International Journal of Pure and Applied Mathematics

Volume 10 No. 2 2004, 161-168

ON SUMSETS $A + B$ WITH $|A| + |B| = |G|$

Shu-Guang Guo [§]

Department of Mathematics
Nanjing Normal University
Nanjing 210097, Jiangsu, P.R. CHINA
and
Department of Mathematics
Yancheng Teachers College
Yancheng, 224002, P.R. CHINA
e-mail: ychgsg@163.com

Abstract: Let G be a finite Abelian group written additively, A and B be nonempty subsets of G with $|A| + |B| = |G|$. In this paper we prove that the cardinality $|A + B|$ of the sumset $A + B = \{a + b : a \in A, b \in B\}$ takes on the values $|G| - k(k = 0, \text{or } 0 < k < |G| \text{ and } k||G|)$, and that both A and B are the union of some cosets of the subgroup $\{ g \in G : g + A + B = A + B \}$ if $|A + B| < |G|$.

AMS Subject Classification: 11B75, 20K01
Key Words: additive number theory, sumset, Abelian group

1. Introduction

Let G be a finite Abelian group written additively. For two subsets A and B of G, as usual, the sumset of A and B is defined as

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

and the stablizer of $A + B$ is defined as

Received: October 23, 2003

[§]Correspondence address: Department of Mathematics, Nanjing Normal University, Nanjing 210097, Jiangsu, P.R. CHINA

$$H = H(A+B) = \{\, g \in G : g + A + B = A + B \,\}.$$

It is readily seen that $H(A+B)$ is a subgroup of G and $H(A+B) = G$ if and only if $A + B = G$. We use the standard notation $|A|$ for the cardinality of the set A, and $gcd(a, b)$ for the greatest common divisor of two integers a and b.

Let p be a prime number and let A and B be two non-empty subsets of the cyclic group Z/pZ. The Cauchy-Davenport Theorem (see [4]) says that $|A + B| \geq \min(p, |A| + |B| - 1)$. For Abelian groups, the Cauchy-Davenport inequality fails for some subsets. A basic problem raised by Kneser [3] was to describe all the subsets A, B of an Abelian group G such that $|A + B| \leq |A| + |B| - 1$. Vosper [5, 6] solved this problem completely for groups with a prime order. Kempermann's theory [2] for small sums describes the structure of these pairs with $|A+B| = |A|+|B|-1$, if $A+B$ is aperiodic ($H(A+B) = \{0\}$) or if there exists a uniquely expressible element in $A + B$. If G contains a fixed subset B satisfying the inequality: for all A such that $1 \leq |A| < \infty, |A + B| \geq \min(|G|, |A| + |B| - 1)$, Hamidoune [1] obtained a recursive description for the subsets A such that $|A + B| \leq |A| + |B| - 1$.

It is well known (see [4]) that if $|A| + |B| > |G|$, then $A + B = G$. In this paper we attempt to determine the values which the cardinality of $A + B$ takes on, and to describe the structure of the subsets A and B of G such that $|A| + |B| = |G|$ and $|A + B| \leq |G| - 1 (= |A| + |B| - 1)$. We shall prove the following theorem.

Theorem 1. *Let G be an Abelian group of order n, A and B be two non-empty subsets of G with $|A| + |B| = n$. If $|A + B| \leq n - 1$, then*

$$A = \bigcup_{a \in A} (a + H), \quad B = \bigcup_{b \in B} (b + H), \quad |A + B| = n - |H|,$$

where $H = \{\, g \in G : g + A + B = A + B \,\}$ is the stablizer of $A + B$.

Theorem 2. *Let G be an Abelian group of order n, and k be an integer such that $k = 0$, or $0 < k < n$ and $k|n$. Then there exist two subsets A and B of G such that $|A| + |B| = n$ and $|A + B| = n - k$.*

Combining Theorem 1 and Theorem 2, we obtain the following Corollary 1 immediately.

Corollary 1. *Let G be an Abelian group of order n. Then*

$$\{\, |A + B| \,|\, \emptyset \neq A, B \subseteq G,\ |A| + |B| = n \} = \{\, n - k \,|\, k = 0, \text{ or } 0 < k < n \text{ and } k|n \,\}.$$

Remark. Corollary 1 shows that $\{\,|A+B|\,|\,\emptyset \neq A, B \subseteq G,\ |A|+|B|=n\}$ only depends on the cardinality of G, but not on its particular Abelian group structure.

Let H be a proper subgroup of G. The fact that both A and B are the union of some $H-$cosets and $|A|+|B|=n$ can't imply that $|A+B|=n-|H|$. For example, let $G=Z/12Z, H=\{0,4,8\}, A=\{1,2,5,6,9,10\}$, and $B=\{1,3,5,7,9,11\}$. Then we have $A+B=Z/12Z$. A natural question is to describe the necessary and sufficient condition of $|A+B|=n-k$. For $k=n/p$ with p being a prime factor of n. we have the following Theorem 3.

Theorem 3. *Let A and B be two non-empty subsets of G with $|A|+|B|=n$. Let p be a prime factor of n. Then*

$$|A+B|=n-\frac{n}{p},$$

if and only if there exists a subgroup H of order $\frac{n}{p}$ of G such that

$$A=\bigcup_{a\in A}(a+H), \quad B=\bigcup_{b\in B}(b+H),$$

and at least one of the following three conditions holds:

(i) A or B is only one $H-$coset,

(ii) $\{a+H\,|\,a\in A\}$ and $\{b+H\,|\,b\in B\}$ are arithmetic progressions with the same common difference in G/H,

(iii) there exists $c\in G$ such that

$$\{c-a+H\,|\,a\in A\}=(G/H)\setminus\{b+H\,|\,b\in B\}.$$

The direct application of Theorem 1 - Theorem 3 leads to following interesting corollaries.

Corollary 2. *Let G be an Abelian group of order n, and let A and B be two subsets of G with $|A|+|B|=n$. If $gcd(\,|A|,|B|\,)=1$, then $|A+B|\geq n-1$.*

Corollary 3. *Let A and B be two subsets of G with $|A|+|B|=n$. Then*

$$|A+B|\geq\frac{n}{2},$$

and equality occurs if and only if n is even and both A and B are cosets of some subgroup H of G with $|H| = \frac{n}{2}$.

Corollary 4. *Let A and B be two subsets of G with $|A| + |B| = n$ and $|A| \neq |B|$. Then*

$$|A + B| \geq \frac{2n}{3},$$

and equality occurs if and only if $3|n$, and one of A and B is a coset of some subgroup H of G with $|H| = \frac{n}{3}$ and the other is the union of two $H-$cosets.

Remark. The fact that $|A| + |B| = n$ and $gcd(\,|A|, |B|\,) > 1$ cannot imply $|A+B| < n-1$. For example, let $A = \{0, 1\} \subseteq Z/12Z$ and $B = \{2, 3, \cdots, 11\} \subseteq Z/12Z$, we have $A + B = \{0, 2, 3, \cdots, 11\}$. It is clear that $gcd(\,|A|, |B|\,) = 2$ but $|A + B| = n - 1$.

2. Proofs

In order to complete the proofs of our theorems, we need the following lemmas.

Lemma 1. (Kneser Theorem, [4]) *Let G be an Abelian group, and A and B be finite non-empty subsets of G. Let $H = H(A + B)$ be the stablizer of $A + B$. Then either $|A + B| \geq |A| + |B|$ or*

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

Lemma 2. (Vosper Theorem, [4]) *Let p be a prime number, and let A and B be non-empty subset of the group $G = Z/pZ$ 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:

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

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

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

Proof of Theorem 1. Since $|A + B| \leq n - 1 = |A| + |B| - 1$, it follows from Kneser Theorem that

$$|A + B| = |A + H| + |B + H| - |H| \geq |A| + |B| - |H| = n - |H|,$$

where $H=H(A+B)$ is the subgroup of G satisfying $H+A+B=A+B$. Therefore

$$A\subseteq A+H,\quad B\subseteq B+H,\quad |H|\big||A+B|.$$

By $|H|\big|n$ and $|A+B|<n$, we have $n-|H|\geq |A+B|$. From the above arguments we obtain

$$|A+B|=n-|H|,\quad |A+H|=|A|,\quad |B+H|=|B|.$$

Hence

$$A=A+H=\bigcup_{a\in A}(a+H),\quad B=B+H=\bigcup_{b\in B}(b+H).$$

This completes the proof of Theorem 1. □

Proof of Theorem 2. Case 1. $k=0$. If G is a simple group, we may assume that $G=Z/pZ$ with p prime. Let $A=\{0,1\}$ and $B=\{0,2,4,5,\cdots,p-1\}$. Then $|A|+|B|=p$ and $A+B=Z/pZ$. If G is not a simple group, then there is a subgroup H of G with $1<|H|<n$. Suppose that $H,a_1+H,\cdots,a_{m-1}+H$ are all the $H-$cosets. Let $a_0\in H$ and let

$$A=H,\quad B=\{a_0\}\cup((a_1+H)\backslash\{a_1\})\cup\bigcup_{i=2}^{m-1}(a_i+H).$$

Then $|A|+|B|=n$ and $A+B=G$.

Case 2. $0<k<n$ and $k|n$. Since G is an finite Abelian group, there exists a subgroup H of order k of G. Let $A=H$ and $B=G\backslash H$. Then $|A|+|B|=n$ and $A+B=G\backslash H$. Thus $|A+B|=n-k$. This completes the proof of Theorem 2. □

Proof of Theorem 3. Suppose that $|A+B|=n-\frac{n}{p}$. It follows that $H=H(A+B)\neq G$. By Theorem 1 we have

$$A=\bigcup_{a\in A}(a+H),\quad B=\bigcup_{b\in B}(b+H),\quad |A+B|=n-|H|.$$

Then $|H|=n/p$, and so $|G/H|=p$.

Let $\bar{A}=\{a+H\,|\,a\in A\}$, $\bar{B}=\{b+H\,|\,b\in B\}$. Then $\bar{A}$ and $\bar{B}$ are two non-empty subsets of quotient group G/H,

$$|\bar{A}|+|\bar{B}|=\frac{|A|}{|H|}+\frac{|B|}{|H|}=\frac{n}{|H|}=p$$

and

$$|\bar{A}+\bar{B}| = \frac{|A+B|}{|H|} = \frac{n-|H|}{|H|} = p-1 = |\bar{A}|+|\bar{B}|-1.$$

By Vosper Theorem, at least one of the following three conditions holds:

(1) $\min\{|\bar{A}|, |\bar{B}|\} = 1$,

(2) $\bar{A}$ and $\bar{B}$ are arithmetic progressions with the same common difference,

(3) there exists $\bar{c} = c + H \in G/H$ such that $\bar{c} - \bar{A} = (G/H) \setminus \bar{B}$.

It follows that at least one of the three conditions (i)-(iii) holds.

Conversely, if there exists a subgroup H of order n/p of G such that

$$A = \bigcup_{a\in A}(a+H), \quad B = \bigcup_{b\in B}(b+H), |A|+|B| = n\,,$$

and at least one of the three conditions (i)-(iii) holds. Let $\bar{A} = \{a+H \,|\, a \in A\}$, $\bar{B} = \{b+H \,|\, b \in B\}$. Then $\bar{A}$ and $\bar{B}$ are two non-empty subsets of quotient group G/H with

$$|\bar{A}|+|\bar{B}| = \frac{|A|}{|H|} + \frac{|B|}{|H|} = \frac{n}{|H|} = p.$$

If the sets A and B satisfy the conditions (i) or (ii), then it is easy to check that

$$|\bar{A}+\bar{B}| = |\bar{A}|+|\bar{B}|-1 = p-1.$$

If the sets A and B satisfy the conditions (iii), then $(c+H)-\bar{A} = (G/H)\setminus\bar{B}$. It follows that $c+H \notin \bar{A}+\bar{B}$, and so $|\bar{A}+\bar{B}| \le p-1$. Moreover, the Cauchy-Davenport Theorem implies that

$$|\bar{A}+\bar{B}| \ge |\bar{A}|+|\bar{B}|-1 = p-1.$$

Combining the above arguments, we have $|\bar{A}+\bar{B}| = p-1$. Therefore

$$|A+B| = |\bar{A}+\bar{B}||H| = n - \frac{n}{p}.$$

This completes the proof of Theorem 3. □

Proof of Corollary 2. Suppose that $|A+B| < n-1$. We claim that $|H| > 1$. Indeed, assume that $H(A+B) = \{0\}$. Since $|A|+|B| = n$, it follows from Kneser Theorem that

$$|A+B| = |A+H|+|B+H|-|H| = |A|+|B|-1 = n-1,$$

contradicting $|A+B| < n-1$. Therefore $|H| > 1$. By Theorem 1, we have $|H|\big|gcd(|A|,|B|)$. This contradicts $gcd(|A|,|B|) = 1$. Hence $|A+B| \geq n-1$. This completes the proof of Corollary 2. □

Proof of Corollary 3. Proof of Corollary 3 follows from Corollary 1 and Theorem 3 immediately. □

Proof of Corollary 4. Suppose that $|A+B| \leq n-1$. Then $H = H(A+B) \neq G$. Since $|A| \neq |B|$, it follows from Corollary 3 that $|A+B| \neq \frac{n}{2}$. By Corollary 1 we have

$$|A+B| = n - |H| \geq n - \frac{n}{3} = \frac{2n}{3}.$$

Now suppose that the equality occurs, then $|H| = \frac{n}{3}$. Hence $3|n$. Again by Theorem 1 we have that one of A and B is a $H-$coset and the other is the union of two $H-$cosets. Conversely, it is easy to check that if $3|n$, and one of A and B is a coset of some subgroup H of G with $|H| = \frac{n}{3}$ and the other is the union of two $H-$cosets, then $|A+B| = \frac{2n}{3}$. This completes the proof of Corollary 4. □

3. Acknowledgments

I am greatly indebted to Professor Yong-Gao Chen for his careful reading of the manuscript and for many helpful discussions.

This work is supported by the National Natural Science Foundation of China (Grant No.10201013).

References

[1] Y.O. Hamidoune, Subsets with a small sum II: The critical pair problem, *Europ. J. Combinatorics*, **21** (2000), 231-239.

[2] J.H.B. Kempermann, On small sumsets in Abelian groups, *Acta Math.*, **103** (1960), 63-88.

[3] M. Kneser, Summenmengen in lokalkompakten Abelesche Gruppen, *Math. Z.*, **66** (1956), 88-110.

[4] M.B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Grad. Texts in Math., **165**, Springer (1996).

[5] G. Vosper, The critical pairs of subsets of a group of prime order, *J. London Math. Soc.*, **31** (1956), 200-205.

[6] G. Vosper, Addendum to "The critical pairs of subsets of a group of prime order", *J. London Math. Soc.*, **31** (1956), 280-282.