Chin. Ann. Math. Ser. B
45(5), 2024, 767–776
DOI: 10.1007/s11401-024-0038-0

Chinese Annals of Mathematics, Series B

A Generalization of Vosper's Theorem*

Yujie WANG[1] Min TANG[2]

Abstract Let $\mathbb{Z}/m\mathbb{Z}$ be the ring of residual classes modulo m, and let A and B be nonempty subsets of $\mathbb{Z}/m\mathbb{Z}$. In this paper, the authors give the structure of A and B for which $|A+B|=|A|+|B|-1=m-2$.

Keywords Sumsets, Inverse problem, Vosper's theorem, Kemperman's theorem
2000 MR Subject Classification 11B13

1 Introduction

Let $\mathbb{Z}/m\mathbb{Z}$ be the ring of residual classes modulo m, and let $U(\mathbb{Z}/m\mathbb{Z})$ be the group of its units. Write $(\mathbb{Z}/m\mathbb{Z})^\star = (\mathbb{Z}/m\mathbb{Z})\backslash\{0\}$. For $A, B \subseteq \mathbb{Z}/m\mathbb{Z}$, let

$$A+B=\{a+b : a\in A, b\in B\}.$$

The classical direct problem for addition in groups is to find the lower bound of the size of $A+B$. In 1813, Cauchy [1] proved the following theorem and Davenport [5] rediscovered the result in 1935. It is known as the Cauchy-Davenport theorem.

Theorem A (Cauchy-Davenport) *Let p be a prime number, and let A and B be nonempty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then*

$$|A+B|\geqslant \min(p, |A|+|B|-1).$$

The Cauchy-Davenport theorem is an example of a direct addition theorem modulo p. The first generalization to cyclic group is due to Chowla [3] in 1935.

Theorem B (Chowla) *Let $m\geqslant 2$, and let A and B be nonempty subsets of $\mathbb{Z}/m\mathbb{Z}$. If $0\in B$ and $B\setminus\{0\}\subseteq U(\mathbb{Z}/m\mathbb{Z})$, then*

$$|A+B|\geqslant \min(m, |A|+|B|-1).$$

The direct problem has many related results (see [2, 6–7, 9]). The inverse problem is to describe the structure of those sets A and B from properties of the sumset $A+B$. In 1956, Vosper [14–15] obtained the following result.

Manuscript received December 8, 2021. Revised October 16, 2023.
[1]School of Mathematics and Statistics, Anhui Normal University, Wuhu 241002, Anhui, China. E-mail: wangyujie9291@126.com
[2]Corresponding author. School of Mathematics and Statistics, Anhui Normal University, Wuhu 241002, Anhui, China. E-mail: tmzzz2000@163.com
*This work was supported by the National Natural Science Foundation of China (Nos. 12101007, 12371003) and the Natural Science Foundation of Anhui Province (No. 2008085QA06).

Theorem C (Vosper) *Let p be a prime number, and let A and B be nonempty subsets of $G=\mathbb{Z}/p\mathbb{Z}$ such that $A+B\neq G$. Then $|A+B|=|A|+|B|-1$ if and only if at least one of the following three conditions holds*:

(1) $\min(|A|,|B|)=1$,

(2) $|A+B|=p-1$, $B=\overline{c-A}$, *where* $\{c\}=G\setminus(A+B)$,

(3) *A and B are arithmetic progressions with the same common difference.*

In 1960, Kemperman [8] generalized Vosper's theorem to arbitrary abelian groups.

Theorem D (Kemperman) *Let G be a finite abelian group, and let A and B be two subsets of G such that $|A|\geqslant 2$, $|B|\geqslant 2$ and $|A+B|=|A|+|B|-1\leqslant p-2$, where p is the smallest prime divisor of $|G|$. Then A and B are arithmetic progressions with the same common difference.*

The Vosper's theorem also has many other generalizations derived by several authors (see [4, 11–13]).

Throughout this paper, for $g\in\mathbb{Z}/m\mathbb{Z}$, let $\langle g\rangle$ denote the additive subgroup of $\mathbb{Z}/m\mathbb{Z}$ generated by g. We call the number of all cosets $t(g)$ the index of $\langle g\rangle$ in $\mathbb{Z}/m\mathbb{Z}$ and write $t(g):=[\mathbb{Z}/m\mathbb{Z}:\langle g\rangle]$. Let

$$x_{1,g}+\langle g\rangle,\cdots,x_{t(g),g}+\langle g\rangle$$

be a list of all the cosets of $\langle g\rangle$ in $\mathbb{Z}/m\mathbb{Z}$. For $A,B\subseteq\mathbb{Z}/m\mathbb{Z}$ and $g\in\mathbb{Z}/m\mathbb{Z}$, let

$$A_{i,g}=A\cap(x_{i,g}+\langle g\rangle),\quad B_{i,g}=B\cap(x_{i,g}+\langle g\rangle),\quad i=1,\cdots,t(g).$$

Write

$$I_{A,g}=\{1\le i\le t(g):A_{i,g}=x_{i,g}+\langle g\rangle\},$$

$$I_{B,g}=\{1\le i\le t(g):B_{i,g}=x_{i,g}+\langle g\rangle\}.$$

Let $J_{A,g}=\{1,\cdots,t(g)\}\setminus I_{A,g}$, $J_{B,g}=\{1,\cdots,t(g)\}\setminus I_{B,g}$.

Write

$$A=\bigcup_{i\in I_{A,g}}A_{i,g}\cup\bigcup_{j\in J_{A,g}}A_{j,g},\quad B=\bigcup_{i\in I_{B,g}}B_{i,g}\cup\bigcup_{j\in J_{B,g}}B_{j,g}.$$

In this paper, we obtain the following results.

Theorem 1.1 *Let $m\geqslant 2$, and let A, B be nonempty subsets of $\mathbb{Z}/m\mathbb{Z}$ with $|A|$, $|B|\geqslant 2$. Let c and d be different elements of $\mathbb{Z}/m\mathbb{Z}$ such that $\overline{A+B}=\{c,d\}$. Then $|A+B|=|A|+|B|-1$ ensures that at least one of the following statements holds*:

(S1) *If $d-c\in U(\mathbb{Z}/m\mathbb{Z})$, then A and B are arithmetic progressions with the same common difference $d-c$.*

(S2) *If $d-c\notin U(\mathbb{Z}/m\mathbb{Z})$ and $I_{A,d-c}=\emptyset$, then A is an arithmetic progression with common difference $d-c$ and*

$$\Big|A+\bigcup_{j\in J_{B,d-c}}B_{j,d-c}\Big|=|A|+\Big|\bigcup_{j\in J_{B,d-c}}B_{j,d-c}\Big|-1.$$

(S3) *If $d-c\notin U(\mathbb{Z}/m\mathbb{Z})$ and $I_{A,d-c}\neq\emptyset$, then $\big|\bigcup_{j\in J_{A,d-c}}A_{j,d-c}\big|=0,1$ or*

$$\bigcup_{j\in J_{A,d-c}}A_{j,d-c}\subsetneqq x_{s,d-c}+\langle d-c\rangle$$

is an arithmetic progression with common difference $d-c$ *for some* $1 \leqslant s \leqslant t(d-c)$. *And*

$$\begin{cases} |(\widetilde{A} \cup \{x_{s,d-c}\}) + \widetilde{B}| \leqslant |(\widetilde{A} \cup \{x_{s,d-c}\})| + |\widetilde{B}| - 1, & \text{if } x_{s,d-c} + \widetilde{B} \subseteq \widetilde{A} + \widetilde{B} + \langle d-c \rangle, \\ |\widetilde{A} + \widetilde{B}| \leqslant |\widetilde{A}| + |\widetilde{B}| - 1, & \text{otherwise}, \end{cases}$$

where $\widetilde{A} = \{x_{i,d-c} : i \in I_{A,d-c}\}$ *and* $\widetilde{B} = \{x_{i,d-c} : B_{i,d-c} \neq \emptyset\}$.

Corollary 1.1 *Let* $m \geqslant 2$, *and let* A, B *be nonempty subsets of* $\mathbb{Z}/m\mathbb{Z}$ *with* $|A|, |B| \geqslant 2$ *and* $|A+B| = |A|+|B|-1$. *Let* c *and* d *be different elements of* $\mathbb{Z}/m\mathbb{Z}$ *such that* $\overline{A+B} = \{c, d\}$. *Let* $\widetilde{A} = \{x_{i,d-c} : i \in I_{A,d-c}\}$ *and* $\widetilde{B} = \{x_{i,d-c} : B_{i,d-c} \neq \emptyset\}$. *If* A *is not an arithmetic progression with common difference* $d-c$ *and* $A \setminus \{0\} \subseteq U(\mathbb{Z}/m\mathbb{Z})$, $0 \in \widetilde{A}$, *then*

$$\begin{cases} |(\widetilde{A} \cup \{x_{s,d-c}\}) + \widetilde{B}| = |(\widetilde{A} \cup \{x_{s,d-c}\})| + |\widetilde{B}| - 1, & \text{if } x_{s,d-c} + \widetilde{B} \subseteq \widetilde{A} + \widetilde{B} + \langle d-c \rangle, \\ |\widetilde{A} + \widetilde{B}| = |\widetilde{A}| + |\widetilde{B}| - 1, & \text{otherwise}, \end{cases}$$

where $1 \leqslant s \leqslant t(d-c)$ *such that* $\bigcup\limits_{j \in J_{A,d-c}} A_{j,d-c} \subsetneqq x_{s,d-c} + \langle d-c \rangle$.

2 Lemmas

Lemma 2.1 *Let* $m \geqslant 2$, *and let* A *be a nonempty subset of* $\mathbb{Z}/m\mathbb{Z}$. *If* $g \in (\mathbb{Z}/m\mathbb{Z})^\star$, *then* $A = g + A$ *if and only if*

$$A = \bigcup_{i \in I_{A,g}} A_{i,g}.$$

Proof (Sufficiency) For any $i \in I_{A,g}$, we have $A_{i,g} = x_{i,g} + \langle g \rangle$, thus

$$g + A_{i,g} = x_{i,g} + \langle g \rangle = A_{i,g}.$$

Hence

$$A = \bigcup_{i \in I_{A,g}} A_{i,g} = \bigcup_{i \in I_{A,g}} (g + A_{i,g}) = g + \bigcup_{i \in I_{A,g}} A_{i,g} = g + A.$$

(Necessity) For any $i \in \{1, \cdots, t(g)\}$, by $A = g + A$, we have

$$g + A_{i,g} = (g + A) \cap (x_{i,g} + \langle g \rangle) = A \cap (x_{i,g} + \langle g \rangle) = A_{i,g}. \tag{2.1}$$

Now, we shall show that $A_{i,g}$ is either empty or equal to $x_{i,g} + \langle g \rangle$ for some $1 \leqslant i \leqslant t(g)$.

If $A_{i,g} \neq \emptyset$, then by the definition of $A_{i,g}$, we have

$$A_{i,g} = A \cap (x_{i,g} + \langle g \rangle) \subseteq x_{i,g} + \langle g \rangle. \tag{2.2}$$

Moreover, for any $x \in A_{i,g}$, by (2.1), we have

$$x + g, \cdots, x + |\langle g \rangle| \cdot g \in A_{i,g}.$$

Thus

$$|A_{i,g}| = |\langle g \rangle| = |x_{i,g} + \langle g \rangle|. \tag{2.3}$$

By (2.2) and (2.3), we have $A_{i,g} = x_{i,g} + \langle g \rangle$. Hence

$$A = \bigcup_{i \in I_{A,g}} A_{i,g}.$$

Lemma 2.2 *Let $m \geqslant 2$, and let A be a nonempty subset of $\mathbb{Z}/m\mathbb{Z}$. If $c, d \in \mathbb{Z}/m\mathbb{Z}$ are two different elements, then $|(c-A) \cap (d-A)| = |A| - 1$ if and only if*

$$A = A_0 \cup \Big(\bigcup_{i \in I_{A,g}} A_{i,g} \Big),$$

where $g = d - c$, $|A_0| = 1$ or A_0 is an arithmetic progression with common difference g and $1 < |A_0| < |\langle g \rangle|$.

Proof Let $g = d - c$. Write

$$H = \bigcup_{i \in I_{A,g}} A_{i,g}, \quad A_0 = \bigcup_{j \in J_{A,g}} A_{j,g}.$$

By Lemma 2.1, we have $H = g + H$, and thus $c - H = d - H$. Since

$$\begin{aligned}(c-A) \cap (d-A) &= (c - (A_0 \cup H)) \cap (d - (A_0 \cup H)) \\ &= [(c-A_0) \cap (d-A_0)] \cup [(c-H) \cap (d-H)] \\ &\quad \cup [(c-A_0) \cap (d-H)] \cup [(c-H) \cap (d-A_0)] \\ &= [(c-A_0) \cap (d-A_0)] \cup [(c-H) \cap (d-H)] \\ &= [(c-A_0) \cap (d-A_0)] \cup (c-H),\end{aligned}$$

we have $|(c-A) \cap (d-A)| = |A| - 1$ if and only if

$$|(c-A_0) \cap (d-A_0)| = |A_0| - 1. \tag{2.4}$$

(Sufficiency) If $|A_0| = 1$, then $|(c-A_0) \cap (d-A_0)| = 0 = |A_0| - 1$. By (2.4), we have $|(c-A) \cap (d-A)| = |A| - 1$. Now we consider $|A_0| > 1$. Since A_0 is an arithmetic progression with common difference g and $|A_0| < |\langle g \rangle|$, without loss of generality, we may assume

$$A_0 = \{a + ig : 0 \leqslant i \leqslant q - 1\}.$$

Then

$$\begin{aligned}d - A_0 &= \{d - a - ig : 0 \leqslant i \leqslant q-1\}, \\ c - A_0 &= \{c - a - ig : 0 \leqslant i \leqslant q-1\} = \{d - a - (i+1)g : 0 \leqslant i \leqslant q-1\}.\end{aligned}$$

Thus $|(c-A_0) \cap (d-A_0)| = |A_0| - 1$. By (2.4), we have $|(c-A) \cap (d-A)| = |A| - 1$.

(Necessity) By Lemma 2.1, we have $A_0 \neq \emptyset$. By the definition of $J_{A,g}$, we have $J_{A,g} \neq \emptyset$. For $j \in J_{A,g}$, we have $A_{j,g} \subsetneqq x_{j,g} + \langle g \rangle$. By Lemma 2.1, we have $A_{j,g} \neq g + A_{j,g}$, that is, $c - A_{j,g} \neq d - A_{j,g}$. Thus

$$|(c - A_{j,g}) \cap (d - A_{j,g})| \leqslant |A_{j,g}| - 1, \quad j \in J_{A,g}.$$

Hence

$$|(c - A_0) \cap (d - A_0)| = \sum_{j \in J_{A,g}} |(c - A_{j,g}) \cap (d - A_{j,g})| \leqslant \sum_{j \in J_{A,g}} |A_{j,g}| - |J_{A,g}| = |A_0| - |J_{A,g}|.$$

By (2.4), we have $|J_{A,g}| \leqslant 1$. Since $J_{A,g} \neq \emptyset$, we have $|J_{A,g}| = 1$.

It is easy to see that the condition $|(c - A_0) \cap (d - A_0)| = |A_0| - 1$ holds for $|A_0| = 1$. Now we assume $|A_0| > 1$. Since $A_0 \subsetneqq x_{j,g} + \langle g \rangle$ for some $j \in \{1, \cdots, t(g)\} \backslash I_{A,g}$, we may assume

$$A_0 = \{x_{j,g} + l_1 g, x_{j,g} + l_2 g, \cdots, x_{j,g} + l_q g\},$$

where $2 \leqslant q < |\langle g \rangle|$ and $0 \leqslant l_1 < \cdots < l_q \leqslant |\langle g \rangle| - 1$. Hence

$$d - A_0 = \{d - x_{j,g} - l_1 g, \cdots, d - x_{j,g} - l_q g\}, \tag{2.5}$$

$$\begin{aligned} c - A_0 &= \{c - x_{j,g} - l_1 g, \cdots, c - x_{j,g} - l_q g\} \\ &= \{d - x_{j,g} - (l_1 + 1)g, \cdots, d - x_{j,g} - (l_q + 1)g\}. \end{aligned} \tag{2.6}$$

By (2.4), we have

$$|(c - A_0) \cup (d - A_0)| = |A_0| + 1 = q + 1. \tag{2.7}$$

We divide the problem into the following two cases.

Case 1 $c - x_{j,g} - l_q g \notin d - A_0$. Since

$$\{c - x_{j,g} - l_i g : 1 \leqslant i \leqslant q - 1\} \subseteq d - A_0$$

and

$$|(c - A_0) \cup \{d - x_{j,g} - l_1 g\}| = q + 1,$$

we have

$$(c - A_0) \cup (d - A_0) = (c - A_0) \cup \{d - x_{j,g} - l_1 g\}. \tag{2.8}$$

By (2.5)–(2.6), (2.8) and $l_i + 1 \leq l_{i+1}, i = 1, \cdots, q - 1$, we have

$$d - x_{j,g} - (l_i + 1)g = d - x_{j,g} - l_{i+1} g, \quad i = 1, \cdots, q - 1.$$

Thus

$$l_i + 1 = l_{i+1}, \quad i = 1, \cdots, q - 1.$$

Hence, A_0 is an arithmetic progression with common difference g.

Case 2 $c - x_{j,g} - l_q g \in d - A_0$. By (2.4), there exists a unique $1 \leqslant k \leqslant q - 1$ such that

$$c - x_{j,g} - l_k g \notin d - A_0.$$

Thus

$$\{c - x_{j,g} - l_i g : 1 \leqslant i \leqslant q, i \neq k\} = \{d - x_{j,g} - (l_i + 1)g : 1 \leqslant i \leqslant q, i \neq k\} \subseteq d - A_0.$$

Again by (2.5)–(2.6) and $l_i + 1 \leq l_{i+1}, i = 1, \cdots, q - 1$, we have

$$d - x_{j,g} - (l_i + 1)g = d - x_{j,g} - l_{i+1} g, \quad i = 1, \cdots, q - 1, \quad i \neq k$$

and

$$c - x_{j,g} - l_q g = d - x_{j,g} - l_1 g.$$

Thus

$$l_i + 1 = l_{i+1}, \quad i = 1, \cdots, q-1, \quad i \neq k.$$

Hence, $A_0 = \{x_{j,g} + l_{k+1}g, \cdots, x_{j,g} + l_q g, x_{j,g} + l_1 g, \cdots, x_{j,g} + l_k g\}$ is an arithmetic progression with common difference g.

Lemma 2.3 *Let $m \geqslant 2$, $g \in (\mathbb{Z}/m\mathbb{Z})^\star$, and let A, B be nonempty subsets of $\mathbb{Z}/m\mathbb{Z}$ such that* $\min(|A|, |B|) \geqslant 2$ *and*

$$|A + B| = |A| + |B| - 1.$$

If $A \subsetneqq x_{s,g} + \langle g\rangle$ for some $1 \leqslant s \leqslant t(g)$, then

$$\Big|A + \bigcup_{j \in J_{B,g}} B_{j,g}\Big| = |A| + \Big|\bigcup_{j \in J_{B,g}} B_{j,g}\Big| - 1.$$

Proof Since

$$B = \Big(\bigcup_{i \in I_{B,g}} B_{i,g}\Big) \cup \Big(\bigcup_{j \in J_{B,g}} B_{j,g}\Big),$$

we have

$$|B| = \Big|\bigcup_{j \in J_{B,g}} B_{j,g}\Big| + |I_{B,g}| \cdot |\langle g\rangle|. \tag{2.9}$$

Moreover, $A \subsetneqq x_{s,g} + \langle g\rangle$ for some $1 \leqslant s \leqslant t(g)$, we have

$$\Big(A + \bigcup_{i \in I_{B,g}} B_{i,g}\Big) \cap \Big(A + \bigcup_{j \in J_{B,g}} B_{j,g}\Big) = \emptyset$$

and

$$\begin{aligned} |A + B| &= \Big|\Big(A + \bigcup_{i \in I_{B,g}} B_{i,g}\Big) \cup \Big(A + \bigcup_{j \in J_{B,g}} B_{j,g}\Big)\Big| \\ &= \Big|\bigcup_{i \in I_{B,g}} (x_{s,g} + B_{i,g})\Big| + \Big|A + \bigcup_{j \in J_{B,g}} B_{j,g}\Big| \\ &= |I_{B,g}| \cdot |\langle g\rangle| + \Big|A + \bigcup_{j \in J_{B,g}} B_{j,g}\Big|. \end{aligned} \tag{2.10}$$

By (2.9), we have

$$|A| + |B| - 1 = |A| + |I_{B,g}| \cdot |\langle g\rangle| + \Big|\bigcup_{j \in J_{B,g}} B_{j,g}\Big| - 1. \tag{2.11}$$

By (2.10)–(2.11), we have

$$\Big|A + \bigcup_{j \in J_{B,g}} B_{j,g}\Big| = |A| + \Big|\bigcup_{j \in J_{B,g}} B_{j,g}\Big| - 1.$$

Lemma 2.4 *Let* $m \geqslant 2$ *and* $g \in U(\mathbb{Z}/m\mathbb{Z})$. *Let* A *and* B *be nonempty subsets of* $\mathbb{Z}/m\mathbb{Z}$ *such that* $\min(|A|,|B|) \geqslant 2$ *and*

$$|A+B| = |A| + |B| - 1.$$

If A *is an arithmetic progression with common difference* g, *then* B *is an arithmetic progression with the same common difference.*

Proof The method of the proof originates from [10, Lemma 2.4], we omit the details.

Lemma 2.5 *Let* $m \geqslant 2$, $g \in (\mathbb{Z}/m\mathbb{Z})^\star$, *and let* A, B *be nonempty subsets of* $\mathbb{Z}/m\mathbb{Z}$ *such that* $\min(|A|,|B|) \geqslant 2$ *and*

$$|A+B| = |A| + |B| - 1.$$

If $I_{A,g} \neq \emptyset$ *and* $|\bigcup_{j \in J_{A,g}} A_{j,g}| = 0, 1$ *or* $\bigcup_{j \in J_{A,g}} A_{j,g} \subsetneqq x_{s,g} + \langle g \rangle$ *is an arithmetic progression with common difference* g *for some* $1 \leqslant s \leqslant t(g)$, *then*

$$\begin{cases} |(\widetilde{A} \cup \{x_{s,g}\}) + \widetilde{B}| \leqslant |(\widetilde{A} \cup \{x_{s,g}\})| + |\widetilde{B}| - 1, & \text{if } x_{s,g} + \widetilde{B} \subseteq \widetilde{A} + \widetilde{B}, \\ |\widetilde{A} + \widetilde{B}| \leqslant |\widetilde{A}| + |\widetilde{B}| - 1, & \text{otherwise}, \end{cases}$$

where $\widetilde{A} = \{x_{i,g} \in \mathbb{Z}/m\mathbb{Z} : i \in I_{A,g}\}$ *and* $\widetilde{B} = \{x_{i,g} \in \mathbb{Z}/m\mathbb{Z} : B_{i,g} \neq \emptyset\}$.

Proof Write $A_0 = \bigcup_{j \in J_{A,g}} A_{j,g}$. Since $I_{A,g} \neq \emptyset$, we have $\widetilde{A} \neq \emptyset$, and thus

$$|A+B| = \Big|\bigcup_{x \in \widetilde{A}+\widetilde{B}} (x + \langle g \rangle) \cup (A_0 + B)\Big|, \tag{2.12}$$

$$|A| + |B| - 1 = |A_0| + |\widetilde{A}| \cdot |\langle g \rangle| + |B| - 1. \tag{2.13}$$

If $A_0 = \emptyset$, then

$$|A+B| = \Big|\bigcup_{x \in \widetilde{A}+\widetilde{B}} (x + \langle g \rangle)\Big| = |\widetilde{A} + \widetilde{B}| \cdot |\langle g \rangle|.$$

By (2.12)–(2.13), we have

$$|\widetilde{A} + \widetilde{B}| \cdot |\langle g \rangle| = |\widetilde{A}| \cdot |\langle g \rangle| + |B| - 1 < (|\widetilde{A}| + |\widetilde{B}|) \cdot |\langle g \rangle|.$$

Hence

$$|\widetilde{A} + \widetilde{B}| \leqslant |\widetilde{A}| + |\widetilde{B}| - 1.$$

Now we consider that $A_0 \subsetneqq x_{s,g} + \langle g \rangle$ is an arithmetic progression with common difference g for some $1 \leqslant s \leqslant t(g)$. We divide it into the following two cases.

Case 1 There exists an element $b \in \widetilde{B}$ such that $x_{s,g} + b \notin \widetilde{A} + \widetilde{B} + \langle g \rangle$. If

$$(\widetilde{A} + \widetilde{B} + \langle g \rangle) \cap (A_0 + b) \neq \emptyset.$$

Then $A_0 + b \subseteq \widetilde{A} + \widetilde{B} + \langle g \rangle$. Since $A_0 + b \subsetneqq x_{s,g} + b + \langle g \rangle$, we have

$$x_{s,g} + b + \langle g \rangle \subseteq \widetilde{A} + \widetilde{B} + \langle g \rangle.$$

Thus $x_{s,g} + b \in \widetilde{A} + \widetilde{B} + \langle g \rangle$, which is false. Hence

$$(\widetilde{A} + \widetilde{B} + \langle g \rangle) \cap (A_0 + b) = \emptyset.$$

So

$$|A + B| \geqslant \Big| \bigcup_{a \in \widetilde{A} + \widetilde{B}} (a + \langle g \rangle) \Big| + |A_0 + b| = |\widetilde{A} + \widetilde{B}| \cdot |\langle g \rangle| + |A_0|.$$

Again by (2.12)–(2.13), we have

$$|\widetilde{A} + \widetilde{B}| \cdot |\langle g \rangle| + |A_0| \leqslant |A_0| + |\widetilde{A}| \cdot |\langle g \rangle| + |B| - 1 < |A_0| + (|\widetilde{A}| + |\widetilde{B}|) \cdot |\langle g \rangle|,$$

that is,

$$|\widetilde{A} + \widetilde{B}| \leqslant |\widetilde{A}| + |\widetilde{B}| - 1.$$

Case 2 $x_{s,g} + \widetilde{B} \subseteq \widetilde{A} + \widetilde{B}$. Then $(\widetilde{A} \cup \{x_{s,g}\}) + \widetilde{B} = \widetilde{A} + \widetilde{B}$. By (2.12)–(2.13), we have

$$|A + B| = |\widetilde{A} + \widetilde{B}| \cdot |\langle g \rangle| = |(\widetilde{A} \cup \{x_{s,g}\}) + \widetilde{B}| \cdot |\langle g \rangle|$$

and

$$|A| + |B| - 1 = |A_0| + |\widetilde{A}| \cdot |\langle g \rangle| + |B| - 1 < |A_0| + (|\widetilde{A}| + |\widetilde{B}|) \cdot |\langle g \rangle|.$$

Hence

$$|(\widetilde{A} \cup \{x_{s,g}\}) + \widetilde{B}| \leqslant |\widetilde{A}| + |\widetilde{B}| = |\widetilde{A} \cup \{x_{s,g}\}| + |\widetilde{B}| - 1.$$

The case $|A_0| = 1$ is similar to the above.

Lemma 2.6 *Let the notations be as in Lemma* 2.5 *and* $A \setminus \{0\} \subseteq U(\mathbb{Z}/m\mathbb{Z})$, $0 \in \widetilde{A}$. *Then*

$$\begin{cases} |(\widetilde{A} \cup \{x_{s,g}\}) + \widetilde{B}| = |(\widetilde{A} \cup \{x_{s,g}\})| + |\widetilde{B}| - 1, & \textit{if } x_{s,g} + \widetilde{B} \subseteq \widetilde{A} + \widetilde{B}, \\ |\widetilde{A} + \widetilde{B}| = |\widetilde{A}| + |\widetilde{B}| - 1, & \textit{otherwise}. \end{cases}$$

Proof Since $A \setminus \{0\} \subseteq U(\mathbb{Z}/m\mathbb{Z})$, we have $\widetilde{A} \setminus \{0\} \subseteq U(\mathbb{Z}/(m/|\langle g \rangle|)\mathbb{Z})$. By Theorem B,

$$\begin{aligned} &|\widetilde{A} + \widetilde{B}| \geqslant |\widetilde{A}| + |\widetilde{B}| - 1, \\ &|(\widetilde{A} \cup \{x_{s,g}\}) + \widetilde{B}| \geqslant |(\widetilde{A} \cup \{x_{s,g}\})| + |\widetilde{B}| - 1. \end{aligned}$$

So we obtain the conclusion by Lemma 2.5.

3 Proofs

Proof of Theorem 1.1 Since $\overline{A + B} = \{c, d\}$, we have $c, d \notin A + B$, and thus

$$B \cap (c - A) = \emptyset, \quad B \cap (d - A) = \emptyset.$$

Hence $B \subseteq \overline{(c - A)} \cap \overline{(d - A)}$, so

$$|B| \leqslant |\overline{(c - A)} \cap \overline{(d - A)}|. \tag{3.1}$$

Moreover,

$$|\overline{(c - A)} \cap \overline{(d - A)}| \leqslant |\overline{(c - A)}| = m - |A|.$$

Since $|A+B| = |A| + |B| - 1 = m-2$, we have

$$|\overline{(c-A)} \cap \overline{(d-A)}| \leqslant m - ((m-2) - |B| + 1) = |B| + 1. \tag{3.2}$$

By (3.1)–(3.2), we have $|\overline{(c-A)} \cap \overline{(d-A)}| = |B|$ or $|B|+1$.

If $|\overline{(c-A)} \cap \overline{(d-A)}| = |B|+1$, then

$$|B|+1 = |\overline{(c-A)} \cap \overline{(d-A)}| \leqslant |\overline{(c-A)}| = m - |c-A| = m - |A| = |B| + 1.$$

It follows that

$$|\overline{(c-A)} \cap \overline{(d-A)}| = |\overline{(c-A)}|.$$

Thus $\overline{(c-A)} = \overline{(d-A)}$. Hence $c-A = d-A$, so $A = d-c+A$. By Lemma 2.1, we have

$$A = \bigcup_{i \in I_{A,d-c}} A_{i,d-c}.$$

If $|\overline{(c-A)} \cap \overline{(d-A)}| = |B|$, then

$$|B| = |\overline{(c-A)} \cap \overline{(d-A)}| = m - (|c-A| + |d-A| - |(c-A) \cap (d-A)|).$$

Thus

$$|(c-A) \cap (d-A)| = (2|A| + |B|) - m = |A| - 1.$$

By Lemma 2.2, we have

$$A = A_0 \cup \Big(\bigcup_{i \in I_{A,d-c}} A_{i,d-c} \Big),$$

where $|A_0| = 1$ or A_0 is an arithmetic progression with common difference $d-c$.

In conclusion, we have

$$A = A_0 \cup \Big(\bigcup_{i \in I_{A,d-c}} A_{i,d-c} \Big),$$

where $|A_0| = 0, 1$ or A_0 is an arithmetic progression with common difference $d-c$.

Since $|A+B| = |A| + |B| - 1 = m-2$, we know that $A, B \subsetneqq \mathbb{Z}/m\mathbb{Z}$. We divide it into the following three cases.

Case 1 $d - c \in U(\mathbb{Z}/m\mathbb{Z})$. Then $\langle d-c \rangle = \mathbb{Z}/m\mathbb{Z}$. Thus $t(d-c) = [\mathbb{Z}/m\mathbb{Z} : \langle d-c \rangle] = 1$. Moreover, $A_0 \subsetneqq \mathbb{Z}/m\mathbb{Z}$, hence $\widetilde{A} = \emptyset$, so $A = A_0$. Since $|A| \geqslant 2$, we have $|A_0| \geqslant 2$. Therefore, A is an arithmetic progression with common difference $d-c$. By Lemma 2.4, B is an arithmetic progression with the same common difference. Hence the statement (S1) holds.

Case 2 $\gcd(d-c, m) > 1$ and $\widetilde{A} = \emptyset$. Then $A = A_0$. Since $|A| \geqslant 2$, we have $|A_0| \geqslant 2$. Therefore, A is an arithmetic progression with common difference $d-c$, thus $A \subsetneqq x_{s,d-c} + \langle d-c \rangle$ for some $1 \leqslant s \leqslant t(d-c)$. By Lemma 2.3, we obtain the statement (S2).

Case 3 $\gcd(d-c, m) > 1$ and $\widetilde{A} \neq \emptyset$. Then by Lemma 2.5, we obtain the statement (S3).

Proof of Corollary 1.2 It follows directly from Lemma 2.6 and Theorem 1.1.

Acknowledgement The authors would like to thank the referees for helpful comments and valuable suggestions.

Declarations

Conflicts of interest The authors declare no conflicts of interest.

References

[1] Cauchy, A. L., Recherches sur les nombres, *J. École polytech.*, **9**, 1813, 99–116.

[2] Chen, Y. G., On addition of two sets of integers, *Acta Arith.*, **80**, 1997, 83–87.

[3] Chowla, S., A theorem on the addition of residue classes: Applications to the number $\Gamma(s)$ in Waring's problem, *Proc. Indian Acad. Sci.*, **2**, 1935, 242–243.

[4] Christine, B., Oriol, S. and Gilles, Z., An analogue of Vosper's theorem for extension fields, *Math. Proc. Cambridge Philos. Soc.*, **163**, 2017, 423–452.

[5] Davenport, H., On the addition of residue classes, *J. London Math. Soc.*, **10**, 1935, 30–32.

[6] Du, S. S. and Pan, H., Restricted sumsets in finite nilpotent groups, *Acta Arith.*, **178**, 2017, 101–123.

[7] Guo, S. G., Restricted sumsets in a finite abelian group, *Discrete Math.*, **309**, 2009, 6530–6534.

[8] Kemperman, J. H. B., On small sumsets in an abelian group, *Acta Math.*, **103**, 1960, 63–88.

[9] Lev, V. F., Restricted set addition in groups. I. The classical setting, *J. London Math. Soc.*, **62**, 2000, 27–40.

[10] Nathanson, M. B., Additive number theory. The classical bases, *Graduate Texts in Math.,* **164**, Springer-Verlag, New York, 1996.

[11] Oriol, S.and Gilles, Z., On a generalization of a theorem by Vosper, **0**, 2000, 10pp.

[12] Shen, X. S. and Yuan, P. Z., An extension of the Kemperman structure theorem, *Acta Math. Sinica* (*Chin. Ser.*), **49**, 2006, 1339–1346.

[13] Tomas, B., Matt, D. and Amanda, M., A new proof of Kemperman's theorem, **15**, 2015, 20pp.

[14] Vosper, A. G., The critical pairs of subsets of a group of primes order, *J. London Math. Soc.*, **31**, 1956, 200–205.

[15] Vosper, A. G., Addendum to "The critical pairs of subsets of a group of primes order", *J. London Math. Soc.*, **31**, 1956, 280–282.