BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 14, Number 1, January 1986

NEW RESULTS FOR COVERING SYSTEMS OF RESIDUE SETS

BY MARC A. BERGER, ALEXANDER FELZENBAUM AND AVIEZRI S. FRAENKEL

We announce some new results about systems of residue sets. A residue set $R \subset \mathbf{Z}$ is an arithmetic progression

$$R = \{a, a \pm n, a \pm 2n, \ldots\}.$$

The positive integer n is referred to as the *modulus* of R. Following Znám [21] we denote this set by $a(n)$. We need several number-theoretic functions.

$p(m)$–the least prime divisor of a natural number m,

$P(m)$–the greatest prime divisor of m,

$\Lambda(m)$–the greatest divisor of m which is a power of a single prime:

$$\Lambda(m) = \max\{d \in \mathbf{Z}\colon d|m, d = p^s, \quad p \text{ prime}\},$$

$f(m) = \sum_{j=1}^{l} s_j(p_j - 1) + 1$, where m has the prime factorization $m = p_1^{s_1} \cdots p_l^{s_l}$,

$g(m) = \prod_{j=1}^{l}(1 + x_j) - \sum_{j=1}^{l} x_j - 1$, where

$$x_j = \frac{\sum_{k=0}^{s_j-1} p_j^k}{p_j^{s_j} - \sum_{k=0}^{s_j-1} p_j^k}$$

and m has the above prime factorization,

$\varphi(m)$–Euler's totient function,

$[x]$–the greatest integer in x.

Recent general surveys on systems of residue sets are Porubský [21] and Znám [26]. Results and problems on residue sets appear also in Erdős and Graham [14] and Guy [16].

1. Disjoint covering systems [1, 2, 3, 6, 9, 10]. These are systems $\mathcal{D} = (a_1(n_1), \ldots, a_t(n_t))$, $t > 1$, which partition $\mathbf{Z}$. The multiplicity of a modulus $n = n_k$ is the number of sets in $\mathcal{D}$ with that modulus. The multiplicity of $\mathcal{D}$ is the maximum multiplicity of its moduli.

THEOREM 1. *The multiplicity of any modulus $n = n_k$ is at least*

$$m_1 = \min_{n_i \neq n} \Lambda\left(\frac{n}{(n, n_i)}\right). \tag{1}$$

The multiplicity of $\mathcal{D}$ is at least

$$m_2 = \left[\frac{P(N)\varphi(N)}{N}\right] + 1, \tag{2}$$

Received by the editors June 7, 1985.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11A07, 11B75, 11H31, 11B25, 20D15, 20D60, 51A15.

where $N = l.c.m.(n_1, \ldots, n_t)$.

If n is maximal in the sense of division, that is,

$$n | n_i \Rightarrow n = n_i,$$

then $m_1 \geq p(n)$. Thus (1) includes the Znám-M. Newman result [**13, 19, 24**] and (2) proves the Burshtein conjecture [**11**]. We have generalized (2) to the setting of coset partitions. Precisely,

THEOREM 2. *Let* $(C_1, \ldots, C_t)$, $t > 1$ *be a coset partition of a finite supersolvable group* G. *Then at least*

$$m = \left\lceil \frac{P(N)\varphi(N)}{N} \right\rceil + 1$$

of the C_i *have the same cardinality, where*

$$N = \frac{|G|}{g.c.d.(|C_1|, \ldots, |C_t|)}.$$

Observe that $m \geq p(N)$ so that this implies the conjectures of Herzog-Schönheim [**17**] for the case of supersolvable groups.

We have classified all disjoint covering systems which have precisely one multiple modulus, the multiplicity of which is at most nine. Up to permutation, the moduli of such a system must be

$$n_i = 2^i, \qquad 1 \leq i \leq r; \qquad n_i = l_{i-r}2^r, \qquad r+1 \leq i \leq t$$

where $r \geq 0$ and there are 12 possibilities for $(l_1, \ldots, l_{t-r})$, aside from the 8 trivial cases $l_1 = \cdots = l_{t-r}$, $2 \leq t - r \leq 9$. The list of 12 appears in [**9**]. This includes the results of Porubský [**20**], Stein [**22**] and Znám [**23**], and proves a conjecture of Porubský for the case of multiplicity 7 [**20**].

2. Incongruent covering systems [**5**]. These are systems $\mathcal{D} = (a_1(n_1), \ldots, a_t(n_t))$, $t > 1$, which cover $\mathbf{Z}$ and for which the moduli n_i are all distinct.

THEOREM 3. *If the moduli* n_i *are all odd then* $g(N) \geq 1$, *where* $N = l.c.m.(n_1, \ldots, n_t)$.

We show that $g(N) < 1$ whenever $\sum_{j=1}^{l} \sum_{k=1}^{s_j} p_j^{-k} < 1$, which is Theorem A conjectured by Churchhouse [**12**]. We have generalized this to the setting of coset partitions.

THEOREM 4. *Let* $(C_1, \ldots, C_t)$, $t > 1$, *be a coset cover of a finite nilpotent group* G *of odd order. If* $g(|G|) < 1$ *then at least two of the* C_i *have the same cardinality.*

Observe that

$$g(m) < \prod_{j=1}^{l} \frac{p_j - 1}{p_j - 2} - \sum_{j=1}^{l} \frac{1}{p_j - 2} - 1,$$

so these theorems put necessary conditions on the prime factors p_j. In particular, this is a generalization to nilpotent groups of the main result (Corollary 2) of [**12**].

3. The covering function [2, 7]. Given a system $\mathcal{D} = (a_1(n_1), \dots, a_t(n_t))$, its covering function $\mathcal{T}_{\mathcal{D}}: \mathbf{Z} \to \mathbf{Z}$ is given by

$$\mathcal{T}_{\mathcal{D}}(k) = \text{the number of sets } a_i(n_i) \text{containing } k.$$

THEOREM 5. *Let* $\mathcal{D} = (a_1(n_1), \dots, a_t(n_t))$ *and* $\mathcal{D}' = (a_1'(n_1'), \dots, a_{t'}'(n_{t'}'))$ *each have multiplicity strictly less than* $p(N)$, *where* $N = l.c.m.(n_1, \dots, n_t, n_1', \dots, n_{t'}')$. *Then*

$$\mathcal{T}_{\mathcal{D}} = \mathcal{T}_{\mathcal{D}'} \Rightarrow \mathcal{D} = \mathcal{D}'.$$

This generalizes Theorem 2 of Znám [**25**] for incongruent covering systems.

THEOREM 6. *If* $\mathcal{T}_{\mathcal{D}}$ *is constant modulo* M, *then each maximal modulus* $n = n_k$ *(maximal in the sense of division) has multiplicity at least* $\min(p(n), M)$.

This is a different generalization of the Znám-Newman result [**13, 19, 24**], since $\mathcal{T}_{\mathcal{D}} \equiv 1$ whenever $\mathcal{D}$ is a disjoint covering system.

4. Minimal covering systems [8]. These are systems

$$\mathcal{D} = (a_1(n_1), \dots, a_t(n_t)),$$

$t > 1$, which cover $\mathbf{Z}$ but contain no proper subsystem which covers $\mathbf{Z}$.

THEOREM 7. *The number of sets* $a_i(n_i)$ *satisfies* $t \geq f(N)$ *where* $N = l.c.m.(n_1, \dots, n_t)$.

This extends the results of Korec [**18**] and Znám [**25**].

5. Generalized arithmetic progressions [4]. These are systems of the form

(3)
$$D = \left\{ \left[n\frac{p_i}{q_i} + \beta_i \right] : p_i, q_i \in \mathbf{N},\ (p_i, q_i) = 1,\ \beta_i \in \mathbf{R},\ i = 1, \dots, t,\ n \in \mathbf{Z} \right\}.$$

THEOREM 8. *Let* $p_1 \leq p_2 \leq \cdots \leq p_t$. *If* (3) *is a disjoint covering system, then*

(a) $p_{t-1} = p_t$;

(b) $t \geq 3$, $p_{t-1}/q_{t-1} \neq p_t/q_t \Rightarrow p_{t-2} = p_{t-1} = p_t$.

Part (a) generalizes the result of Mirsky, D. Newman, Davenport and Rado [**13**] (which is a special case of the Znám-Newman result), since $q_{t-1} = q_t = 1$ implies equality of the two largest moduli. Part (b) proves the weak conjecture in [**15**] for the case where at most two of the moduli are nonintegral, and the strong conjecture for the case where precisely one modulus is nonintegral.

6. Proofs. The main proof techniques in this area have been based on function theory and roots of unity. Most of the above-mentioned results have been obtained by developing a new elementary geometric-combinatorial method. In particular, our proof of Theorem 1 seems to be the first genuine direct combinatorial proof of the Znám-Newman result.

Define the lattice parallelotope

$$P(n; \mathbf{b}) = \{\mathbf{c} = (c_1, \dots, c_n) \in \mathbf{Z}^n : 0 \leq c_i < b_i\ (1 \leq i \leq n)\},$$

and let $\sigma = \sigma_N = \{0, 1, \ldots, N-1\}$ be the cyclic group under addition mod N. Let $N = p_1^{s_1} \cdots p_l^{s_l}$ be the prime factorization of N. Define two bijections from σ_N into two parallelotopes.

Let $k \in \sigma$ and $j \in \{1, \ldots, l\}$. Further, let

$$k \equiv k_j \ (\mathrm{mod}\ p_j^{s_j}), \qquad 0 \leq k_j < p_j^{s_j},$$

and let $k_j = \sum_{i=0}^{s_j-1} a_i^{(j)} p_j^{s_j-1-i}$ be the p_j-ary representation of k_j with $0 \leq a_i^{(j)} < p_j$ $(1 \leq i < s_j)$.

The *high-dimensional parallelotope function*

$$\Phi = \Phi_N : \sigma \to P\left(\sum_{j=1}^{l} s_j ; \overbrace{p_1, \ldots, p_1}^{s_1}, \ldots, \overbrace{p_l, \ldots, p_l}^{s_l}\right)$$

is defined as follows. Let $\Phi^{(j)}(k) = (a_0^{(j)}, \ldots, a_{s_j-1}^{(j)})$. Then

$$\Phi(k) = (\Phi^{(1)}(k), \ldots, \Phi^{(l)}(k)).$$

The *low-dimensional parallelotope function* $\Psi = \Psi_N : \sigma \to P(l; p_1^{s_1}, \ldots, p_l^{s_l})$ is defined by

$$\Psi(k) = (\Psi^{(1)}(k), \ldots, \Psi^{(l)}(k)),$$

where $\Psi^{(j)}(k) = \sum_{i=0}^{s_j-1} a_i^{(j)} p_j^i$ (the $a_i^{(j)}$ as defined above for k_j).

The main idea of the proof method is indicated for a disjoint covering system $D = (a_1(n_1), \ldots, a_t(n_t))$, which is but a coset partition of σ_N, where $N = \mathrm{l.c.m.}(n_1, \ldots, n_t)$. Using Φ or Ψ, this coset partition becomes a *cell partition* of the parallelotope P. Properties of such partitions have been identified and proved, and they translate back into results about residue sets.

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 (to appear).

2. ——, *Lattice parallelepipeds and disjoint covering systems*, Department of Mathematics, The Weizmann Institute of Science, May 1984. (Currently being revised.)

3. ——, *The Herzog-Schönheim conjecture for finite nilpotent groups*, Canad. Math. Bull. (to appear).

4. ——, *Disjoint covering systems of rational Beatty sequences*, J. Combini. Theory A (to appear).

5. ——, *Necessary condition for the existence of an incongruent covering system with odd moduli*, Acta Arith. (to appear).

6. ——, *Improvements to the Newman-Znám result for disjoint covering systems*, Acta Arith. (to appear).

7. ——, *Improvements to two results concerning systems of residue sets*, Ars Combin. (to appear).

8. ——, *Covers of product sets and the Korec-Znám result*, Department of Mathematics, The Weizmann Institute of Science, November, 1984.

9. ——, *Disjoint covering systems with precisely one multiple modulus*, Department of Mathematics, The Weizmann Institute of Science, January, 1985.

10. ——, *Remark on the multiplicity of a partition of a group into cosets*, Fund. Math. (to appear).

11. N. Burshtein, *On natural exactly covering systems of congruences having moduli occurring at most M times*, Discrete Math. **14** (1976), 205–214.

12. R. F. Churchhouse, *Covering sets and systems of congruences*, Computers in Mathematical Research (R. F. Churchhouse and J.-C. Herz, eds.), North-Holland, Amsterdam, 1968, pp. 20–36.

13. P. Erdős, *On a problem concerning covering systems* (Hungarian; English summary), Mat. Lapok. **3** (1952), 122–128.

14. P. Erdős and R. L. Graham, *Old and new problems and results in combinatorial number theory*, Monographie No. 28 de L'Enseignement Mathématique, Université de Genève, 1980.

15. A. S. Fraenkel, *Complementing and exactly covering sequences*, J. Combin. Theory **14** (1973), 8–20.

16. R. K. Guy, *Unsolved problems in number theory*, Springer-Verlag, New York, N. Y., 1981.

17. M. Herzog and J. Schönheim, *Research problem no.* 9, Canad. Math. Bull. **17** (1974), 150.

18. I. Korec, *On a generalization of Mycielski's and Znám's conjectures about coset decomposition of Abelian groups*, Fund. Math. **85** (1974), 41–48.

19. M. Newman, *Roots of unity and covering sets*, Math. Ann. **191** (1971), 279–282.

20. Š. Porubský, *Generalization of some results for exactly covering systems*, Mat. Casopis Sloven. Akad. Vied **22** (1972), 208–214.

21. ——, *Results and problems on covering systems of residue classes*, Mitteilungen aus dem Math. Sem. Giessen, Heft 150, Universität Giessen, 1981.

22. S. K. Stein, *Unions of arithmetic sequences*, Math. Ann. **134** (1958), 289–294.

23. Š. Znám, *On exactly covering systems of arithmetic sequences*, Math. Ann. **180** (1969), 227–232.

24. ——, *On exactly covering systems of arithmetic sequences*, Number Theory, Colloq. Math. Societatis János Bolyai Vol. 2 (P. Turán, ed.), Debrecen, 1968, North-Holland, Amsterdam, 1970, pp. 221–225.

25. ——, *On properties of systems of arithmetic sequences*, Acta Arith. **26** (1975), 279–283.

26. ——, *A survey of covering systems of congruences*, Acta Mathematica Universitatis Comenianae **40–41** (1982), 59–78.

DEPARTMENT OF MATHEMATICS, THE WEIZMANN INSTITUTE OF SCIENCE, REHOVOT 76100, ISRAEL