ACTA ARITHMETICA
143.1 (2010)

The structure of maximal zero-sum free sequences

by

Gautami Bhowmik (Lille), Immanuel Halupczok (Münster) and
Jan-Christoph Schlage-Puchta (Gent)

1. Introduction and results. This paper is a continuation of our investigation of zero-sum (free) sequences of finite abelian groups (see [5] or [3]). As is the tradition, we let G be a finite abelian group, $A \subseteq G$ a multiset and we say that A is zero-sum free if there exists no non-empty subset $B \subseteq A$ such that $\sum_{b\in B} b = 0$. Obviously, in a fixed group G a zero-sum free subset cannot be arbitrarily large. The least integer n such that there does not exist a zero-sum free set with n elements is usually called the *Davenport constant* of G, for which we write $D(G)$. For an overview of this and related problems as well as applications see [13].

Here we consider groups of the form $\mathbb{Z}_n^2$, where $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. It is known since long that $D(\mathbb{Z}_n^2) = 2n-1$ (see, for example, [2] or [16]). Knowing the precise structure of all counterexamples, i.e. zero-sum free sets of $2n-2$ elements, would simplify some inductive arguments for groups of rank ≥ 3, where the Davenport constant is unknown. Up to an automorphism of the group all known examples of zero-sum free sets of maximal size are one of the following: either $(1,0)$ occurs with multiplicity $n-1$, and all other points are of the form $(a_i, 1)$, or $(1,0)$ occurs with multiplicity $n-2$, all other points are of the form $(a_i, 1)$, and we have $\sum_{i=1}^{n} a_i = 1$. We are thus motivated to study the following property introduced by Gao and Geroldinger [9].

Let n be an integer. Then n is said to satisfy *property B*, or $B(n)$ holds true, if in every maximal zero-sum free subset of $\mathbb{Z}_n^2$ some element occurs with multiplicity at least $n-2$. It is easy to see that this definition is equivalent to the statement that every zero-sum free set of $2n-2$ elements is of one of the two forms cited above.

Gao and Geroldinger [9] proved that $B(n)$ holds true for $n \leq 7$, and that for $n \geq 6$, $B(n)$ implies $B(2n)$. Recently, Gao, Geroldinger and Grynkiewicz [11] showed that property B is almost multiplicative, that is, if $B(n)$ and

2010 *Mathematics Subject Classification*: Primary 11B13; Secondary 11B50, 05D05.
Key words and phrases: zero-sum problems, Davenport's constant, property B.

DOI: 10.4064/aa143-1-2

$B(m)$ hold true, then so does $B(nm)$, provided that mn is odd and greater than 9. Hence, combining the results of [9] and [11] it suffices to prove $B(n)$ when n is prime and when $n \in \{8, 9, 10\}$.

From now on, p will always be a prime number. If one tries to prove $B(p)$ by sheer force, the most difficult cases are those which are close to the known maximal zero-sums, that is, some point a has multiplicity only slightly less than $p-2$, and all other points occur in one coset of the subgroup generated by a. Further the method of exponential sums runs into serious problems with situations in which a few points occur with high multiplicity. Therefore, it appears worthwhile to deal with the case of high multiplicities in a uniform way. The aim of this article is to initiate a systematic approach to property B via the highest occurring multiplicities.

In one direction we have the following.

THEOREM 1. *Let $A \subseteq \mathbb{Z}_p^2$ be a set of cardinality $2p-2$, and let $m_1 \geq m_2 \geq m_3$ be the largest occurring multiplicities. Suppose that $m_1 \leq p-3$, and that one of the following statements is true:*

(1) $m_1 = p-3$,
(2) $p > N$ *and* $p - m_1 < cp$, *where* $N, c > 0$ *are two constants not depending on* p,
(3) $m_2 \geq 2p/3$,
(4) $m_1 + m_2 + m_3 \geq 2p-5$.

Then A contains a zero-sum.

Lettl and Schmid [14] proved the existence of a zero-sum under the fourth condition with $2p-5$ replaced by $2p-2$. Our proof of the fourth statement does not involve any new ideas. However, using the first and third conditions we immediately obtain a good lower bound for m_3 which greatly simplifies our arguments. With more effort one can replace $2p-5$ by some other function of the form $2p-c$, however, we do not feel that the amount of work necessary to do so would be justified. The fourth statement appears to be rather technical; the reason that we still believe it to be of some interest is that when one tries to tackle larger groups by an inductive argument along the lines of [5], one is automatically led to situations where $m_1 + m_2 + m_3$ is close to $2p-2$.

In the opposite direction we combine exponential sums with combinatorial methods to prove the following.

THEOREM 2. *There is a positive constant δ such that each set $A \subseteq \mathbb{Z}_p^2$ with $|A| = 2p-2$, $m_1 \leq p-3$, and $m_2 < \delta p$ contains a zero-sum.*

Gao, Geroldinger and Schmid [12, Theorem 4.1] had already shown the existence of a zero-sum under the assumption $m_1 < p^{1/4-\epsilon}$.

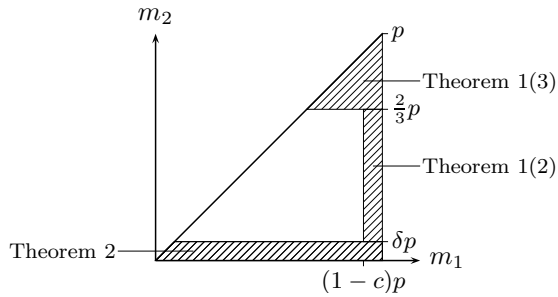


Fig. 1. Property B is proven if p is sufficiently large and (m_1, m_2) lies in the hatched area; c and δ are two constants not depending on p.

We did not try to obtain a good numerical bound for δ, a rather careless estimate shows that $\delta = 4 \cdot 10^{-7}$ is admissible, which is certainly far from optimal. However, any value of δ less than 0.1 would be of little help concerning the computational confirmation of property B, nor do we expect much structural information for maximal zero-sum free sets from such a small value, therefore we did not try to optimize our estimate.

For several of our results, the proof gets more and more complicated as p becomes small. Thus, to simplify the manual parts of the proof, we verified as many cases as possible by brute force using a computer. We also tried how far we could get proving property B completely by computer. In particular, we also considered the missing non-prime cases 8, 9 and 10. The following theorem summarizes the results obtained this way.

THEOREM 3. *Let $A \subseteq \mathbb{Z}_p^2$ be a set, and let $m_1 \geq m_2 \geq m_3$ be the largest occurring multiplicities. Suppose that $m_1 \leq p-3$, and that one of the following statements is true:*

(1) $p \leq 23$,
(2) $p \leq 37$ *and* $m_1 + m_2 + m_3 \geq 2p - 5$.

Then A contains a zero-sum. Moreover, property B holds true for 8, 9, *and* 10.

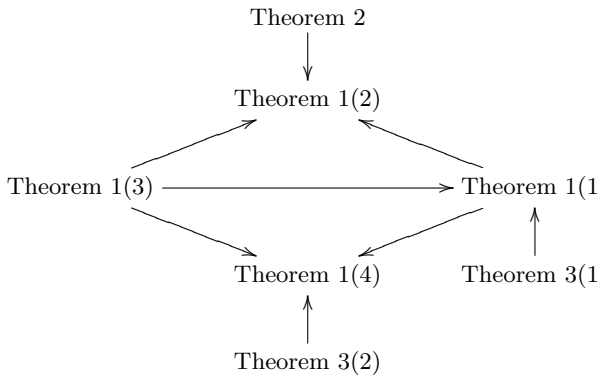
Part (2) does not have any merit in itself, but is used in the proof of Theorem 1.

In view of the multiplicativity results of [9] and [11], Theorem 3 yields:

COROLLARY 4. *Any $n \leq 28$ has property B.*

The remainder of this article is organized as follows. In the next section, we list some general lemmas which we will need later. In Sections 3 to 6, we prove the different statements of Theorems 1 and 2, approximately in the order in which they rely upon each other. Finally, in Section 7 we describe the algorithm used for Theorem 3.

The following diagram describes the dependencies; $A \to B$ means that A is used in the proof of B.



Note that apart from Theorem 3, there is a second place where computer results are used: Lemma 9 below has been proven using a computer, and this lemma is used in the proof of Theorem 1(1). However, for p sufficiently large it can be replaced by Lemma 8, so for sufficiently large p, our results do not depend on computer calculations.

2. Auxiliary results. $\mathbb{Z}_p$ is not an ordered group; however, for our purpose it is useful to view elements such as 5 and 6 as being close together, and elements such as 2 as being small. Of course, this notion does not make sense from a group-theoretic point of view, since $\mathrm{Aut}(\mathbb{Z}_p)$ acts transitively on $\mathbb{Z}_p \setminus \{0\}$. However, after fixing the generator 1, it makes sense to talk about the distance and the size of elements in $\mathbb{Z}_p$. To be precise, we define two functions $\mathbb{Z}_p \to \mathbb{Z}$ as follows. For an element $a \in \mathbb{Z}_p$ denote by $|a| = \min\{|a'| : a' \in \mathbb{Z},\ a' \bmod p = a\}$ the modulus of the least absolute remainder of a, and by $\imath(a) = \min\{a' \geq 0 : a' \bmod p = a\}$ the least positive remainder of a. When we compare elements of $\mathbb{Z}_p$, then we implicitly apply $\imath$ before. For example, for elements $a, b \in \mathbb{Z}_p$, we write $a < b$ to mean $\imath(a) < \imath(b)$ and $a \in [x, 2x]$ to mean $\imath(a) \in [x, 2x]$. However, at some places it is important to distinguish between $\sum_{a\in A} \imath(a)$ and $\imath(\sum_{a\in A} a)$.

For a multiset A we denote by $\Sigma(A)$ the *set* (not multiset) of all subset sums of A, for example, $\Sigma(\{1,1\}) = \{0,1,2\}$, and $\Sigma_k(A)$ is the *set* of all subset sums of A of length k, for example, $\Sigma_2(\{1,1,2\}) = \{2,3\}$.

We will write π_1 and π_2 for the projection from $\mathbb{Z}_p^2$ to the first and second coordinate, respectively.

Lemma 5.

(1) *Let $A \subseteq \mathbb{Z}_p$ be a multiset of size k without zero-sums. Then there are at least k distinct elements representable as non-empty subset sums*

of A, and equality holds true if and only if all elements in A are equal.

(2) *Let $A \subseteq \mathbb{Z}_p$ be a multiset of size $p+k$ with $0 \le k \le p-2$ without zero-sums of length p. There are at least $k+1$ distinct sums of p elements in A, and equality holds if and only if $|A| = p$ or A contains only two distinct elements.*

Proof. (1) We prove our claim by induction on k. For $k = 1$ and $k = 2$ the statement is obvious; similarly, if all elements of A are equal. Now suppose that A contains at least two distinct elements, and let $A = \{x_1, \dots, x_k\}$ with $x_1 \neq x_2$. The induction hypothesis implies that the set Σ of elements representable as non-empty subset sums of $x_1, \dots, x_{k-1}$ contains at least k elements, thus, we only have to show that $(\Sigma \cup \{0\}) + \{0, x_k\} \neq \Sigma \cup \{0\}$. Suppose otherwise. Then $x_k \in \Sigma$, thus, the subgroup $\langle x_k \rangle$ generated by x_k is contained in $\Sigma \cup \{0\}$; in particular, $-x_k \in \Sigma$. However, this contradicts the assumption that A does not contain a non-empty zero-sum subset.

(2) This is a result of Bollobás and Leader [6]. ∎

The following is probably the first non-trivial result proved on sumsets in finite abelian groups.

LEMMA 6 (Cauchy–Davenport). *Let $A, B \subseteq \mathbb{Z}_p$ be sets containing no element twice. Then $|A+B| \ge \min(|A|+|B|-1, p)$, where $A+B$ is interpreted as a set (not a multiset).*

We shall repeatedly use this theorem in the following way.

COROLLARY 7. *Let $A_1, \dots, A_k$ be subsets of $\mathbb{Z}_p$, and suppose that $\sum_{i=1}^{k} (|\Sigma(A_i)| - 1) \ge p - 1$. Then $\Sigma(\bigcup A_i) = \mathbb{Z}_p$.*

Proof. We have

$$\Big|\Sigma\Big(\bigcup A_i\Big)\Big| = |\Sigma(A_1) + \dots + \Sigma(A_k)| \ge \min\Big(1 + \sum_{i=1}^{k} (|\Sigma(A_i)| - 1), p\Big) = p. \ \blacksquare$$

The following result was proven by Olson [15, Theorem 2].

LEMMA 8. *Let $A \subseteq \mathbb{Z}_p$ be a set with all elements distinct and $|A| = s$. Suppose that for all $a \in A$, $-a \notin A$; in particular, $0 \notin A$. Then*

$$|\Sigma(A)| \ge \min\left(\frac{p+3}{2}, \frac{s(s+1)}{2} + \delta\right),$$

where

$$\delta = \begin{cases} 1, & s \equiv 0 \pmod 2, \\ 0, & s \equiv 1 \pmod 2. \end{cases}$$

As shown by $A = \{1, \dots, k\}$, for large p this estimate is optimal up to the value of δ for odd k. For small p however, the estimate is far from

optimal due to the term $(p+3)/2$; this deficiency causes some trouble in our treatment of small primes, which motivated us to prove the following using computer calculations [4].

LEMMA 9. *Let $A \subseteq \mathbb{Z}_p$ be a set with all elements distinct and $|A| = s \le 7$. Suppose that A is zero-sum free. Then $|\Sigma(A)| \ge s(s+1)/2+1$.*

The following is a simple consequence of the lemma of Olson.

LEMMA 10. *Let $A \subseteq \mathbb{Z}_p$ be a set consisting of $n+1$ different elements, or a set consisting of n different elements and not containing 0. Then $|\Sigma(A)| \ge \min(p, n(n+2)/4-1)$.*

Proof. If A contains 0, then remove that element. Now partition A into two sets B and B', with $\lfloor n/2 \rfloor$ and $\lceil n/2 \rceil$ elements respectively, which both satisfy the prerequisites of Lemma 8. Using it and Cauchy–Davenport, we get

$$\Sigma(A) \ge \begin{cases} \min\left(p, \dfrac{n}{2}\left(\dfrac{n}{2}+1\right)-1\right) & \text{if } n \text{ is even,} \\ \min\left(p, \dfrac{(n-1)(n+1)}{8} + \dfrac{(n+1)(n+3)}{8} + 1 - 1\right) & \text{if } n \text{ is odd.} \end{cases}$$

Both cases imply the claim. ∎

The following is due to Dias da Silva and Hamidoune [7].

LEMMA 11. *Let $A \subseteq \mathbb{Z}_p$ be a set, k an integer in the range $1 \le k \le |A|$. Then*

$$|\Sigma_k(A)| \ge \min(p, k(|A|-k)+1).$$

Moreover, if $|A| \ge \ell := \lfloor \sqrt{4p-7} \rfloor + 1$ and $k = \lfloor \ell/2 \rfloor$, then $\Sigma_k(A) = \mathbb{Z}_p$.

The next result is a special case of a theorem due to Gao and Geroldinger [10].

LEMMA 12. *Let $A \subseteq \mathbb{Z}_p^2$ be a zero-sum free subset with $2p-2$ elements. If $x, y \in A$, then they are either the same element of $\mathbb{Z}_p^2$, or linearly independent.*

The following lemma says that to check that a set A satisfies property B, it is sufficient to check that all its elements lie in a subgroup and one coset of that subgroup.

LEMMA 13. *Let $A \subseteq \mathbb{Z}_p^2$ with $|A| = 2p-2$ be a zero-sum free subset such that there exists a subgroup $H < \mathbb{Z}_p^2$, $H \cong \mathbb{Z}_p$, and an element $a \in \mathbb{Z}_p^2$ such that $A \subseteq H \cup a+H$. Then A contains an element with multiplicity $\ge p-2$.*

Proof. Suppose that no element occurs $p-2$ times in A. Set $s = |A \cap H|$, $t = |A \cap (a+H)|$. If $s \ge p$, then $H \cap A$ contains a zero-sum, hence we have $s \le p-1$ and therefore $t = p+k$ with $k \ge -1$. Using Lemma 5, we find that there are at least $k+1$ distinct elements in H representable as sums of

elements from $A \cap (a+H)$, none of which is zero, and there are at least s non-zero elements representable by elements in $A \cap H$. Since $(k+1)+s = p-1$, we find that either there is some element $b \in H$ which is representable by elements in $A \cap (a+H)$, such that $-b$ is representable by elements in $A \cap H$, which would yield a zero-sum, or we have equality in both estimates, that is, all elements in $A \cap H$ are equal, and either $k \le 0$ or there are only two distinct elements in $A \cap (a+H)$. If $k \le 0$, then $s \ge p-2$ and $B(p)$ holds. Otherwise, up to linear equivalence, A is of the form $\{(1,0)^\ell, (0,1)^m, (x,1)^n\}$ with $1 \le x \le p/2$.

If $x = 1$, we have the zero-sum $n \cdot (1,1) + (p-n) \cdot (1,0) + (p-n) \cdot (0,1)$, since

$$\min(\ell, m) = \ell + m - \max(\ell, m) \ge \ell + m - (p-3) = (2p-2-n) - (p-3) > p-n.$$

Otherwise consider the set $U = \{(-s, 0) : 1 \le s \le \ell\}$ of inverses of elements representable as non-zero subsums of $A \cap H$, and the set $V = \{(\nu x, 0) : p - m \le \nu \le n\}$ of elements in H representable by elements in $A \cap (a+H)$. Since A is zero-sum free, we have $0 \notin V$, and U and V are disjoint. Since $|U| + |V| = p-1$, this implies that $V = H \setminus (\{0\} \cup U)$; in particular, there exists only one $r \in \mathbb{Z}_p$ such that $r \notin [p-\ell, p]$ but $r + x \in [p-\ell, p]$. However, we can easily find two such elements and thus get a contradiction. If $x \le \ell$, take $-\ell - 1$ and $-\ell - 2$; this works as $x \ne 1$ and $\ell \le p-3$. If $x > \ell$, take $-x$ and $-x-1$; this works as $x \ne -1$ and $\ell \ne 0$. Hence our statement is proven. ∎

The following is a variant of a result of Gao and Geroldinger [8].

LEMMA 14. *Let $S \subseteq \mathbb{Z}_p$ be a subset with $|S| \ge p/4W$, where $W \ge 1$ is an integer and $p \ge 64W^2$. If every element in S has multiplicity $\le p/40W^2$, then S contains a zero-sum.*

Proof. Suppose that S is zero-sum free, and let m be the maximal multiplicity of elements of S. Let us first treat the case $m = 1$. Then Lemma 10 implies $p - 1 \ge |\Sigma(S)| \ge |S| \cdot (|S|+2)/4 - 1$, which yields

$$4p \ge |S| \cdot (|S|+2) > |S|^2 \ge \frac{p^2}{16W^2},$$

which contradicts $p \ge 64W^2$.

Now suppose $m \ge 2$. Choose disjoint subsets $S_1, \dots, S_m$ of S, each one consisting of $\lfloor |S|/m \rfloor$ different elements. The zero-sum freeness of S implies $\sum_i (|\Sigma(S_i)| - 1) + 1 \le |\Sigma(S)| < p$, hence there exists an i such that $|\Sigma(S_i)| < (p-1)/m + 1 < p/m + 1$. Now Lemma 8 implies $|S_i|(|S_i|+1)/2 < p/m+1$ (as $(p+3)/2 > p/m+1$). Using $|S_i| \ge |S|/m - 1 \ge p/4Wm - 1 \ge 10W - 1 \ge 9W$, we get

$$\frac{p}{m} + 1 > \frac{9W \cdot \frac{p}{4Wm}}{2} = \frac{9p}{8m},$$

which, using $m \le p/40$, yields a contradiction. ∎

LEMMA 15. *Suppose that $A \subset \mathbb{Z}_p$ satisfies $A + [0,m] = \mathbb{Z}_p$. Then there is a subset $A' \subset A$ of cardinality $|A'| \le 2\lceil (p+1)/(m+2)\rceil - 1$ satisfying $A' + [0,m] = \mathbb{Z}_p$.*

Proof. We can assume that $0 \in A$. Then define a sequence $a_i \in \mathbb{N}$ as follows: Set $a_1 = 0$, and choose $a_{i+1} \in a_i + \{1,\dots,m+1\}$ maximal such that $a_{i+1} \bmod p \in A$ (which is possible by assumption). For any i we have $a_{i+2} - a_i \ge m+2$, as otherwise $a_{i+1} - a_i$ would not be maximal, so $a_{2k-1} \ge (m+2)(k-1)$ for $k \ge 1$. We set $k = \lceil \frac{p+1}{m+2} \rceil$ and $A' = \{a_1,\dots,a_{2k-1}\}$. Then $A' + [0,m] = \mathbb{Z}_p$, as

$$a_{2k-1} + m \ge (m+2)\left(\left\lceil \frac{p+1}{m+2} \right\rceil - 1\right) + m \ge p - 1. \ \blacksquare$$

The previous lemma can be applied to give the following, which proves to be useful if we have many different elements in A.

LEMMA 16. *Let $A \subset \mathbb{Z}_p^2$ be a subset. Suppose that $B := \{(1,0)^{m_1}, (0,1)^{m_2}\} \subset A$. Suppose moreover that we can partition $A \setminus B$ into two sets U, V such that*

$$\Sigma(\pi_2(U) \cup \{1^{m_2}\}) = \mathbb{Z}_p, \qquad |\Sigma(\pi_1(V))| > \left(2\left\lceil \frac{p+1}{m_2+2} \right\rceil - 1\right)(p - m_1 - 1).$$

Then A contains a zero-sum.

Proof. Applying Lemma 15 to $\Sigma(\pi_2(U))$ (with $m = m_2$) yields a set $W \subset \Sigma(\pi_2(U))$ with $W + \Sigma(\{(0,1)^{m_2}\}) = \mathbb{Z}_p$ and $|W| \le 2\lceil \frac{p+1}{m_2+2} \rceil - 1$. Then for each element $s \in \Sigma(V)$ there is some element $w \in W$ such that $\pi_2(s+w) \in [p-m_2, p]$. Hence, either we obtain a zero-sum, or $\pi_1(s+w) \in [1, p-m_1-1]$. If this holds true for all $s \in \Sigma(V)$, then $\pi_1(\Sigma(V)) \subseteq [1, p-m_1-1] - \pi_1(W)$. However, the right hand set contains at most $\big(2\lceil \frac{p+1}{m_2+2} \rceil - 1\big)(p - m_1 - 1)$ elements, hence our claim follows. $\blacksquare$

3. The two largest multiplicities of a zero-sum free set in $\mathbb{Z}_p^2$. In this section, we prove Theorem 1(3).

Let m_1, m_2 be the two largest multiplicities, and set $k_i = p - m_i$. We do not assume $m_1 \ge m_2$ in this section, in this way we obtain more symmetry.

We will repeatedly use the following argument, which for the sake of future citation is formulated as a lemma.

LEMMA 17. *Let A be a zero-sum free set, $E \subset A$, and suppose that $\sum_{e \in E} e = k \cdot a$ for some $a \in \mathbb{Z}_p^2$ and some $k \in \mathbb{N}$.*

(1) *If $\{a^{k-1}\} \subseteq A \setminus E$, then $A \cup \{a^k\} \setminus E$ is zero-sum free.*
(2) *If $|A| = 2p-2$ and $\{a^{\min(k-1, \lceil p/2 \rceil - 1)}\} \subseteq A \setminus E$, then $|E| \ge k$.*

Proof. (1) Write $A = A_1 \cup E \cup \{a^{k-1}\}$ and suppose that $A \cup \{a^k\} \setminus E = A_1 \cup \{a^{2k-1}\}$ contains a zero-sum $B_1 \cup \{a^\ell\}$ with $B_1 \subset A_1$ and $\ell \le 2k-1$. If

$\ell \le k-1$, then this is already a zero-sum of A. Otherwise, $B_1 \cup \{a^{\ell-k}\} \cup E$ is a zero-sum of A.

(2) If $\{a^{k-1}\} \subseteq A \setminus E$ this follows from the first part. Otherwise $k-1 > \lceil p/2 \rceil - 1$ and $\{a^{\lceil p/2 \rceil - 1}\} \subseteq A \setminus E$. But then $E \cup \{a^{p-k}\}$, which has sum zero, is a subset of A:

$$p - k \le p - \lceil p/2 \rceil - 1 \le \lceil p/2 \rceil - 1. \ \blacksquare$$

We now fix coordinates in such a way that $(1,0)$ occurs with multiplicity m_1, and $(0,1)$ with multiplicity m_2 in A. Note that in particular, by Lemma 12, A does not contain any element $(k,0)$ or $(0,k)$ for $k \ne 1$.

LEMMA 18. *Suppose that $B = \{a_1, \dots, a_k, b_1, \dots, b_l\} \subset A \setminus \{(1,0)^{m_1}\}$ for some $k, l \ge 1$, with $y = \pi_2(\sum_i a_i) = \pi_2(\sum_i b_i)$. If $-y \in \Sigma(\pi_2(A \setminus B))$, then $|\sum_i \pi_1(a_i) - \sum_i \pi_1(b_i)| \le p - m_1 - 2$. In particular, this is true if $k + l \le p - m_1 - 1$. The same is true with coordinates exchanged.*

Proof. Let c be a sum of elements of $A \setminus (B \cup \{(1,0)^{m_1}\})$ with $\pi_2(c) = -y$. Then $c + \sum_i a_i$ and $c + \sum_i b_i$ both are of the form $(x, 0)$. Such elements can be completed to a zero-sum by copies of $(1,0)$ unless $0 < x < p - m_1$. The statement follows.

If $k + l \le p - m_1 - 1$, then $|A \setminus (B \cup \{(1,0)^{m_1}\})| \ge p - 1$, so $\Sigma(\pi_2(A \setminus B))$ contains the whole of $\langle (0,1) \rangle$. $\blacksquare$

Our argument will have a recursive structure. For $k_1, k_2 \ge 3$ denote by $B(p, k_1, k_2)$ the statement that there does not exist a zero-sum free set $A \subseteq \mathbb{Z}_p^2$ with $|A| = 2p - 2$ and maximal multiplicities $p - k_1$, $p - k_2$. Note that this statement is false if one of k_1, k_2 equals 1 or 2, while it is trivially true if one of k_1, k_2 is ≤ 0. When proving $B(p, k_1, k_2)$ for some pair (k_1, k_2), we may assume that this statement is already proven for all pairs (k_1', k_2') with $k_1 + k_2 > k_1' + k_2'$, such that none of k_1', k_2' equals 1 or 2.

LEMMA 19. *Let $A \subseteq \mathbb{Z}_p^2$ be a zero-sum free set with $|A| = 2p - 2$, and suppose that A contains elements with multiplicities $p - k_1$, $p - k_2$, where $3 \le k_1, k_2 \le p/3$. Then all elements of A different from $(1,0)$ and $(0,1)$ are of the form (x, y) with $1 \le x \le k_1 - 2$, $1 \le y \le k_2 - 2$, of the form $(p - x, y)$ with $1 \le x \le k_1 - 2$, $1 \le y \le k_2 - 1$, or of the form $(x, p - y)$ with $1 \le x \le k_1 - 1$, $1 \le y \le k_2 - 2$.*

Proof. Suppose that $(x, y) \in A$ with $1 \le y < k_2$. Our aim is to show that $|x| \le k_1 - 2$. (Together with the same argument with coordinates exchanged, this implies the lemma.) We apply Lemma 18 to the sum $\pi_2(y \cdot (0,1)) = \pi_2((x, y))$, and deduce that

$$|x| = \left| \pi_1((x,y)) - \sum_{i=1}^{x} \pi_1((0,1)) \right| \le k_1 - 2,$$

provided that $-y \in \Sigma(\pi_2(A \setminus \{(0,1)^y, (x,y)\}))$. Hence, from now on we assume that this is not the case.

If there were an $a \in A$ with $k_2 \le \imath(\pi_2(a)) \le p-y$, then this element together with $(0,1)^{p-k_2-y}$ would represent $-y$, hence there is no element in this range. Denote by B the set of all $a \in A \setminus \{(1,0)^{p-k_1}, (0,1)^{p-k_2}, (x,y)\}$ with $\imath(\pi_2(a)) > p-y$, and by C the set of all $a \in A \setminus \{(1,0)^{p-k_1}, (0,1)^{p-k_2}, (x,y)\}$ with $\imath(\pi_2(a)) < k_2$. Then $-y$ is representable as subsum of $\pi_2(B)$ together with a certain multiple of $(0,1)$, if $\sum_{b\in B}(p - \imath(\pi_2(b))) \ge y$, and $-y$ is representable as subsum of $\pi_2(C)$ together with a certain multiple of $(0,1)$, if $\sum_{c\in C} \imath(\pi_2(c)) \ge k_2$; in particular $|B| \le y-1$ and $|C| \le k_2 - 1$.

We now form the sum s of all elements in B. Then we have $p - \imath(\pi_2(s)) = \sum_{b\in B}(p - \imath(\pi_2(b))) \le y-1 \le p/3$, hence if $\sum_{b\in B} \imath(\pi_1(b)) \ge k_1$, we can add a certain multiple of $(1,0)$ and $(0,1)$ to s and obtain a zero-sum. In particular, $|B| \le k_1 - 1$.

This implies $|C| \ge k_2 - 2$, as $|B| + |C| = k_1 + k_2 - 3$. Since $\sum_{c\in C} \imath(\pi_2(c)) \le k_2 - 1$, we deduce that C contains at most one element c_0 with $\pi_2(c_0) \ne 1$, and, if it exists, this element satisfies $\pi_2(c_0) = 2$.

Similarly, $|C| \le k_2 - 1$ implies $|B| \ge k_1 - 2 \ge 1$, and therefore B contains at most one element b_0 with $\pi_1(b_0) \ne 1$, and this element satisfies $\pi_1(b_0) = 2$.

In particular, B and C are both non-empty.

Suppose that $C = \{c_0\}$. Then $k_2 = 3$ and $|B| = k_1 - 1$, therefore $k_1 = |B| + 1 \le y \le k_2 - 1 = 2$, contrary to the assumption $k_1 \ge 3$. Hence there exists $c \in C$ with $\pi_2(c) = 1$. Choose any $b \in B$. Then $b + c$ can be combined with certain multiples of $(1,0)$ and $(0,1)$ to a zero-sum, unless $\pi_1(c) \in [1, k_1 - 2]$.

Consider again the sum s of all elements in B. This sum satisfies $\pi_1(s) \in \{k_1 - 2, k_1 - 1\}$, $\pi_2(s) \in [p - y + 1, p - |B|]$. Hence, adding c we obtain a zero-sum, unless $\pi_1(c) = 1$ and $\pi_1(s) = k_1 - 2$. In particular, $|B| = k_1 - 2$, $|C| = k_2 - 1$, and b_0, c_0 do not exist, that is, all elements in C are equal to $(1,1)$.

If $x \in [p - |C|, p]$, we add $p - x$ copies of $(1,1)$ to (x,y) to obtain $(0, p + y - x)$ as the sum of $p - x + 1$ elements. Hence, we can replace $p - x + 1$ elements of A by $p - x + y$ copies of $(0,1)$, which gives a zero-sum, unless $y = 1$, which is impossible, since $|B| \le y - 1$. If $x \notin [p - |C|, p]$, we add all copies of $(1,1)$ to (x,y) and obtain an element s with $\pi_1(s) \in [k_1 - 1 + |C|, p] \subseteq [k_1, p]$, $\pi_2(s) \in [y + k_2 - 1, p] \subseteq [k_2, p]$, hence, s can be combined with a certain number of copies of $(1,0)$ and $(0,1)$ to produce a zero-sum. ∎

Note that the three rectangles from Lemma 19 are disjoint. From now on we will denote the set of points in $A \setminus \{(1,0)^{m_1}, (0,1)^{m_2}\}$ of the form (x,y) by B, the set of points of the form $(p - x, y)$ by C, and the set of points of the form $(x, p - y)$ by D $(x < k_1, y < k_2)$.

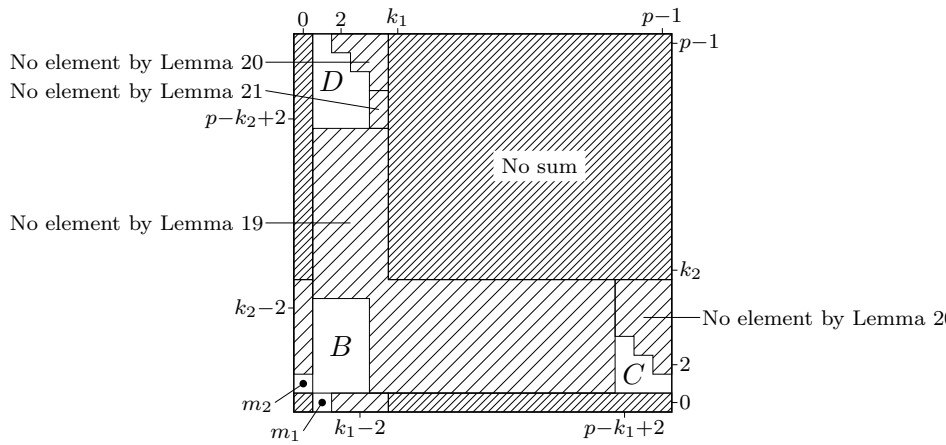


Fig. 2. What we know about $A \setminus \{(1,0)^{m_1}, (0,1)^{m_2}\}$

Our next result further restricts elements in C and D. At this place we use induction on k_1, k_2 for the first time.

LEMMA 20. *Let $A \subseteq \mathbb{Z}_p^2$ be a zero-sum free set with $|A| = 2p-2$, and suppose that $(1,0)$, $(0,1)$ are the elements with highest multiplicity $p-k_1$, $p-k_2$, respectively. Let $A \setminus \{(1,0)^{m_1}, (0,1)^{m_2}\} = B \cup C \cup D$ be the decomposition as above. Then C does not contain an element $(p-x, y)$ with $x < y$, and D does not contain an element $(x, p-y)$ with $y < x$.*

Proof. Suppose that $(p-x, y) \in C$ with $y > x$. Apply Lemma 17 to $E := \{(p-x, y), (1,0)^x\}$. We conclude that the set $A^* = A \setminus E \cup \{(0,1)^y\}$ is zero-sum free. If $y > x+1$, then $|A^*| > 2p-2$, which is impossible. If $y = x+1$, then A^* has cardinality $2p-2$ and maximal multiplicities $p-k_1-y+1$, $p-k_2+y$, hence, by our inductive hypothesis we obtain $p-k_2+y \in \{p-2, p-1\}$. Thus all elements a in A different from $(p-x, y)$ satisfy $\pi_1(a) \in \{0,1\}$. If B is non-empty, say, $b = (1,z) \in B$, we can apply Lemma 17 to $E := \{(p-y+1, y), (1,z), (1,0)^{y-2}\}$, and obtain a contradiction. Hence, $|D| \geq k_1 + k_2 - 3 \geq k_1$. The sum s of k_1 elements of D satisfies $\pi_1(s) = k_1$, hence either we obtain a zero-sum, or $\pi_2(s) \in [1, k_2-1]$. The latter is only possible if the average value of $p - \pi_2(d)$ taken over all elements $d \in D$ is larger than 2. Hence, we can choose a subset D' of D with sum s satisfying $\pi_1(s) \in [1, y/2]$, $\pi_2(s) \in [k_2, p-y]$. But then $s+(p-y+1, y)$ can be combined with some multiples of $(1,0)$ and $(0,1)$ to give a zero-sum. ∎

Now, we can remove the apparent asymmetry in Lemma 19.

LEMMA 21. *C does not contain an element c with $\pi_2(c) = k_2 - 1$, and D does not contain an element d with $\pi_1(d) = k_1 - 1$.*

Proof. By symmetry, it suffices to prove the statement for D.

Suppose that $d = (k_1 - 1, p - y) \in D$. By Lemmas 19 and 20 we have $k_1 - 1 \le y \le k_2 - 2$. Suppose that D contains another element $(x', p - y')$. Then we obtain the zero-sum $(x', p-y')+(k_1-1, p-y)+(p-x'-k_1+1)\cdot(1,0)+(y'+y)\cdot(0,1)$. Next, suppose that B contains an element (x', y'). If $y' \le y$, we obtain the zero-sum $(x', y')+(k_1-1, p-y)+(p-x'-k_1+1)(1,0)+(y-y')(0,1)$, thus all elements $b \in B$ satisfy $\pi_2(b) \ge y + 1 \ge k_1$.

Let s be the sum of all elements in B and C. If $s_2 := \sum_{e\in B\cup C} \imath(\pi_2(e)) \ge k_2 + y$, we can choose some subset sum s' satisfying $\pi_2(s') \in [k_2 + y, 2k_2 + y)$. Then $\pi_2(s'), \pi_2(s'+d) \in [k_2, 3k_2] \subseteq [k_2, p]$, hence either we get a zero-sum by adding a certain multiple of $(1, 0)$ and $(0, 1)$, or $\pi_1(s'), \pi_1(s'+d) \in [1, k_1-1]$. But this is impossible since $\pi_1(s' + d) = \pi_1(s') + k_1 - 1$. Hence, $s_2 < k_2 + y$.

Denote by C_1 the set of all $c \in C$ with $\pi_2(c) = 1$, and by C_2 the set of all c with $\pi_2(c) \ge 2$. Then

$$s_2 \ge (y + 1)|B| + |C| + |C_2| \ge y|B| + |C_2| + k_1 + k_2 - 3,$$

thus, for $|B| \ge 1$ we obtain the inequality $k_1 - 3 < 0$, which is false. Hence, $B = \emptyset$, and $|C_2| \le y + 3 - k_1$, thus,

$$|C_1| = k_1 + k_2 - 3 - |C_2| \ge 2k_1 + k_2 - y - 6 \ge k_1 - 1.$$

Choose a subset $C' \subseteq C_1$ with $\sum_{c\in C'} \imath(p - \pi_1(c)) \ge k_1 - 1$ and $|C'|$ minimal with this property, and let s be the sum of all elements of C'. Then $\pi_1(s+d) \in [p - k_1, p]$, and $\pi_2(s + d) \in [p - y + 1, p]$, hence $s + d$ can be combined with certain multiples of $(1, 0)$ and $(0, 1)$ to produce a zero-sum. ∎

LEMMA 22. *Suppose that B is empty. Then there is a zero-sum.*

Proof. Suppose both $\sum_{c\in C}(p - \imath(\pi_1(c))) \ge k_1 - 1$ and $\sum_{d\in D}(p - \imath(\pi_2(d))) \ge k_2 - 1$. Then we can choose a subset $C' \subset C$ such that the sum s_C of all elements in C' satisfies $\pi_1(s_C) \in [k_1, p - k_1 + 1]$. We may suppose $\pi_2(s_C) \le k_2 - 1$; otherwise we get a zero-sum. Analogously, we may choose a subset $D' \subset D$ whose sum s_D satisfies $\pi_1(s_D) \le k_1 - 1$, $\pi_2(s_D) \in [k_2, p - k_2 + 1]$. Hence, $s_C + s_D$ yields a zero-sum. So we may suppose that $\sum_{d\in D}(p - \imath(\pi_2(d))) \le k_2 - 2$. In particular, this implies $\sum_{d\in D} \imath(\pi_1(d)) \le k_1 - 1$ (otherwise we get a zero-sum), and therefore

$$|C| = k_1 + k_2 - 2 - |D| \ge k_1 + k_2 - 2 - \min(k_2 - 2, k_1 - 1) = \max(k_1, k_2 - 1).$$

There cannot be both an element $c \in C$ with $\pi_2(c) = 1$ and an element $d \in D$ with $\pi_1(d) = 1$; otherwise, we get a zero-sum using $c + d$ and some copies of $(1, 0)$ and $(0, 1)$. Thus $\sum_{c\in C} \imath(\pi_2(c)) \ge k_2$, since otherwise $|C| = k_2 - 1$, $|D| = k_1 - 1$, $\pi_2(c) = 1$ for all $c \in C$ and $\pi_1(d) = 1$ for all $d \in D$.

If there are two elements $c_1, c_2 \in C$ with $\pi_2(c_i) \ge k_2/2$, then we can combine $c_1 + c_2$ with a certain number of copies of $(1, 0)$ and $(0, 1)$ to give a zero-sum, as $\pi_1(c_1 + c_2) \ge p - 2(k_1 - 2) \ge k_1$. We now enumerate the elements in C as $c_1, \ldots, c_{|C|}$, where c_1 is the element satisfying $\pi_2(c_1) \ge$

$k_2/2$, if such an element exists. Set $s_i = \sum_{j=1}^{i} c_j$, and let i_0 be the largest index with $\pi_2(s_i) < k_2$. As $\sum_{c\in C} \imath(\pi_2(c)) \geq k_2$, we have $i_0 < |C|$. Now s_{i_0+1} can be combined with $(1,0)$ and $(0,1)$ to produce a zero-sum, unless $\pi_1(s_{i_0+1}) \in [1, k_1 - 1]$; moreover, we have $\pi_2(s_{i_0+1}) < 3k_2/2 - 1 < p/2 - 1$.

Suppose that $p - \imath(\pi_1(s_{i_0})) + \sum_{j=i_0+1}^{|C|}(p - \imath(\pi_1(c_j))) \geq p$, and let i_1 be the greatest index satisfying $p - \imath(\pi_1(s_{i_0})) + \sum_{j=i_0+1}^{i_1}(p - \imath(\pi_1(c_j))) < p$. Then s_{i_1+1} together with a certain number of copies of $(1,0)$ and $(0,1)$ yields a zero-sum, unless $\sum_{j=1}^{i_1+1} \imath(\pi_2(c_j)) > p$. But then we would have

$$\sum_{j=i_0+2}^{i_1} \imath(\pi_2(c_j)) > p - \imath(\pi_2(s_{i_0+1})) - \pi_2(c_{i_1+1}) > \frac{p}{2} - \frac{k_2}{2}$$
$$> \frac{p}{3} > k_1 - 1 > \sum_{j=i_0+2}^{i_1} (p - \imath(\pi_1(c_j))),$$

which is impossible, since by Lemma 20 we have $p - \imath(\pi_1(c)) \geq \imath(\pi_2(c))$ for all $c \in C$. Hence, $p - \imath(\pi_1(s_{i_0})) + \sum_{j=i_0+1}^{|C|}(p - \imath(\pi_1(c_j))) < p$.

Now suppose first that all elements of C satisfy $\pi_2(c) \geq 2$. Then for any set $C' \subseteq C$ with $|C'| \geq k_2/2$ we have $\sum_{c\in C'} \imath(\pi_2(c)) \geq k_2$; thus either we obtain a zero-sum, or for each such sum we have $\sum_{c\in C'}(p - \imath(\pi_1(c))) > p - k_1$. So, for every set $C'' \subseteq C$ with $|C''| \leq |C| - k_2/2$ we have $\sum_{c\in C''}(p - \imath(\pi_1(c)))$ $\leq k_1 - 2$.

As $|C| \geq k_1$, we may take for C'' the $k_1 - \lceil k_2/2 \rceil$ elements of C with maximal $p - \imath(\pi_1(c))$. In this way we deduce that C contains at most $k_2/4 - 1$ elements with $p - \imath(\pi_1(c)) \geq 3$. Thus (this time using $|C| \geq k_2 - 1$) there are at least $3k_2/4$ elements with $p - \imath(\pi_1(c)) \leq 2$. Now take a minimal subset of these elements such that the sum s satisfies $\pi_2(s) \geq k_2$; this exists as $\pi_2(c) \geq 2$ for all $c \in C$. Then $\pi_1(s) \geq p - k_2$, and s can be combined with copies of $(1,0)$ and $(0,1)$ to yield a zero-sum.

It remains to treat the case where C does contain an element c with $\pi_2(c) = 1$. In that case, D does not contain any element d with $\pi_1(d) = 1$, for otherwise, $c + d$ and some copies of $(1,0)$ and $(0,1)$ would yield a zero-sum. As $\sum_{d\in D} \imath(\pi_1(d)) \leq k_1 - 1$, we get $|D| \leq (k_1 - 1)/2$, so $|C| \geq k_2 + k_1/2 - 3/2$.

Now the same argument as in the previous case works; we only have to exchange some values. We need $|C'| \geq k_2$ to infer $\sum_{c\in C'} \imath(\pi_2(c)) \geq k_2$, hence we get the condition on the sum of C'' provided that $|C''| \leq |C| - k_2$. We get at most $k_1/4 - 1/4$ elements with $p - \imath(\pi_1(c)) \geq 3$ and thus at least $k_2 + k_1/4 - 5/4$ elements with $p - \imath(\pi_1(c)) \leq 2$. Again we take a minimal subset of these elements such that the sum s satisfies $\pi_2(s) \geq k_2$. This time we only get $\pi_1(s) \geq p - 2k_2$, but this is enough to get the zero-sum. ∎

We can now finish the proof of Theorem 1(3).

We first treat the case that both C and D are empty, that is, $|B| = k_1 + k_2 - 2$.

Suppose there are (not necessarily disjoint) subsets $B_1, B_2 \subset B$ satisfying $\sum_{b\in B_i} \imath(\pi_i(b)) \in [k_i, 2k_i]$ and $\sum_{b\in B_i} \imath(\pi_{3-i}(b)) \le p$ for $i = 1, 2$. If $\sum_{b\in B_i} \imath(\pi_{3-i}(b)) \ge k_{3-i}$ for some i, then B_i yields a zero-sum. Otherwise the sum of the union $B_1 \cup B_2$ lies in $[k_1, 3k_1 - 1] \times [k_2, 3k_2 - 1]$ and we get a zero-sum. Hence we may suppose that no set of the form B_2 exists.

Now let $B' \subset B$ be any subset of cardinality $k_1 - 2$. Let $B'' \subset B \setminus B'$ be minimal such that its sum s'' satisfies $\pi_2(s'') \ge k_2$. (Such a B'' exists since $|B \setminus B'| = k_2$.) We have $\pi_1(s'') \in [1, k_1 - 1]$, otherwise we would have a zero-sum. Suppose that $\sum_{b\in B'} \imath(\pi_1(b)) > k_1 - 2$. Let $b'' \in B''$ be an element with $\pi_2(b'')$ maximal, and take a minimal subset $B''' \subset B'$ whose sum s''' satisfies either $\pi_1(s''') \ge k_1 - 1$ or $\pi_2(s''') + \pi_2(b'') \ge k_2$. If $\pi_1(s''') < k_1 - 1$, then $B''' \cup \{b''\}$ satisfies the properties of B_2 excluded above. Otherwise, $\pi_1(s'' + s''') \in [k_1, 3k_1 - 3]$ and $\pi_2(s''') + \pi_2(b'') \le 2k_2 - 1$. Our choice of b'' implies $\pi_2(s'') \in [k_2, k_2 + \pi_2(b'') - 1]$, so $\pi_2(s'' + s''') \in [k_2, 3k_2 - 2]$ and we get a zero-sum. Hence $\sum_{b\in B'} \imath(\pi_1(b)) \le k_1 - 2$.

Since $|B'| = k_1 - 2$, we get $\pi_1(b) = 1$ for all $b \in B'$, and since B' was arbitrary, this holds for all $b \in B$. Now we are done by Lemma 13.

Hence, we may assume that C is non-empty. Fix elements $b \in B$, $c \in C$. Consider the sets $\mathcal{S} = \Sigma(\{(1,0)^{m_1}, (0,1)^{m_2}, b, c\})$, $\mathcal{S}' = \Sigma(\{(1,0)^{m_1}, (0,1)^{m_2}, b - (1,0), c + (1,0)\})$. Then

$$\mathcal{S}' \subset \mathcal{S} \cup \underbrace{\{b + (-1, t) : 0 \le t \le m_2\} \cup \{c + (m_1 + 1, t) : 0 \le t \le m_2\}}_{(*)}$$

and

$$\underbrace{\{0, b + c\} + \Sigma(\{(1,0)^{m_1}, (0,1)^{m_2}\})}_{(**)} \subset S.$$

Since $m_1, m_2 \ge 2p/3$, we see that $(*)$ is contained in $(**)$, and so $\mathcal{S}' \subseteq \mathcal{S}$. Hence, if A is zero-sum free, the set A' obtained by replacing b by $b - (1,0)$ and c by $c + (1,0)$ is also zero-sum free. We can repeat this procedure, until one of b, c is contained in $\langle(0,1)\rangle$. If the element obtained in this way is not equal to $(0,1)$, we can replace it by at least two copies of $(0,1)$, which is impossible. If it is equal to $(0,1)$, our claim follows from the inductive hypothesis, unless the resulting set contains an element with multiplicity $\ge p - 2$. Since the element with multiplicity $\ge p - 2$ is necessarily $(0,1)$, and $(1,0) \in A$, we find that all elements different from the elements b and c chosen at the beginning are contained in $\{(0,1)\} \cup (1,0) + \langle(0,1)\rangle$. In particular, $C = \{c\}$ and $\pi_2(c) = 1$. If $D \ne \emptyset$, we obtain in the same way $d \in D$ with $\pi_1(d) = 1$, but then $c + d$ plus some copies of $(0,1)$ and $(1,0)$ yields a zero-sum.

Hence, it remains to consider the case $|B| = k_1+k_2-3$, $C = \{c\}$, $B\setminus\{b\} \subset (1,0) + \langle(0,1)\rangle$. Moreover, since $|B| \geq 2$, we could use any element $b \in B$ in the argument above and find that all elements in B satisfy $\pi_1(b) = 1$. Hence, replacing c by $c+(1,0)$ and b by $b-(1,0)$ yields a zero-sum free set of cardinality $2p-3+\pi_2(b)$, thus $B = \{(1,1)^{k_1+k_2-3}\}$. But then we can form the zero-sum $(k_1+k_2-3)(1,1) + (p-k_1-k_2+3)((1,0)+(0,1))$. Hence, the theorem is proven.

4. The largest multiplicity of a zero-sum free set in $\mathbb{Z}_p^2$. In this section let $A \subset \mathbb{Z}_p^2$ be a zero-sum free set with $|A| = 2p-2$ and maximal multiplicity $p-3$. Denote by m the second largest multiplicity in A. We may assume that $(1,0)$ occurs in A with multiplicity $p-3$, and $(0,1)$ with multiplicity m. Moreover, by Theorem 3(1) we may suppose $p \geq 29$. By Theorem 1(3), we get $p-m > 29/3$, thus $m \leq p-10$.

LEMMA 23. *Suppose that $(x,y),(x',y) \in A$. Then $|x-x'| \leq 1$. Moreover, there are no two disjoint pairs a, a' of elements in A with $a \neq a'$, $\pi_2(a) = \pi_2(a')$; in particular, the maximal multiplicity of $\pi_2(A \setminus \{(1,0)^{p-3}\})$ is at most $m+1$.*

Proof. The first claim follows from Lemma 18, if we can show that $-y \in \Sigma(\pi_2(A) \setminus \{y^2\})$, which in turn is implied by the Cauchy–Davenport theorem. For the second claim suppose that a_1, a_1', a_2, a_2' are elements of A with $a_i \neq a_i'$, $\pi_2(a_i) = \pi_2(a_i')$. Then we apply Lemma 18 to a_1+a_2, $a_1'+a_2'$, where we may assume $|\pi_1(a_1+a_2) - \pi_1(a_1'+a_2')| = 2$. Note that $S = \pi_2(A \setminus \{a_1, a_2, a_1', a_2', (1,0)^{p-3}\})$ contains $p-3$ non-zero elements, hence, the Cauchy–Davenport theorem together with Lemma 8 implies that $\Sigma(S) = \mathbb{Z}_p$ unless all elements in S are equal with at most one exception, that is, $\pi_2(A)$ contains some non-zero element y with multiplicity $\geq p-5 > 2p/3+2 \geq m+2$. Using the first part of the lemma, we get $\{(x,y)^l, (x+1,y)^{l'}\} \subset A$ for some $x \in \mathbb{Z}_p$ and $l, l' \geq 2$. Now we replace a_1, a_2, a_1', a_2' by two pairs (x,y), $(x+1,y)$ and do the same argument again. As a result, we get $A = \{(1,0)^{p-3}, (x,y)^l, (x+1,y)^{l'}, a\}$ with $l+l' = p$ and both $\leq m \leq 2p/3$. But this contains the zero-sum $l\cdot(x,y) + l\cdot(1,0) + l'\cdot(x+1,y)$. ∎

LEMMA 24. *If $m \leq p/6$, then A contains a zero-sum.*

Proof. It suffices to show that $\pi_2(A \setminus \{(1,0)^{p-3}\})$ contains three disjoint zero-sums: these zero-sums generate three elements in $\langle(1,0)\rangle$, hence, together with some copies of $(1,0)$ we obtain a zero-sum in A. By Lemma 23, we may choose $a \in A$ such that $S = \pi_2(A \setminus \{(1,0)^{p-3}, a\})$ has maximal multiplicity (at most) m. Then we can split S into subsets of given cardinalities, each having no multiple elements, provided that each given cardinality is at

most 6. We do this in the following way: Set $d = \lfloor p/3 \rfloor$ and $r = d \bmod 6$. We form $3 \cdot \lfloor d/6 \rfloor$ sets of cardinality 6, and 3 (possibly empty) sets of cardinality r. Then we group these small sets into three sets S_1, S_2, S_3, each being the union of $\lfloor d/6 \rfloor$ subsets of cardinality 6 and one of cardinality r. If we can show that each S_i contains a zero-sum, we are done. If one of the small sets contains a zero-sum, then so does each larger set, hence, we may assume that each of the small sets is zero-sum free, and we can apply Lemma 9. Thus S_i contains a zero-sum provided that

$$1 + \left\lfloor \frac{d}{6} \right\rfloor \cdot 21 + \frac{r(r+1)}{2} \geq p.$$

The left hand side is equal to

$$1 + \frac{d-r}{6} \cdot 21 + \frac{r(r+1)}{2} = 1 + \frac{7}{2} \cdot \left\lfloor \frac{p}{3} \right\rfloor + \frac{r(r-6)}{2} \geq \frac{7}{6} p - \frac{4}{3} + \frac{r(r-6)}{2}.$$

This is minimal for $r = 3$, so the inequality holds provided that $p/6 \geq 4/3 + 9/2$, i.e. $p \geq 35$.

For $p = 29$ or 31, we apply the same argument but decompose S differently. If $p = 29$, then $m \leq 4$, and we can choose three 9-element sets S_i each one consisting of one set of 7 distinct points and one pair of distinct points, which suffices. If $p = 31$, then $m \leq 5$, and we obtain three 10-element sets consisting of 6 distinct points plus 4 distinct points, which also suffices. ∎

Define $k = \lceil p/m \rceil$. Note that by Lemma 24, only the values $2 \leq k \leq 6$ are left. The introduction of this parameter turns out to be useful for two reasons: first, it distinguishes several cases for which we shall use different arguments, and second, we will apply Lemma 16, which involves k: In the present case, the condition on V of Lemma 16 becomes $|\Sigma(\pi_1(V))| \geq 4k - 1$. Verifying the condition on U is facilitated by the following simple observation.

LEMMA 25. *Let $U \subseteq \mathbb{Z}_p$ be a set satisfying $|u| \leq m$ for all $u \in U$. Then $\Sigma(\{1^m\} \cup U) = \mathbb{Z}_p$ is equivalent to $\sum_{u \in U} |u| \geq p - m - 1$.*

Proof. If $x, y, u \in \mathbb{Z}_p$ satisfy $|u| \leq \iota(y - x)$, then

$$\{x, x+1, \ldots, y\} + \{0, u\} = \begin{cases} \{x, x+1, \ldots, y+u\}, & \iota(u) = |u|, \\ \{x-u, x-u+1, \ldots, y\}, & \iota(u) = p - |u|. \end{cases}$$

Our claim now follows by induction on $|U|$. ∎

LEMMA 26. *Suppose that $k = 2$ (i.e. $m \geq p/2$). Then A contains a zero-sum.*

Proof. Every subset $V \subseteq A \setminus \{(1,0)^{p-3}, (0,1)^m\}$ with $|V| = 6$ satisfies the condition of Lemma 16. As A contains at most one element a with $\pi_2(a) = 1$ different from $(0,1)$, and at most two elements with $\pi_2(a) = -1$, we see that

by putting these elements into V we may assume that all elements of U satisfy $|u| \geq 2$. Since $m \geq p/2$, we can apply Lemma 25, and our claim follows, if

$$p - m - 1 \leq \sum_{u \in U} |\pi_2(u)| \geq 2|U| = 2(p - m - 5),$$

which is true since $p - m \geq 9$. ∎

LEMMA 27. *Suppose* $3 \leq k \leq 6$. *Then* A *contains a zero-sum.*

Proof. Define $E = A \setminus \{(1,0)^{p-3}, a\}$, where a is chosen such that the maximal multiplicity of $\pi_2(E)$ is at most m. As $p/m > k-1$, we can partition $\pi_2(E)$ into $\lfloor p/(k-1) \rfloor$ subsets S_i, each consisting of $k-1$ distinct elements, and leaving $p \bmod k-1$ elements unused. Let ℓ be the number of sets S_i containing a zero-sum.

Note first that if $\ell \geq 3$, we are done: each zero-sum comes from a sum s of elements of A with $\pi_2(s) = 0$; together with the elements $(1,0)^{p-3}$, this yields a zero-sum. If $\ell < 3$, we apply Lemma 16 to the set A' which has been obtained from A by removing the pre-image of each set S_i containing a zero-sum, and adding ℓ copies of $(1,0)$. If A' contains a zero-sum, then so does A, so we are done if we can find sets U, V satisfying the prerequisites of the lemma.

Let m' be the multiplicity of $(0,1)$ in A', and set $k' = \lceil \frac{p+1}{m'+2} \rceil$. The condition on V is $|\Sigma(V)| > (2k'-1)(2-\ell)$; this is satisfied for any set V with $|V| \geq (2k'-1)(2-\ell)$. Note that $k' \leq \lceil (p+1)/m \rceil = \lceil p/m \rceil = k$ as $m' \geq m-2$ and m does not divide p.

Set $\sigma = (k-1)k/2$; by Lemma 9, each set S_i has a sumset of cardinality at least $\sigma + 1$, so by Cauchy–Davenport, to get $\Sigma(\pi_2(U) \cup \{1^{m'}\}) = \mathbb{Z}_p$ it suffices to ensure that $\pi_2(U \cup \{(0,1)^{m'}\})$ contains at least $\lceil (p-1)/\sigma \rceil$ of the sets S_i. Thus we can have all prerequisites of the lemma satisfied if there are at least $\lceil (p-1)/\sigma \rceil + \ell$ sets S_i in $\pi_2(E)$ and at least $(2k'-1)(2-\ell)$ additional elements in $A \setminus \{(1,0)^{p-3}\}$. In other words, we have to check the inequality

$$(*) \qquad \left(\left\lceil \frac{p-1}{\sigma} \right\rceil + \ell \right) \cdot (k-1) + (2k'-1)(2-\ell) \leq p+1.$$

As $k' \leq k$, we may replace k' by k. After that, one sees that the worst case is the one with $\ell = 0$, so the remaining inequality is

$$(**) \qquad \left\lceil \frac{p-1}{\sigma} \right\rceil \cdot (k-1) + 4k - 3 \leq p.$$

Estimating $\lceil (p-1)/\sigma \rceil \leq (p+\sigma-2)/\sigma$ (and using the definition of σ) yields

$$p \geq \frac{5k^2 - 4k - 4}{k-2},$$

i.e. $p \geq 29$ for $k = 3$, $p \geq 30$ for $k = 4$, $p \geq 33\frac{2}{3}$ for $k = 5$ and $p \geq 38$ for $k = 6$. Thus it remains to check the cases $(k, p) = (4, 29)$, $(5, 29)$, $(5, 31)$, $(6, 29)$, $(6, 31)$, $(6, 37)$. One checks case by case that $(**)$ holds in each of these cases with the exception of $k = 6$, $p = 29$. In this last case, we have $m = 5$ and $k' \leq \lceil \frac{p+1}{m+2-\ell} \rceil = \lceil \frac{30}{7-\ell} \rceil$. If $\ell < 2$, this is equal to 5, and if $\ell = 2$, then k' does not appear in $(*)$, hence in $(*)$ we may replace k' by 5, ℓ by 0 (which again is the worst case), and we get $\lceil 28/15 \rceil \cdot 5 + 9 \cdot 2 \leq 30$, which is true. ∎

Theorem 1(1) now follows from Lemmas 24, 26, and 27.

5. The three largest multiplicities of a zero-sum free set in $\mathbb{Z}_p^2$. In this section we prove Theorem 1(4).

Let A be a zero-sum free sequence, m_1, m_2, m_3 be the three largest multiplicities, let a_1, a_2, a_3 be the elements with these multiplicities, and let $\delta = 2p-2-m_1-m_2-m_3$ be the number of remaining elements ($0 \leq \delta \leq 3$). We will prove our theorem by a series of restrictions on the possible shape of A, each stated as a separate lemma.

In view of Theorem 1(1), we will always suppose $\max(m_1, m_2, m_3) \leq p - 4$.

LEMMA 28. *We can suppose that* $p \geq 41$ *and that* $\min(m_1, m_2, m_3) \geq 13$.

Proof. The case $p \leq 37$ is Theorem 3(2) (which has been done by computer). Note that we only have to choose three multiplicities and up to six elements in $\mathbb{Z}_p^2$, hence these computations are feasible even for rather large value of p. The total computation time was 20 minutes.

The lower bound for $\min(m_1, m_2, m_3)$ follows from the fact that the largest multiplicity is at most $p - 4$, and the second largest is less than $2p/3$. ∎

We will not in general assume that $m_1 \geq m_2 \geq m_3$, but will impose different conditions on these integers to exploit symmetries more efficiently. Choose coordinates such that $a_1 = (1, 0)$, $a_2 = (0, 1)$. With respect to these coordinates we can represent a_3 as (x, y); without further mention we fix this meaning of x, y.

LEMMA 29. *We have* $y \neq 1$ (*and, analogously,* $x \neq 1$).

Proof. We first show that $(x, y) = (1, 1)$ is impossible. We try to form the zero-sum $m_3(1, 1) + (p - m_3)(1, 0) + (p - m_3)(0, 1)$, which is possible unless $m_3 + \min(m_1, m_2) < p$, that is, $\max(m_1, m_2) \geq p - 1 - \delta \geq p - 4$; since $(x, y) = (1, 1)$ we still have one symmetry at our disposal and may suppose that $m_1 \geq m_2$. By part (1) of Theorem 1, we get $m_1 = p - 4$ and $\delta = 3$.

Suppose first that there is an element $a \in A$ different from a_2, a_3 satisfying $\pi_2(a) = 1$. We apply Lemma 18 to the equation $\pi_2(a) = \pi_2((0, 1))$ and

obtain a contradiction, unless $|\pi_1(a)| \le 2$. The same argument applied with $(1,1)$ instead of $(0,1)$ yields $|\pi_1(a) - 1| \le 2$, thus $a = (2,1)$ or $a = (-1,1)$. If there were such an element, we could form the zero-sum

$$m_3(1,1) + a + (p - m_3 - 1)(0,1) + (p - m_3 - \pi_1(a))(1,0);$$

note that the required multiplicity of a_1 poses no problem, since

$$m_1 = p - 4 \ge p - m_3 - \pi_1(a).$$

We now apply Lemma 18 to the equation $\pi_2(3(0,1)) = \pi_2(3(1,1))$, and obtain a contradiction, provided that

$$-3 \in \Sigma(\{1^{m_2+m_3-6}\} \cup \pi_2(A \setminus \{a_1^{m_1}, a_2^{m_2}, a_3^{m_3}\})).$$

Let b_1, b_2, b_3 be the three elements in A different from a_1, a_2, a_3. Since $m_2 + m_3 - 6 = p - 7 > p/2$, we get our contradiction unless either $\pi_2(b_1) + \pi_2(b_2) + \pi_2(b_3) \le 3$ (which is impossible), or one of the three elements, say b_1, satisfies $\pi_2(b_1) =: -k \in \{-1, -2\}$. Applying Lemma 17 to $E := \{b_1, (1,1)^k\}$ yields a contradiction, unless we have $b_1 = (1, -k)$. However, even in these cases we can apply part (1) of Lemma 17, thus, $A' = A \setminus \{b_1, (1,1)^k\} \cup \{(1,0)^{k+1}\}$ is zero-sum free. Since $m_3 > 3$, we find that all elements in A' satisfy $\pi_2(a) = 0, 1$. However, b_2 and b_3 contradict this.

Hence, the assumption $(x, y) = (1, 1)$ leads to a contradiction. Moreover, we can change the roles of a_2 and a_3 and find that $(x, y) = (-1, 1)$ is also impossible.

Thus, $m_1 = p - 4$, and $|x| \ge 2$. From Lemma 18 we immediately find $|x| \le 2$, and exploiting the symmetry between a_2 and a_3 we may assume that $x = 2$. We now apply Lemma 18 to the equation $\pi_2(2(0,1)) = \pi_2(2(x,1))$, and obtain a contradiction, provided that $-2 \in \Sigma(\pi_2(A) \setminus \{1^4\})$. But $\pi_2(A)$ contains 1 with multiplicity $\ge p - 5$, hence we are done unless there is an element in A with $\pi_2(a) = -1$. But then we can replace a and one copy of $(2,1)$ by at least three copies of $(1,0)$, and therefore obtain a zero-sum. ∎

LEMMA 30. *We have $y \ne -1$ (and, analogously, $x \ne -1$).*

Proof. We now replace one copy of $(0,1)$ and one copy of $(x,-1)$ by one copy of $(x,0)$, until we run out of elements of the form $(x,-1)$ or $(0,1)$. In this way we obtain $\min(m_2, m_3)$ elements $(x,0)$, hence for A to be zero-sum free it is necessary that $\{1^{m_1}, x^{\min(m_2,m_3)}\}$ be zero-sum free. But $m_1 + \min(m_2, m_3) \ge p - 1$, thus, this set is zero-sum free if and only if it is constant, that is, $x = 1$, and we are in the case covered by Lemma 29. ∎

LEMMA 31. *Each of m_1, m_2, m_3 is less than $p - 5$.*

Proof. Suppose otherwise, i.e. $m_1 \in \{p-5, p-4\}$; this implies $p - 1 \le m_2 + m_3 \le p + 3$. We assume that $m_2 \ge m_3$; thus $m_2 \in [(p-1)/2, 2p/3]$ and $m_3 \in [p/3 - 1, (p+3)/2]$, and in particular $m_3 \ge 13$. We will show that,

for any x, y, the sequence $\{i(x,y) : 1 \le i \le m_3\}$ contains an element of $[5,p] \times [p-m_2, p]$ which thus yields a zero-sum. Set $I := \{i \in \{1,\dots,m_3\} : iy \in [p-m_2, p]\}$.

If I contains three consecutive integers, then we get a zero-sum as $|x| \ge 2$. We claim that $|y| \ge p/6$. Suppose first that $y > 5p/6$. Then $3y \ge (p+1)/2 \ge p - m_2$, so $\{1,2,3\} \subseteq I$. Now suppose $y < p/6$. As $y \le (m_2+1)/3$, a triple in I can only be avoided if $(m_3-2)\imath(y) < p - m_2$. But using $y \ge 2$, this would imply $p > 2(m_3-2) + m_2 \ge p + m_3 - 5$, contradicting $m_3 \ge 13$. This proves the claim.

Next, suppose $|x| \le 4$. Consider the set $J := \{i \in \mathbb{N} : 2 < i \le 2 + p/|y|\}$. Using $|y| \ge p/6$, we find that any $i \in J$ satisfies $i \le 8 \le m_3$. The size of J has been choosen such that $J \cdot y$ necessarily contains an element in $[(p+1)/2, p]$, so in particular $J \cap I \ne \emptyset$. However, for i_0 in this intersection we get $6 \le i_0|x| \le 32$, which yields a contradiction using $p \ge 41$. Hence $|x| \ge 5$.

On the one hand this implies $y < p - m_2 < 2p/3$; on the other hand, it now suffices to find two consecutive integers in I to get a zero-sum. If $y > p/4$, then $2y \ge p - m_2$, so $\{2,3\} \subseteq I$ is such a pair. If $y \le p/4 \le (m_2+1)/2$, then the inequality $(m_3-2)\imath(y) \ge p - m_2$ which we used to find a triple in I still yields a pair. Hence our claim is proven. ∎

From now on we shall assume that m_3 is the least of the three multiplicities. We continue to assume $a_1 = (1,0)$, $a_2 = (0,1)$ and $a_3 = (x,y)$, and we choose a_1, a_2 in such a way that $x \ge y$. Note that the upper bound $\max(m_1, m_2) \le p - 6$ immediately implies the lower bounds $m_3 > p/3 + 1$ and $\min(m_1, m_2) > p/2$.

LEMMA 32. *We have $y \ge (m_1 + m_2 - p + 2)/2 \ge (p-4)/6$; in particular, $y \ge 7$.*

Proof. The second inequality follows from $m_1 + m_2 \ge 2(m_1 + m_2 + m_3)/3 \ge (4p - 10)/3$.

For the first inequality, we distinguish the cases $|x| < y$ and $|x| \ge y$. Suppose first $|x| < y$. By our general assumption $x \ge y$, we have $p - x < y$. Let k be the smallest integer such that $ky \ge p - m_2$. Since $y \ge 2$ and $m_3 > p/3$, we have $k \le m_3$. Assuming $y < (m_1 + m_2 - p + 2)/2$, we want to show that $k(p-x) \le m_1$ and $ky \le p$ to get a contradiction. By $p - x < y$, it suffices to show that $ky \le m_1$. But $ky - m_1 \le p - m_2 + y - m_1 < (p - m_1 - m_2 + 2)/2 \le 0$ for $p \ge 16$.

Now suppose $|x| \ge y$. Set $k = \lceil (p-m_2)/y \rceil$ and $l = \min(m_3, \lfloor p/y \rfloor)$. Then $k \le l$ as $m_3 y > (p/3+1)2 \ge p - m_2$, so it makes sense to consider the expressions $k \cdot (x,y) + (p - ky) \cdot (0,1)$, $(k+1) \cdot (x,y) + (p - (k+1)y) \cdot (0,1)$, $\dots, l \cdot (x,y) + (p - ly) \cdot (0,1)$. By the choice of k and l, each of these expressions is contained in $\Sigma(\{a_2^{m_2}, a_3^{m_3}\})$, and each has second coordinate zero. Hence,

we obtain an arithmetic progression in $\langle(1,0)\rangle$ of length $l-k+1$ with difference $|x|$. This implies $(l-k)|x| \le p-m_1-2$. We obtain

$$|x|\left(\min\left(m_3, \left\lfloor\frac{p}{y}\right\rfloor\right) - \left\lceil\frac{p-m_2}{y}\right\rceil\right) \le p-m_1-2,$$

which by $|x| \ge y$ implies

$$\min(ym_3+m_2-p-y, m_2-2y) \le p-m_1-2.$$

If the first term in the minimum is smaller, we deduce (using $y \ge 2$) that $m_1+m_2+2m_3 \le pn$, which is impossible. Hence, $y \ge (m_1+m_2+2-p)/2$. ∎

LEMMA 33. (*Recall that we are supposing that m_3 is the least of the three multiplicities, and that $x \ge y$.*) *We have $y > 3p/10$.*

Proof. For $p \ge 41$, we have $(p-4)/6 > p/7$, hence, in view of Lemma 32 we may assume that $y > p/7$. Call an integer k *obstructing* if $k \le m_3$ and $ky \bmod p \in [p-m_2, p]$. This definition is motivated by the fact that if k is obstructing, then

$$\frac{x}{p} \in \bigcup_{a=0}^{k-1}\left(\frac{a}{k}, \frac{a}{k}+\frac{p-m_1}{kp}\right),$$

that is, we obtain obstructions to the possible values of x (see Figure 3). For different ranges of y, we obtain different obstructing integers, and we will obtain a contradiction by showing that no possibility for x remains.

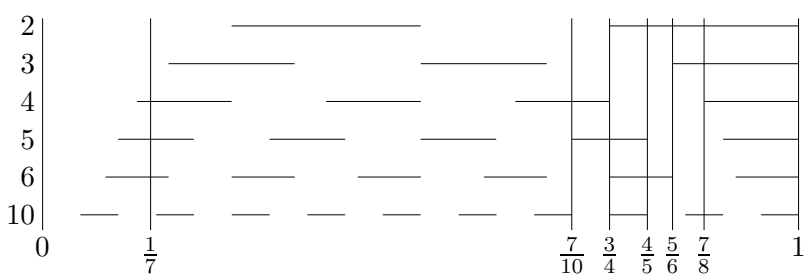


Fig. 3. Obstructions to x/p for $m_1 = p/2$ and different k

We first deal with the range $p/7 < y \le p/5$. Then 4, 5 and at least one of 3, 6 are obstructing. Using the bound $m_1 > p/2$ and $x \ge y > p/7$, we deduce that $x/p \in (4/5, 7/8)$, and that not both 3 and 6 can be obstructing. If $y < p/6$, this implies that $m_2 < 4p/7$, $x/p \in (5/6, 7/8)$, and $m_1 < 2p/3$. Hence, $2p-5 < 2p/3+8p/7 = 38p/21$, which is impossible for $p \ge 41$. If $y > p/6$, we obtain $x/p \in (4/5, 5/6)$, and $m_1 < 3p/5$, hence $m_2 > 4p/5-5$. For $p \ge 41$, we obtain $m_2 > 2p/3$, which implies that 2 is obstructing, and gives a contradiction.

Next, suppose that $p/5 < y \le p/4$. If $m_2 \ge 3p/5$, then $2, 3$ and 4 are obstructing, and we immediately obtain a contradiction. Otherwise, 3, 4 and 8 are obstructing, and we obtain $x/p \in (3/4, 2/3 + (p - m_1)/3p)$. Suppose that $y \le 2p/9$. Then 9 is obstructing, and we see that the intervals $(2/3, 2/3+(p-m_1)/3p)$ and $(7/9, 7/9+(p-m_1)/9p)$ overlap, which is only possible for $m_1 < 2p/3$. But then

$$2p - 5 \le m_1 + m_2 + m_3 \le \frac{2p}{3} + \frac{6p}{5} = \frac{28p}{15},$$

which fails for $p \ge 41$. If $y > 2p/9$, then 2 is obstructing, unless $m_2 < 5p/9$, but then

$$2p - 5 \le m_1 + m_2 + m_3 \le \frac{3p}{4} + \frac{10p}{9} = \frac{67p}{36},$$

which is also impossible.

If $p/4 < y < 3p/10$, then 2, 3, 6 and 10 are obstructing, which implies $x \in (7/10, 3/4)$ and $m_1 < 3p/5$. If $y \le 2p/7$, then 7 is obstructing, and we obtain $m_1 < 4p/7$, which gives

$$2p - 5 \le m_1 + m_2 + m_3 \le \left\lfloor \frac{3p}{4} \right\rfloor + 2\left\lfloor \frac{4p}{7} \right\rfloor \le \frac{53p}{28}.$$

For $p > 43$ this estimate gives a contradiction, while for $p = 41, 43$ we compute explicitly the rounding errors and obtain a contradiction as well. If $y/p \in (2/7, 3/10]$, then 5 is obstructing, which yields a contradiction, unless $m_2 < 4p/7$. But then $m_1 + m_2 + m_3 \le 61p/35$, which is impossible. ∎

We can now finish the proof of Theorem 1(4).

Consider the set

$$I = \{iy : 1 \le i \le m_3,\ iy \bmod p \ge p - m_2\}.$$

If $|I| \ge p - m_1$, then the set $\{i(x, y) : 1 \le i \le m_3\}$ contains some element b satisfying $\pi_1(b) \in [m_1, p]$, $\pi_2(b) \in [p - m_2, p]$, and this element can be combined with some copies of $(1, 0)$ and $(0, 1)$ to produce a zero-sum. Hence, $|I| \le p - m_1 - 1$. Hence,

$$J = \{iy : 1 \le i \le m_3,\ iy \bmod p < p - m_2\}$$

satisfies $|J| \ge m_1 + m_3 - p + 1 \ge p - 4 - m_2$, that is, there are at most three values in the range $[1, p - m_2 - 1]$, which are not in J.

Suppose first that $y < p - m_2$. Then none of the elements $-ky \bmod p$, $1 \le k < p - m_3$, can be contained in J, for otherwise we could represent 0 modulo p as ly with $1 \le l < p$, which would imply that $y = 0$, which is impossible. In this range, there are at least $\lfloor (p - m_3 - 1)\imath(y)/p \rfloor$ indices k for which $-ky \bmod p$ is in $[1, p - m_2 - 1]$, since this is in particular the case for those values k for which $\lfloor k\imath(y)/p \rfloor$ differs from $\lfloor (k + 1)\imath(y)/p \rfloor$. On the other hand, we know that J misses at most three values, which together

with Lemma 33 and $m_3 \le \frac{1}{3}(2p-2)$ yields

$$3 \ge \left\lfloor \frac{(p-m_3-1)\imath(y)}{p} \right\rfloor \ge \lfloor 0.3(p-m_3-1) \rfloor \ge \lfloor 0.1(p-1) \rfloor \ge 4.$$

If $y \ge p-m_2$, then $x < p-m_1 < p/2$. By our assumption we have $y \le x$, hence $2y < p$, and we obtain a zero-sum, unless $2x < p-m_1$. But then $y \le x < p/4$, which contradicts Lemma 33. Hence, Theorem 1(4) is proven.

6. Asymptotic estimates

6.1. Lower bounds for the largest multiplicities. We first establish the following, which is a strengthening of the bound for m_1 implied by Theorem 2.

THEOREM 34. *For every $\epsilon > 0$ there exists some $\delta > 0$ such that for every sufficiently large prime number p and every multiset $A \subseteq \mathbb{Z}_p^2$ such that no element of A has multiplicity $\ge \delta p$, the following holds true:*

(1) *If $|A| > (1+\epsilon)p$, then A contains a zero-sum of length $\le p$.*
(2) *If $|A| > (2+\epsilon)p$, then A contains a zero-sum of length p.*

We will need the following lemma.

LEMMA 35. *There exists an absolute constant W such that the following holds true: If p is a sufficiently large prime, and $A \subseteq \mathbb{Z}_p^2$ is a set with $|A| \ge p/4$, and if for each affine line L we have $|A \cap L| \le |A|/W$, then there exists some n such that*

$$|\Sigma_n(A)| \ge p^2/2.$$

Proof. The proof follows closely the lines of the induction step in Section 2.3 of [1]. In fact, the only changes necessary affect the choice of s in [1, equation (7)], which we have to choose $\le p/24$ to ensure that after using $3s$ elements the remaining set A' still has the property that for each affine line A' we have $|A' \cap L| \le 2|A'|/W$. ∎

Proof of Theorem 34. Define W as in Lemma 35. We distinguish two cases, depending on whether there exists an affine line containing at least p/W elements of A or not. Suppose first that no such line exists. Choose subsets $A_1, A_2 \subseteq A$ with $|A_i| = \lceil p/4 \rceil$. Then both A_1, A_2 satisfy the conditions of Lemma 35, hence there exist some $n_1, n_2 \le p/2$ such that $|\Sigma_{n_i}(A_i)| \ge p^2/2$. For statement (1) this is already sufficient, since $\Sigma_{n_1}(A_1) \cap (-\Sigma_{n_2}(A_2)) \ne \emptyset$, and we obtain a zero-sum of length $n_1 + n_2 \le p$. Note that n_1, n_2 cannot be zero, that is, this zero-sum is in fact non-trivial. For statement (2) we choose $p - n_1 - n_2$ arbitrary elements in $A \setminus (A_1 \cup A_2)$, add them up to obtain an element s, and use the fact that $\Sigma_{n_1}(A_1) \cap (-s - \Sigma_{n_2}(A_2)) \ne \emptyset$ to find a zero-sum using n_1 elements in A_1, n_2 in A_2, and $p - n_1 - n_2$ in $A \setminus (A_1 \cup A_2)$. Hence, in this case our claim follows.

Now suppose that there exists a line L with $|A \cap L| \geq p/W$. For statement (1), if this line passes through 0, we obtain a zero-sum using Lemma 14, provided that $\delta < 1/40W^2$. For statement (2) we can add a vector to all elements in A without changing the statement, hence in both cases we may assume that $L = \{(1,t) : t \in \mathbb{Z}_p\}$. If $\delta < \epsilon/100W^2$, then from $A \cap L$ we can choose $\lfloor \epsilon^2 p/400W \rfloor$ sets B_i containing $100\epsilon^{-1}W$ different elements each, and set $B = \bigcup B_i$; note that $|B| < p\epsilon/4$. From Lemma 11 it follows that

$$|\Sigma_k(B_i)| \geq 2500\epsilon^{-2}W^2,$$

where $k = \lfloor |B_i|/2 \rfloor$. Hence, upon putting $N = k\lfloor \epsilon^2 p/400W \rfloor$ it follows from the Cauchy–Davenport theorem that $\Sigma_N(B)$ contains the whole line $\{(N,t) : t \in \mathbb{Z}_p\}$. Hence, our claim follows if we can show for statement (1) that every element of $\mathbb{Z}_p$ can be written as a subset sum of $\pi_1(A \setminus B)$, and for statement (2) that every element in $\mathbb{Z}_p$ can be written as a subset sum of $\pi_1(A \setminus B)$ of length $p-N$. Suppose that this is not the case. For statement (1) this implies that $\pi_1(A \setminus B)$ contains less than p non-zero elements. However, in this case $\pi_1(A \setminus B)$ contains 0 with multiplicity at least $3\epsilon p/4$, so we may apply Lemma 14 once more to obtain a zero-sum. For statement (2) note that $N \sim \epsilon p/4$. Hence, we obtain a zero-sum, unless there is some element $a \in \mathbb{Z}_p$ such that A contains at least $(1+\epsilon/2)p$ elements mapping to a under π_1. But then we find a zero-sum of length p within this set in the same way as for statement (1). ∎

We now turn to the proof of Theorem 2. Assume that $(1,0)$ is the point with the highest multiplicity m_1 in A. If $m_1 < (1-\epsilon)p - 2$, set $A' = A \setminus \{(1,0)^{m_1}\}$. Then by Theorem 34 we see that A' contains a zero-sum, unless the largest multiplicity of A' is at least δp for some δ depending on ϵ. Hence, it suffices to consider the case $m_1 > 0.9p$.

Choosing W as in Lemma 35, we find that A' contains a zero-sum, unless there is a line L with $|A' \cap L| > p/W$. Again as in the proof of Theorem 34 we see that for δ sufficiently small we can find a set $B \subseteq A \cap L$ with $|B| < 0.1p$ such that $\Sigma(B)$ contains some line $L' = \{(a,b) + (x,y)t : t \in \mathbb{Z}_p\}$. Suppose first that (x,y) is not collinear to $(1,0)$. Then $\langle (x,y) \rangle$ contains at most δ elements of A, hence in $A \setminus B$ we find $p-1$ elements not collinear to (x,y). Thus we can find an element $s \in \Sigma(A \setminus B)$ with $-s \in L'$; together with some elements in B, this yields a zero-sum.

Now we suppose that L' is parallel to $\langle (1,0) \rangle$. We obtain a zero-sum if $\Sigma(\pi_2(A \setminus B)) = \mathbb{Z}_p$. Since $A \setminus B$ contains at least $2p - 2 - 0.1p - m_1 \geq 0.9p$ elements, this is certainly the case unless there is some $a \in \mathbb{Z}_p$ such that $|(A \setminus B) \cap \pi_2^{-1}(a)| > 0.8p$. Thus we may assume that A contains at least $0.8p$ elements a with $\pi_2(a) = 1$ (and $(1,0)$ with multiplicity $> 0.9p$).

For δ sufficiently small we can easily find $p/20$ pairs a_1, a_2 in A such that $\pi_2(a_1) = \pi_2(a_2) = 1$, and $|\pi_1(a_1) - \pi_1(a_2)| > 10$. If there is a pair with

$|\pi_1(a_1) - \pi_1(a_2)| > 0.1p$, we are immediately done by Lemma 18. Otherwise we take $N = \lfloor (p - m_1 - 1)/2 \rfloor \le p/20$ such pairs. Since there are

$$2p - 2 - m_1 - 2\left\lfloor \frac{p - m_1 - 1}{2} \right\rfloor \ge p - 1$$

elements in A which are neither in one of the pairs chosen nor equal to $(1,0)$, there is an element s with $\pi_2(s) = -N$, which can be represented using elements not in one of the chosen pairs nor equal to $(1,0)$. Choosing one element of each pair and adding them to s yields an element of $\langle (1,0) \rangle$; by using different choices, we obtain a sequence of $N+1$ elements $(x_0, 0), \dots, (x_N, 0) \in \Sigma(A \setminus \{(1,0)^{m_1}\})$ with $10 < x_{i+1} - x_i < 0.1p$. This yields a zero-sum unless $0 < x_0 < x_N < p - m_1$, i.e. we get $10N < p - m_1$. But $10N \ge 5(p - m_1) - 10$, which contradicts $p - m_1 \ge 3$.

If the reader has the impression that our dealing with constants in the proof of Theorem 2 is quite wasteful, she is certainly right. However, the real loss occurs in the use of Lemma 35, and we did not try to improve a constant which will still be too small to be of much use.

6.2. Upper bounds for the largest multiplicity. In this section we prove Theorem 1(2). Let p be a prime number and let $A \subseteq \mathbb{Z}_p^2$ be a zero-sum free set with $|A| = 2p - 2$ and maximal multiplicities $m_1 \ge m_2$. We may assume that the elements with maximal multiplicity are $(1,0)$ and $(0,1)$, and that A contains no other element of the form $(x,0)$ or $(0,y)$. Set $\delta = p - m_1$; in several places, we will suppose that δ/p is sufficiently small (but independently of p). We will moreover use the following definitions: μ is the maximal multiplicity of $\pi_2(A \setminus \{(1,0)^{m_1}\})$, and $k = \lceil p/m_2 \rceil$ is the "number of times one would need the elements $(0,1)^{m_2}$ to fill an entire $\mathbb{Z}_p$".

We do already have a lower and an upper bound for m_2: by Theorem 1(3), we may suppose $m_2 < 2p/3$. On the other hand, for δ/p sufficiently small, Theorem 2 yields:

LEMMA 36. *We have $m_2 > 8\delta$, and in particular $k \le p/4\delta$.*

We will now first get precise statements describing the rows $A \cap \pi_2^{-1}(y)$; the important result here is Lemma 38, which bounds the number of elements of each row. Then we use the method of Lemma 16 to finish the proof.

We proceed by induction in the following way. Let A' be another set with cardinality $2p-2$ and maximal multiplicities $p-3 \ge m_1' \ge m_2'$. We suppose that the claim is true if $m_1' \ge m_1$, $m_2' \ge m_2$ and $(m_1, m_2) \ne (m_1', m_2')$. Moreover, for $B \subset \mathbb{Z}_p^2$ consider the sum

$$S(B) := \sum_{(x,y) \in B} \imath(x)^2.$$

We also suppose that the claim is true for A' if $m_1' = m_1$ and $m_2' = m_2$ and $S(A') > S(A)$.

Using this induction hypothesis, we show:

LEMMA 37. *Suppose* $(x,y),(x',y) \in A$ *with* $y \geq 2$. *Then* $x - x' \in \{-1,0,1\}$.

Proof. Suppose otherwise. After possibly exchanging x and x', we may suppose $\imath(x'-x) \leq p-\delta+1$. Then $\Sigma(\{(1,0)^{p-\delta},(x,y),(x',y)\})$ contains the whole interval $(x,y)+\{0,1,\ldots,\imath(x'-x)+p-\delta\}\cdot(1,0)$. In particular, if we replace (x,y) and (x',y) by $(x+k,y)$ and $(x'-k,y)$ for some $0 \leq k \leq \imath(x'-x)$, then we get a new set A' satisfying $\Sigma(A') \subset \Sigma(A)$. Thus it suffices to prove that A' contains a zero-sum. If $\imath(x') > \imath(x)$, then choose $k=1$. As

$$\imath(x+1)^2 + \imath(x'-1)^2 > \imath(x)^2 + \imath(x')^2,$$

the set A' contains a zero-sum by induction. If $\imath(x') < \imath(x)$, then choose $k = \imath(x')$. Then A' contains $(0,y)$, which is impossible. ∎

LEMMA 38. *We have* $\mu \leq m_2 + \delta - 2$.

Proof. Let $B := \pi_2(A \setminus \{(1,0)^{p-\delta}\})$, and let y be an element of maximal multiplicity of B; we assume that this multiplicity is at least $m_2+\delta-1$. By Lemma 36, $m_2 \geq \delta$, so we may set $B' := B \setminus \{y^{2\delta-2}\}$. We claim that if $\Sigma(B')$ contains $-(\delta-1)y$, then A contains a zero-sum.

Choose an element $a \in \Sigma(A)$ with $\pi_2(a) = -(\delta-1)y$, and form $\delta-1$ pairs $(x_i,y),(x_i',y) \in A$ with $x_i \neq x_i'$, that is, $x_i = x_i' \pm 1$. We have

$$|\Sigma(\{x_i' - x_i : 1 \leq i \leq \delta-1\})| = \delta,$$

thus by taking a and one element of each pair, we get δ different sums in $\langle(1,0)\rangle$. Together with $(1,0)^{p-\delta}$, one of them yields a zero-sum. This proves the claim, hence it remains to show that $\Sigma(B')$ contains $-(\delta-1)y$.

As $|B'| = p-\delta$ we have $\Sigma(B') = \mathbb{Z}_p$ unless B' contains an element y' with multiplicity at least $p-2\delta+2$. As this is more than $|B|/2$ and y was chosen maximal, this implies $y' = y$; thus B contains y with multiplicity at least p.

If $y \neq 1$, then there are only $\delta-2$ elements left in A which might be equal to $(0,1)$. This contradicts Lemma 36, so we have $y=1$, and our task simplifies to proving that $-(\delta-1) \in \Sigma(B')$. If $B = \{1^{p-2+\delta}\}$, then A contains a zero-sum by Lemma 13, so we may suppose $\sum_{b\in B'} \imath(b) \geq p-\delta+1$. If B' does not contain any element in $[p-\delta+2, p-1]$, then this together with the high multiplicity of 1 in B' already implies $-(\delta-1) \in \Sigma(B')$, which is what we had to show.

So now let $d \in A$ be an element with $\pi_2(d) \geq p-\delta+2$. Consider the set S of all elements reachable from d by adding $p-\imath(\pi_2(d))$ elements $a \in A$ each satisfying $\pi_2(a) = 1$. By Lemma 17, any $s \in S$ satisfies $1 \leq \pi_1(s) \leq$

$p-\imath(\pi_2(d))$, which is only possible if the set of elements in A with $\pi_2(a)=1$ takes the form $\{(0,1)^{m_2},(\pm1,1)^{\mu-m_2}\}$. As $\mu\ge p$, we may form the sum $m_2\cdot(0,1)+(p-m_2)\cdot(\pm1,1)=(\mp m_2,0)$. Together with copies of $(1,0)$ this yields a zero-sum as $\delta\le m_2\le m_1$. ∎

Recall that we defined $k=\lceil p/m_2\rceil$ and that we already proved $k\le p/4\delta$.

LEMMA 39. *The set A contains a zero-sum.*

Proof. We will apply Lemma 16. We will decompose $A\setminus\{(1,0)^{m_1},(0,1)^{m_2}\}$ into two subsets U and V with $|V|=(2k-1)(\delta-1)$; this implies that V satisfies the condition of that lemma. We claim that by choosing U appropriately, we may ensure that the maximal multiplicity of $U':=\pi_2(U\cup\{(0,1)^{m_2}\})$ is at most m_2. Indeed, using $\mu\le m_2+\delta-2$, there are at most

$$(\delta-2)\cdot\frac{2p-2-(p-\delta)}{m_2+\delta-2}\le(\delta-2)\cdot\frac{p}{m_2}\le(\delta-2)k\le(2k-1)(\delta-1)$$

elements which we are forced to include in V.

We have

$$|U'|=p-2k\delta+2k+2\delta-3,$$

and we want to show $\Sigma(U')=\mathbb{Z}_p$. For any fixed constant c_0 (say, $c_0=10$), $k\le c_0$ implies $|U'|>5p/6$ if we choose δ/p small enough. Using $m_2<2p/3$, we see that $\Sigma(U')=\mathbb{Z}_p$.

Now suppose $k\ge11$, i.e. $m_2<p/10$. Then we can partition U' into subsets consisting of 10 different elements each, leaving at most 9 elements unused. Each of these subsets has a sumset of cardinality at least 29 by Lemma 10, and the total number of sets is $\lfloor|U'|/10\rfloor$. Now $k\le p/4\delta$ implies $|U'|>p/2$, so using Cauchy–Davenport, we obtain $\Sigma(U')=\mathbb{Z}_p$, provided that

$$\left\lfloor\frac{p}{20}\right\rfloor29\ge p-1,$$

which is certainly true for $p>100$. ∎

7. Algorithms to check $B(n)$. We now describe the algorithm used to prove Theorem 3. All three statements ((1), (2) and the "moreover" part) essentially use the same algorithm. In this section we work in $\mathbb{Z}_n$ for n not necessarily prime (because of the cases 8, 9 and 10).

To reduce computation time in the case that n is prime, we will need the following lemma:

LEMMA 40. *Suppose $A\subset\mathbb{Z}_p^2$ contains $\{(1,0)^m,(x_1,y)^k,(x_2,y)^k\}$ where $|x_1-x_2|\le m+1$, $p-k\cdot|x_1-x_2|\le m+1$ and $|A|\ge2k+m+n-1$. Then A contains a zero-sum.*

Proof. By the two prerequisites concerning $|x_1-x_2|$, any interval $[a, a+m] \subset \mathbb{Z}_p$ contains an element of the form $l \cdot x_1 + (k-l) \cdot x_2$ with $0 \le l \le k$; thus $\Sigma(\{(1,0)^m, (x_1,y)^k, (x_2,y)^k\})$ contains the whole coset $\mathbb{Z}_n \times \{ky\}$. By the last prerequisite, we can find a subset of $A \setminus \{(1,0)^m, (x_1,y)^k, (x_2,y)^k\}$ whose sum s satisfies $\pi_2(s) = -ky$; this yields a zero-sum. ∎

The algorithm to check property B in principle just tries every possible multiset $A \subset \mathbb{Z}_n^2$ consisting of $2n-2$ elements and having maximal multiplicity at most $n-3$ (and which, for statement (2), satisfies the additional condition concerning the three maximal multiplicities); however, we need some good methods to reduce the computation time. There are several such methods which only work when n is prime; as the non-prime cases we are interested in are relatively small, this is not a problem.

Let us first suppose that n is prime. Then we may assume that the two elements with maximal multiplicities $m_1 \ge m_2$ are $a_1 = (1,0)$ and $a_2 = (0,1)$. The algorithm has two outer loops to try all possible values m_1 and m_2 and then recursively adds other elements with smaller multiplicities. This is done in the order of decreasing multiplicity, as elements with higher multiplicity tend to yield contradictions more quickly.

During the computation, we always keep an up-do-date copy of the sumset $\Sigma(A)$. Moreover, for each element $z \in \mathbb{Z}_n^2$ which is not yet contained in A, we store an upper bound for the multiplicity that z can have in A. These bounds are updated each time a new element a is added to A:

- No negative of any existing subset sum may be added anymore. (The corresponding upper bounds are set to zero.)
- No other element of the subgroup $\langle a \rangle$ may be added anymore by Lemma 12.
- Applying Lemma 40 with $(x_1, y) = a$ yields upper bounds for the multiplicity of several elements of the form (x_2, y).

Using these upper bounds, after each addition of an element we try to estimate whether there is still enough room for all remaining elements to be added (and stop if this is not the case). If we are adding elements with multiplicity k right now, and there are l cyclic subgroups left which are not yet completely forbidden for new elements, then we have space left for kl elements at most (again using Lemma 12).

If n is not prime, we can apply neither Lemma 12 nor Lemma 40. Moreover, we do not know whether the two elements with maximal multiplicities a_1, a_2 generate the group. However, we may always apply a group automorphism such that $\pi_1(a_1) \mid n$ and $\pi_2(a_1) = 0$; moreover, if $\pi_2(a_2) \neq 0$ we may apply a second group automorphism, fixing a_1 and such that $\pi_2(a_2) \mid n$ and $\pi_1(a_2) \in [0, \pi_2(a_2) - 1]$. Thus if n is not prime, the algorithm has ad-

ditional outer loops iterating through all a_1, a_2 which are possible after the application of such automorphisms.

Verifying (2) of Theorem 3 took 5 minutes. For (1), the total computation time (distributed on several computers) was 2 hours for all cases up to $n = 17$, 31 hours for $n = 19$, and 196 days kindly provided by the Rechenzentrum Universität Freiburg for $n = 23$. The "moreover" part ($n = 8, 9, 10$) took 4 minutes.

Acknowledgements. We would like to thank the Rechenzentrum Universität Freiburg for providing computing resources.

The second author was supported by the Agence Nationale de la Recherche (contract ANR-06-BLAN-0183-01) and by the Fondation Sciences mathématiques de Paris.

References

[1] N. Alon and M. Dubiner, *A lattice point problem and additive number theory*, Combinatorica 15 (1995), 301–309.

[2] P. C. Baayen, *Een combinatorisch probleem voor eindige Abelse groepen*, Colloq. Discrete Wiskunde Caput 3, Math. Centre, Amsterdam, 1968.

[3] G. Bhowmik, I. Halupczok and J.-C. Schlage-Puchta, *Inductive methods and zero-sum free sequences*, Integers 9 (2009), 515–536.

[4] —, —, —, *Zero-sum free sequences with small sum-set*, Math. Comp., to appear.

[5] G. Bhowmik and J.-C. Schlage-Puchta, *Davenport's constant for groups of the form* $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{3d}$, in: Additive Combinatorics, CRM Proc. Lecture Notes 43, Amer. Math. Soc., Providence, RI, 2007, 307–326.

[6] B. Bollobás and I. Leader, *The number of k-sums modulo k*, J. Number Theory 78 (1999), 27–35.

[7] 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.

[8] W. Gao and A. Geroldinger, *On the structure of zerofree sequences*, Combinatorica 18 (1998), 519–527.

[9] —, —, *On zero-sum sequences in* $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, Integers 3 (2003), A8, 45 pp.

[10] —, —, *Zero-sum problems and coverings by proper cosets*, Eur. J. Combin. 24 (2003), 531–549.

[11] W. Gao, A. Geroldinger and D. J. Grynkiewicz, *Inverse zero-sum problems III*, Acta Arith. 141 (2010), 103–152.

[12] W. Gao, A. Geroldinger and W. A. Schmid, *Inverse zero-sum problems*, ibid. 128 (2007), 245–279.

[13] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure Appl. Math. (Boca Raton) 278, Chapman & Hall/CRC, Boca Raton, FL, 2006.

[14] G. Lettl and W. A. Schmid, *Minimal zero-sum sequences in* $C_n \oplus C_n$, Eur. J. Combin. 28 (2007), 742–753.

[15] J. E. Olson, *An addition theorem modulo p*, J. Combin. Theory 5 (1968), 45–52.

[16] —, *A combinatorial problem on finite Abelian groups. II*, J. Number Theory 1 (1969), 195–199.

Gautami Bhowmik
Laboratoire Paul Painlevé
U.M.R. CNRS 8524
Université de Lille 1
59655 Villeneuve d'Ascq Cedex, France
E-mail: bhowmik@math.univ-lille1.fr

Jan-Christoph Schlage-Puchta
Department of Pure Mathematics and Computer Algebra
Universiteit Gent
Building S22, Krijgslaan 281
B-9000 Gent, Belgium
E-mail: jcsp@cage.ugent.be

Immanuel Halupczok
Institut für Mathematische Logik
und Grundlagenforschung
Universität Münster
Einsteinstraße 62
48149 Münster, Germany
E-mail: math@karimmi.de

Received on 27.11.2008
and in revised form on 4.11.2009 (5873)