

การศึกษาปัญหาของผลแบ่งกันของจำนวนเต็มมอดุโล m โดยที่ฟังก์ชันตัวแทนเท่ากัน

Study on a problem of partitions of the integer modulo m with identical representation functions

สุภาดา โตกระแสร¹, นเรศ สวัสดิ์รักษา^{2*}, สมบูรณ์ นิยม², ศศิโสพิท บัวดา²

Supada Tokrasae¹, Nares Sawatraksa^{2*}, Somboon Niyom², Sasisophit Buada²

¹หลักสูตรวิทยาศาสตรมหาบัณฑิต การสอนคณิตศาสตร์, สาขาวิชาคณิตศาสตร์และสถิติ,
คณะวิทยาศาสตร์และเทคโนโลยี, มหาวิทยาลัยราชภัฏนครสวรรค์

¹Master of Science Program in Teaching Mathematics, Division of Mathematics and Statistics,
Faculty of Science and Technology, Nakhon Sawan Rajabhat University

²สาขาวิชาคณิตศาสตร์และสถิติ, คณะวิทยาศาสตร์และเทคโนโลยี, มหาวิทยาลัยราชภัฏนครสวรรค์

²Division of Mathematics and Statistics, Faculty of Science and Technology,
Nakhon Sawan Rajabhat University

บทคัดย่อ

สำหรับทุกจำนวนเต็มบวก m กำหนดให้ $\mathbb{Z}_m$ แทนเซตของชั้นส่วนตกค้างมอดุโล m ซึ่ง $\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$ เมื่อ $\bar{x} = \{y \in \mathbb{Z} : x \equiv y \pmod{m}\}$ กำหนดนิยามอันดับ $\prec$ บนเซต $\mathbb{Z}_m$ ดังนี้ $0 \prec 1 \prec 2 \prec 3 \prec \dots \prec m-1$ และ $\bar{a} \preceq \bar{b}$ ก็ต่อเมื่อ $\bar{a} = \bar{b}$ หรือ $\bar{a} \prec \bar{b}$ สำหรับเซตย่อย $A \subseteq \mathbb{Z}_m$ และ $\bar{n} \in \mathbb{Z}_m$ กำหนดให้

$$R_3(A, \bar{n}) = \left| \{(\bar{a}, \bar{b}) \in A \times A : a + b \equiv n \pmod{m}, \bar{a} \preceq \bar{b}\} \right|$$

ในงานวิจัยฉบับนี้ คณะผู้วิจัยศึกษาปัญหาของ Sárközy ใน $\mathbb{Z}_m$ โดยที่เซตย่อย A และ B ของ $\mathbb{Z}_m$ และ $|(A \cup B) \setminus (A \cap B)| = m-3$ ที่ทำให้ $R_3(A, \bar{n}) = R_3(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ เมื่อ m เป็นจำนวนคี่

คำสำคัญ: ผลแบ่งกัน ฟังก์ชันตัวแทน เซตของชั้นส่วนตกค้างมอดุโล m

Abstract

For every positive integer m , let $\mathbb{Z}_m$ denote the set of residue classes modulo m such that $\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$ when $\bar{x} = \{y \in \mathbb{Z} : x \equiv y \pmod{m}\}$. Define order $\prec$ on $\mathbb{Z}_m$ by $0 \prec 1 \prec 2 \prec 3 \prec \dots \prec m-1$ and define $\bar{a} \preceq \bar{b}$ if and only if $\bar{a} = \bar{b}$ or $\bar{a} \prec \bar{b}$. For a subset $A \subseteq \mathbb{Z}_m$ and $\bar{n} \in \mathbb{Z}_m$, let

* Corresponding author: nares.sa@nsru.ac.th

$$R_3(A, \bar{n}) = \left| \left\{ (\bar{a}, \bar{b}) \in A \times A : a + b \equiv n \pmod{m}, \bar{a} \preceq \bar{b} \right\} \right|.$$

In this paper, we study Sárközy's problem in $\mathbb{Z}_m$ with two subsets A and B of $\mathbb{Z}_m$ and $|(A \cup B) \setminus (A \cap B)| = m - 3$ such that $R_3(A, \bar{n}) = R_3(B, \bar{n})$ for all $\bar{n} \in \mathbb{Z}_m$, when m is an odd integer.

Keywords: partition, representation function, set of residue classes modulo m

1. บทนำ

ให้ X เป็นอาบีเลียนกึ่งกรุปการบวก สำหรับทุก $A \subseteq X$ และ $n \in X$ ให้ $R_1(A, n)$ แทนจำนวนผลเฉลยของสมการ $a + b = n$ โดยที่คู่อันดับ $(a, b) \in A \times A$, $R_2(A, n)$ แทนจำนวนผลเฉลยของสมการ $a + b = n$ โดยที่คู่ไม่อันดับ $(a, b) \in A \times A$ ซึ่ง $a \neq b$ และ $R_3(A, n)$ แทนจำนวนผลเฉลยของสมการ $a + b = n$ โดยที่คู่ไม่อันดับ $(a, b) \in A \times A$ ในปี ค.ศ. 1978 Nathanson (Nathanson. 1978: 16–20) เรียกสัญลักษณ์ดังกล่าวว่า “ฟังก์ชันตัวแทน” ต่อจากนั้นมีนักคณิตศาสตร์จำนวนมากที่ให้ความสนใจในการศึกษาเกี่ยวกับฟังก์ชันตัวแทน เช่น Erdős Sárközy Dombi Yang และ Chen เป็นต้น

ให้ N แทนเซตของจำนวนเต็มที่ไม่เป็นลบ และสำหรับ $i \in \{1, 2, 3\}$ Sárközy (Erdős, Sárközy, Sós 1986: 183–197) ตั้งคำถามว่า “มีเซต $A, B \subseteq \mathbb{N}$ โดยที่ $|(A \cup B) \setminus (A \cap B)| = \infty$ ที่ทำให้ $R_i(A, \bar{n}) = R_i(B, \bar{n})$ สำหรับทุกจำนวนเต็ม n หรือไม่” ในปี ค.ศ. 2002 Dombi (Dombi. 2002: 137–146) ตอบคำถามของ Sárközy ว่า กรณี $i = 1$ ไม่มีเซตย่อย A และ B ของ $\mathbb{N}$ ที่สอดคล้องเงื่อนไขของ Sárközy และกรณี $i = 2$ มีเซตย่อย A และ B ของ $\mathbb{N}$ ที่สอดคล้องเงื่อนไขของ Sárközy และในปีต่อมา Chen และ Wang (Chen, & Wang. 2003: 299–303) พิสูจน์กรณี $i = 3$ มีสองเซตย่อย A และ B ของ $\mathbb{N}$ ที่สอดคล้องกับเงื่อนไขของ Sárközy จากแนวคิดดังกล่าวจึงทำให้นักคณิตศาสตร์หลายท่านให้ความสนใจปัญหาของ Sárközy บนเซตของจำนวนเต็มมอดุโล m

สำหรับจำนวนเต็มบวก m กำหนดให้ $\mathbb{Z}_m$ แทนเซตของชั้นส่วนตกค้างมอดุโล m นั่นคือ $\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$ โดยที่ $\bar{x} = \{y \in \mathbb{Z} : x \equiv y \pmod{m}\}$ และนิยามอันดับ $\prec$ บน $\mathbb{Z}_m$ ดังต่อไปนี้ $0 \prec 1 \prec 2 \prec 3 \prec \dots \prec m-1$ นอกจากนี้ นิยาม $\bar{a} \preceq \bar{b}$ ก็ต่อเมื่อ $\bar{a} = \bar{b}$ หรือ $\bar{a} \prec \bar{b}$ สำหรับ $A \subseteq \mathbb{Z}_m$ และ $\bar{n} \in \mathbb{Z}_m$ กำหนดให้

$$\begin{aligned} R_1(A, \bar{n}) &= \left| \left\{ (\bar{a}, \bar{b}) \in A \times A : \bar{a} \oplus \bar{b} = \bar{n} \right\} \right| \\ R_2(A, \bar{n}) &= \left| \left\{ (\bar{a}, \bar{b}) \in A \times A : \bar{a} \oplus \bar{b} = \bar{n}, \bar{a} \prec \bar{b} \right\} \right| \text{ และ} \\ R_3(A, \bar{n}) &= \left| \left\{ (\bar{a}, \bar{b}) \in A \times A : \bar{a} \oplus \bar{b} = \bar{n}, \bar{a} \preceq \bar{b} \right\} \right| \end{aligned}$$

เมื่อ $\bar{a} \oplus \bar{b} = \overline{a+b}$ สำหรับทุกจำนวนเต็ม a และ b

ในปี ค.ศ. 2012 Yang และ Chen (Yang, & Chen. 2012: 257–262) ได้ศึกษาปัญหาของ Sárközy ใน $\mathbb{Z}_m$ ซึ่งพวกเขากำหนดโครงสร้างของเซต $A, B \subseteq \mathbb{Z}_m$ โดยที่ $|(A \cup B) \setminus (A \cap B)| = m$ สำหรับ $i \in \{1, 2, 3\}$ ที่ทำให้ $R_i(A, \bar{n}) = R_i(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$

ในปี ค.ศ. 2017 Yang และ Tang (Yang, & Tang. 2017: 73–85) ศึกษาปัญหาผลแบ่งกันในกรณี m เป็นจำนวนคี่ โดยที่ $m \geq 3$ ว่า ไม่มีสองเซต $A, B \subseteq \mathbb{Z}_m$ โดยที่ $|(A \cup B) \setminus (A \cap B)| = m-1$ ที่ทำให้ $R_1(A, \bar{n}) = R_1(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ และสำหรับ $i=2$ และ $i=3$ มีสองเซตย่อย $A, B \subseteq \mathbb{Z}_m$ โดยที่ $|(A \cup B) \setminus (A \cap B)| = m-1$ ที่ทำให้ $R_i(A, \bar{n}) = R_i(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$

ในปี ค.ศ. 2021 Chen และ Yan (Chen, & Yan. 2021: 204–209) ศึกษาปัญหาผลแบ่งกันของ $\mathbb{Z}_m$ โดยที่ฟังก์ชันตัวแทนมีค่าเท่ากัน ซึ่งพวกเขาสามารถหาเงื่อนไขของสองเซตย่อย A และ B ของ $\mathbb{Z}_m$ โดยที่ $|(A \cup B) \setminus (A \cap B)| = m-2$ ที่ทำให้ $R_1(A, \bar{n}) = R_1(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ และในปี ค.ศ. 2020 พวกเขา (Chen, & Yan. 2020: 111981) ยังพิจารณากรณี $m = 2^\alpha$ และสามารถกำหนดเงื่อนไขของเซต $A, B \subseteq \mathbb{Z}_m$ โดยที่ $A \cup B = \mathbb{Z}_m$ และ $|A \cap B| = 2$ ที่ทำให้ $R_2(A, \bar{n}) = R_2(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ ต่อมาในปี ค.ศ. 2022 Sun และ Cheng (Sun, & Cheng. 2022: 352–363) พิจารณา $m = 2M$ เมื่อ M เป็นจำนวนคี่ โดยที่ $M \geq 3$ และพิสูจน์ว่ามีเซตย่อย $A, B \subseteq \mathbb{Z}_m$ โดยที่ $A \cup B = \mathbb{Z}_m$ และ $|A \cap B| = 2$ ที่ทำให้ $R_3(A, \bar{n}) = R_3(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ และเมื่อไม่นานมานี้ ในปี ค.ศ. 2023 Chen Wang และ Yu (Chen, & Wang, & Yu. 2023: 102533) สามารถกำหนดเงื่อนไขที่จำเป็นและเพียงพอสำหรับโครงสร้างของเซต $A, B \subseteq \mathbb{Z}_m$ โดยที่ $A \cup B = \mathbb{Z}_m$ และ $|A \cap B| = 2$ ที่ทำให้ $R_2(A, \bar{n}) = R_2(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ ในปี ค.ศ. 2023 สุภาดา โตกระแสรและนเรศ สวัสดิ์รักษา (สุภาดา, & นเรศ. 2023: 352–363) สามารถแสดงว่าไม่มีเซตย่อย $A, B \subseteq \mathbb{Z}_m$ ที่ทำให้ $R_1(A, \bar{n}) = R_1(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ และสามารถหาเงื่อนไขของเซตย่อย $A, B \subseteq \mathbb{Z}_m$ ที่ทำให้ $R_2(A, \bar{n}) = R_2(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$

จากแนวคิดดังกล่าว คณะผู้วิจัยสนใจศึกษาปัญหาผลแบ่งกันของ $\mathbb{Z}_m$ ในกรณีที่สองเซตย่อย A และ B ของ $\mathbb{Z}_m$ โดยที่ $|(A \cup B) \setminus (A \cap B)| = m-3$ สำหรับทุก $i \in \{1, 2, 3\}$ ที่ทำให้ $R_i(A, \bar{n}) = R_i(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ และนำเสนอเงื่อนไขของเซตย่อย $A, B \subseteq \mathbb{Z}_m$ ที่ทำให้ $R_3(A, \bar{n}) = R_3(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$

2. ผลการศึกษา

ในหัวข้อนี้ คณะผู้วิจัยศึกษาปัญหามผลแบ่งกันของ $\mathbb{Z}_m$ โดยที่ฟังก์ชันตัวแทนเท่ากัน ในกรณี $|(A \cup B) \setminus (A \cap B)| = m-3$ สำหรับ $A, B \subseteq \mathbb{Z}_m$ ดังต่อไปนี้

บทนิยาม 2.1 ให้ $A \subseteq \mathbb{Z}_m$ ฟังก์ชันตัวแทน คือ ฟังก์ชันที่มีโดเมนเป็น $\mathbb{Z}_m$ และเรนจ์เป็นเซตย่อยของ $\mathbb{N}$ นิยามโดย

$$R_3(A, \bar{n}) = \left| \{(\bar{a}, \bar{b}) \in A \times A : \bar{a} \oplus \bar{b} = \bar{n}, \bar{a} \leq \bar{b}\} \right| \text{ สำหรับทุก } \bar{n} \in \mathbb{Z}_m$$

เมื่อ N แทนเซตของจำนวนเต็มที่ไม่เป็นลบ

ต่อไปจะเป็นตัวอย่างการหาค่าของฟังก์ชันตัวแทน ในกรณี $m=11$ ดังนี้

ตัวอย่าง 2.1 ให้ $m=11$ จะได้ว่า $\mathbb{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ ให้

$$A = \{0, 2, 3, 5, 9\}$$

เนื่องจาก $R_3(A, \bar{n}) = \left| \left\{ (\bar{a}, \bar{b}) \in A \times A : \bar{a} \oplus \bar{b} = \bar{n}, \bar{a} \preceq \bar{b} \right\} \right|$ จะได้ว่า

$$R_3(A, 0) = \left| \left\{ (\bar{a}, \bar{b}) \in A \times A : \bar{a} \oplus \bar{b} = 0, \bar{a} \preceq \bar{b} \right\} \right| = \left| \left\{ (0, 0), (2, 9) \right\} \right| = 2$$

$$R_3(A, 1) = \left| \left\{ (\bar{a}, \bar{b}) \in A \times A : \bar{a} \oplus \bar{b} = 1, \bar{a} \preceq \bar{b} \right\} \right| = \left| \left\{ (3, 9) \right\} \right| = 1$$

$$R_3(A, 2) = \left| \left\{ (\bar{a}, \bar{b}) \in A \times A : \bar{a} \oplus \bar{b} = 2, \bar{a} \preceq \bar{b} \right\} \right| = \left| \left\{ (0, 2) \right\} \right| = 1$$

$$R_3(A, 3) = \left| \left\{ (\bar{a}, \bar{b}) \in A \times A : \bar{a} \oplus \bar{b} = 3, \bar{a} \preceq \bar{b} \right\} \right| = \left| \left\{ (0, 3), (5, 9) \right\} \right| = 2$$

$$R_3(A, 4) = \left| \left\{ (\bar{a}, \bar{b}) \in A \times A : \bar{a} \oplus \bar{b} = 4, \bar{a} \preceq \bar{b} \right\} \right| = \left| \left\{ (2, 2) \right\} \right| = 1$$

$$R_3(A, 5) = \left| \left\{ (\bar{a}, \bar{b}) \in A \times A : \bar{a} \oplus \bar{b} = 5, \bar{a} \preceq \bar{b} \right\} \right| = \left| \left\{ (0, 5), (2, 3) \right\} \right| = 2$$

$$R_3(A, 6) = \left| \left\{ (\bar{a}, \bar{b}) \in A \times A : \bar{a} \oplus \bar{b} = 6, \bar{a} \preceq \bar{b} \right\} \right| = \left| \left\{ (3, 3) \right\} \right| = 1$$

$$R_3(A, 7) = \left| \left\{ (\bar{a}, \bar{b}) \in A \times A : \bar{a} \oplus \bar{b} = 7, \bar{a} \preceq \bar{b} \right\} \right| = \left| \left\{ (2, 5), (9, 9) \right\} \right| = 2$$

$$R_3(A, 8) = \left| \left\{ (\bar{a}, \bar{b}) \in A \times A : \bar{a} \oplus \bar{b} = 8, \bar{a} \preceq \bar{b} \right\} \right| = \left| \left\{ (3, 5) \right\} \right| = 1$$

$$R_3(A, 9) = \left| \left\{ (\bar{a}, \bar{b}) \in A \times A : \bar{a} \oplus \bar{b} = 9, \bar{a} \preceq \bar{b} \right\} \right| = \left| \left\{ (0, 9) \right\} \right| = 1$$

$$R_3(A, 10) = \left| \left\{ (\bar{a}, \bar{b}) \in A \times A : \bar{a} \oplus \bar{b} = 10, \bar{a} \preceq \bar{b} \right\} \right| = \left| \left\{ (5, 5) \right\} \right| = 1$$

ในงานวิจัยนี้ เราสนใจศึกษาในกรณี $A, B \subseteq \mathbb{Z}_m$ โดยที่ $|(A \cup B) \setminus (A \cap B)| = m-3$ ที่ทำให้

$$R_3(A, \bar{n}) = R_3(B, \bar{n}) \text{ สำหรับทุก } \bar{n} \in \mathbb{Z}_m$$

พิจารณา $|(A \cup B) \setminus (A \cap B)| = m-3$ จะได้ว่าสามารถแบ่งเป็น 4 กรณี ดังนี้

1. $|A \cup B| = m$ และ $|A \cap B| = 3$
2. $|A \cup B| = m-1$ และ $|A \cap B| = 2$
3. $|A \cup B| = m-2$ และ $|A \cap B| = 1$
4. $|A \cup B| = m-3$ และ $|A \cap B| = 0$

เริ่มต้นจะพิจารณา m และจำนวนสมาชิกของเซต A และ B ของทั้ง 4 กรณีข้างต้น ดังต่อไปนี้

บทตั้ง 2.1 (Yang, & Tang, 2017: 73–85) ให้ $A \subseteq \mathbb{Z}_m$ จะได้ว่า

$$\sum_{n=0}^{m-1} R_3(A, \bar{n}) = \binom{|A|}{2} + |A|$$

ทฤษฎีบท 2.1 ให้ $A, B \subseteq \mathbb{Z}_m$ โดยที่ $|(A \cup B) \setminus (A \cap B)| = m-3$ ถ้า $R_3(A, \bar{n}) = R_3(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ แล้ว $|A| = |B|$ และ m เป็นจำนวนคี่

บทพิสูจน์ สมมติว่า $R_3(A, \bar{n}) = R_3(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ โดยบทตั้ง 2.1 จะได้ว่า

$$\binom{|A|}{2} + |A| = \sum_{n=0}^{m-1} R_3(A, \bar{n}) = \sum_{n=0}^{m-1} R_3(B, \bar{n}) = \binom{|B|}{2} + |B|$$

ให้ $|A| = k$ และ $|B| = l$ จะได้ว่า $k, l \geq 1$ และ

$$\frac{k(k-1)}{2} + k = \frac{l(l-1)}{2} + l$$

นั่นคือ $\frac{k^2 - k + 2k}{2} = \frac{l^2 - l + 2l}{2}$ เพราะฉะนั้น $k^2 + k = l^2 + l$ ทำให้ได้ว่า $(k+l)(k-l) = k^2 - l^2 = l - k$
ถ้า $k \neq l$ แล้ว $k-l \neq 0$ และ $k+l = -1$ ซึ่งเกิดข้อขัดแย้ง ดังนั้น $k = l$ นั่นคือ $|A| = |B|$ เนื่องจาก
 $|(A \cup B) \setminus (A \cap B)| = |A| + |B| - 2|A \cap B|$ และ $|(A \cup B) \setminus (A \cap B)| = m - 3$ จะได้ว่า

$$m - 3 = |(A \cup B) \setminus (A \cap B)| = |A| + |B| - 2|A \cap B| = 2|A| - 2|A \cap B| = 2(|A| - |A \cap B|)$$

ดังนั้น $m - 3$ เป็นจำนวนคู่ เพราะฉะนั้น m เป็นจำนวนคี่ □

หลังจากนี้เป็นต้นไป สมมติว่า m เป็นจำนวนคี่ โดยที่ $m \geq 5$

ทฤษฎีบท 2.2 ให้ $A, B \subseteq \mathbb{Z}_m$ โดยที่ $A \cup B = \mathbb{Z}_m$ และ $|A \cap B| = 3$ ถ้า $R_3(A, \bar{n}) = R_3(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ แล้ว $|A| = |B| = \frac{m+3}{2}$

บทพิสูจน์ สมมติว่า $R_3(A, \bar{n}) = R_3(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ โดยทฤษฎีบท 2.1 จะได้ว่า $|A| = |B|$ ดังนั้น

$$2|A| = |A| + |A| = |A| + |B| = |A \cup B| + |A \cap B| = m + 3$$

นั่นคือ $|A| = |B| = \frac{m+3}{2}$ □

สำหรับกรณี 2 – 4 สามารถพิสูจน์ในทำนองเดียวกับกรณีที่ 1 ดังผลลัพธ์ต่อไปนี้

ทฤษฎีบท 2.3 ให้ $A, B \subseteq \mathbb{Z}_m$ โดยที่ $|A \cup B| = m - 1$ และ $|A \cap B| = 2$ ถ้า $R_3(A, \bar{n}) = R_3(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ แล้ว $|A| = |B| = \frac{m+1}{2}$

ทฤษฎีบท 2.4 ให้ $A, B \subseteq \mathbb{Z}_m$ โดยที่ $|A \cup B| = m - 2$ และ $|A \cap B| = 1$ ถ้า $R_3(A, \bar{n}) = R_3(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ แล้ว $|A| = |B| = \frac{m-1}{2}$

ทฤษฎีบท 2.5 ให้ $A, B \subseteq \mathbb{Z}_m$ โดยที่ $|A \cup B| = m - 3$ และ $|A \cap B| = 0$ ถ้า $R_3(A, \bar{n}) = R_3(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ แล้ว $|A| = |B| = \frac{m-3}{2}$

ต่อไปพิจารณากรณี $A \cup B = \mathbb{Z}_m$ และ $|A \cap B| = 3$ ที่ทำให้ฟังก์ชันตัวแทนมีค่าเท่ากัน และแนะนำสัญลักษณ์ที่จะใช้ในการพิสูจน์ทฤษฎีบทต่อไปนี้

สำหรับทุก $A \subseteq \mathbb{Z}_m$ ฟังก์ชันลักษณะเฉพาะ (Characteristic function) $\eta_A : \mathbb{Z} \rightarrow \{0,1\}$ นิยามโดย

$$\eta_A(t) = \begin{cases} 0; & \bar{t} \notin A, \\ 1; & \bar{t} \in A \end{cases} \text{ สำหรับทุก } t \in \mathbb{Z}$$

ทฤษฎีบท 2.6 ให้ $A, B \subseteq \mathbb{Z}_m$ โดยที่ $|A|=|B|=\frac{m+3}{2}$ และให้ $\bar{r}_1, \bar{r}_2, \bar{r}_3 \in \mathbb{Z}_m$ โดยที่ $A \cup B = \mathbb{Z}_m$ และ

$A \cap B = \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}$ จะได้ว่า $R_3(A, \bar{n}) = R_3(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ ก็ต่อเมื่อ

$$A \setminus B = \{\bar{t} \in \mathbb{Z}_m : \exists! \bar{r} \in \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}, \overline{2t-r} \in A\} \cup \{\bar{t} \in \mathbb{Z}_m : \overline{2t-r_i} = \bar{r}_j \wedge \overline{2t-r_k} \in B; \{i, j, k\} = \{1, 2, 3\}\}$$

บทพิสูจน์ สมมติว่า $R_3(A, \bar{n}) = R_3(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ ให้ $\bar{t} \in \mathbb{Z}_m \setminus \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}$ พิจารณาสมการ $\bar{x} \oplus \bar{y} = \overline{2t}$ จะได้ว่า $\bar{a}$ และ $\overline{2t-a}$ เป็นชุดคำตอบของ $\bar{x} \oplus \bar{y} = \overline{2t}$

กรณี 1 $\overline{2t-r_i} \notin \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}$ สำหรับทุก $i \in \{1, 2, 3\}$ ดังนั้น มี $\bar{a}_1, \bar{a}_2, \dots, \bar{a}_{(m-7)/2} \in \mathbb{Z}_m$ ที่ทำให้

$$\mathbb{Z}_m = \bigcup_{i=1}^{(m-7)/2} \{\bar{a}_i, \overline{2t-a_i}\} \cup \{\overline{2t-r_1}\} \cup \{\overline{2t-r_2}\} \cup \{\overline{2t-r_3}\} \cup \{\bar{r}_1, \bar{r}_2, \bar{r}_3\} \cup \{\bar{t}\}$$

ให้ $j = 1, 2$ โดยที่

$$A^{(j)} = \{1 \leq i \leq (m-7)/2 : |A \cap \{\bar{a}_i, \overline{2t-a_i}\}| = j\}$$

$$B^{(j)} = \{1 \leq i \leq (m-7)/2 : |B \cap \{\bar{a}_i, \overline{2t-a_i}\}| = j\}$$

จะได้ว่า $|A^{(1)}| = |B^{(1)}|$ และ

$$|A| = |A^{(1)}| + 2|A^{(2)}| + \eta_A(2t-r_1) + \eta_A(2t-r_2) + \eta_A(2t-r_3) + \eta_A(t) + 3 \quad (1)$$

$$|B| = |B^{(1)}| + 2|B^{(2)}| + \eta_B(2t-r_1) + \eta_B(2t-r_2) + \eta_B(2t-r_3) + \eta_B(t) + 3 \quad (2)$$

$$R_3(A, \overline{2t}) = |A^{(2)}| + \eta_A(2t-r_1) + \eta_A(2t-r_2) + \eta_A(2t-r_3) + \eta_A(t) \quad (3)$$

$$R_3(B, \overline{2t}) = |B^{(2)}| + \eta_B(2t-r_1) + \eta_B(2t-r_2) + \eta_B(2t-r_3) + \eta_B(t) \quad (4)$$

เนื่องจาก $|A| = |B|$ จะได้ว่าสมการ (1) เท่ากับสมการ (2) และทำให้ได้ว่า

$$\begin{aligned} 2|A^{(2)}| + \eta_A(2t-r_1) + \eta_A(2t-r_2) + \eta_A(2t-r_3) + \eta_A(t) &= \\ 2|B^{(2)}| + \eta_B(2t-r_1) + \eta_B(2t-r_2) + \eta_B(2t-r_3) + \eta_B(t) & \end{aligned} \quad (5)$$

เนื่องจาก $R_3(A, \overline{2t}) = R_3(B, \overline{2t})$ จะได้ว่าสมการ (3) เท่ากับสมการ (4) ดังนั้น

$$\begin{aligned} &|A^{(2)}| + \eta_A(2t - r_1) + \eta_A(2t - r_2) + \eta_A(2t - r_3) + \eta_A(t) = \\ &|B^{(2)}| + \eta_B(2t - r_1) + \eta_B(2t - r_2) + \eta_B(2t - r_3) + \eta_B(t) \end{aligned} \quad (6)$$

นำสมการ (5) ลบสมการ (6) จะได้ว่า $|A^{(2)}| = |B^{(2)}|$ ดังนั้น

$$\begin{aligned} &\eta_B(2t - r_1) + \eta_B(2t - r_2) + \eta_B(2t - r_3) + \eta_B(t) = \\ &\eta_A(2t - r_1) + \eta_A(2t - r_2) + \eta_A(2t - r_3) + \eta_A(t) \end{aligned} \quad (7)$$

กรณี 2 มี $\overline{2t - r_i} \in \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}$ สำหรับบาง $i \in \{1, 2, 3\}$ โดยไม่เสียทั่วไป สมมติว่า $\overline{2t - r_1} = \bar{r}_2$ ดังนั้นมี $\bar{a}_1, \bar{a}_2, \dots, \bar{a}_{(m-5)/2} \in \mathbb{Z}_m$ ที่ทำให้

$$\mathbb{Z}_m = \bigcup_{i=1}^{(m-5)/2} \{\bar{a}_i, \overline{2t - a_i}\} \cup \{\overline{2t - r_3}\} \cup \{\bar{r}_1, \bar{r}_2, \bar{r}_3\} \cup \{\bar{t}\}$$

ให้ $j = 1, 2$ โดยที่

$$A^{(j)} = \{1 \leq i \leq (m-5)/2 : |A \cap \{\bar{a}_i, \overline{2t - a_i}\}| = j\}$$

$$B^{(j)} = \{1 \leq i \leq (m-5)/2 : |B \cap \{\bar{a}_i, \overline{2t - a_i}\}| = j\}$$

จะได้ว่า $|A^{(1)}| = |B^{(1)}|$ และ

$$|A| = |A^{(1)}| + 2|A^{(2)}| + \eta_A(2t - r_3) + \eta_A(t) + 3 \quad (9)$$

$$|B| = |B^{(1)}| + 2|B^{(2)}| + \eta_B(2t - r_3) + \eta_B(t) + 3 \quad (10)$$

$$R_3(A, \overline{2t}) = |A^{(2)}| + \eta_A(2t - r_3) + \eta_A(t) + 1 \quad (11)$$

$$R_3(B, \overline{2t}) = |B^{(2)}| + \eta_B(2t - r_3) + \eta_B(t) + 1 \quad (12)$$

เนื่องจาก $|A| = |B|$ จะได้ว่าสมการ (9) เท่ากับสมการ (10) และทำให้ได้ว่า

$$2|A^{(2)}| + \eta_A(2t - r_3) + \eta_A(t) = 2|B^{(2)}| + \eta_B(2t - r_3) + \eta_B(t) \quad (13)$$

เนื่องจาก $R_3(A, \overline{2t}) = R_3(B, \overline{2t})$ จะได้ว่าสมการ (11) เท่ากับสมการ (12) ดังนั้น

$$|A^{(2)}| + \eta_A(2t - r_3) + \eta_A(t) = |B^{(2)}| + \eta_B(2t - r_3) + \eta_B(t) \quad (14)$$

นำสมการ (13) ลบสมการ (14) จะได้ว่า $|A^{(2)}| = |B^{(2)}|$ ทำให้ได้ว่า

$$\eta_A(2t - r_3) + \eta_A(t) = \eta_B(2t - r_3) + \eta_B(t) \quad (15)$$

ต่อไปจะแสดงว่า

$$A \setminus B = \{\bar{t} \in \mathbb{Z}_m : \exists! \bar{r} \in \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}, \overline{2t - r} \in A\} \cup \{\bar{t} \in \mathbb{Z}_m : \overline{2t - r_i} = \bar{r}_j \wedge \overline{2t - r_k} \in B; \{i, j, k\} = \{1, 2, 3\}\}$$

ดังต่อไปนี้

($\subseteq$) ให้ $\bar{t} \in A \setminus B$ จะได้ว่า $\bar{t} \notin B$ ดังนั้น $\eta_A(t) = 1$ และ $\eta_B(t) = 0$

กรณี 1 $\overline{2t-r_i} \notin \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}$ สำหรับทุก $i \in \{1, 2, 3\}$ จากสมการ (7) จะได้ว่า

$$\eta_B(2t-r_1) + \eta_B(2t-r_2) + \eta_B(2t-r_3) = \eta_A(2t-r_1) + \eta_A(2t-r_2) + \eta_A(2t-r_3) + 1 \quad (16)$$

ถ้า $\overline{2t-r_i} \in B$ สำหรับทุก $i \in \{1, 2, 3\}$ จะได้ว่า $\overline{2t-r_i} \notin A$ สำหรับทุก $i \in \{1, 2, 3\}$ ดังนั้น $\eta_B(2t-r_1) = 1$, $\eta_B(2t-r_2) = 1$, $\eta_B(2t-r_3) = 1$, $\eta_A(2t-r_1) = 0$, $\eta_A(2t-r_2) = 0$ และ $\eta_A(2t-r_3) = 0$ ซึ่งทำให้ได้สมการ (16) ไม่จริง ดังนั้นจะมี $i \in \{1, 2, 3\}$ ที่ทำให้ $\overline{2t-r_i} \in A$ โดยไม่เสียเลยทั่วไป สมมติว่า $\overline{2t-r_1}$ และ $\overline{2t-r_2}$ เป็นสมาชิกของ A จะได้ว่า $\overline{2t-r_1}, \overline{2t-r_2} \notin B$ เพราะฉะนั้น $\eta_A(2t-r_1) = 1$, $\eta_A(2t-r_2) = 1$, $\eta_B(2t-r_1) = 0$ และ $\eta_B(2t-r_2) = 0$ ซึ่งทำให้ได้สมการ (16) ไม่จริง ดังนั้น จะมี $\bar{r} \in \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}$ มีเพียงตัวเดียวเท่านั้น ที่ทำให้ $\overline{2t-r} \in A$ นั่นคือ $\bar{t} \in \{\bar{t} \in \mathbb{Z}_m : \exists! \bar{r} \in \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}, \overline{2t-r} \in A\}$

กรณี 2 มี $\overline{2t-r_i} \in \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}$ สำหรับบาง $i \in \{1, 2, 3\}$ โดยไม่เสียเลยทั่วไป สมมติว่า $\overline{2t-r_1} = \bar{r}_2$ จะได้ว่า $\overline{2t-r_2} = \bar{r}_1$ ดังนั้น $\overline{2t-r_1}, \overline{2t-r_2} \in B$ จากสมการ (15) จะได้ว่า $\eta_B(2t-r_3) = \eta_A(2t-r_3) + 1$ ซึ่งเป็นจริง เมื่อ $\eta_B(2t-r_3) = 1$ และ $\eta_A(2t-r_3) = 0$ นั่นคือ $\overline{2t-r_3} \in B$ ดังนั้น

$$\bar{t} \in \{\bar{t} \in \mathbb{Z}_m : \overline{2t-r_i} = \bar{r}_j \wedge \overline{2t-r_k} \in B; \{i, j, k\} = \{1, 2, 3\}\}$$

($\supseteq$) ให้

$$\bar{t} \in \{\bar{t} \in \mathbb{Z}_m : \exists! \bar{r} \in \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}, \overline{2t-r} \in A\} \cup \{\bar{t} \in \mathbb{Z}_m : \overline{2t-r_i} = \bar{r}_j \wedge \overline{2t-r_k} \in B; \{i, j, k\} = \{1, 2, 3\}\}$$

กรณี 1 $\bar{t} \in \{\bar{t} \in \mathbb{Z}_m : \exists! \bar{r} \in \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}, \overline{2t-r} \in A\}$ จะได้ว่า มี r_1 เพียงตัวเดียวเท่านั้น ที่ทำให้ $\overline{2t-r_1} \in A$ เพราะฉะนั้น $\overline{2t-r_2}, \overline{2t-r_3} \in B$ ดังนั้น $\overline{2t-r_i} \notin \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}$ สำหรับทุก $i \in \{1, 2, 3\}$ จะได้ว่า $\eta_A(2t-r_1) = 1$, $\eta_A(2t-r_2) = 0$, $\eta_A(2t-r_3) = 0$, $\eta_B(2t-r_1) = 0$, $\eta_B(2t-r_2) = 1$, $\eta_B(2t-r_3) = 1$ จากสมการ (7) จะได้ว่า

$$\eta_A(t) = \eta_B(t) + 1$$

ซึ่งเป็นจริง เมื่อ $\eta_A(t) = 1$ และ $\eta_B(t) = 0$ ดังนั้น $\bar{t} \in A \setminus B$

กรณี 2 $\bar{t} \in \{\bar{t} \in \mathbb{Z}_m : \overline{2t-r_i} = \bar{r}_j \wedge \overline{2t-r_k} \in B; \{i, j, k\} = \{1, 2, 3\}\}$ โดยไม่เสียเลยทั่วไป สมมติว่า $\overline{2t-r_1} = \bar{r}_2$ และ $\overline{2t-r_3} \in B$ จะได้ว่า $\overline{2t-r_2} = \bar{r}_1$ ดังนั้น $\overline{2t-r_1}, \overline{2t-r_2} \in B$ เพราะฉะนั้น $\eta_B(2t-r_3) = 1$ จากสมการ (15) จะได้ว่า

$$\eta_A(t) = 1 + \eta_B(t)$$

ซึ่งเป็นจริง เมื่อ $\eta_A(t) = 1$ และ $\eta_B(t) = 0$ ดังนั้น $\bar{t} \in A \setminus B$

ดังนั้นเราสามารถสรุปได้ว่า

$$A \setminus B = \{\bar{t} \in \mathbb{Z}_m : \exists! \bar{r} \in \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}, \overline{2t-r} \in A\} \cup \{\bar{t} \in \mathbb{Z}_m : \overline{2t-r_i} = \bar{r}_j \wedge \overline{2t-r_k} \in B; \{i, j, k\} = \{1, 2, 3\}\}$$

ในทางกลับกัน ให้

$$A \setminus B = \{\bar{t} \in \mathbb{Z}_m : \exists! \bar{r} \in \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}, \overline{2t-r} \in A\} \cup \{\bar{t} \in \mathbb{Z}_m : \overline{2t-r_i} = \bar{r}_j \wedge \overline{2t-r_k} \in B; \{i, j, k\} = \{1, 2, 3\}\}$$

และ $\bar{t} \in \mathbb{Z}_m \setminus \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}$ โดยไม่เสียนัยทั่วไป สมมติว่า $\bar{t} \in A \setminus B$

กรณี 1 $\overline{2t-r_i} \notin \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}$ สำหรับทุก $i \in \{1, 2, 3\}$ ดังนั้น

$$\bar{t} \in \{\bar{t} \in \mathbb{Z}_m : \exists! \bar{r} \in \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}, \overline{2t-r} \in A\}$$

จะได้ว่า

$$R_3(A, \overline{2t}) = |A^{(2)}| + \eta_A(2t-r_1) + \eta_A(2t-r_2) + \eta_A(2t-r_3) + \eta_A(t) = |A^{(2)}| + 2$$

$$R_3(B, \overline{2t}) = |B^{(2)}| + \eta_B(2t-r_1) + \eta_B(2t-r_2) + \eta_B(2t-r_3) + \eta_B(t) = |B^{(2)}| + 2$$

และ

$$\eta_A(2t-r_1) + \eta_A(2t-r_2) + \eta_A(2t-r_3) + \eta_A(t) = \eta_B(2t-r_1) + \eta_B(2t-r_2) + \eta_B(2t-r_3) + \eta_B(t)$$

จากสมการ (1), (2) และ $|A| = |B|$ จะได้ว่า

$$\begin{aligned} 2|A^{(2)}| + \eta_A(2t-r_1) + \eta_A(2t-r_2) + \eta_A(2t-r_3) + \eta_A(t) &= \\ 2|B^{(2)}| + \eta_B(2t-r_1) + \eta_B(2t-r_2) + \eta_B(2t-r_3) + \eta_B(t) & \end{aligned}$$

ดังนั้น $2|A^{(2)}| = 2|B^{(2)}|$ นั่นคือ $R_3(A, \overline{2t}) = R_3(B, \overline{2t})$

กรณี 2 $\overline{2t-r_i} \in \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}$ สำหรับบาง $i \in \{1, 2, 3\}$ โดยไม่เสียนัยทั่วไป สมมติว่า $\overline{2t-r_1} = \bar{r}_2$

ดังนั้น

$$\bar{t} \in \{\bar{t} \in \mathbb{Z}_m : \overline{2t-r_i} = \bar{r}_j \wedge \overline{2t-r_k} \in B; \{i, j, k\} = \{1, 2, 3\}\}$$

จะได้ว่า

$$R_3(A, \overline{2t}) = |A^{(2)}| + \eta_A(2t-r_3) + \eta_A(t) + 1 = |A^{(2)}| + 2$$

$$R_3(B, \overline{2t}) = |B^{(2)}| + \eta_B(2t-r_3) + \eta_B(t) + 1 = |B^{(2)}| + 2$$

และ

$$\eta_A(2t-r_3) + \eta_A(t) = \eta_B(2t-r_3) + \eta_B(t)$$

จากสมการ (9),(10) และ $|A| = |B|$ จะได้ว่า

$$2|A^{(2)}| + \eta_A(2t - r_3) + \eta_A(t) = 2|B^{(2)}| + \eta_B(2t - r_3) + \eta_B(t)$$

ดังนั้น $2|A^{(2)}| = 2|B^{(2)}|$ นั่นคือ $R_3(A, 2\bar{t}) = R_3(B, 2\bar{t})$

จากทั้งสองกรณี จะได้ว่า $R_3(A, 2\bar{n}) = R_3(B, 2\bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ โดยที่ $2\bar{n} \notin \{2\bar{r}_1, 2\bar{r}_2, 2\bar{r}_3\}$

ต่อไปจะแสดงว่า

$$R_3(A, 2\bar{r}_1) = R_3(B, 2\bar{r}_1), \quad R_3(A, 2\bar{r}_2) = R_3(B, 2\bar{r}_2) \quad \text{และ} \quad R_3(A, 2\bar{r}_3) = R_3(B, 2\bar{r}_3)$$

ให้ $\bar{c} \in \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}$ เราเลือก $\bar{b}_1, \bar{b}_2, \dots, \bar{b}_{(m-1)/2} \in \mathbb{Z}_m$ ที่ทำให้

$$\mathbb{Z}_m = \bigcup_{i=1}^{(m-1)/2} \{\bar{b}_i, 2\bar{c} - \bar{b}_i\} \cup \{\bar{c}\}$$

ให้ $j = 3, 4$ โดยที่

$$A^{(j)} = \{1 \leq i \leq (m-1)/2 : |A \cap \{\bar{b}_i, 2\bar{c} - \bar{b}_i\}| = j-2\}$$

$$B^{(j)} = \{1 \leq i \leq (m-1)/2 : |B \cap \{\bar{b}_i, 2\bar{c} - \bar{b}_i\}| = j-2\}$$

จะได้ว่า $|A^{(3)}| = |B^{(3)}|$ และ

$$|A| = |A^{(3)}| + 2|A^{(4)}| + 1$$

$$|B| = |B^{(3)}| + 2|B^{(4)}| + 1$$

$$R_3(A, 2\bar{c}) = |A^{(4)}| + 1$$

$$R_3(B, 2\bar{c}) = |B^{(4)}| + 1$$

เนื่องจาก $|A| = |B|$ จะได้ว่า $|A^{(3)}| + 2|A^{(4)}| + 1 = |B^{(3)}| + 2|B^{(4)}| + 1$ ดังนั้น $|A^{(4)}| = |B^{(4)}|$ และ

$$R_3(A, 2\bar{c}) = R_3(B, 2\bar{c})$$

นี้แสดงว่า $R_3(A, 2\bar{n}) = R_3(B, 2\bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ เนื่องจาก m เป็นจำนวนเต็มคี่ จะได้ว่า

$$R_3(A, \bar{n}) = R_3(B, \bar{n}) \quad \text{สำหรับทุก} \quad \bar{n} \in \mathbb{Z}_m \quad \square$$

ต่อไปพิจารณากรณี $|A \cup B| = m-1$ และ $|A \cap B| = 2$

ทฤษฎีบท 2.7 ให้ $A, B \subseteq \mathbb{Z}_m$ โดยที่ $|A| = |B| = \frac{m+1}{2}$ และให้ $\bar{r}_1, \bar{r}_2, \bar{r}_3 \in \mathbb{Z}_m$ โดยที่ $A \cap B = \{\bar{r}_1, \bar{r}_2\}$ และ

$A \cup B = \mathbb{Z}_m \setminus \{\bar{r}_3\}$ จะได้ว่า $R_3(A, \bar{n}) = R_3(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ ก็ต่อเมื่อ

$$A \setminus B = \{\bar{t} \in \mathbb{Z}_m : \exists \bar{r} \in \{\bar{r}_1, \bar{r}_2\}, \overline{2t-r} \in A \wedge \overline{2t-r_3} \in A\} \cup \{\bar{t} \in \mathbb{Z}_m : \overline{2t-r} \in B, \forall \bar{r} \in \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}\} \\ \cup \{\bar{t} \in \mathbb{Z}_m : \overline{2t-r_1} = \bar{r}_2 \wedge \overline{2t-r_3} \in A\}$$

บทพิสูจน์ สมมติว่า $R_3(A, \bar{n}) = R_3(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ ให้ $\bar{t} \in \mathbb{Z}_m \setminus \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}$ พิจารณาสมการ $\bar{x} \oplus \bar{y} = \bar{2t}$ จะได้ว่า $\bar{a}$ และ $\overline{2t-a}$ เป็นชุดคำตอบของสมการ $\bar{x} \oplus \bar{y} = \bar{2t}$

กรณี 1 $\overline{2t-r_i} \notin \{\bar{r}_1, \bar{r}_2\}$ สำหรับทุก $i \in \{1, 2\}$ ดังนั้น มี $\bar{a}_1, \bar{a}_2, \dots, \bar{a}_{(m-7)/2} \in \mathbb{Z}_m \setminus \{\bar{r}_3\}$ ที่ทำให้

$$\mathbb{Z}_m \setminus \{\bar{r}_3\} = \bigcup_{i=1}^{(m-7)/2} \{\bar{a}_i, \overline{2t-a_i}\} \cup \{\overline{2t-r_1}\} \cup \{\overline{2t-r_2}\} \cup \{\overline{2t-r_3}\} \cup \{\bar{r}_1, \bar{r}_2\} \cup \{\bar{t}\}$$

ให้ $j = 1, 2$ โดยที่

$$A^{(j)} = \left\{1 \leq i \leq (m-7)/2 : \left|A \cap \{\bar{a}_i, \overline{2t-a_i}\}\right| = j\right\}$$

$$B^{(j)} = \left\{1 \leq i \leq (m-7)/2 : \left|B \cap \{\bar{a}_i, \overline{2t-a_i}\}\right| = j\right\}$$

จะได้ว่า $|A^{(1)}| = |B^{(1)}|$ และ

$$|A| = |A^{(1)}| + 2|A^{(2)}| + \eta_A(2t-r_1) + \eta_A(2t-r_2) + \eta_A(2t-r_3) + \eta_A(t) + 2 \quad (1)$$

$$|B| = |B^{(1)}| + 2|B^{(2)}| + \eta_B(2t-r_1) + \eta_B(2t-r_2) + \eta_B(2t-r_3) + \eta_B(t) + 2 \quad (2)$$

$$R_3(A, \overline{2t}) = |A^{(2)}| + \eta_A(2t-r_1) + \eta_A(2t-r_2) + \eta_A(t) \quad (3)$$

$$R_3(B, \overline{2t}) = |B^{(2)}| + \eta_B(2t-r_1) + \eta_B(2t-r_2) + \eta_B(t) \quad (4)$$

เนื่องจาก $|A| = |B|$ จะได้ว่าสมการ (1) เท่ากับสมการ (2) และทำให้ได้ว่า

$$2|A^{(2)}| + \eta_A(2t-r_1) + \eta_A(2t-r_2) + \eta_A(2t-r_3) + \eta_A(t) = \\ 2|B^{(2)}| + \eta_B(2t-r_1) + \eta_B(2t-r_2) + \eta_B(2t-r_3) + \eta_B(t) \quad (5)$$

เนื่องจาก $R_3(A, \overline{2t}) = R_3(B, \overline{2t})$ จะได้ว่าสมการ (3) เท่ากับสมการ (4) ดังนั้น

$$|A^{(2)}| + \eta_A(2t-r_1) + \eta_A(2t-r_2) + \eta_A(t) = |B^{(2)}| + \eta_B(2t-r_1) + \eta_B(2t-r_2) + \eta_B(t) \quad (6)$$

นำสมการ (5) ลบสมการ (6) จะได้ว่า

$$|A^{(2)}| + \eta_A(2t-r_3) = |B^{(2)}| + \eta_B(2t-r_3)$$

แทน $|A^{(2)}| = |B^{(2)}| + \eta_B(2t-r_3) - \eta_A(2t-r_3)$ ในสมการ (6) จะได้ว่า

$$\begin{aligned} \eta_A(2t-r_1) + \eta_A(2t-r_2) + \eta_B(2t-r_3) + \eta_A(t) = \\ \eta_B(2t-r_1) + \eta_B(2t-r_2) + \eta_A(2t-r_3) + \eta_B(t) \end{aligned} \quad (7)$$

กรณี $2\overline{2t-r_i} \notin \{\overline{r_1}, \overline{r_2}\}$ สำหรับบาง $i \in \{1, 2\}$ เพราะฉะนั้น $\overline{2t-r_1} = \overline{r_2}$ ดังนั้น มี $\overline{a_1}, \overline{a_2}, \dots, \overline{a_{(m-5)/2}} \in \mathbb{Z}_m \setminus \{\overline{r_3}\}$ ที่ทำให้

$$\mathbb{Z}_m \setminus \{\overline{r_3}\} = \bigcup_{i=1}^{(m-5)/2} \{\overline{a_i}, \overline{2t-a_i}\} \cup \{\overline{2t-r_3}\} \cup \{\overline{r_1}, \overline{r_2}\} \cup \{\overline{t}\}$$

ให้ $j=1, 2$ โดยที่

$$A^{(j)} = \{1 \leq i \leq (m-5)/2 : |A \cap \{\overline{a_i}, \overline{2t-a_i}\}| = j\}$$

$$B^{(j)} = \{1 \leq i \leq (m-5)/2 : |B \cap \{\overline{a_i}, \overline{2t-a_i}\}| = j\}$$

จะได้ว่า $|A^{(1)}| = |B^{(1)}|$ และ

$$|A| = |A^{(1)}| + 2|A^{(2)}| + \eta_A(2t-r_3) + \eta_A(t) + 2 \quad (9)$$

$$|B| = |B^{(1)}| + 2|B^{(2)}| + \eta_B(2t-r_3) + \eta_B(t) + 2 \quad (10)$$

$$R_3(A, \overline{2t}) = |A^{(2)}| + \eta_A(t) + 1 \quad (11)$$

$$R_3(B, \overline{2t}) = |B^{(2)}| + \eta_B(t) + 1 \quad (12)$$

เนื่องจาก $|A| = |B|$ จะได้ว่าสมการ (9) เท่ากับสมการ (10) และทำให้ได้ว่า

$$2|A^{(2)}| + \eta_A(2t-r_3) + \eta_A(t) = 2|B^{(2)}| + \eta_B(2t-r_3) + \eta_B(t) \quad (13)$$

เนื่องจาก $R_3(A, \overline{2t}) = R_3(B, \overline{2t})$ จะได้ว่าสมการ (11) เท่ากับสมการ (12) ดังนั้น

$$|A^{(2)}| + \eta_A(t) = |B^{(2)}| + \eta_B(t) \quad (14)$$

นำสมการ (13) ลบสมการ (14) จะได้ว่า

$$|A^{(2)}| + \eta_A(2t-r_3) = |B^{(2)}| + \eta_B(2t-r_3)$$

แทน $|A^{(2)}| = |B^{(2)}| + \eta_B(2t-r_3) - \eta_A(2t-r_3)$ ในสมการ (14) จะได้ว่า

$$\eta_B(2t-r_3) + \eta_A(t) = \eta_A(2t-r_3) + \eta_B(t) \quad (15)$$

ต่อไปจะแสดงว่า

$$\begin{aligned} A \setminus B = \{ \overline{t} \in \mathbb{Z}_m : \exists \overline{r} \in \{\overline{r_1}, \overline{r_2}\}, \overline{2t-r} \in A \wedge \overline{2t-r_3} \in A \} \cup \{ \overline{t} \in \mathbb{Z}_m : \overline{2t-r} \in B, \forall \overline{r} \in \{\overline{r_1}, \overline{r_2}, \overline{r_3}\} \} \\ \cup \{ \overline{t} \in \mathbb{Z}_m : \overline{2t-r_1} = \overline{r_2} \wedge \overline{2t-r_3} \in A \} \end{aligned}$$

($\subseteq$) ให้ $\overline{t} \in A \setminus B$ และ $\overline{2t-r} \notin B$ สำหรับบาง $\overline{r} \in \{\overline{r_1}, \overline{r_2}, \overline{r_3}\}$ จะได้ว่า $\overline{t} \notin B$ ดังนั้น

$$\eta_A(t) = 1 \text{ และ } \eta_B(t) = 0$$

กรณี 1 $\overline{2t-r_i} \notin \{\overline{r_1}, \overline{r_2}\}$ สำหรับทุก $i \in \{1, 2\}$ จะแสดงว่า $\overline{2t-r_3} \in A$ สมมติว่า $\overline{2t-r_3} \notin A$ จะได้ว่า $\overline{2t-r_3} \in B$ จากสมการ (7) จะได้ว่า

$$\eta_A(2t-r_1) + \eta_A(2t-r_2) + 2 = \eta_B(2t-r_1) + \eta_B(2t-r_2)$$

ซึ่งทำให้ได้ว่า $\eta_B(2t-r_1)=1$ และ $\eta_B(2t-r_2)=1$ นั่นคือ $\overline{2t-r_1}, \overline{2t-r_2} \in B$ จะได้ว่า $\overline{2t-r_1}, \overline{2t-r_2}, \overline{2t-r_3} \in B$ ซึ่งเกิดข้อขัดแย้ง ดังนั้น $\overline{2t-r_3} \in A$ นั่นคือ $\overline{2t-r_3} \notin B$ เพราะฉะนั้น $\eta_A(2t-r_3)=1$ และ $\eta_B(2t-r_3)=0$ ต่อไปจะแสดงว่ามี $\overline{r} \in \{\overline{r_1}, \overline{r_2}\}$ เพียงตัวเดียวเท่านั้น ที่ทำให้ $\overline{2t-r} \in A$ สมมติว่า $\overline{2t-r_1}, \overline{2t-r_2} \notin A$ ทำให้ได้ว่า $\eta_A(2t-r_1)=0$ และ $\eta_A(2t-r_2)=0$ ซึ่งเกิดข้อขัดแย้งกับสมการ (7) ดังนั้น จะมี $\overline{r} \in \{\overline{r_1}, \overline{r_2}\}$ ที่ทำให้ $\overline{2t-r} \in A$ ถ้า $\overline{2t-r} \in A$ สำหรับทุก $\overline{r} \in \{\overline{r_1}, \overline{r_2}\}$ จะได้ว่า $\eta_A(2t-r_1)=1$ และ $\eta_A(2t-r_2)=1$ ซึ่งเกิดข้อขัดแย้งกับสมการ (7) ดังนั้นเราจะสรุปได้ว่า มี $\overline{r} \in \{\overline{r_1}, \overline{r_2}\}$ เพียงตัวเดียวเท่านั้น ที่ทำให้ $\overline{2t-r} \in A$ นั่นคือ

$$\begin{aligned} \bar{t} \in & \left\{ \bar{t} \in \mathbb{Z}_m : \exists! \bar{r} \in \{\overline{r_1}, \overline{r_2}\}, \overline{2t-r} \in A \wedge \overline{2t-r_3} \in A \right\} \cup \left\{ \bar{t} \in \mathbb{Z}_m : \overline{2t-r} \in B, \forall \bar{r} \in \{\overline{r_1}, \overline{r_2}, \overline{r_3}\} \right\} \\ & \cup \left\{ \bar{t} \in \mathbb{Z}_m : \overline{2t-r_1} = \overline{r_2} \wedge \overline{2t-r_3} \in A \right\} \end{aligned}$$

กรณี 2 $\overline{2t-r_i} \notin \{\overline{r_1}, \overline{r_2}\}$ สำหรับบาง $i \in \{1, 2\}$ เพราะฉะนั้น $\overline{2t-r_1} = \overline{r_2}$ จะได้ว่า $\overline{2t-r_2} = \overline{r_1}$ ดังนั้น $\overline{2t-r_1}, \overline{2t-r_2} \in B$ จากสมการ (15) จะได้ว่า $\eta_B(2t-r_3)+1 = \eta_A(2t-r_3)$ ซึ่งเป็นจริง เมื่อ $\eta_A(2t-r_3)=1$ และ $\eta_B(2t-r_3)=0$ ดังนั้น $\overline{2t-r_3} \in A$ นั่นคือ

$$\bar{t} \in \left\{ \bar{t} \in \mathbb{Z}_m : \overline{2t-r_1} = \overline{r_2} \wedge \overline{2t-r_3} \in A \right\}$$

($\Rightarrow$) ให้

$$\begin{aligned} \bar{t} \in & \left\{ \bar{t} \in \mathbb{Z}_m : \exists! \bar{r} \in \{\overline{r_1}, \overline{r_2}\}, \overline{2t-r} \in A \wedge \overline{2t-r_3} \in A \right\} \cup \left\{ \bar{t} \in \mathbb{Z}_m : \overline{2t-r} \in B, \forall \bar{r} \in \{\overline{r_1}, \overline{r_2}, \overline{r_3}\} \right\} \\ & \cup \left\{ \bar{t} \in \mathbb{Z}_m : \overline{2t-r_1} = \overline{r_2} \wedge \overline{2t-r_3} \in A \right\} \end{aligned}$$

กรณี 1 ถ้า $\bar{t} \in \left\{ \bar{t} \in \mathbb{Z}_m : \exists! \bar{r} \in \{\overline{r_1}, \overline{r_2}\}, \overline{2t-r} \in A \wedge \overline{2t-r_3} \in A \right\}$ แล้วจะมี $\bar{r} \in \{\overline{r_1}, \overline{r_2}\}$ เพียงตัวเดียวเท่านั้น ที่ทำให้ $\overline{2t-r} \in A$ และ $\overline{2t-r_3} \in A$ โดยไม่เสียเลยทั่วไป สมมติว่า $\overline{2t-r_1} \in A$ และ $\overline{2t-r_2} \notin A$ ดังนั้น $\overline{2t-r_i} \notin \{\overline{r_1}, \overline{r_2}\}$ สำหรับทุก $i \in \{1, 2\}$ จะได้ว่า $\eta_A(2t-r_1)=1$ และ $\eta_A(2t-r_2)=0$ จากสมการ (7) และ $\overline{2t-r_3} \in A$ จะได้ว่า $\eta_A(t)+1 = \eta_B(t)+2$ นั่นคือ

$$\eta_A(t) = \eta_B(t) + 1 \quad (16)$$

ซึ่งเป็นจริง เมื่อ $\eta_B(t)=0$ และ $\eta_A(t)=1$ ดังนั้น $\bar{t} \notin B$ และ $\bar{t} \in A$

กรณี 2 ถ้า $\bar{t} \in \left\{ \bar{t} \in \mathbb{Z}_m : \overline{2t-r} \in B, \forall \bar{r} \in \{\overline{r_1}, \overline{r_2}, \overline{r_3}\} \right\}$ แล้ว $\overline{2t-r} \in B$ สำหรับทุก $\bar{r} \in \{\overline{r_1}, \overline{r_2}, \overline{r_3}\}$ ดังนั้น $\overline{2t-r_i} \notin \{\overline{r_1}, \overline{r_2}\}$ สำหรับทุก $i \in \{1, 2\}$ นั่นคือ $\eta_A(2t-r_1)=0$, $\eta_A(2t-r_2)=0$, $\eta_A(2t-r_3)=0$, $\eta_B(2t-r_1)=1$, $\eta_B(2t-r_2)=1$ และ $\eta_B(2t-r_3)=1$ จากสมการ (7) จะได้ว่า $\eta_A(t)+1 = \eta_B(t)+2$ นั่นคือ

$$\eta_A(t) = \eta_B(t) + 1 \quad (17)$$

ซึ่งเป็นจริง เมื่อ $\eta_B(t) = 0$ และ $\eta_A(t) = 1$ ดังนั้น $\bar{t} \in A \setminus B$

กรณี 3 ถ้า $\bar{t} \in \{\bar{t} \in \mathbb{Z}_m : \overline{2t-r_1} = \bar{r}_2 \wedge \overline{2t-r_3} \in A\}$ แล้ว $\overline{2t-r_1} = \bar{r}_2$ และ $\overline{2t-r_3} \in A$ ดังนั้น

$\eta_A(2t-r_3) = 1$ และ $\eta_B(2t-r_3) = 0$ จากสมการ (15) จะได้ว่า

$$\eta_A(t) = \eta_B(t) + 1 \quad (18)$$

ซึ่งเป็นจริง เมื่อ $\eta_B(t) = 0$ และ $\eta_A(t) = 1$ ดังนั้น $\bar{t} \in A \setminus B$

ดังนั้น

$$A \setminus B = \{\bar{t} \in \mathbb{Z}_m : \exists! \bar{r} \in \{\bar{r}_1, \bar{r}_2\}, \overline{2t-r} \in A \wedge \overline{2t-r_3} \in A\} \cup \{\bar{t} \in \mathbb{Z}_m : \overline{2t-r} \in B, \forall \bar{r} \in \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}\} \\ \cup \{\bar{t} \in \mathbb{Z}_m : \overline{2t-r_1} = \bar{r}_2 \wedge \overline{2t-r_3} \in A\}$$

ในทางกลับกัน สมมติว่า

$$A \setminus B = \{\bar{t} \in \mathbb{Z}_m : \exists! \bar{r} \in \{\bar{r}_1, \bar{r}_2\}, \overline{2t-r} \in A \wedge \overline{2t-r_3} \in A\} \cup \{\bar{t} \in \mathbb{Z}_m : \overline{2t-r} \in B, \forall \bar{r} \in \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}\} \\ \cup \{\bar{t} \in \mathbb{Z}_m : \overline{2t-r_1} = \bar{r}_2 \wedge \overline{2t-r_3} \in A\}$$

ให้ $\bar{t} \in \mathbb{Z}_m \setminus \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}$ โดยไม่เสียทั่วไป สมมติว่า $\bar{t} \in A \setminus B$

กรณี 1 $\overline{2t-r_i} \notin \{\bar{r}_1, \bar{r}_2\}$ สำหรับทุก $i \in \{1, 2\}$ จะได้ว่า

$$\bar{t} \in \{\bar{t} \in \mathbb{Z}_m : \exists! \bar{r} \in \{\bar{r}_1, \bar{r}_2\}, \overline{2t-r} \in A \wedge \overline{2t-r_3} \in A\} \cup \{\bar{t} \in \mathbb{Z}_m : \overline{2t-r} \in B, \forall \bar{r} \in \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}\}$$

ดังนั้น

$$R_3(A, \bar{2t}) = |A^{(2)}| + \eta_A(2t-r_1) + \eta_A(2t-r_2) + \eta_A(t) \\ R_3(B, \bar{2t}) = |B^{(2)}| + \eta_B(2t-r_1) + \eta_B(2t-r_2) + \eta_B(t)$$

และ

$$\eta_A(2t-r_1) + \eta_A(2t-r_2) + \eta_B(2t-r_3) + \eta_A(t) = \eta_B(2t-r_1) + \eta_B(2t-r_2) + \eta_A(2t-r_3) + \eta_B(t)$$

จาก (1), (2) และ $|A| = |B|$ จะได้ว่า

$$2|A^{(2)}| + \eta_A(2t-r_1) + \eta_A(2t-r_2) + \eta_A(2t-r_3) + \eta_A(t) = \\ 2|B^{(2)}| + \eta_B(2t-r_1) + \eta_B(2t-r_2) + \eta_B(2t-r_3) + \eta_B(t)$$

ดังนั้น $2|A^{(2)}| = 2|B^{(2)}|$ นั่นคือ $R_3(A, \bar{2t}) = R_3(B, \bar{2t})$

กรณี 2 $\overline{2t-r_i} \notin \{\bar{r}_1, \bar{r}_2\}$ สำหรับบาง $i \in \{1, 2\}$ เพราะฉะนั้น $\overline{2t-r_1} = \bar{r}_2$ จะได้ว่า $\overline{2t-r_2} = \bar{r}_1$

ดังนั้น

$$\bar{t} \in \{\bar{t} \in \mathbb{Z}_m : \overline{2t-r_1} = \bar{r}_2 \wedge \overline{2t-r_3} \in A\}$$

จะได้ว่า

$$R_3(A, \bar{2t}) = |A^{(2)}| + \eta_A(t) + 1 = |A^{(2)}| + 2$$

$$R_3(B, \overline{2t}) = |B^{(2)}| + \eta_B(t) + 1 = |B^{(2)}| + 2$$

และ

$$\eta_B(2t - r_3) + \eta_A(t) = \eta_A(2t - r_3) + \eta_B(t)$$

จาก (8), (9) และ $|A| = |B|$ จะได้ว่า

$$2|A^{(2)}| + \eta_A(2t - r_3) + \eta_A(t) = 2|B^{(2)}| + \eta_B(2t - r_3) + \eta_B(t)$$

ดังนั้น $2|A^{(2)}| = 2|B^{(2)}|$ นั่นคือ $R_3(A, \overline{2t}) = R_3(B, \overline{2t})$

จากทั้งสองกรณี จะได้ว่า $R_3(A, \overline{2n}) = R_3(B, \overline{2n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ โดยที่ $\overline{2n} \notin \{\overline{2r_1}, \overline{2r_2}, \overline{2r_3}\}$

ต่อไปจะแสดงว่า $R_3(A, \overline{2r_1}) = R_3(B, \overline{2r_1})$ และ $R_3(A, \overline{2r_2}) = R_3(B, \overline{2r_2})$ ให้ $\bar{c} \in \{\bar{r}_1, \bar{r}_2\}$

เราสามารถเลือก $\bar{b}_1, \bar{b}_2, \dots, \bar{b}_{(m-3)/2} \in \mathbb{Z}_m$ ที่ทำให้

$$\mathbb{Z}_m \setminus \{\bar{r}_3\} = \bigcup_{i=1}^{(m-3)/2} \{\bar{b}_i, \overline{2c - b_i}\} \cup \{\overline{2c - r_3}\} \cup \{\bar{c}\}$$

ให้ $j = 3, 4$ โดยที่

$$A^{(j)} = \{1 \leq i \leq (m-3)/2 : |A \cap \{\bar{b}_i, \overline{2c - b_i}\}| = j - 2\}$$

$$B^{(j)} = \{1 \leq i \leq (m-3)/2 : |B \cap \{\bar{b}_i, \overline{2c - b_i}\}| = j - 2\}$$

จะได้ว่า $|A^{(3)}| = |B^{(3)}|$ และ

$$|A| = |A^{(3)}| + 2|A^{(4)}| + \eta_A(2c - r_3) + 1$$

$$|B| = |B^{(3)}| + 2|B^{(4)}| + \eta_B(2c - r_3) + 1$$

$$R_3(A, \overline{2c}) = |A^{(4)}| + 1$$

$$R_3(B, \overline{2c}) = |B^{(4)}| + 1$$

เนื่องจาก $|A| = |B|$ และ $|A^{(3)}| = |B^{(3)}|$ จะได้ว่า

$$2|A^{(4)}| + \eta_A(2c - r_3) = 2|B^{(4)}| + \eta_B(2c - r_3)$$

เพราะฉะนั้น $2(|A^{(4)}| - |B^{(4)}|) = \eta_B(2c - r_3) - \eta_A(2c - r_3)$ ทำให้ได้ว่า $\eta_B(2c - r_3) - \eta_A(2c - r_3) = 0$

ดังนั้น $|A^{(4)}| = |B^{(4)}|$ และ $R_3(A, \overline{2c}) = R_3(B, \overline{2c})$

สุดท้ายนี้ เราจะแสดงว่า $R_3(A, \overline{2r_3}) = R_3(B, \overline{2r_3})$ พิจารณา $\bar{b}_1, \bar{b}_2, \dots, \bar{b}_{(m-1)/2} \in \mathbb{Z}_m$ ที่ทำให้

$$\mathbb{Z}_m \setminus \{\bar{r}_3\} = \bigcup_{i=1}^{(m-1)/2} \{\bar{b}_i, \overline{2r_3 - b_i}\}$$

ให้ $j = 5, 6$ โดยที่

$$A^{(j)} = \{1 \leq i \leq (m-1)/2 : |A \cap \{\bar{b}_i, \overline{2r_3 - b_i}\}| = j - 4\}$$

$$B^{(j)} = \{1 \leq i \leq (m-1)/2 : |B \cap \{\bar{b}_i, \overline{2r_3 - b_i}\}| = j - 4\}$$

จะได้ว่า $|A^{(5)}| = |B^{(5)}|$ และ

$$|A| = |A^{(5)}| + 2|A^{(6)}|$$

$$|B| = |B^{(5)}| + 2|B^{(6)}|$$

$$R_3(A, \overline{2r_3}) = |A^{(6)}|$$

$$R_3(B, \overline{2r_3}) = |B^{(6)}|$$

เนื่องจาก $|A| = |B|$ และ $|A^{(6)}| = |B^{(6)}|$ จะได้ว่า

$$R_3(A, \overline{2r_3}) = R_3(B, \overline{2r_3})$$

ดังนั้น $R_3(A, \overline{2n}) = R_3(B, \overline{2n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ เนื่องจาก m เป็นจำนวนคี่ จะได้ว่า $R_3(A, \bar{n}) = R_3(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ □

สำหรับกรณี 3 และ 4 สามารถพิสูจน์ในทำนองเดียวกับทฤษฎีบท 2.6 และ 2.7 ดังผลลัพธ์ต่อไปนี้

ทฤษฎีบท 2.8 ให้ $A, B \subseteq \mathbb{Z}_m$ โดยที่ $|A| = |B| = \frac{m-1}{2}$ และให้ $\bar{r}_1, \bar{r}_2, \bar{r}_3 \in \mathbb{Z}_m$ โดยที่ $A \cap B = \{\bar{r}_1\}$ และ $A \cup B = \mathbb{Z}_m \setminus \{\bar{r}_2, \bar{r}_3\}$ จะได้ว่า $R_3(A, \bar{n}) = R_3(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ ก็ต่อเมื่อ

$$A \setminus B = \{\bar{t} \in \mathbb{Z}_m : \exists! \bar{r} \in \{\bar{r}_2, \bar{r}_3\}, \overline{2t-r} \in B \wedge \overline{2t-r_1} \in B\} \cup \{\bar{t} \in \mathbb{Z}_m : \overline{2t-r} \in A, \forall \bar{r} \in \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}\}$$

ทฤษฎีบท 2.9 ให้ $A, B \subseteq \mathbb{Z}_m$ โดยที่ $|A| = |B| = \frac{m-3}{2}$ และให้ $\bar{r}_1, \bar{r}_2, \bar{r}_3 \in \mathbb{Z}_m$ โดยที่ $A \cap B = \emptyset$ และ $A \cup B = \mathbb{Z}_m \setminus \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}$ จะได้ว่า $R_3(A, \bar{n}) = R_3(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ ก็ต่อเมื่อ

$$A = \{\bar{t} \in \mathbb{Z}_m : \exists! \bar{r} \in \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}, \overline{2t-r} \notin A\}$$

3. อภิปรายและสรุปผลการวิจัย

งานวิจัยที่ศึกษาเกี่ยวกับปัญหาของ Sárközy ใน $\mathbb{Z}_m$ ซึ่งผลการศึกษาที่ได้มีความสอดคล้องและเป็นไปตามแนวคิดของ Yang และ Chen (Yang, & Chen. 2012: 257-262) ในปี ค.ศ. 2012 ที่เริ่มศึกษาปัญหาของ Sárközy ใน $\mathbb{Z}_m$ และให้เงื่อนไขของเซตย่อย $A, B \subseteq \mathbb{Z}_m$ โดยที่ $|(A \cup B) \setminus (A \cap B)| = m$ ที่ทำให้ $R_3(A, \bar{n}) = R_3(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ ก็ต่อเมื่อ m เป็นจำนวนคู่ และ

$$A = \{\bar{t} \in \mathbb{Z}_m : \bar{0} \leq \bar{t} \leq \overline{m/2-1}, \overline{t+m/2} \notin A\}$$

ต่อมาในปี ค.ศ. 2017 Yang และ Tang (Yang, & Tang. 2017: 73-85) แสดงว่าสำหรับ m เป็นจำนวนคี่ จะมีสองเซตย่อย A และ B ของ $\mathbb{Z}_m$ โดยที่ $|(A \cup B) \setminus (A \cap B)| = m-1$ ที่ทำให้ $R_3(A, \bar{n}) = R_3(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ ก็ต่อเมื่อ $A = \{\bar{t} \in \mathbb{Z}_m : \overline{2t-r} \in B\}$ โดยที่ $\bar{r} \in A \cap B$ และสุดท้ายในกรณี $|(A \cup B) \setminus (A \cap B)| = m-2$ ในปี ค.ศ. 2022 Sun และ Cheng (Sun, & Cheng. 2022: 352-363) พิจารณา $m = 2M$ เมื่อ M เป็นจำนวนคี่ โดยที่ $M \geq 3$ และผลการศึกษาสำหรับเซตย่อย $A, B \subseteq \mathbb{Z}_m$ โดยที่ $A \cup B = \mathbb{Z}_m$ และ $|A \cap B| = 2$ ถ้า $2 \nmid \text{ord}_p(2)$ สำหรับทุกจำนวนเฉพาะ p ซึ่ง $p|M$ แล้ว

$R_3(A, \bar{n}) = R_3(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ ก็ต่อเมื่อ $B = A \oplus \overline{m/2}$ ในงานวิจัยฉบับนี้ คณะผู้วิจัยได้ศึกษากรณี $|(A \cup B) \setminus (A \cap B)| = m-3$ ซึ่งผลการศึกษาแบ่งเป็น 4 กรณี ดังนี้

1. ให้ $A, B \subseteq \mathbb{Z}_m$ โดยที่ $|A|=|B|=\frac{m+3}{2}$ และให้ $\bar{r}_1, \bar{r}_2, \bar{r}_3 \in \mathbb{Z}_m$ โดยที่ $A \cup B = \mathbb{Z}_m$ และ $A \cap B = \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}$ จะได้ว่า $R_3(A, \bar{n}) = R_3(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ ก็ต่อเมื่อ

$$A \setminus B = \{\bar{t} \in \mathbb{Z}_m : \exists! \bar{r} \in \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}, \overline{2t-r} \in A\} \cup \{\bar{t} \in \mathbb{Z}_m : \overline{2t-r_i} = \bar{r}_j \wedge \overline{2t-r_k} \in B; \{i, j, k\} = \{1, 2, 3\}\}$$

2. ให้ $A, B \subseteq \mathbb{Z}_m$ โดยที่ $|A|=|B|=\frac{m+1}{2}$ และให้ $\bar{r}_1, \bar{r}_2, \bar{r}_3 \in \mathbb{Z}_m$ โดยที่ $A \cap B = \{\bar{r}_1, \bar{r}_2\}$ และ $A \cup B = \mathbb{Z}_m \setminus \{\bar{r}_3\}$ จะได้ว่า $R_3(A, \bar{n}) = R_3(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ ก็ต่อเมื่อ

$$A \setminus B = \{\bar{t} \in \mathbb{Z}_m : \exists! \bar{r} \in \{\bar{r}_1, \bar{r}_2\}, \overline{2t-r} \in A \wedge \overline{2t-r_3} \in A\} \cup \{\bar{t} \in \mathbb{Z}_m : \overline{2t-r} \in B, \forall \bar{r} \in \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}\} \cup \{\bar{t} \in \mathbb{Z}_m : \overline{2t-r_1} = \bar{r}_2 \wedge \overline{2t-r_3} \in A\}$$

3. ให้ $A, B \subseteq \mathbb{Z}_m$ โดยที่ $|A|=|B|=\frac{m-1}{2}$ และให้ $\bar{r}_1, \bar{r}_2, \bar{r}_3 \in \mathbb{Z}_m$ โดยที่ $A \cap B = \{\bar{r}_1\}$ และ $A \cup B = \mathbb{Z}_m \setminus \{\bar{r}_2, \bar{r}_3\}$ จะได้ว่า $R_3(A, \bar{n}) = R_3(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ ก็ต่อเมื่อ

$$A \setminus B = \{\bar{t} \in \mathbb{Z}_m : \exists! \bar{r} \in \{\bar{r}_2, \bar{r}_3\}, \overline{2t-r} \in B \wedge \overline{2t-r_1} \in B\} \cup \{\bar{t} \in \mathbb{Z}_m : \overline{2t-r} \in A, \forall \bar{r} \in \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}\}$$

4. ให้ $A, B \subseteq \mathbb{Z}_m$ โดยที่ $|A|=|B|=\frac{m-3}{2}$ และให้ $\bar{r}_1, \bar{r}_2, \bar{r}_3 \in \mathbb{Z}_m$ โดยที่ $A \cap B = \emptyset$ และ $A \cup B = \mathbb{Z}_m \setminus \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}$ จะได้ว่า $R_3(A, \bar{n}) = R_3(B, \bar{n})$ สำหรับทุก $\bar{n} \in \mathbb{Z}_m$ ก็ต่อเมื่อ

$$A = \{\bar{t} \in \mathbb{Z}_m : \exists! \bar{r} \in \{\bar{r}_1, \bar{r}_2, \bar{r}_3\}, \overline{2t-r} \notin A\}$$

ซึ่งผลการศึกษาดังกล่าวเป็นเพียงเงื่อนไขที่จะใช้ตรวจสอบเซตย่อย A และ B ของ $\mathbb{Z}_m$ ที่ทำให้ฟังก์ชันตัวแทนมีค่าเท่ากัน

4. เอกสารอ้างอิง

- Chen, S.Q., & Yan, X.H. (2020). On certain properties of partitions of $\mathbb{Z}_m$ with the same representation function. *Discrete Mathematics*, 343(9), 111981. <https://doi.org/10.1016/j.disc.2020.111981>
- Chen, S.Q., & Yan, X.H. (2021). Partitions of $\mathbb{Z}_m$ with Identical Representation Function. *Bulletin of the Australian Mathematical Society*, 103(2), 204–209. <https://doi.org/10.1017/S0004972720000945>
- Chen, Y.G., & Wang, B. (2003). On additive properties of two special sequences. *Acta Arithmetica*, 110, 299–303. <https://doi.org/10.4064/aa110-3-7>

- Chen, S.Q., Wang, R.J., & Yu, W.X. (2023). On the structure of sets in a residue class ring with the same representation function. *Advances in Applied Mathematics*, 148, 102533. <https://doi.org/10.1016/j.aam.2023.102533>
- Dombi, G. (2002). Additive properties of certain sets. *Acta Arith*, 103(2), 137–146. <https://eudml.org/doc/278550>
- Erdős, P., Sárközy, A. & Sós, V. T. (1986). Problems and results on additive properties of general sequences, V. *Monatshefte für Mathematik*, 102, 183–197. <https://link.springer.com/article/10.1007/BF01294598>
- Nathanson, M.B. (1978). Representation functions of sequences in additive number theory. *Proceedings of the American Mathematical Society*, 72(1), 16–20. <https://doi.org/10.2307/2042524>
- Sun, C.F., & Cheng, Z. (2022). On the structure of finite sets with the same representation functions. *Journal of Number Theory*, 241, 352–363. <https://doi.org/10.1016/j.jnt.2022.03.014>
- Yang, Q.H. & Chen F.J. (2012). Partitions of $\mathbb{Z}_m$ with the same representation functions. *Australasian Journal of Combinatorics*, 53, 257–262. https://ajc.maths.uq.edu.au/pdf/53/ajc_v53_p257.pdf
- Yang, Q.H. & Tang M. (2017). Representation functions on finite sets with extreme symmetric differences. *Journal of Number Theory*, 180, 73–85. <https://doi.org/10.1016/j.jnt.2017.03.024>