BULL. AUSTRAL. MATH. SOC. MOS 05B10, 20K99
VOL. 5 (1971), 43-54. (20D99)

# Maximal sum-free sets in finite abelian groups, II

H.P. Yap

Maximal sum-free sets in groups $Z_n$ , where $n$ is any positive integer such that every prime divisor of $n$ is congruent to 1 modulo 3 , are completely characterized.

Let $G$ be an additive group. If $S$ and $T$ are non-empty subsets of $G$ , we write $S \pm T$ for $\{s \pm t;\ s \in S,\ t \in T\}$ respectively, $|S|$ for the cardinality of $S$ and $\bar{S}$ for the complement of $S$ in $G$ . We say that $S$ is sum-free in $G$ if $S$ and $S + S$ have no common element and that $S$ is maximal sum-free in $G$ if $S$ is sum-free in $G$ and $|S| \geq |T|$ for every $T$ sum-free in $G$ . We denote by $\lambda(G)$ the cardinality of a maximal sum-free set in $G$ . We say that $S$ is in a.p. (arithmetic progression) with difference $d$ if $S = \{s, s+d, \ldots, s+nd\}$ for some $s, d \in G$ and some integer $n \geq 0$ . We say that $S$ is quasi-periodic if there exists a subgroup $H$ , of order $\geq 2$ , of $G$ such that $S$ is the disjoint union of a non-empty set $S'$ consisting of $H$-cosets and a residue set $S''$ contained in a remaining $H$-coset. We say that a prime $p$ is a bad prime if $p$ is congruent to 1 modulo 3 .

Erdös [2] gives certain upper and lower bounds for $\lambda(G)$ of finite abelian groups $G$ . Exact values $\lambda(G)$ for all finite abelian groups $G$ , except when every prime divisor of $|G|$ is bad, were determined by Diananda and Yap [1]. In this exceptional case,

$$|G|(m-1)/3m \leq \lambda(G) \leq (|G|-1)/3$$

where $m$ is the exponent of $G$ . For elementary abelian $p$-groups $G$ of

Received 4 January 1971.

order $p^n$, Rhemtulla and Street [5] prove that $\lambda(G) = kp^{n-1}$, where $p = 3k + 1$ is a prime.

The structure of maximal sum-free sets in the following groups were completely characterized:

(i) $G$ is any abelian group such that $|G|$ has a prime divisor congruent to 2 modulo 3 [1, 7];

(ii) $G = Z_p$ where $p$ is a bad prime [8, 5];

(iii) $G$ (abelian and non-abelian) is of order $3p$, where $p$ is a bad prime [9];

(iv) $G$ is an elementary abelian $p$-group where $p$ is a bad prime [6];

(v) $G$ is an elementary abelian 3-group and $G = Z_3 \oplus Z_3 \oplus Z_p$ where $p$ is a bad prime [10].

We shall apply a Lemma in [5] and Theorem 2.1 in [3], which are restated respectively as Lemma 1 and Theorem 1 here, to prove Theorem 2 which generalizes some results in [8] and [5].

LEMMA 1. *Let* $G = Z_n$, $n = 3k + 1$ *and* $S$ *be a sum-free set in* $G$ *satisfying* $|S| = k$, $-S = S$ *and* $\bar{S} = S + S$. *Then*

*(i) if* $|(S+g)\cap S| = 1$ *for some* $g$ *in* $G$, *then* $|(S+g^*)\cap S| \geq k - 3$ *where* $g^* = 3g/2$ *and* $\pm g/2 \in S$;

*(ii) if* $|(S+g)\cap S| = \lambda > 1$ *for some* $g \neq 0$ *in* $G$, *then* $g^* = s_1 - s_2$, *where* $s_1, s_2$ $(\neq s_1) \in S$ *and* $s_1+g, s_2+g \in \bar{S}$, *is such that* $|(S+g^*)\cap S| \geq k - (\lambda+1)$.

THEOREM 1 (Kemperman). *Let* $G$ *be an abelian group with subsets* $A$ *and* $B$ *such that* $|A|, |B| \geq 2$. *If* $|A+B| = |A| + |B| - 1$, *then either* $A + B$ *is in* a.p. *or* $A + B$ *is quasi-periodic.*

We first prove the following lemmas.

LEMMA 2. *Let* $G = Z_n$ *where* $n$ *is any positive integer such that every prime divisor* $p$ *of* $n$ *is bad. If* $S$ *is a maximal sum-free set in* $G$, *then*

https://doi.org/10.1017/S0004972700046864 Published online by Cambridge University Press

*(i) if* $-S \neq S$ , $|S+S^*| = |S| + |S^*| - 1$ , *where* $S^* = -S \cup S$ ;

*(ii) if* $-S = S$ , *either* $|S+S| = 2|S| - 1$ *or* $\overline{S} = S + S$ .

Proof. By Kneser's Theorem [4], there exists a subgroup $K$ of $G$ such that $S + S + K = S + S$ and $|S+S| \geq 2|S+K| - |K|$ . It is clear that $K$ is a proper subgroup of $G$ .

Suppose that $|K| = q > 1$ . Let $n = 3k + 1 = pq$ , $p = 3r + 1$ , $q = 3s + 1$ . Then $\lambda(G) = k = rq + s$ and

$$|G| - |S| = 2k + 1 \geq |S+S| \geq 2(k/q]q - q$$

where $(x]$ denotes the smallest positive integer $\geq x$ .

Thus $2k + 1 \geq |S+S| \geq (2r+1)q$ , which is impossible. Hence $|S+S| \geq 2|S| - 1$ .

If $-S = S$ , then $|S+S|$ is odd and from $2k + 1 \geq |S+S| \geq 2k - 1$ , it follows that either $|S+S| = 2|S| - 1$ or $|S+S| = 2|S| + 1$ and thus $\overline{S} = S + S$ .

If $-S \neq S$ , then again by Kneser's Theorem there exists a proper subgroup $K$ of $G$ such that $S + S^* + K = S + S^*$ and $|S+S^*| \geq |S+K| + |S^*+K| - |K|$ .

In this case, we can show that $|K| = 1$ . Thus

$$2k + 1 \geq |S+S^*| \geq |S| + |S^*| - 1 \geq |S| + (|S|+2) - 1 = 2k + 1 .$$

Hence $|S^*| = |S| + 2$ and $|S+S^*| = |S| + |S^*| - 1$ .

The proof of Lemma 2 is now complete.

LEMMA 3. *Let* $G = Z_n$ *where* $n$ *is any positive integer such that every prime divisor* $p$ *of* $n$ *is bad. Let* $S$ *be a maximal sum-free set in* $G$ .

(I) *If* $-S \neq S$ , *then* $S$ *can be mapped onto* $\{k, k+1, \ldots, 2k-1\}$ *under an automorphism of* $G$ .

(II) *If* $-S = S$ *and* $|S+S| = 2|S| - 1$ , *then* $S$ *can be mapped onto* $\{k+1, k+2, \ldots, 2k\}$ *under an automorphism of* $G$ .

Proof (I). If $-S \neq S$ , then by Lemma 2, $|S+S^*| = |S| + |S^*| - 1$ . By Kemperman's Theorem, we have either $S + S^*$ is in a.p. or $S + S^*$ is quasi-periodic.

https://doi.org/10.1017/S0004972700046864 Published online by Cambridge University Press

Suppose that $S + S^*$ is quasi-periodic, then from $\overline{S} = S + S^*$ it follows that $S$ is also quasi-periodic. Thus $S'$ , which is a subset of $S$ consisting of $H$-cosets, will be a maximal sum-free set in $G/H$ while the non-empty residue set $S''$ which is contained in a remaining $H$-coset will violate the sum-free property of $S$ . Hence $S + S^*$ cannot be quasi-periodic.

Let $S + S^* = \{a'+id;\ i = 0, 1, \ldots, 2k\}$ . Since $|S+S^*| = 2k + 1$ , therefore $(d, n) = 1$ (the g.c.d. of $d$ and $n$ ). Hence under an automorphism of $G$ , we can write $S + S^* = \{a+i;\ i = 0, 1, \ldots, 2k\}$ . Then $S = \overline{S + S^*} = \{a+i;\ i = 2k+1, \ldots, 3k\}$ . From $|S^*| = |S| + 2$ , we have either

(i) $2a + 2k + 3 + 3k \equiv 0 \pmod{n}$ , that is $a \equiv -(k+1) \pmod{n}$ , or

(ii) $2a + 2k + 1 + 3k - 2 \equiv 0 \pmod{n}$ , that is $a \equiv -(k-1) \pmod{n}$ .

(i) gives the maximal sum-free set $S = \{k, k+1, \ldots, 2k-1\}$ .

(ii) gives $S = \{k+2, k+3, \ldots, 2k+1\}$ which can be mapped onto $\{k, k+1, \ldots, 2k-1\}$ under an automorphism of $G$ .

Proof (II). Applying similar methods we can show that under an automorphism of $G$ , $S + S$ can be mapped onto $S + S = \{a+i;\ i = 0, 1, \ldots, 2k-2\}$ . Since $-S = S$ , therefore $2a + 2k - 2 \equiv 0 \pmod{n}$ , that is $a \equiv -(k-1) \pmod{n}$ .

Then $S + S = \{-(k-1), -(k-2), \ldots, k-1\}$ , and

$$S \subseteq \overline{S + S} = \{k, k+1, \ldots, 2k+1\} .$$

But $2k = k + k \notin S + S$ , therefore $k \notin S$ . Hence $S = \{k+1, \ldots, 2k\}$ .

The proof of Lemma 3 is now complete.

LEMMA 4. *Let* $G = Z_n$ , $n = 3k + 1$ *and* $S$ *be a sum-free set in* $G$ *satisfying* $|S| = k$ , $-S = S$ *and* $\overline{S} = S + S$ . *Then* $|(S+g)\cap S| > 1$ *for every* $g \in \overline{S}$ *with* $(g, n) > 1$ .

Proof. We first note that $(S+g) \cap S \neq \emptyset$ if and only if $g \notin S$ .

Suppose that $|(S+g)\cap S| = 1$ for some $g \in \overline{S}$ with $(g, n) > 1$ . Then

https://doi.org/10.1017/S0004972700046864 Published online by Cambridge University Press

by Lemma 1, $|(S+f)\cap S| \geq k - 3$ where $f = 3g/2$ .

Now $|(S+f)\cap S| \neq k$ , since $S$ cannot be a union of cosets of a nontrivial subgroup of $G$ . Thus $|(S+f)\cap S| = k - 1$ , $k - 2$ or $k - 3$ .

Let $H = [f]$ , the subgroup of $G$ generated by $f$ , where $|H| = p = 3r + 1 > 1$ , $pq = n$ , $q = 3s + 1$ , $|S| = sp + r$ .

(i) If $|(S+f)\cap S| = k - 1$ , then

$$S = \cup H_i \cup \{a_1, a_1+f, \ldots, a_1+m_1f\}$$

where each $H_i$ is a coset of $H$ , $|\cup H_i| = sp$ and $m_1 = r - 1$ . In this case it is clear that $S'' = \{a_1, a_1+f, \ldots, a_1+m_1f\} \subseteq H$ . But $H \subseteq S + S$ which contradicts the fact that $(S+S) \cap S = \emptyset$ .

(ii) If $|(S+f)\cap S| = k - 2$ , then

$$S = \cup H_i \cup \{a_1, a_1+f, \ldots, a_1+m_1f\} \cup \{a_2, a_2+f, \ldots, a_2+m_2f\} , \quad m_1 \leq m_2 .$$

Since $-S = S$ , $s \geq 2$ , therefore $H \subseteq S + S$ , and

$$-\{a_1, a_1+f, \ldots, a_1+m_1f\} = \{a_2, a_2+f, \ldots, a_2+m_2f\} .$$

Hence $m_1 + m_2$ is even. If $|\cup H_i| = (s-1)p$ , then $m_1 + m_2 = p + r - 2$ is odd, which is impossible. Hence $|\cup H_i| = sp$ and $m_1 + m_2 = r - 2$ . But then

$$\{a_1, \ldots, a_1+m_1f, a_2, \ldots, a_2+m_2f\} + \{a_1, \ldots, a_1+m_1f, a_2, \ldots, a_2+m_2f\}$$

contains elements from 3 distinct cosets of $H$ , which contradicts the fact that $\bar{S} = S + S$ .

(iii) If $|(S+f)\cap S| = k - 3$ , then

$$S = \cup H_i \cup \{a_1, \ldots, a_1+m_1f, a_2, \ldots, a_2+m_2f, a_3, \ldots, a_3+m_3f\} ,$$
$$m_1 \leq m_2 \leq m_3 .$$

Suppose that $S \cap H = \emptyset$ . Then from $-S = S$ we know that

$$\{a_1, \ldots, a_1+m_1f, a_2, \ldots, a_2+m_2f, a_3, \ldots, a_3+m_3f\}$$

is contained in exactly two distinct cosets of $H$ . Without loss of generality, assume that $a_2 \in a_1 + H$ . Then

$$-\{a_1, \ldots, a_1+m_1f, a_2, \ldots, a_2+m_2f\} = \{a_3, \ldots, a_3+m_3f\}$$

which is impossible, because the right hand side is in a.p. with difference $f$ while the left hand side is not in a.p. with difference $f$. Hence $S \cap H \neq \emptyset$. But then $|\cup H_i| = 0$ and $s = 2$, $m_1 + m_2 + m_3 = 2p + r - 3$. In this case, $S + S$ will contain 5 distinct full cosets of $H$ which is impossible.

The proof of Lemma 4 is now complete.

THEOREM 2. *Let $G = Z_n$ where $n$ is any positive integer such that every prime divisor of $n = 3k + 1$ is bad. If $S$ is a maximal sum-free set in $G$, then $S$ can be mapped, under an automorphism of $G$, to one of the following:*

*(i)* $\{k+1, k+2, \ldots, 2k\}$ ;

*(ii)* $\{k, k+1, \ldots, 2k-1\}$ ;

*(iii)* $\{k, k+2, k+3, \ldots, 2k-1, 2k+1\}$ .

Proof. By Lemmas 2 and 3, it remains to show that if $-S = S$, $\bar{S} = S + S$, then $S$ can be mapped to $\{k, k+2, k+3, \ldots, 2k-1, 2k+1\}$ under an automorphism of $G$. The method used here is a modification of a method due to Rhemtulla and Street [5].

If $|(S+g)\cap S| = 1$ for some $g \in G$ such that $(g, n) = 1$, then by the same method as the proof of Theorem 2 in [5], we can show that under an automorphism of $G$, $S$ can be mapped onto $\{k, k+2, k+3, \ldots, 2k-1, 2k+1\}$.

We are now left with the case where $S$ satisfies the conditions of Lemma 1 and $|(S+g)\cap S| \neq 1$ for any $g$ in $G$ satisfying $(g, n) = 1$. If $|(S+g)\cap S|$ is maximal for some $g$ satisfying $(g, n) = 1$, then by taking an automorphism of $G$ if necessary, assume that $|(S+1)\cap S|$ is maximal. We write

(1) $\quad S = \{a_1, \ldots, a_1+m_1, a_2, \ldots, a_2+m_2, \ldots, a_h, \ldots, a_h+m_h\}$ ,

where $1 < a_1 \leq a_1+m_1 < a_2-1 < a_2+m_2 < \ldots < a_h-1 < a_h+m_h < n$, and $a_i, \ldots, a_i+m_i$ denotes a string of $(m_i+1)$ consecutive elements of $S$.

https://doi.org/10.1017/S0004972700046864 Published online by Cambridge University Press

We have

(2) $\left|(S+1)\cap S\right| = k - h \geq \left|(S+g)\cap S\right|$ for every $g \neq 0$ in $G$.

Hence $h$ is minimal in (1).

Let $X = \{a_1, a_2, \ldots, a_h\}$. Then

$$Y = \{a_1+m_1+1, \ldots, a_h+m_h+1\} = 1 - X ,$$

since $-S = S$.

For each $i = 1, \ldots, h$, $a_i - 1 \notin S$. Since $\overline{S} = S + S$ and $\left|(S+g)\cap S\right| \geq 2$ for any $g$ $(\neq 0) \in \overline{S}$ (by assumption and Lemma 4), therefore there exist $s_1, s_2$ $(\neq s_1)$ in $S$ such that $a_i - 1 = s_2 - s_1$ and $g = -s_1 - s_2 \neq 0$. We have now $s_1 + g$, $s_2 + g \in S$ and $k - h \geq \left|(S+g)\cap S\right| \geq 2$, therefore, by Lemma 1, we have $\left|(S+a_i-1)\cap S\right| \geq h - 1$. But for any $s_1, s_2 \in S$, $s_1 + a_i - 1 = s_2$ implies that $s_1 \in X$, $s_2 \in -X$ and $s_1 + a_i \in Y$. Hence

(3) $h \geq \left|(X+a_i)\cap Y\right| \geq h - 1$ for all $i = 1, \ldots, h$.

Suppose that $h \geq 3$.

If for each $j = 1, \ldots, h$, $X + a_j = Y = 1 - X$, then $X + [X-X] = X$, $h = |X| = \left|[X-X]\right| = p$, which divides $n$, and

(4) $2\sum_{i=1}^{h} a_i + ha_j \equiv h \pmod{n}$ for each $j = 1, \ldots, h$.

Thus

(5) $h\left(a_i-a_j\right) \equiv 0 \pmod{n}$ for every $i, j = 1, \ldots, h$.

If $n$ is a prime, we already get a contradiction here. Otherwise, $X = a + H$ where $H = [q]$, $pq = n$. We then have

(6) $a_1 = a$, $a_2 = a+q, \ldots, a_p = a + (p-1)q$.

Substituting (6) into (4) for $j = 1$, we get $(3a-1)p \equiv 0 \pmod{n}$ from which it follows that $a = 2s + 1$ $(q = 3s+1)$ and

$$S = \{2s+1, \ldots, 2s+1+m_1, \ldots, 2s+1+(p-1)q+m_p\} .$$

https://doi.org/10.1017/S0004972700046864 Published online by Cambridge University Press

But $2s + 1 + 2s + 1 + (p-1)q + m_p > n$ which contradicts the fact that $a_1 + a_p + m_p = n$. Hence, for at least one $t \in \{1, \ldots, h\}$, $|(X+a_t) \cap Y| = h - 1$.

If there is only one $t \in \{1, \ldots, h\}$ such that $|(X+a_t) \cap Y| = h - 1$, then there are at least two distinct $i, j \in \{1, \ldots, h\}$ such that $X + a_i = Y = X + a_j$ and thus $X + a_i - a_j = X$ from which it follows that $X$ is the union of cosets of a nontrivial subgroup of $G$. (If $n$ is a prime, we get a contradiction here.) Thus $|(X+a_t) \cap Y| \neq h - 1$ which contradicts the hypothesis.

Hence there are at least two $t_1, t_2 \in \{1, \ldots, h\}$ such that $|(X+a_{t_1}) \cap Y| = h - 1 = |(X+a_{t_2}) \cap Y|$. Then

$$(7) \quad \{a_1, \ldots, a_{t-1}, a_{t+1}, \ldots, a_h\} + a_t = 1 - \{a_1, \ldots, a_{t-1}, a_{t+1}, \ldots, a_h\}, \quad t = t_1, t_2,$$

from which it follows that

$$(8) \qquad 2\sum_{i=1}^{h} a_i + (h-3)a_t \equiv h - 1 \pmod{n}, \quad t = t_1, t_2,$$

and thus

$$(9) \qquad (h-3)(a_{t_1} - a_{t_2}) \equiv 0 \pmod{n}.$$

Suppose there are also at least two $r_1, r_2 \in \{1, \ldots, h\}$ such that $|(X+a_{r_i}) \cap Y| = h$. Divide $\{1, \ldots, h\}$ into the union of two disjoint subsets $R = \{r_1, \ldots, r_u\}$, $u \geq 2$, $T = \{t_1, \ldots, t_v\}$, $v \geq 2$ such that $\left|\left(X+a_{r_i}\right) \cap Y\right| = h$ and $\left|\left(X+a_{t_i}\right) \cap Y\right| = h - 1$. Then

$$(10) \qquad h(a_r - a_{r'}) \equiv 0 \pmod{n} \text{ for every } r, r' \in R,$$

$$(11) \qquad (h-3)(a_t - a_{t'}) \equiv 0 \pmod{n} \text{ for every } t, t' \in T.$$

Let

(12) $$a_{t_1} + a_{r_1} \equiv 1 - a_{p_1} \pmod{n} ,$$

(13) $$a_{t_2} + a_{r_1} \equiv 1 - a_{p_2} \pmod{n} .$$

Then $a_{t_1} - a_{t_2} \equiv a_{p_2} - a_{p_1} \pmod{n}$ from which it follows that at least one of $p_1$, $p_2$ is in $T$. Suppose that $p_1 = t \in T$. Let

(14) $$a_{t_1} + a_{r_2} \equiv 1 - a_{p_3} \pmod{n} .$$

Then from (12) and (14), we have $a_{r_1} - a_{r_2} \equiv a_{p_3} - a_t \pmod{n}$ and thus $p_3 = r \in R$. Then $h(a_r - a_t) \equiv 0 \pmod{n}$, and thus from (10), we have

(15) $$h(a_r - a_t) \equiv 0 \pmod{n} \text{ for every } r \in R .$$

Let

(16) $$a_{t_2} + a_{r_2} \equiv 1 - a_{p_4} \pmod{n} .$$

Then from (14) and (16), we have $a_{t_1} - a_{t_2} \equiv a_{p_4} - a_r \pmod{n}$ from which it follows that $p_4 = t' \in T$. Hence $(h-3)(a_{t'} - a_r) \equiv 0 \pmod{n}$. Then from (11), we have

(17) $$(h-3)(a_t - a_r) \equiv 0 \pmod{n} \text{ for every } t \in T .$$

But (15) and (17) cannot occur at the same time. Hence for at most one $j \in \{1, \ldots, h\}$, $|(X+a_j) \cap Y| = h$. But then (9) is true for every $t_1, t_2 \in \{1, 2, \ldots, j-1, j+1, \ldots, h\}$. We have either

(i) $h - 3 = vp > 0$, $p | n$, $(v, n) = 1$ and

$$X' = \{a_1, \ldots, a_{j-1}, a_{j+1}, \ldots, a_h\} = a + A'$$

where $A' \subseteq H = [q]$, $pq = n$, which is impossible because $h - 1 = vp + 2 > |G/H|$; or

(ii) $h = 3$ and thus

$$S = \{a, \ldots, a+c-1, k+c+1, \ldots, 2k-c, 3k+2-a-c, \ldots, 3k+1-a\}$$

where $a \le k$ and $c < k/2$.

Then from (8) we get

$$0 \equiv 3 - 1 - 2\{a+k+c+1-(a+c-1)\} \pmod{n} ,$$

https://doi.org/10.1017/S0004972700046864 Published online by Cambridge University Press

that is $1 \equiv k + 2 \pmod{n}$ which is impossible.

Thus $h \le 2$. But $h \ne 1$, because $S$ is not in a.p. If $h = 2$, then $S = \{\pm k/2, \pm(1+k/2), \ldots, \pm(k-1)\}$ which maps, under an automorphism of $G$, to $\{k, k+2, k+3, \ldots, 2k-1, 2k+1\}$.

Finally, suppose that $|(S+g) \cap S| \ge 2$ for every $g \ne 0$ in $G$ with $(g, n) = 1$ and that $|(S+g) \cap S|$ is maximal for some $g$ in $G$ with $(g, n) > 1$. By taking an automorphism of $G$, if necessary, suppose that $g | n$. Then we can write

$$S = \cup H_i \cup \{a_1, a_1+g, \ldots, a_1+m_1 g, \ldots, a_h, a_h+g, \ldots, a_h+m_h g\}$$

where each $H_i$ is a coset of $H = [g]$,

$$S'' = \{a_1, a_1+g, \ldots, a_1+m_1 g, \ldots, a_h, a_h+g, \ldots, a_h+m_h g\}$$

does not contain a whole coset of $H$, $a_i + (m_i+1)g \not\equiv a_j \pmod{n}$ for any $i, j = 1, \ldots, h$, $1 \le a_1 < a_2 < \ldots < a_h < n$, and

$$|(S+g) \cap S| = k - h \ge |(S+g') \cap S| \text{ for every } g' \ne 0 \text{ in } G .$$

Let $X = \{a_1, a_2, \ldots, a_h\}$. Then

$$Y = \{a_1+(m_1+1)g, \ldots, a_h+(m_h+1)g\} = g - X ,$$

since $-S'' = S''$. By a similar method we can show that (3) holds good. Suppose that $h \ge 3$. If for each $j = 1, \ldots, h$, $X + a_j = Y = g - X$, then $h = |X| = |[X-X]| = p$, and this divides $n$, and (6) also holds good. We have then $a \equiv (2s+1)g \pmod{q}$. Now if $|\cup H_i| \ne 0$, then $H \cap S = \emptyset$. We note that the number of elements of $a_i$ in $X$ that belong to a particular coset $H_i$ of $H$ and the number of $a_j$ in $X$ that belong to $-H_i$ are the same, therefore since $p$ is odd, there is at least one $a_i \in X$ such that $a_i \in H$ which contradicts the fact that $H \cap S = \emptyset$. Hence in this case, $|\cup H_i| = 0$ and $H \cap S \ne \emptyset$. Now if $(g, q) = d > 1$, then $d | a$ and thus $d$ divides each element in $S$ which is impossible. Hence $(g, p) = g$ and $q \le n/g$. It is then clear that each $m_i < q - 1$. Otherwise for some $i$ with $1 \le i \le p$,

https://doi.org/10.1017/S0004972700046864 Published online by Cambridge University Press

$a + (g+i-1)q \in S$ will be one of the elements of $S$ that belong to $\{a+(i-1)q+g, \ldots, a+(i-1)q+m_i g\}$ or $a + (g+i-1)q = a + (i-1)q + (m_i+1)g$, which is not true. From this, it can be shown that each of the cosets $K_i$ of $K = [q]$ which is contained in $S$ is of the form $a + ig + K$, $i < q - 1$. Since $3a \equiv g \pmod{q}$, we have $3a - g = 2q$ if $g < q$ and $g - 3a = xq$ if $g > q$ where $x \equiv 1 \pmod{3}$. Now since $a + K \subseteq S$, therefore $-a + K \subseteq S$. We have $-a + K = a + (g+2q)/3 - g + K$ if $g < q$ and $-a + K = a + (g-xq)/3 - g + K$ if $g > q$. But neither $(g+2q)/3$ nor $(g-xq)/3$ is of the form $ig$, $1 \le i \le q-1$, for otherwise $g$ will divide $q$.

By a similar method and the proof of Lemma 4, we can show that all the other possibilities cannot occur. Hence $h \le 2$. If $h = 1, 2$, then using the proof of Lemma 4 again, we can show that these cases cannot occur also. Hence the possibility that $|(S+g)\cap S|$ is maximal for some $g$ with $(g, n) > 1$ is excluded.

This is the end of the proof of Theorem 2.

## References

[1] Palahenedi Hewage Diananda and Hian Poh Yap, "Maximal sum-free sets of elements of finite groups", *Proc. Japan Acad.* 45 (1969), 1-5.

[2] P. Erdös, "Extremal problems in number theory", *Proc. Sympos. Pure Math.* 8, 181-189 (Amer. Math. Soc., Providence, Rhode Island, 1965).

[3] J.H.B. Kemperman, "On small sumsets in an abelian group", *Acta Math.* 103 (1960), 63-88.

[4] Henry B. Mann, *Addition theorems: The addition theorems of group theory and number theory* (Interscience Tracts in Pure and Applied Mathematics, Number 18, John Wiley, New York, London, Sydney, 1965).

[5] A.H. Rhemtulla and Anne Penfold Street, "Maximal sum-free sets in finite abelian groups", *Bull. Austral. Math. Soc.* 2 (1970), 289-297.

https://doi.org/10.1017/S0004972700046864 Published online by Cambridge University Press

[6] A.H. Rhemtulla and Anne Penfold Street, "Maximal sum-free sets in elementary abelian $p$-groups", *Canad. Math. Bull.* (to appear).

[7] H.P. Yap, "The number of maximal sum-free sets in $C_p$", *Nanta Math.* 2 (1968), 68-71.

[8] H.P. Yap, "Structure of maximal sum-free sets in $C_p$", *Acta Arith.* 17 (1970), 29-35.

[9] Hian Poh Yap, "Structure of maximal sum-free sets in groups of order $3p$", *Proc. Japan Acad.* 46 (1970), 758-762.

[10] H.P. Yap, "Maximal sum-free sets in finite abelian groups", *Bull. Austral. Math. Soc.* 4 (1971), 217-223.

University of Alberta,
Edmonton,
Canada.

https://doi.org/10.1017/S0004972700046864 Published online by Cambridge University Press