Combinatorics, Probability and Computing (1998) 7, 81–87. Printed in the United Kingdom
© 1998 Cambridge University Press

Adding Distinct Congruence Classes

Y. O. HAMIDOUNE

Université P. et M. Curie, E. Combinatoire, Case 189,
4 Place Jussieu, 75005 Paris, France
(e-mail: yha@ccr.jussieu.fr)

Received 4 October 1995; revised 14 February 1997

Let S be a generating subset of a cyclic group G such that $0 \notin S$ and $|S| \geqslant 5$. We show that the number of sums of the subsets of S is at least $\min(|G|, 2|S|)$. Our bound is best possible. We obtain similar results for abelian groups and mention the generalization to nonabelian groups.

1. Introduction

Let G be an abelian group and let $a_1, \ldots, a_k$ be distinct elements of G such that $0 \neq \sum_{i \in J} a_i$, for every nonempty subset $J \subset [1,k]$. Improving a bound of Eggleton and Erdős, Szemerédi proved in [10] that there are $k^2/100$ distinct sums in the family $\{\sum_{i \in J} a_i ; J \subset [1,k]\}$. Olson showed in [9] that this result holds with 100 replaced by 9. Notice that Olson's result holds for nonabelian groups if one allows reordering of the sequence elements (*cf.* [9]).

In the nonabelian case, White obtained the following result in [11].

- Let $a_1, \ldots, a_k$ be distinct elements of a noncyclic nondihedral group G having no nonempty subsequence with product $= 1$. Then there are $\min(|G| - 1, 2k)$ distinct elements in the family $\{\prod_{i \in J} a_{(i)} ; J \subset [1,k]\}$.

As far as we are aware, no good estimate is known for the number of subset sums in the general case. We obtain here a best possible one.

Our main results, proved using Olson's methods [8, 9], are the following.

- Let S be a generating subset of a cyclic group G such that $0 \notin S$ and $|S| \geqslant 5$. Then the number of sums of the subsets of S is at least $\min(|G|, 2|S|)$.
- Let S be a generating subset of an abelian group G such that $0 \notin S$ and $|S| \geqslant 5$. Then the number of sums of the subsets of S is at least $\min(|G| - 1, 2|S|)$.

https://doi.org/10.1017/S0963548397003180 Published online by Cambridge University Press

This bound is attained as shown by the following example.

- Let $k \geqslant 3$ be an integer and set $n = 3k$. Let S be the set of the congruence classes of the integers $1, 3, 6, \ldots, 3(k-1) \pmod{n}$. The number of distinct sums of the subsets of S is clearly $2|S|$.

In the nonabelian case, we obtain the bound proved by White if one allows reordering of the elements of the sequence without the assumption that the product of every nonempty subsequence is $\neq 1$.

Better bounds are known in a prime order, where there are estimates of the number of sums of the subsets with a given cardinality. We mention below the existing results.

Let p be a prime and let $A \subset \mathbb{Z}_p$. It was proved in [2] that the set of sums of the j-subsets of A has cardinality $\geqslant \min(p, j(|A| - j) + 1)$. The case $j = 2$ of this result solves a conjecture of Erdős and Heilbronn [4]. An easier proof is contained in [1].

The above example shows that such a formula could not hold for composite numbers. However, we have the following conjecture.

Conjecture 1.1. Let $n \geqslant k$ be natural numbers and let $A \subset \mathbb{Z}_n \setminus 0$ such that $|A| \geqslant (n-1)/k + k - 1$. Then $0 \in \bigcup_{2 \leqslant j \leqslant k} j \wedge A$.

The case $k = 2$ of this conjecture is easy, since in this case $|A| \geqslant (n+1)/2$. It follows by a counting argument that A must contain a 2-subset with sum $= 0$.

2. Preliminaries

Recall the following well-known lemma.

Lemma 2.1. [7] *Let A, B be subsets of a finite group such that $|A| + |B| \geqslant |G| + 1$. Then $A + B = G$.*

Let G be an abelian group and let A be a finite subset of G; we write

$$\Sigma(A) = \left\{ \sum_{x \in T} x \mid T \subset A \right\}.$$

Set $A = \{a_1, \ldots, a_j\}$. Clearly $\Sigma(A) = \{0, a_1\} + \cdots + \{0, a_j\}$. Let G be an abelian group, $B \subset G$ a subset of G and $x \in G$. Following Olson, define:

$$\lambda_B(x) = |(B + x) \cap \overline{B}|.$$

We use the following lemma.

Lemma 2.2. [8, 9] *For any B, x, we have*

$$\lambda_B(x) = \lambda_{\overline{B}}(x).$$

https://doi.org/10.1017/S0963548397003180 Published online by Cambridge University Press

Let $B = \Sigma(S)$. For every $y \in S$, we have

$$|\Sigma(S)| \geqslant |\Sigma(S \setminus y)| + \lambda_B(y). \tag{2.1}$$

As a main tool we use the following result of Olson.

Proposition 2.3. [9] *Let B and S be subsets of G such that $0 \notin S$ and $G = \langle S \rangle$. If $1 \leqslant |B| \leqslant |\overline{B}|$, then there exists $x \in S$ such that*

$$\lambda_B(x) \geqslant \min((|B|+1)/2, (|S|+2)/4). \tag{2.2}$$

From this result we shall deduce the following one.

Corollary 2.4. *Let S be a generating subset of an abelian group G such that $0 \notin S$ and $|S| \geqslant 3$. Set $B = \Sigma(S)$ and suppose $2 \leqslant |B| \leqslant |G| - 2$. There exists $x \in S$ such that $\lambda_B(x) \geqslant 2$.*

Proof. By Lemma 2.2, we may assume $|B| \leqslant |\overline{B}|$. By (2.2), we have

$$\lambda_B(x) \geqslant \min((|B|+1)/2, (|S|+2)/4) \geqslant \min(3/2, 5/4). \qquad \square$$

3. Big subsets

In this section we shall generalize Lemma 2.1 to subset sum in cyclic groups.

Let A, B be subsets of an abelian group G. We shall write

$$A \wedge B = \{x + y \mid x \in A \ \& \ y \in B \ \& \ x \neq y\}.$$

As usual, we shall write $2 \wedge A = A \wedge A$.

We also recall a lemma from [6], which is the analogue of Lemma 2.1: for an integer m, put $\epsilon(m) = 0$, if m is odd and $\epsilon(m) = 1$ if m is even.

Lemma 3.1. *Let A, B be subsets of $\mathbb{Z}_m$ such that $|A|+|B| \geqslant m+2+\epsilon(m)$. Then $A \wedge B = \mathbb{Z}_m$.*

Proof. Suppose the contrary and take $a \in \mathbb{Z}_m \setminus (A \wedge B)$. Let $X = \{x : a = 2x\}$. Clearly $|X| \leqslant \epsilon(m) + 1$. Take $X = X_1 \cup X_2$, where $0 \leqslant |X_1|, |X_2| \leqslant 1$. By Lemma 2.1, $a \in (A \setminus X_1) + (B \setminus X_2)$. It follows that $a \in A \wedge B$, a contradiction. $\square$

Notice that the above lemma is best possible. In fact, one may choose A as the set of congruence classes of the integers $\{0, 1, \ldots, [m/2]\}$. In this case the congruence class of $0 \notin A \wedge A$.

Lemma 3.2. *Let A, B be subsets of an abelian finite group G with odd order such that $|A| + |B| \geqslant |G| + 2$. Then $A \wedge B = G$.*

The proof is similar to the one above. $\square$

https://doi.org/10.1017/S0963548397003180 Published online by Cambridge University Press

Notice also that Lemma 3.2 fails for groups with even order. In fact, one may take $V = \mathbb{Z}_2^n$. Clearly $0 \notin V \wedge V$.

Lemma 3.3. *Let A be a subset of $\mathbb{Z}_m \setminus 0$ such that $2|A| \geqslant m$. Then $A \cup (2 \wedge A) = \mathbb{Z}_m$.*

Proof. The proof is by induction, the result being obvious for $m \leqslant 2$. Suppose the result is proved for all $m' < m$.

Consider first the case where m is odd. We clearly have $|A| \geqslant (m+1)/2$. Set $A' = A \cup \{0\}$. By Lemma 3.1, $A \wedge A' = \mathbb{Z}_m$. Hence $A \cup 2 \wedge A = \mathbb{Z}_m$.

Now, suppose m is even. Let H be the subgroup of order $m/2$. Put $A_0 = A \cap H$ and $A_1 = A \setminus H$. Since $0 \notin A$, we have $A_1 \neq \emptyset$. Choose $a \in A_1$. We may assume $A \neq A_1$, since otherwise $A = a + H$, and hence $\mathbb{Z}_m = A \cup 2 \wedge A$.

By Lemma 2.1, $A_1 + H = (\{0\} \cup A_0) + A_1 \subset A \cup 2 \wedge A$.

It remains to show that $H \subset A \cup 2 \wedge A$. This follows by induction if $|A_0| \geqslant |H|/2$. If we assume the contrary, it follows that $|A_1| > |H|/2$.

Consider first the case where $|H|$ is odd. We have $|A_1| \geqslant (|H| + 1)/2$. By Lemma 3.1, $(A_1 - a) \wedge (A_1 - a \cup \{0\}) = H$. Hence $((A_1 - a) \wedge (A_1 - a)) \cup (A_1 \setminus a) = H$. It follows that $A_1 \wedge A_1 \cup ((A_1 \setminus a) + a) = H$. In this case we have $H \subset 2 \wedge A$.

Now assume that $|H|$ is even. We have in this case $|A| \geqslant |H|/2 + 1$. Let $B_1 = A_1 \setminus a$. By the induction hypothesis $(B_1 - a) \cup (2 \wedge (B_1 - a)) = H$. It follows that $(B_1 + a) \cup (2 \wedge B_1) = H + 2a = H$. □

4. Subset sums

Let us prove a weaker bound which is reached only for subsets with size $\leqslant 4$.

Lemma 4.1. *Let G be an abelian group of order n and let S be a generating subset of G such that $0 \notin S$ and $|S| \geqslant 5$. Then $|\Sigma(S)| \geqslant \min(|G| - 1, 2|S| - 1)$.*

Proof. The proof is by induction on $|G|$, the result being obvious for $|S| \leqslant 2$. Put $|G| = n$, $B = \Sigma(S)$ and suppose $|B| \leqslant n - 2$. We clearly have $2 \leqslant |B| \leqslant n - 2$. By Corollary 2.4, there exists $x \in S$ such that $\lambda_B(x) \geqslant 2$.

Assume $|S| \geqslant 3$. Consider first the case $G \neq \langle S' \rangle$, where $S' = S \setminus x$. By (2.1), $|\Sigma(S)| = |\Sigma(S') \cup (x + \Sigma(S'))| = 2|\Sigma(S')| \geqslant \min(2|\langle S' \rangle| - 2, 4|S| - 4)$. The result clearly holds unless $S' \cup \{0\}$ is a subgroup. But in this last case $|\Sigma(S')| = |S|$. Now $|\Sigma(S)| = |\Sigma(S') \cup (x + \Sigma(S'))| = 2|\Sigma(S')| = 2|S|$.

Assume now that $G = \langle S' \rangle$. By (2.1), we have $|\Sigma(S)| \geqslant |\Sigma(S')| + \lambda(x) \geqslant 2|S| - 3 + 2 = 2|S| - 1$. □

We use the following easy lemma for $|B| \leqslant 7$.

Lemma 4.2. *Let B be a subset of G which is an arithmetic progression with difference d such that $3 \leqslant |B| \leqslant |\langle d \rangle| - 3$. Then $\lambda_B(x) \geqslant 3$ for every $x \notin \{-2d, -d, 0, d, 2d\}$.*

https://doi.org/10.1017/S0963548397003180 Published online by Cambridge University Press

Proof. In order that the two arithmetic progressions B and $x + B$ have an intersection $\geqslant |B| - 2$, one clearly needs $x \in \{-2d, -d, 0, d, 2d\}$. □

Lemma 4.3. *Let G be an abelian group of order n. Let S be a generating subset of G such that $0 \notin S$ and $|S| = 3$.*

Then one of the following conditions holds:

(i) *there is an element a such that $S = \{-a, a, 2a\}$*
(ii) $|\Sigma(S)| \geqslant \min(|G| - 1, 6)$.

Proof. Set $B = \Sigma(S)$ and suppose $|B| \leqslant n - 2$. We clearly have $2 \leqslant |B| \leqslant n - 2$. By Corollary 2.4, there exists $x \in S$ such that $\lambda_B(x) \geqslant 2$.

Consider first the case $G \neq \langle S' \rangle$, where $S' = S \setminus x$. By (2.1) and Lemma 4.1, $|\Sigma(S)| = |\Sigma(S') \cup (x + \Sigma(S'))| = 2|\Sigma(S')| \geqslant \min(2|\langle S' \rangle| - 2, 6)$.

In this case (i) holds unless $S' \cup \{0\}$ is a subgroup. But in this last case $|\Sigma(S')| = 3$. Now $|\Sigma(S)| = |\Sigma(S') \cup (x + \Sigma(S'))| = 2|\Sigma(S')| = 6$.

Now assume that $G = \langle S' \rangle$. By (2.1), we have $|\Sigma(S)| \geqslant |\Sigma(S')| + \lambda(x) \geqslant 2 + |\Sigma(S')|$.

Now (ii) holds unless $\lambda(x) = 2$ and $|\Sigma(S')| = 3$. It follows that $S' = \{-b, b\}$, for some b. In particular, $\Sigma(S') = \{-b, 0, b\}$. The condition $\lambda(x) = 2$ forces $x = -b$ or $x = b$. In this case we clearly have (i). □

Lemma 4.4. *Let G be an abelian group of order n. Let S be a generating subset of G such that $0 \notin S$ and $|S| = 4$. Then one of the following conditions holds:*

(i) *there is an element a such that $S = \{-2a, -a, a, 2a\}$*
(ii) $|\Sigma(S)| \geqslant \min(|G| - 1, 8)$.

Proof. Set $B = \Sigma(S)$ and suppose $|B| \leqslant n - 2$. We clearly have $2 \leqslant |B| \leqslant n - 2$. By Corollary 2.4, there exists $x \in S$ such that $\lambda_B(x) \geqslant 2$.

Consider first the case $G \neq \langle S' \rangle$, where $S' = S \setminus x$. By (2.1) and Lemma 4.1, $|\Sigma(S)| = |\Sigma(S') \cup (x + \Sigma(S'))| = 2|\Sigma(S')| \geqslant \min(2|\langle S' \rangle| - 2, 10)$.

In this case (i) holds unless $S' \cup \{0\}$ is a subgroup. But in this last case $|\Sigma(S')| = 4$. Now $|\Sigma(S)| = |\Sigma(S') \cup (x + \Sigma(S'))| = 2|\Sigma(S')| = 8$.

Assume now that $G = \langle S' \rangle$. By (2.1), we have $|\Sigma(S)| \geqslant |\Sigma(S')| + \lambda(x) \geqslant 2 + |\Sigma(S')|$.

Now (ii) holds unless $\lambda(x) = 2$ and $|\Sigma(S')| = 5$. It follows by Lemma 4.4 that $S' = \{-b, b, 2b\}$, for some b. In particular, $\Sigma(S') = \{-b, 0, b, 2b, 3b\}$. The condition $\lambda(x) = 2$ forces $x = -2b$. In this case we clearly have (i). □

Lemma 4.5. *Let G be an abelian group of order n. Let S be a generating subset of G such that $0 \notin S$ and $|S| = 5$. Then $|\Sigma(S)| \geqslant \min(|G| - 1, 10)$.*

Proof. Set $B = \Sigma(S)$ and suppose $|B| \leqslant n - 2$. We clearly have $2 \leqslant |B| \leqslant n - 2$. By Corollary 2.4, there exists $x \in S$ such that $\lambda_B(x) \geqslant 2$.

Consider first the case $G \neq \langle S' \rangle$, where $S' = S \setminus x$. By (2.1) and Lemma 4.1, $|\Sigma(S)| = |\Sigma(S') \cup (x + \Sigma(S'))| = 2|\Sigma(S')| \geqslant \min(2|\langle S' \rangle| - 2, 10)$.

https://doi.org/10.1017/S0963548397003180 Published online by Cambridge University Press

In this case (i) holds unless $S' \cup \{0\}$ is a subgroup. But in this last case $|\Sigma(S')| = 5$. Now $|\Sigma(S)| = |\Sigma(S') \cup (x + \Sigma(S'))| = 2|\Sigma(S')| = 10$.

Now assume that $G = \langle S' \rangle$. By (2.1), we have $|\Sigma(S)| \geqslant |\Sigma(S')| + \lambda(x) \geqslant 2 + |\Sigma(S')|$.

Now the result holds unless $|\Sigma(S')| = 5$. By Lemma 4.4, it follows that, for some b, $S' = \{-2b, -b, b, 2b\}$. In particular, $\Sigma(S') = \{-3b, -2b, -b, 0, b, 2b, 3b\}$. In this case we may easily see that $\lambda(x) \geqslant 3$ (of course, this follows by Lemma 4.2). □

Theorem 4.6. *Let G be an abelian group of order n and let S be a generating subset of G such that $0 \notin S$ and $|S| \geqslant 5$. Then $|\Sigma(S)| \geqslant \min(|G| - 1, 2|S|)$.*

Proof. The proof is by induction on $|G|$, the result being true for $|S| = 5$, by Lemma 4.5. Set $B = \Sigma(S)$ and suppose $|B| \leqslant n - 2$. We clearly have $2 \leqslant |B| \leqslant n - 2$. By Corollary 2.4, there exists $x \in S$ such that $\lambda_B(x) \geqslant 2$.

Consider first the case $G \neq \langle S' \rangle$, where $S' = S \setminus x$. By (2.1) and Lemma 4.1, $|\Sigma(S)| = |\Sigma(S') \cup (x + \Sigma(S'))| = 2|\Sigma(S')| \geqslant \min(2|\langle S' \rangle| - 2, 2(2|S| - 3))$.

The result clearly holds unless $S' \cup \{0\}$ is a subgroup. But in this last case $|\Sigma(S')| = |S|$. Now $|\Sigma(S)| = |\Sigma(S') \cup (x + \Sigma(S'))| = 2|\Sigma(S')| = 2|S|$.

Now assume that $G = \langle S' \rangle$. By the induction hypothesis and (2.1), we have $|\Sigma(S)| \geqslant |\Sigma(S')| + \lambda(x) \geqslant (2|S| - 2) + 2 = 2|S|$. □

For cyclic groups, we have the following theorem.

Theorem 4.7. *Let S be a generating subset of a cyclic group G such that $0 \notin S$ and $|S| \geqslant 5$. Then $|\Sigma(S)| \geqslant \min(|G|, 2|S|)$.*

Proof. This follows by Theorem 4.6 for $2|S| \leqslant |G| - 1$. Suppose $2|S| \geqslant |G|$. By Lemma 3.3, $|\Sigma(S)| = |G|$. □

In the case of nonabelian groups, the reader could adapt the above methods to show the following theorem.

Theorem 4.8. *Let G be a noncyclic multiplicative group. Let $a_1, \ldots, a_k$ be distinct elements $G \setminus 1$. Then there is a permutation σ of $[1, k]$ such that $|\{1, a_{\sigma(1)}\} \cdots \{1, a_{\sigma(k)}\}| \geqslant \min(|G| - 1, 2k)$.*

The proof in the abelian case works with almost no change, since Olson's results also hold for nonabelian groups.

References

[1] Alon, N., Nathanson, M. B. and Rusza, I. (1996) The polynomial method and restricted sums of congruence classes. *J. Number Theory* **56**(2) 404–417.

[2] Dias da Silva, J. A. and Hamidoune, Y. O. (1994) Cyclic subspaces of Grassmann derivations. *Bull. London Math. Soc.* **26** 140–146.

https://doi.org/10.1017/S0963548397003180 Published online by Cambridge University Press

[3] Eggleton, R. B. and Erdős, P. (1972) Two combinatorial problems in group theory. *Acta Arith.* **21** 112–116.
[4] Erdős, P. and Graham, R. (1980) Old and new problems and results in combinatorial number theory. *L'Enseignement Mathématique* **28** 1–128.
[5] Erdős, P. and Heilbronn, H. (1964) On the addition of residue classes mod *p*. *Acta Arith.* **9** 149–159.
[6] Hamidoune, Y. O. (1995) On inverse additive problems. Report IBP (Univ. Paris 6), EC 95/01.
[7] Mann, H. B. (1976) *Addition Theorems*, 2nd edn. Krieger, New York.
[8] Olson, J. E. (1968) An addition theorem mod *p*. *J. Combin. Theory* **5** 45–52.
[9] Olson, J. E. (1975) Sum of sets of group elements. *Acta Arith.* **28** 147–156.
[10] Szemerédi, E. (1970) On a conjecture of Erdős and H. Heilbronn. *Acta Arith.* **17** 227–229.
[11] White, E. T. (1978) Ordered sums of group elements. *J. Combin. Theory, Ser. A* **24** 118–121.

https://doi.org/10.1017/S0963548397003180 Published online by Cambridge University Press