and $(p^m + f\sqrt{d})/2$ are the fundamental units of $Q(\sqrt{d})$ for the cases of $D = 1+4p^{2m}$ and $p^{2m}+4$ respectively. Since D and 3 are relatively prime we may consider the case of the ideal $T = (9)$. If ϵ is a cubic residue modulo T, then we have

$\varepsilon \equiv \xi^3 \mod T$ for some integer $\xi = (x + y\sqrt{d})/2$ in $Q(\sqrt{d})$.

In the former case we get the congruences:

$-2(3p)^m \equiv x^3 + 3xy^2 d \mod 9$ and $-f \equiv 3x^2 y + y^3 d \mod 9$.

Then $0 \equiv x \mod 3$ and $f^2(-f) \equiv f^2 y^3 d \equiv 5y^3 \equiv -y^3 \mod 3$, hence $f \equiv y \mod 3$ hold, which implies that $-f \equiv f^3 d \mod 3$. Since $f^2 d \equiv 1 \mod 3$, it follows $2f \equiv 0 \mod 3$, which is a contradiction.

In the latter case we get:

$4p^m \equiv x^3 + 3xy^2 d \mod 9$ and $4f \equiv 3x^2 y + y^3 d \mod 9$.

Then $\pm 1 \equiv x \mod 3$ and $f \equiv -y \mod 3$ hold. Hence

$4f \equiv 3(-f) + (-f)^3 d \mod 9$. By $f^2 d \equiv 5 \mod 9$, it follows $12f \equiv 0 \mod 9$, which is impossible. Therefore we have proved Proposition 2.

Combining Theorem 1, Lemma 2 and Proposition 2 we obtain

THEOREM 2. *There exist infinitely many real quadratic fields $Q(\sqrt{d})$ whose fundamental units are not of semi-cube while the class numbers of imaginary quadratic fields $Q(\sqrt{-3})$ are divisible by 3.*

4. THE DATA OF THE 3-SYLOW GROUPS IN REAL QUADRATIC FIELDS $Q(\sqrt{D})$ WITH $D \leq 1{,}000{,}002$

In this Section we shall describe a part of our experimental data for the last six years [6]. In the table '...(n)...' means the number n of real quadratic fields omitted here, whose class numbers are divisible by 9. For any square-free $D > 1$, $H3$, H, L and N denote the structure of the 3-Sylow group of the class group of $Q(\sqrt{D})$, the class number, the number of the reduced forms in the principal class and the number of the reduced forms in all the classes respectively. The minus sign of H means the negative norm of the fundamental unit of $Q(\sqrt{D})$.

We found the nine fields $Q(\sqrt{D})$ whose class numbers are divisible by 81 for $1 < D \leq 1{,}000{,}002$ i.e., in addition to our table the next seven cases:

$D =$ 538267 (H3 = 81), 577601 (H3 = 81), 700571 (H = 81),
705091 (H =162), 837286 (H =162), 861898 (H = -162),
882526 (H3 = 81).

D	$H3$	H	L	N
1129	9	- 9	3	51
	.....(18)	.....		
8761	27	- 27	3	165
	.....(58)	.....		
23659	3 x 3	18	10	280
	.....(802)	.....		
156566	9 x 3	27	10	422
	....(1642)	.....		
389911	27 x 3	81	8	1184
	.....(701)	.....		
484417	81	- 81	3	491
	....(4382)	.....		
999869	9	- 18	5	192
1000002	27	54	2	636

The number $\sum$ of all the $Q(\sqrt{D})$ with $H \equiv 0 \bmod 9$ for $1 < D \leq 1000002$ is equal to 7611.

The structure $H3$ of class group	9	3 x 3	27	9 x 3	81 H
# of $Q(\sqrt{D})$	6684	417	477	24	9
Ratio of each case to $\sum$	87.8%	5.5%	6.3%	0.3%	0.1%

Our experiments were carried out mainly by TOSBAC

7/70B in our department and partially by FACOM M-150 F in the computer center of Saga University and FACOM M-380 + VP100 of Kyushu University.

REFERENCES

[1] COHEN, H., Sur la distribution asymptotique des groupes de classes, *C.R. Acad. Sc. Paris, Série* I, 296(1983), 245-247.

[2] DIAZ Y DIAZ, F., LLORENTE, P. and QVER J., Cubic fields, a congruential criterion for Scholz's theorem and new real quadratic fields with 3-rank equal to 4, Preprint.

[3] GRAS, G., Extension abéliennes non ramifiées de degré premier d'un corps quadratique, *Bull. Soc. math. France*, 100(1972), 177-193.

[4] LEVEQUE, W.J., *Topics in number theory*, Vol. II, Addison-Wesley, Reading, Mass., 1961.

[5] NAKAHARA, T., On real quadratic fields whose ideal class groups have a cyclic p-subgroup, *Rep. Fac. Sci. Engrg. Saga Univ. Math.*, 6(1978), 15-26.

[6] NAKAHARA, T., Table of class numbers and of 3-ranks of class groups in real quadratic fields $Q(\sqrt{D})$ with $1 < D \leq 1069091$, Unpublished.

[7] SCHOLZ, A., Über die Beziehung der Klassenzahl quadratischer Körper zueinander, *J. reine angew. Math.*, 166(1932), 201-203.

[8] SHANKS, D. and WEINBERGER, P., A quadratic field of prime discriminant requiring three generators for its class group, and related theory, *Acta Arith.*, 21(1972), 71-87.

[9] VAUGHAN, T. P., The construction of unramified abelian cubic extensions of a quadratic field, *Acta Arith.*, 44(1984), 379-387.

[10] WEINBERGER, P.J., Real quadratic fields with class numbers divisible by n, *J. Number Theory*, 5(1973), 237-241.

NAKAHARA, T.

Department of Mathematics
Faculty of Science and Engineering
Saga University
Saga 840, J a p a n

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

DIVISIBILITY PROPERTIES OF LINEAR RECURSIVE SEQUENCES

ATTILA PETHŐ*

1. INTRODUCTION

Let R be a ring, $k \geq 1$ an integer, $G_1,\ldots,G_{k-1}$, $A_1,\ldots,A_k \in R$, $A_k \neq 0$ and let $G_{n+k} = A_1G_{n+k-1}+\ldots+A_kG_n$ for $n \geq 0$. We shall call $(G_n)_{n\in N}$ a linear recursive sequence, in the following lrs, over R, and $x^k - A_1x^{k-1} - \ldots - A_k$ the characteristic polynomial of $(G_n)_{n\in N}$. We denote by Z the ring of integers, by N the set of non-negative integers, and by Q as well as by C the field of rational and complex numbers.

P. Bundschuh and A. Pethő [1] proved theorems on transcendency of real numbers, which are defined by quickly convergent series using W.M. Schmidt's approxima-

* Research supported by Hungarian National Fundation for Scientific Research Grant No. 273/86.

tions theorem [9]. There occurs, beside natural analytical conditions, an assumption on divisibility property of lrs's over Z. In the appendix of [1] we proved (Satz 6.) that if $(G_n)_{n\in N}$ is a lrs over Z, such that $G_n \neq 0$ for infinitely many n then there exists a strictly increasing sequence $(n_i)_{i\in N}$ with $G_{n_i} | G_{n_{i+1}}$ for all i=0,1,... .

In this paper we prove

THEOREM 1. *Let* R *be a Dedekind domain such that* R/P *is finite for every prime ideal* P *of* R, *and* $(G_n)_{n\in N}$ *a lrs over* R *such that* $G_n \neq 0$ *for infinitely many* n. *Then there exists a strictly increasing sequence* $(n_i)_{i\in N}$ *with* $G_{n_i} | G_{n_{i+1}}$ *for all* i=0,1,... .

The maximal orders of algebraic number fields and univariate polynomial rings over finite fields satisfy the conditions of Theorem 1.

We remark that in Theorem 1 the assumption R/P is finite for every prime ideal P of R is necessary. More precisely it holds:

THEOREM 2. *Let* $p_1(x), p_2(x) \in Q[x]$ *such that* $(p_1(x), p_2(x))=1$ *and* $p_1(x)/p_2(x) \notin Q$. *Let further* $a,b \in Q\setminus\{0\}$ *with* $|a/b| \neq 1$, *and* $G_n(x)=ap_1(x)^n-bp_2(x)^n$ *a lrs over* Q[x]. *Then there exists at most one* $n>0$ *with* $G_n(x) \in Q$, *and if*

$n,m \in N$ *such that* $G_n(x), G_m(x) \notin Q$ *then* $(G_n(x), G_m(x))=1$.

Let now $(G_n)_{n\in N}$ be as in Theorem 1 and

$$I(G) = \{(n_i)_{i\in N} \text{ strictly increasing, with } G_{n_i} \mid G_{n_{i+}} \text{ for all } i=0,1,\ldots\}.$$

By Theorem 1 $I(G)\neq\emptyset$, hence there exists

$$\omega(G) = \inf_{(n_i)\in I(G)} \liminf_{i\to\infty} \frac{n_{i+1}}{n_i} .$$

It is evident that $\omega(G)=1$ for $k=1$. M. Hall [4] called a lrs over Z divisibility sequence if $G_n \mid G_{nm}$ for any m and n not zero. This concept is naturally meaningful for lrs's over arbitrary integer domains. It is also clear that $\omega(G)\leq 2$ for divisibility sequences. A typical divisibility sequence is the well-known Fibonacci sequence, which is defined by $k=2$, $G_0=0$, $G_1=A_1=A_2=1$.

We proved in [1] (Satz 7.) that if $(G_n)_{n\in N}$ is a lrs over Z with $k=2$ and such that the quotient of the roots of its characteristic polynomial is not a root of unity, then $\omega(G)\geq 2$. We generalize here this result too.

THEOREM 3. *Let* $(G_n)_{n\in N}$ *be a lrs over the maximal order* Z_k *of an algebraic number field* K *with* $k=2$, *and such that not both of* G_0, G_1 *are zero, and neither the*

roots nor the quotient of the roots of its characteristic polynomial are roots of unity, then $\omega(G)\leq 2$.

Theorem 3 is much sharper than Corollary 3.6 of T.N. Shorey and R. Tijdeman [10].

M. Hall [4] observed, that the only second order divisibility sequences over Z are defined by $G_n=t(\alpha_1^n-\alpha_2^n)/(\alpha_1-\alpha_2)$ or $G_n=tna^{n-1}$ according as the roots of $x^2-A_1x-A_2$ are distinct - α_1 and α_2 - or equal to a. Combining this result and Theorem 3 we get

COROLLARY 1. *Let* $(G_n)_{n\in N}$ *be a second order divisibility sequence over* Z, *then* $\omega(G)=2$.

2. AUXILIARY RESULTS

LEMMA 1. *Let* R *be a commutative unitary ring, and* M *be an ideal of* R *such that* R/M *is finite. If* $(G_n)_{n\in N}$ *is a lrs over* R, *then* $(G_n \bmod M)_{n\in N}$ *is periodic, and if in addition* $(A_k, M)=1$ *then* $(G_n \bmod M)_{n\in N}$ *is purely periodic.*

In the case R=Z this Lemma is due to Carmichael [2] and in general to E.C. Dade, D.W. Robinson, O. Taussky and M. Ward [3].

LEMMA 2. *Let* R *be an integer domain and* $(G_n)_{n\in N}$ *be a lrs over* R *with characteristic polynomial* $x^k-A_1x^{k-1}-\ldots-A_k$. *Let* $a,b\in N$, $b\neq 0$. *Then* $G^a_{(b)}=(G_{a+bn})_{n\in N}$ *is also a lrs over* R *and its characteristic polynomial looks like* $x^k-A_1^*x^{k-1}-\ldots-A_k^*$, *where* $A_k^*=-(-A_k)^b$.

PROOF. Let K be the quotient field of R, and let $\prod_{j=1}^{k}(x-\alpha_j)$ be the factorization of $f(x)=x^k-A_1x^{k-1}-\ldots-A_k$ over the algebraic closure $\bar{K}$ of K. Then by Theorem 1 of H. Niederreiter [6], which is acutally true for any fields not only for finite ones, the characteristic polynomial $f_b(x)$ of $G^a_{(b)}$ has the factorization $\prod_{j=1}^{k}(x-\alpha_j^b)$ in $\bar{K}$. Hence the coefficients of $f_b(x)$ are symmetric polynomials with integer coefficients of the elementary symmetric polynomials of $\alpha_1,\ldots,\alpha_k$, i.e. of $A_1,\ldots,A_k$, so $f_b(x)\in R[x]$. The absolute term of $f_b(x)$ is $(-\alpha_1^b)\ldots(-\alpha_k^b) = ((-\alpha_1)\ldots(-\alpha_k))^b = (-A_k)^b$.

3. PROOF OF THEOREM 1 AND 2

PROOF OF THEOREM 1. If R has infinitely many prime ideals then there exist $a,b\in N$, $b\neq 0$ such that $G_{a+bn}\neq 0$ for $n\in N$. Let namely $G_0 = \ldots = G_{r-1} = 0$, $G_r \neq 0$, where $r\leq k-1$. There exists a prime ideal P of R which does not divide G_r and A_k. Consider $(G_n \bmod P)_{n\in N}$. This is by

Lemma 1 purely periodic with period length say p. Then $G_{ps+r} \equiv G_r \not\equiv 0 \pmod{P}$ for all $s \in \mathbb{N}$, therefore $G_{ps+r} \neq 0$ for $s \in \mathbb{N}$. By Lemma 2 $G^r_{(p)}$ is a lrs over R.

Hence if R has infinitely many prime ideals we may assume that $G_n \neq 0$ for $n \in \mathbb{N}$. In this case let $P_1, \ldots, P_t$ denote all the distinct prime ideal divisore of $A_k R = (A_k)$ and take $P = \{P_1, \ldots, P_t\}$.

If R has only finitely many prime ideals then let P be their set.

In the sequel $\nu_P(A)$ will denote the exact exponent in which the prime ideal P divides the ideal A.

Let $P_1^{0} = \{ P \in P$: for each $m \in \mathbb{N}$ there exist only finitely many $k \in \mathbb{N}$ with $\nu_P(G_k) < m\}$

and $P_2^{(0)} = P \setminus P_1^{(0)}$.

In case $P_2^{(0)} \neq \emptyset$ shall the arrangement be refined in the following way. Let $P \in P_2^{(0)}$, we may assume $P = P_1$; and let $N_1 \in \mathbb{N}$ such that $\nu_{P_1}(G_k) < N_1$ for infinitely many $k \in \mathbb{N}$. By Lemma 1 $(G_n \bmod P_1^{N_1})_{n \in \mathbb{N}}$ is periodic, hence there exist $a_1, b_1 \in \mathbb{N}$, $b_1 \neq 0$ with $G_{a_1+b_1 s} \equiv G_{a_1} \equiv 0 \pmod{P_1^{N_1}}$ for all $s \in \mathbb{N}$. By Lemma 2 $(G_{a_1+b_1 s})_{s \in \mathbb{N}}$ is a lrs over R and all prime ideal divisors of the absolute term of its characteristic polynomial belong to P. Take $(G_n^{(1)})_{n \in \mathbb{N}} = (G_{a_1+b_1 s})_{s \in \mathbb{N}}$.

Let now $P_1^{(1)} = \{P \in P$: for each $m \in N$ there exist only finitely many $k \in N$ with $\nu_P(G_k^{(1)}) < m\}$

and $P_2^{(1)} = P \setminus P_1^{(1)}$. There hold $P_1^{(1)} \supset P_1^{(0)}$ and $P_1 \in P_2^{(1)}$. If now $P_2^{(1)} \setminus \{P_1\} \neq \emptyset$ is true, then will the above procedure with a from P_1 distinct element of $P_2^{(1)}$ be repeated. After finitely many, say τ steps where $\tau \in \{0,\ldots,t\}$ one will get a disjoint partition $P_1^{(\tau)} \cup P_2^{(\tau)}$ of P with the following properties:

(i) For all $P \in P_1^{(\tau)}$ and $m \in N$ there exist at most finitely many $k \in N$ with $\nu_P(G_k^{(\tau)}) < m$.

(ii) For any $P_i \in P_2^{(\tau)}$, $1 \leq i \leq \tau$, there exist $N_i \in N$ and $g_i \neq 0$ with $\nu_{P_i}(g_i) < N_i$ and $G_k^{(\tau)} \equiv g_i \pmod{P_i^{N_i}}$ $(k=0,1,\ldots)$.

(iii) All prime ideal divisors of the absolute term in the characteristic polynomial of $(G_k^{(\tau)})_{k \in N}$ belong to P.

(iv) $G_k^{(\tau)} \neq 0$ for inifinitely many k.

For brevity take $P_1 = P_1^{(\tau)}$, $P_2 = P_2^{(\tau)}$ and $G_k = G_k^{(\tau)}$ for $k \in N$ and define:

$$T_k = \prod_{P \notin P} P^{\nu_P(G_k)}, \quad U_k = \prod_{P \in P_1} P^{\nu_P(G_k)}, \quad V_k = \prod_{P \in P_2} P^{\nu_P(G_k)}.$$

It is clear that $(G_k) = T_k U_k V_k$, $(k=0,1,\ldots)$. By (ii) V_k is independent of k and equal to an ideal V. If R has only finitely many prime ideals then $I_k = (1)$.

Now we are in the position to construct a subsequence of $(G_k)_{k\in N}$ with the property stated in the Theorem. Take $k_0=-1$, $G_{-1}=1$, $k_1=1$ and assume that there were found integers $k_0<k_1<\ldots<k_t$ with $G_{k_i} | G_{k_{i+1}}$, $i=0,1,\ldots,t-1$, and $G_{k_t}\neq 0$.

By Lemma 1 $(G_k \bmod T_{k_t})_{k\in N}$ is purely periodic, hence there exists a positive integer b_t with

$$G_{k_t+b_t s} \equiv G_{k_t} \equiv 0 \pmod{T_{k_t}}$$

for all $s\in N$. From this and from $(T_{k_t}, u_{k_t+b_t s} V) = (1)$ one gets $T_{k_t} | T_{k_t+b_t s}$ for all $s\in N$. We have further $G_{k_t+b_t s} \neq 0$ for infinitely many s.

If $u_{k_t} \nmid u_{k_t+b_t s}$ would hold for all $s\in N$ with $G_{k_t+b_t s} \neq 0$, then there would exist for all such $s\in N$ a $\mathfrak{Q}_s \in P_1$ with

$$\nu_{\mathfrak{Q}_s}(u_{k_t}) > \nu_{\mathfrak{Q}_s}(u_{k_t+b_t s}) .$$

P_1 is finite, hence there exists a $\mathfrak{Q}\in P_1$ such that

$$\nu_{\mathfrak{Q}}(u_{k_t}) > \nu_{\mathfrak{Q}}(u_{k_t+b_t s}),$$

for inifinitely many $s\in N$, but this contradicts (i). Hence there exists $0 \neq s_0 \in N$ with $u_{k_t} | u_{k_t+b_t s_0}$ and $G_{k_t+b_t s_0}$. So choosing $k_{t+1} = k_t+b_t s_0 > k_t$ we have $G_{k_{t+1}} \neq 0$ and $G_{k_t} | G_{k_{t+1}}$ and Theorem 1 is proved.

PROOF OF THEOREM 2. Let $n > m > 0$ and assume that $G_n(x)$, $G_m(x) \in Q$. This means that $ap_1(x)^n - bp_2(x)^n \in Q$ and so deg $p_1(x)$ = deg $p_2(x) > 0$. Let $p_i(x) = a_{ik}x^k + \ldots + a_{i0}$, $(i=1,2)$ then $aa_{1k}^n - ba_{2k}^n = aa_{1k}^m - ba_{2k}^m = 0$ and so $a/b = (a_{2k}/a_{1k})^n = (a_{2k}/a_{1k})^m$, but this is impossible by the assumption $\frac{|a|}{|b|} \neq 1$.

Let now n be chosen such that $G_n(x) \notin Q$ and let $P(x) \in Q[x]$ be an irreducible divisor of $G_n(x)$. Let α be a complex root of $P(x)$, then $Q[x]/(P(x))$ is isomorphic to $Q(\alpha)$. Hence $P(x) | G_m(x)$ for some $m \in N$ if and only if $G_m(\alpha) = ap_1(\alpha)^m - bp_2(\alpha)^m = 0$. If $p_2(\alpha) = 0$ would hold, then $p_1(\alpha) = 0$ would be satisfied too, which implies $(p_1(x), p_2(x)) \neq 1$. Hence $p_1(\alpha), p_2(\alpha) \neq 0$. Assume now that there exists a $m \neq n$ with $P(x) | G_m(x)$. Then $ap_1(\alpha)^m - bp_2(\alpha)^m = ap_1(\alpha)^n - bp_2(\alpha)^n = 0$ leads to a contraticion with $\frac{|a|}{|b|} \neq 1$ in the same way as in the first part of the proof.

4. LEMMAS ON ALGEBRAIC RECURRENCE SEQUENCES

In the sequel let A, B, G_0, G_1 be algebraic integers, $B \neq 0$, G_0 and G_1 not zero at the same time and $(G_n)_{n\in N}$ be defined by the recursion

$$(1) \qquad G_{n+2} = AG_{n+1} - BG_n \qquad (n = 0,1,\ldots).$$

Let $K = Q(A,B,G_0,G_1)$ and denote Z_K the maximal order of K. Let α and β be the roots of the characteristic polynomial of $(G_n)_{n\in N}$, and $a = (G_1 - \beta G_0)/(\alpha - \beta)$, $b = (G_1 - \alpha G_0)/(\alpha - \beta)$. We call $(G_n)_{n\in N}$ non-degenerated if neither α, β nor α/β is a root of unity and $ab \neq 0$. $(\alpha,\beta,\ldots)$ will denote the ideal generated by $\alpha,\beta,\ldots \in Z_K$.

LEMMA 3. *Let* $(G_n)_{n\in N}$ *be a non-degenerated lrs over* Z_K. *Then there exist a positive integer* h *and* $\omega \in Z_K$ *such that* $(\alpha^{2h}/\omega\ ,\ \beta^{2h}/\omega) = (1)$ *and if*

$$(2) \qquad G_{i,n} = a\alpha^i\left(\frac{\alpha^{2h}}{\omega}\right)^n - b\beta^i\left(\frac{\beta^{2h}}{\omega}\right)^n \quad (n=0,1,\ldots;\ i=0,\ldots,2h-1)$$

then $(\alpha-\beta)^2 G_{i,n} \in Z_K$ *and* $\omega^n G_{i,n} = G_{2hn+i}$.

PROOF. Let $A = (A^2,B)$ in K. Because the ideal class group of K is finite there exist an integer $h > 0$ and $\omega \in Z_K$ with $A^h = (\omega)$. Let $F = K(\sqrt[h]{\omega})$ and $\bar{A} = (A^2,B)$ in F. Then by Theorem 98 [5], $\bar{A} = (\sqrt[h]{\omega})$, hence $A^2/\sqrt[h]{\omega}$ and $B/\sqrt[h]{\omega}$ are algebraic integers and $(A^2/\sqrt[h]{\omega},\ B/\sqrt[h]{\omega}) = (1)$. It follows that $\alpha/\sqrt[2h]{\omega}$ and $\beta/\sqrt[2h]{\omega}$ are algebraic integers and $(\alpha/\sqrt[2h]{\omega},\ \beta/\sqrt[2h]{\omega}) = (1)$ in $L = F(\alpha)$. From this we conclude that $\mathfrak{B} = (\alpha^{2h}/\omega,\ \beta^{2h}/\omega) = 1$ in K. The other assertions of the Lemma are clear.

LEMMA 4. *Let* $(G_n)_{n\in N}$ *be as in Lemma 3 and* $\mathfrak{p}$ *be a prime ideal of* K *which is lying above the prime number* p. *Then*

$$\nu_{\mathfrak{p}}(G_n) = \frac{n}{2}\nu_{\mathfrak{p}}(A^2,B)+p^{4m+4}(\log p)^{-7}0(\log^3 n+p^{3m})$$

holds uniformly in p, *where* $m=[K,Q]$ *or* $2[K,Q]$ *according as* $\alpha\in K$ *or not.*

PROOF. One can argue in Z_K literally lika A. Schinzel in Z in proving (118) in [8].

LEMMA 5. *Let* $(G_n)_{n\in N}$ *be as in Lemma 3,* $K^{(j)}$ $(j=1,\ldots,m)$ *the different conjugate fields in* C *of* K *and let* α_j, β_j *be the roots of* $x^2 - A^{(j)}x + B^{(j)}$ $(j=1,\ldots,m)$. *Then there exist for all* $\varepsilon>0$ *constants* c *and* $n_0(\omega)$ *such that for all* $n>n_0(\omega)$

$$M^{n(1-\varepsilon)} \le |N_{K/Q}(G_n)| \le cM^n,$$

where $M = \prod_{j=1}^{m} \max\{|\alpha_j|, |\beta_j|\} > 1$.

PROOF. Let $K=K^{(1)}$. By the assumptions α_1, β_1 and α_1/β_1 are not roots of unity, hence α_j, β_j and α_j/β_j $(j=1,\ldots,m)$ are not too. With the notations

$$a_j = \frac{G_1^{(j)} - \beta_j G_0^{(j)}}{\alpha_j - \beta_j} \quad \text{and} \quad b_j = \frac{G_1^{(j)} - \alpha_j G_0^{(j)}}{\alpha_j - \beta_j} \quad \text{we have}$$

$$G_n^{(j)} = a_j\alpha_j^n - b_j\beta_j^n$$

which immediately implies

$$|G_n^{(j)}| \leq c_j(\max\{|\alpha_j|, |\beta_j|\})^n$$

with a constant c_j. From this one gets the upper bound for $|N_{K/Q}(G_n)|$.

On the other hand, by a result of van der Poorten and Schlickewei [7] there exists for every $\varepsilon > 0$ and $j=1,\ldots,m$ a constant d_j such that if $n > d_j$ then

$$|G_n^{(j)}| \geq (\max\{|\alpha_j|, |\beta_j|\})^{n(1-\varepsilon)}.$$

Hence if $n > \max\{d_1,\ldots,d_m\} = n_0$, then multiplying together the last inequalities for $j=1,\ldots,m$ we get the stated lower bound.

It remains only to prove that $M > 1$. From $\alpha_j\beta_j = B^{(j)}$ $(j=1,\ldots,m)$ we have $|\prod_{j=1}^{m}\alpha_j| \, |\prod_{j=1}^{m}\beta_j| = |N_{K/Q}(B)| \geq 1$. This implies

$$\prod_{j=1}^{m} \max\{|\alpha_j|, |\beta_j|\} \geq \max\{|\prod_{j=1}^{m}\alpha_j|, |\prod_{j=1}^{m}\beta_j|\} \geq 1,$$

where equality holds only if $|N_{K/Q}(B)| = 1$ and $|\alpha_j| = |\beta_j|$ $(j=1,\ldots,m)$. In the exceptional case β_j $(j=1,\ldots,m)$ are units, hence α_j/β_j $(j=1,\ldots,m)$ are

algebraic integers. The coefficients of $Q_j(x) = (x-\alpha_j/\beta_j)(x-\overline{\alpha_j/\beta_j})$ belong to $K^{(j)}$ and they are conjugates of each other. Hence $\prod_{j=1}^{m} Q_j(x) \in Z[x]$ and so all conjugates of α_1/β_1 are roots of this polynomial. On the other hand the absolute value of every root of the last polynomial is 1, therefore they are roots of unity, which contradicts the assumption. This proves the Lemma.

5. PROOF OF THEOREM 3.

PROOF OF THEOREM 3. Let $(G_n)_{n\in N}$ be defined by (1) h, ω and $(G_{i,n})_{n\in N}$ be defined in Lemma 3; $T_k = \prod_{P|B} P^{\nu_p(G_k)}$ and $S_k = G_k/T_k$ for those k with $G_k \neq 0$ while $T_k = (1)$, $S_k = (0)$ for the one possible k with $G_k = 0$. From the easily provable identity

$$G_k^2 - AG_kG_{k-1} + BG_{k-1}^2 = B^{k-1}ab$$

we get

$$(S_k, S_{k-1}) \mid (ab). \tag{3}$$

Let $k = q2h + i$ with $i \in \{0,\dots,2h-1\}$, then $G_k = \omega^q G_{i,q}$, hence by Lemma 3

$$T_k = \omega^q \prod_{P|B} P^{\nu_p(G_{i,q})} = \omega^q T_k^* . \tag{4}$$

Putting $A_1 = (\alpha^{2h} + \beta^{2h})/\omega$ and $B_1 = B^{2h}/\omega^2$, $(G_{i,q})_{n\in N}$ satisfy the difference equation

$$u_{n+2} = A_1 u_{n+1} - B_1 u_n \qquad (n=0,1,\ldots).$$

From $(\alpha^{2h}/\omega,\ \beta^{2h}/\omega) = (1)$ it follows $(A_1^2, B_1) = (1)$. B has only finitely many prime ideal divisors, hence by Lemma 4

$$\nu_p(T_k^*) = \nu_p(G_{i,q}) = O(\log^3 q) \tag{5}$$

for every prime ideal divisor p of B, where the constant implied by O is independent from k.

Let $(R_n)_{n\in N}$ be the recursive sequence with $R_0 = 0$, $R_1 = 1$ which satisfies (1). Take for $k > 0$

$$U_k = \prod_{p|B} p^{\nu_p(G_k)}, \quad V_k = (R_k)/U_k$$

which is meaningful because $R_k \neq 0$ for $k > 0$. Updating (4) and (5) we get

$$U_k = \omega^q U_k^* \tag{6}$$

with

$$\nu_p(U_k^*) = O(\log^3 k) \tag{7}$$

for all $p|B$.

Let now $k_0 \in \mathbb{N}$ be fixed such that $G_k \neq 0$ for $k > k_0$. Let $m, k \in \mathbb{N}$ be chosen so that $m > k > k_0$ and $G_k | G_m$. With $t = m - k$ we have the well-known identity

$$G_m = G_k R_{t+1} - BG_{k-1} R_t ,$$

from which $G_k | BG_{k-1} R_t$ immediately follows. This divisibility relation is by (4) and (6) equivalent to

$$\omega^{[k/2h]} T_k^* S_k \mid \omega^{[(k-1)/2h] + [t/2h]} B S_{k-1} T_{k-1}^* U_t^* V_t .$$

using (3) and $(B, S_k) = (\omega, S_k) = (1)$ one gets from this $S_k | (ab) V_t$ and so

$$S_k T_k^* = G_{i,q} | (ab) V_t T_k^* .$$

Taking conjugates we conclude from this

$$(G_{i,q}^{(j)}) | (ab)^{(j)} V_t^{(j)} T_k^{*(j)} \quad (j = 1, \ldots, m).$$

Hence

$$N_{K/Q}(G_{i,q}) | N_{K/Q}(ab) N(V_t) N(T_k^*)$$

where $N(\ )$ denotes the ideal norm. This implies

$$|N_{K/Q}(G_{i,q})| \leq |N_{K/Q}(ab) N(V_t) N(T_k^*)| . \tag{8}$$

By Lemma 5 there exists for every $\varepsilon > 0$ a q_1 such that if $q > q_1$ then

$$|N_{K/Q}(G_{i,q})| \geq \prod_{j=1}^{m} (\max\{|\alpha_j^{2h}/\omega|, |\beta_j^{2h}/\omega|\})^{q(1-\varepsilon)}$$

holds, and

$$|N(V_t)| \leq |N_{K/Q}(R_t)| \leq c_1 \prod_{j=1}^{m} (\max\{|\alpha_j^{2h}/\omega|, |\beta_j^{2h}/\omega|\})^{[t/2h]} .$$

$|N_{K/Q}(ab)|$ is a constant and by (5)

$$|N(T_k^*)| < \prod_{j=1}^{m} (\max\{|\alpha_j^{2h}/\omega|, |\beta_j^{2h}/\omega|\})^{q\varepsilon} .$$

So one gets from (8) using the last inequalities

$$k(1-2\varepsilon) \geq t + c_2$$

with a from k, m and t independent c_2.

If $(k_s)_{s\in N}$ is a strictly increasing sequence from I(G), then one has from the last inequality $\frac{k_{s+1}}{k_s} \geq 2(1-\varepsilon)$ for all large enough s, and so

$$\liminf_{s\to\infty} \frac{k_{s+1}}{k_s} \geq 2,$$

and this proves Theorem 3.

REFERENCES

[1] BUNDSCHUH, P. and PETHŐ, A.: Zur Transzendenz gewisser Reihen, *Monatshefte Math.* 104, 199-223 (1987).

[2] CARMICHAEL, R.D.: On sequences of integers defined by recurrence relations, *Quart. J. Math.* 48, 343-372 (1920).

[3] DADE, E.C., ROBINSON, D.W., TAUSSKY, O. and WARD, M.: Divisors of recurrent sequences, *J. Reine Angew. Math.* 214/215, 180-183 (1964).

[4] HALL, M.: Divisibility sequences of the third order, *Amer. J. Math.* 58, 577-584 (1936).

[5] HECKE, E.: Lecture on the Theory of Algebraic Numbers, Graduate Texts in Mathematics V. 77, Springer Verlag, New York-Heidelberg-Berlin, 1981.

[6] NIEDERREITER, H.: Some new cryptosystems based on feedback shift register sequences, *Math. J. Okayama Univ.* (to appear).

[7] VAN DER POORTEN, A.J. and SCHLICKEWEI, H.P.: The growth conditions for recurrence sequences, Macquarie Univ. Math. Report 82-0041, North Ryde, Australia, 1982.

[8] SCHNIZEL, A.: On two theorems of Gelfond and some of their applications, *Acta Arith.* 13, 177-236 (1967).

[9] SCHMIDT, W.M.: Simultaneous approximation to algebraic numbers by rationals, *Acta Math.* 125, 189-201 (1970).

[10] SHOREY, T.N. and TIJDEMAN, R.: Exponential Diophantine Equations, Cambridge Univ. Press, Cambridge, 1986.

ATTILA PETHŐ
Mathematical Institute
Kossuth Lajos University
H-4010 Debrecen P.O.Box 12
Hungary

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

ON THE DIOPHANTINE EQUATION $1 + p^{\alpha_1} + p^{\alpha_2} + \ldots + p^{\alpha_k} = y^2$

ROTKIEWICZ A. and ZŁOTKOWSKI W.

We will denote by $\sigma(n)$ the sum of positive divisors of n. Fermat proposed on January 3,1657 to Wallis (see Dickson [3], the following two problems:

I Find n such, that $\sigma(n^3) = t^2$

II Find n such, that $\sigma(n^2) = t^3$

The history of the above problems up to 1918 is presented in Dickson's "History of the Theory of Numbers" Vol.I on pages 54-58 and we will only mention that the least positive composite integer n such that $\sigma(n^3) = t^2$ is $n = 2.3.5.13.41.47$. Ferrier found in 1954 (see [4]) further 20 solutions of the equation in Problem I and 20 solutions of the equation in Problem II, but we do not know whether there exist infinitely many such

solutions.

A. Takaku (see [13]) considered in 1984 the equation $\sigma(p^{\alpha}) = t^2$, where p is a prime number. He proved the following theorem.

Let α be an odd integer greater or equal to 3. Then all prime numbers p such that $\sigma(p^{\alpha})$ is a perfect square satisfy $p < 2^{2^{\alpha+1}}$.

A much stronger theorem follows from the theorem of W. Ljunggren [6] of 1943, who using the results of D. Schepel [10] of 1935 and K. Mahler [7] of 1935 and T. Nagell [8] of 1921 proved that

The diophantine equation

$$\frac{x^n - 1}{x - 1} = y^2 \quad (n > 2)$$

is impossible in integers $x, y, |x| > 1$, except when $n = 4$, $x = 7$ and $n = 5$, $x = 3$.

The above theorem for even n was proved by T. Nagell [8] in 1921. From Ljunggren's theorem we get at once the following.

THEOREM 1. If p is a prime number then all solutions of the given equation $\sigma(p^{\alpha}) = y^2$ are given by $\alpha = 1$, $p = 3$; $\alpha = 3$, $p = 7$ and $\alpha = 4$, $p = 3$.

For odd α we can give the following direct and elementary proof of Theorem 1.

Let $p = 2$; then $\sigma(2^{\alpha}) = 2^{\alpha+1} - 1 \equiv 3 \pmod 4$ and

$\sigma(2^\alpha)$ is not a perfect square. We distinguish two cases:

I. $\alpha + 1 = 2m$, where $2 \nmid m \geq 1$, $p > 3$. We have

$$\frac{p^{2m}-1}{p-1} = t^2, \quad \left(\frac{p^m-1}{p-1}\right)(p^m+1) = t^2, \quad 2 \nmid \frac{p^m-1}{p-1}, \quad (p^m-1, p^m+1) \mid 2,$$

hence $\left(\frac{p^m-1}{p-1}, p^m + 1\right) = 1$. Thus $p^m + 1 = n^2$, $p^m = (n-1)(n+1)$,

$n - 1 = 1$, $n = 2$, $p^m = 3$, hence $m = 1$, $\alpha = 1$, $p = 3$.

II. Let $\alpha + 1 = 2^\beta m, \beta \geq 2$, $p > 3$. We have

$$\frac{p^{2^\beta m} - 1}{p - 1} = \frac{(p^m - 1)(p^m + 1)(p^{2m}+1)\ldots(p^{2^{\beta-1}m}+1)}{p - 1} = t^2.$$

But, since $(p^{2^i m} + 1, p^{2^j m}+1) = 2$ for $i \neq j$ and $\left(\frac{p^m-1}{p-1}, p^{2^k m} + 1\right) = 1$, we have $(p^m + 1)(p^{2m} + 1) = \ell^2$,

$$1 + p^m + p^{2m} + p^{3m} = \ell^2.$$

It follows from the theorem of E. Gerono of 1877 that the only integral solutions of $1 + x + x^2 + x^3 = y^2$ are $(x,y) = (-1,0)$, $(0, \pm 1)$, $(1, \pm 2)$, $(7, \pm 20)$ (see Dickson [3] p. 56), hence $p = 7$, $m = 1$. The same conclusion follows from Theorem 3 B below.

Concerning the equation $1 + x^{\alpha_1} + \ldots + x^{\alpha_k} = y^z$, where x is not restricted to primes, we have the following theorem suggested by B. Brindza acting as the referee

(the original formulation concerned only z = 2).

THEOREM 2. Let $1 \leq \alpha_1 < \alpha_2 < \ldots < \alpha_k$, $\alpha_k > 1$. All solutions of the equation

$$(1) \qquad f(x) = 1 + x^{\alpha_1} + \ldots + x^{\alpha_k} = y^z$$

in $x,y,z \in Z$ with $|y| > 1$, $z > 1$ satisfy $\max\{|x|,|y|, z\} < C$, where C is an effectively computable constant which depends only on $\alpha_1,\ldots,\alpha_k$.

LEMMA 1. If $0 < \alpha_1 < \alpha_2 < \ldots < \alpha_k$, $\alpha_k > 1$ then

$$1 + \sum_{i=1}^{k} x^{\alpha_i} \neq cP(x)^p$$

for every prime p, every polynomial $P \in Z[x]$ and every $c \in Z$.

PROOF. Let $P(x) = \sum_{i=0}^{\ell} b_i x^{\beta_i}$, where $\beta_0 < \beta_1 < \ldots < \beta_\ell$, $b_i \neq 0$. Then

$$P(x)^p = b_o^p x^{p\beta_o} + pb_o^{p-1} b_1 x^{p\beta_o+\beta_1-\beta_o} + \ldots$$

and the equation

$$1 + \sum_{i=1}^{k} x^{\alpha_i} = c\, P(x)^p$$

implies

$$\beta_o = 0,\ \beta_1 = \alpha_1,\ cpb_o^{p-1}b_1 = 1,$$

which is impossible as a congruence mod p.

LEMMA 2. Let p be a prime, $0 < \alpha_1 < \ldots < \alpha_k$.

If $\alpha_k > 1$ and $\alpha_k \equiv 1 \mod (p,2)$ the polynomial

$$1 + \sum_{i=1}^{k} x^{\alpha_i}$$

has at least $(p,2)+1$ zeros of order non-divisible by p.

PROOF (due to J. Browkin and A. Schinzel).

Assume to the contrary that at most $(p,2)$ zeros have the order non-divisible by p. The condition $\alpha_k \equiv 1 \mod (p,2)$ and Lemma 1 imply that

$$f(x) = 1 + \sum_{i=1}^{k} x^{\alpha_i} = c(ax+b)^q g(x)^p,$$

where $a,b,c \in Z$, $g \in Z[x]$ $1 \leq q \leq p$, Clearly $a,b,c \in \{1,-1\}$ and since $f(1) \neq 0$, we may assume without loss of generality that

$$f(x) = (x+1)^q g(x)^p. \tag{2}$$

Let $g(x) = \sum_{j=0}^{\ell} b_j x^{\beta_j}$ $(\beta_0 < \ldots < \beta_\ell)$. Considering the equation (2) mod p we obtain

$$1 + \sum_{i=1}^{k} x^{\alpha_i} \equiv (x+1)^q \sum_{j=0}^{\ell} b_j x^{p\beta_j} \mod p. \tag{3}$$

Comparing the constant terms and the coefficients of x on both sides of (3) we obtain $\beta_0 = 0$,

$$1 \equiv b_o \bmod p,$$

$$0 \text{ or } 1 \equiv qb_o \bmod p,$$

hence $q \equiv 0$ or $1 \bmod p$ and since $1 \leq q < p$ eventually

(4) $\quad q = 1.$

Moreover $\alpha_1 = 1$, $\alpha_{2j+r} = p\beta_j + r$ $(1 \leq j \leq \ell,\ r = 0 \text{ or } 1)$. Therefore

$$(5) \qquad f(x) = 1 + \sum_{i=1}^{k} x^{\alpha_i} = (1+x) \sum_{j=0}^{\ell} x^{p\beta_j}.$$

Since $\alpha_k > 1$, we have $\ell > 0$. Comparing (2) with (4) and (3) we infer that

$$\sum_{j=0}^{\ell} x^{p\beta_j} = g(x)^p,$$

contrary to Lemma 1. The obtained contradiction completes the proof.

PROOF OF THE THEOREM (due to A. Schinzel).

By Lemma 1 $f(x)$ has at least two distinct zeros, hence by the result of [11] the equation (1) with the conditions $|y| > z > 1$, implies $z < z_o$, where z_o is an effectively computable constant. Like other constants mentioned in the sequel z_o depends on $\alpha_1, \ldots, \alpha_k$. Now if

$$f(x) = \prod_{i=1}^{n}(x - x_i)^{r_i},\quad t_i = z/(z,r_i),$$

by virtue of Lemma 2 $\{t_1,\ldots,t_n\}$ is neither a permutation of $\{t,1,\ldots,1\}$ nor of $\{2,2,1,\ldots,1\}$ unless $\alpha_k \equiv z \equiv 0 \bmod 2$. By virtue of the theorems of Siegel [12] and LeVeque [5], made effective by Baker [1] and Brindza [2], all solutions of the equation (1) with a fixed $z > 1$ and $|y|>1$ satisfy

$$\max\{|x|, |y|\} < C(z)$$

unless $\alpha_k \equiv z \equiv 0 \bmod 2$. In the latter case, however, the polynomial $f(x)-y^z$ is irreducible over Q in virtue of Lemma 1 and its highest isobaric part $x^{\alpha_k} - y^z$ factorizes

$$x^{\alpha_k} - y^z = (x^{\alpha_k/2} - y^{z/2})(x^{\alpha_k/2} + y^{z/2}),$$

the two factors being relatively prime. It follows from Runge's theorem [9] that

$$\max\{|x|,|y|\} < C(1).$$

Therefore the theorem holds with

$$C = \max\{z_o, \max_{1 \le z < z_o} C(z)\}.$$

Now, we shall consider the equation

$$1 + p^{\alpha_1} + p^{\alpha_2} + \ldots + p^{\alpha_k} = y^2, \tag{6}$$

where p is an odd prime and $1 \le \alpha_1 < \alpha_2 < \ldots < \alpha_k$, $k > 1$.

We see that equation (6) has the trivial solution

(7) $1 + 3^1 + 3^n + 3^{n+1} + 3^{2n} = (2 + 3^n)^2$ for every $n \geq 2$.

Let p be an odd prime, y a positive integer and

(8) $1 \leq \alpha_1 < \ldots < \alpha_k$, $k > 1$,

(9) $\alpha_2 \geq \ell\alpha_1$, $\alpha_k \leq 2\ell\alpha_1$.

We ignore the trivial solutions given by (7).

We shall prove the following

THEOREM 3.

A) For $\ell = 1$ the equation (6) has no solutions.

B) For $\ell = 2$ the equation (6) has only one solution

(a) $1 + 7 + 7^2 + 7^3 = 20^2$.

C) For $\ell = 3$ the equation (6) has only two solutions

(b) $1 + 3^2 + 3^8 + 3^9 + 3^{11} = 451^2$ and

(c) $1 + 3^3 + 3^{10} + 3^{13} + 3^{14} = 2537^2$.

D) For $\ell = 4$ the equation (6) has only one solution given by (b).

Proof of Theorem 3.

Let $k > 1$. From (6)

$$p^{\alpha_1} + p^{\alpha_2} + \ldots + p^{\alpha_k} = (y - \varepsilon)(y + \varepsilon), \text{ where } \varepsilon = \pm 1.$$

Hence, $y - \varepsilon = p^{\alpha_1} x_1$, $x_1 > 0$. Thus $p^{\alpha_1} + p^{\alpha_2} + \ldots + p^{\alpha_k} = p^{\alpha_1} x_1 (p^{\alpha_1} x_1 + 2\varepsilon)$, $1 + p^{\alpha_2 - \alpha_1} + \ldots + p^{\alpha_k - \alpha_1} = p^{\alpha_1} x_1^2 + 2\varepsilon x_1$

and so

$$(10)\quad p^{\alpha_1}x_1^2 + 2\varepsilon x_1 - (1+p^{\alpha_2-\alpha_1}+\ldots+p^{\alpha_k-\alpha_1}) = 0$$

$$0 < x_1 = \frac{-\varepsilon+\sqrt{1+p^{\alpha_1}+p^{\alpha_2}+\ldots+p^{\alpha_k}}}{p^{\alpha_1}} = -\frac{\varepsilon}{p^{\alpha_1}}+\sqrt{\frac{1}{p^{2\alpha_1-\alpha_k}}+\frac{1}{p^{2\alpha_1-\alpha_{k-1}}}+\ldots}$$

$$<\frac{1}{p}+\sqrt{1+\frac{1}{p^1}+\frac{1}{p^2}+\ldots} \leq \frac{1}{p}+\sqrt{\frac{p}{p-1}} \leq \frac{1}{3}+\sqrt{\frac{3}{2}} < 2$$

Hence $x_1 = 1$, $y = \pm 1 + p^{\alpha_1}$.

If $y = 1 + p^{\alpha_1}$ then $y^2 = (1 + p^{\alpha_1})^2 = 1 + 2p^{\alpha_1} + p^{2\alpha_1}$, which contradicts with (6).

If $y = -1 + p^{\alpha_1}$ then $y^2 = (-1 + p^{\alpha_1})^2 = 1-2p^{\alpha_1} + p^{2\alpha_1} =$

$= 1 + (p-2)p^{\alpha_1} + (p-1)p^{\alpha_1+1}+\ldots+(p-1)p^{2\alpha_1-1}$, which is in a contradiction with (6) for $k > 1$.

Now let $\ell = 2$.

First we shall prove the following

LEMMA 3. If $\alpha_2 \geq 2\alpha_1$, $\alpha_k \leq 4\alpha_1$, the inequality (8) and the equation (6) hold, p is an odd prime, then

$$(11)\quad p \mid 4x_2 + d,$$

$$(12)\quad p^{2\alpha_1-1}x_2^2 + 2p^{\alpha_1-1}x_2 + \frac{4x_2 + d}{p} = 4(p^{\alpha_i-2\alpha_1-1} + \ldots + p^{\alpha_k-2\alpha_1-1}),$$

where $d = 1$, $i = 2$ for $\alpha_2 > 2\alpha_1$ and $d = -3$, $i = 3$ for

$\alpha_2 = 2\alpha_1$ and

a) $x_2 = \pm 1$ or b) $x_2 = -3$, $\alpha_1 = 1$, $p = 3$.

PROOF OF LEMMA 3.

By (10) there exists an integer x_2 such that

(13) $$2\varepsilon x_1 - 1 = p^{\alpha_1} x_2 .$$

If $\alpha_2 \geq 2\alpha_1$, then by (10),

$$\left(\frac{p^{\alpha_1} x_2 + 1}{2}\right)^2 + x_2 - (p^{\alpha_2 - 2\alpha_1} + \ldots + p^{\alpha_k - 2\alpha_1}) = 0. \text{ Hence}$$

(14) $$p^{2\alpha_1} x_2^2 + (2p^{\alpha_1} + 4)x_2 + 1 - 4(p^{\alpha_2 - 2\alpha_1} + p^{\alpha_3 - 2\alpha_1} + \ldots + p^{\alpha_k - 2\alpha_1}) = 0.$$

If $\alpha_2 > 2\alpha_1$ then $p \mid 4x_2 + 1$ and (12) holds for $d = 1$.

If $\alpha_2 = 2\alpha_1$ then $p \mid 4x_2 - 3$ and (12) holds for $d = -3$.

Now, we shall prove that $x_2 = \pm 1$ or $x_2 = -3$, $\alpha_1 = 1$, $p = 3$.

By (14)

$$x_2 = \frac{-(2p^{\alpha_1} + 4) \pm \sqrt{D}}{2p^{2\alpha_1}} \text{ where } D = 16\,(1 + p^{\alpha_1} + \ldots + p^{\alpha_k}). \text{ Thus}$$

$$x_2 = \frac{-p^{\alpha_1} - 2 \pm 2\sqrt{1 + p^{\alpha_1} + \ldots + p^{\alpha_k}}}{p^{2\alpha_1}} = -\frac{1}{p^{\alpha_1}} - \frac{2}{p^{2\alpha_1}} \pm$$

$$\pm\ 2\sqrt{\frac{1}{p^{4\alpha_1-\alpha_k}} + \frac{1}{p^{4\alpha_1-\alpha_{k-1}}} + \ldots + \frac{1}{p^{4\alpha_1}}}\,.$$

If $x_2 > 0$ then, since $4\alpha_1 \geq \alpha_k$, we have

$$x_2 < -\frac{1}{p^{\alpha_1}} - \frac{2}{p^{2\alpha_1}} + 2\sqrt{1 + \frac{1}{p} + \frac{1}{p^2}} + \ldots < 2\sqrt{\frac{3}{2}} < 3.$$

From (13) it follows that x_2 is odd. Thus $x_2 = 1$.

If $x_2 < 0, \alpha_1 > 1$ then $|x_2| < \frac{1}{p^{\alpha_1}} + \frac{2}{p^{2\alpha_1}} + 2\sqrt{\frac{p}{p-1}} \leq \frac{1}{3^2} + \frac{2}{3^4} +$

$+2\sqrt{\frac{3}{2}} < 3$ and $x_2 = -1$.

If $p \geq 5$, $\alpha_1 = 1$ then $|x_2| \leq \frac{1}{p} + \frac{2}{p^2} + 2\sqrt{\frac{p}{p-1}} \leq \frac{1}{5} + \frac{2}{25} + 2\sqrt{\frac{4}{5}} < 3$ and

$x_2 = -1$.

Thus $x_2 = 1$ or $x_2 = -3$, $\alpha_1 = 1, p = 3$ and Lemma 3 is proved.

Proof of Theorem 3B, for $\ell = 2$

By Lemma 2 it is enough to consider the cases $x_2 = \pm 1$ and $x_2 = -3$, $p = 3$, $\alpha_1 = 1$.

Let $x_2 = 1$.

If $\alpha_2 = 2\alpha_1$ then by Lemma 2, $p \mid 4x_2 - 3 = 1$, which is impossible. If $\alpha_2 > 2\alpha_1$ then by Lemma 2, $p \mid 4x_2 + 1 = 5$,

hence p = 5 and by (12)

$5^{2\alpha_1-1} + 2.5^{\alpha_1-1} + 1 = 4(5^{\alpha_2-2\alpha_1-1} + \ldots + 5^{\alpha_k-2\alpha_1-1})$, which is impossible since the left-hand side of the above equality is $\equiv 3, 1 \pmod 5$ and the right-hand side is $\equiv 4, 0 \pmod 5$.

Let $x_2 = -1$.

If $\alpha_2 \equiv 2\alpha_1$ then by Lemma 2, $p \mid 4x_2 - 3 = -7$, $p = 7$ and by (12),

$$(15)\quad 7^{2\alpha_1-1} - 2 \cdot 7^{\alpha_1-1} - 1 = 4(7^{\alpha_3-2\alpha_1-1} + \ldots + 7^{\alpha_k-2\alpha_1-1}).$$

If $\alpha_1 = 1$ we have $\alpha_2 = 2$ and $7-2-1 = 4(7^{\alpha_3-3} + \ldots + 7^{\alpha_k-3})$, $7^{\alpha_3-3} + \ldots + 7^{\alpha_k-3} = 1$, hence $k = 3$, $\alpha_3 = 3$ and we get the solution

$$1 + 7 + 7^2 + 7^3 = 20^2.$$

If $\alpha_1 > 1$ then the left hand side of (15) is $\equiv -1 \pmod 7$ and the right-hand side is $\equiv 0, 4 \pmod 7$.

For $\alpha_2 > 2\alpha_1$, by Lemma 2, $p \mid 4x_2 + 1$, hence $p = 3$ and we have

$$(16)\quad 3^{2\alpha_1-1} - 2 \cdot 3^{\alpha_1-1} - 1 = 4(3^{\alpha_2-2\alpha_1-1} + \ldots + 3^{\alpha_k-2\alpha_1-1}).$$

If $\alpha_1 = 1$ from (16) we get $3 - 3 = 4(3^{\alpha_2-3} + \ldots + 3^{\alpha_k-3})$ which is impossible.

If $\alpha_1 > 1$ then the left-hand side of (16) is $\equiv -1 \pmod 3$ and the right-hand side is $\equiv 0,1 \pmod 3$.

It remains to consider the case $p = 3$, $\alpha_1 = 1$, $x_2 = -3$. For $\alpha_2 > 2\alpha_1$ by Lemma 2 we have $3 \mid 4x_2 + 1 = -11$, which is impossible.

For $\alpha_2 = 2\alpha_1 = 2$, $p = 3$ and by (12),

$$3(-3)^2 + 2.3^0(-3) - 5 = 4(3^{\alpha_3 - 3} + \ldots + 3^{\alpha_k - 3}),\ 3^{\alpha_3 - 3} + \ldots + 3^{\alpha_k - 3} = 4,$$

$\alpha_3 = 3$, $\alpha_4 = 4$ and we get the trivial solution

$1 + 3 + 3^2 + 3^3 + 3^4 = 11^2$. (This solution we get from the identity (7) if we put $n = 2$.)

The proofs of Theorems 3 C and 3D are analogous.

PROBLEM. For any fixed $\ell \geq 1$ find all solutions of the equation $1 + p^{\alpha_1} + p^{\alpha_2} + \ldots + p^{\alpha_k} = y^2$, where p is an odd prime and $\alpha_2 \geq \ell\alpha_1$, $\alpha_k \leq 2\ell\alpha_1$, $1 \leq \alpha_1 < \alpha_2 < \ldots < \alpha_k$.

Postscript by A. Schinzel:

A generalization of the method used by A. Rotkiewicz and W. Złotkowski to prove Theorem 3B of their paper leads to the following result

THEOREM 4. If an odd prime p and positive integers $\alpha_1 < \alpha_2 < \ldots < \alpha_k$ satisfy the conditions (6) and (9) ($\ell \geq 3$)

then we have the following congruences

$$(17)\quad p^{\ell\alpha_1}x+2^{\ell+\lambda-1}\sum_{j=0}^{\ell-1}\binom{1/2}{j}p^{\alpha_1 j}\equiv 0 \pmod{2^{\ell+\lambda-1}}$$

and

$$(18)\quad 2^{\ell+\mu-1}\left(2\binom{1/2}{\ell}+\sum_{i=2}^{k}p^{\alpha_i-\ell\alpha_1}\right)\equiv 2^{1+\mu-\lambda}x \pmod{p^{\alpha_1}},$$

where x is an (odd) integer such that

$$(19)\quad |x|\leq 2^{\ell+\lambda-1}\,\frac{32}{25}$$

Here $\lambda = \mathrm{ord}_2(\ell-1)!$, $\mu = \mathrm{ord}_2\ell!$.

COROLLARY 1. The conditions (6) and (9) have only finitely many solutions for fixed k and $\ell \geq 3$.

COROLLARY 2. For fixed $\ell \geq 3$ and p^{α_1} the conditions (6) and (9) have at most two solutions with $y > 0$.

LEMMA 4. Let $o_n = \mathrm{ord}_2 n!$. The number

$$2^{n+o_n}\binom{1/2}{n} \quad \text{is an odd integer.}$$

PROOF. We have

$$\binom{1/2}{n} = \frac{(-1)^{n-1}(2n-3)!!}{2^n\, n!} \quad (n>1).$$

hence $2^{n+o_n}\binom{1/2}{n}$ is a 2 - adic integer not divisible by 2.

On the other hand

$$2^{2n-2}\, n\binom{1/2}{n} = \binom{2n-3}{n-1} \in Z,$$

$$2^{2n-2}\,(n-2)\binom{1/2}{n} = \binom{2n-3}{n} \in Z$$

thus

$$2^{2n-2}\,(n,2)\binom{1/2}{n} \in Z$$

and $\binom{1/2}{n}$ is a q-adic integer for every odd prime q .

LEMMA 5. For every odd prime p and $\alpha_1 \geq 1$ we have

$$(20)\quad \left(\sum_{j=0}^{\ell-1}\binom{1/2}{j}p^{\alpha_1 j}\right)^2 \equiv 1 + p^{\alpha_1} - 2\binom{1/2}{\ell}p^{\alpha_1 \ell} \bmod p^{\alpha_1(\ell+1)}$$

PROOF. In the p-adic field we have from the Taylor formula

$$\sqrt{1 + p^{\alpha_1}} = \pm \sum_{j=0}^{\infty}\binom{1/2}{j}p^{\alpha_1 j},$$

hence

$$\left(\sum_{j=0}^{\ell}\binom{1/2}{j}p^{\alpha_1 j}\right)^2 \equiv 1 + p^{\alpha_1} \bmod p^{\alpha_1(\ell+1)}.$$

This gives

$$\left(\sum_{j=0}^{\ell-1}\binom{1/2}{j}p^{\alpha_1 j}\right)^2 \equiv 1 + p^{\alpha_1} - 2\binom{1/2}{\ell}p^{\alpha_1\ell}\sum_{j=0}^{\ell-1}\binom{1/2}{j}p^{\alpha_1 j}$$

$$\equiv 1 + p^{\alpha_1} - 2\binom{1/2}{\ell}p^{\alpha_1\ell} \bmod p^{\alpha_1(\ell+1)}.$$

Proof of the theorem 4. Since for odd p the congruence

$$y^2 \equiv 1 + \sum_{i=1}^{k} p^{\alpha_i} \bmod p^{\alpha_1\ell}$$

has only two solutions, we get from (6), (9) and (20)

$$y \equiv \varepsilon \sum_{j=0}^{\ell-1}\binom{1/2}{j}p^{\alpha_1 j} \bmod p^{\alpha_1\ell}, \quad \varepsilon = \pm 1.$$

Multiplying by $2^{\ell+\lambda-1}$ we get, by virtue of Lemma 3, integers on both sides, hence

$$(21)\quad 2^{\ell+\lambda-1}y = p^{\alpha_1\ell}t + \varepsilon 2^{1+\lambda-1}\sum_{j=0}^{\ell-1}\binom{1/2}{j}p^{\alpha_1 j},$$

where t is an integer. We have for $\ell \geq 3$

$$\left|\sum_{j=0}^{\ell-1}\binom{1/2}{j}p^{\alpha_1 j}\right| \leq \frac{11}{216}p^{\alpha_1\ell}$$

hence by (21) for $x = \varepsilon t$

$$|x| \leq \frac{11}{216}\, 2^{\ell+\lambda-1} + 2^{\ell+\lambda-1}\, p^{-\alpha_1 \ell} \sqrt{1 + p^{\alpha_1} + \ldots + p^{\alpha_k}}$$

$$\leq 2^{\ell+\lambda-1} \left(\frac{11}{216} + \sqrt{\frac{3}{2}}\right) \leq 2^{\ell+\lambda-1} \cdot \frac{32}{25}\,.$$

Moreover, x is odd since in (21) the left-hand side is even and the second term on the right-hand side is odd by Lemma 4.

Substituting (21) to (6) and considering it as a congruence mod $p^{\alpha_1(\ell+1)}$ we obtain by Lemma 5

$$2^{\ell+\lambda}\, p^{\alpha_1 \ell}\, x + 2^{2\ell+2\lambda-2} \left(1 + p^{\alpha_1} - 2\binom{1/2}{\ell} p^{\alpha_1 \ell}\right)$$

$$\equiv 2^{2\ell+2\lambda-2} \left(1 + p^{\alpha_1} + \sum_{i=2}^{k} p^{\alpha_i}\right) \bmod p^{\alpha_1(\ell+1)}$$

which after reduction and division by $2^{\ell+2\lambda-\mu-1}\, p^{\alpha_1 \ell}$ gives (18); (17) is an immediate consequence of (21).

PROOF OF COROLLARY 1. Let in the interval $(\ell\alpha_1, (1+\ell)\alpha_1)$ be exactly $r \geq 0$ elements of the sequence α_i. We put

$$\beta_1 = 0,\ \beta_i = \alpha_i - \ell\alpha_1\ (2 \leq i \leq r+1),\ \beta_{r+2} = \alpha_1.$$

Denoting by $\beta_m - \beta_{m-1}$ the maximal difference $\beta_i - \beta_{i-1}$ we obtain

$$\beta_m - \beta_{m-1} \geq \frac{\beta_{r+2} - \beta_1}{r+1} \geq \frac{\alpha_1}{k}.$$

Since

$$\sum_{i=2}^{k} p^{\alpha_i - \ell\alpha_1} \equiv \sum_{i=2}^{m-1} p^{\beta_i} \mod p^{\beta_m}$$

considering the congruence (18) modulo p^{β_m} we obtain

$$2^{\ell+\mu-1}\left(2\binom{1/2}{\ell} + \sum_{i=2}^{m-1} p^{\beta_i}\right) \equiv 2^{1+\mu-\lambda} x \pmod{p^{\beta_m}}.$$

The left-hand side is odd, the right-hand side is even, hence they are different and

$$p^{\beta_m} \leq 2^{\ell+\mu-1}\left(2\binom{1/2}{\ell} + \sum_{i=2}^{m-1} p^{\beta_i}\right) + 2^{1+\mu-\lambda}|x|$$

$$\leq 2^{\ell+\mu}\left(\frac{1}{16} + \frac{3}{4} p^{\beta_{m-1}} + \frac{32}{25}\right) \leq 2^{\ell+\mu}\left(\frac{537}{400} + \frac{3}{4} p^{\beta_m - \frac{\alpha_1}{k}}\right).$$

It follows that

$$p^{\alpha_1/k} \leq 2^{\ell+\mu} \cdot \frac{837}{400} < 2^{\ell+\mu+2}$$

thus

$$p^{\alpha_1} \leq 2^{(\ell+\mu+2)k} \leq 2^{(2\ell+1)k}$$

which implies the assertion.

PROOF OF COROLLARY 2. The congruence (17) determines x uniquely mod $2^{\ell+\lambda-1}$, the congruence (18) gives for x two possible residues mod p, corresponding to $\alpha_2 = \ell\alpha_1$ and $\alpha_2 > \ell\alpha_1$. Hence there are two possible residues of x mod $p \cdot 2^{\ell+\lambda-1}$. However by (19) x lies in the interval of length

$$2^{\ell+\lambda-1} \cdot \frac{64}{25} < 2^{\ell+\lambda-1} p$$

This shows that there are at most two possible values of x. To each of them corresponds by (21) exactly one value of $y > 0$ and ℓ, p^{α_1} and y determine uniquely $\alpha_2, \ldots \alpha_k$.

REMARK. The proof of Theorem 3C reduces almost completely to the determination of all solutions of the systems of conditions (17), (18), (19). Only to exclude the solutions of the system

$$x = -1,\ p = 3,\ \alpha_1 = 2i-3,\ \alpha_j = 3\alpha_1+(2j-3)\ (2 \leq j \leq i),$$

$$x = -9,\ p = 3,\ \alpha_1 = 2i-3,\ \alpha_j = 3\alpha_1+(2j-3)\ (2 \leq j \leq i)$$

one needs a congruence stronger that (18), namely

$$2^{\ell+\nu}\left(2\binom{1/2}{\ell} + p^{\alpha_1}\left(\binom{1/2}{\ell}+2\binom{1/2}{\ell+1} + \sum_{i=2}^{k} p^{\alpha_i-\ell\alpha_1}\right)\right) \equiv$$

$$\equiv 2^{2+\nu-\lambda} x(\ell + \tfrac{1}{2})p^{\alpha_1}) \bmod (p^{2\alpha_1})$$

where $\nu = \mathrm{ord}_2(\ell + 1)!$

REFERENCES

[1] A. BAKER, Bounds for the solutions of the hyperelliptic equation, *Proc. Camb. Phil. Soc.* 65 (1969), 439-444.

[2] B. BRINDZA, On S-integral solutions of the equation $y^m = f(x)$, *Acta Math. Hung.* 44(1984), 133-139.

[3] L.E. DICKSON, History of the theory of numbers, New York 1952.

[4] A. FERRIER, Au sujet de deux problémes de Fermat, *Mathesis* 63 (1954), 291-293.

[5] W.J. LEVEQUE, On the equation $y^m = f(x)$, *Acta Arith.* 9(1964), 209-219.

[6] W. LJUNGGREN, Noen steninger om ubestemts likniger av formen $\frac{x^n - 1}{x - 1} = y^2$, *Norsk Mat. Tidsskr.* 1 Hafte, 25(1943), 17-20.

[7] K. MAHLER, Über den grössten Primteiler spezieller Polynome zweiten Grades, *Archiv for Math. og Naturv.* B. XLI Nr 6 (1935).

[8] NAGELL, Sur l'équation indéterminée $\frac{x^n-1}{x-1} = y^2$, *Norsk. Mat. Forenings Skrifter I*, No. 3(1921), 17 pp.

[9] C. RUNGE, Über ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen, *J. reine angew. Math.* 100(1887),425-435.

[10] D. SCHEPEL, On the Pell equation (Dutch), *Nieuw Arch. Wiskunde* 18(1935), 1-30.

[11] A. SCHINZEL and R. TIJDEMAN, On the equation $y^m=P(x)$, *Acta Arith.* 31(1976), 199-204.

[12] C.L. SIEGEL, The integer solutions of the equation $y^2 = ax^n + bx^{n-1}+...+ k$, *J. Lond. Math. Soc.*, 1(1920), 66-68.

[13] A. TAKAKU, Prime numbers such that the sums of the divisors of their powers are perfect squares, *Colloq. Math.* 49(1984), 117-121.

ROTKIEWICZ, A.

Institute of Mathematics
Polish Academy of Sciences
ul. Śniadeckich 8
00-950 Warszawa, P o l a n d

ZŁOTKOWSKI, W.

Warsaw University in Białystok
ul. Akademicka 2
15-424 Białystok, P o l a n d

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

A P-ADIC ANALOGUE OF THE LEGENDRE SYSTEM

JERZY RUTKOWSKI

1. Let Z_p, Q_p and C_p denote the ring of p-adic integers, the field of p-adic numbers and the completion of the algebraic closure of Q_p respectively. The p-adic integral over Z_p of a function $f:Z_p \to C_p$ can be defined by the following formula

$$I(f)= \lim_{r\to\infty} p^{-r} \sum_{i=0}^{p^r-1} f(i) ,$$

in case the limit exists (see e.g. [3]). In particular it is known that $I(x^n) = B_n$ $(n=0,1,\ldots)$ where B_n is the n-th Bernoulli number.

Using the above p-adic integral we can introduce the inner product in the linear space $C_p[x]$ by

$$\langle f,g\rangle = I(fg) = \lim_{r\to\infty} p^{-r} \sum_{i=0}^{p^r-1} f(i)g(i) \ .$$

In this note we want to present the orthogonalization of the basis $1, x, x^2, \ldots$ of $C_p[x]$. This leads to p-adic analogues of classical Legendre polynomials. The result is as follows

THEOREM. *There exists a sequence* $f_0, f_1, f_2, \ldots$ *of polynomials, determined uniquely up to their signs, such that*

$$\text{(1.1)} \quad \deg f_k = k \qquad (k=0,1,2,\ldots)$$

and

$$\text{(1.2)} \quad \langle f_k, f_\ell\rangle = \delta_{k\ell} \qquad (k,\ell=0,1,2,\ldots)$$

where $\delta_{k\ell}$ *denotes the well known Kronecker symbol. The polynomials* f_n *are defined by*

$$\text{(1.3)} \quad f_n(x) = \sqrt{(-1)^n(2n+1)} \sum_{j=0}^{n} \binom{n+j}{j}\binom{n}{j}\binom{x}{j} \quad (n=0,1,2,\ldots).$$

The first six polynomials of the sequence are

$$f_0(x) = \pm 1, \ f_1(x) = \sqrt{-3}(2x+1), \ f_2(x) = \sqrt{5}(3x^2+3x+1)$$

$$f_3(x) = \frac{1}{3}\sqrt{-7}(10x^3 + 5x^2 + 11x + 3),$$

$$f_4(x) = \pm\frac{1}{4}(35x^4 + 70x^3 + 85x^2 + 50x + 12),$$

$$f_5(x) = \frac{1}{60}\sqrt{-11}(126x^5 + 315x^4 + 560x^3 + 525x^2 + 274x + 60).$$

It is interesting that the sums $\sum_{j=0}^{n}\binom{n+j}{j}\binom{n}{j}\binom{k}{j}$ appear in "real" combinatories (see [2], p. 42).

Note that there always exists a non-zero polynomial $f \in C_p[x]$ such that $\langle f,f\rangle = 0$. For example we can take $f(x) = (3+\sqrt{3})x+1$.

The p-adic Legendre polynomials provide a useful route for obtaining some combinatorial identities. For example, using the expansion of the polynomial $\binom{x}{m}$ we shall prove the following

COROLLARY. For $m > 1$

$$(1.4)\qquad \sum_{i=1}^{m}(2i-1)\binom{m}{i}\binom{-m}{i}^{-1} = 0,$$

for $m \geq 1$

$$(1.5)\qquad \sum_{i=1}^{m}(-1)^i(2i-1)\binom{m}{i}\binom{-m}{i}^{-1} = m$$

and for $m \geq 0$

$$(1.6)\qquad \sum_{i=0}^{m}(-1)^i(2i+1)\binom{m}{i}^2\binom{m+i+1}{i}^{-2} = (m+1)\binom{2m+1}{m}^{-1}.$$

2. PROOF OF THE THEOREM. We shall construct the sequence (f_n) satisfying (1.1) and (1.2).

From (1.1), (1.2) it follows that we are forced to put $f_0 = 1$ or $f_0 = -1$. Let us assume that the first n polynomials $f_0, f_1, \ldots, f_{n-1}$ are already defined. Let us write

$$f_n(x) = a_0 + a_1\binom{x}{1} + \ldots + a_n\binom{x}{n}$$

where the coefficients $a_0, a_1, \ldots, a_n$ are to be determined. The polynomial f_n has to satisfy the following system of equalities

$$(2.1) \quad \langle f_n, f_k \rangle = 0 \qquad (k=0,1,\ldots,n-1)$$

and

$$(2.2) \quad \langle f_n, f_n \rangle = 1$$

which is equivalent to

$$(2.3) \quad I(g_k) = 0 \qquad (k=0,1,\ldots,n-1)$$

and

$$(2.4) \quad I(g_n) = c$$

where g_k are polynomials given by

$$(2.5) \quad g_k(x) = (x+k)\cdot\ldots\cdot(x+1)f_n(x) = \sum_{j=0}^{n}\binom{x+k}{j+k}\frac{(j+k)!}{j!}a_j$$

and c is a suitable non-zero constant which will be defined later.

We start from the evaluation of $I(g_k)$. For $j,k \in N \cup \{0\}$ we have

$$I\left(\binom{x+k}{j+k}\right) = \lim_{r\to\infty} p^{-r} \sum_{i=0}^{p^r-1} \binom{i+k}{j+k} =$$

$$= \lim_{r\to\infty} p^{-r} \binom{p^r+k}{j+k+1} = \frac{(-1)^j\, j!\, k!}{(j+k+1)!} .$$

Now, putting $x_j = (-1)^{j-1} a_{j-1}$ we see that (2.3) and (2.4) are equivalent to the system of equations

$$(2.6) \qquad \sum_{j=1}^{n+1} \frac{1}{j+k} x_j = 0 \qquad (k=0,1,\ldots,n-1)$$

and

$$(2.7) \qquad \sum_{j=1}^{n+1} \frac{1}{j+n} x_j = \frac{c}{n!} .$$

We solve this system by Cramer's roule, namely $x_j = \det A_j / \det A$. The determinant $\det A$ of the last system is of Hankel type and it is known that

$$(2.8) \qquad \det A = \frac{(1!\ 2!\ \ldots\ n!)^3}{(n+1)!(n+2)!\ \ldots\ (2n+1)!} .$$

If $j \in \{1,2,\ldots,n+1\}$ then we have

$$(2.9) \qquad \det A_j = (-1)^{n+j+1} \frac{c}{n!} \det D_{nj} ,$$

where

$$D_{nj} = \begin{bmatrix} 1 & 1/2 & 1/3 & \ldots & 1/(j-1) & 1/(j+1) & \ldots 1/(n+1) \\ 1/2 & 1/3 & 1/4 & \ldots & 1/j & 1/(j+2) & \ldots 1/(n+2) \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 1/n & 1/(n+1) & 1/(n+2) & \ldots & 1/(n+j-2) & 1/(n+j) & \ldots 1/2n \end{bmatrix}$$

According to (2.8) we have

$$(2.10) \qquad \det D_{n,n+1} = \frac{[1!\ 2!\ \ldots\ (n-1)!]^3}{n!(n+1)!\ \ldots\ (2n-1)!} .$$

If $j \in \{1,\ldots,n\}$ then $\det D_{nj}$ can be calculated similarly to $\det A$. Namely, we first multiply each i-th row of D_{nj} by $n+i$ obtaining

$$\det D_{nj} = \frac{n!}{(2n)!} \det(a_{ik}),$$

where (a_{ik}) is the $n \times n$ matrix with

$$a_{ik} = \begin{cases} \dfrac{n+i}{i+k-1} & \text{if} \quad k < j, \\ \dfrac{n+i}{i+k} & \text{if} \quad k \geq j. \end{cases}$$

Then, we subtract the last row from all others. Using the equality

$$\frac{n+i}{i+\ell} - \frac{2n}{n+\ell} = \frac{(n-i)(n-\ell)}{(i+\ell)(n+\ell)}$$

we obtain

$$\det D_{nj} = \frac{n!}{(2n)!} \prod_{i=1}^{n-1} (n-i) \cdot \prod_{\substack{\ell=0 \\ \ell \neq j-1}}^{n-1} \frac{n-\ell}{n+\ell} \cdot \det D_{n-1,j} =$$

$$= \frac{[n!(n-1)!]^2}{(2n)!(2n-1)!} \frac{n+j-1}{n-j+1} \det D_{n-1,j} \cdot$$

The above recurrence, the value $D_{11} = \frac{1}{2}$ and the equality (2.10) imply that for each $j \in \{1,2,\ldots,n+1\}$ we have

$$D_{nj} = \binom{n+j-1}{j-1} \binom{n}{j-1} \frac{[1!\ 2!\ \ldots\ (n-1)!]^3 n!}{(n+1)!(n+2)!\ \ldots\ (2n)!} \cdot$$

Therefore

$$x_j = (-1)^{n+j+1} c \binom{n+j-1}{j-1} \binom{n}{j-1} \frac{(2n+1)!}{(n!)^3} \qquad (j=1,2,\ldots,n+1)$$

and finally

$$(2.11) \quad a_j = (-1)^j x_{j+1} = (-1)^n c \binom{n+j}{j} \binom{n}{j} \frac{(2n+1)!}{(n!)^3} \qquad (j=0,1,\ldots,n).$$

One has to define the constant c. We have

$$\langle f_n, f_n \rangle = 1 \iff \langle f_n, a_n \binom{x}{n} \rangle = 1 \iff a_n \ \langle f_n, \binom{x}{n} \rangle = 1 \iff$$

$$\iff \frac{1}{n!} \ a_n I(g_n) = 1 \ .$$

From the last equality together with (2.11) in the case j=n follows

$$\frac{1}{n!}\,(-1)^n\,c\binom{2n}{n}\,\frac{(2n+1)!}{(n!)^3}\,c = 1.$$

Thus

$$(-1)^n\,c = \sqrt{(-1)^n(2n+1)}\;n!\;(2n+1)^{-1}\binom{2n}{n}^{-1}$$

and finally

$$(2.12)\qquad a_j = \sqrt{(-1)^n(2n+1)}\;\binom{n+j}{j}\binom{n}{j} \qquad (j=0,1,\ldots,n)$$

under the condition that the value of root in all equalities (2.12) is arbitrary but fixed.

The proof is complete.

REMARK. Substituting the obtained values of x_j see (2.11) and (2.12) we get the following combinatorial identities

$$\sum_{j=0}^{n}\frac{(-1)^j}{k+j+1}\binom{n+j}{j}\binom{n}{j} = 0 \qquad (k=0,1,\ldots,n-1)$$

and

$$\sum_{j=0}^{n}\frac{(-1)^j}{n+j+1}\binom{n+j}{j}\binom{n}{j} = (-1)^n\,\frac{(n!)^2}{(2n+1)!}\,.$$

The last identity is very similar to the following identity of Turán:

$$\sum_{j=0}^{n} \frac{(-1)^j}{n+j+1} \binom{n}{j} = \frac{(n!)^2}{(2n+1)!}$$

(see [4], p. 141).

3. PROOF OF THE COROLLARY. We shall find the expansion of the polynomial $\binom{x}{m}$ with respect to our p-adic orthogonal system. For this purpose we have to calculate the p-adic integral $I\left(\binom{x}{m}\binom{x}{n}\right)$.

Using combinatorial identities

$$\binom{x}{m}\binom{x}{n} = \sum_{k=0} \binom{m}{k}\binom{n}{k}\binom{x+k}{m+n}$$

(see [2], p. 24, (10)),

$$(3.1) \qquad \sum_{k=0} (-1)^k \binom{n}{k}\binom{x}{k}\binom{y}{k}^{-1} = \binom{y-x}{n}\binom{y}{n}^{-1}$$

(see [1], p. 443, (76)) and previously obtained equality

$$I\left(\binom{x+k}{\ell}\right) = \frac{(-1)^{\ell-k} k!(\ell-k)!}{(\ell+1)!} =$$

$$= (-1)^{k+\ell}\left[(\ell+1)\binom{\ell}{\ell-k}\right]^{-1}$$

$$(k \in \{0,1,\ldots,\ell-1\})$$

we get

$$I\left(\binom{x}{m}\binom{x}{n}\right) = \sum_{k=0}\binom{m}{k}\binom{n}{k} I\left(\binom{x+k}{m+n}\right) =$$

$$= \sum_{k=0}\binom{m}{k}\binom{n}{k} \frac{(-1)^{m+n+k}}{(m+n+1)\binom{m+n}{k}} =$$

$$= \frac{(-1)^{m+n}}{m+n+1} \sum_{k=0} (-1)^k \binom{m}{k}\binom{n}{k}\binom{m+n}{k}^{-1} =$$

$$= (-1)^{m+n}\left[(m+n+1)\binom{m+n}{n}\right]^{-1} .$$

Therefore

$$(3.2) \qquad I\left(\binom{x}{m}\binom{x}{n}\right) = (-1)^{m+n}\left[(m+n+1)\binom{m+n}{n}\right]^{-1} .$$

From (3.2), (1.3) and (3.1) we get

$$[(-1)^n(2n+1)]^{-1/2} <\binom{x}{m}, f_n(x)> = I\left(\sum_{j=0}^{n}\binom{n+j}{j}\binom{n}{j}\binom{x}{j}\binom{x}{m}\right) =$$

$$= \sum_{j=0}^{n}\binom{n+j}{j}\binom{n}{j}(-1)^{m+j}\left[(m+j+1)\binom{m+j}{j}\right]^{-1} =$$

$$= (-1)^m(m+1)^{-1} \sum_{j=0}^{n} (-1)^j \binom{n}{j}\binom{-n-1}{j}\binom{-m-2}{j}^{-1}$$

$$= (-1)^m(m+1)^{-1}\binom{n-m-1}{n}\binom{-m-2}{n}^{-1} = (-1)^m\binom{m}{n}\left[(m+n+1)\binom{m+n}{n}\right]^{-1} .$$

Thus

$$\binom{x}{m} = \sum_{i=0}^{m} c_i f_i(x) \qquad (m \in N \cup \{0\}) \tag{3.3}$$

where

$$c_i = (-1)^m \binom{m}{i} [(-1)^i (2i+1)]^{1/2} \left[(m+i+1) \binom{m+i}{i} \right]^{-1} . \tag{3.4}$$

$$(i=0,1,\ldots,m)$$

Putting $x = 0$ in (3.3) we get the equality

$$0 = \sum_{i=0}^{m} (-1)^m \binom{m}{i} (-1)^i (2i+1) \left[(m+i+1) \binom{m+i}{i} \right]^{-1} \qquad (m \in N)$$

which gives (1.4).

Similarly, putting $x = -1$ in (3.3) we obtain (1.5).

The third formula (1.6) can be proved as follows. Applying the p-adic Parseval identity to (3.3) we get

$$I\left(\binom{x}{m}^2 \right) = \sum_{i=0}^{m} c_i^2 .$$

Now, an application of (3.2) and (3.4) ends the proof.

REFERENCES

[1] KAUCKÝ, J., Kombinatorické identity, Bratislava, Veda, 1975.

[2] RIORDAN, J., Combinatorial identities, New York, Wiley, 1968.

[3] SCHIKHOF, W.H., Ultrametric calculus, *Cambridge University Press*, 1984.

[4] TURÁN, P., *Matematikai Lapok 7* (1956).

dr. Jerzy RUTKOWSKI

Institute of Mathematics
A. Mickiewicz University
Poznan, P o l a n d

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

BOUNDS FOR ZEROS OF QUADRATIC FORMS

SCHLICKEWEI, H.P. and SCHMIDT, W.M.

1. BOUNDS FOR THE SMALLEST ZERO. Let

$$F(\underline{\underline{X}}) f_{ij} = \sum_{i,j=1}^{n} f_{ij} X_i X_j \neq 0$$

be a quadratic form with real coefficients having $f_{ij} = f_{ji}$. For simplicity we shall assume throughout that F is non-degenerate, although most of the results in this note hold - mutatis mutandis - under much weaker conditions.

In 1955 Cassels [4] showed that *if F has integral coefficients and if it has an integral zero $\underline{\underline{x}} \neq \underline{0}$, then in fact it has a nontrivial integral zero $\underline{\underline{x}}$ with*

$$|\underline{\underline{x}}| \ll F^{(n-1)/2}. \tag{1}$$

Here $|\underline{x}| = \max\{|x_1|,\dots,|x_n|\}$, F is the maximum modulus of the coefficients f_{ij}. Moreover here and in the remaineder of the paper constants in $\ll$ depend only on n. Raghavan [11] extended (1) to the number field case. Birch and Davenport [2] proved the following generalization of (1):

Let Λ *be a lattice in* R^n *of determinant* Δ. *Suppose that*

$$F(\Lambda) \subset Z \tag{2}$$

and that F *has a zero* $\underline{x} \in \Lambda \setminus \{0\}$. *Then it has such a zero satisfying*

$$|\underline{x}| \ll F^{(n-1)/2}\Delta. \tag{3}$$

An example of Kneser (see [4]) shows that (1) and (3) are essentially best possible: given $n > 1$, there are infinitely many forms F with integral coefficients which do have nontrivial integral zeros, and every such zero has

$$|\underline{x}| \gg F^{(n-1)/2}.$$

Now let S be a d-dimensional linear subspace of R^n and Λ be a lattice in R^n. We call S a Λ-rational subspace if $S \cap \Lambda$ is a sublattice Γ of Λ of rank d. A Z^n-rational subspace will be simply called rational

subspace. For a Λ-rational subspace we define the heights H(S) to be the d-dimensional volume of a fundamental parallelepiped of Γ:

$$H(S) = \det(S \cap \Lambda) = \det\Gamma.$$

In 1985 Sclickewei [13] extended the results of Cassels, Birch and Davenport:

THEOREM 1. *Let be a lattice in* R^n. *Suppose* F *satisfies* (2). *Let* $d > 0$. *Suppose moreover that*

(4) F *vanishes on a* d*-dimensional* Λ*-rational subspace* S. *Then there is a* d*-dimensional* Λ*-rational subspace* S *on which* F *vanishes having*

$$H(S) \ll F^{(n-d)/2} \Delta. \tag{5}$$

It is clear that as F is nondegenerate we have in (4) $d \leq (n/2)$. An essential tool in the proof of Theorem 1 is Minkowski's geometry of numbers. Theorem 1 was generalized by Vaaler [19] to number fields.

If we choose a reduced basis of S in Λ we see that Theorem 1 implies that there exist d linearly independent lattice points $\underline{x}_1,\ldots,\underline{x}_d$ with $F(\underline{x}_i) = 0$ $(i = 1,\ldots,d)$ and with

(6) $$|\underline{x}_1| \cdot \ldots \cdot |\underline{x}_d| \ll F^{(n-d)/2} \Delta .$$

In particular we may infer from (6) that there is a lattice point $\underline{x} \neq \underline{0}$ with $F(\underline{x}) = 0$ having

(7) $$|\underline{x}| \ll F^{(n-d)/2d} \Delta^{1/d} .$$

Theorem 1 as well as (6) and (7) are best possible. This was proved by Schmidt [17]. In fact we have

THEOREM 2. *Given* $n > 1$ *and* $0 < d \leq (n/2)$, *there are infinitely many forms* F *with integral coefficients which vanish on a* d*-dimensional rational subspace such that every integral zero* $\underline{x} \neq \underline{0}$ *of* F *has*

(8) $$|\underline{x}| \gg F^{(n-d)/2d} .$$

Since every rational subspace S of dimension d has an integral basis $\underline{x}_1, \ldots, \underline{x}_d$ with

$$|\underline{x}_1| \cdot \ldots \cdot |\underline{x}_d| \gg \ll H(S),$$

Theorem 2 and Theorem 1 complement each other, and therefore both are best possible.

If d divides n, Theorem 2 is obtained via an exten-

sion of Kneser's example [4]. This case was treated by Watson [20]. The case $d \nmid n$ causes much more trouble. Here the reader is refered to Schmidt's paper [17] for more details. (cf. also Schlickewei and Schmidt [16]).

If one wants to apply Theorem 1, the parameter d appearing in (4) sometimes is only given implicitely. Suppose now that F has integral coefficients and is of type (r,s), i.e. $r + s = n$ and F is equivalent over the reals to $X_1^2 + \ldots + X_r^2 - Y_1^2 - \ldots - Y_s^2$. We will assume that

$$r \geq s > 0 \quad \text{and} \quad n = r + s \geq 5. \tag{9}$$

Using a classical theorem of Meyer it can be shown that F vanishes on a d-dimensional rational subspace where

$$d = \begin{cases} s & \text{if } r \geq s + 3 \\ s - 1 & \text{if } r = s + 2 \text{ or } r = s + 1 \\ s - 2 & \text{if } r = s. \end{cases} \tag{10}$$

Put

$$\alpha = \alpha(r,s) = \begin{cases} 1/2 \cdot (r/s) & \text{if } r \geq s + 3 \\ 1/2 \cdot (s + 2)/(s + 1) & \text{if } r = s + 2 \text{ or } r = s + 1 \\ 1/2 \cdot (s + 1)/(s - 2) & \text{if } r = s. \end{cases} \tag{11}$$

Schlickewei [13] derived from Theorem 1 using (10) and an ad hoc argument.

COROLLARY. *Suppose* F *has integral coefficients and is of type* (r,s) *with* (9). *Then* F *has an integral zero* $\underline{x} \neq \underline{0}$ *with*

$$|\underline{x}| \ll F^{\alpha}, \tag{12}$$

where α *is defined in* (11).

It is an easy consequence of Theorem 2 that the exponent α in (12) is best possible if $r \geq s + 3$. Moreover in [17] Schmidt shows that for $n = 5$, $r = 3$, $s = 2$ the exponent $\alpha(3,2) = 2$ is best possible as well. His proof uses p-adic methods. In all the other cases when $r = s + 2$ or $s + 1$ or s, the question of the best possible exponent in (12) remains open.

It should be mentioned that the bounds obtained in (1), (3) and (7) were applied in the context of Oppenheim's conjecture: Let $Q(x_1,\ldots,x_n)$ be a nondegenerate indefinite quadratic form in $n \geq 3$ variables which is not a multiple of an integral form. Then Oppenheim's conjecture says that given $\varepsilon > 0$ there is an integral point $\underline{x} \neq \underline{0}$ satisfying

$$|Q(x_1,\ldots,x_n)| < \varepsilon. \tag{13}$$

Using (3), Birch, Davenport and Ridout showed in a series of papers ([3], [9], [12]) that the conjecture holds true provided $n \geqq 21$. R.C. Baker and Schlickewei [1] could reduce the number of variables needed to 18, 19 and 20 respectively provided that the form Q is of type (r,s) with $\min(r,s) \geqq 9$, $\geqq 8$ or $\geqq 7$ respectively. A major tool in their proof is the use of (7). But naturally all these partial results are exceeded by the celebrated Theorem of Margulis [10] in which Oppenheim's conjecture is proved in full generality even for three variables. His approach is quite different and uses ergodic theory and algebraic groups.

2. BOUNDS FOR BASES CONSISTING OF ZEROS.

Davenport [8] generalized the inequality (3) in a different direction. Again let Λ be a lattice in R^n and suppose that F satisfies (2). He proved that if there exists an $\underline{x} \in \Lambda \setminus \{\underline{0}\}$ with $F(\underline{x}) = 0$, then there exist *two* linearly independent lattice points $\underline{x}_1$, $\underline{x}_2$ with

$$|\underline{x}_1||\underline{x}_2| \ll F^{n-1}\Delta. \tag{14}$$

Chalk [6] generalized (14) to number fields.
The hypothesis in (14) says that (4) is satisfied with $d = 1$. A natural question is to ask what can be shown if

we assume d > 1. This question was studied by Schlickewei and Schmidt ([14],[15]).
A particular instance of their results in [15] is as follows.

THEOREM 3. *Suppose that* F *satisfies* (2) *and* (4). *Then there exist two* Λ*-rational subspaces* S_1, S_2 *on which* F *vahishes having*

$$S_1 \cap S_2 = \{\underline{\underline{0}}\} \quad \textit{and} \tag{15}$$

$$H(S_1) \cdot H(S_2) \ll F^{n-d} \Delta^2 . \tag{16}$$

The proof of Theorem 3 uses geometry of numbers as well as a particular results obtained in [14]. It is clear that Theorem 3 is the natural extension of (14) to the case $d \geq 1$, in fact if d = 1 (16) is identical with (14). An easy consequence of Theorem 3 is that there exist 2d linearly independent lattice points $\underline{\underline{x}}_1, \ldots, \underline{\underline{x}}_{2d}$ with $F(\underline{\underline{x}}_i) = 0$ $(i = 1, \ldots, 2d)$ and

$$|\underline{\underline{x}}_1| \cdot \ldots \cdot |\underline{\underline{x}}_{2d}| \ll F^{n-d} \Delta^2 . \tag{17}$$

Again using Theorem 2 it is seen that Theorem 3 is best possible.

In view of (3) and (14), Davenport raised in [8] the

question whether in analogy with Minkowski's inequality for the successive minima of a convex body with respect to a lattice it is possible to prove the existence of n linearly independent lattice points $\underline{x}_1,\ldots,\underline{x}_n$ with $F(\underline{x}_i) = 0$ $(i = 1,\ldots,n)$ satisfying

$$|\underline{x}_1|\cdot\ldots\cdot|\underline{x}_n| \ll F^{n(n-1)/2}\Delta^n .$$

If we assume (4) to hold, then because of (7) the natural extension of this conjecture should be

$$|\underline{x}_1|\cdot\ldots\cdot|\underline{x}_n| \ll F^{n(n-d)/2d}\Delta^{n/d}. \tag{18}$$

However it was pointed out by Schulze-Pillot [18] that given any function h depending only upon n, F and Δ, there is for each $n \geq 3$ a quadratic form F and a lattice Λ with $F(\Lambda)\subset Z$ such that F has a zero $\underline{x}\in\Lambda\setminus\{\underline{0}\}$, and such that for any n linearly independent zeros of F in Λ we have

$$|\underline{x}_1|\cdot\ldots\cdot|\underline{x}_n| > h(n,F,\Delta). \tag{19}$$

But if we allow for weights in the product, we have:

THEOREM 4. *Suppose that* F *satisfies* (2) *and* (4). *Then there exist linearly independent lattice points*

$\underline{x}_1,\ldots,\underline{x}_n$ *with* $F(\underline{x}_i) = 0 \quad (i = 1,\ldots,n)$ *and*

$$(20)\quad (|\underline{x}_1|\cdot\ldots\cdot|\underline{x}_d|)^{n-d}(|\underline{x}_{d+1}|\cdot\ldots\cdot|\underline{x}_n|^d \ll F^{(n-d)^2}\,\Delta^{2(n-d)}\ .$$

The case d = 1 of this Theorem is due to Schulze-Pillot [18]. For general d it was shown by Schlickewei and Schmidt [15]. It is derived from a more detailed version of Theorem 3 as given in [15] by means of combinatorial arguments.

If in Theorem 4 we have n = 2d, then (20) implies

$$|\underline{x}_1|\cdot\ldots\cdot|\underline{x}_n| = |\underline{x}_1|\cdot\ldots\cdot|\underline{x}_{2d}| \ll F^{n-d}\Delta^2 = F^{n(n-d)/2d}\Delta^{n/d}.$$

Hence in the particular case n = 2d Davenport's conjecture (18) holds true.

Schulze-Pillot's example mentioned in (19) uses lattices Λ which are rather different from $\mathbb{Z}^n$. The situation changes if we restrict ourselves to forms F with integral coefficients and to $\Lambda = \mathbb{Z}^n$. In fact with this assumption we do obtain an inequality for the product of the norms without weights:

THEOREM 5. *Suppose* F *has integral coefficients and vanishes on a* d*-dimensional rational subspace, where* d > 0. *Then there exist* n *linearly independent integral*

zeros $\underline{x}_1,\ldots,\underline{x}_n$ *of* F *satisfying*

$$|\underline{x}_1|\cdot\ldots\cdot|\underline{x}_n| \ll F^{(n^2/2d)-d}. \tag{21}$$

The case d = 1 of Theorem 5 was proved by Schulze-Pillot [18], whereas for arbitrary d > 0 it is due to Schlickewei and Schmidt [15]. Cook and Raghvan [7] proved some variations of Schulze-Pillot's result.

According to Davenport's conjecture (18) one should hope to obtain the exponent $(n^2/2d) - (n/2)$ in (21). Hence the exponents in (18) and (21) are identical only if $n = 2d$. However it turns out that (21) is sharp. In fact Schlickewei and Schmidt [16] proved:

THEOREM 6. *Given* $n \geq 2$, $0<d\leq n/2$, *there are infinitely many quadratic forms* F *with integral coefficients which vanish on a* d*-dimensional rational subspace such that any* n *linearly independent integral zeros* $\underline{x}_1,\ldots,\underline{x}_n$ *of* F *satisfy*

$$|\underline{x}_1|\cdot\ldots\cdot|\underline{x}_n| \gg F^{(n^2/2d)-d}. \tag{22}$$

Notice that the exponent in (21) is the same as that in (22). Therefore both Theorem 5 and Theorem 6 are best possible. And therefore Davenport's conjecture (18) even in the case $\Lambda = Z^n$ holds only true if $n = 2d$, i.e. for

quadratic forms which split up into a direct sum of hyperbolic planes.

REFERENCES

[1] BAKER, R.C. and SCHLICKEWEI, H.P., Indefinite quadratic forms. *Proc. London Math. Soc.* 54 (1987), 385-411.

[2] BRICH, B.J. and DAVENPORT, H., Quadratic equations in several variables. *Proc. Camb. Phil. Soc.* 54 (1958), 135-138.

[3] BIRCH, B.J. and DAVENPORT, H., Indefinite quadratic forms in many variables. *Mathematika* 5 (1958), 8-12.

[4] CASSELS, J.W.S., Bounds for the least solutions of homogeneous quadratic equations. *Proc. Camb. Phil. Soc.* 51 (1955), 262-264.

[5] CASSELS, J.W.S., Addendum to the above paper. *Proc. Camb. Phil. Soc.* 52 (1956), 604.

[6] CHALK, J.H.H., Linearly independnet zeros of quadratic forms over number-fields. *Monatsh. Math.* 90 (1980), 13-25.

[7] COOK, R.J. and RAGHAVAN, S., Small independent zeros of quadratic forms. *Math. Proc. Camb. Phil. Soc.* 102 (1987), 5-16.

[8] DAVENPORT, H., Homogeneous quadratic equations. *Mathematika* 18 (1971), 1-4.

[9] DAVENPORT, H. and RIDOUT, D., Indefinite quadratic forms. *Proc. London Math. Soc.* (3) 9 (1959), 544-555.

[10] MARGULIS, G.A., Indefinite quadratic forms and unipotent flows on homogeneous spaces. To appear.

[11] RAGHAVAN, S., Bounds for minimal solutions of diophantine equations. *Nachr. Akad. Wiss. Göttingen, Math.-Phys. Kl.* 9 (1975), 109-114.

[12] RIDOUT, D., Indefinite quadratic forms. *Mathematika* 5 (1958), 122-124.

[13] SCHLICKEWEI, H.P., Kleine Nullstellen homogener quadratischer Gleichungen. *Monatsh. Math.* 100 (1985), 35-45.

[14] SCHLICKEWEI, H.P., and SCHMIDT, W.M., Quadratic geometry of numbers. *Trans. A.M.S.* 301 (1987), 679-690.

[15] SCHLICKEWEI, H.P., and SCHMIDT, W.M., Isotrope Unterräume rationaler quadratischer Formen. To appear in Math. Zeitschrift.

[16] SCHLICKEWEI, H.P., and SCHMIDT, W.M., Quadratic forms which have only large zeros. To appear. *Monatsh.Math.*105(1988), 295-311.

[17] SCHMIDT, W.M., Small zeros of quadratic forms. *Trans. A.M.S.* 291 (1985), 87-102.

[18] SCHULZE-PILLOT, R., Small linearly independent zeros of quadratic forms. *Monatsh.Math.* 95 (1983), 241-249.

[19] VAALER, J.D., Small zeros of quadratic forms over number fields. *Trans. A.M.S.* 302 (1987), 281-296.

[20] WATSON, G.L., Least solutions of homogeneous quadratic equations. *Proc. Camb. Phil. Soc.* 53 (1956), 541-543.

SCHLICKEWEI, H.P.
Abteilung Mathematik II
der Universität Ulm
Oberer Eselsberg
D-7900 Ulm
Federal Republic of Germany

SCHMIDT, W.M.
Department of Mathematics
University of Colorado
Boulder, Colo. 80309
USA

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

THE NUMBER OF SOLUTIONS OF NORM FORM EQUATIONS

SCHMIDT W.M.

1. It might seem unlikely that a situation could arise in number theory where one can prove the finiteness of a set of integers, yet where one is unable to give a bound on the cardinality of such a set. Yet as A. Schinzel has remarked to me, such a situation arises, e.g., if one is able to show that when an integer n is in a set, then every integer in the set is in fact $<2n$. A situation very much like this occurs in the method of Thue-Siegel-Roth in diophantine approximation.

For instance, Siegel's method shows that when α is algebraic of degree $r \geq 3$, then the possible rational approximations x/y with

$$|\alpha - \frac{x}{y}| < y^{-\mu} \tag{1}$$

with fixed $\mu > \sqrt{2r}$ can only be of two kinds. Either y is in some interval $1 \leq y \leq B = B(\alpha,\mu)$ with explicitly given B--in this case there is no problem-- or possibly y lies in some interval

$$C \leq y \leq C^{D(\alpha,\mu)},$$

where D is given, but we know nothing about C. Thus we have an exponentiated version of the situation above: if y is a solution > B, then any other such solution is $\leq y^D$.

However, luckily we can still give a bound for the number of solutions of (1) by the "gap principle". If x/y and x'/y' are distinct solutions (in reduced form) of (1), and if $y \leq y'$, then

$$\frac{1}{yy'} \leq \left|\frac{x}{y} - \frac{x'}{y'}\right| < y^{-\mu} + y'^{-\mu} \leq 2y^{-\mu},$$

so that

$$y' > \frac{1}{2} y^{\mu-1},$$

and when y is sufficiently large, this certainly will indicate a wide gap between y and y'. So if, say, $C \geq 2$ and $\mu > 3$, solutions $x_1/y_1, \ldots, x_\nu/y_\nu$ of (1) with $C \leq y_1 \leq \ldots \leq y_\nu \leq C^D$ will have $y_{i+1} > \frac{1}{2} y_i^{\mu-1} \geq y_i^{\mu-2}$ and $y_\nu \geq C^{(\mu-2)^{\nu-1}}$, so that $(\mu-2)^{\nu-1} \leq D$ and $\nu \leq 1 + \log D / \log(\mu-2)$.

Unfortunately, the situation is not so good for simultaneous approximation. The main theorem here is the

Subspace Theorem [5] (see also [6]) which may be formulated as follows.

Let $L_1,\ldots, L_n$ be independent linear forms is n variables with real or complex algebraic coefficients. Then given $\delta > 0$, the integer points $\underline{x} = (x_1,\ldots,x_n) \neq \underline{0}$ with

$$|L_1(\underline{x}) \ldots L_n(\underline{x})| < |\underline{x}|^{-\delta} \tag{2}$$

(where $|\underline{x}|$ is the Euclidean norm) lie in finitely many (n-1)-dimensional subspaces.

Recently I proved the following quantitative version. Suppose that $0 < \delta < 1$. Then integer points $\underline{x} \neq \underline{0}$ with

$$|L_1(\underline{x})\ldots L_n(\underline{x})| < |\underline{x}|^{-\delta} |\det(L_1,\ldots,L_n)| \tag{3}$$

lie in the union of the ball

$$|\underline{x}| \leq \max((n!)^{8/\delta}, H), \tag{4}$$

where H is a bound on the "heights" of $L_1,\ldots,L_n$, and of t subspaces, where

$$t \leq (2d)^{2^{\frac{26n-2}{\delta}}}, \tag{5}$$

with d being the degree of the number field containing the coefficients of our linear forms.

The bound (5) is almost certainly too large. In the case n = 2, i.e. for Roth's Theorem, the number of exceptional solutions was recently estimated by Bombieri and

Van der Poorten [2] in a more efficient way, but this is because in this case a recent theorem of Esnault and Viehweg [3], which sor far has not been generalized so as to be applicable to simultaneous approximation, could be used. Now actually, one is usually most interested in the number of solutions of (2) or (3), rather than in the minimum number of subspace which contain these solutions. If a subspace of dimension n-1 is parametrized as $\underline{x} = T\underline{y}$ where $y = (y_1,\ldots,y_{n-1})$, then one is led to $|L_1'(\underline{y}) \ldots L_n'(\underline{y})| < c|\underline{y}|^{-\delta}$, where $L_i'(\underline{y}) = L_i(T\underline{y})$, and if, say, $|L_1'(\underline{y})| \leq \ldots \leq |L_n'(\underline{y})|$, then one is led to

$$|L_1'(\underline{y}) \ldots L_{n-1}'(\underline{y})| < c'|\underline{y}|^{-\delta}.$$

In other words, induction on n suggests itself. However, there is a difficulty with a quantitative argument: since we don't know the subspace, we don't know T, and hence we don't know the heights of the forms $L_1',\ldots,L_{n-1}'$. Thus if we try to apply the quantitative version of the Subspace Theorem, a bound for $|\underline{y}|$ analogous to (4) is up in the air, since we have no bound H' for the heights of $L_1',\ldots,L_{n-1}'$.

Let me illustrate this difficulty by an example. Suppose that $\alpha_1,\ldots,\alpha_n,1$ are linearly independent algebraic numbers, and we wish to count the number of solutions of

$$(6) \qquad |\alpha_i - \frac{x_i}{y}| < \frac{1}{y^{1+(1/n)+\delta}} \qquad (i = 1,\ldots,n)$$

in integers $y,x_1,\ldots,x_n$. With the notation $L_i=\alpha_i y-x_i$ $(i = 1,\ldots,n)$ and $L_{n+1} = y$, the relations (6) when y is sufficiently large imply that

$$|L_1(\underline{x}) \ \ldots \ L_{n+1}(\underline{x})| < |\underline{x}|^{-\delta/2}$$

with $\underline{x} = (x_1,\ldots,x_n,y)$. By the Subspace Theorem (applied with n + 1 in place of n), the solutions either have small norm $|\underline{x}|$, or they lie in one of a few rational subspaces. Let the equation

$$a_1x_1 + \ldots + a_nx_n + by = 0$$

with rational coefficients define such a subspace. Then solutions of (6) in this subspace have

$$|a_1\alpha_1+\ldots+a_n\alpha_n+b| \leq |a_1||\alpha_1-\frac{x_1}{y}|+\ldots+|a_n||\alpha_n-\frac{x_n}{y}|$$

$$+ |a_1\frac{x_1}{y}+\ldots+a_n\frac{x_n}{y}+b| < (|a_1|+\ldots+|a_n|)y^{-1-(1/n)-\delta}.$$

Since $a_1\alpha_1 + \ldots + a_n\alpha_n + b \neq 0$, this gives a bound for y, so that (6) has only finitely many solutions. However, we don't know the subspace, so that we don't know the coefficients $a_1,\ldots,a_n,b$, and hence we cannot give an explicit bound on y, or on the number of solutions of (6).

Now a *norm form* equation is an equation

(7) $$F(\underline{x}) = h,$$

where h is constant and $F(\underline{x}) = F(x_1,\ldots,x_n)$ is a norm form,

$$F(\underline{x}) = a\,N_K(\alpha_1 x_1 + \ldots + \alpha_n x_n) = a\prod_{i=1}^{r}(\alpha_1^{(i)}x_1 + \ldots + \alpha_n^{(i)}x_n),$$

where $a \neq 0$ is in $\mathbb{Q}$, where $\alpha_1,\ldots,\alpha_n$ are linearly independent in an algebraic number field K of degree r, and $\alpha \to \alpha^{(i)}$ $(i = 1,\ldots,r)$ signify the isomorphic embeddings of K into $\mathbb{C}$. We shall further suppose that the coefficients of F (which are necessarily rational) are integers. Some years ago I proved [5] that when the form F is *nondegenerate*, then (7) has only finitely many solutions in integers. I do not wish to give here a definition of a nondegenerate form, but roughly one could say that (7) has only finitely many solutions unless it has infinitely many solutions by Dirichlet's theorem on units. For example, the equation

$$N_K(x_1 + \alpha x_2 + \alpha^2 x_3) = 1$$

with $\alpha = \sqrt[4]{2}$ and $K = \mathbb{Q}(\alpha)$ has infinitely many solutions, for if we set $x_2 = 0$, the equation becomes

$$N_K(x_1 + \alpha^2 x_3) = (N_L(x_1 + \sqrt{2}\,x_3))^2 = (x_1^2 - 2x_3^2)^2 = 1$$

where $L = \mathbb{Q}(\sqrt{2})$, and this has infinitely many solutions

since L has infinitely many units.

Now since the result of [5] was derived with the aid of simultaneous approximation, one might think that there would be no way at present to give an estimate on the number of solutions. However, an explicit estimate may be given. In the special case h = 1 we have the

THEOREM *Suppose* $F(\underline{x})$ *is a non-degenerate norm form. Then the number of solutions of*

$$F(\underline{x}) = 1 \tag{8}$$

is under some bound $B = B(n,r)$. *In particular, one may take*

$$B(n,r) = (2r)^{2^{31n}r^2}.$$

It is remarkable that the bound is independent of the coefficients of F. For the case n = 2, i.e., for a Thue equation

$$F(x,y) = h,$$

the existence of a bound independent of the coefficients of F had been conjectured by Siegel and first proved by Evertse [4], with a better bound recently established by Bombieri and Schmidt [1].

Now let us turn to the proof. When dealing with (8) it is not hard to see that we may suppose

$$F = L^{(1)} \ldots L^{(r)}, \tag{9}$$

where

$$L(\underline{x}) = x_1 + a_2x_2 + \ldots + a_nx_n \tag{10}$$

is a form such that the coefficient of x_1 is 1. We have

BASIC LEMMA A. *Suppose* F *is nondegenerate and of the type indicated above. Suppose* $\underline{x}$ *is a solution of* (8) *which is large, where "large" is defined in terms of the height* H(L) *of* L . *Then there are* $i_1,\ldots,i_n$ *with*

$$|L^{(i_1)}(\underline{x})\ldots L^{(i_n)}(\underline{x})| < \det(L^{(i_1)},\ldots,L^{(i_n)})\,|\underline{x}|^{-\delta},$$

where $\delta = \delta(L) > 0$.

The larger δ is, the better, and in a particular situation one can try to find a rather good value. In general, one may take $\delta = 1/(6r)$. We now apply the quantitative Subspace Theorem. For large solutions, (4) may not arise, so that we are left with t subspaces. Since the field generated by the coefficients of $L^{(i_1)},\ldots,L^{(i_n)}$ is of degree $d \le r^n$, we are left with

$$t \le (2r^n)^{2^{26n}.36r^2} < (2r)^{2^{30n}r^2}$$

subspaces.

The small solutions are dealt with by a different method. We observe that when $T \in SL(n,Z)$ and $F^T(\underline{x}) = F(T\underline{x})$,

the number of solutions of (8) remains unchanged when F is replaced by F^T. We therefore write $F \sim F'$ if $F' = F^T$ for some $T \in SL(n,Z)$. We put $H(F)=H(L)$ when $F=L^{(1)} \ldots L^{(r)}$ as in (9), and

$$H(F) = \min_{F' \sim F} H(F'),$$

where the minimum is over forms $F' \sim F$, again of the type (9), (10). It will suffice to consider forms F which are *reduced* in the sense that $H(F) = H(F)$.

Also, as in the case of Thue equations considered in [1], it is convenient to "jack up the height": there is a simple way to reduce to the situation when $H(F)$ is large, say when

$$H(F) > n^{10n}. \tag{11}$$

BASIC LEMMA B. *Suppose* F *is a norm form as indicated above with* (11). *Then when* $\underline{x}$ *is a solution of* (8), *there are* $i_1,\ldots,i_n$ *with*

$$|L^{(i_1)}(\underline{x}) \ldots L^{(i_n)}(\underline{x})| < \frac{c_1(n)}{H(F)} \det(L^{(i_1)},\ldots,L^{(i_n)}).$$

We cannot go into a proof of this lemma, which is the most important new ingredient. To see how this lemma may be applied, I will first present another version of the "gap principle" on approximations to a number α. Suppose we consider rational approximations x/y in their

lowest terms with

$$|\alpha - \frac{x}{y}| < \frac{1}{Py^2} \tag{12}$$

where $P \geq 4$, say. If x/y and x'/y' are distinct such approximations with $y' \geq y > 0$, then

$$\frac{1}{yy'} \leq |\frac{x}{y} - \frac{x'}{y'}| \leq |\alpha - \frac{x}{y}| + |\alpha - \frac{x'}{y'}| < \frac{2}{Py^2},$$

and

$$y' > (P/2)y.$$

If $x_1/y_1, \ldots, x_\nu/y_\nu$ are such approximations with $0 < y_1 \leq \ldots \leq y_\nu \leq Y$, then $y_j \geq (P/2)^{j-1}$, so that $(P/2)^{\nu-1} \leq y_\nu \leq Y$, and

$$\nu \leq 1 + \frac{\log Y}{\log(P/2)} \leq 1 + 2\frac{\log Y}{\log P} \leq 3\frac{\log y}{\log P}$$

if $Y \geq P$. Since (12) may be written as $|y(\alpha y - x)| < P^{-1}$, the following is a generalization.

LEMMA C. *Suppose* $n!^4 \leq P \leq Y$, *and put* $Q = \log Y/\log P$. *Consider integer solutions of*

$$|L_1(\underline{x}) \ldots L_n(\underline{x})| < P^{-1}|\det(L_1, \ldots, L_n)|,$$

where $L_1, \ldots, L_n$ *are independent linear forms in* n *variables with real coefficients. Solutions of this inequality with*

$$|\underline{x}| \leq Y$$

lie in the union of not more than $c_2(n)Q^{n-1}$ *proper subspaces.*

As for the proof, write (L,M) for the inner product of the coefficient vectors belonging to L, M. One reduces the problem to the situation when

$$(L_i, L_j) = \delta_{ij} \qquad \text{(the Kronecker Symbol)}.$$

Then $|\underline{x}| \leq Y$ implies

$$|L_i(\underline{x})| \leq Y,$$

and we have

$$(13) \quad |L_1(\underline{x}) \ldots L_n(\underline{x})| < \frac{1}{P} = \frac{1}{n!C^{n-1}} \text{ with } C = \left(\frac{P}{n:}\right)^{1/(n-1)}.$$

The solutions either satisfy

$$(14) \qquad |L_i(\underline{x})| < \frac{1}{n!\,Y^{n-1}} \quad \text{for some } i.$$

Then if $\underline{x}_1, \ldots, \underline{x}_n$ are such solutions with fixed i,

$$(15) \qquad \det(\underline{x}_1, \ldots, \underline{x}_n) = \det(\underline{x}_1, \ldots, \underline{x}_n)\det(L_1, \ldots, L_n)$$

$$= \begin{vmatrix} L_1(\underline{x}_1) & \ldots & L_n(\underline{x}_1) \\ & & \\ L_1(\underline{x}_n) & \ldots & L_n(\underline{x}_n) \end{vmatrix} < n!Y^{n-1} \frac{1}{n!Y^{n-1}} = 1.$$

So $\det(\underline{x}_1, \ldots, \underline{x}_n) = 0$. So all the solutions with (14)

for a fixed value of i are linearly dependent; they lie in a subspace. If (14) does not hold, then

$$YC^{-R} = \frac{1}{n!Y^{n-1}} \leq |L_i(\underline{x})| \leq Y$$

with

$$R = \frac{\log(n!Y^n)}{\log C} << Q.$$

Say

$$YC^{-p_i-1} \leq |L_i(\underline{x})| \leq YC^{-p_i},$$

with integers p_i in $0 \leq p \leq R$. Say this holds for $i = 1,\ldots,n-1$ and fixed $p_1,\ldots,p_{n-1}$. Then by (13),

$$|L_n(\underline{x})| < \frac{1}{n!C^{n-1}|L_1(\underline{x})\ldots L_{n-1}(\underline{x})|} < \frac{C^{p_1+\ldots+p_{n-1}}}{n!Y^{n-1}}.$$

Again the product of elements from the n columns of the center determinant in (15) is

$$<YC^{-p_1} \ldots YC^{-p_{n-1}} \frac{C^{p_1+\ldots+p_{n-1}}}{n!Y^{n-1}} = \frac{1}{n!},$$

so that the determinant has modulus <1, hence is 0. The solutions with given $p_1,\ldots,p_{n-1}$ lie in a fixed subspace. But the number of possibilities for $p_1,\ldots,p_{n-1}$ is

$$<<R^{n-1} \quad <<Q^{n-1}.$$

The small solutions of (8) are those with $|\underline{x}|$ small

as compared to the height $H(F)$; more precisely, $|\underline{x}| \leq H(F)^{6n^2r^{n+1}}$. In view of Basic Lemma B we may apply Lemma C with $P = H(F)/c(n) \approx H(F)$ (we are sloppy in this lecture) and with $Y = H(F)^{6^2r^{n+1}}$, so that $Q = 6n^2r^{n+1}$. Thus $H(F)$ (and hence all reference to the coefficients of F drops out, and we are left with $\leq c(n)Q^{n-1}$ subspaces.

Combining our results for the large and the small solutions, we see that all the solutions lie in not more than $t_1 = t_1(n,r)$ subspaces of dimension n-1. After introducing parameter representations of these subspaces, we are led to at most t_1 norm form equations in n-1 variables. Since being non-degenerate is unaffected by our substitutions, we now may apply induction, either by reducing to the trivial case n = 1, or to the case n=2 of Thue equations treated in earlier work.

Among the questions which should be taken up next is the dependency of the number of solutions of (7) on h, as well as a treatment of degenerate equations. For degenerate equations, the solutions lie in a finite number of "families of solutions" (or "orbits"), and one should estimate the number of such families.

Detailed proofs will be given in [7] , [8].

REFERENCES

[1] E. BOMBIERI and W.M. SCHMIDT. On Thue's equation. *Invent. Math.* 88, 69-81 (1987).

[2] E. BOMBIERI and A.J. van der Poorten. Some quantitative results related to Roth's Theorem. *MacQuarie Univ. Reports* 1987.

[3] H. ESNAULT and E. Viehweg. Dyson's Lemma for polynomials in several variables (and the theorem of Roth). *Invent. Math.* 78, 445-490 (1984).

[4] J.H. EVERTSE. Upper bounds for the number of solutions of diophantine equations. *Math. Centrum Amsterdam*, 1-127 (1983).

[5] W.M. SCHMIDT. Norm form equations. *Ann. of Math.* 96, 526-551(1972).

[6] W.M. SCHMIDT. Diophantine Approximation. *Springer Lecture Notes*, 785 (1980).

[7] W.M. SCHMIDT. The Subspace Theorem in Diophantine Approximation. Compositio Math(to appear).

[8] W.M. SCHMIDT. The number of Solution of Norm Form Equations. Transactions A.M.S.(to appear).

SCHMIDT, W.M.

Dept. of Math.
Univ. of Colorado
Boulder, Colo 803090426

U S A

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

THE NUMBER OF SOLUTIONS OF DIOPHANTINE EQUATIONS

R. TIJDEMAN

0. INTRODUCTION

In two recent papers [4], [30], Erdős, Stewart and the author showed that certain diophantine equations have many solutions. In this way they indicated how far certain results are capable for improvements at most. First we mention some relevant results from the literature on upper bounds for the numbers of solutions of diophantine equations and then we sketch how our method leads to opposite results.

1. THUE AND THUE-MAHLER EQUATIONS

Let $f(x,y) = a_0x^n + a_1x^{n-1}y + \ldots + a_ny^n \in \mathbf{Z}[x,y]$ be a binary form (i.e. homogeneous polynomial) of degree

$n \geq 3$. Put $A := \max_{j=0,\ldots,n} |a_j|$. Let $m \in \mathbf{Z}$ be non-zero. In 1908 Thue [31] proved that, for irreducible polynomials f, the equation

$$(1) \qquad f(x,y) = m$$

has only finitely many solutions in $x,y \in \mathbf{Z}$ and in 1929 Siegel [26] showed that there exists an explicit upper bound for the number of solutions of (1). An equation of type (1) is said to be a Thue equation.

Thue's result was extended by Mahler in 1933. Let $p_1,\ldots,p_s$ be distinct prime numbers. Consider the equation

$$(2) \qquad f(x,y) = p_1^{z_1} \ldots p_s^{z_s}.$$

in $x,y \in \mathbf{Z}$, $z_1, z_2, \ldots, z_s \in \mathbf{Z}_{\geq 0}$ with $\gcd(x,y) = 1$. Mahler [17] proved that, for irreducible f, equation (2) has at most c_1^{s+1} solutions where c_1 is some number depending only on f. An equation of type (2) is said to be a Thue-Mahler equation. Without much trouble the condition 'f is irreducible' can be relaxed to 'f has at least three distinct linear factors in its factorisation over the complex numbers'.

Here we list some out of several upper bounds for the numbers of solutions of Thue and Thue-Mahler equations. In 1955 Davenport and Roth [3] proved that, for irreducible f, equation (1) has at most

$$(4A)^{2n^2}\,|m|^3 + e^{643n^2}$$

solutions (x,y). Lewis and Mahler [15] showed that, for f with non-zero discriminant, equation (2) has at most

(3) $$c_2(An)^{c_3\sqrt{n}} + (c_4 n)^{s+1}$$

solutions $(x,y,z_1,\ldots,z_s)$ with $\gcd(x,y) = 1$. Here c_2, c_3, c_4 are constants of the order of magnitude of 100. In 1984 Evertse [6] proved this result with (3) replaced by

(4) $$e^{n^3(4s+7)}$$

The fact that this bound is independent of f confirmed an old conjecture of Siegel. The dependence on n was greatly improved by Bombieri and Schmidt [1] for the Thue equation. They proved that, for irreducible f, equation (1) has at most

$$c_5 n^{s+1}$$

relatively prime solutions (x,y). Here c_5 may be of the order of magnitude of 10^6 in general, but it can be taken to be 215 for sufficiently large n.

There are a number of related results which we only briefly indicate. There are upper bounds for the number of solutions beyond some bound (see e.g. Mahler [19]), for the number of solutions of equation (2) in case about

f only the degree and the splitting field is given (see Evertse and Győry [8]), for the number of solutions of Thue-Mahler equations over algebraic number fields (see Evertse [6]), and for the sizes of the solutions themselves (see e.g. Győry [11]). Recently Schmidt and Mueller gave upper bounds for the number of solutions of (1) in terms of the number $v + 1$ of non-zero coefficients of f. Schmidt [24] proved that, for irreducible f. the inequality $|f(x,y)| \leq m$ has at most

$$c_6(nv)^{1/2} m^{2/n}(1 + \log m^{1/n})$$

solutions (x,y) and Mueller and Schmidt [20] showed that the upper bound can be replaced by

$$c_7 v^2 m^{2/n}(1 + \log m^{1/n}) .$$

2. S-UNIT EQUATIONS IN TWO VARIABLES

Let $p_1, \ldots, p_s$ be given prime numbers with (2≤) $Q \leq p_1 < p_2 < \ldots < p_s \leq R$. Put

$$S = \{p_1^{k_1} \ldots p_s^{k_s} : k_1, \ldots, k_s \in \mathbf{Z}_{\geq 0}\} .$$

Equation (2) can now be written as $f(x,y) \in S$. From his result on equation (2), Mahler [16] derived that the equation

(5) $\qquad x + y = z \quad \text{in } x,y,z \in S \quad \text{with} \quad \gcd(x,y,z) = 1$

has only finitely many solutions. Twenty-eight years later Lewis and Mahler [15] proved that the number of solutions of (5) is at most

$$\left(c_8 s \frac{\log R}{\log Q}\right)^s + c_9^{s+1},$$

where c_8 and c_9 are explicitly given constants. In 1984 Evertse [6] and Silverman [28], independently of each other, showed that the dependence on Q and R is not necessary by proving that (5) has at most c_{10}^{s+1} solutions where c_{10} is some absolute constant. Evertse generalized this result to the equation

(6) $\qquad ax + by = cz \quad \text{in} \quad x,y,z \in S \quad \text{with} \quad \gcd(x,y,z) = 1$

where a,b and c are fixed positive rational integers. He proved that, for any a,b,c, equation (6) has at most $3 \times 7^{2s+3}$ solutions. Note that this bound is independent of a,b and c. Last year Evertse et al. [10] showed that an equation (6) having many solutions is rather exceptional. Without loss of generality we may assume that $\gcd(a,b,c,p_1,\ldots,p_s) = 1$. They showed that there are only finitely many triples (a,b,c) subject to this

assumption such that (6) has more than 2 solutions with x,y,z positive (cf. [9] §5). For this result and generalisations to the more general S-unit equation

$$(7) \qquad a_0x_0 + a_1x_1 + \ldots + a_nx_n = 0 \text{ in } x_0,\ldots,x_n \in S,$$

I refer to the paper of Evertse and Győry [7] in the same Proceedings.

It may not be clear why (5), (6) and (7) are called S-unit equations. By definition a rational S-integer is a number of the form x/s with $x \in \mathbf{Z}$, $s \in S$. The units in the ring of S-integers are called S-units. Hence a rational S-unit is a number of the form $\pm s_1/s_2$ with $s_1, s_2 \in S$. Obviously, equation (6) is equivalent to the S-unit equation $a\xi + b\eta = c$ in the two S-unit variables ξ and η. So (5), (6) and (7) are just homogeneous forms of linear S-unit equations. S-unit equations are closely linked with Thue-Mahler equations. For example, there are only 3^S possibilities for the cubefree part A of $x \in S$ and also 3^S possibilities for the cubefree part B of $y \in S$. Hence all solutions of (5) can be found by solving 3^{2S} Thue-Mahler equations

$$Ax^3 + By^3 \in S .$$

Moreover, (5) is equivalent to the Thue-Mahler equation $xy(x + y) \in S$. Conversely, any Thue-Mahler equation can

be reduced to finitely many S-unit equations. The notion of S-units is particularly useful in cases where the ground field is not Q, but an arbitrary algebraic number field or some other finitely generated field of characteristic 0.

3. INTEGER SUMS COMPOSED OF FIXED PRIMES

Let $a_1, \ldots, a_k$ be distinct positive integers. Let $\omega(x)$ denote the number of distinct prime factors of x. In 1934 Erdős and Turán [5] proved that

$$\omega\Big(\prod_{i=1}^{k}\prod_{j=1}^{k}(a_i + a_j)\Big) \geq \frac{1}{\log 2}\log k\ .$$

They wondered whether similar results can be obtained for products $\prod_{i=1}^{k}\prod_{j=1}^{k}(a_i + b_j)$, where $b_1, \ldots, b_k$ is another set of distinct positive integers. In 1986 Győry et al. [12] solved their problem by showing that even

$$\omega\Big(\prod_{i=1}^{k}\prod_{j=1}^{2}(a_i + b_j)\Big) \geq c_{11}\log k \tag{8}$$

where c_{11} is some positive constant. A survey of related results can be found in Stewart and Tijdeman [29].

There is a straightforward connection between this problem and the S-unit equation (6). Suppose

$\prod_{i=1}^{k} \prod_{j=1}^{2}(a_i + b_j)$ is composed of the primes $p_1, \ldots, p_s$. Then the equation

$$x - y = c, \quad c = b_2 - b_1$$

has k solutions, $x = a_i + b_2$, $y = a_i + b_1$ for $i = 1,\ldots,k$. However, by Evertse's result on equation (6), we know that there are at most $3 \times 7^{2s+3}$ coprime solutions (x,y). One essential point here is that this upper bound does not depend on c.

4. THE MASSER-OESTERLÉ CONJECTURE

In recent years some problems and conjectures on diophantine inequalities have been posed which have important connections with algebraic geometry (cf. Serre [25]). Ribet [23] has proved that the so-called Taniyama-Weil conjecture implies Fermat's Last Theorem. In connection with this implication, Oesterlé posed the problem of proving the existence of constants c_{12} and c_{13} such that if

(9) $\quad a + b = c$ with $a,b,c \in \mathbb{Z}_{>0}$ and $\gcd(a,b,c) = 1$

then

$$c \leq c_{12} \prod_{p \mid abc} p^{c_{13}}.$$

Put $G = \prod_{p|abc} p$. Let $\ll$ be the Vinogradov symbol. Then the inequality is equivalent to

$$c \ll G^{c_{13}} \quad . \tag{10}$$

Masser even conjectured that, for any $\varepsilon > 0$, (9) implies

$$c \ll_\varepsilon G^{1+\varepsilon} \quad . \tag{11}$$

This is now called the Masser-Oesterlé conjecture or the abc-conjecture. There is also the slightly weaker conjecture

$$abc \ll_\varepsilon G^{3+\varepsilon} \tag{12}$$

in the literature. This conjecture implies a conjecture of Szpiro on elliptic curves. To indicate the connection of conjectures (10), (11) and (12) with Fermat's Last Theorem, suppose x,y and z are relatively prime positive integers such that $x^n + y^n = z^n$. Then, provided that (9) implies (10),

$$(xyz)^n = x^n y^n z^n \ll G^{3c_{13}} \le (xyz)^{3c_{13}} \quad ,$$

hence n is bounded. Similarly (12) implies that $n < 4$ if xyz is sufficiently large. For a survey of such conjectures and their implications, see Vojta [32], Appendix ABC of Chapter 5.

Using a p-adic version of Baker's estimate on linear forms in logarithms of algebraic numbers, Stewart and Tijdeman [30] derived that (9) implies the rather weak inequality

$$\log c \ll G^{15} ,$$

but this is the best result we know. In this case both van der Poorten's p-adic version [22] and Yu's p-adic version [34] are applicable.

5. THE MASSER-OESTERLÉ CONJECTURE (CONTINUED)

Stewart and I wondered how large c can be made with respect to G, that is how sharp the Masser-Oesterlé conjecture is. Actually, we had no hope to be able to prove it, so we tried to disprove it.

Let $\psi_o(x,y)$ be the set of all positive odd integers at most x composed of primes at most y. By the box principle, there are two elements $a < c$ in this set such that

$$2^{\left\lfloor \frac{\log \psi_o(x,y)}{\log 2} \right\rfloor} \mid c - a .$$

Without loss of generality we may assume that $\gcd(a,c) = 1$. Put $b = c - a$. Then $a + b = c$ and $\gcd(a,b,c) = 1$. Moreover

$$G = \prod_{p \mid abc} p \le \Big(\prod_{p \le y} p\Big) \frac{b}{2^{\left[\frac{\log \psi_0(x,y)}{\log 2}\right]-1}} \le$$

$$\le \frac{4c}{\psi_0(x,y)} \prod_{p \le y} p \,.$$

The surprising fact is that

$$\min_{1 \le y \le x} \frac{\prod_{p \le y} p}{\psi_0(x,y)}$$

is rather small. On taking $y = \sqrt{\log x}$ an elementary estimation yields that, for any $\delta > 0$, there exist infinitely many positive integers a,b and c such that $a + b = c$, $\gcd(a,b,c) = 1$ and

$$G \le c \exp(-(4 - \delta) \sqrt{\log c / \log\log c}) \,,$$

or, equivalently,

(13) $$c \ge G \exp((4 - \delta)\sqrt{\log G / \log\log G}),$$

see Stewart and Tijdeman [30]. The exponential factor in (13) grows much faster than any constant power of log G, but not as fast as G^{ε} required to disprove the Masser--Oesterlé conjecture (11).

Masser himself has shown to the author how to prove a comparable result opposite to the conjecture (12):

There exist positive integers a,b,c as above such that, for any N,

$$abc \gg_N G^3(\log G)^N .$$

It is likely that this result can be sharpened.

For some numerical examples related to the Masser--Oesterlé conjecture, see De Weger [33] section 5E.

6. INTEGER SUMS COMPOSED OF FIXED PRIMES (CONTINUED)

It is obvious that the important input in the derivation of (13) is the behaviour of the function $\psi_0(x,y)$. Dickson, Ramaswami, Buchstab, De Bruijn, Norton, Hildebrand and others have made an extensive study of the function

$$\psi(x,y) = \{n \leq x : P(n) \leq y\}$$

where $P(n) = \max_{p|n} p$ (see Norton [21] and Hildebrand and Tenenbaum [14]). For extreme values of y the behaviour of $\psi(x,y)$ is relatively simple, but only very recently Hildebrand and Tenenbaum [14] established the complete asymptotic behaviour of $\psi(x,y)$ over the full range of y. We only need lower bounds. If $y \leq (\log x)^{1-\varepsilon}$ then elementary estimates are sufficiently sharp. This was the case in our deduction of inequality (13). However,

for $y > \log x$ the behaviour of $\psi(x,y)$ is totally different. The lower bound of Hildebrand and Tenenbaum is not suitable for our purposes, but for $y \geq (\log x)^{1+\varepsilon}$ a useful lower bound has been obtained by Canfield, Erdős and Pomerance [2]: For $u \geq 3$

$$(14) \qquad \psi(x,x^{1/u}) \geq x \exp\{-u(\log u + \log\log u - 1 + c_{14} \frac{\log\log u}{\log u})\}$$

where c_{14} is some constant.

In the sequel of my paper I shall report on joint work with Erdős and Stewart [4]. Recall result (8) of Győry et al. How sharp is this estimate? Consider the $\psi(x,y)$ positive integers at most x composed of primes at most y. There are $\binom{\psi(x,y)}{2}$ pairs of such integers and x possible differences, hence there is some b such that

$$k := \binom{\psi(x,y)}{2}/x \geq (\psi(x,y))^2/3x$$

pairs have exactly difference b. Call these pairs $(a_1, a_1 + b), \ldots, (a_k, a_k + b)$ with $a_1 < \ldots < a_k$. Then

$$\omega(\Pi_{i=1}^{k}(a_i(a_i + b)) \leq \pi(y) .$$

Again, the difficulty is to make the best choice for y. The surprising fact is that the choice $y = ((\log x)/2)^2$ led to a much better result than we expected. Using (14) we obtained

$$P(\Pi_{i=1}^{k}(a_i(a_i+b)) < ((1+\varepsilon)\frac{\log k}{2}\log(\frac{\log k}{2}))^2 \text{ for } k \geq k_0(\varepsilon)$$

which implies that there are infinitely many choices of $a_1, \ldots, a_k$ and b such that

$$(15) \qquad \omega(\Pi_{i=1}^{k} a_i(a_i+b)) < (\frac{1}{8}+\varepsilon)(\log k)^2 \log\log k.$$

Thus (8) is not bad at all. It is consistent with a conjecture of Stewart, to be mentioned in the next section, to guess that the right order of magnitude is $(\log k)^{3/2}$.

We further studied what happens if ℓ becomes larger than 2. I shall only indicate the power of our results. As long as $\ell/\log k \to 0$ we found the existence of infinitely many sets $\{a_1, \ldots, a_k\}$ and $\{b_1, \ldots, b_\ell\}$ of positive integers such that

$$(16) \qquad P(\prod_{i=1}^{k}\prod_{j=1}^{\ell}(a_i+b_j)) < ((1+\varepsilon)\frac{\log k}{\ell}\log(\frac{\log k}{\ell}))^{\ell}$$

$$\text{for } k \geq k_1(\varepsilon,\ell) .$$

If $\ell \sim \theta \log k$ for some constant θ with $0 < \theta < 1$, then the upper bound can still be made k^η with $\eta = \eta(\theta) < 1$. For ℓ around $\log k$ a bound ηk with $0 < \eta < 1$ is still possible. For larger values of ℓ nothing better than the trivial

bound $k + \ell$ could be obtained. This bound can be reached if we take $a_i = i$ and $b_j = j$ for all i and j. A simple example due to Ruzsa shows that it is possible that

$$\omega\Big(\prod_{i=1}^{k}\prod_{j=1}^{\ell}(a_i + b_j)\Big) < \pi(k+\ell)$$

even if $\ell = k$. Ruzsa's choice is $k = \ell = 4$, $a_1 = b_1 = 1$, $a_2 = b_2 = 2$, $a_3 = b_3 = 4$, $a_4 = b_4 = 8$. I conjecture that, for any $\varepsilon > 0$,

$$\omega\Big(\prod_{i=1}^{k}\prod_{j=1}^{\ell}(a_i + b_j)\Big) \gg_\varepsilon k^{1-\varepsilon}$$

when $\ell = k$. Perhaps this inequality is even valid for $\ell > (\log k)^{1+\varepsilon}$.

7. S-UNIT EQUATIONS IN TWO VARIABLES (CONTINUED)

Looking more closely to the proof of (15), we see that b can be chosen such that $b < \exp(\log k \operatorname{loglog} k)$. Thus $\omega(b) \ll \log k$ whence

$$\omega\Big(b\prod_{i=1}^{k} a_i(a_i + b)\Big) < \Big(\frac{1}{8}+\varepsilon\Big)(\log k)^2 \operatorname{loglog} k$$

for $k \geq k_2(\varepsilon)$.

The equation $x+y=z$ can therefore have at least k solutions in positive integers $x=a_i, y=b, z=a_i+b$ with all prime factors of xyz from a set of $(\log k)^2 \operatorname{loglog} k$ prime numbers. Put $d_i=\gcd(a_i,b)$. Then $x=a_i/d_i, y=b/d_i, z=(a_i+b)/d_i$ $(i=1,\ldots,k)$ are k distinct triples satisfying

$$x+y=z \text{ and } \gcd(x,y,z)=1.$$

Putting $s \approx (\frac{1}{8}+\varepsilon)(\log k)^2 \operatorname{loglog} k$, we obtain that (5) can have as many as

$$k \geq \exp((4-\varepsilon)(\frac{s}{\log s})^{1/2})$$

solutions. This shows that Evertse's upper bound $3 \times 7^{2s+3}$ is not far from the best possible. Stewart has made a heuristic analysis which shows that $\exp(s^{2/3})$ might be the right order of magnitude.

8. THUE AND THUE-MAHLER EQUATIONS (CONTINUED)

Consider (16) with $n := \ell$ fixed. Put

$$f(x) = (x+b_1)(x+b_2)\ldots(x+b_n). \tag{17}$$

Then f is a monic polynomial of degree n. Let S be the set of integers composed of primes less than

$$((1 + \varepsilon) \frac{\log k}{n} \log(\frac{\log k}{n}))^n .$$

Then

(18) $\quad f(x) \in S \quad$ for $\quad x = a_1, a_2, \ldots, a_k.$

Note that $s \approx ((\log k)/n)^n$, hence $k \approx \exp(ns^{1/n})$. By a slight refinement of the argument we obtain that in (18) k can be as large as

(19) $$\exp((n^2 - \varepsilon) \frac{s^{1/n}}{(\log s)^{(n-1)/n}}) \text{ for } s \geq s_0(\varepsilon,n).$$

This should be compared with the upper bound (4) of Evertse. A guess consistent with Stewart's conjecture mentioned in section 7 is that the right order of magnitude of the upper bound for the number of solutions of (2) is $\exp(s^{2/n})$ where n denotes the degree of f and $s \geq s_1(n)$.

Note that in our result f given by (17) has non-zero discriminant, but is far from being irreducible. It would be extremely interesting to have a similar lower bound for the original Thue-Mahler equation (2), where f is irreducible. To obtain such a bound, it seems that an extension of estimate (14) on $\psi(x,y)$ to algebraic number fields is needed. There are some preliminary results by Hazlewood (e.g. [13]) in this direction.

As far as I know, (19) is the first lower bound with respect to s for the number of solutions of Thue-Mahler equations. The only non-trivial lower bounds available in the literature concern the Thue equation of degree 3,

$$f(x,y) = m, \quad m \neq 0.$$

In 1935 Mahler [18] proved that, for any f with non-zero discriminant, there can be $c_{15}(\log|m|)^{1/4}$ solutions x,y and in 1983 Silverman [27] improved this to $c_{16}(\log|m|)^{1/3}$ for any f and to $c_{17}(\log|m|)^{2/3}$ for suitable f. Here c_{15}, c_{16} and c_{17} are positive constants. It is still possible that the number of coprime solutions of any cubic Thue equation is bounded by some absolute constant. It may also be true that the number of coprime solutions of any Thue equation corresponding to a curve of genus $g > 1$ can be bounded in terms of g only.

ACKNOWLEDGEMENT

I thank J.-H. Evertse, K. Győry and F. Oort for their remarks on an earlier version of this paper.

REFERENCES

[1] E. BOMBIERI and W.M. SCHMIDT, On Thue's equation, *Invent. Math.* 88 (1987), 69-81.

[2] E.R. CANFIELD, P. ERDŐS and C. POMERANCE, On a problem of Oppenheim concerning "Factorisatio Numerorum", *J. Number Th.* 17 (1983), 1-28.

[3] H. DAVENPORT and K.F. ROTH, Rational approximations to algebraic numbers, *Mathematika* 2 (1955), 160-167.

[4] P. ERDŐS, C.L. STEWART and R. TIJDEMAN, Some diophantine equations with many solutions, *Compositio Math.*, 66(1988),37-56.

[5] P. ERDŐS and P. TURÁN, On a problem in the elementary theory of numbers, *Amer. Math. Monthly* 41 (1934), 608-611.

[6] J.-H. EVERTSE, On equations in S-units and the Thue-Mahler equation, *Invent. Math.* 75 (1984), 561-584.

[7] J.-H. EVERTSE and K. GYŐRY, On the numbers of solutions of unit equations and decomposable polynomial equations, these proceedings, to appear.

[8] J.-H. EVERTSE and K. GYŐRY, Thue-Mahler equations having a small number of solutions, to appear.

[9] J.-H. EVERTSE, K. GYŐRY, C.L. STEWART and R. TIJDEMAN, S-unit equations and their applications, *New Advances in Transcendence Theory, Cambridge Univ. Press*, to appear.

[10] J.-H. EVERTSE, K. GYŐRY, C.L. STEWART and R. TIJDEMAN, On S-unit equations in two unknowns, *Invent. Math.*, to appear.

[11] K. GYŐRY, Explicit upper bounds for the solutions of some diophantine equations, *Ann. Acad. Sci. Fenn. Ser. A I 5* (1980), 3-12.

[12] K. GYŐRY, C.L. STEWART and R. TIJDEMAN, On prime factors of sums of integers I, *Compositio Math.* 59 (1986), 81-88.

[13] D.G. HAZLEWOOD, On ideals having only small prime factors, *Rocky Mountain J. Math.* 7 (1977), 753-768.

[14] A. HILDEBRAND and G. TENENBAUM, On integers free of large prime factors, *Trans. Amer. Math. Soc.* 296 (1986), 265-290.

[15] D.J. LEWIS and K. MAHLER, On the representations of integers by binary forms, *Acta Arith.* 6 (1960), 333-363.

[16] K. MAHLER, Zur Approximation algebraischer Zahlen, I: Über den grössten Primteiler binärer Formen, *Math. Ann.* 107 (1933), 691-730.

[17] K. MAHLER, Zur Approximation algebraischer Zahlen, II: Über die Anzahl der Darstellungen grösser Zahlen durch binäre Formen, *Math. Ann.* 108 (1933), 37-55.

[18] K. MAHLER, On the lattice points on curves of genus 1, *Proc. London Math. Soc.* (2) 39 (1935), 431-466.

[19] K. MAHLER, On Thue's equation, *Math. Scand.* 55 (1984), 188-200.

[20] J. MUELLER and W.M. SCHMIDT, Thue's equation and a conjecture of Siegel, to appear.

[21] K.K. NORTON, Numbers with small prime factors, and the least k-th power non-residue, *Memoirs of the Amer. Math. Soc.* 106 (1971).

[22] A.J. van der POORTEN, Linear forms in logarithms in the p-adic case, Transcendence Theory: Advances and Applications, *Academic Press, London,* 1977, 29-57.

[23] K. RIBET, On modular representations of Gal ($\bar{\mathbb{Q}}/\mathbb{Q}$) arising from modular forms, *Invent. Math.*, to appear.

[24] W.M. SCHMIDT, Thue equations with few coefficients, Trans. Amer. Math. Soc. 303(1987), 241-255.

[25] J.-P. SERRE, Sur les représentations modulaires de degré 2 de Gal $(\bar{Q}/Q)$, *Duke Math. J.* 54 (1987), 179-230.

[26] C.L. SIEGEL, Über einige Anwendungen diophantischer Approximationen, *Abh. Preuss. Akad. Wiss. Phys.-math. Kl.*, 1929, No. 1, 70 pp.

[27] J.H. SILVERMAN, Integer points on curves of genus 1, *J. London Math. Soc.* (2) 28 (1983), 1-7.

[28] J.H. SILVERMAN, Quantitative results in diophantine geometry, Preprint, M.I.T. (1984).

[29] C.L. STEWART and R. TIJDEMAN, On prime factors of sums of integers II, Diophantine Analysis, *LMS Lecture Notes 109, Cambridge University Press*, 1986, pp. 83-99.

[30] C.L. STEWART and R. TIJDEMAN, On the Oesterlé-Masser conjecture, *Monatsh. Math.* 102 (1986), 251-257.

[31] A. THUE, Über Annäherungswerte algebraischer Zahlen, *J. reine angew. Math.* 135 (1909), 284-305.

[32] P. VOJTA, Diophantine Approximations and Value Distribution Theory, *Lecture Notes Math. 1239, Springer-Verlag, Berlin etc.*, 1987.

[33] B.M.M. de WEGER, Solving exponential diophantine equations using lattice basis reduction algorithms, *J. Number Th.* 26 (1987), 325-367.

[34] K.R. YU, Linear Forms in the p-adic Logarithms, *Dissertation, Univ. Bonn, Germany,* 1986.

R. TIJDEMAN
Mathematical Institute
Postbus 9512
2300 RA Leiden
The Netherlands.

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

ON THE PRACTICAL SOLUTION OF THE THUE EQUATION - AN OUTLINE

NIKOS TZANAKIS

This paper was presented at the Colloquium on Number Theory, held in Budapest, in July 1987. It reports on a joint paper of the author (speaker) and B.M.M. de Weger.

The purpose of this paper is to give an outline of a practical method for the solution of the general Thue equation

$$F(X,Y) = m \quad , \tag{1}$$

where m is a given rational integer and $F(X,Y) \in \mathbf{Z}[X,Y]$ is an irreducible form of degree $n \geq 3$. A detailed exposition, including examples, can be found in a forthcoming paper by the author and B.M.M. de Weger.

A. Thue in 1909 [6] proved that (1) has at most finitely many solutions $(X,Y) \in \mathbf{Z}^2$, but his proof was ineffective. An effective proof has been given by A. Baker in 1968 [1], as a result of his deep study of the linear form in logarithms of algebraic numbers.

Since Baker's work, several papers have been published, in which examples of Thue equations are completely solved, using Baker's results. These are mostly cubic equations and only very recently Pethő & Schulenberg [4] and Blass-Glass-Meronk & Steiner [2] have solved explicitly several quartic equations in which 3 fundamental units are involved. The last mentioned paper provides also a practical method for the solution of the general Thue equation, which in several respects is quite different from ours. A general treatment of the Thue equation with the use of Baker-type theorems can be found in Sprindžuk's book of 1982 [5, Chapter IV], but from this, one cannot find a practical way for solving explicitly a given Thue equation.

Let $F(X,1) = 0$ have s real roots and t pairs of complex-conjugate roots, so that $s + 2t = n$. If $s = 0$, then the solution of (1) is trivial; one can elementarily compute "small" upper bounds for $|X|$ and $|Y|$. So, we suppose from now on that $s \geq 1$. Denote the roots of $F(X,1) = 0$ by $\xi^{(1)},\ldots,\xi^{(n)}$ the first s being the real

ones. We work in the field $K = \mathbb{Q}(\xi)$, where $F(\xi,1) = 0$. In the ring of integers of K, as well as in any other order of K, the group of units has r generators of infinite order (the so-called fundamental units), where

$$r = s + t - 1$$

(Dirichlet's Unit Theorem). Then (1) implies a finite number of equations of the form

$$\beta := X - Y\xi = \mu\varepsilon_1^{a_1}\ldots\varepsilon_r^{a_r}, \tag{2}$$

where $\mu \in K$ is an explicitly known algebraic integer, $\varepsilon_1,\ldots,\varepsilon_r$ are the fundamental units of an appropriate order R containing ξ and $(a_1,\ldots,a_r) \in \mathbb{Z}^r$ is a sought - for r - tuple with the property that the element $\mu\varepsilon_1^{a_1}\ldots\varepsilon_r^{a_r}$ be of the special shape: Integer + Integer$\cdot\xi$.

From (2) we proceed as follows: First, we show that for some $i_o \le s$ the i_o-conjugate of β is very small and every other conjugate of β is large, in the sense that

$$\begin{aligned} &|\beta^{(i_o)}| < \text{const} \cdot |Y|^{-(n-1)}, \\ &|\beta^{(j)}| > \text{const} \cdot |Y|, \qquad (j \neq i_o), \end{aligned} \tag{3}$$

provided that $|Y|$ is "large enough".

If $s \ge 3$ ("real case") we choose indices j, $k \in \{1,\ldots,s\}$ such that $i_o \neq j \neq k \neq i_o$ and if $s = 1$ or 2

("complex case") we choose indices $j,k > s$ such that $\xi^{(k)} = \overline{\xi^{(j)}}$. In both cases we consider the i_o, j,k-conjugate relations of (2) to eliminate X and Y and then, by some more or less standard arguments, we are led to an inequality

$$(4) \qquad 0 < |\Lambda| < c_1 \exp(-c_2 A),$$

where $A = \max_i |a_i|$, c_1 and c_2 are explicitly computable positive constants and Λ is a linear form in logarithms of algebraic numbers. Specifically,

$$\Lambda = \log|\delta| + \sum_{h=1}^{r} a_h \log|\delta_h| ,$$

where $\delta = \dfrac{\xi^{(i_o)} - \xi^{(j)}}{\xi^{(i_o)} - \xi^{(k)}}$ and $\delta_h = \varepsilon_h^{(k)}/\varepsilon_h^{(j)}$ in the "real case", and

$$\Lambda i = \mathrm{Log}\delta + \sum_{h=1}^{r} a_h \mathrm{Log}\delta_h + a_{r+1}\mathrm{Log}(-1) ,$$

where δ and δ_h are as before, a_{r+1} is an extra unknown integer and the logarithms are principal, in the "complex case". Using a result of M. Waldschmidt [7] we find, on the other hand,

$$(5) \qquad |\Lambda| > \exp(-c_3(\log A + c_4)) ,$$

where c_3 and c_4 are, again, explicitly computable positive constants. Combine now (4) and (5) to get an upper bound for A, which in practice is very large. Having an upper bound for A, provides us with an effective method for solving (2) and, consequently (1), too. On the other hand, such a large upper bound for A (in a typical example it can be as large as 10^{40}) cannot provide us with a practical method for solving (2) (and, hence, (1)).

In what follows I shall describe a process, which reduces considerably the upper bound for A. It is based on the Lenstra-Lenstra & Lovász Basis Reduction Algorithm [3]. (I will refer to it as the L^3-algorithm). In this algorithm the input data is an arbitrary basis of a lattice Γ and the output data is a so-called "reduced" basis of Γ. This is a good basis, in the sense that, roughly speaking, its vectors are "almost orthogonal" and of "almost equal lengths". We use the "integral version" of the L^3-algorithm, due to de Weger [8], which works only with vectors having integral coordinates and in which all necessary divisions are exact. Thus, we completely avoid the rounding-off errors at this stage.

Let's come back to our reduction problem: Its more general shape is the following: Put

$$\Lambda = \mu_0 + a_1\mu_1 + \ldots + a_r\mu_r \ ,$$

where the μ's are known real numbers, and find all $(a_1,\ldots,a_r) \in \mathbf{Z}^r$, which satisfy the system

$$(6) \qquad 0 < |\Lambda| < K_1 \exp(-K_2 A) \text{ and } A < K_3 \quad (A = \max_i |a_i|)$$

with K_1, K_2, K_3 explicitly known positive constants and K_3 "very large". We reduce the size of K_3 as follows: Let c_o be a constant somewhat larger than K_3^r and let Γ be the lattice generated by the column-vectors of the $r \times r$ matrix

$$A = \begin{pmatrix} 1 & & o \\ & \ddots & \\ o & & 1 \\ [c_o\mu_1] & [c_o\mu_{r-1}] & [c_o\mu_r] \end{pmatrix} .$$

By the aforementioned algorithm we find a reduced basis $\underline{b}_1,\ldots,\underline{b}_r$ of Γ. If we denote the matrix whose columns are $\underline{b}_1,\ldots,\underline{b}_r$ by B, then the same algorithm finds easily a matrix U such that $B = AU$, as well as U^{-1}. Consequently, we can easily compute, in view also of the simple form of A, the matrix $B^{-1} = U^{-1} A^{-1}$. Then, if we put

$$\underline{x} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -[c_o\mu_o] \end{pmatrix} \in \mathbf{R}^r$$

we have $\underline{x} = \sum_{i=1}^{r} s_i \underline{b}_i$ and $\begin{pmatrix} s_1 \\ \vdots \\ s_r \end{pmatrix} = A^{-1}\underline{x}$, so that the s_i's can be explicitly computed. On the other hand, if we denote by $l(\underline{x},\Gamma)$ the distance from $\underline{x}$ to the closest to $\underline{x}$ point of Γ (if $\underline{x} = \underline{0}$, then $l(\underline{x},\Gamma)$ denotes the minimal distance of non-zero points of Γ from $\underline{0}$), then we can prove that

$$(7) \qquad l(\underline{x},\Gamma) \geq \text{const} \cdot |\underline{b}_1|$$

where the constant is explicitly computable and depends on $\|s_i\|$ $i=1,\ldots,r$ ($\|\cdot\|$ means the distance from the nearest integer). Since the volume of the parallelepiped of $\underline{b}_1,\ldots,\underline{b}_r$ is $[c_o\mu_r]$, which is of the size of K_3^r, and all the $\underline{b}_i$'s have "almost the same length", we expect that $|\underline{b}_1|$ is of the size of $[c_o\mu_r]^{1/r}$, i.e. of the size of K_3. Therefore, if no $\|s_i\|$ is extremely small, then, by (7), $l(\underline{x},\Gamma)$ is of the size of K_3.

Let now $(a_1,\ldots,a_r) \in \mathbb{Z}^r$ be a solution of (6) and consider the point of Γ

$$A \begin{pmatrix} a_1 \\ \vdots \\ a_r \end{pmatrix} = \begin{pmatrix} a_1 \\ \vdots \\ a_{r-1} \\ \lambda_o \end{pmatrix}, \text{ where } \lambda_o = \sum_{i=1}^{r} a_i [c_o\mu_i] \quad .$$

Its distance from $\underline{x}$ must satisfy $a_1^2 + \ldots + a_{r-1}^2 + \lambda^2 \geq$ $\geq l(\underline{x},\Gamma)^2$, where $\lambda = \lambda_o + [c_o\mu_o]$. From this and (7), it

follows that $|\lambda| > \text{const} \cdot K_3$. On the other hand, it is clear that $|\lambda| \leq c_o|\Lambda| + (\text{small error})$ and the right-hand side is of the size of $K_3^r|\Lambda|$. Thus, $\text{const} \cdot K_3 < |\lambda| < K_3^r|\Lambda|$, from which it follows $|\Lambda| > \text{const} \cdot K_3^{-(r-1)}$. Combine this with the first relation (6) to get $K_1\exp(-K_2A) > \text{const} \cdot K_3^{-(r-1)}$, from which an upper bound for A can be found, of the size of $\log K_3$.

If necessary, we repeat this process to reduce the upper bound of A even more, until the upper bound is so small that we can check by direct computations all possibilities.

As an application of this method we have computed all integral points on the elliptic curve

$$y^2 = x^3 - 4x + 1 . \tag{8}$$

As it is well known, the solution of such an equation is reduced to the solution of a finite number of quartic Thue equations. In the case of (8), this finite set of Thue equations consists of reducible equations, which can be solved trivially and of the following two irreducible Thue equations:

$$X^4 - 4X^3Y - 12X^2Y^2 + 4Y^4 = 1 \tag{9}$$

$$X^4 - 12X^2Y^2 - 8XY^3 - 4Y^4 = 1 \tag{10}$$

By the method described in the previous pages, we found out that the only solutions to (9) are $(X,Y) = \pm(1,0)$ and to (10) are $(X,Y) = \pm(1,0), \pm(1,-1), \pm(1,3), \pm(3,-1)$. Tracing back from the solutions of the quartic Thue equations to (8), we find that the only integral points on (8) are the following 22:

$$(x,\pm y) = (-2,1), (-1,2), (0,1), (2,1), (3,4), (4,7), (10,31), (12,41), (20,89), (114,1217), (1274,45473).$$

A direct corollary to this is that the only triangular numbers $T_n := (n+1)n/2$, which are product of three consecutive integers, are $T_3, T_{15}, T_{20}, T_{44}, T_{608}, T_{22736}$. Indeed, following S.P. Mohanty (private communication), we consider the equation

$$(11) \qquad T_n = m(m+1)(m+2)$$

and put $m = (x-2)/2$, $n = (y-1)/2$, where x is even > 2 and y odd > 1. Then (11) is transformed into (8) and our claim becomes obvious.

REFERENCES

[1] BAKER, A., Contributions to the theory of Diophantine equations I. On the representation of integers by binary forms, *Phil. Trans. Royal Soc. London*, A 263 (1968), 173-191.

[2] BLASS, J., GLASS, A., MERONK, D. and STEINER, R., Practical solutions to Thue equations over the rational integers (submitted).

[3] LENSTRA, A.K., LENSTRA, H.W. and LOVÁSZ, L., Factoring polynomials with rational coefficients, *Math. Annalen* 261 (1982), 515-534.

[4] PETHŐ, A. and SCHULENBERG, R., Effectives Lösen von Tnue Gleichungen, to appear in Publ. Math. Debrecen.

[5] SPRINDŽUK, V.G., Classical diophantine equations with two unknowns (Russian),Nauka, Moscow, 1982.

[6] THUE, A., Über Annäherungswerte algebraischer Zahlen, *J. reine und angew. Math.* 135 (1909), 284-305.

[7] WALDSCHMIDT, M., A lower bound for linear forms in logartihms, *Acta Arithm.* 37 (1980), 257-283.

[8] DE WEGER, B.M.M., Solving exponential diophantine equations using lattice basis reduction algorithms, *J. Number Th.* 26 (1987), 325-367.

NIKOS TZANAKIS
Department of Mathematics,
University of Crete,
Iraklion, Greece.

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

DEPENDENCE OF LOGARITHMS OF ALGEBRAIC POINTS

WALDSCHMIDT, M.

INTRODUCTION

Let G be a commutative connected algebraic group over the field $\bar{\mathbf{Q}}$ of algebraic numbers, $\exp_G: T_G(\mathbf{C}) \to G(\mathbf{C})$ the exponential map of the Lie group $G(\mathbf{C})$, and Λ the inverse image in $T_G(\mathbf{C})$ of $G(\bar{\mathbf{Q}})$. We study the distribution of Λ in $T_G(\mathbf{C})$. More precisely, we give a necessary and sufficient condition on a $\mathbf{C}$-vector subspace V of $T_G(\mathbf{C})$ for $V \cap \Lambda$ to be of finite dimension over $\mathbf{Q}$, and for such a V we give upper bounds for this dimension.

We consider first (§1) the case where G is a torus G_m^d, next (§2) we take for G a linear algebraic group. In §3 we deal with an arbitrary commutative algebraic

group, and in §4 we refine the estimate for a product of a linear algebraic group by an arbitrary commutative algebraic group. The proofs are given in §5.

§1. USUAL LOGARITHMS

We denote by L the set of logarithms of algebraic numbers:

$$L = \{\log\alpha,\ \alpha \in \bar{\mathbf{Q}}^*\} = \{\ell \in \mathbf{C},\ e^{\ell} \in \bar{\mathbf{Q}}\} \subset \mathbf{C}.$$

We fix an integer $d \geq 2$. The set L^d is a $\mathbf{Q}$-vector subspace of $\mathbf{C}^d$. Let V be a $\mathbf{C}$-vector subspace of $\mathbf{C}^d$ of dimension n. If $V \cap \mathbf{Q}^d \neq 0$, then $V \cap L^d$ is a $\mathbf{Q}$-vector space of infinite dimension. Indeed, let $\underline{b} = (b_1,\ldots,b_d) \in V \cap \mathbf{Q}^d$, $\underline{b} \neq 0$; then

$$(b_1 \log\alpha,\ldots,b_d \log\alpha) \in V \cap L^d$$

for all $\log\alpha \in L$.

Conversely, M. Emsalem proved that if $V \cap \mathbf{Q}^d = 0$, then the $\mathbf{Q}$-vector space $V \cap L^d$ is of finite dimension (see [E] theorem 1), and that this dimension is at most nd (see [E] theorem 2). Emsalem gave interesting applications of these results to a problem considered by Greenberg on the arithmetic of $\mathbf{Z}_p$-extension.

Here is an example where this dimension is finite, and $\geq n(n+1)/2$ (compare with Langevin's example in [Wa1], p. 1635). We choose V defined by the equations

$$z_1 \log\alpha_1 + \ldots + z_{n+1} \log\alpha_{n+1} = 0, \quad z_{n+2} = \ldots = z_d = 0,$$

where $\log\alpha_1, \ldots, \log\alpha_{n+1}$ are $\mathbf{Q}$-linearly independent elements of L. Hence $V \cap \mathbf{Q}^d = 0$, and $V \cap L^d$ contains the $n(n+1)/2$ points

$$y_{ij} = (y_{ij1}, \ldots, y_{ijd}) \in \mathbf{C}^d, \quad (1 \leq i < j \leq d),$$

where

$$y_{ijs} = \begin{cases} \log\alpha_j & \text{for } s = i \\ -\log\alpha_i & \text{for } s = j \\ 0 & \text{otherwise, } 1 \leq s \leq d. \end{cases}$$

It is plain that these $n(n+1)/2$ points of $V \cap L^d$ are $\mathbf{Q}$linearly independent. (This construction works as well if we replace L by any $\mathbf{Q}$-vector subspace of $\mathbf{C}$ of dimension $>n$).

Here is an improvement of Emsalem's bound:

THEOREM 1.1: If $V \cap \mathbf{Q}^d = 0$, *then the dimension over* $\mathbf{Q}$ of $V \cap L^d$ *is at most* $n(n+1)$, *where* n *is the dimension of* V.

It easily follows that for any V, there exists a rational subspace W of $\mathbf{C}^d$, contained in V, such that $\dim_{\mathbf{Q}}(V \cap L^d / W \cap L^d) \leq \nu(\nu+1)$ with $\nu = n - \dim_{\mathbf{C}} W$ (compare with [E] theorem 2).

In some cases we can improve the preceeding upper bound. Let us denote by t the dimension of the complex vector subspace of $\mathbf{C}^d$ generated by $V \cap \bar{\mathbf{Q}}^d$. Hence we have $0 \leq t \leq n < d$.

THEOREM 1.2: *If* $V \cap \mathbf{Q}^d = 0$, *then* $V \cap L^d$ *is of dimension over* $\mathbf{Q}$ *at most* $d(d-1-t)$.

Here is an example of V with $V \cap L^d$ of finite dimension $\geq (n-t)(n+1-t)/2$: we take V defined by the equations

$$(\beta_1 z_1 + \beta_2 z_2 + \ldots + \beta_t z_t + z_{t+1}) \log\alpha_{t+1} + z_{t+2} \log\alpha_{t+2} + \ldots + z_{n+1} \log\alpha_{n+1} = 0.$$

$$z_{n+2} = \ldots = z_d = 0,$$

with $1, \beta_1, \ldots, \beta_t$ $\mathbf{Q}$-linearly independent in $\bar{\mathbf{Q}}$, and $\log\alpha_{t+1}, \ldots, \log\alpha_{n+1}$ $\mathbf{Q}$-linearly independent in L.

Let us give a few examples.

1) For $n = 1$, theorem 1.1 shows that the only lines of $\mathbf{C}^d$ containing three linearly independent points of L^d are those which contain a non-zero point of $\mathbf{Q}^d$.

COROLLARY 1.3: *Let* $\log\alpha_{ij}$, $(1 \leq i \leq d, \ 1 \leq j \leq \ell)$ *be* ℓd *elements of* L. *Assume that at least two of the* d *rows of the matrix*

$$\begin{bmatrix} \log\alpha_{11} & \cdots & \log\alpha_{1\ell} \\ \vdots & & \vdots \\ \log\alpha_{d1} & \cdots & \log\alpha_{d\ell} \end{bmatrix}$$

are **Q**-*linearly independent, and that at least three of the* ℓ *columns are* **Q**-*linearly independent. Then the rank of the matrix is at least* 2.

Corollary 1.3 is equivalent to the six exponentials theorem: if the rank of the matrix were 1, then we would have $\log\alpha_{ij} = x_i y_j$, $(1 \le i \le d, \quad 1 \le j \le \ell)$, with at least two of $x_1,\ldots,x_d$ linearly independent and at least three of $y_1,\ldots,y_\ell$ independent over **Q**, which is impossible (e.g. [Wa2]§2).

The rank of the matrix may be 2, even if ℓ and d are large and all the d rows as well as the ℓ columns are linearly independent (for instance take all the entries equal to zero, apart from one row and one column).

2) We consider the case $t = n = d-1$ of theorem 1.2. This means that V is a hyperplane of $\mathbf{C}^d$ which is defined over $\bar{\mathbf{Q}}$. Let

$$\beta_1 z_1 + \ldots + \beta_d z_d = 0$$

be an equation of V, with algebraic $\beta_1,\ldots,\beta_d$. The assumption $V \cap \mathbf{Q}^d = 0$ means that $\beta_1,\ldots,\beta_d$ are **Q**-linearly independent, and the conclusion is $V \cap L^d = 0$, which

reads $\beta_1 \log\alpha_1 + \ldots + \beta_d \log\alpha_d \neq 0$ when $\log\alpha_1, \ldots, \log\alpha_d$ are not all zero in L. This is equivalent with the homogeneous case of Baker's theorem:

COROLLARY 1.4: *Let* $\log\alpha_1, \ldots, \log\alpha_n$ *be* Q*-linearly independent elements of* L. *Then* $\log\alpha_1, \ldots, \log\alpha_n$ *are* $\bar{Q}$*-linearly independent.*

3) We now give an example with $d = 3$, $n = 2$, and $t = 1$. Let V be the hyperplane of C^3 of equation $\eta z_1 + \theta z_2 = z_3$, where η is algebraic (so that $(1,0,\eta) \in V$, and $t \geq 1$), and η is irrational, while θ is transcendental. This ensure that $1, \eta$ and θ are Q-linearly independent, hence $V \cap Q^3 = 0$. From theorem 1.2 we deduce that the dimension of $V \cap L^3$ over Q is at most 3:

COROLLARY 1.5: *Let* α_i, β_i, $(i = 1,2,3,4)$ *and* η *be non-zero algebraic numbers, and* $t \in C$ *be a transcendental number. Assume that* η *is irrational, and that the four points* $(\log\alpha_i, \log\beta_i)$, $(1 \leq i \leq 4)$ *are* Q*-linearly independent in* $L \times L$. *Then one at least of the four numbers*

$$\alpha_i^{\eta} \cdot \beta_i^{t}, \quad (i = 1,2,3,4)$$

is transcendental.

4) Finally we give an example involving exponentials in several variables (compare with [Be] II §1).

COROLLARY 1.6: *Let* $t_1,\dots,t_m$ *be* Q*-linearly independent complex numbers, and* $\lambda_1,\dots,\lambda_\ell$ *be* ℓ Q*-linearly independent elements of* L^m. *We write*

$$\lambda_j = (\log\alpha_{1j},\dots,\log\alpha_{mj}), \qquad (1 \le j \le \ell),$$

and, as usual,

$$\prod_{\nu=1}^{m} \alpha_{\nu j}^{t_\nu} = \exp\Big(\sum_{\nu=1}^{m} t_\nu \log\alpha_{\nu j}\Big), \qquad (1 \le j \le \ell).$$

Assume $\ell \geq (r-1)(n+1)$, *where* r *is the dimension of the* $\bar{Q}$*-vector space generated by* $1,t_1,\dots,t_m$. *Then one at least of the* ℓ *numbers*

$$\prod_{\nu=1}^{m} \alpha_{\nu j}^{t_\nu}, \qquad (1 \le j \le \ell)$$

is transcendental.

§2. LINEAR ALGEBRAIC GROUPS

Let $d_0 \ge 0$ and $d_1 \ge 0$ be non negative integers with $d = d_0 + d_1 \ge 2$. We consider the Q-vector subspace $\bar{Q}^{d_0} \times L^{d_1}$ of C^d. If V is a Q-vector subspace of C^d, we are interested to know whether the intersection $V \cap (\bar{Q}^{d_0} \times L^{d_1})$ is of finite dimension over Q or not.

Clearly, if $V \cap (0 \times \mathbf{Q}^{d_1}) \neq 0$, or if $V \cap (\bar{\mathbf{Q}}^{d_0} \times 0) \neq 0$, then this dimension is infinite. We will see that the converse holds.

Let us denote by t the dimension of the $\mathbf{C}$-vector subspace of $\mathbf{C}^d$ generated by $V \cap \bar{\mathbf{Q}}^d$.

THEOREM 2.1: *Assume* $V \cap (0 \times \mathbf{Q}^{d_1}) = 0$ *and* $V \cap (\bar{\mathbf{Q}}^{d} \times 0) = 0$. *Then* $V \cap (\bar{\mathbf{Q}}^{d_0} \times \mathbf{L}^{d_1})$ *is of finite dimension over* $\mathbf{Q}$, *and this dimension is at most* $d_1(d-t-1)$.

We will see also that this dimension is at most $n(n+1)$.

EXAMPLES

1) If we take $d_0 = 0$, we just get theorem 1.2.

2) (Baker's theorem by Schneider's method). We first deduce Corollary 1.4 from Theorem 2.1. Assume $\log\alpha_1,\ldots,\log\alpha_{n+1}$ are $\mathbf{Q}$-linearly independent, but $\bar{\mathbf{Q}}$-linearly dependent:

$$\beta_1 \log\alpha_1 + \ldots + \beta_n \log\alpha_n = \log\alpha_{n+1}.$$

We may assume that $\log\alpha_1,\ldots,\log\alpha_n$ are $\bar{\mathbf{Q}}$-linearly independent. We choose $d_0 = n$, $d_1 = 1$, $t = 0$, and V is the hyperplane

$$z_1\log\alpha_1 + \ldots + z_n\log\alpha_n = z_{n+1}.$$

We get $n+1$ $\mathbf{Q}$-linearly independent points $\lambda_1,\ldots,\lambda_{n+1}$ in $V \cap (\bar{\mathbf{Q}}^n \times L)$:

$$\lambda_i = (\delta_{i1},\ldots,\delta_{in},\ \log\alpha_i), \qquad (1 \le i \le n),$$

and

$$\lambda_{n+1} = (\beta_1,\ldots,\beta_n,\ \log\alpha_{n+1}).$$

This contradicts the upper bound provided by Theorem 2.1.

We now prove the non-homogeneous case of Baker's theorem:

COROLLARY 2.2: *Let* $\log\alpha_1,\ldots,\log\alpha_n$ *be* $\mathbf{Q}$*-linearly independent elements of* $\mathbf{L}$. *Then the numbers* $1, \log\alpha_1,\ldots,\log\alpha_n$ *are* $\bar{\mathbf{Q}}$*-linearly independent.*

Indeed, if

$$\beta_0+\beta_1\ \log\alpha_1+\ldots+\beta_{n-1}\ \log\alpha_{n-1} = \log\alpha_n,$$

with $\log\alpha_1,\ldots,\log\alpha_n$ $\mathbf{Q}$-linearly independent and $1, \log\alpha_1,\ldots,\log\alpha_{n-1}$ $\bar{\mathbf{Q}}$-linearly independent, then we choose $d_0 = n$, $d_1 = 1$, and V is the hyperplane

$$z_0 + z_1\ \log\alpha_1+\ldots+z_{n-1}\ \log\alpha_{n-1} = z_n.$$

We have $t = 1$ because $(1,0,\ldots,0,1) \in V$. We now get n $\mathbf{Q}$-linearly independent points $\lambda_1,\ldots,\lambda_n$ in $V \cap (\bar{\mathbf{Q}}^n \times L)$:

$$\lambda_i = (0, \delta_{i1}, \ldots, \delta_{in-1}, \log\alpha_i), \quad (1 \leq i \leq n-1),$$

and

$$\lambda_n = (\beta_0, \beta_1, \ldots, \beta_{n-1}, \log\alpha_n).$$

which contradicts theorem 2.1.

3) We also deduce Corollary 2.2 from Theorem 2.1 by Gel'fond-Baker's method: we start from a non trivial relation

$$\beta_0 + \beta_1 \log\alpha_1 + \ldots + \beta_{n-1} \log\alpha_{n-1} = \log\alpha_n,$$

with algebraic α's and β's. We may assume (by induction) that $1, \beta_1, \ldots, \beta_{n-1}$ are $\mathbf{Q}$-linearly independent, and $(\beta_0, \log\alpha_1, \ldots, \log\alpha_n) \neq 0$. For $d_0 = 1$, $d_1 = t = n$, the hyperplane V of equation

$$z_0 + \beta_1 z_1 + \ldots + \beta_{n-1} z_{n-1} = z_n,$$

contains a non-zero point $(\beta_0, \log\alpha_1, \ldots, \log\alpha_n)$ of $\bar{\mathbf{Q}} \times L^n$, which contradicts Theorem 2.1.

4) We now deduce from Theorem 2.1 the "strong six exponentials theorem" of [Wa2].

COROLLARY 2.3: *Let* x_1, x_2 *be two complex numbers which are* $\mathbf{Q}$*-linearly independent, and let* y_1, y_2, y_3 *be three complex numbers which are* $\mathbf{Q}$*-linearly independent. Further let* α_{ij} ($i = 1,2$; $j = 1,2,3$) *be six algebraic numbers. Assume that the six numbers*

$$\exp(x_i y_j - \alpha_{ij}), \quad (i = 1,2; \quad j = 1,2,3)$$

are algebraic. Then

$$x_i y_j = \alpha_{ij} \quad \textit{for} \quad i = 1,2 \textit{ and } j = 1,2,3.$$

We take $d_0 = d_1 = t = 2$, and V is the hyperplane of C^4 of equation $x_2(z_1+z_3) = x_1(z_2+z_4)$. It contains the three points

$$(\alpha_{1j}, \alpha_{2j}, x_1 y_j - \alpha_{1j}, x_2 y_j - \alpha_{2j}), \quad (j = 1,2,3).$$

and these points are $\mathbb{Q}$-linearly independent. From theorem 2.1 we deduce $V \cap (\bar{\mathbb{Q}}^2 \times 0) \neq 0$, hence $\gamma = x_2/x_1$ is algebraic and irrational. Define

$$\log\delta_{ij} = x_i y_j - \alpha_{ij}, \quad (i = 1,2; \quad j = 1,2,3).$$

We get

$$\gamma\log\delta_{1j} - \log\delta_{2j} = \alpha_{2j} - \gamma\alpha_{1j}, \quad (j = 1,2,3),$$

and Corollary 2.2 implies:

$$\log\delta_{1j} = 0, \quad \log\delta_{2j} = 0, \text{ and } \alpha_{2j} = \gamma\alpha_{1j}$$

for $j = 1,2,3$, which is the desired conclusion.

4) Here is an example with $d_0 = 1$, $d_1 = 2$, $d = 3$ and, $t = 0$.

COROLLARY 2.4: *Let* $\log\alpha_1$, $\log\alpha_2$, $\log\alpha_3$, $\log\alpha_4$ *be* $\mathbf{Q}$*-linearly independent elements of* $\mathbf{L}$, *and* β_1, β_2 *two algebraic numbers. Then one at least of the two numbers*

$$\exp\left(\frac{\log\alpha_1}{\log\alpha_2}\cdot\log\alpha_3 + \beta_1\log\alpha_1\right), \exp\left(\frac{\log\alpha_1}{\log\alpha_2}\cdot\log\alpha_4 + \beta_2\log\alpha_1\right).$$

is transcendental.

If these two numbers γ_1, γ_2 are algebraic, then we take for V the hyperplane

$$z_1\log\alpha_1 = z_2 + z_3\frac{\log\alpha_1}{\log\alpha_2}, \text{ with the 5 points}$$

$$(0,\log\alpha_1,-\log\alpha_2),\ (1,\log\alpha_1,0),\ (1,0,\log\alpha_2),$$

and

$$(\beta_1,\log\gamma_1,-\log\alpha_3),\ (\beta_2,\log\gamma_2,-\log\alpha_4).$$

5) Finally we give a further example involving exponential functions in several variables.

COROLLARY 2.5: *Let* $t_1,\ldots,t_m$ *be* $\mathbf{Q}$*-linearly independent elements of* $\mathbf{L}$, *and* $\lambda_1,\ldots,\lambda_\ell$ *be* ℓ $\mathbf{Q}$*-linearly independent elements of* $\mathbf{L}^m$. *We write*

$$\lambda_j = (\log\alpha_{1j},\ldots,\log\alpha_{mj}), \qquad (1 \le j \le \ell)$$

and, as usual,

$$\prod_{\nu=1}^{m} \alpha_{\nu j}^{t_\nu} = \exp\Big(\sum_{\nu=1}^{m} t_\nu \log_{\nu j}\Big), \qquad (1 \le j \le \ell).$$

Assume $\ell > m^2$; *then one at least of the* ℓ *numbers*

$$\prod_{\nu=1}^{m} \alpha_{\nu j}^{t_\nu} \qquad (1 \le j \le \ell)$$

is transcendental.

PROOF: We first notice that $1, t_1, \ldots, t_m$ are $\bar{\mathbf{Q}}$-linearly independent by Corollary 2.2. We take $d_0 = m$, $d_1 = m+1$, $n = 2m$, $t = m$; the hyperplane V of equation

$$t_1(z_{n+1}-z_1)+\ldots+t_n(z_{2n}-z_n) = z_{2n+1},$$

contains the points

$$(0,\ldots,0,\log\alpha_{j1},\ldots,\log\alpha_{jm}), \qquad (1 \le j \le \ell).$$

and

$$(\delta_{\nu 1},\ldots,\delta_{\nu m},-\delta_{\nu 1},\ldots,-\delta_{\nu m}), \qquad (1 \le \nu \le m).$$

§3. COMMUTATIVE ALGEBRAIC GROUPS

Let G be a commutative algebraic group of dimension $d \ge 2$ which is defined over the field $\bar{\mathbf{Q}}$ of algebraic numbers. We view the complex points $G(\mathbf{C})$ of G as a Lie group, we denote by $T_G(\mathbf{C})$ the Lie algebra of G

at the origin, and by $\exp_G : T_G(C) \to G(C)$ the exponential map of $G(C)$.

We denote by $G(\bar{\mathbf{Q}})$ the group of points of G which are rational over $\bar{\mathbf{Q}}$, and by $\Lambda_G = \Lambda$ the inverse image in $T_G(\mathbf{C})$ of $G(\bar{\mathbf{Q}})$ by the exponential map. Hence Λ is a $\mathbf{Q}$-vector subspace of $T_G(C)$.

Let V be a $\mathbf{C}$-vector subspace of $T_G(C)$ of dimension n. Obviously, if there exists an algebraic subgroup H of G, of positive dimension, which is defined over $\bar{\mathbf{Q}}$, such that $T_H(\mathbf{C})$ is contained in V, then $V \cap \Lambda$ is of infinite dimension over $\mathbf{Q}$ (because it contains $\exp_H^{-1}(H(\bar{\mathbf{Q}}))$). Such a $T_H(\mathbf{C})$ is nothing else than a non-zero $\bar{\mathbf{Q}}$-algebraic Lie sub-algebra of $T_G(\mathbf{C})$ (see [B]).

From the arguments of [E] §1 it follows that the converse is true. It is easy to give an example where $V \cap \Lambda$ is of finite dimension $\geq n(n+1)$: we take a power of an elliptic curve with complex multiplication, and we repeat the example of §1.

THEOREM 3.1: *Assume that* V *does not contain any non-zero* $\bar{\mathbf{Q}}$*-algebraic Lie sub-algebra of* $T_G(\mathbf{C})$ *defined over* $\bar{\mathbf{Q}}$. *Then* $V \cap \Lambda$ *is of finite dimension over* $\mathbf{Q}$, *and this dimension is at most* $2n(n+1)$.

Therefore for any V there exists a $\bar{\mathbf{Q}}$-algebraic Lie sub-algebra $T_H(\mathbf{C})$ of $T_G(\mathbf{C})$, which is contained in V, such that $\dim_{\mathbf{Q}}(V \cap \Lambda_G/\Lambda_H) \leq 2\nu(\nu+1)$, where $\nu = n - \dim H$.

Here $\Lambda_H = \Lambda_G \cap T_H(C)$.

Since T_G is the tangent space of G at the origin, it has also a $\bar{\mathbf{Q}}$-structure: we denote by $T_G(\bar{\mathbf{Q}})$ the space of $\bar{\mathbf{Q}}$-rational points on T_G, and by t the dimension of the C-vector subspace of $T_G(C)$ generated by $V \cap T_G(\bar{\mathbf{Q}})$.

THEOREM 3.2: *Assume that* V *does not contain any non-zero* $\bar{\mathbf{Q}}$*-algebraic Lie sub-algebra of* $T_G(C)$ *defined over* $\bar{\mathbf{Q}}$. *Then the dimension of* $V \cap \Lambda$ *is at most* $2d(d-t-1)$.

If we choose $G = G_m^d$ where G_m is the multiplicative group, then $\Lambda = L^d$. If we choose $G = G_a^{d_0} \times G_m^{d_1}$ where G_a is the additive group, then $\Lambda = \bar{\mathbf{Q}}^{d_0} \times L^{d_1}$. However, our Theorem 3.2 does not give as sharp a bound as we announced in Theorems 1.2 and 2.1 for these special cases. In order to achieve an estimate which includes these results, we will consider in the next section a product of a linear group by any commutative algebraic group.

For $t = d-1$, i.e. when V is a hyperplane of $T_G(C)$ which is defined over $\bar{\mathbf{Q}}$, the conclusion is $V \cap \Lambda = 0$. This is a result due to Wüstholz (see [Be]).

COROLLARY 3.3: *Let* G *be a commutative algebraic group defined over* $\bar{\mathbf{Q}}$, *and let* $u \in T_G(C)$ *be such that*

$\exp_G u \in G(\bar{\mathbf{Q}})$. *Then the smallest vector subspace of* $T_G(\mathbf{C})$ *defined over* $\bar{\mathbf{Q}}$ *which contains* $\bar{\mathbf{Q}}$ *is a* $\bar{\mathbf{Q}}$*-algebraic Lie sub-algebra of* $T_G(\mathbf{C})$.

§4. MULTIHOMOGENEOUS SITUATION

Let $d_0 \geq 0$ $d_1 \geq 0$ $d_2 \geq 0$ be non negative integers with $d = d_0+d_1+d_2 \geq 2$. Let G_2 be a commutative algebraic group, which is defined over $\bar{\mathbf{Q}}$, of dimension d_2. We define $G = \mathbf{G}_a^{d_0} \times \mathbf{G}_m^{d_1} \times G_2$. Then, with the notations of §3, we have

$$\Lambda_G = \bar{\mathbf{Q}}^{d_0} \times L^{d_1} \times \Lambda_{G_2}.$$

Let V be a $\mathbf{C}$-vector subspace of $T_G(\mathbf{C})$, of dimension n. We denote by t the dimension of the $\mathbf{C}$-vector subspace of $T_G(\mathbf{C})$ generated by $V \cap T_G(\bar{\mathbf{Q}})$, and by k the rank over $\mathbf{Z}$ of the intersection of V with the kernel of $\exp_G$ (this kernel is a discrete subgroup of $T_G(\mathbf{C})$).

THEOREM 4.1. *Assume that* V *does not contain a non-zero algebraic Lie sub-algebra of* $T_G(\mathbf{C})$ *defined over* $\bar{\mathbf{Q}}$. *Then* $V \cap \Lambda_G$ *is a* $\mathbf{Q}$*-vector space of dimension at most*

$$(d_1+2d_2-k)(d-t-1).$$

This result generalizes Theorem 2.1 (choose $d_2 = 0$), hence it contains Theorem 1.2. Theorem 3.2 follows also, by taking $d_0 = d_1 = 0$.

Theorem 4.1 is proved in [Wa2] when V is a hyperplane ($n = d-1$), and we will deduce the general case in §5.

Here is an example, with $d_0 = 0$, $d_1 = 2$, $d_2 = 1$, $t = 1$, $k = 1$:

COROLLARY 4.2: *Let p be an elliptic function of Weierstrass with algebraic invariants g_2, g_3; further, let ω be a non-zero period of p, and let u_1, u_2, u_3 be three complex numbers, such that ω, u_1, u_2, u_3 are $\mathbf{Q}$-linearly independent, and $p(u_1)$, $p(u_2)$, $p(u_3)$ are algebraic numbers. Furthermore, let $\log\alpha_1$, $\log\alpha_2$, $\log\alpha_3$ be three $\mathbf{Q}$-linearly independent elements of $\mathbf{L}$. Then one at least of the three numbers*

$$e^{u_1 \cdot \alpha_1^{\omega/2i\pi}}, \quad e^{u_2 \cdot \alpha_2^{\omega/2i\pi}}, \quad e^{u_3 \cdot \alpha_3^{\omega/2i\pi}}$$

is transcendental.

PROOF: We take $G = G_m^2 \times E$, where E is the elliptic curve associated to p. In $T_G(\mathbf{C}) = \mathbf{C}^3$, we have $\wedge_G = L^2 \times \wedge_E$, and we take for V the hyperplane of equation $\omega z_1 - 2i\pi(z_2 - z_3) = 0$. From Theorem 4.1 we

deduce that $\dim_{\mathbf{Q}}(V \cap \Lambda_G) \leq 3$, and therefore if the four points.

$(2i\pi,0,-\omega)$, $(\log\alpha_1,\log\beta_1,u_1)$, $(\log\alpha_2,\log\beta_2,u_2)$, $(\log\alpha_3,\log\beta_3,u_3)$ are in Λ_G and $\mathbf{Q}$-linearly independent, then one at least of them is not in V.

§5. PROOFS

a) PROOF OF THEOREM 1.1. From [Wa2] we deduce that, under the assumptions of Theorem 1.1, there exists an algebraic subgroup G' of G, which is defined over $\bar{\mathbf{Q}}$, with $G' \neq G$, such that

$$\dim_{\mathbf{Q}}(\Lambda \cap V/\Lambda \cap V \cap T_{G'}) \leq \frac{n}{d-n} \dim G/G'.$$

By induction we have also

$$\dim_{\mathbf{Q}} \Lambda \cap V \cap T_{G'} \leq n_1(n_1+1),$$

where $n_1 = \dim V \cap T_{G'}$. Let $d_1 = \dim G'$. Since V does not contain $T_{G'}$, we have $n_1 < d_1$, and

$$\dim_{\mathbf{Q}} \Lambda \cap V \leq \frac{n}{d-n}(d-d_1) + n_1(n_1+1).$$

There is no loss of generality in assuming that the

Zariski closure of $\exp_G V$ is $G(C) = C^{*d}$. Therefore $V \cap T_{G'} \neq V$, hence $n_1 < n$. The desired result then follows from the following lemma:

LEMMA 5.1: *For* $d > n > n_1$ *and* $d_1 > n_1$, *we have*

$$n(d-d_1)+(d-n)(n_1+1)n_1 \leq (d-n)(n+1)n.$$

PROOF: Notice first that the left hand side is an increasing function of n_1.

a) Assume $2n \leq d+d_1$. Then $d-d_1 \leq 2(d-n)$ and

$$d-d_1+(d-n)(n-1) \leq (d-n)(n+1),$$

which gives what we want since $n_1 \leq n-1$.

b) Assume $2n > d+d_1$. Therefore we get $n \geq d_1-1$, hence

$$n(n-d_1+1)+d_1(d_1-1) \leq n(n+1),$$

which gives the desired result when $n_1 = d_1-1$ and $n = d-1$. We deduce

$$n(d-d_1)+(d-n)d_1(d_1-1) \leq (d-n)(n+1)n.$$

Indeed, this inequality holds for $d = n+1$, and the difference between the coefficient of d in the left hand side and the coefficient of d in the right hand side is

$$n(n+1)-d_1(d_1-1)-n = n^2-d_1(d_1-1) > 0.$$

Since $n_1 \leq d_1-1$, this concludes the proof.

The same proof gives Theorem 3.2.

b) PROOF OF THEOREM 4.1: This result is proved in [Wa2] in the case where V is a hyperplane of $T_G(\mathbf{C})$. Therefore it is sufficient to prove:

LEMMA 5.2: *Let* V *be a subspace of* $T_G(\mathbf{C})$ *which does not contain any non-zero* $\bar{\mathbf{Q}}$*-algebraic Lie sub-algebra of* $T_G(\mathbf{C})$. *Then there exists a hyperplane* H *of* $T_G(\mathbf{C})$, *defined over* $\bar{\mathbf{Q}}$, *which contains* V, *and which does not contain any non-zero* $\bar{\mathbf{Q}}$*-algebraic Lie sub-algebra of* $T_G(\mathbf{C})$.

PROOF: We write V as intersection of hyperplanes $H_1,\ldots,H_{d-n}$, where each H_j is the kernel of a linear form L_j on $T_G(\mathbf{C})$. We take for H the kernel of a generic linear combination $t_1L_1+\ldots+t_{n-d}L_{n-d}$. The points $(t_1,\ldots,t_{n-d})$ in $\mathbf{C}^d$ for which the corresponding H does not satisfies the desired property belong to a set of measure zero (for the Lebesgue measure on $T_G(\mathbf{C}) \simeq \mathbf{C}^d$).

§6. FURTHER PROBLEMS

It should be possible to deduce an estimate containing both Theorem 4.1 and Theorem 3.1. From [Wa2] one could expect the bound

$$(6.1) \qquad (n-t)\,(d_1+2d_2-k)/(d-n)$$

for the dimension of $V \cap \Lambda$ in Theorem 4.1. Indeed, Theorem 4.1 of [Wa2] states that if $\dim_{\mathbf{Q}}(V \cap \Lambda)$ exceeds the number in (6.1), then some kind of degeneracy occurs: in particular there is a $\bar{\mathbf{Q}}$-algebraic Lie sub-algebra of positive dimension in $T_G(\mathbf{C})$ such that many points of $V \cap \Lambda$ are in $V \cap \Lambda \cap T_{G'}(\mathbf{C})$. However we cannot garantee in general that $T_{G'}(\mathbf{C})$ is contained in V. The trivial case $G' = G$ is excluded by requiring that V is not contained in any $\bar{\mathbf{Q}}$-algebraic Lie sub-algebra $T_{G'}(\mathbf{C})$ different from $T_G(\mathbf{C})$ (this is anyway a natural assumption if we want to improve the bound of Theorem 4.1 when n is smaller than d-1). This assumption is not sufficient to get the upper bound (6.1) for $\dim_{\mathbf{Q}}(V \cap \Lambda)$, even in the situation of §1, as shown by the following example: we choose $n > d/2$, we take $\log\alpha_1,\ldots,\log\alpha_d$ linearly independent in L, and we define V in $\mathbf{C}^d$ by the d-n equations

$$z_1\log\alpha_1+\ldots+z_{2n-d+2}\log\alpha_{2n-d+2} = 0,$$

$$z_{d-2k-1}\log\alpha_{d-2k-1}+z_{d-2k}\log\alpha_{d-2k} = 0, \qquad (0 \le k \le d-n-2).$$

Then V contains at least

$$\left\{ \begin{matrix} 2n-d+2 \\ 2 \end{matrix} \right\} + d - n - 1 = \frac{1}{2} \cdot d(d-1) - 2n(d-n-1)$$

points of L^d, and this can be larger than $nd/(d-n)$ (for instance when $d \geq 18$ and $n = d-3$).

Another related but quite different problem is to work out the consequences of Schanuel's conjecture for the problem which we considered in §1 and §2, or more precisely the consequences of the assertion according to which linearly independent elements of L are algebraically independent(*). It seems one should investigate the linear subvarieties of the algebraic hypersurface $\det(X_{ij}) = 0$ in P_{d^2-1}.

The next step could be to study $C \cap L^d$ (or more generally $C \cap \Lambda_G$ in the situation of §3), when C is a curve in C^d (resp. in $T_G(C)$). The example of the surface $z_1 z_2 = z_3 z_4$ shows that algebraic varieties of higher dimension can contain a lot of points of L^d (resp. Λ_G).

(*) Added in proof (December 1988). This problem has been recently solved by Damien Roy.

REFERENCES

[B] BERTRAND, D., *Lemmes de zeros et nombres transcendants*; Seminaire Bourbaki, Novembre 1985, N°652; Asterisque 145-146 (1987), 21-44.

[E] EMSALEM, M., Sur les idéaux dont l'application d'Artin dans une Z_p-extension est triviale: *J. reine angew. Math. (Crelle J.)*, 382 (1987), 181-198.

[Wa1] WALDSCHMIDT, M., A lower bound for the p-adic rank of the units of an algebraic number field, *Coll. Math. Soc. Janos Bolyai* 34, Topics in Classical Number Theory, Budapest (1981), p. 1617-1650.

[Wa2] WALDSCHMIDT, M., On the transcendence methods of Gel'fond and Schneider in several variables, *Proc. Conf. Durham 1986*, (ed. A. Baker), *New Advances in Transcendence Theory*, Cambridge Univ. Press, (1988), p. 375-398.

WALDSCHMIDT, M.

C.N.R.S.-U.A. 763
Problèmes diophantiens
Institut Henri Poincaré
11. rue P. et M. Curie
75231 PARIS CEDEX 05., F r a n c e

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

ON THE PRACTICAL SOLUTION OF THUE-MAHLER EQUATIONS, AN OUTLINE

B.M.M. de WEGER

This paper was presented at the Colloquium on Number Theory, July 20-25, 1987, in Budapest. It reports on work that was done in close cooperation with N. Tzanakis. The author was supported by the Netherlands Foundations for Mathematics (SMC) with financial aid from the Netherlands Organization for the Advancement of Pure Research (ZWO). He also thanks Shell Nederland B.V. for financial support.

Dedicated to Alda, with love.

1. INTRODUCTION

Let $F(X,Y)$ be a binary form with at least three distinct linear factors over $\mathbb{C}$. Let $p_1, \ldots, p_s$ be fixed distinct prime numbers. The diophantine equation

$$F(X,Y) = \pm \prod_{i=1}^{s} p_i^{n_i}$$

in the variables $X, Y \in \mathbb{Z}$, $n_1, \ldots, n_s \in \mathbb{N}_0$, with $(X,Y) = 1$, is known as a Thue-Mahler equation. It was proved by Mahler [1933] that this equation has only finitely many solutions, and by Sprindžuk and Vinogradov [1968] and Coates [1969], [1970] that all the solution can, at least in principle, be determined effectively, since an effectively computable upper bound for the variables can be derived from the p-adic theory of linear forms in logarithms. For the history of this equation we refer to Shorey and Tijdeman [1986], Chapter 7.

It is the purpose of this paper to show that it is possible to solve Thue-Mahler equations, not only in principle, but in practice, by reducing the above mentioned upper bounds considerably. This is done by a combination of real and p-adic computational diophantine approximation techniques, based on the L^3-algorithm for reducing bases of lattices (cf. Lenstra, Lenstra and

Lovász [1982], and for an integral version de Weger [1987[a]]). The method can be considered as a p-adic analogue of the method for solving Thue equations, on which Tzanakis [1987] reports. For a more general treatment of the application of the L^3-algorithm to solving diophantine equations, see de Weger [1987[b]], especially Chapter 3.

A similar idea, but without using the L^3-algorithm, was used by Agrawal, Coates, Hunt and van der Poorten [1980], who determined all solutions of the equation

$$X^3 - X^2 \cdot Y + X \cdot Y^2 + Y^3 = \pm 11^n .$$

This is, to the author's knowledge, one of the only two examples in the literature where a Thue-Mahler equation has been solved completely, the other one being

$$X^3 + 3 \cdot Y^3 = 2^n ,$$

which was solved by Tzanakis [1984] by a different method. It is an example of the simplest kind, in view of the fact that the cubic field $Q(\theta)$, where θ is a root of $F(x,1) = 0$, has only one fundamental unit, and there occurs only one prime. Therefore it was sufficient to use two-dimensional real continued fractions and one-dimensional p-adic continued fractions, in stead of the

more complicated L^3-algorithm (which was not yet available at the time). We now extend the method to the situation where there are more than one fundamental units, and more than one primes, thus to the general situation. Then the L^3-algorithm becomes very useful. (However, a more or less technical problem will show up for forms of large degree, that has not yet been solved). In this paper we only give an outline of the method. In a paper to be published. Tzanakis and the present author have used the method of this paper to solve the Thue-Mahler equation

$$X^3 - 3 \cdot X \cdot Y^2 - Y^3 = \pm 3^{n_1} \cdot 17^{n_2} \cdot 19^{n_3}.$$

Here, two fundamental units and three primes are involved. Note that if (X_0, Y_0) is a solution, then so is $(-Y_0, X_0+Y_0)$. Thus solutions come in six-tuples, of which exactly one satisfies $X > 0$ and $Y \geq 0$. It turns out that there are 26 such solutions, all satisfying $X \leq 896$, $Y \leq 379$, $n_1 \leq 1$, $n_2 \leq 3$, $n_3 \leq 5$.

2. UPPER BOUNDS

In this section we give a short account of the classical arguments for deriving upper bounds for the solutions of a Thue-Mahler equation. Any Thue-Mahler

equation reduces in a routine manner to a finite number of equations of the type

$$(1) \qquad \delta_1 \cdot \beta_1 - 1 = \delta_2 \cdot \beta_2 ,$$

where δ_1, δ_2 are algebraic constants, and β_1, β_2 are of the form

$$\frac{X - Y \cdot \theta'}{X - Y \cdot \theta''} ,$$

where θ', θ'' are conjugates of the root θ of $F(x,1) = 0$. From the Thue-Mahler equation it follows that there exist algebraic units $\varepsilon_1, \ldots, \varepsilon_r$ and algebraic constants $\alpha, \pi_1, \ldots, \pi_t$, and rational integers $\nu_1, \ldots, \nu_t$ closely related to $n_1, \ldots, n_s$, such that β_1, β_2 are of the type

$$\alpha' \cdot \prod_{i=1}^{r} \varepsilon_i'^{a_i} \cdot \prod_{j=1}^{t} \pi_j'^{\nu_j} ,$$

the prime sign indicating a proper conjugate, and the a_i being rational integers. For a given solution $(X,Y,n_1,\ldots,\ldots,n_s)$ of the Thue-Mahler equation and for a given index $i \in \{1,\ldots,s\}$ these conjugates can be taken in such a way that (supposing that n_i is large enough)

$$\operatorname{ord}_{p_i}(\beta_1) = c_1, \ \operatorname{ord}_{p_i}(\beta_2) = c_2 + c_3 \cdot n_i ,$$

where c_1, c_2, c_3 are small constants. Put

$$A = \max|a_i|, \ N = \max(n_i), \ H = \max(A, N).$$

The theory of p-adic linear forms in logarithms (see e.g. Yu [1987]) provides an explicit constant C_1 such that

$$\operatorname{ord}_{p_i}(\delta_1 \cdot \beta_1 - 1) < C_1 \cdot \log H .$$

It follows that a constant C_2 such that

$$N < C_2 \cdot \log H$$

can be computed explicitly. It will be very large in practice (even for a Thue-Mahler equation of low degree it may be as large as 10^{50}). Put

$$\mu = \prod_{j=1}^{t} \pi_j^{\nu_j} .$$

Then $|\log|\mu|| < c_4 \cdot N < C_3 \cdot \log H$. Suppose that A is large enough. Then, since β_1, β_2 have the form

$$\alpha' \cdot \mu' \cdot \prod_{i=1}^{r} \varepsilon_i'^{a_i} ,$$

the conjugates can be taken such that β_2 is close to 0, namely

$$|\beta_2| < c_5 \cdot |\mu'| \cdot \exp(-c_6 \cdot A)$$

for small constants c_5, c_6. The theory of real linear forms in logarithms (see e.g. Waldschmidt [1980]) provides an explicit (large) constant C_4 such that

$$|\delta_1 \cdot \beta_1 - 1| > \exp(-C_4 \cdot \log A).$$

Combining all the estimates it follows that H is bounded by an explicit constant C_0.

3. REDUCING UPPER BOUNDS

Above we derived an upper bound C_0 for H, using an interplay between p-adic and real arguments. We now show, again combining p-adic and real arguments, and using a computer, how this upper bound C_0 can be reduced to an upper bound for H of the size of log C_0. See also de Weger [1987[b]], Chapter 3.

Our computational tool is the L^3-algorithm, that is capable of finding good lower bounds for the length of the shortest nonzero vector in a given lattice Γ, and for the distance of a given point to the nearest lattice point. These lower bounds are expected to be of the size

$$\det(\Gamma)^{1/\dim(\Gamma)} .$$

Write

$$\beta_1 = \delta \cdot \prod_{i=1}^{r} \varepsilon_i^{a_i} \cdot \prod_{j=1}^{t} \pi_j^{\nu_j} .$$

We assume that we know the numbers δ, ε_i, π_j explicitly, and that we can compute their complex and p-adic values

to arbitrary (but finite) precision.

First we make a p-adic step. Put for a fixed prime $p \in \{p_1,\ldots,p_s\}$

$$\eta_i = -\log_p(\varepsilon_i)/\log_p(\pi_t) \text{ for } i = 1,\ldots,r,$$

$$\tau_j = -\log_p(\pi_j)/\log_p(\pi_t) \text{ for } j = 1,\ldots,t-1,$$

$$\varphi = \log_p(\delta)/\log_p(\pi_t) .$$

We assume that these numbers η_i, τ_j, φ are in $\mathbf{Q}_p$, and not in some algebraic extension. This is in general not obvious, but it can be proved in the cases where the degree of the binary form $F(X,Y)$ is not larger than 4. (This is the unsolved problem announced in the introduction)*). Further, we may assume without further loss of generality that they are even in $\mathbf{Z}_p$. For any p-adic integer γ and for any $m \in \mathbf{N}_0$ we denote by $\gamma^{(m)}$ the unique rational integer such that

$$\gamma \equiv \gamma^{(m)} \pmod{p^m},\ 0 \le \gamma^{(m)} \le p^m - 1.$$

We now define the lattice Γ_m by the matrix

*) Note added in proof: This problem is solved now, due to J.-H. Evertse.

$$\begin{bmatrix} 1 & & & & & & \\ & \ddots & & 0 & & & \\ & & 1 & & & & \\ & 0 & & 1 & & & \\ & & & & \ddots & & \\ & & & & & 1 & \\ \eta_1^{(m)} & \cdots & \eta_r^{(m)} & \tau_1^{(m)} & \cdots & \tau_{t-1}^{(m)} & p^m \end{bmatrix},$$

where the column vectors of the matrix are the basis vectors of Γ_m. Here we take m large enough, such that p^m is of the size C_o^{r+t}. Then the distance of the point

$$\underline{x} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ \varphi^{(m)} \end{bmatrix}$$

to the nearest lattice point can be bounded from below, from the result of the L^3-algorithm (cf. de Weger [1987^b], Section 3.4). It will, in a typical situation, be at least $c_7 \cdot C_o$ for a suitable constant c_7 (small compared to C_o). If c_7 is not large enough, one should try with a larger value of m. For a solution $a_1, \ldots, a_r$, $\nu_1, \ldots, \nu_t$ of (1) it follows easily that if $\mathrm{ord}_p(\delta_1 \cdot \beta_1 - 1) \geq$ $\geq m + \mathrm{ord}_p(\log_p(\pi_t))$ then

$$\underline{x} + \begin{bmatrix} a_1 \\ \vdots \\ a_r \\ \nu_1 \\ \vdots \\ \nu_t \end{bmatrix} \in \Gamma_m \quad .$$

Now $\mathrm{ord}_p(\delta_1 \cdot \beta_1 - 1) = c_2 + c_3 \cdot n_i$, where i is the index such that $p = p_i$. This contradicts the upper bound C_o. Hence

$$n_i < m/c_3 + (\mathrm{ord}_p(\log_p(\pi_t)) - c_2)/c_3 \ ,$$

which is only of size log C_o. We repeat this procedure for all $p = p_1, \ldots, p_s$, and find a reduced upper bound N_o for N, of size log C_o.

Next we make a real step. Choose a constant C of size $C_o^r \cdot N_o^t$, large enough. Put

$$\eta_i = [C \cdot \log|\varepsilon_i|] \quad \text{for } i = 1, \ldots, r \ ,$$

$$\tau_j = [C \cdot \log|\pi_j|] \quad \text{for } j = 1, \ldots, t \ ,$$

$$\varphi = - [C \cdot \log|\delta|] \ .$$

Define the lattice Γ by the matrix

$$\begin{bmatrix} C_0/N_0 & & & & & \\ & \ddots & & 0 & & \\ & & \ddots & & & \\ & & & \ddots & & \\ 0 & & C_0/N_0 & & & \\ & & & 1 & \ddots & \\ & & & & \ddots & \\ & & & & & 1 \\ \tau_1 \ldots \tau_t & & \eta_1 \ldots \eta_{r-1} & & \eta_r & \end{bmatrix},$$

and suppose that C is so large that the distance from the fixed point

$$\underline{x} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ \varphi \end{bmatrix}$$

to the nearest lattice point is at least $c_8 \cdot C_0$ for a small constant c_8, following from the L^3-algorithm. It follows that $|\delta_1 \cdot \beta_1 - 1| > c_9 \cdot C_0/C$ for a small constant c_9. By the upper bounds for $|\beta_2|$ and $|\log|\mu||$ a reduced bound for A follows, which is of size log C_0.

We now may repeat the whole procedure, with the bound C_0 replaced by the new, reduced upper bound for H, that is of size C_0, until no further improvement is reached. Then we can check all remaining possibilities, for example by

using the fact that for a solution of the Thue-Mahler equation, the quotient X/Y must be near to one of the conjugates of the root θ (in the p-adic sense). We also may use some more subtle techniques using approximation lattices, such as the Fincke and Pohst algorithm (cf. de Weger [1987^a], [1987^b]).

We expect that it is possible in this way to solve completely any Thue-Mahler equation of small degree within a few minutes of computer rime.

REFERENCES

AGRAWAL, M.K., COATES, J.H., HUNT, D.C. and van der POORTEN, A.J. [1980], Elliptic curves of conductor 11, *Math. Comp.* 35, 991-1002.

COATES, J. [1969], An effective p-adic analogue of a theorem of Thue, *Acta Arith.* 15, 279-305.

COATES, J. [1970], An effective p-adic analogue of a theorem of Thue II: The greatest prime factor of a binary form, *Acta Arith.* 16, 399-412.

LENSTRA, A.K., LENSTRA jr., H.W. and LOVÁSZ, L. [1982], Factoring polynomials with rational coefficients, *Math. Ann.* 261, 515-534.

SHOREY, T.N. and TIJDEMAN, R. [1986], *Exponential diophantine equations*, Cambridge University Press.

SPRINDŽUK, V.G. and VINOGRADOV, A.I. [1968], The representation of numbers by binary forms (Russian), *Mat. Zametki 3*, 369-376.

TZANAKIS, N. [1984], The complete solution in integers of $x^3 + 3 \cdot y^3 = 2^n$, *J. Number Th.* 19, 203-208.

TZANAKIS, N. [1987], On the practical solution of the Thue equations; an outline, these Proceedings.

TZANAKIS, N. and de WEGER, B.M.M. [1987], On the practical solution of the Thue equation, *Memorandum* 668, Faculty of Applied Mathematics, University of Twente, to appear in *J. Number Th.*

WALDSCHMIDT, M. [1980], A lower bound for linear forms in logarithms, *Acta Arith.* 37, 257-283.

de WEGER, B.M.M. [1987[a]], Solving exponential diophantine equations using lattice basis reduction algorithms, *J. Number Th.* 26, 325-367.

de WEGER, B.M.M. [1987[b]], *Algorithms for diophantine equations*, PhD Thesis, University of Leiden, to appear as *CWI-Tract.*

YU, K.R. [1987], Linear forms in the p-adic logarithms, *Report* MPI/87-20, Max Planck Institut für Mathematik, Bonn, to appear in *Acta Arith.*

de WEGER, B.M.M.
Faculty of Applied Mathematics,
University of Twente,
P.O. Box 217,
7500 AE ENSCHEDE,
The Netherlands

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

VALUES OF GAUSS' CONTINUED FRACTIONS

WOLFART, J.

SUMMARY: It is shown that - up to some obvious exceptions - Gauss' continued fractions with rational parameters a, b, c, take transcendental values for algebraic arguments z.

$$F(a,b,c;z) = 1 + \frac{ab}{c}z + \frac{a(a+1)b(b+1)}{2!\ c(c+1)}z^2 + \dots$$

denotes the hypergeometric function and

$$G(z) = G(a,b,c;z) = \frac{F(a,b+1,c+1;z)}{F(a,b,c;z)} = \frac{1}{|1} - \frac{g_1 z}{|1} - \frac{g_2 z}{|1} - \dots$$

the associated Gauss' continued fraction with coefficients

$$g_{2n-1} = \frac{(a+n-1)\ (c-b+n-1)}{(c+2n-2)\ (c+2n-1)}$$

$$g_{2n} = \frac{(b+n)\quad(c-a+n)}{(c+2n-1)\,(c+2n)}$$

(compare [Kℓ, p.11]). In some recent papers (Vasilenko [Va], Huttner [Hu]) questions of irrationality and irrationality measures for the values of G(a,b,c;z) with rational parameters at algebraic arguments z are treated. In the present contribution a different approach is proposed: We use results of Wüstholz [WW],[Wü 1 , 2] about transcendence and $\bar{\mathbb{Q}}$ - linear independence of periods on abelian varieties to prove the transcendence of G(z), without giving measures.

The usual hypotheses $|z|<1$ for the definition of F and z not real ≥ 1 for G (compare [Pe, p.151 ff.]) are irrelevant for our method, because the integral representations of F and G used in the proof are valid for any analytic continuation; only the integration path has to be moved. We prove

THEOREM 1. *Let* a,b,c *be rational parameters,* $c \neq 0, -1, -2, \ldots$, *and suppose that* G(a,b,c;z) *is not an algebraic function of* z. *Then at almost all algebraic arguments* $\xi = z$, *Gauss' continued fraction has transcendental values.*

REMARKS. 1) If in addition $a, b, a-c, b-c, \notin \mathbb{Z}$ "almost all" means " $\xi \notin \bar{\mathbb{Q}} - \{0, 1\}$" ; only for integral a , b , a-c or b-c are a finite number of further exceptions possible.

2) It is explicitly known under which conditions on a , b , c Gauss' continued fractions are algebraic functions of z. If a , b , a-c , $b - c \notin \mathbb{Z}$, both $F(a,b,c;z)$ and $F(a,b+1, c+1;z)$ are periods on the same abelian variety (up to a normalizing factor, see proof below), so their monodromy groups are isomorphic [Wo 2, §5] and a classical result of H.A. Schwarz [Schw] says: $F(a,b,c;z)$ is an algebraic function of z iff the monodromy group Δ is finite iff $F(a,b+1, c+1; z)$ is an algebraic function of z, and the triples (a,b,c) for which this situation occurs are explicitly known ([Schw] or [Wo2,§6]). On the other hand we will show that the condition "Δ infinite" is sufficient to prove the transcendence of $G(a,b,c;\xi)$, $\xi \notin \bar{\mathbb{Q}} - \{0, 1\}$, so it implies the transcendence of $G(a,b,c;z)$ as function of z. Of course, a direct proof using ramification properties of G in the points 0 , 1 and ∞ is also possible.

3) For integers a, b , a-c or b-c the situation is different, as the example of the algebraic function

$$F(1,0,1;z) = 1$$

and the transcendental function

$$F(1,1,2;z) = -\frac{1}{z}\log(1-z)$$

shows. This example is typical; using Kummer's and Gauss' transformations, the proof will reduce the problem to the case $b = 0$, so that $G(a,b,c;z)$ is a transcendental function iff at least one of the functions $F(a,b,c;z)$ and $F(a,b+1,c+1;z)$ is transcendental.

4) There are other possibilities to construct continued fractions as quotients of contiguous hypergeometric functions ([Pe, p.283 ff.]). For those, the statement of theorem 1 is valid as well. In fact, theorem 1 and its generalizations follow from

THEOREM 2. *Let* a, b, c *be rationals,* n, m, ℓ *integers, neither* c *nor* $c + \ell = 0, -1, -2, \ldots$. *If the associated hypergeometric functions*

$F(a,b,c;z)$ *and* $F(a+n,b+m,c+\ell z)$

are linearly independent over the field $\overline{\mathbb{Q}(z)}$ *of algebraic functions of* z, *then their values are* $\overline{\mathbb{Q}}$ *- linearly independent at almost all algebraic arguments* $\xi = z$.

REMARK 5) Theorem 2 is only a formal generalization of theorem 1 because in general any two associated hypergeometric functions form a basis of the $\mathbb{Q}(z)$-vector

space generated by all associated hypergeometric functions [Kℓ, §1]. The assumption of $\overline{\mathbb{Q}(z)}$ - linear independence can be weakened to $\mathbb{Q}(z)$ - linear independence and transcendence of at least one of the functions. This is needed to exclude not only the case of finite monodromy group, but also trivial counterexamples as

$$F(a,a+1,c;z) \qquad \text{and} \qquad F(a+1,a,c;z).$$

For theorem 2, remark 1 is no longer true; as the argument $z = \xi = \frac{c-1}{2c-a-b-1}$ in Gauss' relation

$$c[c-1-z(2c-a-b-1)]\ F(a,b,c;z)+(c-a)(c-b)\ F(a,b,c+1;z)=$$
$$= c(c-1)(1-z)\ F(a,b,c-1;z)$$

shows, a finite number of exceptional arguments does occur.

We start the *proof* of theorem 2 under the additional assumption $a\ ,\ b\ ,\ a-c,\ b-c \notin \mathbb{Z}$. As in [Wo 1 , 2] we reduce the problem to the question of the existence of a certain abelian subvariety V in another abelian variety T. But in contrast to the transcendence problem for F(a,b,c;z) itself our subvariety V will have such a special position in T that its existence is much easier to disprove than in [Wo 1 , 2]. We consider in the integral representation

$$F(a,b,c;z) = \frac{1}{B(b,c-b)} \int_0^1 x^{b-1}(1-x)^{c-b-1}(1-zx)^{-a}dx$$

the integration path as "Pochhammer cycle" around $x = 0$ and $x = 1$ [Kℓ, p.80] on the curve

$$X(N,z): \qquad y^N = x^A (1-x)^B (1-zx)^C ;$$

here $N \in \mathbb{N}$ is the least common denominator of a,b,c,

$$A := (1-b)N , \quad B := (b+1-c)N , \quad C := aN .$$

In contrast to [Wo 1 , 2] we do not exclude the case $c \in \mathbb{N}$; it causes difficulties only if in additon $z = 0$ or 1 , where

$$\eta = \frac{dx}{y} = x^{b-1} (1-x)^{c-b-1} (1-zx)^{-a} dx$$

becomes a differential of the third kind. In all other cases η is of the second kind, as is also the differential

$$\eta^* = \frac{x^m (1-x)^{\ell-m} (1-zx)^{-n}}{y} =$$

$$= x^{b+m-1} (1-x)^{c-b+\ell-m-1} (1-zx)^{-a-n} dx$$

occuring in the integral representation of $F(a+n,b+m,c+\ell;z)$.

Since for $z = 0$ and 1 the homology of the curve $X(N,z)$ breaks down and $G(a,b,c;z)$ becomes algebraic or singular, we assume in the following $z \neq 0, 1$, and we restrict our attention to algebraic z. Then $X(N,z)$ and η , η^* are defined over $\bar{\mathbb{Q}}$; this extends also to the

Jacobian of X(N,z) - or more correctly to the Jacobian of a non-singular model of X(N,z) - and to the abelian subvariety T of Jac X(N,z) which has now to be constructed: X(D,z) denotes a curve as X(N,z) with the same exponents A, B, C, only N is replaced by a proper divisor D of N; then, up to isogeny "$\triangleq$", there is a splitting ([Wo 1, Satz 1], [Wo 2, §2])

$$\text{Jac } X(N,z) = T \oplus \sum_{\substack{D \mid N \\ D \neq N}} \text{Jac } X(D,z)$$

whose essential factor T is an abelian variety of dimension $\phi(N)$ (Euler's function). As a complex torus it can be written as $\mathbb{C}^{\phi(N)}/\Lambda$ with a period lattice of the first kind

$$(1)\quad \Lambda := \{(\sigma_n(u)\int_0^1 \omega + \sigma_n(v)\int_{1/z}^{\infty} \omega)_{\omega \in S} \mid u,v \in \mathbb{Z}\ [\zeta_N]\}\ ,$$

where the notions are explained as follows: The vector space $H^0(X(N,z),\Omega)$ of first kind - differentials on X(N,z) splits into eigenspaces under the operation of the automorphism

$$K : X(N,z) \longrightarrow X(N,z) : \begin{cases} x \mapsto x \\ y \mapsto \zeta_N^{-1} y \end{cases}$$

of the curve ($\zeta_N := e^{\frac{2\pi i}{N}}$). Therefore, a basis can be given consisting of eigendifferentials

$$y^{-n} q(x)\, dx \qquad \text{with} \qquad q \in \mathbb{Q}(x).$$

The set S corresponding to the coordinates of $\Lambda \subset \mathbb{C}^{\phi(N)}$ consists of those basis - differentials for the eigenvalues ζ_N^n with $n \in (\mathbb{Z}/N\mathbb{Z})^*$; σ_n denotes the corresponding embedding

$$\mathbb{Z}[\zeta_N] \to \mathbb{C} \quad \text{with} \quad \zeta_N \mapsto \zeta_N^n \quad ,$$

and $\int_0^1$, $\int_{1/z}^{\infty}$ denote period integrals over fixed Pochhammer cycles around 0 , 1 and $\frac{1}{z}$, ∞ respectively.

If $<\alpha>$ denotes the fractional part $\alpha - [\alpha]$ of $\alpha \in \mathbb{Q}$, the multiplicity of this embedding σ_n in Λ or - in other words - the dimension of the κ -eigenspace of $H^0(X(N,z),\Omega)$ with eigenvalue ζ_N^n is given by

$$(2) \qquad r_n := <n\tfrac{A}{N}> + <n\tfrac{B}{N}> + <n\tfrac{C}{N}> - <n\tfrac{A+B+C}{N}>$$

[Wo 1, §4]. So r_n is always 0 , 1 or 2 with $r_n + r_{-n} = 2$. The remaining basis differentials with eigenvalues ζ_N^n , $(n,N) \neq 1$, belong to the subvarieties Jac X(D,z) of Jac X(N,z).

Since both normalizing factors B(b,c-b) and B(b+m,c-b+ℓ-m) in the integral representation of any two associated functions F(a,b,c;z) and F(a+n,b+m,c+ℓ;z) differ only by a rational factor, theorem 2 will follow from the $\bar{\mathbb{Q}}$ - linear independence of $\int_0^1 \eta$ and $\int_0^1 \eta^*$. Now we can read these integrals as periods of the second kind on T, and at first we have to ask if η and η^* are

$\bar{\mathbb{Q}}$ - linearly independent in $H^1_{DR}(T)$. This vector space of differentials of the second kind splits in κ-eigenspaces in the same way as $H^0(X(N,z),\Omega)$ and $H^0(T,\Omega)$, and an easy calculation reading Gauss' "relationes inter functiones contiguas" as relations between differentials modulo exact differentials shows that all these eigenspaces are two-dimensional. η and η^*lie in the eigenspace of $H^1_{DR}(T)$ belonging to the eigenvalue ζ_N . By the hypotheses of the theorem and by Gauss' relations, all functions associated to $F(a,b,c;z)$ are $\mathbb{Q}(z)$ - linear combinations

(3) $\quad r(z)\, F(a,b,c;z) + s(z)\, F(a+n,b+m,c+\ell;z)$;

for all $z \in \mathbb{Q}$ with the possible exception of the poles of r and s this implies that η and η^* generate their eigenspace in $H^1_{DR}(T)$, so they are linearly independent for almost all $z \in \bar{\mathbb{Q}}$. A closer look on Gauss'relations [EMOT] shows even more: For contiguous functions, i.e. for the case

$$|n| + |m| + |\ell| = 1 ,$$

or for the case $m = \ell = 1$, $n = 0$ occuring in theorem 1 the only possible poles of r and s in (3) are $\xi = z = 0$ and 1 (hence remark 1).

So we will assume that η and η^* are $\bar{\mathbb{Q}}$ -linearly independent but the periods $\int_0^1 \eta$ and $\int_0^1 \eta^*$ were $\bar{\mathbb{Q}}$ - linearly dependent. Then there would exist an (eigen-) differential $\eta^{**} \neq 0$ in $H^1_{DR}(T)$ whose periods

$$\int_\gamma \eta^{**} = 0$$

vanish for all Pochhammer cycles around 0 and 1. An argument due to Wüstholz ([WW, Satz 2] and [Wü 1]) shows that this is possible iff T contains a proper abelian subvariety V; this V is obviously again $\mathbb{Z}[\zeta_N]$ -invariant, so by a classical result of Shimura and Taniyama [ST] $\frac{1}{2}\ \phi(N)$ divides dim V; this implies

$$\dim V = \frac{1}{2}\,\phi(N),$$

i.e. V is an abelian variety of type CM. The eigenbasis S of $H^0(T,\Omega)$ can be chosen in such a way that exactly one half of the $\omega \in S$, say all $\omega \in S_V \subset S$, can be identified with a basis of $H^0(V,\Omega)$, so that their periods $\int_\gamma \omega$ vanish on all Pochhammer cycles around 0 and 1.

The existence of such a V is only possible if both hypergeometric functions are algebraic functions of z, as the following argument shows: If not, the monodromy group Δ is infinite (compare remark 2), and this implies the existence of one-dimensional eigenspaces of $H^0(T,\Omega)$, i.e. of an $n \in (\mathbb{Z}/N\mathbb{Z})^*$ with

$$r_n = 1 = r_{-n}$$

([Wo 1, §7] or [Wo 2, §6]). At least one such eigenspace must belong to $H^0(V,\Omega)$ since for abelian varieties of type CM $H^0(V,\Omega)$ splits into one - dimensional $\mathbb{Z}[\zeta_N]$-

eigenspaces which correspond to some $n \in (\mathbb{Z}/N\mathbb{Z})^*$ forming a representative system of $(\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\}$ ([ST], [WW] or [Wo 1, §2]). But an eigendifferential $\omega \in S_v \subset S$ generating a one-dimensional eigenspace of $H^0(T,\Omega)$ has periods $\int_\gamma \omega$ again expressible by hypergeometric functions $F(a',b',c';z)$, and these hypergeometric functions have no zeros, since their associated triangle functions map the upper and the lower half-plane onto simple hyperbolic triangles ([Wo 1], (7) and Satz 3). So we get a contradiction to $\int_\gamma \omega = 0$.

We have to complete the proof by a discussion of the exceptional cases a, b, $c-a$ or $c-b \in \mathbb{Z}$. Exchanging a and b and applying the Kummer identity

$$F(a,b,c;z) = (1-z)^{-a} F(a,c-b,c;\frac{z}{z-1})$$

we can reduce the proof to the case $b \in \mathbb{Z}$. The associated value of the normalizing Beta-factor is rational, and Gauss' relations between contiguous functions show that it is sufficient to prove the $\bar{\mathbb{Q}}$ - linear independence of

$$F(a,0,c;z) = 1 \quad \text{and} \quad F(a,1,c;z)$$

for almost all algebraic z and $c>1$. But then the transcendence of $F(a,1,c;z)$ or

$$\int_0^1 (1-x)^{c-2}(1-zx)^{-a}\,dx$$

follows as in [Wo 1, §3] from a general theorem of Wüstholz [Wü 2] on abelian integrals. Note that the

differential $(1-x)^{c-2}(1-zx)^{-a}\,dx$ is exact iff $F(a,1,c;z)$ is an algebraic function of z.

REFERENCES

[EMOT] A.ERDÉLYI, W.MAGNUS, F.OBERHETTINGER, F.G. TRICOMI, Higher transcendental functions, *Bateman manuscript project*, McGraw-Hill 1953.

[HU] M.HUTTNER, Irrationalité de certaines intégrales hypergéometriques, *J. Number Th.* 26(1987), 166-178.

[Kℓ] F.KLEIN, *Vorlesungen über die hypergeometrische Funktion*, Springer, Berlin 1933.

[Pe] O.PERRON, *Die Lehre von den Kettenbrüchen*, Bd. II, Teubner, Stuttgart 1957.

[SCHW] H.A.SCHWARZ, Über diejenigen Falle, in welchen die Gaussische hypergeometrische Reihe eine algebraische Funktion ihres vierten Elements darstellt, *Journal f.d. reine u. angew. Math.* 75(1873), 292-335.

[ST] G.SHIMURA, Y.TANIYAMA, Complex multiplication of abelian varieties and its applications to number theory, *Publ. Math. Soc. Japan*, No.6, 1961.

[VA] O.N. VASILENKO, Irrationality of the values of the Gauss hypergeometric function, Vestnik

Moskov. *Univ. Ser. I. Mat. Mekh.* 1985 No.3, 15-18,101 (Russian); *Moscow Univ. Math. Bull.* 40 (1985)No.3, 20-24 (engl. transl.), zit. nach *Math. Rev.* 87e, 11084, *Zbl. Math.* 574 (1986) 10037.

WO 1 J.WOLFART, Werte hypergeometrischer Funktionen, *Invent. math.* 92(1988)187-216.

WO 2 J.WOLFART, Functions hypergéométriques, arguments exceptionnels et groups de monodromie, *Publ. Math. Univ. P. et M. Curie* No.79, Problèmes Diophantiens 1985-1986, IX.1-IX.24.

WW J.WOLFART, G.WÜSTHOLZ, Der Überlagerungsradius gewisser algebraischer Kurven und die Werte der Betafunktion an rationalen Stellen, *Math. Ann.* 273(1985),1-15.

WÜ 1 G.WÜSTHOLZ, Some remarks on a conjecture of Waldschmidt, pp. 329-336 in "Approximations diophantiennes et nombres transcendants", *Birkhäuser*, Baselo, Boston, Stuttgart 1983.

WÜ 2 G.WÜSTHOLZ, Recent progress in transcendence theory, pp. 280-296 in "Number theory Noordwijkerhout 1983", *Springer LN in Math.* 1068, Berlin-Heidelberg-New York-Tokyo 1984.

WOLFART Jürgen

Mathematisches Seminar der Johann Wolfgang Goethe-Universität
Robert-Mayer-Str. 6-10.
D-6000 Frankfurt 1, F R G

JANOS BOLYAI MATHEMATICAL SOCIETY
Budapest, Anker köz 1-3.
H-1061
Phone: 142-741

COLLOQUIUM ON NUMBER THEORY
20-25th July, 1987
Budapest (Hungary)

LIST OF PARTICIPANTS

S. AGOU
89 Rue Garibaldi
F-69006 LYON

J.-P. ALLOUCHE
VA 226 VER de Math. et d'Info.
351 coms de la Liberation
F - 33405 TALENCE
Cedex

R. BALASUBRAMANIAN
The Institute of Math. Sci.
C.I.T. Campus
MADRAS 600113, India

M. BALAZARD
17. chemin de la cote
F-87000 LIMOGES

A. BALOG
MTA MKI
BUDAPEST,
Reáltanoda u.13-15.
H-1053

É. BAYER
Université de Genéve
Section de Mathématiques
2-4 rue de Liévre, C.P.240
CH-1211 GENÉVE 24

J. BECK
MTA MKI
BUDAPEST,
Reáltanoda u. 13-15.
H-1053

M.-J. BERTIN
16 Av. Gein Malleret
Tainville
F-94140 ALFORTVILLE

W. BOSMA
Univ. of Amsterdam
Math. Institut
Roeterstraat 15
NL-1018 WB
AMSTERDAM

B. BRINDZA
KLTE Mat. Int.
DEBRECEN
Egyetem tér 1.
H-4010

W.D. BROWNAWELL
Mössnerstr. 27
D-7 STUTTGART 80

P. BUI MINH
ELTE Számítóközpont
BUDAPEST
Bogdánfy út 10/B
H-1117

P. BUNDSCHUH
Math. Inst. der Univ.
Weyertal 86-90
D-5000 KÖLN 41

J.W.S. CASSELS
Dept. of Pure Mathematics
and Mathematical Statistics
16 Mill Lane
CAMBRIDGE CB2 1SB
UK

J. CHAHAL
Math. Dept.
B.Y.U.
PROVO, UT 84602
USA

W.W.L. CHEN
Dept. of Mathematics
Imperial College
LONDON SW7 2B2
UK

R. COOK
Dept. of Pure Maths.
Hicks Building
Univ. of Scheffield
Housfield RF.
SHEFFIELD 53 7RH
UK

D. CORAY
Section de Mathématiques
CH-1211 GENÈVE 24

H. DABOUSSI
Bat 425 Université Paris Sud
F-91405 ORSAY Cedex

M. DENERT
Eendracht straat 102
B-9000 GENT

J.-M. DESHOUILLERS
30 Rue Descartes
F-33000 BORDEAUX

H.G. DIAMOND
Univ. of Illinois
Math. Dept.
1409 W. Green St.
URBANA, ILL 61801
USA

P.D.T.A. ELLIOTT
Dept. of Math., Box 426
Univ. of Colorado
BOULDER, CO 80309
USA

P. ERDŐS
MTA MKI
BUDAPEST,
Reáltanoda u. 13-15.
H-1053

G.R. EVEREST
School of Maths. and Physics,
Univ. of East Anglia
NORWICH, Norfolk
NR4 7TJ
UK

J.-H. EVERTSE
Filips van Bourgondies - traat 41A
NL - 3117 SC SCHIEDAM

G. FALTINGS
Univ. Wuppertal
Gauss - Strasse 20
D-5600 WUPPERTAL

J. FEHÉR
PÉCS, Báthory u. 20.
H-7624

E. FOUVRY
Univ. de Paris-Sud
Math. Bat. 425
F-91405 ORSAY Cedex

R. FREUD
BUDAPEST
Rajk L. u. 19.
H-1136

J. FRIEDLANDER
1265 Military Trail
SCARBOROUGH, ONT
M1C 1A4
Canada

A. FUJII
2-8-24 Nakamachi
Koganeishi
TOKYO
Japan

J. GALAMBOS
Dept. Maths.
Temple Univ.
PHILADELPHIA,
PA 19122
USA

A. GEROLDINGER
Inst. für Math.
Halbärth Gasse 1/1
A-8010 GRAZ

G. GREAVES
Dept. of Pure Maths.
Univ. College, Box 78
CARDIFF CF1 1XL

A. GRYTCZUK
ul.. Sucharskiego 18m. 14
PL-65-562 ZIELONA GORA

K. GYŐRY
KLTE Mat. Intézet
DEBRECEN
Egyetem tér 1.
H-4010

J.A. HAIGHT
Dept. of Maths.
Univ. College London
LONDON WCIE GBT
UK

G. HALÁSZ
MTA MKI
BUDAPEST
Reáltanoda u. 13-15.
H-1053

F. HALTER-KOCH
Math. Inst. d. Univ.
Halbaerth Gasse 1
A-8010 GRAZ

D.R. HEATH-BROWN
Magdalen College
OXFORD OX1 4AU
UK

M. HINDRY
Institut Poincaré
11 Rue P. et M. Curie
F-75005 PARIS

M.N. HUXLEY
Pure Maths. Dept.
University College
CARDIFF CF1 1X4
UK

K.-H. INDLEKOFFER
Füllekengrund 12
D-4799 BORCHEN-
DÖRENHAGEN

S. ITO
Dept. of Math.
Tsuda College
TOKYO
Japan

A. IVIĆ
S. Kovacevica 40, Stan 41
11000 BEOGRAD
Yugoslavia

W. JEHNE
Math. Inst., Univ. Köln
Weyertal 86-90
D-5000 KÖLN 41

M.I. JUTILA
Dept. of Math.
Univ. of Turku
SF-205000 TURKU

J. KACZOROWSKI
ul. Rycerska 24/9
PL-60-347 POZNAN

I. KÁTAI
ELTE Számítóközpont
BUDAPEST
Bogdánfy út 10\B
H-1117

P. KISS
EGER
Csiky S. u. 7.
H-3300

H. KLEIMAN
188-83 85th Road
HOLLISWOOD, NY 11423
USA

G. KOLESNIK
Dept. of Maths.
Cal. State Univ.
LOS ANGELES, CA 90032
USA

J.-M. DE KONINCK
Dept. of Math.
Univ. Laval
QUÉBEC, G1K 7P4
Canada

I. KOREC
Faculty of Maths.
Comenius University
842 15 BRATISLAVA
CZECHOSLOVAKIA

S. KOTOV
Belgosuniversitet
Vichislitelnij center
220080 MINSK
USSR

B. KOVÁCS
KLTE Mat. Intézet
DEBRECEN
Egyetem tér
H-4010

K. KOVÁCS
BUDAPEST
Darvas J. u. 31. I.6.
H-1033

E. KRÄTZEL
Friedrich-Schiller-Univ.
Universitäts-hochhaus
DDR-6900 JENA

K. LAKKIS
Dept. of Maths.
Univ. Thessaloniki
THESSALONIKI
GREECE

E. LAMPRECHT
Fachbereich 9 Math.
Univ. der Saarlandes
D-6600 SAARBRÜCKEN

M. LANGEVIN
VA 763, I.H.P.
11, rue P. et M. Curie
F-75231 PARIS Cedex 05

M. LAURENT
13 Rue Perrault
F-228000 CHARTES

H.W. LENSTRA, Jr.
Dept. of Mathematics
Univ. of California
BERKELEY, CA 94720
USA

A. LEUTBECHER
Math. Inst. der TU
München
Arcisstrasse 21
D-8000 MÜNCHEN 2

F. LORENZ
Staufenstrasse 43
D-4400 MÜNSTER

L. LOVÁSZ
BUDAPEST
Kútvölgyi út 71.,
H-1225

J. LOXTON
School of Mathematics
Macquarie Univ.
P.O.Box 1
KENSINGTON NSW 2109
Australia

H. MAIER
Dept. of Maths.
Univ. of Georgia
ATHENS, GA 30602
USA

E. MANSTAVIČIUS
Faculty of Maths.
Vilnius University
Partizan 24
VILNIUS 232006
USSR

F. MARKO
Math. Inst.
Slovak Acad. Sci.
Obrancov mieru 49
81473 BRATISLAVA
Czechoslovakia

D. MASSER
Dept. of Maths.
Univ. of Michigan
ANN ARBOR, MI 48109
USA

Ch. MAUDUIT
41-C rue d'isoard
F-13001 MARSEILLE

M. MENDES FRANCE
Dept. of Maths.
Univ. Bordeaux 1
351, cours de la Liberation
F-33405 TALENCE Cedex

H. MENZER
Friedrich-Schiller-
Universität
Sektion Mathematik
Universitätshochhaus,
17.OGG
DDR-6900 JENA

A. MERCIER
Dept. of Maths.
Univ. Québec
CHICOUTIMI, QC G7H
2B1
Canada

T.R. MEURMAN
Hakapellonkatu 8A7
SF-20540 TURKU

M. MIGNOTTE
Univ. Louis Pasteur, Math.
F-67084 STRASOURG

R. MOLLIN
Univ. of Calgary
Dept. of Maths. and Stat.
2500 University Dr.N.W
CALGARY,
ALTA T2N 1N4
Canada

B. MOROZ
M.P.I. f. Math.
Gottfried-Claren-Str. 26
D-5300 BONN 3

B. MOSSÉ
U.E.R. de Mathématiques
Univ. de Provance
Place Victor Hugo
F-113331 MARSEILLE
Cedex 3

K. NAGASAKA
5-15-14, Higashi-Nakano
Nakano-Ku
164 TOKYO
Japan

M. NAIR
Dept. of Maths.
Univ. of Glasgow
GLASGOW, G12 8QW
UK

T. NAKAHARA
Dept. of Maths.,
Fac. of Sci.,
Saga Univ.
SAGA 840
Japan

M. NATHANSON
Office of the Provost
Lehman College of the
City Univ.
of the New York
BRONX, NY 10468
USA

J.-L. NICOLAS
Dept. de Math.
Univ. de Limoges
123, ave Albert Thomas
F-87060 LIMOGES Cedex

H. NIEDERREITER
Math. Inst.,
Austrian Acad of Sci.
Dr. Ignaz-Seipel-Platz 2
A-1010 VIENNA

W.G. NOWAK
Inst. of Math. Univ. of
Bodenkultur
G. Mendel-Str. 33.
A-1180 VIENNA

A.M. ODLYZKO
Bell Laboratories
Room 2C-355
MURRAY HILL, NJ 07974
USA

M. PASTEKA
Math. Inst. of S.A.S.
Obrancov mieru 49
81473 BRATISLAVA
Czechoslovakia

A. PERELLI
Dip. di Matematica
via L.B. Alberti 4
I-16132 GENOVA

A. PETHŐ
KLTE Mat. Intézet
DEBRECEN
Egyetem tér 1.
H-4010

J. PINTZ
MTA MKI
BUDAPEST
Reáltanoda u. 13-15.
H-1053

A. POLLINGTON
Math. Dept., BYU
PROVO, UTAH 84602

S. PORUBSKY
Math. Inst. of S.A.S.
Obrancov mieru 49
81473 BRATISLAVA
Czechoslovakia

K. RAMACHANDRA
T.I.F.R., Maths.
Homi Bhabha Rd.
BOMBAY 400005
India

E. REYSSAT
1 Allée Traversiére
F-94260 FRESNES

SZ.GY. RÉVÉSZ
BUDAPEST
Kopolya u. 11.c.
H-1172

A. ROTKIEWICZ
Inst. of Mats. P.A.S.
ul. Sniadeckich 8
PL-00-950 WARSZAWA

J. RUTKOWSKI
Inst. of Maths.
A. Miczkiewicz Univ.
Matejki 48/49
PL-POZNAN

I. RUZSA
MTA MKI
BUDAPEST,
Reáltanoda u. 13-15.
H-1053

A. SÁRKÖZY
MTA MKI
BUDAPEST,
Reáltanoda u. 13-15.
H-1053

W. SCHAAL
Fachbereich Math.
Univ. Marburg
D-3550 MARBURG/L 6

A. SCHINZEL
ul. Brozozowa 12m 24
PL-00-286 WARSZAWA

H.P. SCHLICKEWEI
Abt. Mathematik II.
Univ. Ulm
Oberer Eselsberg
D-7900 ULM

W.M. SCHMIDT
Dept. of Math. Box 426
Univ. of Colorado
BOULDER, CO 80309
USA

Eira J. SCOURFIELD
Math. Dept., Royal
Holloway and Bedford
New College
EGHAM, Surrey
TW20 OEX
UK

I. SHIOKAWA
14-1 Hiyoshi
3 Chome
Kohokuku,
YOKOHAMA 223
Japan

T.N. SHOREY
Dept. of Maths.
Univ. of Leiden
P.Box 9512
Wassenaarsweg 80
NL-2300 RA LEIDEN

V.T. SÓS
MTA MKI
BUDAPEST,
Reáltanoda u. 13-15.
H-1053

R.P. STEINER
Math. Dept./BGSU
BOWLING GREEN,
OHIO 43403
USA

S. STEPANOV
Steklov Institut of Math.
ul. Vavilova 42
MOSCOW 117966
USSR

P. STEVENHAGEN
Mathematisch Institut
Univertiteit van Amsterdam
Roetersstraat 15
NL-1018 WB
AMSTERDAM

K.B. STOLARSKY
Mathematics Dept.
University of Illinois
1409 W. Green
URBANA, ILL 61801
USA

J. SURÁNYI
BUDAPEST
Zichy Jenö u. 39.
H-1066

M. SZALAY
ELTE TTK
Algebra és Számelmélet
Tsz.
BUDAPEST
Múzeum krt. 6-8.
H-1088

G. SZEKERES
School of Math. Univ. New
S. Wales
KENSINGTON, NSW
2033
Australia

J.-I. TAMURA
Azamino 3-3-7-307
Midoru-Ku
YOKOHAMA-SHI 227
Japan

G. TENENBAUM
102 rue Saint-Dizier
F-54000 NANCY

R. TICHY
Abteilung für Technische
Mathematik, TU Wien
A-1040 WIEN

R. TIJDEMAN
Mathematisch Instituut
Postbus 9512
NL-2300 RA LEIDEN

L.A. TRELINA
Inst. Mathem.
Acad. Sciences BSSR
ul. Surganova 11
MINSK, 220604
USSR

S. TULJAGANOV
Institut Matematiky
AN Y3 SSR
ul. F. Hodnajeva 29
700143 TASKENT,
Akadem Gorod
USSR

S. TURJÁNYI
KLTE MAT. Intézet
DEBRECEN
Egyetem tér 1.
H-4010

N. TZANAKIS
Solomou 8
713 06 IRAKLION, Crete
Greece

B. UHRIN
MTA SZTAKI
BUDAPEST
Victor H. u. 18-22.
H-1132

P. VARBANEC
ul. Sonechnaya 7/9, KV.18
270056 ODESSA
USSR

C. VIOLA
Dipartimento di Matematica
Via Buonarroti 2
I-56100 PISA

B. VIZVÁRI
MTA SZTAKI
BUDAPEST
Victor H. u. 18-22.
H-1132

M. WALDSCHMIDT
Institut Henri Poincaré
11, rue P. et M. Curie
F-75 231 PARIS Cedex 05

R. WALLISSER
Universität Freiburg
Math. Institut
Albertstr. 23b.
D-78 FREIBURG

L. WANG
University of Leiden
Department of Mathematics
and Computer Science
P.O.Box 9512
NL-2300 RA LEIDEN

B. de WEGER
Dept. of Applied Math.
University of Twente
P.O.Box 217
NL-7500 AE ENSCHEDE

E. WIRSING
Abteilung Mathematik II
Universität Ulm
D-7900 ULM/DONAU

J. WOLFART
Mathematisches Seminar
der Universität Frankfurt
Postfach 11 19 32
D-6000 FRANKFURT

G. WÜSTHOLZ
Bergische Universität
Gesamthochschule
Wuppertal
D-5600 WUPPERTAL 1

P. ZARZYCKI
Department of Math.
Univ. of Gdansk
ul. Wita Stwosza 57
PL-80-952 GDANSK

H.G. ZIMMER
Fachbereich 9 Math.
Universität des Saarlandes
D-6600 SAARBRÜCKEN

1346 -2 b

K. GYÖRY
and
G. HALÁSZ
editors

NUMBER THEORY, Vol. II.