and since there are at most n_K ideals P^m (P prime) of a given norm in K, we have

$$\psi_C(x) = \theta_C(x) + \sum_{\substack{P \text{unramified in } L \\ N_{K/Q}P^m \leqslant x,\, m \geqslant 2 \\ \left(\frac{L/K}{P}\right) = C}} \log N_{K/Q} P = \theta_C(x) + O(n x \log x)$$

and this shows that the estimates of Lemma 6 hold when $\psi_C(x)$ is replaced by $\theta_C(x)$.

Theorem B now follows from Lemma 6 by a modified form of partial summation (see [4], Lemma 7.3).

References

[1] K. M. Bartz, *An effective order of Hecke–Landau zeta functions near the line $\sigma = 1$*, Acta Arith. 50 (1988), 183–193.

[2] J. G. Hinz, *Eine Erweiterung des nullstellenfreien Bereiches der Heckeschen Zetafunktion und Primideale in Idealklassen*, ibid. 38 (1980), 209–254.

[3] J. C. Lagarias and A. M. Odlyzko, *Effective Versions of the Chebotarev Density Theorem*, pp. 409–464 in *Algebraic Number Fields*, A. Fröhlich, ed., Academic Press, London and New York 1977.

[4] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Polish Scientific Publishers (PWN), Warsaw 1974.

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

[6] H. M. Stark, *Some effective cases of the Brauer–Siegel theorem*, Invent. Math. 23 (1974), 135–152.

[7] W. Staś, *Über einige Abschätzungen in Idealklassen*, Acta Arith. 6 (1960), 1–10.

INSTITUTE OF MATHEMATICS
OF THE ADAM MICKIEWICZ UNIVERSITY
Poznań, Poland

Received on 27.7.1987 (1738)

ACTA ARITHMETICA
LII (1989)

On the linear independence of roots of unity over finite extensions of Q

by

UMBERTO ZANNIER (Pisa)

The problem we shall treat in the present paper seems to have been first considered by H. B. Mann.

In [4], among other things, the following theorem is proved:

Let

$$\alpha_0 + \alpha_1 \zeta^{n_1} + \ldots + \alpha_{k-1} \zeta^{n_k - 1} = 0 \tag{1}$$

be an equation, where ζ is a primitive N-th root of unity, the α_i are rational numbers, such that no proper subsum of its left-hand side vanishes (Mann calls such an equation "irreducible").

Then $N/(N, n_1, \ldots, n_{k-1})$ divides the product of prime numbers up to k.

This result was improved in one direction by Conway and Jones who showed in [2] that, if $p_1, \ldots, p_s$ are the primes dividing $N/(N, n_1, \ldots, n_{k-1})$ then

$$\sum (p_i - 2) \leqslant k - 2.$$

In another direction Schinzel considered recently the analogous problem to obtain an estimate for the above quotient assuming the coefficients α_i to be elements of some algebraic extension L of the rationals. (A particular case of this had been treated by Loxton [3]: he assumes $\alpha_0 \in L$, while $\alpha_i \in Q$ for $1 \leqslant j \leqslant k-1$.)

Schinzel proves in [5] that there is some bound for the quotient which depends only on k and on the degree $d = [L:Q]$.

However his proof uses van der Waerden's Theorem on arithmetic progressions and so leads to extremely large values for such a bound.

The question arises whether Mann's method (for instance), which is different from Schinzel's one, can be adapted to obtain a more satisfactory estimate.

In this paper we show that the answer is to some extent affirmative.

We remark that the problem is simplified if one looks for bounds

depending on k and the field L (not only on k and d): in this case the adaptation of Mann's arguments is almost straightforward.

Our results are the following:

THEOREM 1. *Let (1) be a relation with no proper subsum equal to zero, where $\alpha_i \in L$, L being an algebraic extension of $\mathbf{Q}$ of degree d, and where ζ is a primitive N-th root of unity.*

Let H be the maximal cyclotomic subfield of L and set $d' = [H: \mathbf{Q}]$, $\Delta = \operatorname{disc}(H)$. Then

$$\frac{N}{(N, n_1, \ldots, n_{k-1})} \Big| \eta \prod_{\substack{p^a \| d \\ a \geqslant 1 \\ p \mid \Delta}} p^{a+1} \prod_{\substack{p \nmid \Delta \\ p \leqslant k}} p \prod_{\substack{p \mid \Delta \\ p \leqslant (d, p-1)(k-1)+1}} p = N(H).$$

(Here $\eta = 2$ if $d' \equiv \Delta \equiv 0 \pmod 2$ and $\eta = 1$ otherwise.)

A straighforward use of the Brun-Titchmarsh Theorem (see for instance [1]) gives the following

COROLLARY. *Notation being as in Theorem 1 we have the estimate*

$$\frac{N}{(N, n_1, \ldots, n_{k-1})} \leqslant \exp\left(c \frac{\sigma_0(d)\, d}{\varphi(d)} \log(dk) \frac{k}{\log k}\right)$$

where c is an absolute constant and $\sigma_0(m) = \sum_{d \mid m} 1$.

Throughout the paper the letter p will denote a prime number and ζ_m will stand for a primitive mth root of unity.

Proofs. We shall need several preliminary lemmata.

LEMMA 1. *Let F be a field, $a_1, \ldots, a_k$ be distinct elements of F. Let e, h be positive integers such that*

$$k \leqslant e, \quad eh < \operatorname{char} F \quad (\text{if } \operatorname{char} F > 0).$$

Then the polynomials

$$1, \quad (x+a_u)^{ve}, \quad u = 1, \ldots, k, \ v = 1, \ldots, h$$

are linearly independent over F.

Proof. By induction on h. Let $h = 1$ and take a relation

$$\sum_{u=1}^{k} r_u (x+a_u)^e = r_0.$$

Taking derivatives and using $e \neq 0$ (in F) we get

$$\sum_{u=1}^{k} r_u (x+a_u)^{e-1} = 0.$$

Now the Wronskian of the polynomials $(x+a_u)^{e-1}$, $u = 1, \ldots, k$, is proportional to

$$D = \det_{u,v}\left(\binom{e-1}{u}(x+a_v)^{e-u-1}\right), \quad u = 0, 1, \ldots, k-1.$$

But

$$D = \binom{e-1}{0}\binom{e-1}{1}\cdots\binom{e-1}{k-1}(x+a_1)^{e-k}\ldots(x+a_k)^{e-k}\det\left((x+a_i)^j\right).$$

Since $k-1 \leqslant e-1 < \operatorname{char} F$ the first factors are nonzero, and since the a_i are distinct the last Vandermonde determinant does not vanish.

So the polynomials $(x+a_u)^{e-1}$ are linearly independent over F, whence $r_1 = r_2 = \ldots = r_k = 0$. But then $r_0 = 0$ and this completes the first step of our induction.

Assume now $h > 1$ and the lemma true up to $h-1$.

If there is a relation

$$r_0 + \sum_{u,v} r_{u,v}(x+a_u)^{ve} = 0, \quad u = 1, \ldots, k, \quad v = 1, \ldots, h,$$

let us differentiate e times. We shall obtain

$$\sum_{u,v} \binom{ve}{e} r_{u,v}(x+a_u)^{(v-1)e} = 0.$$

The inductive assumption and the inequality $he < \operatorname{char} F$ give

$$r_{u,v} = 0 \quad \text{for } v \geqslant 2$$

thus reducing to the case $h = 1$, which has just been treated.

Let now p be a prime number, χ a character of order h on F_p^*. As usual we extend χ to a function on F_p setting $\chi(0) = 0$(1).

LEMMA 2. *With the above notation let $a_1, \ldots, a_k$ be distinct elements of F_p, $c_{i,j}$, $i = 1, \ldots, k$, $j = 1, \ldots, h$, c_0 be complex numbers such that*

$$c_0 + \sum_{i,j} c_{i,j}\chi^j((x+a_i)) = 0 \quad \text{for all } x \in F_p.$$

Then, if $p \geqslant hk+1$ we have necessarily $c_{i,j} = c_0 = 0$ for all i, j.

Proof. Let ϱ be a primitive hth root of unity, and observe that χ takes values in $\mathbf{Q}(\varrho)$.

Let $w_1, \ldots, w_m$ be a basis for the vector space spanned by c_0, $c_{i,j}$ over $\mathbf{Q}(\varrho)$.

(1) Even if $h = 1$.

Then we may write

$$c_0 = \sum_{s=1}^{m} \xi_s w_s, \qquad c_{i,j} = \sum_{s=1}^{m} \xi_{ijs} w_s$$

where ξ_s, $\xi_{ijs} \in \boldsymbol{Q}(\varrho)$, and

$$\sum_{s=1}^{m} w_s \{\xi_s + \sum_{i,j} \xi_{ijs} \chi^j((x+a_i))\} = 0 \quad \text{for every } x \in \boldsymbol{F}_p.$$

The linear independence of $w_1, \ldots, w_m$ over $\boldsymbol{Q}(\varrho)$ then gives

$$\xi_s + \sum_{i,j} \xi_{ijs} \chi^j((x+a_i)) = 0 \quad \text{for every } x \in \boldsymbol{F}_p \text{ and for all } s.$$

Thus in proving our lemma we may assume that c_0 and the c_{ij}'s all belong to $\boldsymbol{Q}(\varrho)$.

Now it is well known from elementary algebraic number theory that there exists a prime ideal $\mathfrak{p}$ of $Z[\varrho]$ such that $\mathfrak{p} \mid p$ and

$$\chi(x) \equiv x^{(p-1)/h} \pmod{\mathfrak{p}} \quad \text{for } x \in \boldsymbol{F}_p.$$

If our lemma is not true, that is if $p \geqslant hk+1$ and the c's are not all zero, it is clear that we may further assume them to be $\mathfrak{p}$-integers not all divisible by $\mathfrak{p}$. (One can achieve this last condition dividing eventually such coefficients by some power of an element $\pi \in Z[\varrho]$ having order 1 at $\mathfrak{p}$.)

When such a normalisation has been carried out we may reduce our linear relation mod $\mathfrak{p}$ obtaining

$$\bar{c}_0 + \sum_{i,j} \bar{c}_{ij} (x+a_i)^{j(p-1)/h} \equiv 0 \pmod{\mathfrak{p}} \quad \text{for } x \in \boldsymbol{F}_p. \tag{2}$$

Here the bar denotes of course reduction mod $\mathfrak{p}$; observe also that all reductions belong to $\boldsymbol{F}_p$, since $\mathfrak{p}$ lies above p and since p splits completely in $Z[\varrho]$.

Since the polynomial on the left-hand side of (2) has degree $\leqslant p-1$, and since it vanishes on all $\boldsymbol{F}_p$, it must vanish identically.

But then we may apply Lemma 1, setting $e = (p-1)/h$, $F = \boldsymbol{F}_p$: observe that with our assumptions $e \geqslant k$, while the condition $eh < \operatorname{char} F$ is automatically satisfied.

From Lemma 1 we obtain $\bar{c}_0 = \bar{c}_{ij} = 0$, i.e. all the coefficients are divisible by $\mathfrak{p}$, a contradiction which proves the assertion.

LEMMA 3. *For $i = 1, \ldots, k$, let F_i: $\boldsymbol{F}_p \to \boldsymbol{C}$ be functions such that*

(i) $F_i(0) = 0$;

(ii) *The restriction $F_i|_{\boldsymbol{F}_p^\circ}$ is constant on cosets modulo the subgroup of $\boldsymbol{F}_p^*$ of index $h \mid p-1$;*

(iii) *For some distinct $a_1, \ldots, a_k \in \boldsymbol{F}_p$ assume that*

$$\sum_i F_i(x+a_i) = c_0 \in \boldsymbol{C} \quad \text{for all } x \in \boldsymbol{F}_p.$$

Then, if $p \geqslant hk+1$ each F_i is identically zero.

Proof. In view of (i) and (ii) we have, for each i, an expansion

$$F_i(x) = \sum_{j=1}^{h} c_{ij} \chi^j(x)$$

where χ is a character of order h on $\boldsymbol{F}_p^*$.

The use of (iii) together with Lemma 2 give at once the result.

LEMMA 4. *Let H be a cyclotomic field with $d = [H:\boldsymbol{Q}]$ and $\Delta = \operatorname{disc}(H)$. Define*

$$\eta = \begin{cases} 2 & \text{if } d \equiv \Delta \equiv 0 \pmod 2, \\ 1 & \text{otherwise.} \end{cases}$$

Then

$$H \subset \boldsymbol{Q}(\zeta_m)$$

where

$$m = \eta \prod p^{a+1}$$

the product being extended to primes such that $p \mid \Delta$ and $p^a \| d$.

The proof of this lemma appears in the paper of Loxton [3] mentioned in the introduction.

Proof of main Theorem. We shall treat first the case when $L = H$ is a cyclotomic field.

Let $\zeta = \zeta_N$ be a primitive Nth root of unity, $H \subset \boldsymbol{Q}(\zeta_m)$, where m is as in Lemma 4.

We may clearly assume that $(N, n_1, \ldots, n_{k-1}) = 1$, and agree that $n_0 = 0$.

Let $p^s \| N$. We shall distinguish several possibilities.

Assume first that $p \mid \Delta$, whence $p \mid m$, and that $p \neq 2$, $s \geqslant a+2$.

There exists a primitive (N/p)-th root of unity ζ_* and a primitive p^s-th root of unity ϱ such that

$$\zeta = \zeta_* \varrho.$$

Each ζ^{n_i} may be clearly written in the form $\zeta_*^{n_i} \varrho^v$ where $0 \leqslant v < p$ and $n_i \equiv v \pmod p$.

Substituting into the fundamental relation (1) we get

$$\sum_{v=0}^{p-1} \varrho^v S(v) = 0$$

where

$$S(v) = \sum_{n_i \equiv v} \alpha_i \zeta_*^{n_i} \in \boldsymbol{Q}(\zeta_m, \zeta_*) \subset \boldsymbol{Q}(\zeta_{[m,N/p]}).$$

But $\boldsymbol{Q}(\varrho, \zeta_*, \zeta_m)$ has degree p over $\boldsymbol{Q}(\zeta_*, \zeta_m)$ (since $s \geqslant a+2$), whence $S(v) = 0$ for all v and

$$\varrho^v S(v) = \sum_{n_i \equiv v} \alpha_i \zeta^{n_i} = 0.$$

Since no proper subsum of (1) can vanish, this implies that $n_i \equiv 0 \pmod p$ for all i, whence $p \mid (N, n_1, \ldots, n_{k-1})$, a contradiction.

We have proved that

(3) $\begin{cases} p^s \| N,\ p \mid \Delta,\ p^a \| d,\ p \equiv 1 \pmod 2 \Rightarrow s \leqslant a+1, \\ \text{and a completely analogous argument proves } s \leqslant a+2 \text{ for } p = 2. \end{cases}$

Assume now $p \nmid \Delta$.

Arguing as above we have a contradiction if $s > 1$.

If $s = 1$ we obtain that all the $S(v)$ must be equal (now ϱ has degree $p-1$ over $\boldsymbol{Q}(\zeta_*, \zeta_m)$ with minimal polynomial $1 + x + \ldots + x^{p-1}$).

But at most k of the $S(v)$ are nonzero whence, if $p > k$, all the $S(v)$ must vanish and we have a contradiction as before.

We have shown that

(4) $$p^s \| N, \quad p \nmid \Delta \Rightarrow s = 1 \quad \text{and} \quad p \leqslant k.$$

(These arguments follow strictly Mann's ones.)

To make estimates depend only on d and k (not merely on d, k and Δ), we must treat further the case

$$p^s \| N, \quad p \mid \Delta, \quad p \nmid d.$$

Assertion (3) gives $s \leqslant 2$ if $p = 2$, and $s = 1$ if $p \neq 2$, as we shall assume from now on.

Write as above $\zeta = \zeta_* \varrho$ and find a primitive mth root of unity $\zeta_m = \zeta' \varrho$ where ζ' is a primitive (m/p)-th root of unity.

Observe that $p \nmid m/p$.

Each α_i has the expression

(5) $$\alpha_i = \sum_{u=1}^{p-1} \varrho^u S_i(u), \quad S_i(u) \in \boldsymbol{Q}(\zeta').$$

Let $\sigma \in \mathrm{Gal}(\boldsymbol{Q}(\zeta_m) \mid H\boldsymbol{Q}(\varrho))$. Then

(6) $$\alpha_i = \sum_{u=1}^{p-1} \varrho^u \sigma S_i(u), \quad \sigma S_i(u) \in \boldsymbol{Q}(\zeta').$$

But the expression (5) is clearly unique, since ϱ has degree $p-1$ over $\boldsymbol{Q}(\zeta')$, and comparison with (6) leads to the result that σ fixes each $S_i(u)$, whence

(7) $$S_i(u) \in H' = H\boldsymbol{Q}(\varrho) \cap \boldsymbol{Q}(\zeta').$$

To compute $d' = [H' : \boldsymbol{Q}]$ observe that

$$\varphi(m) = [\boldsymbol{Q}(\zeta_m) : \boldsymbol{Q}] = [\boldsymbol{Q}(\zeta')\,\boldsymbol{Q}(\varrho) : \boldsymbol{Q}] = [\boldsymbol{Q}(\zeta')\,H\boldsymbol{Q}(\varrho) : \boldsymbol{Q}]$$
$$= \varphi(m/p)\,[H\boldsymbol{Q}(\varrho) : \boldsymbol{Q}]\,[H' : \boldsymbol{Q}]^{-1} = [H : \boldsymbol{Q}]\,[H \cap \boldsymbol{Q}(\varrho) : \boldsymbol{Q}]^{-1}\,[H' : \boldsymbol{Q}]^{-1}\,\varphi(m)$$

whence

(8) $$d' = [H' : \boldsymbol{Q}] = \frac{[H : \boldsymbol{Q}]}{[H \cap \boldsymbol{Q}(\varrho) : \boldsymbol{Q}]} = \frac{d}{[H \cap \boldsymbol{Q}(\varrho) : \boldsymbol{Q}]}.$$

Let $\sigma \in \mathrm{Gal}(\boldsymbol{Q}(\zeta_m) \mid HH') = G$ correspond to $g \in (\boldsymbol{Z}/(m))^*$.

Applying σ to (5) we have

(9) $$\alpha_i = \sum_{u=1}^{p-1} \varrho^{gu} S_i(u) = \sum_{u=1}^{p-1} \varrho^{gu} S_i(gu).$$

(Here we think of S_i as a function $S_i \colon \boldsymbol{F}_p \to \boldsymbol{Q}(\zeta')$ such that $S_i(0) = 0$.) Whence

(10) $$S_i(gu) = S_i(u) \quad \text{for all } i, u \text{ and } g \in G.$$

Let $\pi \colon (\boldsymbol{Z}/(m))^* \to \boldsymbol{F}_p^*$ be the reduction map. The image $\pi(G)$ has cardinality $|G| / |G \cap \ker \pi|$.

On the other hand $\ker \pi$ corresponds to the subgroup of $(\boldsymbol{Z}/(m))^*$ fixing $\boldsymbol{Q}(\varrho)$, whence

$$G \cap \ker \pi = \mathrm{Gal}(\boldsymbol{Q}(\zeta_m) \mid H\boldsymbol{Q}(\varrho)) \quad (\text{since } H' \subset H\boldsymbol{Q}(\varrho))$$

and the above remark leads to the formulas

$$|\pi(G)| = \frac{[H\boldsymbol{Q}(\varrho) : \boldsymbol{Q}]}{[HH' : \boldsymbol{Q}]} = \varphi(p) \frac{[H \cap H' : \boldsymbol{Q}]}{[H' : \boldsymbol{Q}]\,[H \cap \boldsymbol{Q}(\varrho) : \boldsymbol{Q}]}$$
$$= \varphi(p) \frac{[H \cap H' : \boldsymbol{Q}]}{[H : \boldsymbol{Q}]} \quad (\text{by (8)}).$$

Combining this with (10) we see that we have proved that $S_i|_{\boldsymbol{F}_p^*}$ depends only on cosets modulo a subgroup $\Gamma \subset \boldsymbol{F}^*$ (independent of i) of index $\dfrac{[H : \boldsymbol{Q}]}{[H \cap H' : \boldsymbol{Q}]}$, which divides $(d, p-1)$.

Substitute now relations (5) into the fundamental equation (1), obtaining

$$\sum_{i=0}^{k-1} \sum_{u=1}^{p-1} \zeta_*^{n_i} \varrho^{n_i + u} S_i(u) = 0$$

and

$$\sum_{v=0}^{p-1} \varrho^v \sum_{n_i + u \equiv v(p)} \zeta_*^{n_i} S_i(u) = 0.$$

Since the inner sums are contained in $Q(\zeta_*, \zeta')$ and since ϱ has degree $p-1$ over that field, we infer that all these sums have the same value whence the function

$$x(\in F_p) \mapsto \sum_{i=0}^{k-1} \zeta_*^{n_i} S_i(x-n_i) \text{ is constant } (= c_0). \tag{12}$$

Set $B = \{n_i \bmod p\}$. (12) gives

$$\sum_{\beta \in B} \Big\{ \sum_{n_i \equiv \beta(p)} \zeta_*^{n_i} S_i(x-n_i) \Big\} = c_0. \tag{13}$$

We may now apply Lemma 3, setting $\{-a_i\} = B$, $h = (d, p-1)$, and, for $\beta \in B$

$$F_\beta(x) = \sum_{n_i \equiv \beta(p)} \zeta_*^{n_i} S_i(x).$$

If $p \geqslant h|B|+1$ that lemma implies (in view also of (11)) that each F_β is identically zero, i.e.

$$\sum_{n_i \equiv \beta} \zeta_*^{n_i} (x-\beta) = \sum_{n_i \equiv \beta} \zeta_*^{n_i} S_i(x-n_i) = 0$$

for all $x \in F_p$ and for all $\beta \in B$.

Multiplying this relation by ϱ^x and summing over $x \in F_p$ we are led to

$$\sum_{n_i \equiv \beta(p)} \alpha_i \zeta^{n_i} = 0.$$

Since no subsum of (1) vanishes and since not all the n_i can be congruent mod p (otherwise, since $n_0 = 0$, p would divide $(N, n_1, \ldots, n_{k-1})$), we have a contradiction, showing that

$$p < h|B|+1$$

and, since $h = (d, p-1) \mid p-1$, this implies

$$p \leqslant (d, p-1)(|B|-1)+1 \leqslant (d, p-1)(k-1)+1. \tag{14}$$

This result completes the proof of Theorem 1 when L is a cyclotomic field.

Let us now consider the case of a general field L.

Let H be the maximal cyclotomic subfield of L, and write

$$l = [L:H], \quad d' = [H:Q]$$

and let ξ be a generator for L over H.

With the α_i as in (1) set

$$\alpha_i = \sum_{u=0}^{l-1} \alpha_{i,u} \xi^u, \quad \alpha_{i,u} \in H.$$

(1) then reads

$$\sum_{u=0}^{l-1} \xi^u \sum_{i=0}^{k-1} \alpha_{i,u} \zeta^{n_i} = 0.$$

Since the intersection $L \cap HQ(\zeta)$ is just H (by definition), and since $HQ(\zeta)$ is normal over H, it follows that ξ has degree 1 still over $HQ(\zeta)$, whence

$$\sum_{i=0}^{k-1} \alpha_{i,u} \zeta^{n_i} = 0 \quad \text{for } u = 0, 1, \ldots, l-1. \tag{15}$$

The proof can now be completed in more than one way, appealing to the particular case treated before.

The simplest method seems to me the following, which depends on

LEMMA 5. *Let $w_1, \ldots, w_k$ be complex numbers, H be some subfield of C and assume we have l linear relations*

$$\sum_{i=1}^{k} \beta_{i,u} w_i = 0, \quad u = 0, 1, \ldots, l-1$$

with $\beta_{i,u} \in H$.

Then either there is a proper non empty subset $\Gamma \subset \{1, \ldots, k\}$ such that

$$\sum_{i \in \Gamma} \beta_{i,u} w_i = 0, \quad u = 0, 1, \ldots, l-1$$

or there is a relation

$$\sum_{i=1}^{k} \beta_i w_i = 0, \quad \beta_i \in H$$

such that no proper subsum can vanish.

The proof of this lemma is very simple. For $\Gamma \subset \{1, \ldots, k\}$, set

$$V_\Gamma = \{(x_0, \ldots, x_{l-1}) \in H^l, \sum_{i \in \Gamma} w_i \sum_{u=0}^{l-1} x_u \beta_{i,u} = 0\}.$$

It is clear that the V_Γ are vector spaces over H. Observe that, if the first possibility does not hold, then

$$V_\Gamma \neq H^l \quad \text{for } \emptyset \neq \Gamma \subsetneq \{1, \ldots, k\}.$$

Since H is infinite and since V_Γ runs over a finite number of proper

subspaces of H, we have that

$$V = \bigcup_{\emptyset \neq \Gamma \subseteq \{1,\dots,k\}} V_\Gamma \neq H^l.$$

Choose $(x_0, \dots, x_{l-1}) \in H^l \setminus V$ and set

$$\beta_i = \sum_{u=0}^{l-1} x_u \beta_{i,u}.$$

Then clearly

$$\sum_{i=1}^{k} \beta_i w_i = 0.$$

Moreover, if there was a vanishing proper subsum, corresponding to $i \in \Gamma$, we would have $(x_0, \dots, x_{l-1}) \in V_\Gamma$, a contradiction.

To complete the proof of Theorem 1, take relations (15) and apply Lemma 5 with $\zeta^{n_i} = w_i$.

If the first possibility occurs then

$$\sum_{i \in \Gamma} \alpha_{i,u} \zeta^{n_i} = 0, \quad u = 0, 1, \dots, l-1;$$

whence

$$\sum_{i \in \Gamma} \alpha_i \zeta^{n_i} = 0$$

a contradiction.

In the second case there is a relation

$$\sum_{i=0}^{k-1} \beta_i \zeta^{n_i} = 0, \quad \beta_i \in H$$

with no proper subsum vanishing, and we may apply the particular case proving completely Theorem 1.

Proof of corollary. Let us estimate separately the three factors which appear in the definition of $N(H)$ in the statement of Theorem 1.

The first factor is clearly bounded by $2d^2$.

The logarithm of the second factor is, by Tchebycheff's inequality, $\ll k$.

Forgetting the condition $p \mid \Delta$, the logarithm of the third factor is bounded by

$$\sum_{p \leq (d', p-1)(k-1)+1} \log p \leq \sum_{e \mid d'} \sum_{\substack{p \equiv 1 (e) \\ p \leq ek}} \log p.$$

Now, by the Brun–Titchmarsh Theorem, the inner sum can be estimated

by

$$\log(ek) \sum_{\substack{p \equiv 1 (e) \\ p \leq ek}} 1 \leq c \log(dk) \frac{ek}{\varphi(e) \log k}$$

where c is an absolute constant (one may even take $c = 2$).

Summing over $e \mid d$ and observing that, trivially,

$$\sum_{e \mid d} \frac{e}{\varphi(e)} \leq \sigma_0(d) \frac{d}{\varphi(d)}$$

one gets the stated result.

Remarks. 1. I have found no satisfactory lower bound for $N/(N, n_1, \dots, n_{k-1})$. However inequality (14) is clearly the best we can obtain looking at a single prime p dividing the crucial quotient, for let $d \mid p-1$, set $k = (p-1)/d+1$, and let H be the unique subfield of $\boldsymbol{Q}(\zeta_p)$ having degree d over $\boldsymbol{Q}$.

Then ζ_p satisfies an equation $\alpha_0 + \alpha_1 \zeta_p + \dots + \alpha_{k-1} \zeta_p^{k-1} = 0$, $\alpha_i \in H$, with no proper subsum vanishing; moreover $p = (d, p-1)(k-1)+1$.

2. The inequality for p required for the validity of Lemma 2 cannot be strengthened, as is easily seen by observing that the space of complex functions defined on F_p has dimension p (over $\boldsymbol{C}$).

3. Observe that the proof of Theorem 1 gives the following slightly stronger result:

"If $p \mid N/(N, n_1, \dots, n_{k-1})$ and $p^2 \nmid m$, then the number of incongruent (p) ones among the n_i's is at least $(p-1)/(d, p-1)+1$".

4. Fairly complicated arguments (following anyway similar lines as those exposed here) prove the following

"Let p, q be distinct primes such that $pq \mid N/(N, n_1, \dots, n_{k-1})$ and p^2, $q^2 \nmid m$. Then

$$\frac{p-1}{(p-1, d)} + \frac{q-1}{(q-1, d)} \leq k-1.$$

Since the strengthening is asymptotically not very satisfactory, I have decided not to include the proof of this result, in order to make the paper neater.

Anyway this would perhaps suggest that an analogue of the theorem of Conway and Jones could have the following form:

If $p_1, \dots, p_s \mid N/(N, n_1, \dots, n_{k-1})$ but $p_j^2 \nmid m$, then

$$\sum \left(\frac{p_j - 1}{(d, p_j - 1)} - 1 \right) \leq k-2.$$

Acknowledgement. I would like to thank Professor A. Schinzel for introducing me to the subject of the paper and for his kind attention.

References

[1] E. Bombieri, *Le grand crible dans la théorie analytique des nombres*, Asterisque 18 (1974), Societé Mathématique de France, page 22.
[2] J. H. Conway and A. J. Jones, *Trigonometric diophantine equations (on vanishing sums of roots of unity)*, Acta Arith. 30 (1976), 229–240.
[3] J. H. Loxton, *On two problems of R. M. Robinson about sums of roots of unity*, ibid. 26 (1974), 159–174.
[4] H. B. Mann, *On linear relations between roots of unity*, Mathematika 12 (1965), 107–117.
[5] A. Schinzel, *Reducibility of lacunary polynomials VIII*, Acta Arith. 50 (1988), 91–106.

Received on 7.8.1987 (1743)

ACTA ARITHMETICA
LII (1989)

Some number-theoretical properties of generalized sum-of-digit functions

by

GERHARD LARCHER (Salzburg) and ROBERT F. TICHY (Wien)

1. Introduction. There has been a great deal of work in investigating the number-theoretical properties of the sum of digits of positive integers in a given number system. In the special case of a q-ary number system ($q \geqslant 2$) write n in the digit representation

$$n = \sum_{i=0}^{\infty} \varepsilon_i q^i \tag{1.1}$$

with $\varepsilon_i = \varepsilon_i(q, n) \in \{0, \ldots, q-1\}$ and $\varepsilon_i = 0$ for $i > [\log n/\log q]$; $[x]$ denotes, as usual, the greatest integer $\leqslant x$. Then by a famous result of Delange [3]

$$\frac{1}{n}\sum_{k=0}^{n-1} s(q, k) = \frac{q-1}{2}\frac{\log n}{\log q} + nF\left(\frac{\log n}{\log q}\right), \tag{1.2}$$

where $s(q, k) = \sum_{j=0}^{\infty} \varepsilon_j(q, k)$ denotes the sum of q-ary digits and F is a suitable continuous and nowhere differentiable function with period 1. Exact bounds of the error term $F(\log n/\log q)$ have been given by Drazin and Griffiths [4]. A further precise information on the average value of the sum of q-ary digits is given in a recent paper of Foster [6]. In the case $q = 2$ he proved

$$-\frac{2}{13} < \frac{2}{n}\sum_{k=0}^{n-1} s(2, k) - \left[\frac{\log n}{\log q}\right] < 1, \tag{1.3}$$

where both bounds are best possible. A paper of Stolarsky [12] contains a brief survey of the history of such problems and cites many references.

Other authors, expecially French mathematicians investigated certain exponential sums, e.g.

$$\sum_{k=0}^{n-1} e^{2\pi i h s(q,k) x} \quad (h \text{ integral, } x \text{ irrational}) \tag{1.4}$$

in connection with the uniform distribution of the sequence $(s(q, n)\, x)_{n=0}^{\infty}$.