ELECTRONIC RESEARCH ANNOUNCEMENTS
OF THE AMERICAN MATHEMATICAL SOCIETY
Volume 9, Pages 51–60 (July 10, 2003)
S 1079-6762(03)00111-2

UNIFICATION OF ZERO-SUM PROBLEMS, SUBSET SUMS AND COVERS OF $\mathbb{Z}$

ZHI-WEI SUN

(Communicated by Ronald L. Graham)

In memory of Paul Erdös

ABSTRACT. In combinatorial number theory, zero-sum problems, subset sums and covers of the integers are three different topics initiated by P. Erdös and investigated by many researchers; they play important roles in both number theory and combinatorics. In this paper we announce some deep connections among these seemingly unrelated fascinating areas, and aim at establishing a unified theory! Our main theorem unifies many results in these three realms and also has applications in many aspects such as finite fields and graph theory. To illustrate this, here we state our extension of the Erdös-Ginzburg-Ziv theorem: If $A = \{a_s(\text{mod } n_s)\}_{s=1}^k$ covers some integers exactly $2p-1$ times and others exactly $2p$ times, where p is a prime, then for any $c_1, \cdots, c_k \in \mathbb{Z}/p\mathbb{Z}$ there exists an $I \subseteq \{1, \cdots, k\}$ such that $\sum_{s\in I} 1/n_s = p$ and $\sum_{s\in I} c_s = 0$.

1. BACKGROUND

In 1961 Erdös, Ginzburg and Ziv [EGZ] established the following celebrated theorem and thus laid the foundation of the zero-sum theory.

The EGZ Theorem. *For any $c_1, \cdots, c_{2n-1} \in \mathbb{Z}$, there is an $I \subseteq [1, 2n-1] = \{1, \cdots, 2n-1\}$ with $|I| = n$ such that $\sum_{s\in I} c_s \equiv 0 \pmod n$. In other words, given $2n-1$ (not necessarily distinct) elements of the ring $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ of residues modulo n, we can select n of them with the sum vanishing.*

The EGZ theorem can be easily reduced to the case where n is a prime (and hence $\mathbb{Z}_n$ is a field), and then deduced from the well-known Cauchy-Davenport theorem or the Chevalley-Warning theorem (see, e.g., Nathanson [N, pp. 48–51]).

Here is another fundamental result due to Olson [O].

Received by the editors March 20, 2003.

2000 *Mathematics Subject Classification.* Primary 11B75; Secondary 05A05, 05C07, 11B25, 11C08, 11D68, 11P70, 11T99, 20D60.

Key words and phrases. Zero-sum, subset sums, covers of $\mathbb{Z}$.

The website `http://pweb.nju.edu.cn/zwsun/csz.htm` is devoted to the topics covered by this paper.

Supported by the Teaching and Research Award Fund for Outstanding Young Teachers in Higher Education Institutions of MOE, and the National Natural Science Foundation of P. R. China.

Theorem 1.1 (Olson). *Let p be a prime and $\mathbb{Z}_p^l$ be the direct sum of l copies of the ring $\mathbb{Z}_p$. Given $c, c_1, \cdots, c_{l(p-1)+1} \in \mathbb{Z}_p^l$ we have*

$$\sum_{\substack{I \subseteq [1, l(p-1)+1] \\ \sum_{s \in I} c_s = c}} (-1)^{|I|} \equiv 0 \pmod{p}; \tag{1.1}$$

in particular there exists a nonempty $I \subseteq [1, l(p-1)+1]$ with $\sum_{s \in I} c_s = 0$.

Observe that the additive group of the finite field with p^l elements is isomorphic to $\mathbb{Z}_p^l$. For convenience we let $\mathbb{Z}_p^0$ be the additive subgroup $\{\bar{0} = p\mathbb{Z}\}$ of $\mathbb{Z}_p$ throughout this paper; thus Theorem 1.1 remains valid even if $l = 0$.

Let p be a prime and $c, c_1, \cdots, c_{2p-1} \in \mathbb{Z}_p$. In 1996 Gao [G] proved that

$$\left| \left\{ I \subseteq [1, 2p-1] \colon |I| = p \text{ and } \sum_{s \in I} c_s = c \right\} \right| \equiv [c = 0] \pmod{p},$$

where for a predicate P we let $[P]$ be 1 or 0 according to whether P holds or not. Note that Gao's result clearly follows from Olson's congruence (1.1) in the case $l = 2$.

In 1994 Alford, Granville and Pomerance [AGP] employed a result of zero-sum type to prove that there are infinitely many Carmichael numbers. For results and conjectures on zero-sum problems, the reader is referred to the survey [C].

What is the smallest integer $k = s(\mathbb{Z}_n^2)$ such that every sequence of k elements in $\mathbb{Z}_n^2$ contains a zero-sum subsequence of length n? In 1983 Kemnitz [K] conjectured that $s(\mathbb{Z}_n^2) = 4n - 3$. In 1993 Alon and Dubiner [AD] showed that $s(\mathbb{Z}_n^2) \leqslant 6n - 5$. In 2000 Rónyai [R] was able to prove that $s(\mathbb{Z}_p^2) \leqslant 4p - 2$ for every prime p.

For a finite set $S = \{a_1, \cdots, a_k\}$ contained in the ring $\mathbb{Z}$ or a field, sums of the form $\sum_{s \in I} a_s$ with $I \subseteq [1, k]$ are called subset sums of S. It is interesting to provide a nontrivial lower bound for the cardinality of the set

$$\{a_1 x_1 + \cdots + a_k x_k \colon x_1, \cdots, x_k \in \{0, 1\}\} = \left\{ \sum_{s \in I} a_s \colon I \subseteq [1, k] \right\}.$$

A more general problem is to study restricted sumsets in the form

$$\{x_1 + \cdots + x_k \colon x_1 \in X_1, \cdots, x_k \in X_k,\ P(x_1, \cdots, x_k) \neq 0\}, \tag{1.2}$$

where $X_1, \cdots, X_k$ are subsets of a field and $P(x_1, \cdots, x_k)$ is a polynomial with coefficients in the field. In 1964 Erdös and Heilbronn [EH] conjectured that if p is a prime and $\emptyset \neq X \subseteq \mathbb{Z}_p$, then

$$|\{x + y \colon x, y \in X \text{ and } x \neq y\}| \geqslant \min\{p, 2|X| - 3\}.$$

This conjecture was first confirmed by Dias da Silva and Hamidoune [DH] in 1994, who obtained a generalization which implies that if $S \subseteq \mathbb{Z}_p$ and $|S| > \sqrt{4p - 7}$, then any element of $\mathbb{Z}_p$ is a subset sum of S. In this direction the most powerful tool is the following remarkable principle (see Alon [A99], [A03]), rooted in Alon and Tarsi [AT] and applied in [AF], [ANR1], [ANR2], [DKSS], [HS], [LS] and [PS].

Combinatorial Nullstellensatz. *Let $X_1, \cdots, X_k$ be finite subsets of a field F with $|X_s| > l_s$ for $s \in [1, k]$, where $l_1, \cdots, l_k \in \mathbb{N} = \{0, 1, 2, \cdots\}$. If $f(x_1, \cdots, x_k) \in F[x_1, \cdots, x_k]$, $[x_1^{l_1} \cdots x_k^{l_k}] f(x_1, \cdots, x_k)$ (the coefficient of the monomial $\prod_{s=1}^k x_s^{l_s}$ in f) is nonzero and $\sum_{s=1}^k l_s$ is the total degree of f, then there are $x_1 \in X_1, \cdots, x_k \in X_k$ such that $f(x_1, \cdots, x_k) \neq 0$.*

One of the many applications of the Combinatorial Nullstellenstaz is the following result of [AT] on finite fields.

Theorem 1.2 (Alon and Tarsi). *Let F be a finite field with $|F|$ not a prime, and let M be a nonsingular $k \times k$ matrix over F. Then there exists a vector $\vec{x} \in F^k$ such that neither $\vec{x}$ nor $M\vec{x}$ has zero component.*

Now we turn to covers of $\mathbb{Z}$.

For $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+ = \{1, 2, 3, \cdots\}$ we call

$$a(n) = a + n\mathbb{Z} = \{a + nx\colon x \in \mathbb{Z}\}$$

a residue class with modulus n. For a finite system

$$A = \{a_s(n_s)\}_{s=1}^k \tag{1.3}$$

of residue classes, its *covering function* $w_A(x) = |\{1 \leqslant s \leqslant k\colon x \in a_s(n_s)\}|$ is periodic modulo the least common multiple N_A of the moduli $n_1, \cdots, n_k$. Sun [S99] called $m(A) = \min_{x\in\mathbb{Z}} w_A(x)$ the *covering multiplicity* of (1.3). One can easily verify the following well-known inequality:

$$\sum_{s=1}^k \frac{1}{n_s} = \frac{1}{N_A} \sum_{x=0}^{N_A-1} w_A(x) \geqslant m(A). \tag{1.4}$$

If $\bigcup_{s=1}^k a_s(n_s) = \mathbb{Z}$ (i.e., $m(A) \geqslant 1$), then we call (1.3) a *cover* (or *covering system*) of $\mathbb{Z}$. The concept of cover was first introduced by Erdös in the 1930's (cf. [E]); it has many surprising applications (cf. [Cr], [S00] and [S01]). Erdös was very proud of this invention; he said: *"Perhaps my favorite problem of all concerns covering systems."*

For $m \in \mathbb{Z}^+$, if $m(A) \geqslant m$, then A is said to be an *m-cover* of $\mathbb{Z}$; general m-covers were first studied by the author in [S95]. If (1.3) forms an m-cover of $\mathbb{Z}$ but $A_t = \{a_s(n_s)\}_{s\neq t}$ does not, then we say that (1.3) is an m-cover of $\mathbb{Z}$ with $a_t(n_t)$ *essential*.

If $w_A(x) = m$ for all $x \in \mathbb{Z}$, then we call (1.3) an *exact m-cover* of $\mathbb{Z}$. (Note that in this case we have $\sum_{s=1}^k 1/n_s = m$ by (1.4).) Such covers were first introduced by Porubský [P] in 1976. Clearly m copies of $0(1)$ form a trivial exact m-cover of $\mathbb{Z}$. Using a graph-theoretic argument Zhang [Z91] proved that for each $m = 2, 3, \cdots$ there are exact m-covers of $\mathbb{Z}$ which are not unions of an n-cover and an $(m-n)$-cover with $0 < n < m$.

There are many problems and results on covers; the reader is recommended to consult the introduction part of [S96] and the recent survey [P-S].

Here we mention some properties of covers related to Egyptian fractions. The first nontrivial result of this nature is the following one discovered by Zhang [Z89] with the help of the Riemann zeta function: If (1.3) forms a cover of $\mathbb{Z}$, then

$$\sum_{s\in I} \frac{1}{n_s} \in \mathbb{Z} \quad \text{for some nonempty } I \subseteq [1, k]. \tag{1.5}$$

The author [S95], [S96], [S99] obtained the following further extensions of Zhang's result.

Theorem 1.3 (Sun). *Let (1.3) be an m-cover of $\mathbb{Z}$ and let $m_1, \cdots, m_k \in \mathbb{Z}^+$.*

(i) *There are at least m positive integers in the form $\sum_{s\in I} m_s/n_s$ with $I \subseteq [1, k]$. Also, $|\{|I|\colon I \subseteq [1, k]$ and $\sum_{s\in I} m_s/n_s \in \mathbb{Z}^+\}| \geqslant m$.*

(ii) *For any* $J \subseteq [1,k]$ *there are at least* m *subsets* $I \neq J$ *of* $[1,k]$ *such that* $\{\sum_{s\in I} m_s/n_s\} = \{\sum_{s\in J} m_s/n_s\}$, *where* $\{\alpha\}$ *denotes the fractional part of a real number* α.

Zero-sum problems and subset sums seem to have nothing to do with covers of $\mathbb{Z}$. Before this work no one has realized their close connections. Can you imagine that the EGZ theorem and the Alon-Tarsi theorem are related to covers of $\mathbb{Z}$? The purpose of this paper is to announce a surprising unified theory and embed the study of zero-sum problems and subset sums in the investigation of covers.

In the next section we will present the Main Theorem together with its various consequences. In Section 3 we will state two key lemmas, the first of which connects the zero-sum problems with the study of subset sums, and the second plays an important role in the proof of the Main Theorem. Detailed proofs of the results in this announcement appeared in the preprint [S03], which contains a more general version of the Main Theorem.

2. Our main results

For a prime p we let $\mathbb{Z}'_p$ denote the ring of p-integers (i.e., the rationals with denominators not divisible by p). (Recall that $\mathbb{Z}_p$ denotes $\mathbb{Z}/p\mathbb{Z}$.) If $a,b,c \in \mathbb{Z}$ and $p \nmid b$, then the congruence $a/b \equiv c \pmod p$ over $\mathbb{Z}'_p$ is equivalent to the usual congruence $a \equiv bc \pmod p$ over $\mathbb{Z}$.

Let Ω be the ring of all algebraic integers. For $\omega_1,\omega_2,\gamma \in \Omega$, by $\omega_1 \equiv \omega_2 \pmod \gamma$ we mean $\omega_1 - \omega_2 \in \gamma\Omega$. For $a,b,m \in \mathbb{Z}$ it is well known that $a-b \in m\Omega$ if and only if $a-b \in m\mathbb{Z}$. For $m \in \mathbb{Z}$ and a root ζ of unity, if $\zeta \equiv 0 \pmod m$, then $1 = \zeta\zeta^{-1} \equiv 0 \pmod m$ (since $\zeta,\zeta^{-1} \in \Omega$) and hence m must be 1 or -1.

Theorem 1.1 of zero-sum nature and Theorem 1.3 on covers of $\mathbb{Z}$ are both special cases of part (i) of the following general result.

The Main Theorem. *Let* (1.3) *be a (finite) system of residue classes.*

(i) *Let* $m_s \in \mathbb{Z}$ *and* $c_t, c_{st} \in \mathbb{Q}$ *for all* $s \in [1,k]$ *and* $t \in [0,l]$. *Let* p *be a prime and let* $0 \leqslant \theta < 1$. *Assume that whenever* $I \subseteq [1,k]$ *and* $\{\sum_{s\in I} m_s/n_s\} = \theta$ *we have* $\sum_{s\in I} c_{st} - c_t \in \mathbb{Z}'_p$ *for all* $t \in [0,l]$. *Set*

$$\mathcal{I} = \left\{ I \subseteq [1,k]\colon \left\{ \sum_{s\in I} \frac{m_s}{n_s} \right\} = \theta,\ \sum_{s\in I} c_{st} - c_t \in p\mathbb{Z}'_p \textit{ for all } t \in [1,l] \right\}.$$

Then, either we have the inequality

$$\left| \left\{ \sum_{s\in I} c_{s0} - c_0 \bmod p\colon I \in \mathcal{I} \right\} \right| > m(A) - l(p-1), \tag{2.1}$$

or $|\{I \in \mathcal{I}\colon \sum_{s\in I} c_{s0} - c_0 \in p\mathbb{Z}'_p\}| \neq 1$ *and furthermore*

$$\sum_{\substack{I\in\mathcal{I} \\ \sum_{s\in I} c_{s0} - c_0 \in p\mathbb{Z}'_p}} (-1)^{|I|} e^{2\pi i \sum_{s\in I} a_s m_s/n_s} \equiv 0 \pmod p. \tag{2.2}$$

(ii) *Suppose that* $m(A) < m(A')$, *where* $A' = \{a_1(n_1), \cdots, a_k(n_k), a(n)\}$, $a \in \mathbb{Z}$, $n \in \mathbb{Z}^+$ *and* $w_A(a) = m(A)$. *Let* $m_1,\cdots,m_k \in \mathbb{Z}$ *be relatively prime to* $n_1,\cdots,n_k$, *respectively. Let* $J \subseteq \{1 \leqslant s \leqslant k\colon a \in a_s(n_s)\}$ *and* $P(x_1,\cdots,x_k) \in F[x_1,\cdots,x_k]$, *where F is a field with characteristic not dividing N_A. Assume that $0 \leqslant \deg P \leqslant |J|$ and*

$$\left[\prod_{j\in J} x_j\right] P(x_1,\cdots,x_k)(x_1+\cdots+x_k)^{|J|-\deg P} \neq 0.$$

Let $X_1 = \{b_1, c_1\}, \cdots, X_k = \{b_k, c_k\}$ be subsets of F such that $b_s = c_s$ only if $a \in a_s(n_s)$ and $s \notin J$. Then for some $0 \leqslant \alpha < 1$ we have

$$|S_r| \geqslant |J| - \deg P + 1 > 0 \quad \textit{for all } r = 0, 1, \cdots, n-1, \tag{2.3}$$

where

$$S_r = \left\{ \sum_{s=1}^{k} x_s \colon x_s \in X_s,\ P(x_1,\cdots,x_k) \neq 0,\ \left\{ \sum_{\substack{s=1\\ x_s\neq b_s}}^{k} \frac{m_s}{n_s} \right\} = \frac{\alpha + r}{n} \right\}. \tag{2.4}$$

When $l = \theta = 0$, $c_{s0} \in \{1, m_s/n_s\}$ and p is a sufficiently large prime, part (i) of the Main Theorem yields Theorem 1.3(i). Theorem 1.3(ii) follows from the first part of the Main Theorem in the case $l = 0$ and $c_{s0} = 2^s$ because two subsets I, J of $[1, k]$ are equal if and only if $\sum_{s\in I} 2^s = \sum_{s\in J} 2^s$.

In the case $n_1 = \cdots = n_k = n = 1$, part (ii) of the Main Theorem yields the following basic lemma of the so-called polynomial method due to Alon, Nathanson and Ruzsa [ANR1], [ANR2]: Let $X_1, \cdots, X_k$ be subsets of a field F with $|X_s| = h_s \in \{1, 2\}$ for $s \in [1, k]$. If $P(x_1, \cdots, x_k) \in F[x_1, \cdots, x_k] \setminus \{0\}$, $\deg P \leqslant \sum_{s=1}^{k}(h_s - 1)$ and

$$[x_1^{h_1-1}\cdots x_k^{h_k-1}]P(x_1,\cdots,x_k)(x_1+\cdots+x_k)^{\sum_{s=1}^{k}(h_s-1)-\deg P} \neq 0,$$

then

$$\left|\left\{ \sum_{s=1}^{k} x_s \colon x_s \in X_s \text{ and } P(x_1,\cdots,x_k) \neq 0 \right\}\right| \geqslant \sum_{s=1}^{k}(h_s - 1) - \deg P + 1.$$

Actually this remains valid even if h_s may be greater than two.

In the rest of this section we will list various other results deduced from the Main Theorem.

Theorem 2.1. *Let (1.3) be an $l(p-1)+1$-cover of $\mathbb{Z}$, where $l \in \mathbb{N}$ and p is a prime. Let $m_1, \cdots, m_k \in \mathbb{Z}$ and $c_1, \cdots, c_k \in \mathbb{Z}_p^l$. Then for any $0 \leqslant \theta < 1$ and $c \in \mathbb{Z}_p^l$ we have*

$$\sum_{\substack{I\subseteq[1,k]\\ \sum_{s\in I} c_s = c\\ \{\sum_{s\in I} m_s/n_s\}=\theta}} (-1)^{|I|} e^{2\pi i \sum_{s\in I} a_s m_s/n_s} \equiv 0 \pmod{p}; \tag{2.5}$$

in particular, there is a nonempty subset I of $[1, k]$ such that $\sum_{s\in I} c_s = 0$ and $\sum_{s\in I} m_s/n_s \in \mathbb{Z}$.

Since a system of k copies of $0(1)$ forms a k-cover of $\mathbb{Z}$, Theorem 1.1 is a special case of Theorem 2.1. In the case $l = 0$ Theorem 2.1 yields Zhang's result (1.5) on covers of $\mathbb{Z}$.

In 1984 Alon, Friedland and Kalai [AFK1], [AFK2] proved that if p is a prime, then any loopless graph with average degree bigger than $2p - 2$ and maximum degree at most $2p - 1$ must contain a p-regular subgraph. Now we apply Theorem 2.1 to strengthen this result.

Corollary 2.1. *Let G be a loopless graph of l vertices with the edge set $\{1,\cdots,k\}$. Suppose that all the vertices of G have degree not greater than $2p-1$ and that* (1.3) *forms an $l(p-1)+1$-cover of $\mathbb{Z}$, where p is a prime. Then for any $m_1,\cdots,m_k\in\mathbb{Z}$ we have*

$$\mathcal{H}=\left\{p\text{-regular subgraph } H \text{ of } G\colon \sum_{s\in E(H)}\frac{m_s}{n_s}\in\mathbb{Z}\right\}\neq\emptyset,$$

where $E(H)$ denotes the edge set of the subgraph H; furthermore

$$\sum_{H\in\mathcal{H}}(-1)^{|E(H)|}e^{2\pi i\sum_{s\in E(H)}a_s m_s/n_s}\equiv -1 \pmod p. \tag{2.6}$$

Theorem 2.2. *Let* (1.3) *be a system of residue classes with $m(A)>(l+1)(p-1)$, where $l\in\mathbb{N}$ and p is a prime. Let $m_1,\cdots,m_k\in\mathbb{Z}$ and $c_1,\cdots,c_k\in\mathbb{Z}_p^l$. Then for any $c\in\mathbb{Z}_p^l$ and $r\in\mathbb{Q}$ we have*

$$\sum_{\substack{I\subseteq[1,k]\\ \sum_{s\in I}c_s=c\\ \sum_{s\in I}m_s/n_s\in r+p\mathbb{Z}}}(-1)^{|I|}e^{2\pi i\sum_{s\in I}a_s m_s/n_s}\equiv 0 \pmod p; \tag{2.7}$$

in particular, there is a nonempty subset I of $[1,k]$ such that $\sum_{s\in I}c_s=0$ and $\sum_{s\in I}m_s/n_s\in p\mathbb{Z}$.

Corollary 2.2. *Let* (1.3) *be a system of residue classes, and let p be a prime.*

(i) *If $2p-1\in\{w_A(x)\colon x\in\mathbb{Z}\}\subseteq\{2p-1,2p\}$, then for any $c_1,\cdots,c_k\in\mathbb{Z}_p$ there exists an $I\subseteq[1,k]$ such that $\sum_{s\in I}1/n_s=p$ and $\sum_{s\in I}c_s=0$.*

(ii) *If* (1.3) *forms an exact $3p$-cover of $\mathbb{Z}$, then for any $c_1,\cdots,c_k\in\mathbb{Z}_p^2$ with $c_1+\cdots+c_k=0$, there exists an $I\subseteq[1,k]$ such that $\sum_{s\in I}1/n_s=p$ and $\sum_{s\in I}c_s=0$.*

The EGZ theorem and Lemma 3.2 of Alon and Dubiner [AD] are parts (i) and (ii) of our Corollary 2.2 in the case $n_1=\cdots=n_k=1$. An interesting open question is whether we can replace the prime p in Corollary 2.2 by any positive integer n. The answer is affirmative if n is a prime power.

Theorem 2.3. *Suppose that* (1.3) *is an m-cover of $\mathbb{Z}$ with $a_k(n_k)$ essential. Let $m_1,\cdots,m_{k-1}\in\mathbb{Z}$ be relatively prime to $n_1,\cdots,n_{k-1}$, respectively. Let F be a field with characteristic p not dividing N_A, and let $X_1=\{b_1,c_1\},\cdots,X_{k-1}=\{b_{k-1},c_{k-1}\}$ be any subsets of F with cardinality 2. Then for some $0\leqslant\alpha<1$ we have*

$$\left|\left\{\sum_{s=1}^{k-1}x_s\colon x_s\in X_s,\ \left\{\sum_{\substack{1\leqslant s<k\\ x_s=c_s}}\frac{m_s}{n_s}\right\}=\frac{\alpha+r}{n_k}\right\}\right|\geqslant\min\{p',m\} \tag{2.8}$$

for all $r\in[0,n_k-1]$, where $p'=p$ if p is a prime, and $p'=+\infty$ if $p=0$.

Theorem 2.3 implies the second result stated in the abstract of [S99]. Provided that (1.3) forms an exact m-cover of $\mathbb{Z}$, in 1997 the author [S97] proved that for any $a=0,1,\cdots,mn_k-1$ we have

$$\left|\left\{I\subseteq[1,k-1]\colon\sum_{s\in I}\frac{1}{n_s}=\frac{a}{n_k}\right\}\right|\geqslant\binom{m-1}{\lfloor a/n_k\rfloor}.$$

We can show that this remains true if (1.3) is only an m-cover of $\mathbb{Z}$ with $\sum_{s=1}^{k-1}1/n_s<m$.

Corollary 2.3. *Suppose that* (1.3) *is a p-cover of $\mathbb{Z}$ with $a_k(n_k)$ essential, where p is a prime not dividing N_A. Let $m_1, \cdots, m_{k-1} \in \mathbb{Z}$ be relatively prime to $n_1, \cdots, n_{k-1}$, respectively. Then, for any $c, c_1, \cdots, c_{k-1} \in \mathbb{Z}_p$ with $c_1 \cdots c_{k-1} \neq 0$ the set*

$$\left\{\left\{\sum_{s\in I}\frac{m_s}{n_s}\right\}: I \subseteq [1, k-1] \text{ and } \sum_{s\in I} c_s = c\right\} \tag{2.9}$$

contains an arithmetic progression of length n_k with common difference $1/n_k$.

Theorem 2.4. *Assume that* (1.3) *does not form an $m+1$-cover of $\mathbb{Z}$ but $A' = \{a_1(n_1), \cdots, a_k(n_k), a(n)\}$ does, where $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. Let $m_1, \cdots, m_k$ be integers relatively prime to $n_1, \cdots, n_k$, respectively. Let F be a field of prime characteristic p, and let $a_{ij}, b_i \in F$ for all $i \in [1, m]$ and $j \in [1, k]$. Set*

$$X = \left\{\sum_{j=1}^{k} x_j : x_j \in [0, p-1] \text{ and } \sum_{j=1}^{k} x_j a_{ij} \neq b_i \text{ for all } i \in [1, m]\right\}. \tag{2.10}$$

If p does not divide N_A and the matrix $(a_{ij})_{1\leqslant i\leqslant m, 1\leqslant j\leqslant k}$ has rank m, then the set

$$\left\{\left\{\sum_{s\in I}\frac{m_s}{n_s}\right\}: I \subseteq [1, k] \text{ and } |I| \in X\right\} \tag{2.11}$$

contains an arithmetic progression of length n with common difference $1/n$.

We mention that Theorem 1.2 follows from Theorem 2.4.

Theorem 2.5. *Let* (1.3) *be an m-cover of $\mathbb{Z}$ with $a_k(n_k)$ essential and $n_k = N_A$. Let $m_1, \cdots, m_{k-1} \in \mathbb{Z}$ be relatively prime to $n_1, \cdots, n_{k-1}$, respectively. Then for any $r \in [0, N_A - 1]$ we have the inequality*

$$\left|\left\{I \subseteq [1, k-1]: \left\{\sum_{s\in I}\frac{m_s}{n_s}\right\} = \frac{r}{N_A}\right\}\right| \geqslant 2^{m-1}. \tag{2.12}$$

Theorem 2.5 in the special case $m = m_1 = \cdots = m_{k-1} = 1$ was first observed by Z. H. Sun on the basis of the author's work [S95]. If $m_1, \cdots, m_{n-1} \in \mathbb{Z}$ are relatively prime to n, then by applying Theorem 2.5 to the disjoint cover $\{r(n)\}_{r=0}^{n-1}$ we find that $\{\sum_{s\in I} m_s : I \subseteq [1, n-1]\}$ contains a complete system of residues modulo n.

3. Two technical lemmas

Lemma 3.1. *Let R be a ring with identity, and let $f(x_1, \cdots, x_k)$ be a polynomial over R. If $J \subseteq [1, k]$ and $|J| \geqslant \deg f$, then we have the identity*

$$\sum_{I\subseteq J}(-1)^{|J|-|I|} f([1 \in I], \cdots, [k \in I]) = \left[\prod_{j\in J} x_j\right] f(x_1, \cdots, x_k). \tag{3.1}$$

Our Lemma 3.1 is powerful; it implies Lemma 2.2 of [R] (used by Rónyai in his study of the Kemnitz conjecture), as well as Combinatorial Nullstellenstaz in the case $l_1, \cdots, l_k \in \{0, 1\}$.

By applying Lemma 3.1, we obtain the following two theorems.

Theorem 3.1. *Let p be a prime. If $c_{st}, c_t \in \mathbb{Z}$ for all $s \in [1, l(p-1)]$ and $t \in [1, l]$, then*

$$\sum_{\substack{I_1\cup\cdots\cup I_l = [1, l(p-1)] \\ |I_1| = \cdots = |I_l| = p-1}} \prod_{t=1}^{l}\prod_{s\in I_t} c_{st} \equiv \sum_{\substack{I\subseteq[1, l(p-1)] \\ p \mid \sum_{s\in I} c_{st} - c_t \text{ for } t\in[1, l]}} (-1)^{|I|} \pmod{p}. \tag{3.2}$$

In particular, if $c, c_1, \cdots, c_{2p-2} \in \mathbb{Z}$*, then*

$$\sum_{\substack{I\subseteq[1,p-1]\\ p\mid\sum_{s\in I}c_s-c}}(-1)^{|I|}\equiv c_1\cdots c_{p-1}\pmod p \tag{3.3}$$

and

$$\left|\left\{I\subseteq[1,2p-2]\colon |I|=p-1,\ p\ \Big|\ \sum_{s\in I}c_s-c\right\}\right|\equiv\sum_{\substack{I\subseteq[1,2p-2]\\ |I|=p-1}}\prod_{s\in I}c_s\pmod p.$$

We mention that Theorem 3.1 implies Theorem 1.1.

Theorem 3.2. *Let* $a_1, \cdots, a_{4p-3}, b_1, \cdots, b_{4p-3} \in \mathbb{Z}$*, where* p *is a prime. If*

$$\sum_{\substack{I,J\subseteq[1,4p-3]\\ |I|=|J|=p-1\\ I\cap J=\emptyset}}\Big(\prod_{i\in I}a_i\Big)\Big(\prod_{j\in J}b_j\Big)\not\equiv 2\pmod p, \tag{3.4}$$

then there exists an $I \subseteq [1, 4p-3]$ *with* $|I| = p$ *such that* $\sum_{s\in I} a_s \equiv \sum_{s\in I} b_s \equiv 0 \pmod p$.

This provides an advance on the Kemnitz conjecture.

Our proof of the Main Theorem depends heavily on the following lemma.

Lemma 3.2. *Let* (1.3) *be a system of residue classes, and let* $m_1, \cdots, m_k$ *be any integers. Let* F *be a field containing an element* ζ *of (multiplicative) order* N_A*, and let* $f(x_1, \cdots, x_k) \in F[x_1, \cdots, x_k]$ *and* $\deg f \leqslant m(A)$*. Set* $I_z = \{1 \leqslant s \leqslant k\colon z \in a_s(n_s)\}$ *for* $z \in \mathbb{Z}$*. If* $[\prod_{s\in I_z} x_s]f(x_1, \cdots, x_k) = 0$ *for all* $z \in \mathbb{Z}$*, then*

$$\sum_{\substack{I\subseteq[1,k]\\ \{\sum_{s\in I}m_s/n_s\}=\theta}}(-1)^{|I|}f([1\in I],\cdots,[k\in I])\zeta^{N_A\sum_{s\in I}a_sm_s/n_s}=0$$

for all $0 \leqslant \theta < 1$*. The converse holds when* $m_1, \cdots, m_k$ *are relatively prime to* $n_1, \cdots, n_k$*, respectively.*

Observe that Lemma 3.2 in the case $n_1 = \cdots = n_k = 1$ follows from Lemma 3.1.

References

[AGP] W. R. Alford, A. Granville and C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. Math. **139** (1994), 703–722. MR **95k:**11114

[A99] N. Alon, *Combinatorial Nullstellensatz*, Combin. Probab. Comput. **8** (1999), 7–29. MR **2000b:**05001

[A03] N. Alon, *Discrete mathematics: methods and challenges*, in: Proceedings of the International Congress of Mathematicians (Beijing, 2002), Vol. I, Higher Education Press, Beijing, 2003, pp. 119–136.

[AD] N. Alon and M. Dubiner, *Zero-sum sets of prescribed size,* in: Combinatorics, Paul Erdös is Eighty, János Bolyai Math. Soc., Budapest, 1993, pp. 33–50. MR **94j:**11016

[AFK1] N. Alon, S. Friedland and G. Kalai, *Regular subgraphs of almost regular graphs*, J. Combin. Theory Ser. B **37** (1984), 79–91. MR **86d:**05064a

[AFK2] N. Alon, S. Friedland and G. Kalai, *Every 4-regular graph plus an edge contains a 3-regular subgraph*, J. Combin. Theory Ser. B **37** (1984), 92–93. MR **86d:**05064b

[AF] N. Alon and Z. Füredi, *Covering the cube by affine hyperplanes*, European J. Combin. **14** (1993), 79–83. MR **94a:**52039

[ANR1] N. Alon, M. B. Nathanson and I. Z. Ruzsa, *Adding distinct congruence classes modulo a prime*, Amer. Math. Monthly **102** (1995), 250–255. MR **95k:**11009

[ANR2] N. Alon, M. B. Nathanson and I. Z. Ruzsa, *The polynomial method and restricted sums of congruence classes*, J. Number Theory **56** (1996), 404–417. MR **96k:**11011

[AT] N. Alon and M. Tarsi, *A nowhere-zero point in linear mappings*, Combinatorica **9** (1989), 393–395. MR **92a:**11147

[C] Y. Caro, *Zero-sum problems—a survey*, Discrete Math. **152** (1996), 93–113. MR **97c:**05156

[Cr] R. Crocker, *On a sum of a prime and two powers of two*, Pacific J. Math. **36** (1971), 103–107. MR **43:**3200

[DKSS] S. Dasgupta, G. Károlyi, O. Serra and B. Szegedy, *Transversals of additive Latin squares*, Israel J. Math. **126** (2001), 17–28. MR **2002j:**05027

[DH] J. A. Dias da Silva and Y. O. Hamidoune, *Cyclic spaces for Grassmann derivatives and additive theory*, Bull. London Math. Soc. **26** (1994), 140–146. MR **95i:**11007

[E] P. Erdös, *On integers of the form 2^k+p and some related problems*, Summa Brasil. Math. **2** (1950), 113–123. MR **13:**437i

[EGZ] P. Erdös, A. Ginzburg and A. Ziv, *Theorem in the additive number theory*, Bull. Research Council Israel **10** (1961), 41–43.

[EH] P. Erdös and H. Heilbronn, *On the addition of residue classes mod p*, Acta Arith. **9** (1964), 149–159. MR **29:**3463

[G] W. D. Gao, *Two addition theorems on groups of prime order*, J. Number Theory **56** (1996), 211–213. MR **96m:**11008

[HS] Q. H. Hou and Z. W. Sun, *Restricted sums in a field*, Acta Arith. **102** (2002), 239–249. MR **2003e:**11025

[K] A. Kemnitz, *On a lattice point problem*, Ars Combin. **16** (1983), 151–160. MR **85c:**52022

[LS] J. X. Liu and Z. W. Sun, *Sums of subsets with polynomial restrictions*, J. Number Theory **97** (2002), 301–304.

[N] M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets* (Graduate texts in mathematics; 165), Springer-Verlag, New York, 1996. MR **98f:**11011

[O] J. E. Olson, *A combinatorial problem on finite abelian groups (I)*, J. Number Theory **1** (1969), 8–10. MR **38:**5922

[PS] H. Pan and Z. W. Sun, *A lower bound for $|\{a+b\colon a\in A,\ b\in B,\ P(a,b)\neq 0\}|$*, J. Combin. Theory Ser. A **100** (2002), 387–393.

[P] Š. Porubský, *On m times covering systems of congruences*, Acta Arith. **29** (1976), 159–169. MR **53:**2884

[P-S] Š. Porubský and J. Schönheim, *Covering systems of Paul Erdös: past, present and future*, in: Paul Erdös and his Mathematics. I (edited by G. Halász, L. Lovász, M. Simonvits, V. T. Sós), Bolyai Soc. Math. Studies 11, Budapest, 2002, pp. 581–627.

[R] L. Rónyai, *On a conjecture of Kemnitz*, Combinatorica **20** (2000), 569–573. MR **2001k:**11025

[S95] Z. W. Sun, *Covering the integers by arithmetic sequences*, Acta Arith. **72** (1995), 109–129. MR **96k:**11013

[S96] Z. W. Sun, *Covering the integers by arithmetic sequences* II, Trans. Amer. Math. Soc. **348** (1996), 4279–4320. MR **97c:**11011

[S97] Z. W. Sun, *Exact m-covers and the linear form $\sum_{s=1}^k x_s/n_s$*, Acta Arith. **81** (1997), 175–198. MR **98h:**11019

[S99] Z. W. Sun, *On covering multiplicity*, Proc. Amer. Math. Soc. **127** (1999), 1293–1300. MR **99h:**11012

[S00] Z. W. Sun, *On integers not of the form $\pm p^a \pm q^b$*, Proc. Amer. Math. Soc. **128** (2000), 997–1002. MR **2000i:**11157

[S01] Z. W. Sun, *Algebraic approaches to periodic arithmetical maps*, J. Algebra **240** (2001), 723–743. MR **2002f:**11009

[S03] Z. W. Sun, *A unified theory of zero-sum problems, subset sums and covers of $\mathbb{Z}$*, preprint, Nanjing University, March 1, 2003. arXiv:math.NT/0305369

[Z89] M. Z. Zhang, *A note on covering systems of residue classes*, J. Sichuan Univ. (Nat. Sci. Ed.) **26** (1989), Special Issue, 185–188. MR **92c:**11003

[Z91] M. Z. Zhang, *On irreducible exactly m times covering system of residue classes*, J. Sichuan Univ. (Nat. Sci. Ed.) **28** (1991), 403–408. MR **92j:**11001

Department of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China

E-mail address: `zwsun@nju.edu.cn`