第46卷第6期 数 学 进 展 Vol. 46, No. 6
2017年11月 ADVANCES IN MATHEMATICS (CHINA) Nov., 2017

doi: 10.11845/sxjz.2016131b

# On Partitioning $\mathbb{Z}_m$ Into Pairs of Prescribed Differences

CHENG Zhi*, SUN Cuifang**

(*School of Mathematics and Computer Science, Anhui Normal University, Wuhu, Anhui, 241003, P. R. China*)

**Abstract:** Let $m = 2n$ be a positive integer and $\mathbb{Z}_m$ be the ring of residue classes modulo $m$. Suppose $d_1, d_2, \cdots, d_n$ to be any odd elenents (not necessarily distinct) of $\mathbb{Z}_m$. In this paper, we give the sufficient and necessary condition of partitioning $\mathbb{Z}_m$ into $n$ pairs with differences $d_1, d_2, \cdots, d_n$. The conjecture on the seating couples problem proved by Kohen and Sadofschi Costa can be seen as a corollary of our result. Based on this work, we obtain two corollaries and we also confirm a conjecture of Kézdy and Snevily, which is the special case of our first corollary.

**Keywords:** partition; prescribed difference; ring of residue classes

**MR(2010) Subject Classification:** 11B13; 05B10; 05E15 / **CLC number:** O156

**Document code:** A **Article ID:** 1000-0917(2017)06-0952-05

## 0 Introduction

For any positive integer $m$, let $\mathbb{Z}_m = \{0, 1, \cdots, m-1\}$ be the ring of residue classes modulo $m$ and $\mathbb{Z}_m^*$ be the group of its units, i.e., $\mathbb{Z}_m^* = \{s : s \in \mathbb{Z}_m \text{ and } \gcd(s, m) = 1\}$. Let $S_m$ be the symmetric group of $m$ elements. In 2009, Preissmann and Mischler[6] proved the following conjecture, which is posed by Bacher.

**Conjecture 1** Let $p = 2n + 1$ be an odd prime. Suppose that we are given $n$ elements $d_1, d_2, \cdots, d_n \in \mathbb{Z}_p^*$. Then there exists a partition of $\mathbb{Z}_p^*$ into pairs with differences $d_1, d_2, \cdots, d_n$.

In 2012, Karasev and Petrov[2] gave two new proofs of this result with the algebraic and topological methods and provided further generalizations. They also posed the following two conjectures for further research.

**Conjecture 2**[2, Conjecture 1] Let $m = 2n + 1$ be a positive integer. Suppose that we are given $n$ elements $d_1, d_2, \cdots, d_n \in \mathbb{Z}_m^*$. Then there exists a partition of $\mathbb{Z}_m \setminus \{0\}$ into pairs with differences $d_1, d_2, \cdots, d_n$.

**Conjecture 3**[2, Conjecture 2] Let $m = 2n$ be a positive integer. Suppose that we are given $n$ elements $d_1, d_2, \cdots, d_n \in \mathbb{Z}_m^*$. Then there exists a partition of $\mathbb{Z}_m$ into pairs with differences $d_1, d_2, \cdots, d_n$.

In 2013, Mezei[5] showed that Conjecture 3 holds when $N = 2p$ for $p$ a prime number.

Received date: 2016-11-14. Revised date: 2017-02-21.
Foundation item: This work was supported by NSFC (No. 11471017) and the Doctoral Research Foundation and the Research Culture Foundation of Anhui Normal University (No. 2014xmpy11).
E-mail: * chengzhimath@126.com; ** cuifangsun@163.com

In 2016, Kohen and Sadofschi Costa[4] confirmed Conjecture 3. In this paper, we consider the partitions of $\mathbb{Z}_m$ into pairs with prescribed differences and obtain the following results.

**Theorem** Let $m = 2n$ be a positive integer and $d_1, d_2, \cdots, d_n$ be any odd elements (not necessarily distinct) of $\mathbb{Z}_m$. Then we can select $m$ distinct numbers $a_1, a_2, \cdots, a_n, b_1, b_2, \cdots, b_n \in \mathbb{Z}_m$ such that all $a_i$ are even, all $b_i$ are odd and $a_i + d_i \equiv b_i \pmod m$ for all $i = 1, 2, \cdots, n$ if and only if $\sum_{i=1}^n d_i \equiv n \pmod m$.

By Cauchy-Davenport Theorem, Kohen and Sadofschi Costa[4] showed that if $d_1, d_2, \cdots, d_n \in \mathbb{Z}_{2n}^*$, then there exist $s_1, s_2, \cdots, s_n \in \{1, -1\}$, such that

$$s_1 d_1 + s_2 d_2 + \cdots + s_n d_n \equiv n \pmod{2n}.$$

Thus Conjecture 3 can be seen as a corollary of our Theorem. We can also get the following two corollaries.

**Corollary 1** Let $n$ be a positive integer and $a$ be any element of $\mathbb{Z}_n$. Suppose that $d_1, d_2, \cdots, d_{n-1}$ are any elements (not necessarily distinct) of $\mathbb{Z}_n$. Then there is a permutation $\{a_1, a_2, \cdots, a_{n-1}\}$ of elements of $\mathbb{Z}_n \setminus \{a\}$ such that the sums

$$a_1 + d_1, \quad a_2 + d_2, \quad \cdots, \quad a_{n-1} + d_{n-1}$$

are pairwise distinct in $\mathbb{Z}_n$. Furthermore,

$$\{a_1 + d_1, a_2 + d_2, \cdots, a_{n-1} + d_{n-1}\} = \mathbb{Z}_n \setminus \{a - (d_1 + d_2 + \cdots + d_{n-1})\}.$$

**Corollary 2** Let $m = 2n + 1$ be a positive integer. Suppose that $d_1, d_2, \cdots, d_n$ are any elements (not necessarily distinct) of $\mathbb{Z}_m$. Then there is a permutation $\{a_1, a_2, \cdots, a_{2n}\}$ of elements of $\mathbb{Z}_m \setminus \{0\}$ such that

$$\{a_1 + d_1, a_2 + d_2, \cdots, a_n + d_n, a_{n+1} - d_1, a_{n+2} - d_2, \cdots, a_{2n} - d_n\} = \mathbb{Z}_m \setminus \{0\}.$$

**Remark 1** Kézdy-Snevily's conjecture in [3] is a special case of Corollary 1 on the condition that $a = 0$. The special case is particularly intriguing as it is closely related to $N$-permutations, which in turn are related to cyclic neofields.

**Remark 2** If $d_i = 0$ for $i = 1, 2, \cdots, n$, then Corollary 2 is trivial. If $d_i \in \mathbb{Z}_m \setminus \{0\}$ for $i = 1, 2, \cdots, n$, then by Corollary 2, we have

$$\{a_1 + d_1, a_2 + d_2, \cdots, a_n + d_n, a_{n+1} - d_1, a_{n+2} - d_2, \cdots, a_{2n} - d_n\} = \{a_1, a_2, \cdots, a_{2n}\}.$$

However, we can not claim that there exists a partition of $\mathbb{Z}_m \setminus \{0\}$ into pairs with differences $d_1, d_2, \cdots, d_n$.

**Example** Let $m = 15$ and $d_1 = 2$, $d_2 = 4$, $d_3 = 5$, $d_4 = 7$, $d_5 = 9$, $d_6 = 11$, $d_7 = 12$. If we choose $a_1 = 3$, $a_2 = 10$, $a_3 = 8$, $a_4 = 2$, $a_5 = 12$, $a_6 = 11$, $a_7 = 4$, $a_8 = 5$, $a_9 = 14$, $a_{10} = 13$, $a_{11} = 9$, $a_{12} = 6$, $a_{13} = 7$, $a_{14} = 1$, then

$$\{a_1 + d_1, a_2 + d_2, \cdots, a_7 + d_7, a_8 - d_1, a_9 - d_2, \cdots, a_{14} - d_7\} = \{a_1, a_2, \cdots, a_{14}\}.$$

Furthermore, we can obtain $a_{7+i} - a_i = d_i$ for $i = 1, 2, \cdots, 7$. However, if we choose $a_1 = 1$, $a_2 = 2$, $a_3 = 3$, $a_4 = 4$, $a_5 = 5$, $a_6 = 6$, $a_7 = 8$, $a_8 = 14$, $a_9 = 13$, $a_{10} = 12$, $a_{11} = 11$, $a_{12} = 10$, $a_{13} = 9$, $a_{14} = 7$, then we can not obtain the partitioning results by

$$\{a_1 + d_1, a_2 + d_2, \cdots, a_7 + d_7, a_8 - d_1, a_9 - d_2, \cdots, a_{14} - d_7\} = \{a_1, a_2, \cdots, a_{14}\}.$$

# 1 Proofs

To prove our Theorem, we need the following lemma.

**Lemma**[1] Let $G$ be an abelian group of order $n$ and $a_1, a_2, \cdots, a_n$ be a numbering of the elements of $G$. Let $d_1, d_2, \cdots, d_n \in G$ such that $\sum_{i=1}^n d_i = 0$. Then there are permutations $\sigma, \tau \in S_n$ such that

$$a_i - a_{\sigma(i)} = d_{\tau(i)}.$$

**Proof of Theorem** First we prove the necessity of Theorem. If $a_i + d_i \equiv b_i \pmod m$ for all $i = 1, 2, \cdots, n$, then

$$0 + 2 + \cdots + (2n-2) + \sum_{i=1}^n d_i = \sum_{i=1}^n (a_i + d_i) \equiv \sum_{i=1}^n b_i \equiv 1 + 3 + \cdots + (2n-1) \pmod m.$$

It follows that

$$\sum_{i=1}^n d_i \equiv n \pmod m.$$

Now we prove the sufficiency of Theorem. Suppose that $\sum_{i=1}^n d_i \equiv n \pmod m$. Then $\sum_{i=1}^n (d_i + 1) \equiv 0 \pmod m$. Since all $d_i + 1$ are even, we have

$$\sum_{i=1}^n \frac{d_i + 1}{2} \equiv 0 \pmod n.$$

By Lemma, there are permutations $\sigma, \tau \in S_n$, such that

$$i - \sigma(i) \equiv \frac{d_{\tau(i)} + 1}{2} \pmod n.$$

It implies that

$$(2i - 1) - 2\sigma(i) \equiv d_{\tau(i)} \pmod m,$$

or equally

$$2\sigma(i) + d_{\tau(i)} \equiv 2i - 1 \pmod m.$$

Without loss of generality, we suppose that $a_i = 2\sigma(i)$, $b_i = 2i - 1$, $d_{\tau(i)} = d_i$. Then we can select $m$ distinct numbers $a_1, a_2, \cdots, a_n, b_1, b_2, \cdots, b_n \in \mathbb{Z}_m$ such that all $a_i$ are even, all $b_i$ are odd and $a_i + d_i \equiv b_i \pmod m$ for all $i = 1, 2, \cdots, n$. $\square$

**Proof of Corollary 1** Let $d_i' \equiv 2d_i + 1 \pmod{2n}$ for $i = 1, 2, \cdots, n-1$ and let

$$d_n' \equiv n - \sum_{i=1}^{n-1} d_i' \equiv 1 - 2\sum_{i=1}^{n-1} d_i \pmod{2n}.$$

Then $d'_1, d'_2, \cdots, d'_n$ are all odd in $\mathbb{Z}_{2n}$ satisfying

$$\sum_{i=1}^{n} d'_i \equiv n \pmod{2n}.$$

By Theorem, there exist $n$ distinct even elements $b'_1, b'_2, \cdots, b'_n \in \mathbb{Z}_{2n}$ such that the sums $b'_i + d'_i$ are pairwise distinct in $\mathbb{Z}_{2n}$. Let $a'_i \equiv \frac{b'_i}{2} \pmod{n}$ for $i = 1, 2, \cdots, n$. Then

$$\{a'_1, a'_2, \cdots, a'_n\} = \mathbb{Z}_n.$$

Thus

$$\{a'_1 - (a'_n - a), a'_2 - (a'_n - a), \cdots, a'_n - (a'_n - a)\} = \mathbb{Z}_n.$$

Let $d_n \equiv \frac{d'_n - 1}{2} \pmod{n}$. Define

$$f : \mathbb{Z}_{2n} \setminus \{0, 2, \cdots, 2n-2\} \to \mathbb{Z}_n; \quad x \pmod{2n} \mapsto \frac{x-1}{2} \pmod{n}.$$

Then $f$ is a bijection. Since

$$\{b'_1 + d'_1, b'_2 + d'_2, \cdots, b'_n + d'_n\} = \mathbb{Z}_{2n} \setminus \{0, 2, \cdots, 2n-2\},$$

we have

$$\{a'_1 + d_1, a'_2 + d_2, \cdots, a'_n + d_n\} = \mathbb{Z}_n.$$

Thus

$$\{(a'_1 - (a'_n - a)) + d_1, (a'_2 - (a'_n - a)) + d_2, \cdots, (a'_n - (a'_n - a)) + d_n\} = \mathbb{Z}_n.$$

For $i = 1, 2, \cdots, n$, let $a_i = a'_i - (a'_n - a)$. Then

$$\{a_1, a_2, \cdots, a_{n-1}\} = \mathbb{Z}_n \setminus \{a\}$$

and

$$\{a_1 + d_1, a_2 + d_2, \cdots, a_{n-1} + d_{n-1}, a_n + d_n\} = \mathbb{Z}_n.$$

Thus there is a permutation $\{a_1, a_2, \cdots, a_{n-1}\}$ of elements of $\mathbb{Z}_n \setminus \{a\}$ such that the sums

$$a_1 + d_1, \quad a_2 + d_2, \quad \cdots, \quad a_{n-1} + d_{n-1}$$

are pairwise distinct in $\mathbb{Z}_n$ and

$$\{a_1 + d_1, a_2 + d_2, \cdots, a_{n-1} + d_{n-1}\} = \mathbb{Z}_n \setminus \{a - (d_1 + d_2 + \cdots + d_{n-1})\}.$$

This completes the proof of Corollary 1. □

**Proof of Corollary 2** For $i = 1, 2, \cdots, n$, let $d_{n+i} = -d_i$. For $i = 1, 2, \cdots, 2n$, let $d'_i \equiv 2d_i + 1 \pmod{2m}$. Let $d'_m \equiv m - \sum_{i=1}^{2n} d'_i \pmod{2m}$ and $d_m \equiv \frac{d'_m - 1}{2} \equiv 0 \pmod{m}$. Then $d_m \equiv 0 \pmod{m}$. By Corollary 1, we know that there is a permutation $\{a_1, a_2, \cdots, a_{2n}\}$ of elements of $\mathbb{Z}_m \setminus \{0\}$ such that the sums

$$a_1 + d_1, \quad a_2 + d_2, \quad \cdots, \quad a_n + d_n, \quad a_{n+1} + d_{n+1}, \quad a_{n+2} + d_{n+2}, \quad \cdots, \quad a_{2n} + d_{2n}$$

are pairwise distinct in $\mathbb{Z}_m$. Noticing that $d_1 + d_2 + \cdots + d_{2n} \equiv 0 \pmod{m}$, we have

$$\{a_1 + d_1, a_2 + d_2, \cdots, a_n + d_n, a_{n+1} - d_1, a_{n+2} - d_2 \cdots, a_{2n} - d_n\} = \mathbb{Z}_m \setminus \{0\}.$$

This completes the proof of Corollary 2. □

## References


[1] Hall, M.Jr., A combinatorial problem on abelian groups, *Proc. Amer. Math. Soc.*, 1952, 3(4): 584-587.

[2] Karasev, R.N. and Petrov, F.V., Partitions of nonzero elements of a finite field into pairs, *Israel J. Math.*, 2012, 192(1): 143-156.

[3] Kézdy, A.E. and Snevily, H.S., Distinct sums modulo $n$ and tree embeddings, *Combin. Probab. Comput.*, 2002, 11(1): 35-42.

[4] Kohen, D. and Sadofschi Costa, I., On a generalization of the seating couples problem, *Discrete Math.*, 2016, 339(12): 3017-3019.

[5] Mezei, T.R., Seating couples and Tic-Tac-Toe, Master's Thesis, Budapest: Eötvös Loránd University, 2013.

[6] Preissmann, E. and Mischler, M., Seating couples around the King's table and a new characterization of prime numbers, *Amer. Math. Monthly*, 2009, 116(3): 268-272.


# 关于将 $\mathbb{Z}_m$ 分拆为给定差的集合对


程 智, 孙翠芳

(安徽师范大学数学计算机科学学院, 芜湖, 安徽, 241003)



**摘要:** 设 $m = 2n$ 是正整数, $\mathbb{Z}_m$ 是模 $m$ 的剩余类环. 设 $d_1, d_2, \cdots, d_n$ 是 $\mathbb{Z}_m$ 中的任意奇元素 (没必要不同). 本文给出了将 $\mathbb{Z}_m$ 分拆为差是 $d_1, d_2, \cdots, d_n$ 的集合对的充分必要条件. 由 Kohen 和 Sadofschi Costa 证明的关于夫妇座位问题的猜想可看成是本文结果的一个推论. 本文在此基础上获得了两个推论, 并证明了 Kézdy 和 Snevily 的一个猜想, 该猜想是第一个推论的特殊情形.



**关键词:** 分拆; 给定差; 剩余类环