Conspectus materiae tomi L, fasciculi 1

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

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

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

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

ISBN 83-01-07915-0 ISSN 0065-1036

PRINTED IN POLAND

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

ACTA ARITHMETICA
L (1988)

Improvements to the Newman–Znám result for disjoint covering systems*

by

Marc A. Berger, Alexander Felzenbaum and Aviezri S. Fraenkel (Rehovot, Israel)

1. Preliminary results. For $a \in Z$, $m \in N$, denote by $a(m)$ the *residue class*

$$a(m) = \{a+km:\ k \in Z\}. \tag{1}$$

We refer to m as the *modulus* of this residue class. Let $\Delta = \{a_i(n_i):\ 1 \leqslant i \leqslant t\}$ be a *disjoint covering system*; i.e., a system of residue classes which exactly partition Z. The modulus n_k is said to be *divmax* if

$$n_k \mid n_i \Rightarrow n_k = n_i, \qquad 1 \leqslant i \leqslant t. \tag{2}$$

M. Newman [3] and Znám [4] showed that if n_k is divmax then at least $p(n_k)$ residue classes in Δ must have n_k as modulus, where $p(n)$ denotes the least prime divisor of n. Our main result is an improvement of this bound.

Theorem I. *If n_k is divmax then at least*

$$\min_{n_i \neq n_k} G\left(\frac{n_k}{(n_i,\, n_k)}\right) \tag{3}$$

residue classes in Δ must have n_k as modulus, where $G(n)$ denotes the greatest divisor of n which is a power of a single prime:

$$G(n) = \max(d \in N:\ d \mid n \text{ and } d = p^e \text{ for some prime } p). \tag{4}$$

To see that this is in fact an improvement of the Newman–Znám bound, observe that since n_k is divmax

$$n_i \neq n_k \Rightarrow (n_i,\, n_k) \neq n_k \Rightarrow G\left(\frac{n_k}{(n_i,\, n_k)}\right) \geqslant p(n_k). \tag{5}$$

Theorem I applies to disjoint covering systems which have at least two distinct moduli – otherwise the minimum in (3) would be over a vacuous set. In Section 2 we provide a geometric proof of this theorem, and in Section 3 we provide an analytic proof in the spirit of Newman [3]. In Section 4 we improve the Newman–Znám bound in a different direction.

* This research was supported by grant No. 85-00368 from the United States–Israel Binational Science Foundation (BSF), Jerusalem, Israel.

For subsets $X, Y \subset Z$ denote by $X+Y$ the set

(6) $$X+Y = \{x+y\colon\ x \in X,\ y \in Y\}.$$

Let $N \in \mathbf{N}$. A finite nonempty subset $S \subset \mathbf{Z}$ is said to be *N-uniform* if

(7) $$a(m) \subset [a(m) \cap S] + O(|S|)$$

for all $a \in \mathbf{Z}$, $m \in N$ satisfying $m|N$ and $a(m) \cap S \neq \emptyset$.

THEOREM II. *Let $M, N \in N$ with $M|N$. There exists an N-uniform set of cardinality M. In fact if N has the prime factorization*

(8) $$N = \prod_{i=1}^{l} p_i^{d_i}$$

and if

(9) $$M = \prod_{i=1}^{l} p_i^{e_i},$$

where the e_i are allowed to be zero, then

(10) $$S = \{0 \leqslant k < N\colon\ k(\operatorname{mod} p_i^{d_i}) < p_i^{e_i};\ 1 \leqslant i \leqslant l\}$$

is N-uniform and $|S| = M$. Here $k(\operatorname{mod} x)$ denotes the least nonnegative residue of k modulo x.

Let $\sigma = \sigma_N$ be the additive (cyclic) group $\{0, \ldots, N-1\}$ modulo $N = \prod_{i=1}^{l} p_i^{d_i}$. For any subgroup $G \subset \sigma$ define

(11) $$G^{\perp} = \{k \in \sigma\colon\ k(\operatorname{mod} p_i^{d_i}) < p_i^{e_i};\ 1 \leqslant i \leqslant l\}$$

where $M = \prod_{i=1}^{l} p_i^{e_i}$ is the generator of G. If M is the generator of G then

(12) $$G = O(M) \cap \sigma.$$

Thus to establish (7) it suffices to show that

(13) $$C \subset (C \cap G^{\perp}) + G$$

for any coset C of σ with $C \cap G^{\perp} \neq \emptyset$. We prove this with the help of two lemmas. To simplify notation in their proofs we use $k^{(i)}$ to denote $k(\operatorname{mod} p_i^{d_i})$.

LEMMA III. *For $k_1, k_2 \in G^{\perp}$*

(14) $$k_1 - k_2 \in G \ \Rightarrow\ k_1 = k_2.$$

In particular $\sigma = G + G^{\perp}$.

Proof.

(15) $$\begin{aligned} k_1 - k_2 \in G &\Rightarrow k_1 \equiv k_2 (\operatorname{mod} p_i^{e_i}), \quad 1 \leqslant i \leqslant l \\ &\Rightarrow k_1^{(i)} \equiv k_2^{(i)} (\operatorname{mod} p_i^{e_i}), \quad 1 \leqslant i \leqslant l \\ &\Rightarrow k_1^{(i)} = k_2^{(i)}, \quad 1 \leqslant i \leqslant l \quad \Rightarrow \quad k_1 = k_2, \end{aligned}$$

the next-to-last step following from the definition of $G^{\perp}$. ∎

LEMMA IV. *If $l_1 \in G$, $l_2 \in G^{\perp}$ then*

(16) $$l_1^{(i)} + l_2^{(i)} < p_i^{d_i}, \quad 1 \leqslant i \leqslant l.$$

Thus there is no "overflow" when adding l_1 and l_2 modulo $p_i^{d_i}$. Therefore

(17) $$(l_1 + l_2)^{(i)} = l_1^{(i)} + l_2^{(i)}, \quad 1 \leqslant i \leqslant l.$$

From this follows that if H is another subgroup of σ and if, as above, $l_1 \in G$, $l_2 \in G^{\perp}$ then

(18) $$l_1 + l_2 \in H \Leftrightarrow l_1, l_2 \in H,$$

(19) $$l_1 + l_2 \in H^{\perp} \Leftrightarrow l_1, l_2 \in H^{\perp}.$$

Equivalently

(20) $$H = (H \cap G) + (H \cap G^{\perp}),$$

(21) $$H^{\perp} = (H^{\perp} \cap G) + (H^{\perp} \cap G^{\perp}).$$

It also follows that if $t \in H^{\perp} \cap G^{\perp}$ then

(22) $$(H+t) \cap G^{\perp} = (H \cap G^{\perp}) + t.$$

Proof. Since

(23) $$p_i^{e_i} | l_1^{(i)}, \quad 0 \leqslant l_1^{(i)} < p_i^{d_i}, \quad 0 \leqslant l_2^{(i)} < p_i^{e_i}$$

(16) is obvious, as is then the implication

(24) $$l_1 + l_2 \in H^{\perp} \Rightarrow l_1, l_2 \in H^{\perp}.$$

Of course the implication

(25) $$l_1, l_2 \in H \Rightarrow l_1 + l_2 \in H$$

is also obvious, since H is closed under addition. Let $\prod_{i=1}^{l} p_i^{f_i}$ be the generator of H; $0 \leqslant f_i \leqslant d_i$, $1 \leqslant i \leqslant l$, and suppose $l_1 + l_2 \in H$. Then

(26) $$p_i^{f_i} | l_1^{(i)} + l_2^{(i)}, \quad 1 \leqslant i \leqslant l.$$

If $f_i \leqslant e_i$ then by (23) $p_i^{f_i} | l_1^{(i)}$. Otherwise if $f_i > e_i$ then by (26) we must have

$l_2^{(i)} = 0$. In any event it follows that

(27) $$p_i^{f_i} \mid l_1^{(i)}, \quad 1 \leqslant i \leqslant l$$

and thus l_1, and consequently l_2, belongs to H.

Suppose next that $l_1, l_2 \in H^{\perp}$. Then

(28) $$p_i^{e_i} \mid l_1^{(i)}, \quad 0 \leqslant l_1^{(i)} < p_i^{d_i}, \quad 0 \leqslant l_2^{(i)} \leqslant \min(p_i^{e_i}, p_i^{f_i}).$$

If $f_i \leqslant e_i$ then $l_1^{(i)} = 0$ and $l_1^{(i)} + l_2^{(i)} = l_2^{(i)} < p_i^{f_i}$. Otherwise if $f_i > e_i$ then

(29) $$l_1^{(i)} + l_2^{(i)} < l_1^{(i)} + p_i^{e_i} < p_i^{f_i}.$$

In any event it follows that

(30) $$(l_1 + l_2)^{(i)} = l_1^{(i)} + l_2^{(i)} < p_i^{f_i}, \quad 1 \leqslant i \leqslant l$$

and thus $l_1 + l_2 \in H^{\perp}$.

To see (22), suppose that $h \in H$ and $t \in H^{\perp}$. Observe now that $h + t \in G^{\perp}$ if and only if $h, t \in G^{\perp}$. ∎

Proof of Theorem II. That S (in (10)) satisfies $|S| = M$ follows from the Chinese Remainder Theorem. Let C be any coset of any subgroup H of σ, $C \cap G^{\perp} \neq \emptyset$. According to Lemma III there exists $t \in C \cap H^{\perp}$. Since $C \cap G^{\perp} \neq \emptyset$ we have $h + t \in G^{\perp}$ for some $h \in H$. Thus by (19) (reversing the roles of H, G) we conclude that $t \in G^{\perp}$. By (20), (22) then

(31) $$\begin{aligned} C &= H + t = (H \cap G) + (H \cap G^{\perp}) + t \subset G + (H \cap G^{\perp}) + t \\ &= G + ((H+t) \cap G^{\perp}) = G + (C \cap G^{\perp}). \end{aligned}$$

This establishes (13). ∎

We make two observations about N-uniform sets now. Say that a finite nonempty subset $S \subset \mathbf{Z}$ is *uniformly distributed* if

(32) $$\{x \,(\mathrm{mod}\, |S|)\colon x \in S\} = \{0, \ldots, |S|-1\}.$$

Our first observation is that N-uniform sets are uniformly distributed. To see this simply choose $m = 1$ in (7). Next observe that if S is N-uniform then

(33) $$a((m, |S|)) \subset [a(m) \cap S] + O(|S|)$$

for all $a \in \mathbf{Z}$, $m \in N$ satisfying $m \mid N$ and $a(m) \cap S \neq \emptyset$. Indeed, it follows from Euclid's algorithm for the g.c.d. that

(34) $$a((m, |S|)) = a(m) + O(|S|),$$

and (33) now follows at once from (7).

Given a disjoint covering system $\Delta = \{a_i(n_i)\colon 1 \leqslant i \leqslant t\}$ and a finite nonempty subset $S \subset \mathbf{Z}$ define the *reduced system* $\mathrm{red}(\Delta|S)$ to be the multiset

(35) $$\mathrm{red}(\Delta|S) = \{a_i((n_i, |S|))\colon i \in I\}$$

where

(36) $$I = I_{\Delta,S} = \{1 \leqslant i \leqslant t\colon a_i(n_i) \cap S \neq \emptyset\}.$$

Theorem V. *If S is N-uniform, where*

(37) $$[n_1, \ldots, n_t] \mid N,$$

then $\mathrm{red}(\Delta|S)$ *is a disjoint covering system.*

Proof. First we show that $\mathrm{red}(\Delta|S)$ covers $\mathbf{Z}$. Since the moduli of $\mathrm{red}(\Delta|S)$ are all divisors of $|S|$, and since S is uniformly distributed, it suffices to show that $\mathrm{red}(\Delta|S)$ covers S. But this is immediate:

(38) $$S = \bigcup_{i \in I} (a_i(n_i) \cap S) \subset \bigcup_{i \in I} a_i(n_i) \subset \bigcup_{i \in I} a_i((n_i, |S|)).$$

Next we show that the sets in $\mathrm{red}(\Delta|S)$ are all disjoint. Suppose

(39) $$x \in a_i((n_i, |S|)) \cap a_j((n_j, |S|)); \quad i, j \in I.$$

According to (33)

(40) $$x = y + \alpha|S| = z + \beta|S|$$

where $y \in a_i(n_i) \cap S$, $z \in a_j(n_j) \cap S$ and $\alpha, \beta \in \mathbf{Z}$. Thus $y \equiv z \,(\mathrm{mod}\, |S|)$. Since S is uniformly distributed this implies that $y = z$, and since the sets in Δ are disjoint, we must have $i = j$. ∎

Remarks. (i) If S is uniformly distributed, then every set $a(m)$ intersects S, whenever $m \| S|$. In particular, then, if S is uniformly distributed

(41) $$\mathrm{red}(\mathrm{red}(\Delta|S)|S) = \mathrm{red}(\Delta|S).$$

(ii) Let n_k be divmax. If S is uniformly distributed, $|S| = n_k$, then the residue classes of modulus n_k in $\mathscr{D}$ and $\mathrm{red}(\Delta|S)$ coincide. Thus we may always assume, without loss of generality, that a divmax modulus of a disjoint covering system is in fact the maximum modulus of a disjoint covering system, *all of whose moduli are factors of it* – without altering the residue classes which have n_k as modulus.

(iii) Let $F\colon N \to N$ be any function. Denote

(42) $$\hat{F}(n; \Delta) = \min_{n_i \neq n} F\left(\frac{n}{(n, n_i)}\right).$$

If $|S| = n$ then

(43) $$\hat{F}(n; \Delta) \leqslant \hat{F}(n; \mathrm{red}(\Delta|S)).$$

Indeed,

(44) $$\hat{F}(n; \mathrm{red}(\Delta|S)) = \min_{\substack{(n_i, n) \neq n \\ i \in I}} F\left(\frac{n}{(n_i, n)}\right) \geqslant \min_{n_i \neq n} F\left(\frac{n}{(n_i, n)}\right).$$

We next introduce some of the lattice geometry described in [1]. A *product set*, $\mathcal{R}$, in Z^n is any finite nonempty set of the form

(45) $$\mathcal{R} = R_1 \times \ldots \times R_n$$

where $R_1, \ldots, R_n \subset Z$. The set R_i is referred to as the ith *projection of* $\mathcal{R}$, denoted

(46) $$R_i = \pi_i(\mathcal{R}); \quad 1 \leqslant i \leqslant n.$$

For $b = (b_1, \ldots, b_n) \in N^n$ the set

(47) $$\mathcal{P} = \{c = (c_1, \ldots, c_n) \in Z^n:\ 0 \leqslant c_i < b_i;\ 1 \leqslant i \leqslant n\}$$

is called the $(n; b)$-*parallelotope*. If $b_1 = \ldots = b_n = b$ then this parallelotope is called the $(n; b)$-*cube*.

We define now the *parallelotope function* ψ. (This is not the same function used in [1].) Again let $\sigma = \sigma_N$ where N has the prime factorization (8). Let $\mathcal{T} = \mathcal{T}_N$ be the $(l; (p_1^{d_1}, \ldots, p_l^{d_l}))$-parallelotope. Given $k \in \sigma$ and $j \in \{1, \ldots, l\}$ set

(48) $$\psi^{(j)}(k) = \sum_{i=1}^{d_j} a_i^{(j)} p_j^{i-1},$$

where

(49) $$k(\text{mod}\, p_j^{d_j}) = \sum_{i=1}^{d_j} a_i^{(j)} p_j^{d_j - i}.$$

(Observe that the coefficients for $\psi^{(j)}(k)$ are in reverse order to those for k.) Then set

(50) $$\psi(k) = \left(\psi^{(1)}(k), \ldots, \psi^{(l)}(k)\right).$$

In this way $\psi = \psi_N$: $\sigma \to \mathcal{T}$.

Proposition VI. *ψ is bijective, and if C is a coset of σ,*

(51) $$|C| = \prod_{j=1}^{l} p_j^{f_j},$$

then

(52) $$\psi(C) = c + \mathcal{T}'$$

where $\mathcal{T}'$ is the $(l; (p_1^{f_1}, \ldots, p_l^{f_l}))$-parallelotope and $c = (c_1, \ldots, c_l) \in \mathcal{T}$ satisfies

(53) $$p_j^{f_j} \mid c_j, \quad 1 \leqslant j \leqslant l.$$

Proof. Observe first that $\psi^{(j)}(k)$ uniquely determines $k(\text{mod}\, p_j^{d_j})$. Thus it follows from the Chinese Remainder Theorem that ψ is one-to-one. Since $|\sigma| = |\mathcal{T}|$, ψ must be a bijection. Next observe that if H is a subgroup of σ,

(54) $$|H| = \prod_{j=1}^{l} p_j^{f_j},$$

then for each $h \in H$

(55) $$p_j^{d_j - f_j} \mid h(\text{mod}\, p_j^{d_j}), \quad 1 \leqslant j \leqslant l.$$

This means that the first $d_j - f_j$ p_j-ary coefficients for $h(\text{mod}\, p_j^{d_j})$ are zero. Thus for any $k \in \sigma$ the first $d_j - f_j$ p_j-ary coefficients for $(h+k)(\text{mod}\, p_j^{d_j})$, or equivalently the last $d_j - f_j$ p_j-ary coefficients for $\psi^{(j)}(h+k)$, must be independent of $h \in H$. From this it follows that

(56) $$\psi^{(j)}(h+k) = \alpha_j p_j^{f_j} + \beta_j$$

where α_j is independent of h and $0 \leqslant \beta_j < p_j^{f_j}$, $1 \leqslant j \leqslant l$. Since ψ is one-to-one it now follows from a cardinality consideration that

(57) $$\psi(H+k) = (\alpha_1 p_1^{f_1}, \ldots, \alpha_l p_l^{f_l}) + \mathcal{T}'. \ \blacksquare$$

2. Geometric proof of Theorem I. Let $N = [n_1, \ldots, n_t]$ with prime factorization (1.8). We can restate Theorem I in terms of an exact partition $\Gamma = \{C_i:\ 1 \leqslant i \leqslant t\}$ of σ into cosets. Say that C_k is *divmin* if

(1) $$|C_i| \,\big|\, |C_k| \Rightarrow |C_i| = |C_k|.$$

Theorem I. *If C_k is divmin then at least*

(2) $$\min_{|C_i| \neq |C_k|} G\left(\frac{|C_i|}{(|C_i|, |C_k|)}\right)$$

cosets in Γ have cardinality $|C_k|$.

Proof. According to Remarks (ii), (iii) above we may assume, without loss of generality, that C_k is a singleton. Set

(3) $$x = \min_{|C_i| \neq 1} G(|C_i|).$$

Let ψ: $\sigma \to \mathcal{T}$ be the parallelotope function, and set

(4) $$\mathcal{R} = \mathcal{C} \cap \mathcal{T},$$

where $\mathcal{C}$ is the $(l; x)$-cube. Observe that

(5) $$|\pi_j(\mathcal{R})| = \min(x, p_j^{d_j}), \quad 1 \leqslant j \leqslant l.$$

(In general, x may be larger than $p_j^{d_j}$ for some values of j. In other words, $\mathcal{C}$ need not be contained in $\mathcal{T}$.) By translating $\mathcal{R}$ if necessary we may assume that $\psi(C_k) \subset \mathcal{R}$. Let C be any coset of σ with $|\pi_j(\psi(C))| \geqslant |\pi_j(\mathcal{R})|$ for some j.

It follows from (1.52), (1.53) that

(6) $$\psi(C)\cap\mathscr{R}\neq\emptyset \Leftrightarrow \pi_j(\psi(C))=\pi_j(\mathscr{R}).$$

Consider now one of the cosets C_i, $|C_i|\neq 1$, and let $G(|C_i|)=p_j^{f_j}\geqslant x$. Then

(7) $$|\pi_j(\psi(C_i))|=p_j^{f_j}\geqslant x=|\pi_j(\mathscr{R})|,$$

and thus according to (6)

(8) $$\psi(C_i)\cap\mathscr{R}\neq\emptyset \Leftrightarrow |\pi_j(\psi(C_i)\cap\mathscr{R})|=|\pi_j(\psi(C_i))\cap\pi_j(\mathscr{R})|=|\pi_j(\mathscr{R})|=x.$$

In particular

(9) $$x\,\big|\,|\psi(C_i)\cap\mathscr{R}|.$$

Observe next that

(10) $$\Lambda=\{\psi(C_i)\cap\mathscr{R}\colon\ \psi(C_i)\cap\mathscr{R}\neq\emptyset\}$$

forms an exact partition of $\mathscr{R}$. Since the cardinality of $\mathscr{R}$ is a multiple of x it follows from (9) that the number of singletons in Λ must be a multiple of x. This number is at least one, since $\psi(C_k)\in\Lambda$, and thus it must be at least x. Finally, $\psi(C_i)\cap\mathscr{R}$ is a singleton only if C_i is a singleton. ■

3. Analytic proof of Theorem I. In this section and the next we consider a disjoint covering system $\Delta=\{a_i(n_i)\colon 1\leqslant i\leqslant t\}$ and make the reasonable assumption

(1) $$0\leqslant a_i<n_i,\quad 1\leqslant i\leqslant t.$$

Under this assumption the identity

(2) $$\sum_{i=1}^{t}\frac{z^{a_i}}{1-z^{n_i}}=\frac{1}{1-z}$$

is valid for $z\in C$, $|z|<1$. In particular, if n_k is divmax then it follows from (2) that $P(\omega_{n_k})=0$, where ω_{n_k} is a primitive n_kth root of unity and $P(z)$ is the polynomial

(3) $$P(z)=\sum_{n_i=n_k} z^{a_i}.$$

M. Newman [3] used this condition to obtain the bound $p(n_k)$ for the number of residue classes in Δ having n_k as modulus. In fact he proved the following

LEMMA VII. *Suppose* $Q(\omega_n)=0$ *for*

(4) $$Q(z)=\sum_{i=1}^{L}\alpha_i z^{a_i},$$

where $a_1,\ldots,a_L$ *are distinct integers between* 0 *and* $n-1$, *and* $\alpha_1,\ldots,\alpha_L$ *are nonzero rationals. Then* $L\geqslant p(n)$.

We improve upon this estimate by exploiting the fact that $P(\omega)=0$ for several roots of unity of different orders, simultaneously. Precisely, if

(5) $$n\,|\,n_i \Leftrightarrow n_i=n_k,\quad 1\leqslant i\leqslant t$$

then $P(\omega_n)=0$. Thus we are led to consider equations satisfied simultaneously be several different roots of unity.

LEMMA VIII. *Let* $M_1, M\in N$ *with* $M_1\,|\,M$, *and let* M *have the prime factorization*

(6) $$M=\prod_{j=1}^{l}p_j^{d_j}.$$

Write

(7) $$M_1=\prod_{j=1}^{l}p_j^{e_j}$$

where the e_j *are allowed to be zero. Suppose* $Q(\omega_n)=0$ *for every* n *in the quotient range*

(8) $$M_1\,|\,n\,|\,M,$$

where $Q(z)$ *is as in Lemma* VII. *Then*

(9) $$L\geqslant\min_{e_j>0}p_j^{d_j-e_j+1}.$$

Observe that if $M_1=M$ then (9) becomes $L\geqslant p(n)$, as in Lemma VII.

Proof. If $(n,s)=1$ then

(10) $$Q(\omega_n)=0\Leftrightarrow Q(\omega_n^s)=0.$$

We claim that

(11) $$\sum_{i=1}^{L}\alpha_i\omega_M^{sa_i}=Q(\omega_M^s)=0$$

for every s in the range $1\leqslant s<x$, where

(12) $$x=\min_{e_j>0}p_j^{d_j-e_j+1}.$$

To see this observe that $\omega_M^s=\omega_n^{s'}$, where

(13) $$n=\frac{M}{(s,M)},\qquad s'=\frac{s}{(s,M)}.$$

For s in the range $1\leqslant s<x$ this value of n lies in the quotient range (8). Furthermore $(n,s')=1$. Since $Q(\omega_n)=0$, it follows from (10) that $Q(\omega_M^s)=Q(\omega_n^{s'})=0$, as claimed.

Now we consider the equations (10), $1\leqslant s<x$, as a system of $x-1$ linear equations for $\alpha_1,\ldots,\alpha_L$ (with complex coefficients). If $L<x$ then the

first L such equations would form a homogeneous $L\times L$ system with the Vandermonde matrix $(\omega_M^{ia_j})$ as coefficient matrix. The determinant of this matrix is

$$\omega_M^{a_1+\ldots+a_L}\prod_{1\leqslant i<j\leqslant L}(\omega_M^{a_j}-\omega_M^{a_i}), \tag{14}$$

which is manifestly nonzero. This contradiction thereby proves that $L\geqslant x$. ∎

Remark. Newman [3] used precisely this proof with $x=p(n)$. In this case every s, $1\leqslant s<x$, is clearly relatively prime to n, and so $Q(\omega_n^s)=0$. We simply observe here that if $Q(\omega)=0$ for several different roots of unity, one can take advantage of this to increase x.

Proof of Theorem I. Let $N=[n_1,\ldots,n_t]$ have the prime factors $p_1,\ldots,p_l$ and write

$$n_k=\prod_{j=1}^{l}p_j^{d_j}. \tag{15}$$

For $n_i\neq n_k$ define

$$\gamma_i=p_{j(i)}^{e(i)+1} \tag{16}$$

where $j(i)$, $e_{j(i)}$ are defined through

$$G\left(\frac{n_k}{(n_i,n_k)}\right)=p_{j(i)}^{d_{j(i)}-e_{j(i)}}. \tag{17}$$

Then $e_{j(i)}$ is the exponent of $p_{j(i)}$ in the prime factorization of n_i. Set

$$M_1=[\gamma_i\colon\ n_i\neq n_k],\qquad M=n_k. \tag{18}$$

Since $e_{j(i)}$ is strictly less than $d_{j(i)}$ it follows that each γ_i (hence $M-1$) is a divisor of n_k. On the other hand no γ_i is a divisor of the corresponding n_i, and thus M_1 is not a divisor of any n_i, $n_i\neq n_k$. The upshot of this is that every n in the quotient range (8) satisfies (5). Correspondingly, then, for these values of n, $P(\omega_n)=0$. Thus according to Lemma VIII the number of terms in the polynomial $P(z)$ must be at least

$$\min_{n_i\neq n_k}p_{j(i)}^{d_{j(i)}-e_{j(i)}}=\min_{n_i\neq n_k}G\left(\frac{n_k}{(n_i,n_k)}\right).\ ∎$$

4. A consequence of the Conway–Jones vanishing sum criteria. A disjoint covering system $\Delta=\{a_i(n_i)\colon 1\leqslant i\leqslant t\}$ is said to be *n_k-reducible* if some of its residue classes of modulus n_k can be combined into a single residue class of smaller modulus — precisely, if

$$\bigcup_{n_i=n_k}a_i(n_i)\supset a(m) \tag{1}$$

for some $a\in Z$ and proper divisor, m, of n_k. Otherwise Δ is said to be *n_k-irreducible.*

THEOREM IX. *Let n_k be divmax and suppose Δ is n_k-irreducible. Then n_k must have at least three distinct prime factors; and at least*

$$p_1+p_2+p_3-4 \tag{2}$$

residue classes in Δ must have n_k as modulus, where p_1, p_2, p_3 are the three smallest prime divisors of n_k.

Before proving this theorem we introduce another type of reduction for a disjoint covering system, in addition to that one described in Section 1. Let $N=[n_1,\ldots,n_t]$ have the prime factorization

$$N=\prod_{i=1}^{l}p_i^{d_i}. \tag{3}$$

Any divisor $M\in N$ of N has a factorization

$$M=\prod_{i=1}^{l}p_i^{e_i} \tag{4}$$

where $0\leqslant e_i\leqslant d_i$, $1\leqslant i\leqslant l$. Denote

$$\tilde{M}=\prod_{d_i=e_i}p_i. \tag{5}$$

We now define the *square-free system* $\mathrm{SQF}(\Delta)$ to be

$$\mathrm{SQF}(\Delta)=\{a_i'(\tilde{n}_i)\colon\ i\in J\} \tag{6}$$

where

$$J=J_\Delta=\{1\leqslant i\leqslant t\colon\ a_i(n_i)\cap O(N/\tilde{N})\neq\emptyset\} \tag{7}$$

and, for $i\in J$, $a_i'\dfrac{N}{\tilde{N}}$ is the least nonnegative integer in $a_i(n_i)\cap O(N/\tilde{N})$. Since

$$a_i(n_i)\cap O\left(\frac{N}{\tilde{N}}\right)=a_i'\frac{N}{\tilde{N}}\left(\tilde{n}_i\frac{N}{\tilde{N}}\right),\qquad i\in J, \tag{8}$$

it is clear that $\mathrm{SQF}(\Delta)$ *is also a disjoint covering system.*

Remarks. (i) The moduli of $\mathrm{SQF}(\Delta)$ are square-free, and

$$[\tilde{n}_i\colon\ i\in J]=\tilde{N}. \tag{9}$$

(ii) If $n_i=N$ then

$$i\in J\ \Leftrightarrow\ \frac{N}{\tilde{N}}\bigg|a_i \tag{10}$$

in which case $a_i'=a_i\dfrac{\tilde{N}}{N}$; and conversely

$$\tilde{n}_i=\tilde{N}\ \Leftrightarrow\ n_i=N. \tag{11}$$

This shows that if $O(N)\in\Delta$ then $\mathrm{SQF}(\Delta)$ *is N-irreducible whenever* Δ *is.*

Proof of Theorem IX. By translating if necessary assume that $a_k = 0$. We first replace Δ with $\mathrm{red}(\Delta|S)$, where S is an N-uniform set, $|S| = n_k$, for $N = [n_1, \ldots, n_t]$. This in effect allows us to assume in our original system Δ that $n_k = [n_1, \ldots, n_t]$, without changing any of the residue classes of Δ with modulus n_k. Next we apply our square-free reduction, SQF. This allows us to assume that n_k is square-free, while preserving n_k-irreducibility and not increasing the number of residue classes with modulus n_k. Furthermore we still have $O(n_k)\in\Delta$. Summarizing all of this we assume, without loss of generality, that $a_k = 0$ and n_k is square-free.

Let now

$$S(z) = \sum_{i\in K} z^{a_i} \tag{12}$$

be a minimal subsum of $\sum_{n_i=n_k} z^{a_i}$ such that (i) $k\in K$, and (ii) $S(\omega_{n_k}) = 0$. Define an integer n by $\frac{n_k}{n} = (n_k, a_i\colon i\in K)$ and set

$$\bar{S}(z) = \sum_{i\in K} z^{a_i\frac{n}{n_k}}. \tag{13}$$

Then $\bar{S}(\omega_n) = 0$. According to Conway and Jones ([2], Thm. 5)

$$|K| \geqslant \sum_{\substack{p|n\\ p\ \text{prime}}} (p-2)+2, \tag{14}$$

and thus it suffices to show that n must have at least three distinct prime factors.

The only polynomials with rational coefficients of degree $p-1$ or less, p prime, which vanish at ω_p are scalar multiples of

$$1+z+\ldots+z^{p-1}. \tag{15}$$

Thus if $n = p$ then $\left\{a_i\frac{p}{n_k}\colon i\in K\right\} = \{0, 1, \ldots, p-1\}$, contradicting the n_k-irreducibility of Δ. It remains then to rule out the case $n = pq$, for two distinct primes p and q. For this case decompose $\bar{S}(z)$ as

$$\bar{S}(z) = \sum_{i=0}^{p-1} z^{iq} R_i(z^p), \tag{16}$$

where

$$R_i(z) = \sum_{j=0}^{q-1} \alpha_{ij} z^j, \quad 0 \leqslant i < p \tag{17}$$

and each α_{ij} is either zero or one. It follows from [2], Lemma 1, that

$$R_0(\omega_q) = \ldots = R_{p-1}(\omega_q). \tag{18}$$

By what we said above regarding (15) it follows that $\alpha_{0j}-\alpha_{1j}$ must be constant, independent of j. If this constant is ± 1 then α_{0j} must also be constant, and $R_0(\omega_q) = 0$. Otherwise, if this constant is 0 then $R_0(z) \equiv R_1(z)$. Arguing along these lines we see that either

$$R_0(\omega_q) = \ldots = R_{p-1}(\omega_q) = 0 \tag{19}$$

or else

$$R_0(z) \equiv \ldots \equiv R_{p-1}(z). \tag{20}$$

Alternative (19): Since the $R_i(z)$ cannot all be identically zero, one of them, say $R_0(z)$, must be of the form (15). But then $\left\{a_i\frac{q}{n_k}\colon i\in K\right\} \supset \{0, 1, \ldots, q-1\}$, contradicting the n_k-irreducibility of Δ.

Alternative (20): Since $R_0(z)$ cannot be identically zero, some coefficient, say α_{00}, must be one. But then each α_{i0} is one, and $\left\{a_i\frac{p}{n_k}\colon i\in K\right\} \supset \{0, 1, \ldots, p-1\}$, contradicting the n_k-irreducibility of Δ. ∎

Remark. If Δ is n_k-reducible then either it can be reduced to a disjoint covering system in which n_k does not appear at all, or else Theorem IX applies. Disjoint covering systems which can be completely reduced (all the way to $O(1)$) are precisely the *natural* systems of Znám. Thus Theorem IX can be considered a result concerning *unnatural* systems.

Acknowledgment. The authors gratefully acknowledge the help of the referee who pointed out the Conway–Jones paper and suggested its applicability here.

References

[1] M. A. Berger, A. Felzenbaum, and A. S. Fraenkel, *A non-analytic proof of the Newman–Znám result for disjoint covering systems*, Combinatorica 6 (1986), pp. 235–243.
[2] J. H. Conway and A. J. Jones, *Trigonometric diophantine equations*, Acta Arith. 30 (1976), pp. 229–240.
[3] M. Newman, *Roots of unity and covering sets*, Math. Ann. 191 (1971), pp. 279–282.
[4] Š. Znám, *On exactly covering systems of arithmetic sequences*, in: *Number Theory*, Colloq. Math. Societatis János Bolyai Vol. 2 (P. Turán, ed.), Debrecen 1968, North-Holland, Amsterdam 1970, pp. 221–225.

FACULTY OF MATHEMATICAL SCIENCES
THE WEIZMANN INSTITUTE OF SCIENCES
Rehovot 76100, Israel

Received on 5.11.1984
and in revised form on 18.3.1986 (1470)