Exhaustion Numbers of Subsets of Abelian Groups

A. Y. M. Chin

Institute of Mathematical Sciences
Faculty of Science
University of Malaya
50603 Kuala Lumpur
Malaysia
E-mail: acym@mnt.math.um.edu.my

Abstract

Let G be a finite group written additively and S a non-empty subset of G. We say that S is *e-exhaustive* if $G = S+\cdots+S$ (e times). The minimal integer $e > 0$, if it exists, such that S is e-exhaustive, is called the *exhaustion number* of the set S and is denoted by $e(S)$. In this paper we completely determine the exhaustion numbers of subsets of Abelian groups which are in arithmetic progression. The exhaustion numbers of various subsets of Abelian groups which are not in arithmetic progression are also determined.

Keywords: exhaustion number, Abelian group, arithmetic progression.

ARS COMBINATORIA 68(2003), pp. 65-76

1 Introduction

Let G be a finite group written additively. For any non-empty subset S of G, we say that S is *e-exhaustive* if G is 'covered' by the sum of e copies of S, that is,

$$G = S + \cdots + S \quad (e \text{ times}).$$

For convenience, we shall use S^{+e} to denote $S + \cdots + S$ (e times). The minimal integer $e > 0$, if it exists, such that S is e-exhaustive, is called the *exhaustion number* of the set S and is denoted by $e(S)$. If such $e > 0$ does not exist, we say that the exhaustion number of the set S is infinite and write $e(S) = \infty$. If $e(S)$ is finite, then we say that S is *exhaustive* in G. Clearly if S is e-exhaustive, then it is also e'-exhaustive for any $e' > e$. It is also clear that if S is exhaustive in G then $S \not\subseteq H$ for any proper subgroup H of G.

It is of interest to note that the 'covers' discussed in this paper are somewhat analogous to the more well-known covers of finite sets in the literature (see [2] for example): A *cover* of a set T is a collection of non-empty subsets of T, the union of which is T; a cover is said to be *minimal* if none of its proper subsets covers T. A cover of a finite group G as discussed in this paper can be considered as a collection of non-empty subsets of G, the sum of which is G. A cover of G is then said to be minimal if none of its proper subsets covers G.

In this paper we are interested in 'covering' a finite Abelian group G by as few sum of copies of the same subset of G as possible. To be more precise, we shall determine the exhaustion numbers of various subsets of Abelian groups. The layout of this paper is as follows: In Section 2 we determine the exhaustion numbers of subsets of cyclic groups which are in arithmetic progression. Using this result, we then determine in Section 3 the exhaustion numbers of subsets (in arithmetic progression) of finite Abelian groups which are direct sums of the cyclic groups $\mathbb{Z}/m_1, \ldots, \mathbb{Z}/m_n$ where the m_i are relatively

prime. We also show that in the case where the m_i are not relatively prime, subsets of $\mathbb{Z}/m_1 \oplus \cdots \oplus \mathbb{Z}/m_n$ which are in arithmetic progression are not exhaustive. In Section 4 we consider subsets of the cyclic group $\mathbb{Z}/p$, where p is an odd prime. Using a result from additive number theory, we obtain upper bounds for the exhaustion numbers of subsets of $\mathbb{Z}/p$. We also determine the exhaustion numbers of subsets S of $\mathbb{Z}/p$ which are obtained from arithmetic progressions of size $|S|+1$.

Throughout this paper we shall use the notation $\lceil x \rceil$ to mean the smallest integer $\geq x$. We shall also use the notation $[x]$ to mean the largest integer $\leq x$. Clearly, $\lceil x \rceil = [x] + 1$ if x is not an integer.

2 Exhaustion numbers of subsets of $\mathbb{Z}/m$, $m \geq 2$ which are in arithmetic progression

We first prove the following lemma:

Lemma 2.1 *Let m and s be positive integers with $s \geq 2$. If $s-1$ does not divide $m-1$, then*

$$m \leq \left\lceil \frac{m-1}{s-1} \right\rceil (s-1) + 1 \leq m + (s-2).$$

Proof: Since $s-1$ does not divide $m-1$, we may write $\left\lceil \frac{m-1}{s-1} \right\rceil = \left[\frac{m-1}{s-1} \right] + 1$. Suppose that $\left(\left[\frac{m-1}{s-1} \right] + 1 \right)(s-1) + 1 < m$. Then

$$\left[\frac{m-1}{s-1} \right] (s-1) < m - s$$

and hence

$$\left[\frac{m-1}{s-1} \right] < \frac{m-s}{s-1} = \frac{m-1}{s-1} - 1,$$

which is not possible. Therefore $\left(\left[\frac{m-1}{s-1} \right] + 1 \right)(s-1) + 1 \geq m$.

Now suppose that $\left(\left[\frac{m-1}{s-1}\right]+1\right)(s-1)+1 \geq m+(s-1)$. Then

$$\left[\frac{m-1}{s-1}\right](s-1) \geq m-1$$

and hence

$$\left[\frac{m-1}{s-1}\right] \geq \frac{m-1}{s-1},$$

which is not possible. We thus have $\left(\left[\frac{m-1}{s-1}\right]+1\right)(s-1)+1 \leq m+(s-2)$. □

Theorem 2.2 *Let $S \subseteq \mathbb{Z}/m$, $m \geq 2$ with $s = |S| > 1$. If S is in arithmetic progression with difference d relatively prime to m, then*

$$e(S) = \left[\frac{m-1}{s-1}\right].$$

If S is in arithmetic progression with difference d not relatively prime to m, then $e(S) = \infty$.

Proof: Let $S = \{a, a+d, a+2d, \ldots, a+(s-1)d\}$. By induction, it can be shown that for any positive integer k, the first term in the (multi)set S^{+k} is ka while the last term is $ka + k(s-1)d$. Suppose first that $s-1$ divides $m-1$ and let $e = \frac{m-1}{s-1}$. Then

$$e(s-1)d + d = (m-1)d + d = md \equiv 0 \pmod{m}$$

and it follows that

$$(ea + e(s-1)d) + d \equiv ea \pmod{m};$$

that is, the difference between the first and last terms of S^{+e} is d. Since d is relatively prime to m, so we must have that $S^{+e} = \mathbb{Z}/m$. Note that

$$(e-1)a + id \not\equiv (e-1)a + jd \pmod{m}$$

for any $i, j = 0, 1, \ldots, (e-1)(s-1)\,(= m-s)$. Otherwise, there would exist $i, j \in \{0, 1, \ldots, m-s\}$ such that $(i-j)d \equiv 0 \pmod{m}$. Since d is relatively prime to m, so $i - j \equiv 0 \pmod{m}$. But this is impossible since $m - s < m$. We also note that

$$\begin{aligned}(e-1)(s-1)d+d &= (m-s)d+d \\ &= (m-(s-1))d \\ &\not\equiv 0 \pmod{m}.\end{aligned}$$

Therefore $((e-1)a + (e-1)(s-1)d) + d \not\equiv (e-1)a \pmod{m}$. It thus follows that $S^{+(e-1)} \neq \mathbb{Z}/m$ and hence $e(S) = e = \frac{m-1}{s-1}$.

Now suppose that $s-1$ does not divide $m-1$. Let $f = \left\lfloor \frac{m-1}{s-1} \right\rfloor + 1 = \lceil \frac{m-1}{s-1} \rceil$. Then by Lemma 2.1,

$$\begin{aligned}fa+f(s-1)d+d &= fa+\left\lceil \frac{m-1}{s-1} \right\rceil (s-1)d+d \\ &= fa+(m+i)d \\ &\equiv fa+id \pmod{m}\end{aligned}$$

for some $i \in \{0, 1, \ldots, s-2\}$. We thus have that either the difference between the first and last terms of S^{+f} is d (this happens if $i = 0$) or the last term in the (multi)set S^{+f} coincides with one of its earlier terms (this happens if $i \in \{1, \ldots, s-2\}$). In either case, since d is relatively prime to m it must follow that $S^{+f} = \mathbb{Z}/m$. Note that

$$(f-1)(s-1) = \left\lceil \frac{m-1}{s-1} \right\rceil (s-1) < \left(\frac{m-1}{s-1} \right) (s-1) = m-1 < m.$$

Therefore

$$(f-1)a+id \not\equiv (f-1)a+jd \pmod{m}$$

for any $i, j = 0, 1, \ldots, (f-1)(s-1)$. Since $(f-1)(s-1)d+d < md$ and d is relatively prime to m, so $(f-1)a+(f-1)(s-1)d+d \not\equiv (f-1)a \pmod{m}$. It follows that $S^{+(f-1)} \neq \mathbb{Z}/m$ and hence $e(S) = f = \left\lceil \frac{m-1}{s-1} \right\rceil + 1$.

Finally, suppose that m and d are not relatively prime. Let n be the smallest positive integer such that $nd \equiv 0 \pmod{m}$. Then $(da + (n-1)d) + d \equiv da \pmod{m}$ and we thus have that

$$\begin{aligned} S^{+d} &\subseteq \{da, da+d, da+2d, \ldots, da+(n-1)d\} \\ &= \{da, d(a+1), d(a+2), \ldots, d(a+n-1)\}. \end{aligned}$$

Note that $\{da, d(a+1), d(a+2), \ldots, d(a+n-1)\}$ is the subgroup of $\mathbb{Z}/m$ of order n. Thus $S^{+(rd)} \neq \mathbb{Z}/m$ for any positive integer r and hence, S is not exhaustive. □

Corollary 2.3 *Let e be a positive integer. If S is a non-empty subset of $\mathbb{Z}/m$, $m \geq 2$ such that S is in arithmetic progression with difference d relatively prime to m and $e(S) = e$, then $|S| \geq \left[\frac{m-1}{e}\right] + 1$.*

Proof: Let $S \subseteq \mathbb{Z}/m$ such that S is in arithmetic progression with difference d relatively prime to m and with $e(S) = e$. Suppose that $|S| = s$. Note that $s > 1$; for otherwise, S would not be exhaustive. If $s-1$ divides $m-1$, then by Theorem 2.2, $\frac{m-1}{s-1} = e$. It follows easily that $s = \frac{m-1}{e} + 1$. Now suppose that $s-1$ does not divide $m-1$. By Theorem 2.2 again, $\left[\frac{m-1}{s-1}\right] = e-1$. We claim that $\left[\frac{m-1}{e}\right] + 1 < s$. Indeed, if $s \leq \left[\frac{m-1}{e}\right] + 1$, then

$$s - 1 \leq \left[\frac{m-1}{e}\right] < \frac{m-1}{e}.$$

It follows that

$$\frac{m-1}{s-1} > e$$

and hence,

$$e - 1 = \left[\frac{m-1}{s-1}\right] \geq e;$$

which is not possible. Thus, $\left[\frac{m-1}{e}\right] + 1 < s$. □

3 Exhaustion numbers of subsets of finite Abelian groups which are in arithmetic progression

Let G be a finite Abelian group written additively. We may write

$$G = \mathbb{Z}/p_1^{n_1} \oplus \cdots \oplus \mathbb{Z}/p_k^{n_k}$$

for some primes $p_1 \leq \cdots \leq p_k$ and some positive integers $n_1, \ldots, n_k$. If the p_i are all distinct, then

$$G = \mathbb{Z}/p_1^{n_1} \oplus \cdots \oplus \mathbb{Z}/p_k^{n_k} \cong \mathbb{Z}/p_1^{n_1} \ldots p_k^{n_k}$$

and the following result follows readily from Theorem 2.2:

Theorem 3.1 *Let $S \subseteq \mathbb{Z}/p_1^{n_1} \oplus \cdots \oplus \mathbb{Z}/p_k^{n_k}$ where the p_i are distinct primes and the n_i are positive integers. Let $s = |S| > 1$. If S is in arithmetic progression with difference $d = (d_1, \ldots, d_k)$ where d_i is relatively prime to p_i $(i = 1, \ldots, k)$, then*

$$e(S) = \left\lceil \frac{p_1^{n_1} \ldots p_k^{n_k} - 1}{s - 1} \right\rceil.$$

If d_i is not relatively prime to p_i for some i, then $e(S) = \infty$.

Suppose now that not all the p_i are distinct. Let $S = \{a, a + d, \ldots, a + (s-1)d\} \subseteq \mathbb{Z}/p_1^{n_1} \oplus \cdots \oplus \mathbb{Z}/p_k^{n_k}$ with difference $d = (d_1, \ldots, d_k)$. For each $i = 1, \ldots, k$, let $|d_i|$ denote the order of d_i. Then the order L of d is lcm $(|d_1|, \ldots, |d_k|) < p_1^{n_1} \ldots p_k^{n_k}$. Note that for any positive integer k, the last term in the (multi)set S^{+k} is $ka + k(s-1)d$. Therefore, for any integer $r \geq \frac{L-1}{s-1}$, we have

$$S^{+r} = \{ra, ra + d, \ldots, ra + (L-1)d\}.$$

Clearly, $|S^{+t}| = L < p_1^{n_1} \ldots p_k^{n_k}$ for all $t \geq r$. We thus have the following result:

Theorem 3.2 *Let $S \subseteq \mathbb{Z}/p_1^{n_1} \oplus \cdots \oplus \mathbb{Z}/p_k^{n_k}$ where the p_i are not all distinct and the n_i are positive integers. If S is in arithmetic progression, then S is not exhaustive.*

4 Exhaustion numbers of subsets of $\mathbb{Z}/p$, p an odd prime

The following example shows that the exhaustion numbers obtained in Theorem 2.2 do not hold for non-arithmetic progressions, even in the case when $m = p$ is a prime.

Example 4.1 *Consider the prime* $p = 11$. *Let* $S = \{1, 2, 3, 5\}$ *which is not in arithmetic progression. Then*

$$\begin{aligned} S^{+2} &= \{2, 3, 4, 5, 6, 7, 8, 10\}, \\ S^{+3} &= \{3, 4, 5, 6, 7, 8, 9, 10, 0, 1, 2\} = \mathbb{Z}/11. \end{aligned}$$

Hence $e(S) = 3 \neq \lceil \frac{10}{3} \rceil$.

In the following proposition, we obtain an upper bound for the exhaustion numbers of subsets of $\mathbb{Z}/p$ (p an odd prime). The main tool used in the proof is the Cauchy-Davenport Theorem (see [3, Corollary 1.2.3] or [4, Theorem 2.2]) which states that for any two non-empty subsets A, B of $\mathbb{Z}/p$, either $A + B = \mathbb{Z}/p$ or $|A + B| \geq |A| + |B| - 1$.

Proposition 4.2 *Let* $S \subseteq \mathbb{Z}/p$ *with* $s = |S| > 1$. *Then*

$$e(S) \leq \left\lceil \frac{p-1}{s-1} \right\rceil.$$

Proof: We first consider the case where $s - 1$ divides $p - 1$. If $S^{+(\frac{p-1}{s-1})} \neq \mathbb{Z}/p$, then by the Cauchy-Davenport Theorem and induction we have that

$$\begin{aligned} \left|S^{+(\frac{p-1}{s-1})}\right| &\geq \left(\frac{p-1}{s-1}\right)(s-1) + 1 \\ &= p, \end{aligned}$$

which is not possible. Hence we must have $S^{+(\frac{p-1}{s-1})} = \mathbb{Z}/p$ and therefore $e(S) \leq \frac{p-1}{s-1}$.

Now consider the case where $s-1$ does not divide $p-1$. If $S^{+(\left[\frac{p-1}{s-1}\right]+1)} \neq \mathbb{Z}/p$, then again by the Cauchy-Davenport Theorem and induction we have that

$$\begin{aligned}\left|S^{+(\left[\frac{p-1}{s-1}\right]+1)}\right| &\geq \left(\left[\frac{p-1}{s-1}\right]+1\right)(s-1)+1 \\ &> \left(\left(\frac{p-1}{s-1}-1\right)+1\right)(s-1)+1 \\ &= p,\end{aligned}$$

which is not possible. Therefore $\left(S^{+(\left[\frac{p-1}{s-1}\right]+1)}\right) = \mathbb{Z}/p$ and we must have $e(S) \leq \left[\frac{p-1}{s-1}\right]+1 = \left\lceil\frac{p-1}{s-1}\right\rceil$. □

We note that the upper bounds given in Proposition 4.2 are best possible, as demonstrated in the following examples:

Example 4.3 *Let* $S = \{1, 2, 3, 4, 5, 7\} \subseteq \mathbb{Z}/11$. *Then* $S^{+2} = \mathbb{Z}/11$ *and hence* $e(S) = 2 = \left\lceil\frac{11-1}{6-1}\right\rceil$.

Example 4.4 *Let* $S = \{1, 2, 3, 4, 6\} \subseteq \mathbb{Z}/11$. *Then* $e(S) = 3 = \left\lceil\frac{11-1}{5-1}\right\rceil$.

We say that a non-empty subset S of a group is an *almost arithmetic progression*, abbreviated as *a.a.p.*, if S can be obtained from an arithmetic progression of size $|S|+1$, say $\{a, a+d, a+2d, \ldots, a+(s-1)d, a+sd\}$, by either dropping the element $a+d$ next to the bottom or the element $a+(s-1)d$ next to the top. We say that S is a *near arithmetic progression*, abbreviated as *n.a.p.*, if S can be obtained from an arithmetic progression of size $|S|+1$, say $\{a, a+d, a+2d, \ldots, a+(s-1)d, a+sd\}$, by dropping one of the elements $a+(i+1)d$ ($i \in \{1, 2, \ldots, s-3\}$) which is not next to the bottom or next to the top. In the following main result of this section we determine the exhaustion numbers of subsets of $\mathbb{Z}/p$ which are a.a.p. or n.a.p. .

Theorem 4.5 *Let $S \subseteq \mathbb{Z}/p$.*

(i) If $s = |S| \geq 3$ and S is an a.a.p., then $e(S) = \left[\frac{p}{s}\right] + 1$.

(ii) If $s = |S| \geq 4$ and S is an n.a.p., then $e(S) = \left\lceil \frac{p-1}{s} \right\rceil$.

Proof:

(i) We consider the case where S is obtained from an arithmetic progression of size $|S|+1$ by dropping the element next to the bottom. The case where S is obtained from an arithmetic progression by dropping the element next to the top follows by symmetry. Let

$$S = \{a, a + 2d, a + 3d, \ldots, a + sd\}$$

where $a, d \in \mathbb{Z}/p$ and $d \not\equiv 0 \pmod{p}$. Then

$$S^{+2} = \{2a, 2a + 2d, 2a + 3d, \ldots, 2a + 2sd\}$$

and by induction, it can be shown that for any positive integer k such that $ks < p$,

$$S^{+k} = \{ka, ka + 2d, ka + 3d, \ldots, ka + ksd\}.$$

Hence, $|S^{+k}| = ks$ if $ks < p$. In particular, $|S^{+\left[\frac{p}{s}\right]}| = \left[\frac{p}{s}\right] s$ since $\left[\frac{p}{s}\right] s < \left(\frac{p}{s}\right) s = p$. Note that we may write

$$p = \left[\frac{p}{s}\right] s + r$$

where $0 < r \leq s - 1$. Then

$$\left[\frac{p}{s}\right] s + s = p - r + s \geq p + 1$$

and it thus follows from the Cauchy–Davenport Theorem that $S^{+\left(\left[\frac{p}{s}\right]+1\right)} = \mathbb{Z}/p$. Hence, $e(S) = \left[\frac{p}{s}\right] + 1$.

(ii) Let

$$S = \{a, a + d, \ldots, a + id, a + (i + 2)d, \ldots, a + (s - 1)d, a + sd\}$$

where $a, d \in \mathbb{Z}/p$, $d \not\equiv 0 \pmod{p}$ and $i \in \{1, \ldots, s-3\}$. Then

$$S^{+2} = \{2a,\ 2a+d,\ 2a+2d,\ \ldots,\ 2a+2sd\}$$

and by induction, it can be shown that for any positive integer $k > 1$ such that $ks < p$,

$$S^{+k} = \{ka,\ ka+d,\ ka+2d,\ \ldots,\ ka+ksd\}.$$

Hence, $|S^{+k}| = ks+1$ if $ks < p$.

Suppose first that s divides $p-1$. Since $\left(\frac{p-1}{s} - 1\right) s$, $\left(\frac{p-1}{s}\right) s < p$, then

$$|S^{+(\frac{p-1}{s}-1)}| = \left(\frac{p-1}{s} - 1\right) s + 1 = p - s$$

and

$$|S^{+(\frac{p-1}{s})}| = \left(\frac{p-1}{s}\right) s + 1 = p.$$

It thus follows that $e(S) = \frac{p-1}{s} = \left\lceil \frac{p-1}{s} \right\rceil$.

Next suppose that s does not divide $p-1$. We can write

$$p - 1 = \left[\frac{p-1}{s}\right] s + r$$

where $0 < r < s-1$. (Note that $r \neq s-1$; for otherwise p would be divisible by s which is not possible.) Since

$$\left[\frac{p-1}{s}\right] s < \left(\frac{p-1}{s}\right) s = p - 1 < p,$$

so $|S^{+\left[\frac{p-1}{s}\right]}| = \left[\frac{p-1}{s}\right] s + 1 = p - r\ (< p)$. Then since

$$|S^{+\left[\frac{p-1}{s}\right]}| + s = p - r + s \geq p + 2,$$

we must have by the Cauchy-Davenport Theorem that $|S^{+(\left[\frac{p-1}{s}\right]+1)}| = \mathbb{Z}/p$. Hence, $e(S) = \left[\frac{p-1}{s}\right] + 1 = \left\lceil \frac{p-1}{s} \right\rceil$. □

Acknowledgement. Much of the work in this paper arose from the joint report [1]. The author should like to thank Dr. Thomas Bier for bringing exhaustion numbers to her attention.

References

[1] T. Bier and A. Y. M. Chin, *Some properties of subsets of Abelian groups*, Research Report 2/98, University of Malaya, 1998.

[2] T. Hearne and C. Wagner, *Minimal covers of finite sets*, Discrete Math. **5** (1973), 247–251.

[3] H. B. Mann, Addition Theorems: The Addition Theorems of Group Theory and Number Theory, Interscience Traits in Pure and Applied Mathematics, No. 18, John Wiley, New York/London/Sydney, 1965.

[4] M. B. Nathanson, Additive Number Theory: Inverse Problems and the Geometry of Sumsets, Springer (GTM **165**), New York, 1996.