ELSEVIER
Available online at www.sciencedirect.com
SCIENCE DIRECT®
Discrete Mathematics 297 (2005) 196–201
DISCRETE MATHEMATICS
www.elsevier.com/locate/disc

Note

Kemnitz' conjecture revisited

Svetoslav Savchev[1], Fang Chen[a]

[a] *Oxford College of Emory University, Oxford, GA 30054, USA*

Received 13 December 2004; accepted 25 February 2005
Available online 28 July 2005

Abstract

A conjecture of Kemnitz remained open for some 20 years: each sequence of $4n-3$ lattice points in the plane has a subsequence of length n whose centroid is a lattice point. It was solved independently by Reiher and di Fiore in the autumn of 2003. A refined and more general version of Kemnitz' conjecture is proved in this note. The main result is about sequences of lengths between $3p-2$ and $4p-3$ in the additive group of integer pairs modulo p, for the essential case of an odd prime p. We derive structural information related to their zero sums, implying a variant of the original conjecture for each of the lengths mentioned. The approach is combinatorial.

MSC: 11B50; 11P21

Keywords: Kemnitz' conjecture; Zero-sums

1. Introduction

Let $\mathbb{Z}_n^2$ denote the additive group of integer pairs considered modulo n. What is the minimum number $s(n,2)$ with the property that each sequence of length $s(n,2)$ in $\mathbb{Z}_n^2$ has a subsequence of length n whose sum is the zero element of $\mathbb{Z}_n^2$? The $(4n-4)$-term sequence containing $n-1$ copies of each of the pairs $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$ shows that $s(n,2) \geqslant 4n-3$.

E-mail addresses: svetsavchev@yahoo.com (S. Savchev), fchen2@learnlink.emory.edu (F. Chen).

[1] No current affiliation.

0012-365X/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2005.02.018

Kemnitz [3] conjectured that $s(n, 2) = 4n - 3$ for all n. His conjecture is multiplicative: if true for some two positive integers, it is also true for their product. This observation reduces the question to the essential case where n is a prime. Hence it suffices to establish $s(p, 2) \leqslant 4p - 3$ for all primes p. The first linear upper bound for $s(p, 2)$ was given by Alon and Dubiner [1], who proved that $s(p, 2) \leqslant 6p - 5$ for each prime p. Rónyai [5] showed that $s(p, 2) \leqslant 4p - 2$, implying that $s(p, 2)$ is either $4p - 2$ or $4p - 3$ for every prime p.

In October 2003, Reiher [4] announced that he had proved Kemnitz' conjecture. At the same time, in October 2003 again, we witnessed an informal meeting where di Fiore [2] presented an independent proof of his own. The crucial argument in the two proofs is the same; they differ only in their preparatory parts. One cannot help expressing high esteem for the work of Christian Reiher, an undergraduate student, and Carlos di Fiore, still a high-school student at that time. A couple of weeks later we obtained the version included below.

In the sequel, p will denote a prime and all congruences will be modulo p. Let σ be a sequence of elements in $\mathbb{Z}_p^2$. A subsequence of σ is called a *zero subsequence* or a *zero sum* if the sum of its terms is the zero element in $\mathbb{Z}_p^2$. The empty subsequence of σ is assumed to be a zero sum by definition. The zero subsequences of σ with length k will be called *k-zero subsequences* or *k-zero sums*. We denote their number by $N(k, \sigma)$. Most of the work on zero-sum problems in $\mathbb{Z}_p^2$ is based on linear congruences involving the quantities $N(k, \sigma)$, modulo the prime p. Typical examples are the next two propositions.

Proposition 1. *Let p be a prime and α a sequence of length $m \geqslant 2p - 1$ in $\mathbb{Z}_p^2$. Then*

$$N(0, \alpha) - N(1, \alpha) + \cdots + (-1)^m N(m, \alpha) \equiv 0.$$

Proposition 2. *Let p be a prime and α a sequence of length at least $3p - 2$ in $\mathbb{Z}_p^2$. Then, for each $r \in \{0, 1, \ldots, p - 1\}$,*

$$N(r, \alpha) - N(r + p, \alpha) + N(r + 2p, \alpha) - \cdots \equiv 0.$$

Such congruence relations are obtained by algebraic means, for instance multilinear polynomials over finite fields and the Chevalley–Warning theorem.

However, algebraic considerations alone are probably not enough to prove Kemnitz' conjecture. The proof of Reiher and di Fiore is indirect and starts with easy-to-obtain or known congruence relations like the above. But it is a clever combinatorial argument that yields a contradiction.

Our intention here is not deriving yet another formal proof of Kemnitz' conjecture. We study a more subtle structural question about the role of the so-called *short* zero sums, ones of lengths less than p. It appears that in a “typical” sequence of length $4p - 3$ in $\mathbb{Z}_p^2$ two short zero sums can be lumped together to produce a p-zero sum. Are short zero sums not sufficient to guarantee a p-zero sum in “most” cases? Our main theorem shows that reality is not as simple as that. Sequences of length $4p - 3$ in $\mathbb{Z}_p^2$ differ significantly in the structure and organization of their p-zero sums. Still, their diversity can be described consistently from the viewpoint of short zero sums, which is done in Corollary 7. In particular, the conclusions imply Kemnitz' conjecture, revealing a variety of structural reasons for it to be true. The results generalize naturally to all lengths between $3p-2$ and $4p-3$. As a consequence, a variant of Kemnitz' conjecture is obtained for each of these lengths.

The quantities $N(k,\sigma)$ cannot express the idea of combining together zero sums to produce longer ones. So we introduce more general combinatorial quantities as follows. Let σ be a sequence in $\mathbb{Z}_p^2$. If an ℓ-zero sum β of σ contains a k-zero sum α, we call the ordered pair (α,β) a (k,ℓ)- *tower*. The number of (k,ℓ)-towers in σ will be denoted by $T(k,\ell,\sigma)$. An ℓ-zero sum β in σ can be regarded as a $(0,\ell)$-tower, because it contains the empty subsequence which is a zero sum by definition. Hence $T(0,\ell,\sigma)=N(\ell,\sigma)$ for all ℓ, meaning that towers indeed generalize zero sums.

Our main result is a congruence relation involving the tower-type quantities $T(k,\ell,\sigma)$. Not surprisingly, the substantial part of the proof is combinatorial, although its starting point is a certain algebraic relation proved in Lemma 4. The following statement by Alon and Dubiner [1] is also needed.

Proposition 3. *Each sequence with length $3p$ and sum zero in $\mathbb{Z}_p^2$ contains a subsequence with length p and sum zero.*

It is worth noting that this simple assertion is present in all proofs known so far of upper bounds for $s(p,2)$.

2. The main result

The core of this note is Theorem 5, which is a congruence relation for sequences of lengths between $3p-2$ and $4p-3$. Theorem 6 states explicitly the most interesting special case, where the length is $4p-3$. To prepare for the proof, in the next lemma we establish a relation for zero subsums in a sequence of length $2p$. In what follows, $\frac{1}{2}$ stands for the multiplicative inverse of 2 modulo a given odd prime p.

Lemma 4. *Let p be an odd prime. Each sequence α of length $2p$ and sum zero in $\mathbb{Z}_p^2$ satisfies the relation*

$$N(0,\alpha)-N(1,\alpha)+\cdots+N(p-1,\alpha)-\tfrac{1}{2}\,N(p,\alpha)\equiv 0.$$

Proof. We apply Proposition 1 to the sequence α. For p odd and $m=2p$, the relation takes the form

$$N(0,\alpha)-N(1,\alpha)+\cdots+N(p-1,\alpha)-N(p,\alpha)+\cdots+N(2p,\alpha)\equiv 0.$$

Since α has sum zero, taking complementary subsequences maps bijectively its k-zero sums onto its $(2p-k)$-zero sums. Hence $N(k,\alpha)=N(2p-k,\alpha)$ for all $k=0,1,\ldots,p-1$. It remains to notice that $N(k,\alpha)$ and $N(2p-k,\alpha)$ enter the sum above with the same sign, because k and $2p-k$ are of the same parity. $\square$

Theorem 5. *Let p be an odd prime and $\ell \in \{1, 2, \ldots, p\}$. Each sequence σ of length $3p - 3 + \ell$ in $\mathbb{Z}_p^2$ satisfies the relation*

$$\sum_{k=0}^{\ell-1} (-1)^k [T(k, p, \sigma) + T(k, 3p, \sigma)] + \sum_{k=\ell}^{p-1} (-1)^k T(k, 2p, \sigma) - \frac{1}{2} T(p, 2p, \sigma) \equiv 1.$$

Proof. We first apply Lemma 4 to all $(2p)$-zero subsequences of σ and sum up the resulting congruences. For a given k, as α ranges over the $(2p)$-zero sums of σ, the sum of the respective $N(k, \alpha)$ counts each $(k, 2p)$-tower of σ exactly once. Hence the summation gives

$$T(0, 2p, \sigma) - T(1, 2p, \sigma) + \cdots + T(p-1, 2p, \sigma) - \tfrac{1}{2} T(p, 2p, \sigma) \equiv 0. \tag{1}$$

Furthermore, by Proposition 2 (with $r = 0$), the original sequence σ satisfies the relation $\{N(0, \sigma) - N(p, \sigma) + N(2p, \sigma) - N(3p, \sigma) \equiv 0\}$. Since $N(0, \sigma) = 1$, by the definitions this is the same as

$$T(0, p, \sigma) - T(0, 2p, \sigma) + T(0, 3p, \sigma) \equiv 1. \tag{2}$$

Finally, another counting argument will show that the $T(k, 2p, \sigma)$ in (1) can be replaced by $T(k, p, \sigma) + T(k, 3p, \sigma)$ for all $k = 1, 2, \ldots, \ell - 1$.

Fix a $k \in \{1, \ldots, \ell - 1\}$ and consider any k-zero subsequence β of σ. Its complementary subsequence $\overline{\beta}$ has length $(3p - 3 + \ell) - k$, which is at least $3p - 2$. Hence Proposition 2 can be applied to $\overline{\beta}$, and we apply it with $r = p - k$. Since the length of $\overline{\beta}$ is less than $4p - k$, this gives

$$N(p - k, \overline{\beta}) - N(2p - k, \overline{\beta}) + N(3p - k, \overline{\beta}) \equiv 0.$$

Let us sum this congruence over all k-zero sums β of σ. Adjoining to β the $(p - k)$-zero sums of its complement $\overline{\beta}$ produces all (k, p)-towers in σ with first coordinate β. Hence as β runs through the k-zero subsequences of σ, the sum of the respective $N(p - k, \overline{\beta})$ counts each (k, p)-tower in σ exactly once. Analogous conclusions hold for $2p - k$ and $3p - k$, therefore our second summation yields

$$T(k, p, \sigma) - T(k, 2p, \sigma) + T(k, 3p, \sigma) \equiv 0 \quad \text{for each } k = 1, \ldots, \ell - 1. \tag{3}$$

The desired relation in the theorem statement follows from (1) and (2) for $\ell = 1$ and from (1)–(3) for $2 \leqslant \ell \leqslant p$. □

The most important special case of Theorem 5 is naturally $\ell = p$.

Theorem 6. *Let p be an odd prime. Each sequence σ of length $4p - 3$ in $\mathbb{Z}_p^2$ satisfies the relation*

$$\sum_{k=0}^{p-1} (-1)^k [T(k, p, \sigma) + T(k, 3p, \sigma)] - \frac{1}{2} T(p, 2p, \sigma) \equiv 1. \tag{4}$$

3. Corollaries

We first derive conclusions from Theorem 6, about the p-zero sums in a sequence of length $4p-3$ in $\mathbb{Z}_p^2$.

Corollary 7. *Let p be an odd prime. Each sequence σ of length $4p-3$ in $\mathbb{Z}_p^2$ satisfies at least one of the following conditions*:

(i) *σ contains two disjoint nonempty zero subsequences whose lengths add up to p.*
(ii) *σ contains two disjoint zero subsequences of length p.*
(iii) *σ contains two disjoint zero subsequences, one of length p and one of length $2p$.*
(iv) $N(p,\sigma)\equiv 1$.

Proof. By Theorem 6, σ satisfies (4). Clearly at least one of the tower-type quantities on the left-hand side must be nonzero modulo p. If $T(k,\ p,\sigma)\not\equiv 0$ for some $k\in\{1,2,\dots,p-1\}$, then (i) is true. If $T(p,2p,\sigma)\not\equiv 0$, then (ii) is true. If $T(k,3p,\sigma)\not\equiv 0$ for some $\{k\in\{0,1,\dots,p-1\}\}$, then σ has a $3p$-zero subsum τ. By Proposition 3, τ contains a p-zero sum, which implies (iii). If all quantities mentioned so far are zero modulo p, then $T(0,\ p,\sigma)\equiv 1$, hence (iv) is true. □

It is important to note that each of the alternatives (i)–(iv) can actually occur without the other three. For every condition among (i)–(iv), there is a sequence of length $4p-3$ in $\mathbb{Z}_p^2$ which satisfies this condition but fails the remaining three. Not all of these examples are evident, yet we do not include them here.

A look at the alternatives (i)–(iv) shows that our preliminary expectations about short zero sums were a bit too high. Sequences of length $4p-3$ in $\mathbb{Z}_p^2$ prove to be rather diverse with respect to their p-zero sums. However, Corollary 7 contains a description of this diversity, with one alternative the class of sequences where short zero sums do guarantee a p-zero sum. In particular, Kemnitz' conjecture follows directly, since each alternative among (i)–(iv) implies the existence of a p-zero subsequence.

Corollary 8 (*Reiher–di Fiore*). *Let p be a prime number. Each sequence of length $4p-3$ in $\mathbb{Z}_p^2$ has a subsequence of length p and sum zero.*

A comparison with length $4p-2$ is in order here. Rónyai's result in [5] essentially states that each sequence σ of length $4p-2$ in $\mathbb{Z}_p^2$ (for p odd) satisfies $N(p,\sigma)-N(3p,\sigma)\equiv 2$. Hence at least one of $N(p,\sigma)$ and $N(3p,\sigma)$ is nonzero modulo p, so σ must have a p-zero sum by Proposition 3. The picture is considerably more complicated for length $4p-3$, as Corollary 7 suggests. No linear congruence involving only $N(p,\sigma)$ and $N(3p,\sigma)$ seems to be available. The existence of a p-zero sum is due to a whole range of reasons, mostly of structural nature.

In view of Theorem 5, Corollary 7 generalizes to all lengths between $3p-2$ and $4p-3$.

Corollary 9. *Let p be an odd prime and* $\ell \in \{1, 2, \ldots, p\}$. *Each sequence* σ *of length* $3p - 3 + \ell$ *in* $\mathbb{Z}_p^2$ *satisfies at least one of the following conditions*:

(i) *For some* $k \in \{1, \ldots, \ell - 1\}$, σ *has a pair of disjoint zero subsequences, one of length k and one of length* $p - k$.
(ii) *For some* $k \in \{\ell, \ldots, p\}$, σ *has a pair of disjoint zero subsequences, one of length k and one of length* $2p - k$.
(iii) σ *contains two disjoint zero subsequences, one of length p and one of length* $2p$.
(iv) $N(p, \sigma) \equiv 1$.

The proof is completely analogous to the one of Corollary 7.

Of course, a sequence in $\mathbb{Z}_p^2$ of length less than $4p - 3$ may not have *p*-zero sums. However, by Corollary 9 this can be the case only if condition (ii) holds true, with $k \neq p$, while the other three conditions fail. Thus we obtain a variant of Kemnitz' conjecture for each length between $3p - 2$ and $4p - 3$.

Corollary 10. *Let p be an odd prime and* $\ell \in \{1, 2, \ldots, p\}$. *At least one of the following holds for each sequence* σ *of length* $3p - 3 + \ell$ *in* $\mathbb{Z}_p^2$:

(i) σ *has a zero subsequence of length p*.
(ii) *For some* $k \in \{\ell, \ldots, p - 1\}$, σ *has a pair of disjoint zero subsequences, one of length k and one of length* $2p - k$.

The larger the ℓ in Corollary 10, the more interesting the conclusion. We state separately the case $\ell = p - 1$ corresponding to the critical length $4p - 4$.

Corollary 11. *Let p be an odd prime. Each sequence of length* $4p - 4$ *in* $\mathbb{Z}_p^2$ *either contains a zero subsequence of length p or a pair of disjoint zero subsequences, one of length* $p - 1$ *and one of length* $p + 1$.

In conclusion, we do not find a way to deduce Corollaries 7 and 9–11 from the theorem of Reiher and di Fiore, nor to obtain them directly (without Theorem 5) by other means known to us.

References

[1] N. Alon, M. Dubiner, Zero-sum sets of prescribed size, Combinatorics, Paul Erdős is Eighty, János Bolyai Mathematical Society, Budapest, 1993, pp. 33–50.
[2] C. di Fiore, October 2003, personal communication.
[3] A. Kemnitz, On a lattice point problem, Ars Combin. 16b (1983) 151–160.
[4] C. Reiher, On Kemnitz' conjecture concerning lattice-points in the plane, preprint.
[5] L. Rónyai, On a conjecture of Kemnitz, Combinatorica 20 (4) (2000) 569–573.