

**An improvement on Olson's constant for  $\mathbb{Z}_p \oplus \mathbb{Z}_p$** 

by

GAUTAMI BHOWMIK (Lille) and  
JAN-CHRISTOPH SCHLAGE-PUCHTA (Freiburg)

**1. Introduction.** Let  $G$  be a finite additive abelian group of order  $n$ . A subset  $A$  of  $G$  is said to be a *zero-sum set* if the sum of all its elements is zero. *Olson's constant*  $\text{Ol}(G)$  of  $G$  is defined to be the smallest integer  $k$  such that every set of  $k$  elements of  $G$  contains a non-empty zero-sum subset.

The exact value of this constant is only known for a few cases. As far as bounds are concerned, Szemerédi [6] proved the Erdős–Heilbronn conjecture that  $\text{Ol}(G) \leq c\sqrt{n}$ ,  $c$  being an absolute constant. For cyclic groups, the conjectural value of  $c$  (due to Erdős and Graham)  $\sqrt{2}$  was recently attained by Nguyen, Szemerédi and Vu [4]. The conjecture was verified by Gao, Ruzsa and Thangadurai [2] for  $\mathbb{Z}_p \oplus \mathbb{Z}_p$  for all  $p > 4.67 \cdot 10^{34}$ . They in fact proved that  $\text{Ol}(\mathbb{Z}_p^2) = p - 1 + \text{Ol}(\mathbb{Z}_p)$  for such  $p$ . Our aim is to improve the bound for  $p$ , and we prove

**THEOREM 1.** *Let  $p > 6000$  be a prime number. Then  $\text{Ol}(\mathbb{Z}_p^2) = p - 1 + \text{Ol}(\mathbb{Z}_p)$ .*

Our proof falls into two parts, the first one being combinatorial and dealing with the case where the elements of  $A$  are not well-distributed over  $\mathbb{Z}_p^2$ , the second one being analytical, using exponential sums. Unfortunately, our bound is still too large to allow for explicit computations. Though our method could be used to lower the bound for  $p$  further, we would not be able to go below  $p < 200$ .

**2. Proof.** For a set  $A$ , we use  $\Sigma(A)$  for the set of all its subset sums while  $\Sigma_k(A)$  denotes the set of all sums of those subsets of  $A$  which have  $k$  elements. We may use the same notation for a multiset  $A$ , though even then  $\Sigma(A)$  would still be a set, that is, for example,  $\Sigma(\{1, 1, 5\}) = \{0, 1, 2, 5, 6, 7\}$ . We will use the fact that  $\text{Ol}(\mathbb{Z}_p) \geq \lfloor \sqrt{2p} \rfloor$  (see [3]).

The following is due to Dias da Silva and Hamidoune [1] which for the case  $k = 2$  was a conjecture of Erdős–Heilbronn.

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

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

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

LEMMA 2. *For  $A, B \subseteq \mathbb{Z}_p$  we have  $|A + B| \geq \min(p, |A| + |B| - 1)$ .*

The following result was proven by Olson [5, Theorem 2].

LEMMA 3. *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*

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

where

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

We will prove the following, which is slightly stronger than our initial claim.

THEOREM 2. *Let  $A \subseteq \mathbb{Z}_p^2$  be a zero-sum free set of size  $p - 2 + \text{Ol}(\mathbb{Z}_p)$ . Then there exists a subgroup  $U \cong \mathbb{Z}_p$  such that  $|A \cap U| = \text{Ol}(\mathbb{Z}_p) - 1$ , and all other elements of  $A$  are contained in one coset of  $U$ .*

Theorem 2 implies Theorem 1, since if  $A \subseteq \mathbb{Z}_p^2$  were a zero-sum free set with  $|A| = p - 1 + \text{Ol}(\mathbb{Z}_p)$ , then deleting one point we would obtain a set as described in Theorem 2. Hence, for each  $x \in A$  we see that  $A \setminus \{x\}$  is contained in one subgroup and one coset of this subgroup, both of which may depend on  $x$ . In particular, for  $\text{Ol}(\mathbb{Z}_p) > 2$ , that is,  $p \geq 5$ , there is a unique subgroup containing more than two elements, and there is a unique coset of this subgroup containing more than one element, hence the choice of the subgroup and the coset does not depend on  $x$ , that is,  $A$  itself is contained within one subgroup and a coset of this subgroup. But then  $A$  obviously has a zero-sum.

For the rest of the article we fix a set  $A$  of size  $p - 2 + \text{Ol}(\mathbb{Z}_p)$ , for which no subgroup  $U$  as in the above theorem exists.

Our aim now is to show that  $A$  contains a zero-sum.

For an affine subspace  $x + U$  and a set  $B$  we define  $N(x, U, B) = |B \cap (x + U)|$  and set  $M = M(A) = \max_{x, U} N(x, U, A)$ . For a subgroup  $U < \mathbb{Z}_p^2$  with  $|U| = p$ , we denote by  $\pi_U : \mathbb{Z}_p^2 \rightarrow \mathbb{Z}_p$  a surjection with kernel  $U$ . Note that this map is not unique but any such choice serves our purpose.

Similar to Gao, Ruzsa and Thangadurai we begin by reducing the size of  $M$ . On the one hand, the result below is slightly better than [2, Lemma 3.4]

and [2, Lemma 3.5], since here the set  $A$  under consideration is smaller in cardinality by 1; on the other hand, our bound on  $p$  is worse, for the sake of considerable simplification of the proof.

LEMMA 4. *Suppose that  $M \geq 2p/5$  and  $p > 100$ . Then  $A$  contains a zero-sum.*

*Proof.* Let  $U$  be a subgroup for which the maximum of  $N(x, U, A)$  is attained and set  $B = A \cap (x + U)$  and  $\ell = |A \cap U|$ . Let  $V$  be a subgroup with  $\langle U, V \rangle = \mathbb{Z}_p^2$ . We have  $M - 3 > p/3$  for all  $p > 45$ . Thus Lemma 1 shows that for  $3 \leq k \leq M - 3$ , we have  $\Sigma_k(\pi_V(B)) = \mathbb{Z}_p$ , hence if we can represent 0 as a subset sum of  $\pi_U(A)$  using between 3 and  $M - 3$  elements from  $B$ , then we can choose the elements in  $B$  in such a way that we obtain a zero-sum in  $\mathbb{Z}_p^2$ . In particular, if we can choose six points  $\{x_1, \dots, x_6\}$  from  $B$  such that  $\Sigma(\pi_U(A \setminus \{x_1, \dots, x_6\})) = \mathbb{Z}_p$ , we can construct a zero-sum in  $\pi_U(A)$  which contains  $x_1, x_2, x_3$  but not  $x_4, x_5, x_6$ . Then by suitably replacing certain points chosen in  $B$  we obtain a zero-sum in  $A$  using between 3 and  $M - 3$  elements in  $B$ . Set  $A' = A \setminus (U \cup \{x_1, \dots, x_6\})$ . Then  $|A'| = p + \text{Ol}(\mathbb{Z}_p) - 2 - (\ell + 6)$ . If  $\ell \geq \text{Ol}(\mathbb{Z}_p)$ , we already obtain a zero-sum in  $A \cap U$ , while for  $\ell \leq \text{Ol}(\mathbb{Z}_p) - 7$ , we find  $|A'| \geq p - 1$ , and we have  $\Sigma(\pi_U(A')) = \mathbb{Z}_p$ . Hence, we only have to consider the case  $\text{Ol}(\mathbb{Z}_p) - 6 \leq \ell \leq \text{Ol}(\mathbb{Z}_p) - 1$  and  $p - 7 \leq |A'| \leq p - 2$ .

Suppose that in  $\pi_U(A')$  we can find six pairs  $(x_i, y_i)$  such that  $x_i \neq \pm y_i$ . Then from Lemma 2 we obtain

$$\begin{aligned} & |\Sigma(\pi_U(A'))| \\ & \geq \min\left(p, |\Sigma(\pi_U(A') \setminus \{x_1, y_1, \dots, x_6, y_6\})| + \sum_{i=1}^6 (|\Sigma(\{x_i, y_i\})| - 1)\right) \\ & \geq \min(p, p - 18 + 6 \cdot 3) = p, \end{aligned}$$

and our claim follows in this case. If there are six elements in  $A'$  which are neither in  $x + U$  nor in  $-x + U$ , we can find such pairs by taking one such element and one element in  $B$ . If there are three elements in  $-x + U$ , we take three elements in  $-x + U \cap A$  and three in  $x + U \cap A$ , that is, we find a zero-sum in  $\pi_U(A)$  using three elements in  $B$ . Hence, it only remains to consider the case that there are at most two elements in  $A \cap (-x + U)$ , and at most five elements  $a \in A$  with  $\pi_U(a) \notin \{\pm x, 0\}$ , in particular,  $M \geq p - 8$ . If  $\pi_U(A)$  contains a zero-sum which uses some, but not all, elements of  $\pi_U(B)$ , we can obtain  $p - 8$  different elements in  $U$  as subset sums of  $A \setminus U$ . Since  $|A \cap U| \geq \text{Ol}(\mathbb{Z}_p) - 6 > 8$  for  $p > 100$ , one of these sums can be combined with some element in  $A \cap U$  to form a zero-sum. Since  $|A \setminus U| \geq p - 1$  the only possibility to avoid this situation is when all elements of  $A \setminus U$  are in one coset of  $U$ , but this situation was excluded from the outset. Hence, our claim follows in any case. ■

Hence, to prove Theorem 2 it suffices to show that for  $p \geq 6000$  any set  $A$  with  $|A| = p - 2 + \text{Ol}(\mathbb{Z}_p)$  and  $M < 2p/5$  contains a zero-sum.

The following is the main technical result of the combinatorial part.

LEMMA 5. *Let  $U$  be a non-trivial subgroup, and  $B \subseteq A$  a set. Let  $x_1, \dots, x_p$  be representatives of  $\mathbb{Z}_p^2/U$ . Suppose that the multi-set  $\pi_U(B)$  represents each element of  $\mathbb{Z}_p$  as a (possibly empty) subset sum, and that*

$$\sum_i [N(x_i, U, A \setminus B)/2][N(x_i, U, A \setminus B)/2] \geq p - 1.$$

*Then  $A$  contains a zero-sum.*

*Proof.* In each set  $(A \setminus B) \cap (x_i + U)$  we choose all subsets of size  $[N(x_i, U, A \setminus B)/2]$  and add them up. By Lemma 1 we obtain at least  $[N(x_i, U, A \setminus B)/2][N(x_i, U, A \setminus B)/2] + 1$  elements in  $\mathbb{Z}_p^2$  in this way, each of which has the same image under  $\pi_U$ . By Lemma 2 and the assumption we find that there exists some  $x$  such that every element of  $x + U$  is a subset sum of  $A \setminus B$ . On the other hand, there is a subset of  $B$  with sum contained in  $(-x) + U$ , hence we can combine a subset sum of  $B$  with a subset sum of  $A \setminus B$  to obtain a zero-sum. ■

Now we shall repeatedly apply this lemma to reduce the size of the numbers  $N(x, U, A)$ .

LEMMA 6. *Suppose that  $p > 120$  and  $2p/5 \geq M \geq \lfloor \sqrt{4p - 7} \rfloor + 1$ . Then  $A$  contains a zero-sum.*

*Proof.* Let  $U$  be a subgroup such that there exists some  $x$  with  $N(x, U, A) = M$ . We choose a set  $C$  of size  $\lfloor \sqrt{4p - 7} \rfloor + 1$  elements in one coset, and set  $B = A \setminus (C \cup \pi^{-1}(0))$ . Since  $U$  contains at most  $\text{Ol}(\mathbb{Z}_p) - 1$  elements, we have  $|B| \geq p - 2\sqrt{p} - 1$ . Consider the multi-set  $\overline{B} = \pi_U(B)$ . By assumption,  $\overline{B}$  contains no element with multiplicity  $\geq 2p/5$ , hence in  $\overline{B}$  we can find a system of  $p/5 - 2\sqrt{p} - 1$  disjoint subsets containing three different elements, that is, we find  $p/5 - 2\sqrt{p} - 1$  subsets containing two different elements which are not inverse to each other. We apply Lemma 3 to these pairs and obtain

$$\begin{aligned} p &\geq |\Sigma(\overline{B})| \geq \min(p, 3(p/5 - 2\sqrt{p} - 1) + p - 2(p/5 - 2\sqrt{p} - 1)) \\ &= \min(p, (6/5)p - 2\sqrt{p} - 1) = p, \end{aligned}$$

where we used  $p > 120$ . Hence, we can apply Lemma 5 to obtain our claim. ■

We now combine Lemma 5 with an estimate for exponential sums to obtain a criterion for our theorem to hold which is numerically applicable.

LEMMA 7. *Let  $p > 800$  be a prime number. Let  $A \subseteq \mathbb{Z}_p^2$  be a subset with  $|A| = p - 2 + \text{Ol}(\mathbb{Z}_p)$ . For a subgroup  $U \cong \mathbb{Z}_p$  fix a complement  $V$ , and define*

$\lambda_j^U = N(j, U, A)$ , where  $j$  is viewed as an element of  $V$  via the isomorphism  $\mathbb{Z}_p \cong V$ . Suppose that one of the following two conditions holds true.

- (1) There exists a subgroup  $U$  such that the following holds true. Denote by  $J$  the set of indices  $j$  such that  $\lambda_j$  is odd. Suppose there exists a set of integers  $I \subseteq \mathbb{Z}_p$ , disjoint from  $J$ , such that  $\lambda_i \geq 1$  for all  $i \in I$ ,  $\Sigma(I \cup J) = \mathbb{Z}_p$ , and  $\sum_i \lfloor \lambda_i^*/2 \rfloor \lceil \lambda_i^*/2 \rceil \geq p - 1$ , where

$$\lambda_i^* = \begin{cases} \lambda_i - 1, & i \in I, \\ \lambda_i, & \text{otherwise.} \end{cases}$$

- (2) For all subgroups  $U$  and all isomorphisms  $\mathbb{Z}_p \cong V$  we have the bound

$$\prod_{j=0}^{p-1} \left| \cos \frac{j\pi}{p} \right|^{\lambda_j} \leq \frac{1}{p^2}.$$

Then  $A$  contains a zero-sum.

*Proof.* We begin by proving that the first assumption is sufficient. The idea of the proof is to partition  $A$  into two subsets  $A_1, A_2$  such that  $\Sigma(A_1)$  contains a coset of  $U$ , while  $\pi_U(\Sigma(A_2)) = \mathbb{Z}_p$ . To achieve the first goal we consider not all subset sums of  $A_1$ , but only those which contain precisely  $\lfloor \lambda_i^*/2 \rfloor$  or  $\lfloor \lambda_i^*/2 \rfloor + 1$  summands in  $\pi_U^{-1}(U)$ .

More precisely, we set  $x = \sum i \lfloor \lambda_i^*/2 \rfloor$ . Since  $\Sigma(I) + \Sigma(J) = \mathbb{Z}_p$ , we can choose a subset of  $I \cup J$  adding up to  $-x$ ; let  $I', J'$  be the intersection of this set with  $I$  and  $J$ , respectively. Set  $C_k = \pi_U^{-1}(k) \cap A$  and, for every  $i \in I'$ , choose an element  $x_i \in C_i$ . If we choose subsets  $A_k \subseteq C_k$  with  $|A_k| = \lfloor \lambda_k^*/2 \rfloor$  for  $k \notin J'$ , and  $|A_k| = \lfloor \lambda_k^*/2 \rfloor + 1$  for  $k \in J'$ , and  $x_k \notin A_k$  for  $k \in I'$ , then

$$s = \sum_{i \in I'} x_i + \sum_{k=0}^{p-1} \sum_{a \in A_k} a$$

is an element in  $U$ . To prove that  $A$  contains a zero-sum, it suffices to show that by choosing the sets  $A_k$  in all possible ways, all elements in  $U$  can be obtained. The number of subset sums obtained by varying  $A_k$  depends on the index  $k$  as follows: For  $k \in J'$  this quantity is

$$|\Sigma_{\lfloor \lambda_k^*/2 \rfloor + 1}(C_k)| = |\Sigma_{\lceil \lambda_k^*/2 \rceil}(C_k)| = |\Sigma_{\lfloor \lambda_k^*/2 \rfloor}(C_k)|,$$

since for  $k \in J'$  we know that  $\lambda_k^*$  is odd. By Lemma 1 this quantity is bounded below by  $\lfloor \lambda_k^*/2 \rfloor \lceil \lambda_k^*/2 \rceil + 1$ . If  $k \in I'$ , the number of possible sums is now  $|\Sigma_{\lfloor \lambda_k^*/2 \rfloor}(C_k \setminus \{x_k\})|$ , which by the definition of  $\lambda_i^*$  has the same lower bound. If  $k$  is neither in  $I'$  nor in  $J'$ , we also obtain the same lower bound.

Applying the Cauchy–Davenport inequality we see that we obtain a zero-sum provided that  $\sum_k \lfloor \lambda_k^*/2 \rfloor \lceil \lambda_k^*/2 \rceil \geq p - 1$ . Thus, the first condition is sufficient.

Hence, we may assume that for each subgroup  $U$  the partition  $N(i, U, A)$  satisfies the second condition. Write  $e(x) = e^{2\pi ix/p}$ ; we view this as a function  $e : \mathbb{Z}_p \rightarrow \mathbb{C}$ . Then using orthogonality we see that the number of subsets of  $A$  adding up to 0 equals

$$\frac{1}{p^2} \sum_{\alpha \in \mathbb{Z}_p^2} \prod_{a \in A} 1 + e(\langle a, \alpha \rangle).$$

Clearly, the summand  $\alpha = 0$  contributes  $2^{|A|}/p^2$ . We have

$$\begin{aligned} \prod_{a \in A} |1 + e(\langle a, (0, 1) \rangle)| &= \prod_{j \in \mathbb{Z}_p} |1 + e(j)|^{N(j, \langle (0,1) \rangle, A)} \\ &= 2^{|A|} \prod_{j \in \mathbb{Z}_p} |\cos(\pi j/p)|^{N(j, \langle (0,1) \rangle, A)} \leq \frac{2^{|A|}}{p^2}, \end{aligned}$$

where in the last step we used the second condition. Hence, the number of zero-sums is bounded from below by

$$\frac{2^{|A|}}{p^2} - \frac{p^2 - 1}{p^2} \frac{2^{|A|}}{p^2} = \frac{2^{|A|}}{p^4} \geq 2$$

provided that  $p \geq 13$ , that is, there exists a non-empty subset with sum 0. ■

Note that the two conditions in the lemma work in different directions: While the first condition says that most of the  $\lambda_j$  are small, the second condition says that most of the weight of the partition lies on indices  $i$  which are close to 0 or to  $p$ . From this difference we shall obtain our result.

LEMMA 8. *Suppose that  $p > 1024$  and that there exists a subgroup  $U$  such that the image  $\pi_U(A)$  of the projection has fewer than  $p/5$  elements. Then  $A$  contains a zero-sum.*

*Proof.* We distinguish two cases, depending on the size of  $\pi_U(A)$ . Assume first that  $|\pi_U(A)| \geq \sqrt{4p - 7}$ . Then we take for  $B$  an arbitrary set of size  $\lfloor \sqrt{4p - 7} \rfloor$  such that no two elements of  $B$  map to the same element under  $\pi_U$ . Then  $|A \setminus B| \geq p - \sqrt{p}$ . Set  $f(\ell) = \lfloor \ell/2 \rfloor \lceil \ell/2 \rceil$ . Using the convexity of the function  $f$  it can be established that  $\sum_x f(N(x, U, A \setminus B)) \geq p$  and we can apply Lemma 5. In fact, we have

$$\sum_x f(N(x, U, A \setminus B)) \geq \frac{f(5)}{5} |A \setminus B| = \frac{6}{5} |A \setminus B|,$$

and we consider the minimum of  $\sum_{i=1}^k f(n_i)$ , where the  $n_i$  are natural numbers. We can assume that  $\sum n_i = p - \lfloor \sqrt{p} \rfloor$  and  $k = \lfloor p/5 \rfloor$ . Suppose there is some  $j$  with  $n_j \leq n_i - 2$ . Then if we increase  $n_j$  by 1, and decrease  $n_i$  by 1,

the sum changes by

$$f(n_j + 1) - f(n_j) - f(n_i) + f(n_i - 1) = \left\lfloor \frac{n_j + 1}{2} \right\rfloor - \left\lfloor \frac{n_i}{2} \right\rfloor \leq 0.$$

Thus, for the tuple realizing the minimum we may assume  $|n_i - n_j| \leq 1$  for all  $i, j$ . Note that for  $p > 25$  there is some  $i$  with  $n_i \geq 5$ , and therefore we have  $n_i \geq 4$  for all  $i$ . If  $n_i \geq 5$  for all  $i$  we would have  $p - \lfloor \sqrt{p} \rfloor \leq 5 \cdot p/5$ , which is absurd, and we conclude that  $n_i \in \{4, 5\}$  for all  $i$ , and that there are  $\lceil \sqrt{p} \rceil$  sets of size 4, and  $\lfloor p/5 \rfloor - \lceil \sqrt{p} \rceil$  sets of size 5. Hence the sum is bounded below by

$$\lceil \sqrt{p} \rceil f(4) + (\lfloor p/5 \rfloor - \lceil \sqrt{p} \rceil) f(5) \geq 4\sqrt{p} + \frac{6p}{5} - 6\sqrt{p} - 16 \geq p$$

provided that  $p > 1000$ .

In the second case there are  $p/2$  elements in  $A$  contained in pre-images of  $\pi_U$  of single points, which contain  $\sqrt{p}/4$  elements. Let  $B$  be the complement of this set. Again from convexity we see that  $\sum_x f(N(x, U, A \setminus B)) \geq p$  provided that  $\sqrt{p}/4 \geq 8$ , which is the case for  $p > 1024$ . On the other hand, the remaining points may be partitioned into sets containing  $p/2$  elements altogether, and no  $2\sqrt{p}$  have the same image under  $\pi_U$ , hence we see that  $\Sigma(\pi_U(B)) = \mathbb{Z}_p$  as well. ■

LEMMA 9. *Suppose that  $p > 6000$ . Then  $A$  contains a zero-sum.*

*Proof.* By the previous lemma we can select  $\lceil p/5 \rceil$  elements with different values under  $\pi_U$ . It suffices to show that the second condition of Lemma 7 is satisfied for each set consisting of  $\lceil p/5 \rceil$  different elements. Of course, the product over  $\lceil p/5 \rceil$  different factors of the form  $|\cos(j\pi/p)|$  becomes smallest if the relevant values of  $j$  form an interval around 0, which is as symmetric as possible, that is, of the form  $[-x, y]$  with  $|x - y| \leq 1$ . In this case there are at least  $p/10 - 1$  positive and at least that many negative values of  $j$ , hence, the product in question is at most

$$\prod_{- \lceil p/10 \rceil + 1}^{\lceil p/10 \rceil - 1} \cos(j\pi/p).$$

To facilitate the computations, we take logarithms and replace the occurring sum by an integral. For  $n > 0$  we have

$$\int_{n-1}^n \log \cos(t\pi/p) dt > \log \cos(n\pi/p),$$

while for  $n < 0$  we have

$$\int_n^{n+1} \log \cos(t\pi/p) dt > \log \cos(n\pi/p),$$

hence we obtain

$$\begin{aligned} \log \prod_{j=-\lceil p/10 \rceil + 1}^{\lfloor p/10 \rfloor - 1} \cos(j\pi/p) &< \int_{-p/10+1}^{p/10-1} \log \cos(t\pi/p) dt \\ &< p \int_{-1/10}^{1/10} \log \cos(t\pi) dt - 2 \log \cos \frac{\pi}{10} \\ &< -0.00332296p + 0.1004. \end{aligned}$$

Hence, our claim follows provided that  $1.1057p^2 < 1.003328^p$ , which is the case for  $p > 6000$ . ■

There are several obvious ways to improve the argument. First,  $p/5$  in Lemma 8 can be improved though not beyond  $p/4$ . Then,  $1/p^2$  in the second condition of Lemma 7 can be improved since the exponential sum will have a smaller value most of the time. However, it will be difficult to ensure that for some subgroup there will be no large term, that is, we do not expect to obtain anything better than  $1/p$ . Finally, one could consider the set of all partitions explicitly in the second part of Lemma 7; the improvement here would certainly be smaller than the bound obtained by taking  $p/4$  elements four times each. However, none of these improvements are completely straightforward, and even if we suppose that the technical difficulties could be overcome, our method cannot reach  $p < 200$  and 200 is already way beyond our current computational means. Moreover, the technicalities would certainly require very long arguments and this is particularly true for the enumeration of all partitions of  $p$ . Therefore we did not attempt to push our method to its limits. We did, however, formulate Lemma 7 in a way more general than we actually needed, to help possible improvements.

**Acknowledgments.** We are grateful for the very detailed and helpful comments of the referee.

### References

- [1] 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.
- [2] W. D. Gao, I. Ruzsa and R. Thangadurai, *Olson’s constant for the group  $\mathbb{Z}_p \oplus \mathbb{Z}_p$* , J. Combin. Theory Ser. A 107 (2004), 49–67.
- [3] Y. O. Hamidoune and G. Zémor, *On zero-free subset sums*, Acta Arith. 78 (1996), 143–152.
- [4] H. H. Nguyen, E. Szemerédi and V. H. Vu, *Subset sums modulo a prime*, ibid. 131 (2008), 303–316.
- [5] J. E. Olson, *An addition theorem modulo  $p$* , J. Combin. Theory 5 (1968), 45–52.



- [6] E. Szemerédi, *On a conjecture of Erdős and Heilbronn*, Acta Arith. 17 (1970), 227–229.

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

Jan-Christoph Schlage-Puchta  
Mathematisches Institut  
Albert-Ludwigs-Universität  
Eckerstr. 1  
79104 Freiburg, Germany  
E-mail: jcp@math.uni-freiburg.de

*Received on 14.5.2008  
and in revised form on 12.10.2009*

(5706)