ภาคผนวก

เนื้อหาวิชาพีชคณิตนามธรรม

ในวิชาพีชคณิตนามธรรม มีหัวข้อหลักอยู่ 3 หัวข้อที่เราจะต้องศึกษา คือ **กลุ่ม** (group), **วง** (ring), และ **สนาม** (field) โดยกลุ่มเป็นหัวข้อแรกที่เราเริ่มต้นศึกษาและต้องศึกษาอย่างละเอียดเพื่อให้เข้าใจแจ่มแจ้งลึกซึ้ง จนสามารถนำความรู้ความเข้าใจพื้นฐานเกี่ยวกับกลุ่มนั้น ขยายแนวคิดไปสู่วงและสนามต่อไปได้

กลุ่มจะต้องมีองค์ประกอบหนึ่งคู่ คือ **เซต** (ซึ่งเป็นเซตไม่ว่าง) และ **การดำเนินการทวิภาค**บนเซตนั้น โดยทั่วไปนิยมเขียนแทนเซตด้วยตัวอักษร G และเขียนแทนการดำเนินการทวิภาคบนเซต G ด้วย $\circ$ ดังนั้นกลุ่มจึงถูกเขียนแทนด้วยสัญลักษณ์ $(G, \circ)$

– แต่เพื่อความสะดวก ในบางครั้งเมื่อกล่าวถึงกลุ่ม เราอาจเขียนเพียงสั้น ๆ ว่า G เป็นกลุ่ม แทนการเขียนเต็ม ๆ ว่า $(G, \circ)$ เป็นกลุ่ม

คุณสมบัติที่สำคัญของกลุ่มก็คือ

1. $\circ$ **มีคุณสมบัติเปลี่ยนกลุ่ม** (associative) นั่นคือ

$$a \circ (b \circ c) = (a \circ b) \circ c \qquad \text{ทุก ๆ } a, b, c \in G$$

2. มีสมาชิก e ใน G ซึ่ง

$$a \circ e = a = e \circ a \qquad \text{ทุก ๆ } a \in G$$

ซึ่งเราเรียกสมาชิก e ตัวนี้ว่า "**เอกลักษณ์**" (identity) ของ G ภายใต้ $\circ$

3. สำหรับแต่ละสมาชิก a ใน G จะหาสมาชิก b ใน G ได้ ซึ่ง

$$a \circ b = e = b \circ a$$

เราเรียก b ว่า "**ตัวผกผัน**" (inverse) ของ a

เราจะพบว่า ในกลุ่ม G **มีเอกลักษณ์เพียงตัวเดียว**เท่านั้น และสมาชิกแต่ละตัวในกลุ่ม G ก็มีตัวผกผัน**เพียงตัวเดียว**เช่นกัน

เราเรียกจำนวนของสมาชิกทั้งหมดในกลุ่ม G ว่า "**ขนาด**" (order) ของ G ถ้า G มีจำนวนสมาชิก n ตัว เราเรียก G ว่า "**กลุ่มจำกัด**" (finite group) แต่ถ้า G เป็นเซตอนันต์ เราเรียก G ว่า "**กลุ่มอนันต์**" (infinite group)

ถ้าเรามี G เป็นกลุ่ม และ a เป็นสมาชิกในกลุ่ม G เรากล่าวว่า a มี "**ขนาดจำกัด**" (finite order) ถ้ามีจำนวนเต็มบวก m ซึ่ง $a^m = e$ และเรียกจำนวนเต็มบวก n ที่เล็กที่สุด ซึ่ง $a^n = e$ ว่า "**ขนาด**" ของ a

แต่ถ้าไม่มีจำนวนเต็มบวก m ใด ๆ เลยซึ่ง $a^m = e$ เรากล่าวว่า a มี "**ขนาดอนันต์**" (infinite order)

<u>หมายเหตุ</u> a^m หมายถึง $a \circ a \circ \ldots \circ a$ โดยมี a อยู่ m ตัว และ $\circ$ เป็นการดำเนินการทวิภาคบน G

จากบทนิยามข้างต้น เราจะเห็นความแตกต่างระหว่าง "ขนาด" ของกลุ่ม และ "ขนาด" ของสมาชิกในกลุ่มได้ชัดเจน

ให้ H เป็นเซตย่อยของกลุ่ม G และ H มีคุณสมบัติปิดภายใต้การดำเนินการทวิภาคของ G ถ้า H เป็นกลุ่มภายใต้การดำเนินการดังกล่าวนี้ด้วยแล้ว เรากล่าวว่า H เป็น "**กลุ่มย่อย**" (subgroup) ของ G

ถ้า S เป็นเซตย่อยใด ๆ ของกลุ่ม G ให้ C เป็นเซตของกลุ่มย่อยทั้งหมดของ G ที่บรรจุ S และให้ $\langle S \rangle = \bigcap_{H \in C} H$ เราจะได้ว่า $\langle S \rangle$ เป็นกลุ่มย่อยที่เล็กที่สุดของ G ที่บรรจุ S ซึ่งจะเป็นได้อย่างเดียวเท่านั้น (unique) เราเรียก $\langle S \rangle$ นี้ว่า "**กลุ่มย่อยของ G ซึ่งก่อกำเนิดโดย S**" (subgroup of G generated by S)

โดยอาศัยทฤษฎีบท เราอาจคำนวณหา $\langle S \rangle$ ได้ดังนี้

$$\langle S \rangle = \{ a_1^{r_1} a_2^{r_2} \ldots a_m^{r_m} \mid a_i \in S \text{ และ } r_i \text{ เป็นจำนวนเต็มใด ๆ } \}$$

ถ้า S ประกอบด้วยสมาชิกเพียงตัวเดียวคือ a นั่นคือ $S = \{a\}$ เราจะเขียนแทน $\langle S \rangle$ ด้วย $\langle a \rangle$ และเรียก $\langle a \rangle$ ว่า "**กลุ่มย่อยวัฏจักร**" (cyclic subgroup) ของ S เราอาจคำนวณหา $\langle a \rangle$ ได้ในทำนองเดียวกันคือ

$$\langle a \rangle = \{ a^n \mid n \text{ เป็นจำนวนเต็มใด ๆ } \}$$

ถ้า G เป็นกลุ่ม และถ้ามี $a \in G$ ซึ่ง $\langle a \rangle = G$ แล้ว เราเรียก G ว่า "**กลุ่มวัฏจักร**" (cyclic group) และเรียก a ว่า "**ตัวก่อกำเนิด**" (generator) สำหรับ G

ถ้า $a \circ b = b \circ a$ ทุก ๆ $a,b \in G$ เราเรียกกลุ่ม G ว่า "**กลุ่มอาบีเลียน**" (abelian group)

ตัวอย่างของกลุ่มที่น่าสนใจ และเรามักพบบ่อย ๆ ได้แก่

1. กลุ่มของจำนวนเต็มภายใต้การบวก, $(\mathbb{Z}, +)$
2. กลุ่มของกลุ่มเศษตกค้างมอดุโล n ภายใต้การบวกของกลุ่มเศษตกค้าง, $(\mathbb{Z}_n, +)$
3. กลุ่มของตัวก่อกำเนิดของ $\mathbb{Z}_n$ ภายใต้การคูณของกลุ่มเศษตกค้าง, $(U_n, \cdot)$
4. กลุ่มสมมาตรภายใต้การประกอบ (composition), $(S_n, \circ)$

และ 5. กลุ่มที่เกิดจากผลคูณตรงของกลุ่มสองกลุ่มที่ได้กล่าวมาแล้ว

เราจะพบว่า $(\mathbb{Z}, +)$ เป็นกลุ่มอนันต์ ส่วน $(\mathbb{Z}_n, +)$, $(U_n, \cdot)$ และ $(S_n, \circ)$ เป็นกลุ่มจำกัด เมื่อพิจารณาคุณสมบัติสลับที่ของการดำเนินการทวิภาค เราจะพบว่ากลุ่ม $(\mathbb{Z}, +)$, $(\mathbb{Z}_n, +)$ และ $(U_n, \cdot)$ ต่างก็เป็นกลุ่มอาบีเลียนทั้งสิ้น ส่วนกลุ่ม $(S_n, \circ)$ ไม่เป็นกลุ่มอาบีเลียน เมื่อ $n \geq 3$ นอกจากนี้เราพบว่าผลคูณตรงของกลุ่มสองกลุ่ม ซึ่งต่างก็เป็นกลุ่มอาบีเลียน จะยังคงเป็นกลุ่มอาบีเลียนด้วย

ในโปรแกรมช่วยสอนนี้ เราจะให้ความสนใจกลุ่มสี่กลุ่มที่ได้กล่าวถึงข้างต้น รวมทั้งผลคูณตรงของ $\mathbb{Z}_m$ และ $\mathbb{Z}_n$ **หรือ** U_m และ U_n **หรือ** $\mathbb{Z}_m$ และ U_n เป็นต้น

ต่อไปนี้จะขอทบทวนรายละเอียดของแต่ละกลุ่มให้เข้าใจพอสังเขป ก่อนที่จะลงมือทำแบบฝึกหัดหรือทดสอบความรู้ต่อไป

1. กลุ่ม $(\mathbb{Z}, +)$

ถ้าให้ $\mathbb{Z}$ แทนเซตของจำนวนเต็ม เราพบว่า $\mathbb{Z}$ เป็นกลุ่มภายใต้การดำเนินการบวกปรกติ โดยแต่ละสมาชิก a ใน $\mathbb{Z}$ จะมี $-a$ เป็นตัวผกผัน $(\mathbb{Z}, +)$ เป็นกลุ่มที่เราคุ้นเคยมาตั้งแต่ชั้นประถมต้น เพียงแต่เราไม่ได้ตระหนักถึงคุณสมบัติของความเป็นกลุ่มของ $\mathbb{Z}$ $(\mathbb{Z}, +)$ เป็นกลุ่มอนันต์และเป็นกลุ่มอาบีเลียน ยิ่งกว่านั้นเราจะพบว่า $(\mathbb{Z}, +)$ เป็นกลุ่มวัฏจักรด้วยโดยมีตัวก่อกำเนิด 2 ตัวคือ 1 และ -1

ในทฤษฎีจำนวน (number theory) เราจะศึกษาคุณสมบัติที่น่าสนใจต่างๆ บนเซต $\mathbb{Z}$ หนึ่งในความรู้พื้นฐานที่เราศึกษาเกี่ยวกับจำนวนเต็มต่างๆ ใน $\mathbb{Z}$ ก็คือ **การหาตัวหารร่วมมาก** (greatest common divisor) **และการหาตัวคูณร่วมน้อย** (least common multiple) ของจำนวนเต็ม 2 ตัวคือ a และ b ซึ่งเราเขียนย่อ ๆ เป็น ห.ร.ม. (a, b) และ ค.ร.น.(a, b) ตามลำดับ

การหา ห.ร.ม. (a, b) ทำได้โดยอาศัย**ขั้นตอนวิธีหาร** (division algorithm) ซึ่งเราจะพบว่า เมื่อใช้กระบวนการย้อนกลับ เราก็จะสามารถเขียน ห.ร.ม. (a, b) ให้อยู่ใน**รูปการรวมเชิงเส้น** (linear combination) ของ a และ b ได้ ในการพิสูจน์ทฤษฎีบทต่าง ๆ ทาง algebra เราจะพบว่าตัวหารร่วมมากและตัวคูณร่วมน้อยถูกนำมาใช้เป็นเครื่องมือเพื่อช่วยในการพิสูจน์อยู่บ่อย ๆ

เนื่องจาก $\mathbb{Z}$ เป็นกลุ่มวัฏจักร โดยทฤษฎีบทซึ่งกล่าวว่า "ทุกกลุ่มย่อยของกลุ่มวัฏจักรเป็นกลุ่มวัฏจักร" ดังนั้นกลุ่มย่อยทั้งหมดของ $\mathbb{Z}$ จึงเขียนได้ในรูป $\langle a \rangle$ สำหรับบางจำนวนเต็ม a ซึ่งเราอาจคำนวณหา $\langle a \rangle$ ได้ดังที่ได้กล่าวไว้แล้วคือ

$$\langle a \rangle = \{ka \mid k \text{ เป็นจำนวนเต็มใด ๆ}\}$$
$$= \{0, \pm a, \pm 2a, \pm 3a, \pm 4a, \ldots\}$$

ส่วนการคำนวณหากลุ่มย่อยของ $\mathbb{Z}$ ที่ก่อกำเนิดโดยจำนวนเต็มตั้งแต่ 2 ตัวขึ้นไป เราอาจใช้ตัวหารร่วมมากมาช่วย ซึ่งจะทำให้สะดวกและรวดเร็วกว่าการคำนวณหาโดยใช้ทฤษฎีบทโดยตรงดังนี้

$$\langle a, b \rangle = \langle c \rangle$$

โดยที่ $c =$ ห.ร.ม.(a, b)

เราอาจประยุกต์หลักการดังกล่าวนี้เพื่อใช้ในการหากลุ่มย่อย $\langle a, b, c \rangle$ ซึ่งก่อกำเนิดโดยจำนวนเต็ม 3 ตัวคือ a, b และ c ได้ต่อไป

2. กลุ่ม $(\mathbb{Z}_n, +)$

จากที่ได้ศึกษาวิชาพีชคณิตนามธรรมมาแล้ว พบว่าเมื่อกำหนดจำนวนเต็มบวก n มาให้เราจะสามารถหา**กลุ่มเศษตกค้างมอดุโล n** (residue class modulo n) สำหรับจำนวนเต็ม k ใดๆ ได้เสมอ ซึ่งกลุ่มเศษตกค้างดังกล่าวคือ

$$\overline{k} = \{k + ns \mid s \text{ เป็นจำนวนเต็มใดๆ }\}$$

ตัวอย่างเช่น เมื่อกำหนด $n = 6$

ถ้า $k = -2$ เราจะได้ $\overline{-2} = \{-2 + 6s \mid s \text{ เป็นจำนวนเต็มใดๆ }\}$

$= \{\ldots, -14, -8, -2, 4, 10, \ldots\}$

ในทำนองเดียวกัน

ถ้า $k = -4$ เราจะได้ $\overline{-4} = \{\ldots, -16, -10, -4, 2, 8, \ldots\}$

ถ้า $k = 0$ เราจะได้ $\overline{0} = \{\ldots, -12, -6, 0, 6, 12, \ldots\}$

ถ้า $k = 2$ เราจะได้ $\overline{2} = \{\ldots, -10, -4, 2, 8, 14, \ldots\}$

ยิ่งกว่านั้น เราพบว่า สำหรับจำนวนเต็มบวก n ที่กำหนดให้ เราจะหากลุ่มเศษตกค้างมอดุโล n ที่แตกต่างกันได้เพียง n กลุ่มเท่านั้นคือ

$$\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$$

ถ้าเราให้ $\mathbb{Z}_n$ แทนเซตของกลุ่มเศษตกค้างเหล่านี้ นั่นคือ

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$$

เราพบว่า $\mathbb{Z}_n$ มีคุณสมบัติเป็นกลุ่ม (group) ภายใต้การดำเนินการบวกของกลุ่มเศษตกค้าง

ซึ่งการดำเนินการบวกดังกล่าวมีคุณสมบัติดังนี้

$$\overline{a} + \overline{b} = \overline{b} + \overline{a}$$

$$\overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c}$$

$$\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$$

$$(\overline{a} + \overline{b}) \cdot \overline{c} = \overline{a} \cdot \overline{c} + \overline{b} \cdot \overline{c}$$

$$\overline{a} + \overline{0} = \overline{0} + \overline{a} = \overline{a}$$

$$\overline{a} + \overline{(-a)} = \overline{(-a)} + \overline{a} = \overline{0}$$

จากคุณสมบัติสองข้อสุดท้ายของการบวกของกลุ่มเศษตกค้าง ทำให้เราทราบว่า $\bar{0}$ เป็นเอกลักษณ์ของกลุ่ม $\mathbb{Z}_n$ ทุกค่า n และ $\overline{-a}$ เป็นตัวผกผันของสมาชิก $\bar{a}$ ใด ๆ ใน $\mathbb{Z}_n$ โดยที่ $\overline{-0} = \bar{0}$ และ $\overline{-a} = \overline{n-a}$ เมื่อ $0 < a \leq n\text{-}1$

ตัวอย่างเช่น ใน $\mathbb{Z}_6$ ตัวผกผันของ $\bar{4}$ คือ $\overline{-4}$ ซึ่ง $\overline{-4} = \overline{6-4} = \bar{2}$ นั่นเอง

ต่อไปลองนำสมาชิก $\bar{a}$ ใด ๆ ใน $\mathbb{Z}_n$ มาก่อกำเนิดกลุ่มย่อยวัฏจักร $\langle \bar{a} \rangle$ ของ $\mathbb{Z}_n$ ซึ่งเราทราบแล้วว่า เราสามารถคำนวณหา $\langle \bar{a} \rangle$ ได้โดย

$$\langle \bar{a} \rangle = \{(\bar{a})^k \mid k \text{ เป็นจำนวนเต็มใดๆ }\}$$

เนื่องจากการดำเนินการที่เราใช้คือ การบวกของกลุ่มเศษตกค้าง ดังนั้น $(\bar{a})^k$ จึงหมายถึง $\bar{a}+\bar{a}+\ldots+\bar{a}$ โดยมี $\bar{a}$ อยู่ในผลบวกเป็นจำนวน k ตัวเมื่อ k เป็นจำนวนเต็มบวก และหมายถึง $\overline{-a}+\ldots+\overline{-a}$ โดยมี $\overline{-a}$ อยู่ในผลบวกเป็นจำนวน $-k$ ตัว เมื่อ k เป็นจำนวนเต็มลบและ $(\bar{a})^0 = 0$

ตัวอย่างเช่น ใน $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

$$\begin{aligned}\langle \bar{4} \rangle &= \{\ldots, (\bar{4})^{-2}, (\bar{4})^{-1}, (\bar{4})^0, (\bar{4})^1, (\bar{4})^2, \ldots\} \\ &= \{\ldots, \overline{-8}, \overline{-4}, \bar{0}, \bar{4}, \bar{8}, \ldots\} \\ &= \{\ldots, \bar{4}, \bar{2}, \bar{0}, \bar{4}, \bar{2}, \ldots\}\end{aligned}$$

ดังนั้น $\langle \bar{4} \rangle = \{\bar{0}, \bar{2}, \bar{4}\}$

ถ้าต้องการหาขนาดของสมาชิก $\bar{a}$ ใด ๆ ใน $\mathbb{Z}_n$ โดยบทนิยาม ขนาดของ $\bar{a}$ หมายถึง จำนวนเต็มบวก m ตัวที่เล็กที่สุดซึ่ง $(\bar{a})^m = \bar{0}$ แต่ในทางปฏิบัติ เราอาจหาขนาดของ $\bar{a}$ ได้โดยอาศัยทฤษฎีบทหนึ่งในวิชาพีชคณิตนามธรรม ซึ่งกล่าวว่า "ขนาดของสมาชิก $\bar{a}$ = ขนาดของกลุ่มย่อย $\langle \bar{a} \rangle$" ซึ่งโดยบทนิยาม ขนาดของกลุ่ม(ย่อย) $\langle \bar{a} \rangle$ หมายถึง จำนวนของสมาชิกทั้งหมดใน $\langle \bar{a} \rangle$ นั่นเอง

ตัวอย่างเช่น ใน $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ เนื่องจาก $\langle \bar{4} \rangle = \{\bar{0}, \bar{2}, \bar{4}\}$ ดังนั้นขนาดของ $\bar{4} = 3$

เมื่อลองพิจารณารายละเอียดในกลุ่ม $\mathbb{Z}_n$ เพิ่มเติม เราจะพบว่า $\mathbb{Z}_n$ เป็น กลุ่มวัฏจักร นั่นคือ มีสมาชิก $\bar{a}$ ใน $\mathbb{Z}_n$ ซึ่ง $\langle \bar{a} \rangle = \mathbb{Z}_n$ เราเรียกสมาชิก $\bar{a}$ ดังกล่าวนี้ว่า "ตัวก่อกำเนิด" การคำนวณหาตัวก่อกำเนิด $\bar{a}$ ของกลุ่ม $\mathbb{Z}_n$ ทำได้โดยอาศัยทฤษฎีบทที่กล่าวว่า

"$\bar{a}$ เป็นตัวก่อกำเนิดของ $\mathbb{Z}_n$ ก็ต่อเมื่อ ห.ร.ม. $(a, n) = 1$"

ตัวอย่างเช่น ใน $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ จะได้ว่า ตัวก่อกำเนิดของ $\mathbb{Z}_6$ คือ $\bar{1}$ และ $\bar{5}$

เนื่องจาก $\mathbb{Z}_n$ เป็นกลุ่มวัฏจักร โดยทฤษฎีบททำให้เราทราบว่า "ทุกกลุ่มย่อยของกลุ่มวัฏจักรเป็นกลุ่มวัฏจักร" นั่นหมายความว่า กลุ่มย่อยใด ๆ ของ $\mathbb{Z}_n$ ต้องเขียนได้ในรูป $\langle \bar{x} \rangle$ สำหรับบางสมาชิก $\bar{x}$ ใน $\mathbb{Z}_n$

ยิ่งกว่านั้น เนื่องจาก $\mathbb{Z}_n$ เป็นกลุ่มอาบีเลียน ดังนั้น "ทุกกลุ่มย่อยของ $\mathbb{Z}_n$ จึงเป็นกลุ่มย่อยนอร์แมล" เมื่อเรานำกลุ่มย่อย $\langle \bar{a} \rangle$ ใด ๆ ของ $\mathbb{Z}_n$ (ซึ่งเป็นกลุ่มย่อยนอร์แมล) มา**แบ่งกั้น** (partition) $\mathbb{Z}_n$ ออกเป็นส่วนๆ โดยเรียกแต่ละส่วนว่า "โคเซต" เซตของโคเซตทั้งหมดที่ได้นี้จะเป็นกลุ่มภายใต้การดำเนินการบวกซึ่งนิยามโดย

$$(\bar{x} + \langle \bar{a} \rangle) + (\bar{y} + \langle \bar{a} \rangle) = (\bar{x} + \bar{y}) + \langle \bar{a} \rangle$$

เราเรียกกลุ่มดังกล่าวนี้ว่า "กลุ่มผลหารของ $\mathbb{Z}_n$ โดย $\langle \bar{a} \rangle$" เขียนแทนด้วย $\mathbb{Z}_n/\langle \bar{a} \rangle$ ขนาดของกลุ่มผลหารหรือจำนวนสมาชิกทั้งหมดในกลุ่มผลหาร เราเรียกว่า "ดรรชนี" ของ $\langle \bar{a} \rangle$ ใน $\mathbb{Z}_n$

โดยทฤษฎีบท เนื่องจาก $\mathbb{Z}_n$ เป็นกลุ่มวัฏจักร ดังนั้นกลุ่มผลหารของ $\mathbb{Z}_n$ โดย $\langle \bar{a} \rangle$ จึงเป็นกลุ่มวัฏจักรด้วย โดยมี $\bar{x} + \langle \bar{a} \rangle$ เป็นตัวก่อกำเนิดเมื่อ $\bar{x}$ เป็นตัวก่อกำเนิดของ $\mathbb{Z}_n$

ตัวอย่างเช่น $\langle \bar{4} \rangle$ เป็นกลุ่มย่อยหนึ่งของ $\mathbb{Z}_6$ จะเห็นว่าโคเซตทั้งหมดที่แตกต่างกันซึ่งได้จากการนำ $\langle \bar{4} \rangle$ ไปแบ่งกั้น $\mathbb{Z}_6$ มีอยู่ 2 โคเซตคือ

$$\bar{0} + \langle \bar{4} \rangle = \{\bar{0}, \bar{2}, \bar{4}\} = \bar{2} + \langle \bar{4} \rangle = \bar{4} + \langle \bar{4} \rangle$$
$$\bar{1} + \langle \bar{4} \rangle = \{\bar{1}, \bar{3}, \bar{5}\} = \bar{3} + \langle \bar{4} \rangle = \bar{5} + \langle \bar{4} \rangle$$

ดังนั้น ดรรชนีของ $\langle \bar{4} \rangle$ ใน $\mathbb{Z}_6$ เท่ากับ 2 และจะพบว่าตัวก่อกำเนิดของ $\mathbb{Z}_6/\langle \bar{4} \rangle$ มีเพียงตัวเดียวคือ $\bar{1} + \langle \bar{4} \rangle$ เพราะ $\bar{1}$ และ $\bar{5}$ เป็นตัวก่อกำเนิดของ $\mathbb{Z}_6$ และ $\bar{1} + \langle \bar{4} \rangle = \bar{5} + \langle \bar{4} \rangle$

3. กลุ่ม $(U_n, \cdot)$

จากที่ได้ศึกษารายละเอียดเกี่ยวกับกลุ่ม $(\mathbb{Z}_n, +)$ มาแล้ว เราพบว่า $(\mathbb{Z}_n, +)$ เป็นกลุ่มวัฏจักร ที่มี $\bar{a}$ เป็นตัวก่อกำเนิดโดยที่ ห.ร.ม. $(a, n) = 1$ ดังนั้นเราจึงพบว่าตัวก่อกำเนิดของ $\mathbb{Z}_n$ อาจมีได้มากกว่า 1 ตัว

ยิ่งกว่านั้น หากเราพิจารณาเซต $\mathbb{Z}_n$ ภายใต้การดำเนินการบวกและคูณของกลุ่มเศษตกค้าง เราจะพบว่า $(\mathbb{Z}_n, +, \cdot)$ เป็นวง และเป็นวงซึ่งมีหนึ่ง (identity หรือ unity) คือ $\bar{1}$ นั่นคือ

$$\bar{1} \cdot \bar{a} = \bar{a} = \bar{a} \cdot \bar{1} \qquad \text{ทุก ๆ } \bar{a} \in \mathbb{Z}_n$$

และสมาชิก $\bar{a}$ ของ $\mathbb{Z}_n$ จะเป็นหน่วย (unit) ถ้า $\bar{a}$ มีตัวผกผันภายใต้การคูณ นั่นคือ มี $\bar{b}$ ใน $\mathbb{Z}_n$ ซึ่ง $\bar{a} \cdot \bar{b} = \bar{1} = \bar{b} \cdot \bar{a}$ นั่นเอง

มีทฤษฎีบทหนึ่งในพีชคณิตนามธรรมกล่าวว่า "$\bar{a}$ เป็นหน่วยของ $\mathbb{Z}_n$ ก็ต่อเมื่อ ห.ร.ม. $(a, n) = 1$"

ดังนั้นโดยทฤษฎีบทดังกล่าว ทำให้เราทราบว่า $\bar{a}$ เป็นหน่วยของวง $\mathbb{Z}_n$ ก็ต่อเมื่อ $\bar{a}$ เป็นตัวก่อกำเนิดของกลุ่ม $\mathbb{Z}_n$

ถ้าให้ U_n แทนเซตของหน่วยทั้งหมดในวง $\mathbb{Z}_n$ เราจะพบว่า U_n เป็นกลุ่มภายใต้การดำเนินการคูณของกลุ่มเศษตกค้าง และ $(U_n, \cdot)$ เป็นกลุ่มอาบีเลียน แต่ $(U_n, \cdot)$ ไม่เป็นกลุ่มวัฏจักรเสมอไป โดยอาศัยความรู้เพิ่มเติมทางทฤษฎีจำนวน เราพบว่า $(U_n, \cdot)$ จะเป็นกลุ่มวัฏจักร ก็ต่อเมื่อ $n = 2, 4, p^t$ หรือ $2p^t$ เมื่อ p เป็นจำนวนเฉพาะคี่และ t เป็นจำนวนเต็มบวก

เนื่องจาก $\mathbb{Z}_n$ เป็นกลุ่มวัฏจักรที่มีขนาดเท่ากับ n โดยทฤษฎีบทเราจึงทราบว่า $\mathbb{Z}_n$ มีตัวก่อกำเนิดทั้งหมด $\phi(n)$ ตัว โดยที่ $\phi(n)$ คือ Euler's phi function ซึ่งหมายถึง **จำนวน**ของจำนวนเต็มบวกซึ่งน้อยกว่า n และเป็นจำนวนเฉพาะต่อกันกับ n ดังนั้นกลุ่ม U_n จึงมีขนาดเท่ากับ $\phi(n)$ และถ้า U_n เป็นกลุ่มวัฏจักร เราก็จะทราบว่า U_n มีจำนวนของตัวก่อกำเนิดทั้งหมดเท่ากับ $\phi(\phi(n))$

การหาตัวก่อกำเนิดของ U_n ทำได้ค่อนข้างยาก และต้องอาศัยความรู้เพิ่มเติมทาง ทฤษฎีจำนวน ซึ่งไม่อาจหาอ่านได้ในหนังสือพีชคณิตนามธรรมทั่วไป ทฤษฎีบทและขั้นตอนทั้งหลายที่ใช้ในการหาตัวก่อกำเนิดของ U_n ที่จะกล่าวถึงต่อไปนี้ ได้มาจากโครงงานทางคณิตศาสตร์เรื่อง "Exploring the Group of Units in $\mathbb{Z}_n$" จัดทำในปี พ.ศ. 2540 โดยนายเจษฎา ตัณฑนุช ผู้สนใจหาอ่านรายละเอียดเพิ่มเติมได้ที่ ห้องสมุดภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่

<u>ทฤษฎีบท</u> ให้ p เป็นจำนวนเฉพาะคี่

สำหรับ $\phi(p) = p\text{-}1 = q_1^{t_1}q_2^{t_2}\cdots q_r^{t_r}$ เมื่อ $q_1, q_2, \ldots, q_r$ เป็นจำนวนเฉพาะ และ $t_i > 1$, $i = 1, 2, \ldots, r$ จะมี $a_1, a_2, \ldots, a_r$ ซึ่ง $\text{ord}_p\, a_1 = q_1^{t_1}$, $\text{ord}_p\, a_2 = q_2^{t_2}$, ..., $\text{ord}_p\, a_r = q_r^{t_r}$ และจะได้ว่า $a = a_1 a_2 \ldots a_r$ เป็นตัวก่อกำเนิดของ U_p

<u>หมายเหตุ</u> $\text{ord}_p\, a$ หมายถึงจำนวนเต็มบวก r ที่น้อยที่สุด ซึ่ง $a^r \equiv 1 (\text{mod}\, p)$

การหาตัวก่อกำเนิดสำหรับ U_n เมื่อ $n = p^2, p^t$ และ $2p^t$ เมื่อ p เป็นจำนวนเฉพาะคี่ และ $t = 3, 4, 5, \ldots$

1. ถ้า a เป็นตัวก่อกำเนิดของกลุ่ม U_p จะได้ว่า $r = a$ หรือ $r = a + p$ เป็นตัวก่อกำเนิดของ U_{p^2}

2. ถ้า r เป็นตัวก่อกำเนิดของกลุ่ม U_{p^2} จะได้ว่า r เป็นตัวก่อกำเนิดของ U_{p^t}; t = 3, 4, 5, ...

3. ถ้า r เป็นตัวก่อกำเนิดของกลุ่ม U_{p^t} เมื่อ t = 1, 2, 3, ... จะได้ว่า

   ก. ถ้า r เป็นจำนวนคี่ แล้ว r เป็นตัวก่อกำเนิดของกลุ่ม U_{2p^t}

   ข. ถ้า r เป็นจำนวนคู่ แล้ว $r + p^t$ เป็นตัวก่อกำเนิดของกลุ่ม U_{2p^t}

   เมื่อ t = 1, 2, 3, ...

<u>ทฤษฎีบท</u> ถ้า a เป็นตัวก่อกำเนิดของกลุ่ม U_n แล้ว a^{-1} เป็น ตัวก่อกำเนิดของกลุ่ม U_n ด้วย

<u>ตัวอย่าง</u> การหาตัวก่อกำเนิดทั้งหมดของ U_{19}

เนื่องจากขนาดของกลุ่ม $U_{19} = \phi(19) = 18 = 2 \cdot 3^2$ ดังนั้น

หา a_1 โดยที่ $\text{ord}_{19}(a_1) = 2$ หรือ $a_1^2 \equiv 1 (\text{mod}\ 19)$ จะได้ว่า $a_1 = 18$

หา a_2 โดยที่ $\text{ord}_{19}(a_2) = 3^2 = 9$ หรือ $a_2^9 \equiv 1 \pmod{19}$ จะได้ว่า $a_2 = 4, 5, 6, 9, 16$ และ 17

ดังนั้น ตัวก่อกำเนิดทั้งหมดของ U_{19} คือ

$$18 \cdot 4 = 72 \equiv 15 \pmod{19}$$
$$18 \cdot 5 = 90 \equiv 14 \pmod{19}$$
$$18 \cdot 6 = 108 \equiv 13 \pmod{19}$$
$$18 \cdot 9 = 162 \equiv 10 \pmod{19}$$
$$18 \cdot 16 = 288 \equiv 3 \pmod{19}$$
$$18 \cdot 17 = 306 \equiv 2 \pmod{19}$$

นั่นคือ $\bar{2}, \bar{3}, \overline{10}, \overline{13}, \overline{14}$ และ $\overline{15}$ เป็นตัวก่อกำเนิดของ U_{19}

<u>ตัวอย่าง</u> การหาตัวก่อกำเนิดของ U_3, U_6, U_9 และ U_{18}

1. เนื่องจากขนาดของ $U_3 = \phi(3) = 2$ และ $\bar{2}$ เป็นสมาชิกใน U_3 ที่มีขนาดเท่ากับ 2 ดังนั้น $\bar{2}$ เป็นตัวก่อกำเนิดของ U_3 และเนื่องจาก U_3 มีตัวก่อกำเนิดทั้งหมด $\phi(\phi(3)) = \phi(2) = 1$ ตัว ดังนั้น $\bar{2}$ จึงเป็นตัวก่อกำเนิดตัวเดียวเท่านั้นของ U_3

2. เนื่องจาก $\bar{2}$ เป็นตัวก่อกำเนิดของ U_3 ดังนั้น $\bar{2}$ หรือ $\bar{2}+\bar{3} = \bar{5}$ เป็นตัวก่อกำเนิดของ $U_{3^2} = U_9$

เพราะว่า $\text{ord}_9(\bar{2}) = 6 = \phi(9)$ จึงได้ว่า $\bar{2}$ เป็นตัวก่อกำเนิดของ U_9 แต่เนื่องจาก $\bar{5}$ เป็นตัวผกผันของ $\bar{2}$ ใน U_9 ดังนั้น $\bar{5}$ จึงเป็นตัวก่อกำเนิดของ U_9 ด้วย และตัวก่อกำเนิดทั้งหมดใน U_9 มีอยู่เพียง $\phi(\phi(9)) = \phi(6) = 2$ ตัวเท่านั้นคือ $\bar{2}$ และ $\bar{5}$

3. เนื่องจาก $\bar{2}$ เป็นจำนวนคู่ ดังนั้น

$\bar{2} + \bar{3} = \bar{5}$ เป็นตัวก่อกำเนิดของ $U_{2\cdot 3} = U_6$

และ $\bar{2} + (\bar{3})^2 = \overline{11}$ เป็นตัวก่อกำเนิดของ $U_{2\cdot 3^2} = U_{18}$

เนื่องจาก U_6 มีตัวก่อกำเนิดทั้งหมด $\phi(\phi(6)) = \phi(2) = 1$ ตัว

ดังนั้น $\bar{5}$ จึงเป็นตัวก่อกำเนิดตัวเดียวเท่านั้นของ U_6

และเนื่องจาก U_{18} มีตัวก่อกำเนิดทั้งหมด $\phi(\phi(18)) = \phi(6) = 2$ ตัว จึงได้ว่า $\bar{5}$ ซึ่งเป็นตัวผกผันของ $\overline{11}$ เป็นตัวก่อกำเนิดอีกตัวหนึ่งของ U_{18}

4. กลุ่มสมมาตร $(S_n, \circ)$

ถ้า A เป็นเซตไม่ว่าง และ σ เป็นฟังก์ชันหนึ่งต่อหนึ่งแบบทั่วถึงจาก A ไป A เรา เรียก σ ว่า **"วิธีเรียงสับเปลี่ยน"** (permutation) ของ A

ตามปรกติ เรานิยมเขียนแทนวิธีเรียงสับเปลี่ยน 2 วิธีคือ

1. โดยการเขียนแต่ละสมาชิกในโดเมนไว้ในแถวแรก และเขียนภาพ (image) ของแต่ละสมาชิกเหล่านั้นไว้ในตำแหน่งที่สมนัยกันในแถวที่สอง

ตัวอย่างเช่น ถ้า $A = \{1, 2, 3, 4, 5\}$ และ σ เป็นวิธีเรียงสับเปลี่ยนของ A โดยที่ $\sigma : A \to A$ และ $\sigma(1) = 5, \sigma(2) = 3, \sigma(3) = 1, \sigma(4) = 2$ และ $\sigma(5) = 4$ เราอาจเขียนแทน σ ด้วยสัญลักษณ์

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix}$$

เป็นต้น

2. โดยการเขียนอยู่ในรูป**วัฏจักร** (cycle) เป็น $(i_1\ i_2\ \dots\ i_r)$ เมื่อแต่ละ i_j เป็นสมาชิกในโดเมนที่ต่างกัน ในสัญกรณ์วัฏจักร ภาพของแต่ละสมาชิกในโดเมนจะถูกเขียนไว้ทางขวามือของสมาชิกตัวนั้น ยกเว้นภาพของสมาชิกตัวสุดท้ายในวัฏจักรจะปรากฏเป็นสมาชิกตัวแรกในวัฏจักร แต่ถ้าสมาชิกตัวใดในโดเมนไม่ได้ถูกเขียนไว้ในวัฏจักร หมายความว่าสมาชิกตัวนั้นถูกส่งไปยังตัวมันเอง

ตัวอย่างเช่น ถ้า $A = \{1, 2, 3, 4, 5\}$ และ σ, τ เป็นวิธีเรียงสับเปลี่ยนของ A โดยที่

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix} \quad \text{และ} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 1 & 4 \end{pmatrix}$$

ดังนั้น σ และ τ อาจเขียนอยู่ในรูปวัฏจักรได้เป็น

$$\sigma = (15423) \qquad \text{และ} \quad \tau = (154)$$

ตามลำดับ เป็นต้น

ถ้าให้ S_A แทนเซตของวิธีเรียงสับเปลี่ยนของ A ทั้งหมด เราจะพบว่า S_A เป็นกลุ่มภายใต้การประกอบ และถ้า A เป็นเซตจำกัดที่มีสมาชิกทั้งหมด n ตัว เราจะเขียนแทน S_A ด้วย S_n และเรียก $(S_n, \circ)$ ว่า "**กลุ่มสมมาตร**" (symmetric group) บนอักษร n ตัว

โดยทฤษฎีบท เราจะทราบว่า "ถ้า $\sigma \in S_n$ และ $\sigma \neq (1)$ หรือ **ฟังก์ชันเอกลักษณ์** (identity mapping) แล้ว σ สามารถเขียนแสดงได้ในรูปผลคูณ (หรือผลประกอบ) ของวัฏจักรต่างสมาชิก (disjoint) ทั้งหลาย"

ตัวอย่างเช่น ให้ $A = \{1, 2, 3, 4, 5\}$ นั่นคือใน S_5 ถ้า $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$ เราสามารถเขียนแสดง σ ในรูปผลคูณของวัฏจักรต่างสมาชิกได้เป็น

$$\sigma = (123)(45)$$ เป็นต้น

ความยาวของวัฏจักร หมายถึง จำนวนของสมาชิก (ในโดเมน) ที่ปรากฏอยู่ในวัฏจักร เราเรียกวัฏจักรซึ่งมีความยาว 2 ว่า "**คู่สลับ**" (transposition)

โดยทฤษฎีบท เราจะทราบว่า "ถ้า $\sigma \in S_n$ เมื่อ $n \geq 2$ จะได้ว่า σ เขียนอยู่ในรูปผลคูณของ คู่สลับทั้งหลายได้"

ตัวอย่างเช่น ใน S_5 เราสามารถเขียน $\sigma = (123)(45)$ ในรูปผลคูณของคู่สลับทั้งหลายได้เป็น

$$\sigma = (13)(12)(45)$$

เพราะโดยปรกติ $(a_1\, a_2 \ldots a_n) = (a_1\, a_n)\,(a_1\, a_{n-1}) \ldots (a_1\, a_2)$

<u>หมายเหตุ</u> ในที่นี้ผลคูณของวิธีเรียงสับเปลี่ยนจะดำเนินการ**จากขวาไปซ้าย**

เราจะเห็นได้ว่าคู่สลับในผลคูณเหล่านี้ไม่จำเป็นต้องต่างสมาชิกกัน และจำนวนของคู่สลับในผลคูณก็อาจไม่เท่ากัน **แต่**จำนวนของคู่สลับในผลคูณนั้นต้องเป็น**จำนวนคู่หรือจำนวนคี่เหมือนกัน** ตัวอย่างเช่น

$$\begin{aligned}(123)(45) &= (13)(12)(45) \\ &= (13)(12)(34)(34)(45) \\ &= (54)(13)(54)(12)(34)(34)(45)\end{aligned}$$

เป็นต้น

เราเรียกวิธีเรียงสับเปลี่ยน σ ใน S_n ว่า "**วิธีเรียงสับเปลี่ยนคู่**" (even permutation) ถ้า σในรูปผลคูณของคู่สลับ มีจำนวนของคู่สลับในผลคูณเป็นจำนวนคู่ และเรียก σว่า "**วิธีเรียงสับเปลี่ยนคี่**" (odd permutation) ถ้า σ ในรูปผลคูณของคู่สลับ มีจำนวนของคู่สลับในผลคูณเป็นจำนวนคี่

ตัวอย่างเช่น ใน S_5, $\sigma = (123)(45)$ เป็นวิธีเรียงสับเปลี่ยนคี่ ในขณะที่ $\tau = (12345)$ เป็นวิธีเรียงสับเปลี่ยนคู่ เพราะ

$$(12345) = (15)(14)(13)(12)$$

ถ้า σ เป็นวิธีเรียงสับเปลี่ยนคู่ ใน S_n เมื่อ $n \geq 3$ โดยทฤษฎีบท เราพบว่าเราจะสามารถเขียนแสดง σ ในรูปผลคูณของวัฏจักรที่มีความยาว 3 ได้ โดยอาศัยคุณสมบัติของผลคูณของคู่สลับ 2 ตัว ดังต่อไปนี้

$$(ab)(ab) = (1) = (123)(132)$$
$$(ab)(ac) = (acb)$$
$$(ab)(cd) = (acb)(acd)$$

ตัวอย่างเช่น เนื่องจาก (12345) เป็นวิธีเรียงสับเปลี่ยนคู่ ดังนั้น เราเขียนแสดง (12345) ในรูปผลคูณของวัฏจักรที่มีความยาว 3 ได้เป็น

$$(12345) = (15)(14)(13)(12)$$
$$= (145)(123)$$ เป็นต้น

ถ้า σ เป็นวิธีเรียงสับเปลี่ยนซึ่งเขียนอยู่ในรูปวัฏจักรที่มีความยาว r จะได้ว่าขนาดของ σ เท่ากับ r และถ้า σ เป็นวิธีเรียงสับเปลี่ยนที่ไม่อาจเขียนแสดงในรูปวัฏจักรเพียงวัฏจักรเดียวได้ นั่นคือ σ ต้องถูกเขียนแสดงในรูปผลคูณของวัฏจักรต่างสมาชิก เช่น $\sigma = (i_1\, i_2 \ldots\, i_r)(j_1\, j_2 \ldots\, j_s)$ จะได้ว่าขนาดของ σ เท่ากับ ค.ร.น. (r, s)

ตัวอย่างเช่น ขนาดของ (12345) = 5 และขนาดของ (123)(45) = 6 เป็นต้น

ในการศึกษาเกี่ยวกับกลุ่ม เราพบว่าทฤษฎีบทเคย์เลย์มีความสำคัญมาก เพราะทฤษฎีบทนี้อาจถือได้ว่าเป็นตัวอย่างหนึ่งของสิ่งที่เราเรียกว่า **"ทฤษฎีบทตัวแทน"** (representation theorem) ซึ่งเนื้อความของทฤษฎีบทคือ "กลุ่ม G ใด ๆ ถอดแบบกันกับกลุ่มย่อยของ S_G เสมอ" ดังนั้นทฤษฎีบทนี้จึงช่วยให้เราสามารถ "แทน" กลุ่มใดๆ ที่เรามีอยู่ด้วยกลุ่มย่อยของกลุ่มสมมาตรบนกลุ่มนั้น ซึ่งทำให้ความเป็น "นามธรรม" ทั้งหลายเปลี่ยนแปลงเป็น "รูปธรรม" ได้

ตัวอย่าง จงหากลุ่มย่อยของ S_4 ที่ถอดแบบกันกับ Klein 4 – group ดังตารางข้างล่างนี้

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

<u>วิธีทำ</u> ให้ $a_1 = e$, $a_2 = a$, $a_3 = b$ และ $a_4 = c$

ดังนั้น กลุ่มย่อยของ S_4 ที่ถอดแบบกันกับ Klein 4 – group จะประกอบด้วยสมาชิก 4 ตัวคือ φ_e, φ_a, φ_b และ φ_c โดยที่สมาชิกแต่ละตัวหาได้ดังนี้

$$\varphi_e = \varphi_{a_1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1a_1 & a_1a_2 & a_1a_3 & a_1a_4 \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_2 & a_3 & a_4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

โดยลบ a ออกเหลือไว้แต่ดรรชนีล่าง

$$= (1)$$

$$\varphi_a = \varphi_{a_2} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2a_1 & a_2a_2 & a_2a_3 & a_2a_4 \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_1 & a_4 & a_3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$= (12)(34)$$

$$\varphi_b = \varphi_{a_3} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3a_1 & a_3a_2 & a_3a_3 & a_3a_4 \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (13)(24)$$

$$\varphi_c = \varphi_{a_4} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4a_1 & a_4a_2 & a_4a_3 & a_4a_4 \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_3 & a_2 & a_1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (14)(23)$$

นั่นคือ Klein 4 – group ถอดแบบกันกับกลุ่ม {(1), (12)(34), (13)(24), (14)(23)} ซึ่งเป็นกลุ่มย่อยของ S_4

5. ผลคูณตรงของกลุ่มสองกลุ่ม

ถ้า G และ H เป็นกลุ่ม เราจะได้ว่า $G\times H$ ซึ่งเป็นผลคูณคาร์ทีเซียนของ G และ H เป็นกลุ่มภายใต้การดำเนินการทวิภาคโดย

$$(g, h) * (g', h') = (gg', hh')$$

สำหรับทุก ๆ $g, g' \in G$ และ $h, h' \in H$

จะสังเกตเห็นว่าในการนิยาม $*$ นั้น เราใช้การดำเนินการทวิภาคทั้งหมดสามแบบด้วยกัน คือ นอกจากการดำเนินการ $*$ แล้ว ในการสร้าง gg' เราใช้การดำเนินการของ G แต่สำหรับ hh' เราใช้การดำเนินการของ H

เราเรียกกลุ่ม $G\times H$ นี้ว่า "**ผลคูณตรง**" (direct product) ของกลุ่ม G และ H โดยมี (e_G, e_H) เป็นเอกลักษณ์ของ $G\times H$ เมื่อ e_G และ e_H เป็นเอกลักษณ์ของกลุ่ม G และ H ตามลำดับ ส่วนตัวผกผันของ (g, h) ก็คือ (g^{-1}, h^{-1}) เมื่อ g^{-1} และ h^{-1} เป็นตัวผกผันของ g และ h ตามลำดับ

ถ้าทั้ง G และ H เป็นกลุ่มจำกัด จะได้ว่า $G\times H$ เป็นกลุ่มจำกัดด้วย โดยที่ขนาดของกลุ่ม $G\times H$ = (ขนาดของกลุ่ม G) $\times$ (ขนาดของกลุ่ม H)

ตัวอย่างเช่น ถ้า $G = \mathbb{Z}_5$ และ $H = \mathbb{Z}_3$ เราจะได้ว่า $\mathbb{Z}_5\times\mathbb{Z}_3$ เป็นกลุ่มจำกัดที่มีขนาดเท่ากับ 15 และมี $(\bar{0},\bar{0})$ เป็นเอกลักษณ์

เมื่อลองพิจารณาสมาชิก $(\bar{2},\bar{2})$ ใน $\mathbb{Z}_5\times\mathbb{Z}_3$ พบว่า

ตัวผกผันของ $(\bar{2},\bar{2})$ คือ $(\bar{3},\bar{1})$

ขนาดของ $(\bar{2},\bar{2})$ เท่ากับ 15 ดังนั้น จึงได้ว่า $(\bar{2},\bar{2})$ เป็นตัวก่อกำเนิดของ $\mathbb{Z}_5\times\mathbb{Z}_3$

เราพบว่าโดยปรกติ ถึงแม้ว่าทั้ง $\mathbb{Z}_m$ และ $\mathbb{Z}_n$ จะเป็นกลุ่มวัฏจักร กลุ่ม $\mathbb{Z}_m\times\mathbb{Z}_n$ ก็ไม่เป็นกลุ่มวัฏจักรเสมอไป แต่ $\mathbb{Z}_m\times\mathbb{Z}_n$ จะเป็นกลุ่มวัฏจักรเมื่อ ห.ร.ม. $(m, n) = 1$

ถ้า $G = \mathbb{Z}_4$ และ $H = U_3 = \{\bar{1},\bar{2}\}$ ดังนั้นเราจะได้ $\mathbb{Z}_4\times U_3$ เป็นกลุ่มจำกัดที่มีขนาดเท่ากับ 8 และมี $(\bar{0},\bar{1})$ เป็นเอกลักษณ์

เมื่อลองพิจารณาสมาชิก $(\bar{1},\bar{2})$ ใน $\mathbb{Z}_4\times U_3$ พบว่า

ตัวผกผันของ $(\bar{1},\bar{2})$ คือ $(\bar{3},\bar{2})$

ขนาดของ $(\bar{1},\bar{2})$ เท่ากับ 4 ดังนั้น $(\bar{1},\bar{2})$ ไม่เป็นตัวก่อกำเนิดของ $\mathbb{Z}_4\times U_3$ ถึงแม้ว่า $\bar{1}$ จะเป็นตัวก่อกำเนิดของ $\mathbb{Z}_4$ และ $\bar{2}$ เป็นตัวก่อกำเนิดของ U_3 ก็ตาม

ในโปรแกรมช่วยสอนนี้ เราจะให้ความสนใจผลคูณตรงของกลุ่ม $\mathbb{Z}_m$ และ $\mathbb{Z}_n$ **หรือ** $\mathbb{Z}_m$ และ U_n **หรือ** U_m และ U_n เป็นต้น

แบบทดสอบความรู้

แบบทดสอบความรู้เกี่ยวกับกลุ่ม $\mathbb{Z}$

แบบทดสอบความรู้เกี่ยวกับกลุ่ม $\mathbb{Z}$ ประกอบด้วยคำถาม 6 ข้อ ซึ่งเกี่ยวกับการหาค่าห.ร.ม., การเขียนห.ร.ม.ให้อยู่ในรูปการรวมเชิงเส้น, การหาค.ร.น., การหากลุ่มย่อยของ $\mathbb{Z}$ ซึ่งก่อกำเนิดโดยสมาชิก 1 ตัว, 2 ตัว และ 3 ตัว

หลังจากทำแบบทดสอบเสร็จผู้ใช้สามารถที่จะเลือก **พิมพ์ผลการทำแบบทดสอบออกทางเครื่องพิมพ์** หรือ **บันทึกผลการทำแบบทดสอบลงบนแฟ้มข้อมูล** เพื่อที่จะสามารถนำมาพิมพ์ออกทางเครื่องพิมพ์ภายหลัง

แบบทดสอบความรู้เกี่ยวกับกลุ่ม $\mathbb{Z}_n$

แบบทดสอบความรู้เกี่ยวกับกลุ่ม $\mathbb{Z}_n$ ประกอบด้วยคำถาม 9 **ข้อ** ซึ่งเกี่ยวกับการหาสมาชิก, ตัวผกผัน, ตัวก่อกำเนิด, ขนาด และ กลุ่มย่อยซึ่งก่อกำเนิดโดยสมาชิก 1 ตัว รวมทั้งการหาโคเซต, สมาชิกในโคเซต, ดรรชนี และ ตัวก่อกำเนิดของกลุ่มผลหารของกลุ่ม $\mathbb{Z}_n$

กลุ่ม $\mathbb{Z}_n$ ที่ใช้ในแบบทดสอบจะถูกเลือกโดยการสุ่มระหว่างกลุ่ม $\mathbb{Z}_3$ จนถึง $\mathbb{Z}_{50}$

หลังจากทำแบบทดสอบเสร็จผู้ใช้สามารถที่จะเลือก **พิมพ์ผลการทำแบบทดสอบออกทางเครื่องพิมพ์** หรือ **บันทึกผลการทำแบบทดสอบลงบนแฟ้มข้อมูล** เพื่อที่จะสามารถนำมาพิมพ์ออกทางเครื่องพิมพ์ภายหลัง

แบบทดสอบความรู้เกี่ยวกับกลุ่มU_n

แบบทดสอบความรู้เกี่ยวกับกลุ่ม U_n ประกอบด้วยคำถาม 5 ข้อ ซึ่งเกี่ยวกับการหาสมาชิก, ตัวผกผัน, ตัวก่อกำเนิด, ขนาด และ กลุ่มย่อยซึ่งก่อกำเนิดโดยสมาชิก 1 ตัว

กลุ่ม U_n ที่ใช้ในแบบทดสอบจะถูกเลือกโดยการสุ่มระหว่างกลุ่ม U_3 จนถึง U_{50}

หลังจากทำแบบทดสอบเสร็จผู้ใช้สามารถที่จะเลือก **พิมพ์ผลการทำแบบทดสอบออกทางเครื่องพิมพ์** หรือ **บันทึกผลการทำแบบทดสอบลงบนแฟ้มข้อมูล** เพื่อที่จะสามารถนำมาพิมพ์ออกทางเครื่องพิมพ์ภายหลัง

แบบทดสอบความรู้เกี่ยวกับกลุ่ม S_n

แบบทดสอบความรู้เกี่ยวกับกลุ่ม S_n ประกอบด้วยคำถาม 17 ข้อ (16 ข้อสำหรับกรณี $n = 2$ หรือ 3) ซึ่งเกี่ยวกับการเขียนวิธีเรียงสับเปลี่ยนให้อยู่ในรูปวัฏจักร, การหาผลคูณทั้งในรูปวิธีเรียงสับเปลี่ยนและวัฏจักร, การเขียนวัฏจักรให้อยู่ในรูปของผลคูณของคู่สลับ, การเขียนวัฏจักรให้อยู่ในรูปผลคูณของวัฏจักรที่มีความยาว 3, การหากลุ่มย่อยซึ่งก่อกำเนิดโดยวัฏจักรเดี่ยวและผลคูณของวัฏจักรเดี่ยว, การหาขนาดของวิธีเรียงสับเปลี่ยนและวัฏจักร รวมทั้งเมื่อกำหนด**ตารางเคย์เลย์**มาให้จะต้องหากลุ่มย่อยของ S_n ที่สมสัณฐานกับกลุ่มซึ่งมีการดำเนินการสอดคล้องตามตารางเคย์เลย์ที่กำหนดให้ และโดยทฤษฎีบทของเคย์เลย์จะต้องหาค่าของ n ที่กลุ่มย่อยของ S_n สมสัณฐานกับกลุ่มต่อไปนี้ตามลำดับ Z_m U_p และ D_q

กลุ่ม S_n ที่ใช้ในแบบทดสอบจะถูกเลือกโดยการสุ่มระหว่างกลุ่ม S_2 จนถึง S_9

หลังจากทำแบบทดสอบเสร็จผู้ใช้สามารถที่จะเลือก **พิมพ์ผลการทำแบบทดสอบออกทางเครื่องพิมพ์** หรือ **บันทึกผลการทำแบบทดสอบลงบนแฟ้มข้อมูล** เพื่อที่จะสามารถนำมาพิมพ์ออกทางเครื่องพิมพ์ภายหลัง

แบบทดสอบความรู้เกี่ยวกับกลุ่มผลคูณตรง

แบบทดสอบความรู้เกี่ยวกับกลุ่มผลคูณตรง ประกอบด้วยคำถาม 24 ข้อ ซึ่งเกี่ยวกับการหาสมาชิก, ตัวผกผัน, ตัวก่อกำเนิด, ขนาด, กลุ่มย่อยซึ่งก่อกำเนิดโดยสมาชิก 1 ตัว คือ <(a,b)> และ กลุ่มย่อย <a>x<b> ของกลุ่มผลคูณตรง Z_mxZ_n , Z_mxU_n , U_mxZ_n และ U_mxU_n

กลุ่ม Z_n และ U_n ที่ใช้ในแบบทดสอบจะถูกเลือกโดยการสุ่มระหว่างกลุ่ม Z_2 จนถึง Z_{21} และ U_2 จนถึง U_{21} ตามลำดับ

หลังจากทำแบบทดสอบเสร็จผู้ใช้สามารถที่จะเลือก **พิมพ์ผลการทำแบบทดสอบออกทางเครื่องพิมพ์** หรือ **บันทึกผลการทำแบบทดสอบลงบนแฟ้มข้อมูล** เพื่อที่จะสามารถนำมาพิมพ์ออกทางเครื่องพิมพ์ภายหลัง

โปรแกรมช่วยคำนวณ

โปรแกรมช่วยคำนวณเกี่ยวกับกลุ่ม $(\mathbb{Z}, +)$

โปรแกรมช่วยคำนวณเกี่ยวกับกลุ่ม $\mathbb{Z}$ อนุญาตให้ผู้ใช้ใส่ค่าต่างๆ เพื่อที่โปรแกรมจะช่วยคำนวณสิ่งต่อไปนี้ได้

ห.ร.ม.และเขียนห.ร.ม.ให้อยู่ในรูปการรวมเชิงเส้น ให้ผู้ใช้ใส่จำนวนเต็ม 2 ค่า คือ a และ b ที่มีค่ามากกว่า 0

ค.ร.น. ให้ผู้ใช้ใส่จำนวนเต็ม 2 ค่า คือ a และ b ที่มีค่ามากกว่า 0

กลุ่มย่อยซึ่งก่อกำเนิดโดย a หรือ $\langle a \rangle$ ให้ผู้ใช้ใส่ค่าของจำนวนเต็มใดๆ 1 จำนวน

กลุ่มย่อยซึ่งก่อกำเนิดโดย a และ b หรือ $\langle a,b \rangle$ ให้ผู้ใช้ใส่ค่าของจำนวนเต็มใดๆ 2 จำนวน

กลุ่มย่อยซึ่งก่อกำเนิดโดย a, b และ c หรือ $\langle a,b,c \rangle$ ให้ผู้ใช้ใส่ค่าของจำนวนเต็มใดๆ 3 จำนวน

โปรแกรมช่วยคำนวณเกี่ยวกับกลุ่ม $(\mathbb{Z}_n, +)$

โปรแกรมช่วยคำนวณเกี่ยวกับกลุ่ม $\mathbb{Z}_n$ อนุญาตให้ผู้ใช้ใส่ค่าต่างๆ เพื่อที่โปรแกรมจะช่วยคำนวณสิ่งต่อไปนี้ได้

สมาชิกใน $\mathbb{Z}_n$ ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม n ที่มีค่าตั้งแต่ 2 ถึง 200

ตัวผกผันของ a **ใน** $\mathbb{Z}_n$ ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม n ที่มีค่าตั้งแต่ 2 ถึง 200 และจำนวนเต็ม a ที่มีค่าตั้งแต่ 1 ถึง n-1

ตัวก่อกำเนิดของ $\mathbb{Z}_n$ ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม n ที่มีค่าตั้งแต่ 2 ถึง 200

ขนาดของ a **ใน** $\mathbb{Z}_n$ ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม n ที่มีค่าตั้งแต่ 2 ถึง 200 และจำนวนเต็ม a ที่มีค่าตั้งแต่ 1 ถึง n-1

กลุ่มย่อยใน $\mathbb{Z}_n$ **ซึ่งก่อกำเนิดโดย** a ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม n ที่มีค่าตั้งแต่ 2 ถึง 200 และจำนวนเต็ม a ที่มีค่าตั้งแต่ 1 ถึง n-1

โคเซต ดรรชนี และตัวก่อกำเนิด ซึ่งกำหนดโดยกลุ่มย่อย $\langle a \rangle$ **ของ** $\mathbb{Z}_n$ ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม n ที่มีค่าตั้งแต่ 2 ถึง 200 และจำนวนเต็ม a ที่มีค่าตั้งแต่ 1 ถึง n-1

โปรแกรมช่วยคำนวณเกี่ยวกับกลุ่ม $(U_n, \cdot)$

โปรแกรมช่วยคำนวณเกี่ยวกับกลุ่ม U_n อนุญาตให้ผู้ใช้ใส่ค่าต่างๆ เพื่อที่โปรแกรมจะช่วยคำนวณสิ่งต่อไปนี้ได้

สมาชิกใน U_n ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม n ที่มีค่าตั้งแต่ 2 ถึง 200

ตัวผกผันของ a ใน U_n ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม n ที่มีค่าตั้งแต่ 2 ถึง 200 และจำนวนเต็ม a โดยที่ ห.ร.ม.ของ a และ n มีค่าเป็น 1 ($\gcd(a, n) = 1$)

ตัวก่อกำเนิดของ U_n ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม n ที่มีค่าตั้งแต่ 2 ถึง 200

ขนาดของ a ใน U_n ให้ผู้ใช้ใส่ค่าจำนวนเต็ม n ที่มีค่าตั้งแต่ 2 ถึง 200 และจำนวนเต็ม a โดยที่ ห.ร.ม.ของ a และ n มีค่าเป็น 1 ($\gcd(a, n) = 1$)

กลุ่มย่อยใน U_n ซึ่งก่อกำเนิดโดย a ให้ผู้ใช้ใส่ค่าจำนวนเต็ม n ที่มีค่าตั้งแต่ 2 ถึง 200 และจำนวนเต็ม a โดยที่ ห.ร.ม.ของ a และ n มีค่าเป็น 1 ($\gcd(a, n) = 1$)

โปรแกรมช่วยคำนวณเกี่ยวกับกลุ่ม $(S_n, \circ)$

โปรแกรมช่วยคำนวณเกี่ยวกับกลุ่ม S_n อนุญาตให้ผู้ใช้ใส่ค่าต่างๆ เพื่อที่โปรแกรมจะช่วยคำนวณสิ่งต่อไปนี้ได้

สมาชิกใน S_n ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม n ที่มีค่าตั้งแต่ 2 ถึง 5

เขียนวัฏจักรให้อยู่ในรูปวิธีเรียงสับเปลี่ยน หรือ เขียนวิธีเรียงสับเปลี่ยนให้อยู่ในรูปวัฏจักร ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม n ที่มีค่าตั้งแต่ 2 ถึง 9

หาผลคูณของวัฏจักรหรือวิธีเรียงสับเปลี่ยน ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม n ที่มีค่าตั้งแต่ 2 ถึง 9

หากลุ่มย่อยซึ่งก่อกำเนิดโดยวัฏจักรใน S_n ให้ผู้ใช้ใส่ค่าจำนวนเต็ม n ที่มีค่าตั้งแต่ 2 ถึง 9 และวัฏจักรซึ่งเป็นสมาชิกใน S_n นั้น

หาขนาดของวัฏจักรหรือวิธีเรียงสับเปลี่ยน ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม n ที่มีค่าตั้งแต่ 2 ถึง 9

โปรแกรมช่วยคำนวณเกี่ยวกับกลุ่มผลคูณตรงของกลุ่มสองกลุ่ม

โปรแกรมช่วยคำนวณเกี่ยวกับกลุ่ม **ผลคูณตรงของกลุ่มสองกลุ่ม** ซึ่งในที่นี้จะมี 4 กลุ่มได้แก่

1. กลุ่ม $Z_m \times Z_n$
2. กลุ่ม $Z_m \times U_n$
3. กลุ่ม $U_m \times Z_n$
4. กลุ่ม $U_m \times U_n$

โปรแกรมช่วยคำนวณจะอนุญาตให้ผู้ใช้ใส่ค่าต่างๆ เพื่อที่โปรแกรมจะช่วยคำนวณสิ่งต่อไปนี้ได้

กลุ่ม $Z_m \times Z_n$

สมาชิก ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม m และ n ที่มีค่าตั้งแต่ 1 ถึง 10

ตัวผกผัน ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม m และ n ที่มีค่าตั้งแต่ 1 ถึง 100 และคู่อันดับซึ่งเป็นสมาชิกของ $Z_m \times Z_n$

ตัวก่อกำเนิด ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม m และ n ที่มีค่าตั้งแต่ 1 ถึง 10

ขนาด ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม m และ n ที่มีค่าตั้งแต่ 1 ถึง 100 และคู่อันดับซึ่งเป็นสมาชิกของ $Z_m \times Z_n$

กลุ่มย่อยซึ่งก่อกำเนิดโดย (a, b) หรือ $<(a, b)>$ ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม m และ n ที่มีค่าตั้งแต่ 1 ถึง 20 และคู่อันดับซึ่งเป็นสมาชิกของ $Z_m \times Z_n$

กลุ่ม $<a>\times<b>$ ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม m และ n ที่มีค่าตั้งแต่ 1 ถึง 20 โดยที่จำนวนเต็ม a มีค่าตั้งแต่ 0 ถึง $m-1$ และจำนวนเต็ม b มีค่าตั้งแต่ 0 ถึง $n-1$

$Z_m \times U_n$

สมาชิก ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม m ที่มีค่าตั้งแต่ 1 ถึง 10 และจำนวนเต็ม n ที่มีค่าตั้งแต่ 2 ถึง 13

ตัวผกผัน ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม m ที่มีค่าตั้งแต่ 1 ถึง 100 และจำนวนเต็ม n ที่มีค่าตั้งแต่ 2 ถึง 100 และคู่อันดับซึ่งเป็นสมาชิกของ $Z_m \times U_n$

ตัวก่อกำเนิด ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม m ที่มีค่าตั้งแต่ 1 ถึง 10 และ n ที่มีค่าตั้งแต่ 2 ถึง 13

ขนาด ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม m ที่มีค่าตั้งแต่ 1 ถึง 100 และจำนวนเต็ม n ที่มีค่าตั้งแต่ 2 ถึง 100 และคู่อันดับซึ่งเป็นสมาชิกของ $Z_m \times U_n$

กลุ่มย่อยซึ่งก่อกำเนิดโดย (a, b) หรือ $<(a, b)>$ ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม m ที่มีค่าตั้งแต่ 1 ถึง 20 และจำนวนเต็ม n ที่มีค่าตั้งแต่ 2 ถึง 23 และคู่อันดับซึ่งเป็นสมาชิกของ $Z_m \times U_n$

เซต $<a>\times<b>$ ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม m ที่มีค่าตั้งแต่ 1 ถึง 20 และจำนวนเต็ม n ที่มีค่าตั้งแต่ 2 ถึง 23 โดยที่จำนวนเต็ม a มีค่าตั้งแต่ 0 ถึง $m-1$ และจำนวนเต็ม b เป็นจำนวนที่ห.ร.ม.ของ b และ n มีค่าเป็น 1 ($\gcd(b,n) = 1$)

$U_m \times Z_n$

สมาชิก ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม m ที่มีค่า**ตั้งแต่** 2 **ถึง** 13 และจำนวนเต็ม n ที่มีค่า**ตั้งแต่** 1 **ถึง** 20

ตัวผกผัน ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม m ที่มีค่า**ตั้งแต่** 2 **ถึง** 100 และจำนวนเต็ม n ที่มีค่า**ตั้งแต่** 1 **ถึง** 100 และคู่อันดับซึ่งเป็นสมาชิกของ $U_m \times Z_n$

ตัวก่อกำเนิด ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม m ที่มีค่า**ตั้งแต่** 2 **ถึง** 13 และจำนวนเต็ม n ที่มีค่าตั้งแต่ 1 ถึง 10

ขนาด ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม m ที่มีค่า**ตั้งแต่** 2 **ถึง** 100 และจำนวนเต็ม n ที่มีค่า**ตั้งแต่** 1 **ถึง** 100 และคู่อันดับซึ่งเป็นสมาชิกของ $U_m \times Z_n$

กลุ่มย่อยซึ่งก่อกำเนิดโดย (a, b) **หรือ** $\langle (a, b) \rangle$ ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม m ที่มีค่า**ตั้งแต่** 2 **ถึง** 23 และจำนวนเต็ม n ที่มีค่า**ตั้งแต่** 1 **ถึง** 20 และคู่อันดับซึ่งเป็นสมาชิกของ $U_m \times Z_n$

กลุ่ม $\langle a \rangle \times \langle b \rangle$ ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม m ที่มีค่า**ตั้งแต่** 2 **ถึง** 23 และจำนวนเต็ม n ที่มีค่า**ตั้งแต่** 1 **ถึง** 20 โดยที่จำนวนเต็ม a เป็นจำนวนที่ห.ร.ม.ของ a และ m มีค่าเป็น 1 ($\gcd(a,m) = 1$) และจำนวนเต็ม b มีค่าตั้งแต่ 0 ถึง $n-1$

$U_m \times U_n$

สมาชิก ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม m และ n ที่มีค่า**ตั้งแต่** 2 **ถึง** 13

ตัวผกผัน ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม m และ n ที่มีค่า**ตั้งแต่** 2 **ถึง** 100 และคู่อันดับซึ่งเป็นสมาชิกของ $U_m \times U_n$

ตัวก่อกำเนิด ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม m และ n ที่มีค่า**ตั้งแต่** 2 **ถึง** 13

ขนาด ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม m และ n ที่มีค่า**ตั้งแต่** 2 **ถึง** 100 และคู่อันดับซึ่งเป็นสมาชิกของ $U_m \times U_n$

กลุ่มย่อยซึ่งก่อกำเนิดโดย (a, b) **หรือ** $\langle (a, b) \rangle$ ให้ผู้ใช้ใส่ค่าของจำนวนเต็ม m และ n ที่มีค่า**ตั้งแต่** 2 **ถึง** 23 และคู่อันดับซึ่งเป็นสมาชิกของ $U_m \times U_n$

เซต $\langle a \rangle \times \langle b \rangle$ ให้ผู้ใช้ใส่ค่าจำนวนเต็ม m และ n ที่มีค่า**ตั้งแต่** 2 **ถึง** 23 โดยที่จำนวนเต็ม a เป็นจำนวนที่ห.ร.ม.ของ a และ m มีค่าเป็น 1 ($\gcd(a,m) = 1$) และจำนวนเต็ม b เป็นจำนวนที่ห.ร.ม.ของ b และ n มีค่าเป็น 1 ($\gcd(b,n) = 1$)