บทที่ 1
ความรู้เบื้องต้น

พีชคณิตนามธรรมเป็นคณิตศาสตร์แขนงหนึ่งที่ถูกสร้างขึ้นโดยมีวัตถุประสงค์หลักเพื่อขยายแนวความคิดการแก้ปัญหาเชิงพีชคณิตให้ครอบคลุม ซึ่งนักคณิตศาสตร์จากทั่วโลกช่วยกันพัฒนาจนสามารถนำมาใช้ได้อย่างหลากหลาย เช่น พีชคณิตบูลีน โครงสร้างที่สมมาตรของโมเลกุลในทางเคมี ทฤษฎีรหัส เป็นต้น เนื้อหาพีชคณิตนามธรรมมีความซับซ้อน และมีความเป็นนามธรรมสูง ก่อนศึกษาจำเป็นต้องมีความรู้พื้นฐานหลายเรื่อง โดยเฉพาะตัวอย่างต่าง ๆ ที่จะใช้ประกอบคำอธิบายมีความเฉพาะตัว เช่น เซตของคลาสสมมูลของจำนวนเต็มในทฤษฎีจำนวน เป็นต้น สำหรับความรู้เบื้องต้นของตำราเล่มนี้จะขอกล่าวถึงบางส่วนในเรื่อง เซต ความสัมพันธ์สมมูล ฟังก์ชัน และจำนวนเต็ม ซึ่งจะแนะนำนิยาม และทฤษฎีบทที่จะใช้ประกอบคำอธิบายทั้งหมด ดังนี้

เซต ความสัมพันธ์สมมูล และฟังก์ชัน

เซต (set) เป็นคณิตศาสตร์แขนงหนึ่งที่มีมานานแล้วหลายร้อยปี ใช้อธิบายคณิตศาสตร์แขนงอื่นให้มีความรัดกุม กระชับ และมีเหตุผลที่ชัดเจนมากขึ้น ในช่วงแรกความรู้เรื่องเซตไม่ค่อยเป็นระบบและไม่มีทฤษฎีที่ชัดเจนทำให้ยากต่อการขยายแนวคิด ต่อมาช่วงปลายทศวรรษที่ 19 นักคณิตศาสตร์ชาวเยอรมันชื่อ คันเตอร์ เกออร์จ (Cantor Georg) ได้จัดเนื้อหาเรื่องเซตให้เป็นระบบและเขียนทฤษฎีที่ชัดเจน อย่างที่เห็นในปัจจุบัน เซตเป็นคำอนิยาม (undefined) ใช้แทนกลุ่มสิ่งของต่าง ๆ เช่น นก 1 ฝูง นักฟุตบอล 1 ทีม ช้าง 1 โขลง เป็นต้น แต่ในทางคณิตศาสตร์นั้นจะแทนด้วย นก 1 เซต ช้าง 1 เซต นักฟุตบอล 1 เซต เซตจะไม่ใช้กับสิ่งของที่บอกคุณภาพ เช่น เซตของคนสวย เซตของคนดี เรานิยมใช้อักษรตัวพิมพ์ใหญ่ เช่น $A\ B\ C\ \ldots$ แทนชื่อเซต เรียกสิ่งที่อยู่ภายในเซตว่าสมาชิกของเซต ใช้สัญลักษณ์ $\in$ หมายถึง การเป็นสมาชิก และ $\notin$ หมายถึง การไม่เป็นสมาชิก เช่น $a \in B$ หมายถึง a เป็นสมาชิกในเซต B และ $b \notin C$ หมายถึง b ไม่ได้เป็นสมาชิกในเซต C เป็นต้น ส่วนใหญ่มักแบ่งการเขียนเซตออกเป็น 3 รูปแบบใหญ่ ๆ คือ (จักรินทร์ วรรณโพธิ์กลาง, 2551: 5)

1. การเขียนแบบแจกแจงสมาชิก (set tabular form) ทำให้สามารถมองเห็นชัดเจนว่าภายในเซต ๆ นั้นประกอบด้วยสมาชิกตัวใดบ้าง เช่น A เป็นเซตของจำนวนเต็มบวก สามารถเขียน A ในรูปแบบแจกแจงสมาชิก คือ $A = \{1, 2, 3, \ldots\}$ เป็นต้น

2. การเขียนแบบบอกเงื่อนไขของสมาชิก (set builder form) มีไว้สำหรับเขียนในกรณีที่เขียนแจกแจงสมาชิกได้ยากหรือมีคุณสมบัติบางอย่างเฉพาะเจาะจง เช่น เซต A เป็นเซตของจำนวนจริงที่มีค่าอยู่ระหว่าง 1 และ 2 ซึ่งสามารถเขียนแบบบอกเงื่อนไขได้เป็น

$$A = \{x \in \mathbb{R} \mid 1 < x < 2\}$$

นอกจากนี้ยังสามารถเขียนเซตคำตอบของสมการได้อีกด้วย เช่น

$$B = \{x \in \mathbb{R} \mid x^2 + 2x + 1 = 0\}$$

3. การเขียนเซตด้วยแผนภาพเวนน์ – ออยเลอร์ (Venn-Euler Diagram) เป็นแผนภาพที่เขียนแทนเซตรวมถึงแสดงความสัมพันธ์ระหว่างเซต นับว่าเป็นวิธีที่ง่ายต่อความเข้าใจและสามารถ

มองภาพชัดเจนขึ้นซึ่งออยเลอร์ เลออนฮาร์ด (Euler Leonhard) นักคณิตศาสตร์ชาวสวิตเซอร์แลนด์ เป็นผู้นำมาใช้ครั้งแรก หลังจากนั้น เวนน์ จอห์น (Venn John) นักคณิตศาสตร์ชาวอังกฤษได้นำมาใช้อธิบายแนวคิดต่าง ๆ ทางคณิตศาสตร์ นักคณิตศาสตร์ทั้งสองท่านนี้ เขียนแทนเซตด้วยรูปปิดใด ๆ โดยใช้รูปสี่เหลี่ยมผืนผ้าแทนเซตที่กำหนดขอบข่ายของสมาชิกของเซต และเขียนเซตอื่น ๆ ลงในรูปสี่เหลี่ยมผืนผ้า ดังภาพที่ 1.1

ภาพที่ 1.1 การเขียนเซตด้วยแผนภาพเวนน์ – ออยเลอร์
ที่มา: Henry Sharp, JR. (1968: 12)

เซตสามารถจำแนกชนิดโดยพิจารณาจากจำนวนสมาชิกของเซต ดังนี้

บทนิยาม 1.1 เซตจำกัด (finite set) คือ เซตที่ไม่มีสมาชิกหรือมีจำนวนสมาชิกเป็นจำนวนนับ (ราชบัณฑิตยสถาน, 2553: 76)

ถ้า $A = \{0, 1, 2, \ldots, 9\}$ เราสามารถบอกได้ว่า A มีจำนวนสมาชิกเท่ากับ 10 นั่นคือ A เป็นเซตจำกัด สำหรับเซตซึ่งไม่มีสมาชิก เรียกว่าเซตว่าง (empty set) แทนด้วยสัญลักษณ์ $\emptyset$ เช่น $A = \{x \in \mathbb{R} \mid x < 0\}$ จะเห็นว่าไม่มีจำนวนนับตัวใดเลยที่น้อยกว่า 0 นั่นคือ เซต A เป็นเซตว่าง ซึ่งถือว่าเป็นเซตจำกัดเช่นกัน

บทนิยาม 1.2 เซตอนันต์ (infinite set) คือ เซตที่ไม่ใช่เซตจำกัด หรือเซตที่ไม่สามารถหาจำนวนสมาชิกได้ (ราชบัณฑิตยสถาน, 2553: 96)

ถ้า $B = \{0, 1, 2, \ldots\}$ จะสังเกตว่าไม่สามารถหาจำนวนนับที่เท่ากับจำนวนสมาชิกของ B ได้จึงกล่าวได้ว่า B ไม่เป็นเซตจำกัด หรือเรียกเซต B ว่าเซตอนันต์

บทนิยาม 1.3 เอกภพสัมพัทธ์ (universe) คือ เซต $\mathcal{U}$ ซึ่งกำหนดขึ้นเพื่อระบุขอบเขตของเซตต่าง ๆ ที่จะนำมาพิจารณา โดยทุกสมาชิกของเซตต่าง ๆ เหล่านั้นจะเป็นสมาชิกของ $\mathcal{U}$ เสมอ (ราชบัณฑิตยสถาน, 2553: 173)

ข้อตกลง ถ้ากล่าวถึงเซตของจำนวนใด ๆ โดยไม่กำหนดเอกภพสัมพัทธ์ ให้ถือว่าเอกภพสัมพัทธ์ คือ เซตของจำนวนจริง และ $n(A)$ หมายถึง จำนวนสมาชิกในเซต A

เมื่อเราพิจารณาเซตสองเซตใดๆ สิ่งที่น่าสนใจ คือ สองเซตที่เราสนใจนั้นมีความสัมพันธ์กันอย่างไร ความสัมพันธ์ระหว่างเซตแบบแรก คือ เซตย่อย (subset) ซึ่ง ปุณศยา พัฒนางกูร (2555: 4-11) ได้ให้นิยามสับเซต ดังนี้

บทนิยาม 1.4 จะกล่าวว่า A เป็นสับเซตของเซต B ก็ต่อเมื่อ สมาชิกทุกตัวของเซต A เป็นสมาชิกของเซต B ใช้สัญลักษณ์ $\subset$ แทน การเป็นสับเซต และ $\not\subset$ แทน การไม่เป็นสับเซต เขียนแทนด้วยสัญลักษณ์ทางคณิตศาสตร์ได้เป็น

$$A \subset B \Leftrightarrow \forall x\,(x \in A \Rightarrow x \in B)$$

นอกจากนี้ ถ้า $A \subset B$ และ $A \neq B$ แล้วจะเรียก A ว่าเป็นสับเซตแท้ของ B ในกรณี $A = B$ จะเรียก A ว่าเป็นสับเซตไม่แท้ของ B

กรรณิกา กวักเพฑูรย์ (2542: 83) ได้เขียนทฤษฎีที่เกี่ยวข้องกับเซตย่อยดังนี้

ทฤษฎีบท 1.5 กำหนดให้ A B และ C เป็นเซตใด ๆ คุณสมบัติของสับเซต มีดังนี้

1. ถ้า A เป็นเซตจำกัดและมีสมาชิก n ตัว แล้ว A มีสับเซตทั้งหมด 2^n สับเซต
2. ถ้า $A \subseteq B$ และ $B \subseteq C$ แล้ว $A \subseteq C$

ความสัมพันธ์ระหว่างเซตแบบที่สอง คือ เซตที่เท่ากันซึ่งมีความหมายดังบทนิยามที่ 1.6

บทนิยาม 1.6 เซต A เท่ากับเซต B ก็ต่อเมื่อ ทุกสมาชิกของ A เป็นสมาชิกของ B และทุกสมาชิกของ B เป็นสมาชิกของ A ซึ่งเขียนแทนด้วยสัญลักษณ์ $A = B$ ถ้าเซต A และเซต B มีสมาชิกบางตัวแตกต่างกัน เรากล่าวว่า เซต A ไม่เท่ากับเซต B ในกรณีนี้เขียนแทนด้วยสัญลักษณ์ $A \neq B$ (Karen Kai and Rachel Elizabeth, 1970: 4)

พิจารณาเซต A และเซต B ที่กำหนดให้เป็นเซตที่เท่ากัน

$$\begin{array}{lcl} A \text{ เป็นเซตของจำนวนนับ} & \leftrightarrows & B = \{1, 2, 3, \ldots\} \\ A = \{1, -3\} & \leftrightarrows & B = \{x | x^2 + 2x - 3 = 0\} \\ A = \{1, 2, 3, 4, 5\} & \leftrightarrows & B = \{x \in \mathbb{N} | x < 6\} \end{array}$$

ความสัมพันธ์ระหว่างเซตแบบที่สาม คือ เซตที่เทียบเท่ากันซึ่งมีความหมายดังบทนิยามที่ 1.7

บทนิยาม 1.7 จะถูกกล่าวว่าเซตจำกัดสองเซตใด ๆ เป็นเซตที่เทียบเท่ากัน ก็ต่อเมื่อ ทั้งสองเซตมีจำนวนสมาชิกเท่ากัน (Karen Kai and Rachel Elizabeth, 1970: 4)

พิจารณา ถ้า $A = \{1, 2, 3\}$ และ $B = \{a, b, c\}$ เมื่อพิจารณาแล้วเราสามารถกล่าวได้ว่าเซต A เทียบเท่าเซต B เนื่องจาก $n(A) = 3 = n(B)$

บทนิยาม 1.8 เพาเวอร์เซต A คือ เซตที่มีสมาชิกที่เป็นเซตย่อยทั้งหมดของ A ใช้สัญลักษณ์ $P(A)$ แทนเพาเวอร์เซตของ A นั่นคือ $P(A) = \{x | x \subset A\}$ (Henry Sharp, JR., 1968: 12)

ข้อสังเกต กำหนดให้ A เป็นเซตใด ๆ

1. $P(A) \neq \emptyset$ 2. $\emptyset \in P(A)$ 3. $\emptyset \subset P(A)$ 4. $A \in P(A)$

นอกเหนือไปจากความสัมพันธ์ระหว่างเซตแล้ว การดำเนินการของเซตนับว่าเป็นพื้นฐานที่สำคัญ โดยการดำเนินการของเซต คือ การสร้างเซตใหม่ภายใต้การดำเนินการ สามารถจำแนกเป็นการดำเนินการต่าง ๆ ดังนิยามต่อไปนี้

บทนิยาม 1.9 ยูเนียน (Union) เซต A และเซต B คือ เซตที่ประกอบด้วยสมาชิกของ A หรือ B เขียนแทนด้วย $A \cup B = \{x \mid x \in A$ หรือ $x \in B\}$ (วิรัตน์ สุวรรณาภิชาติ, 2556: 1-2)

เมื่อพิจารณา $A \cup B$ เราสามารถเขียนเป็นแผนภาพเวนน์ – ออยเลอร์ได้ ดังภาพที่ 1.2

ภาพที่ 1.2 บริเวณแรเงาแสดง $A \cup B$ ในรูปแบบต่าง ๆ
ที่มา : Henry Sharp, JR. (1968: 12)

บทนิยาม 1.10 อินเตอร์เซคชัน (Intersection) ของเซต A และเซต B คือ เซตที่ประกอบด้วยสมาชิกทั้งหมดของเซต A และเซต B เขียนแทนด้วยสัญลักษณ์ทางคณิตศาสตร์ได้เป็น $A \cap B = \{x \mid x \in A$ และ $x \in B\}$ (Henry Sharp, JR., 1968: 13)

เมื่อพิจารณา $A \cap B$ เขียนเป็นแผนภาพเวนน์ – ออยเลอร์ ดังภาพที่ 1.3

ภาพที่ 1.3 บริเวณแรเงาแสดง $A \cap B$ ในรูปแบบต่าง ๆ
ที่มา : Henry Sharp, JR. (1968: 13)

บทนิยาม 1.11 ให้ A เป็นเซตย่อยของเอกภพสัมพัทธ์ U คอมพลีเมนต์ (Complement) ของเซต A คือ เซตที่ประกอบด้วยสมาชิกซึ่งเป็นสมาชิกของ U แต่ไม่เป็นสมาชิกของ A เขียนแทนด้วยสัญลักษณ์ทางคณิตศาสตร์ได้เป็น $A^c = \{x \mid x \in U$ และ $x \notin A\}$ (Henry Sharp, JR., 1968: 12)

เมื่อพิจารณา A^c สามารถเขียนเป็นแผนภาพเวนน์ – ออยเลอร์ ดังภาพที่ 1.4

ภาพที่ 1.4 บริเวณแรเงาแสดง A^c
ที่มา : Henry Sharp, JR. (1968: 12)

บทนิยาม 1.12 ผลต่าง (Different) ระหว่างเซต A และเซต B คือ เซตที่ประกอบด้วยสมาชิกของเซต A ซึ่งไม่เป็นสมาชิกของเซต B เขียนแทนด้วยสัญลักษณ์ทางคณิตศาสตร์ คือ $A - B = \{x \mid x \in A$ แต่ $x \notin B\}$ (Henry Sharp, JR., 1968: 12)

เมื่อพิจารณา $A - B$ สามารถเขียนเป็นแผนภาพเวนน์ – ออยเลอร์ ดังภาพที่ 1.5

ภาพที่ 1.5 บริเวณแรเงาแสดง $A - B$ ในรูปแบบต่าง ๆ
ที่มา : Henry Sharp, JR. (1968: 12)

เมื่อกำหนดให้ A B และ C เป็นเซตใด ๆ มานัส บุญยัง (2540: 141-153) เขียนทฤษฎีบทและทำการพิสูจน์พีชคณิตของเซต ซึ่งสามารถสรุปเป็นคุณสมบัติต่าง ๆ ได้ดังนี้

ตารางที่ 1.1 แสดงคุณสมบัติต่าง ๆ ภายใต้การดำเนินการของเซต

กฎนิจพล (Idempotent Laws)	1. $A \cup A = A$ 2. $A \cap A = A$
กฎการเปลี่ยนกลุ่ม (Associative Laws)	1. $(A \cup B) \cup C = A \cup (B \cup C)$ 2. $(A \cap B) \cap C = A \cap (B \cap C)$
กฎการสลับที่ (Commutative Laws)	1. $A \cup B = B \cup A$ 2. $A \cap B = B \cap A$
กฎการแจกแจง (Distributive Laws)	1. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ 2.$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
กฎเอกลักษณ์ (Identity Laws)	1. $A \cup \emptyset = A$ 2. $A \cap U = A$ 3. $A - \emptyset = A$
กฎเดอร์มอร์แกน (De Morgan's Laws)	1. $(A \cup B)^c = A^c \cap B^c$ 2. $(A \cap B)^c = A^c \cup B^c$
กฎของคอมพลีเมนต์ (Complement Laws)	1. $A^c \cup A = U$ 2. $A^c \cap A = \emptyset$ 3. $(A^c)^c = A$ 4. $U^c = \emptyset$ 5. $\emptyset^c = U$ 6. $A \cap B^c = A - B$

สิ่งหนึ่งที่เป็นพื้นฐานสำคัญในเรื่องของความสัมพันธ์ คือ คู่อันดับ การเป็นคู่อันดับคือต้องเป็นคู่และมีอันดับ จะเขียนแทนคู่อันดับในรูป (a, b) โดยที่ a เป็นสมาชิกตัวหน้า และ b เป็นสมาชิกตัวหลัง สิ่งสำคัญมากคือทั้ง a และ b จะวางสลับที่ไม่ได้ นอกจาก $a = b$ เท่านั้น กล่าวอีกนัยหนึ่ง คือ $(a, b) = (c, d)$ ก็ต่อเมื่อ $a = c$ และ $b = d$ ซึ่ง วัชรี กาญจน์กีรติ (2551: 7-9) ได้ให้นิยามที่นำไปสู่การนิยามความสัมพันธ์ ดังนี้

บทนิยาม 1.13 ผลคูณคาร์ทีเซียน (cartesian product) ของเซต A และเซต B คือ เซตของคู่อันดับ (a, b) ทั้งหมด โดยที่ a เป็นสมาชิกของเซต A และ b เป็นสมาชิกของเซต B นั่นคือ $A \times B = \{(a, b) | a \in A, b \in B\}$

ตัวอย่างที่ 1.1 กำหนดให้ $A = \{a, b, c\}$ และ $B = \{1, 2\}$ จงหา $A \times B$ และ $B \times A$

วิธีทำ เราสามารถหาคู่อันดับทั้งหมดจากการจับคู่สมาชิกของเซตตัวหน้า 1 ตัว จับกับสมาชิกทุกตัวของเซตตัวหลัง เมื่อทำครบทุกตัวของสมาชิกตัวหน้าเราจะได้คู่อันดับทั้งหมด ดังนั้น

$$A \times B = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$$
$$B \times A = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$$

จากตัวอย่างจะเห็นว่า $A \times B \neq B \times A$ หรือกล่าวอีกนัยหนึ่งว่าการคูณคาร์ทีเชียนไม่มีคุณสมบัติการสลับที่

บทนิยาม 1.14 จะกล่าวว่า r เป็นความสัมพันธ์ (relation) จาก A ไป B ก็ต่อเมื่อ r เป็นเซตย่อยของ $A \times B$ โดยมีเงื่อนไขว่า ถ้า $r \subseteq A \times B$ เรียก r ว่าความสัมพันธ์จาก A ไป B และ ถ้า $r \subseteq A \times A$ เรียก r ว่าความสัมพันธ์บนเซต A

ตัวอย่างที่ 1.2 กำหนดให้ $A = \{1, 2, 3\}$ และ $B = \{4, 6, 9\}$ จงเขียนเซตแบบแจกแจงสมาชิกของ r_1 และ r_2 ถ้า r_1 คือ ความสัมพันธ์สองเท่าจาก A ไป B และ ถ้า r_2 คือ ความสัมพันธ์กำลังสองจาก A ไป B

วิธีทำ ก่อนอื่นต้องเริ่มจากการหาสมาชิกของ $A \times B$ ทั้งหมด
นั่นคือ $A \times B = \{(1, 4), (1, 6), (1, 9), (2, 4), (2, 6), (2, 9), (3, 4), (3, 6), (3, 9)\}$
พิจารณาความสัมพันธ์ $r_1 = \{(2, 4), (3, 6)\}$ และ $r_2 = \{(2, 4), (3, 9)\}$
จะเห็นว่าสมาชิกของ r_1 และ r_2 ถูกเลือกมาจาก $A \times B$
ดังนั้น ไม่ว่าความสัมพันธ์แบบใดจาก A ไป B ก็จะเป็นเซตย่อยของ $A \times B$ เสมอ

จากนิยามของความสัมพันธ์ ถ้าความสัมพันธ์มีคุณสมบัติสะท้อน (reflexive property) สมบัติสมมาตร (symmetric property) และสมบัติถ่ายทอด (transitive property) ความสัมพันธ์ที่มีคุณสมบัติทั้งสาม เรียกว่าความสัมพันธ์สมมูล (equivalence relation) ปุณศยา พัฒนางกูร (2555: 16-17) ได้เขียนนิยาม ตัวอย่างและทฤษฎีบทที่เกี่ยวข้องกับความสัมพันธ์สมมูล ดังนี้

บทนิยาม 1.15 กำหนดให้ r เป็นความสัมพันธ์บนเซต A จะเรียก r ว่าความสัมพันธ์สมมูลบน A ก็ต่อเมื่อ r มีสมบัติ 3 ข้อ ดังนี้

1. สมบัติสะท้อน กล่าวคือ สำหรับสมาชิก a ใด ๆ ใน A จะได้ว่า $(a, a) \in r$
2. สมบัติสมมาตร กล่าวคือ สำหรับสมาชิก a และ b ใด ๆ ใน A ถ้า $(a, b) \in r$ แล้ว $(b, a) \in r$
3. สมบัติถ่ายทอด กล่าวคือ สำหรับสมาชิก a , b และ c ใด ๆ ใน A ถ้า $(a, b) \in r$ และ $(b, c) \in r$ แล้ว $(a, c) \in r$

ถ้า A เป็นเซตใด ๆ ที่ไม่ใช่เซตว่าง แล้วความสัมพันธ์ r ที่กำหนดให้ในแต่ละข้อต่อไปนี้ จะ

เป็นความสัมพันธ์สมมูลบน A เสมอ

1. $a\ r\ b$ ก็ต่อเมื่อ $a = b$ สำหรับทุก $a, b, c \in A$ นั่นคือ $r = \{(a, a)|a \in A\}$ เรียกความสัมพันธ์สมมูล r นี้ว่าความสัมพันธ์เอกลักษณ์ (identity relation)

2. กำหนดความสัมพันธ์ r บน A ดังนี้ $r = A \times A = \{(a, b)|a, b \in A\}$ เรียกความสัมพันธ์สมมูล r นี้ว่าความสัมพันธ์เอกภพ (universal relation)

ตัวอย่างที่ 1.3 กำหนดให้ $\mathbb{Z}_e$ เป็นเซตของจำนวนเต็มคู่ และกำหนดความสัมพันธ์ r บน $\mathbb{Z}$ ดังนี้ $a\ r\ b$ ก็ต่อเมื่อ $a - b \in \mathbb{Z}_e$ สำหรับทุก $a, b \in \mathbb{Z}$ จงพิจารณาว่า r เป็นความสัมพันธ์สมมูลบน $\mathbb{Z}$ หรือไม่

วิธีทำ สมมติให้ $a, b, c \in \mathbb{Z}$ พิจารณาสมบัติต่าง ๆ ดังนี้

1. สมบัติสะท้อน เนื่องจาก $a - a = 0$ และ $0 \in \mathbb{Z}_e$ ดังนั้น $a\ r\ a$
2. สมบัติสมมาตร ถ้า $a\ r\ b$ แล้ว $a - b \in \mathbb{Z}_e$ ดังนั้น $b - a = -(a - b) \in \mathbb{Z}_e$ นั่นคือ $b\ r\ a$
3. สมบัติถ่ายทอด ถ้าให้ $a\ r\ b$ และ $b\ r\ c$ แล้ว $a - b \in \mathbb{Z}_e$ และ $b - c \in \mathbb{Z}_e$ เนื่องจาก $a - c = (a - b) + (b - c)$ ดังนั้น $a - c \in \mathbb{Z}_e$ นั่นคือ $a\ r\ c$ สรุปได้ว่า r เป็นความสัมพันธ์สมมูลบน $\mathbb{Z}$

บทนิยาม 1.16 กำหนดให้ r เป็นความสัมพันธ์สมมูลบนเซต A และ $a \in A$ เรานิยามเซต $[a]$ ดังนี้

$$[a] = \{x \in A|x\ r\ a\}$$

เรียกเซต $[a]$ ว่าชั้นสมมูล (equivalence class) ของ a ใน A ที่มี a เป็นตัวแทน (representation)

จากตัวอย่างที่ 1.3 ถ้ากำหนดความสัมพันธ์ r บน $\mathbb{Z}$ โดย $a\ r\ b$ ก็ต่อเมื่อ $a - b \in \mathbb{Z}_e$ สำหรับทุก $a, b \in \mathbb{Z}$ แล้ว r เป็นความสัมพันธ์สมมูลบน $\mathbb{Z}$ และจาก $0 \in \mathbb{Z}$ จะได้ว่า

$$\begin{aligned}
[0] &= \{x \in \mathbb{Z}|x\ r\ 0\} \\
&= \{x \in \mathbb{Z}|x - 0 \in \mathbb{Z}_e\} \\
&= \{x \in \mathbb{Z}|x \in \mathbb{Z}_e\} \\
&= \mathbb{Z}_e
\end{aligned}$$

จาก 1 ไม่เป็นจำนวนเต็มคู่ นั่นคือ 1 เป็นจำนวนเต็มคี่ ดังนั้น

$$\begin{aligned}
[1] &= \{x \in \mathbb{Z}|x\ r\ 1\} \\
&= \{x \in \mathbb{Z}|x - 1 \in \mathbb{Z}_e\} \\
&= \{x \in \mathbb{Z}|x \notin \mathbb{Z}_e\} \\
&= \mathbb{Z} - \mathbb{Z}_e
\end{aligned}$$

จากตัวอย่างที่ผ่านมา แสดงให้เห็นว่าความสัมพันธ์สมมูล r แบ่งเซต $\mathbb{Z}$ ออกเป็นสองชั้นสมมูลที่แตกต่างกัน ซึ่งโดยทั่วไปแล้วความสัมพันธ์สมมูล r บนเซต A ใด ๆ สามารถแบ่งเซต A ออก

เป็นชั้นสมมูลต่าง ๆ ทฤษฎีบทต่อไปนี้จะกล่าวถึงสมบัติเบื้องต้นของชั้นสมมูล

ทฤษฎีบท 1.17 กำหนดให้ r เป็นความสัมพันธ์สมมูลบนเซต A จะได้ว่า

1. $a \in [a]$ (นั่นคือ $[a] \neq \varnothing$) สำหรับทุก $a \in A$
2. $[a] = [b]$ ก็ต่อเมื่อ $a\ r\ b$ สำหรับทุก $a, b \in A$
3. สำหรับทุก $a, b \in A$ ถ้า $[a] \neq [b]$ แล้ว $[a] \cap [b] = \varnothing$
4. $A = \bigcup_{a \in A} [a]$

บทนิยาม 1.18 กำหนดให้ A เป็นเซตใด ๆ ผลแบ่งกั้น (partition) ของเซต A หมายถึง เซต P ที่ประกอบด้วยเซตย่อย B ของ A ซึ่งมีสมบัติดังนี้

1. $\varnothing \notin P$
2. $p_1 = p_2$ หรือ $p_1 \cap p_2 = \varnothing$ สำหรับทุก $p_1, p_2 \in P$
3. $\cup\{B | B \in P\} = A$

จากบทนิยาม 1.18 สามารถกล่าวได้ว่าแต่ละสมาชิกของ A จะอยู่ในสมาชิกใดสมาชิกหนึ่งเพียงสมาชิกเดียวของ P เท่านั้น จากตัวอย่างที่ 1.3 จะได้ว่า $\{[0], [1]\}$ เป็นผลแบ่งกั้นของ $\mathbb{Z}$ นอกเหนือไปจากความสัมพันธ์สมมูลที่ถูกหยิบยกมาเป็นตัวอย่างสำคัญของพีชคณิตนามธรรมแล้วความสัมพันธ์ที่เป็นฟังก์ชันกลับสำคัญยิ่งกว่า เนื่องจากการดำเนินการทวิภาคเป็นส่วนประกอบหลักของเนื้อหาและเป็นฟังก์ชันชนิดหนึ่ง จึงหลีกเลี่ยงไม่ได้ที่จะกล่าวถึงพื้นฐานบางส่วนของฟังก์ชัน และขอกล่าวรายละเอียดของการดำเนินการทวิภาคในบทถัดไป

ถ้า r เป็นความสัมพันธ์จาก A ไปยัง B แล้วเป็นไปได้ที่สมาชิกบางตัวของ A จะสัมพันธ์กับสมาชิกหลาย ๆ ตัวของ B แต่สำหรับฟังก์ชันแล้วจะให้สัมพันธ์กับสมาชิกของ B เพียงตัวเดียวเท่านั้น วัชรี กาญจน์กีรติ (2551: 11-12) ได้เขียนนิยามต่าง ๆ ของฟังก์ชัน ดังนี้

บทนิยาม 1.19 กำหนดให้ A และ B เป็นเซตที่ไม่ใช่เซตว่าง เรียก f ว่าเป็นฟังก์ชัน (function) จาก A ไปยัง (into) B ก็ต่อเมื่อ

1. f เป็นความสัมพันธ์จาก A ไปยัง B และ
2. สำหรับแต่ละ $(a_1, b_1), (a_2, b_2) \in f$ ถ้า $a_1 = a_2$ แล้ว $b_1 = b_2$ ถ้า $(a, b) \in f$ แล้ว เรียก b ว่าภาพ (image) ของ a ภายใต้ f และเขียนแทน b ด้วย $f(a)$ นั่นคือ $b = f(a)$

ตัวอย่างที่ 1.4 กำหนดให้ $f = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = x^2\}$ และ $g = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid$

$y^2 = x^2\}$ จงพิจารณาว่าความสัมพันธ์ที่กำหนดให้เป็นฟังก์ชันหรือไม่

วิธีทำ จะแสดงว่า $f = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = x^2\}$ เป็นฟังก์ชัน
กำหนดให้ $(a_1, b_1), (a_2, b_2) \in f$
สมมติให้ $a_1 = a_2$
ดังนั้น $a_1^2 = a_2^2$
นั่นคือ $b_1 = b_2$
จึงได้ว่า f เป็นฟังก์ชัน
ต่อไปจะแสดงว่า g ไม่เป็นฟังก์ชัน
เห็นได้ชัดว่า $(1, -1)$ และ $(1, 1)$ เป็นสมาชิกของ g
ดังนั้น g ไม่เป็นฟังก์ชัน

บทนิยาม 1.20 กำหนดให้ A และ B เป็นเซตที่ไม่ใช่เซตว่าง f เป็นฟังก์ชันจากเซต A ไปยังเซต B

1. โดเมน (domain) ของฟังก์ชัน f คือ เซตของสมาชิกตัวแรกของคู่อันดับทั้งหมดที่มีสมาชิกของ f เขียนแทนด้วย D_f นั่นคือ

$$D_f = \{a \mid (a, b) \in f \text{ สำหรับบาง } b \in B\}$$

2. เรนจ์ (range) ของฟังก์ชัน f คือ เซตของสมาชิกตัวหลังของคู่อันดับของคู่อันดับทั้งหมดที่มีสมาชิกของ f เขียนแทนด้วย R_f นั่นคือ

$$R_f = \{b \mid (a, b) \in f \text{ สำหรับบาง } a \in A\}$$

จากตัวอย่างที่ 1.4 จะได้ว่า $D_f = \mathbb{R}$ และ $R_f = [0, \infty)$

บทนิยาม 1.21 กำหนดให้ A และ B เป็นเซตที่ไม่ใช่เซตว่าง และ f เป็นฟังก์ชันจากเซต A ไปยังเซต B ถ้า $D_f = A$ แล้วจะเขียนแทนข้อความที่ว่า “f เป็นฟังก์ชันจาก A ไปยัง (into) B ด้วยสัญลักษณ์ $f : A \longrightarrow B$”

จากบทนิยามของฟังก์ชันจะเห็นว่าฟังก์ชันเป็นเซต ดังนั้น การเท่ากันของฟังก์ชันก็คือการ

เท่ากันของเซตนั่นเอง ดังบทนิยามต่อไปนี้

บทนิยาม 1.22 กำหนดให้ f และ g เป็นฟังก์ชันใด ๆ จะกล่าวว่าฟังก์ชัน f เท่ากับฟังก์ชัน g ซึ่งเขียนแทนด้วยสัญลักษณ์ $f = g$ ก็ต่อเมื่อ

1. $D_f = D_g$ และ
2. $f(x) = g(x)$ สำหรับทุก $x \in D_f \cap D_g$

ต่อไปจะนิยามผลบวก ผลลบ ผลคูณ และผลหารของฟังก์ชัน f และ g ดังนี้

บทนิยาม 1.23 กำหนดให้ f และ g เป็นฟังก์ชันใด ๆ

1. $(f+g)(x) = f(x) + g(x)$ สำหรับทุก $x \in D_f \cap D_g$
2. $(f-g)(x) = f(x) - f(x)$ สำหรับทุก $x \in D_f \cap D_g$
3. $(f \cdot g)(x) = f(x) \cdot g(x)$ สำหรับทุก $x \in D_f \cap D_g$
4. $\left(\dfrac{f}{g}\right)(x) = \dfrac{f(x)}{g(x)}$ สำหรับทุก $x \in D_f \cap D_g - \{x \in D_g | g(x) = 0\}$

ตัวอย่างที่ 1.5 กำหนดให้ $f(x) = 2x - 1$ และ $g(x) = 3x + 2$ จงหา $(f+g)(5)$

วิธีทำ จากบทนิยาม 1.23 จะได้ว่า

$$\begin{aligned}(f+g)(x) &= f(x) + g(x) \\ &= (2x-1) + (3x+2) \\ &= 5x + 1\end{aligned}$$

ดังนั้น

$$\begin{aligned}(f+g)(5) &= 5(5) + 1 \\ &= 26\end{aligned}$$

บทนิยาม 1.24 กำหนดให้ A และ B เป็นเซตที่ไม่ใช่เซตว่าง ถ้า $f : A \longrightarrow B$ จะเรียก f ว่าฟังก์ชันจากเซต A ไปบน (onto) เซต B หรือฟังก์ชันทั่วถึง (onto function or surjective function or surjection) B ซึ่งเขียนแทนสัญลักษณ์ $f : A \xrightarrow{onto} B$ ก็ต่อเมื่อ $R_f = B$ กล่าวคือ f เป็นฟังก์ชันทั่วถึง B ก็ต่อเมื่อ สำหรับแต่ละ $b \in B$ จะมี $a \in D_f$ ที่ซึ่ง $(a, b) \in f$ และ $b = f(a)$

บทนิยาม 1.25 กำหนดให้ A และ B เป็นเซตที่ไม่ใช่เซตว่าง ถ้า $f : A \longrightarrow B$ จะเรียก f ว่าฟังก์ชันหนึ่งต่อหนึ่ง (one - to - one function or injective function or injection) ซึ่งเขียนแทนด้วยสัญลักษณ์ $f : A \xrightarrow{1-1} B$ ก็ต่อเมื่อ ถ้า $a_1, a_2 \in D_f$ โดยที่ $a_1 \neq a_2$ แล้ว $f(a_1) \neq f(a_2)$ กล่าวคือ f เป็นฟังก์ชันหนึ่งต่อหนึ่ง ก็ต่อเมื่อ ถ้า $f(a_1) = f(a_2)$ แล้ว $a_1 = a_2$

สำหรับฟังก์ชันที่เป็นทั้งฟังก์ชันทั่วถึง และฟังก์ชันหนึ่งต่อหนึ่ง เราเรียกฟังก์ชันดังกล่าวว่าฟังก์ชันหนึ่งต่อหนึ่งทั่วถึง ดังบทนิยามต่อไปนี้

บทนิยาม 1.26 กำหนดให้ A และ B เป็นเซตที่ไม่ใช่เซตว่าง ถ้า $f : A \longrightarrow B$ จะเรียก f ว่าฟังก์ชันหนึ่งต่อหนึ่งทั่วถึง (bijective function or bijection) หรือกล่าวว่ามีการสมนัยหนึ่งต่อหนึ่ง (one - to - one correspondennce) ระหว่าง A และ B ซึ่งเขียนแทนด้วยสัญลักษณ์ $f : A \xrightarrow[onto]{1-1} B$ ก็ต่อเมื่อ f เป็นฟังก์ชันหนึ่งต่อหนึ่งจาก A ไปบน B

ตัวอย่างที่ 1.6 กำหนดให้ $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ โดยที่ $f(x) = x + 2$ สำหรับทุก $x \in \mathbb{Z}$ จงพิจารณาว่า f เป็นฟังก์ชันหนึ่งต่อหนึ่งทั่วถึงหรือไม่

วิธีทำ อย่างแรกจะแสดงว่า f เป็นฟังก์ชันทั่วถึง
สมมติให้ $b \in \mathbb{Z}$
จะได้ว่ามี $a = b - 2 \in \mathbb{Z}$ ที่ทำให้ $f(a) = f(b-2) = (b-2) + 2 = b$
ดังนั้น f เป็นฟังก์ชันทั่วถึง $\mathbb{Z}$
ต่อไปจะแสดงว่า f เป็นฟังก์ชันหนึ่งต่อหนึ่ง
สมมติให้ $x_1, x_2 \in \mathbb{Z}$ โดยที่ $f(x_1) = f(x_2)$
จะได้ว่า $x_1 + 2 = x_2 + 2$
ดังนั้น $x_1 = x_2$
แสดงว่า f เป็นฟังก์ชันหนึ่งต่อหนึ่ง
จึงสรุปได้ว่า $f : \mathbb{Z} \xrightarrow[onto]{1-1} \mathbb{Z}$

ปุณศยา พัฒนางกูร (2555: 27-32) ได้ให้นิยาม ทฤษฎีบทที่เกี่ยวข้องกับฟังก์ชัน ดังนี้

บทนิยาม 1.27 กำหนดให้ A และ B เป็นเซตที่ไม่ใช่เซตว่าง เรียกฟังก์ชัน $i_A : A \longrightarrow A$ ที่กำหนดโดย

$$i_A(x) = x \text{ สำหรับทุก } x \in A$$

ว่าฟังก์ชันเอกลักษณ์ (identity function) บน A และถ้า b เป็นสมาชิกตัวหนึ่งของ B แล้วเรียกฟังก์ชัน $f : A \longrightarrow B$ ซึ่งกำหนดโดย $f(x) = b$ สำหรับทุก $x \in A$ ว่าฟังก์ชันคงตัว (constant function) ที่มี $R_f = \{b\}$

บทนิยาม 1.28 กำหนดให้ A และ B เป็นเซตที่ไม่ใช่เซตว่าง ถ้า f เป็นฟังก์ชันจาก A ไปยัง B เรียกเซต f^{-1} ว่าตัวผกผันของ f (inverse of a function f) ก็ต่อเมื่อ $f^{-1} = \{(b, a) \mid (a, b) \in f\} \subseteq B \times A$

ข้อสังเกต f^{-1} ไม่จำเป็นจะต้องเป็นฟังก์ชันจาก B ไปยัง A

ทฤษฎีบท 1.29 กำหนดให้ A, B เป็นเซตที่ไม่ใช่เซตว่าง ถ้า f เป็นฟังก์ชันจาก A ไปยัง B แล้วจะได้ว่า $D_{f^{-1}} = R_f$ และ $R_{f^{-1}} = D_f$

บทนิยาม 1.30 กำหนดให้ f เป็นฟังก์ชันใด ๆ เรียก f^{-1} ว่าฟังก์ชันผกผัน (inverse function) ของ f ก็ต่อเมื่อ f^{-1} เป็นฟังก์ชัน

ตัวอย่างที่ 1.7 กำหนดให้ $f = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = 3x - 7\}$ ซึ่งเป็นฟังก์ชัน จงแสดงว่า f^{-1} เป็นฟังก์ชันผกผันของ f

วิธีทำ จากบทนิยาม 1.30 จะแสดงว่า f^{-1} เป็นฟังก์ชัน

พิจารณา $f^{-1} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x = 3y - 7\}$

$= \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = \dfrac{x+7}{3}\}$

ให้ (x_1, y_1) และ (x_2, y_2) เป็นสมาชิกของ f^{-1}

สมมติว่า $x_1 = x_2$

ดังนั้น $x_1 + 7 = x_2 + 7$

จะได้ว่า $\dfrac{x_1+7}{3} = \dfrac{x_2+7}{3}$

นั่นคือ $f^{-1}(x_1) = f^{-1}(x_2)$

ดังนั้น f^{-1} เป็นฟังก์ชัน

จึงสรุปได้ว่า f^{-1} เป็นฟังก์ชันผกผันของ f

ทฤษฎีบท 1.31 กำหนดให้ f เป็นฟังก์ชันใด ๆ จะได้ว่า ถ้า f เป็นฟังก์ชันหนึ่งต่อหนึ่งแล้ว f^{-1} เป็นฟังก์ชันผกผันของ f

บทนิยาม 1.32 กำหนดให้ A B และ C เป็นเซตที่ไม่ใช่เซตว่าง และให้ $f : A \longrightarrow B$ $g : B \longrightarrow C$ โดยที่ $R_f \cap D_g \neq \varnothing$ ฟังก์ชันประกอบ (composite function) ของ g และ f แทนด้วยสัญลักษณ์ $g \circ f$ หมายถึง $\{(a, c) \in A \times C \mid (a, b) \in f$ และ $(b, c) \in g$ สำหรับบาง $b \in B\}$ นั่นคือ $(g \circ f)(x) = g(f(x))$ สำหรับทุก $x \in D_{g \circ f}$ เมื่อ $D_{g \circ f} = \{a \in D_f | f(a) \in D_g\}$

ทฤษฎีบท 1.33 กำหนดให้ A B และ C เป็นเซตที่ไม่ใช่เซตว่าง และให้ $f : A \longrightarrow B$ $g : B \longrightarrow C$ โดยที่ $R_f \cap D_g \neq \varnothing$ จะได้ว่า $R_f \subseteq D_g$ ก็ต่อเมื่อ $D_{g \circ f} = D_f$

ทฤษฎีบท 1.34 กำหนดให้ A และ B เป็นเซตที่ไม่ใช่เซตว่าง ถ้า $f : A \xrightarrow[onto]{1-1} B$ แล้วจะมี $g : B \xrightarrow[onto]{1-1} A$ ที่ซึ่ง $g \circ f = i_A$, $f \circ g = i_B$ และ $g = f^{-1}$

ทฤษฎีบท 1.35 กำหนดให้ A B C และ D เป็นเซตที่ไม่ใช่เซตว่าง ถ้า $f : A \to B$, $g : B \to C$ และ $h : C \to D$ แล้ว

1. $g \circ f$ เป็นฟังก์ชันจาก A ไปยัง C
2. ถ้า $f : A \xrightarrow{onto} B$ และ $g : B \xrightarrow{onto} C$ แล้ว $g \circ f : A \xrightarrow{onto} C$
3. ถ้า $f : A \xrightarrow{1-1} B$ และ $g : B \xrightarrow{1-1} C$ แล้ว $g \circ f : A \xrightarrow{1-1} C$
4. $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$
5. $(h \circ g) \circ f = h \circ (g \circ f)$
6. $(f^{-1} \circ f)(a) = a$ สำหรับทุก $a \in D_f$
7. $(f \circ f^{-1})(b) = b$ สำหรับทุก $b \in D_{f_{-1}} = R_f$

ทฤษฎีบท 1.36 กำหนดให้ A และ B เป็นเซตที่ไม่ใช่เซตว่าง ถ้า $f : A \to B$ และ $g : B \to A$ โดยที่ $g \circ f = i_A$ แล้ว $f : A \xrightarrow{1-1} B$ และ $g : B \xrightarrow{onto} A$

เนื่องจากเซต และตัวดำเนินการเป็นส่วนประกอบหลักของเนื้อเรื่อง ดังนั้น บทนิยาม และทฤษฎีบทที่กล่าวมาจึงถือว่าเป็นพื้นฐานที่สำคัญ นอกจากนี้บทนิยามต่าง ๆ ของความสัมพันธ์สมมูลจะเป็นพื้นฐานของตัวอย่างที่สำคัญอย่างคลาสสมมูลของจำนวนเต็ม ดังหัวข้อถัดไป

จำนวนเต็ม

ตัวอย่างต่าง ๆ ตลอดทั้งเล่ม จะกล่าวถึงคลาสของจำนวนเต็ม ดังนั้น การสร้างคลาสของจำนวนเต็มจึงนับเป็นพื้นฐานที่สำคัญไม่น้อยไปกว่าความสัมพันธ์และฟังก์ชัน

บทนิยาม 1.37 กำหนดให้ a และ b เป็นจำนวนเต็มโดยที่ $a \neq 0$ จะกล่าวว่า a หาร b ลงตัว (a does divide b) เขียนแทนด้วยสัญลักษณ์ $a \mid b$ ก็ต่อเมื่อ มีจำนวนเต็ม c ที่ทำให้ $b = ac$ ทั้งนี้ ถ้า a หาร b ลงตัวแล้ว เรียก a ว่าตัวหาร (divisor) หรือตัวประกอบ (factor) ของ b และเรียก b ว่าพหุคูณ (multiple) ของ a นอกจากนี้จะกล่าวว่า a หาร b ไม่ลงตัว (a does not divide b) เขียนแทนด้วยสัญลักษณ์ $a \nmid b$ ก็ต่อเมื่อ ไม่มีจำนวนเต็ม c ที่ทำให้ $b = ac$

ปุณศยา พัฒนางกูร (2555: 56-58) ได้ให้ทฤษฎีบทที่เกี่ยวข้องกับการหารลงตัว พร้อมยกตัวอย่าง ดังนี้

ทฤษฎีบท 1.38 กำหนดให้ a, b และ c เป็นจำนวนเต็มใด ๆ จะได้ว่า

1. ถ้า $a \neq 0$ แล้ว $a \mid 0$ และ $a \mid \pm a$
2. $1 \mid b$ และ $-1 \mid b$
3. ถ้า $a \mid b$ และ $b \mid c$ แล้ว $a \mid c$
4. ถ้า $a \mid b$ และ $b \mid c$ แล้ว $a \mid (bx + cy)$ สำหรับทุก $x, y \in \mathbb{Z}$
5. ถ้า $a \mid b$ และ $b \neq 0$ แล้ว $|a| \leq |b|$
6. ถ้า $a \mid b$ และ $b \mid a$ แล้ว $a = b$ หรือ $a = -b$
7. ถ้า $a \mid (b + c)$ และ $a \mid b$ แล้ว $a \mid c$
8. $a \mid 1$ ก็ต่อเมื่อ $a = \pm 1$
9. ถ้า $a \mid b$ แล้ว $a^n \mid b^n$ สำหรับทุก $n \in \mathbb{Z}^+$

ตัวอย่างที่ 1.8 จงพิสูจน์ว่า 4 หาร $5^n - 1$ ลงตัว สำหรับทุก $n \in \mathbb{Z}^+$

วิธีทำ ให้ $P(n)$ แทนข้อความ “4 หาร $5^n - 1$ ลงตัว ”
เนื่องจาก 4 หาร $5^1 - 1$ ลงตัว
ดังนั้น $P(1)$ เป็นจริง
สำหรับ $k \in \mathbb{Z}^+$ สมมติว่า $P(k)$ เป็นจริง
นั่นคือ 4 หาร $5^k - 1$ ลงตัว
พิจารณา $5^{k+1} - 1 = 5(5^k) - 1 = (4 + 1)5^k - 1 = 4(5^k) + 5^k - 1$
เนื่องจาก 4 หาร $4(5^k)$ ลงตัว และ 4 หาร $5^k - 1$ ลงตัว
โดยทฤษฎีบท 1.38 (4.) จะได้ว่า 4 หาร 5^{k+1} ลงตัว
ดังนั้น $P(k + 1)$ เป็นจริง
โดยหลักอุปนัยชิงคณิตศาสตร์ จะได้ว่า $P(n)$ เป็นจริง สำหรับทุก $n \in \mathbb{Z}^+$
นั่นคือ 4 หาร $5^n - 1$ ลงตัว สำหรับทุก $n \in \mathbb{Z}^+$

ทฤษฎีบท 1.39 ขั้นตอนวิธีการหาร (Division Algorithm)
ถ้า a และ b เป็นจำนวนเต็มโดยที่ $b > 0$ แล้วจะมีจำนวนเต็ม q และ r เพียงคู่เดียวเท่านั้น ที่ทำให้

$$a = qb + r \text{ โดยที่ } 0 \leq r < b$$

เราเรียกจำนวนเต็ม q ว่าผลหาร (quotient) ที่ได้จากการหาร a ด้วย b และเรียกจำนวนเต็ม r ว่าเศษเหลือ (remainder) ที่ได้จากการหาร a ด้วย b

บทแทรก 1.40 ถ้า a และ b เป็นจำนวนเต็ม โดยที่ $b \neq 0$ แล้วจะมีจำนวนเต็ม q และ r เพียงคู่เดียวเท่านั้นที่ทำให้ $a = qb + r$ โดยที่ $0 \leq r < |b|$

สำหรับแต่ละจำนวนเต็มบวก n จะมีความสัมพันธ์บน $\mathbb{Z}$ เรียกว่าความสัมพันธ์คอนกรูเอนซ์ นำไปสู่การสร้างเซตของจำนวนเต็มกรูเอนซ์ (congruent integers or congruent number) ดังนี้

บทนิยาม 1.41 กำหนดให้ a และ b เป็นจำนวนเต็ม และ n เป็นจำนวนเต็มบวก จะกล่าวว่า a คอนกรูเอนซ์ b มอดูโล n (a is congruent to b modulo n) เขียนแทนด้วยสัญลักษณ์ $a \equiv b \pmod{n}$ ก็ต่อเมื่อ $n \mid (a-b)$ หรือ $a - b = kn$ สำหรับบางจำนวนเต็ม k และเรากล่าวว่า a ไม่คอนกรูเอนซ์กับ b มอดุโล n (a is congruent to b modulo n) เขียนแทนด้วยสัญลักษณ์ $a \not\equiv b \pmod{n}$ ก็ต่อเมื่อ $n \nmid (a-b)$ เรียกจำนวนเต็ม n ว่ามอดุลัส (modulus)

สมบัติของคอนกรูเอนซ์มีความคล้ายคลึงกับการเท่ากัน ดังนี้

ทฤษฎีบท 1.42 กำหนดให้ a, b, c, d เป็นจำนวนเต็ม และ n เป็นจำนวนเต็มบวก จะได้ว่า

1. $a \equiv a \pmod{n}$
2. ถ้า $a \equiv b \pmod{n}$ แล้ว $b \equiv a \pmod{n}$
3. ถ้า $a \equiv b \pmod{n}$ และ $b \equiv c \pmod{n}$ แล้ว $a \equiv c \pmod{n}$
4. ถ้า $a \equiv b \pmod{n}$ และ $c \equiv d \pmod{n}$ แล้ว $a + c \equiv b + d \pmod{n}$ และ $ac \equiv bd \pmod{n}$
5. ถ้า $a \equiv b \pmod{n}$ แล้ว $a + c \equiv b + c \pmod{n}$ และ $ac \equiv bc \pmod{n}$
6. ถ้า $a \equiv b \pmod{n}$ แล้ว $a^k \equiv b^k \pmod{n}$ สำหรับทุก $k \in \mathbb{Z}$

หมายเหตุ จากทฤษฎีบท 1.42 (1.) (2.) และ (3.) กล่าวได้ว่าความสัมพันธ์คอนกรูเอนซ์ มีสมบัติสะท้อน สมบัติสมมาตร และสมบัติถ่ายทอด ตามลำดับ จึงกล่าวได้ว่าความสัมพันธ์คอนกรูเอนซ์เป็นความสัมพันธ์สมมูล (equivalent relation)

ตัวอย่างที่ 1.9 จงแสดงว่า 41 หาร $2^{20}-1$ ลงตัว

วิธีทำ เนื่องจาก $2^5 \equiv -9 \pmod{41}$
โดยทฤษฎีบท 1.42 (6.) จะได้ว่า $(2^5)^4 \equiv (-9)^4 \pmod{41}$
นั่นคือ $2^{20} \equiv (81)(81) \pmod{41}$
แต่ $81 \equiv -1 \pmod{41}$
โดยทฤษฎีบท 1.42 (4.) จะได้ว่า $(81)(81) \equiv 1 \pmod{41}$
โดยทฤษฎีบท 1.2.6 (3.) จะได้ว่า $2^{20} \equiv 1 \pmod{41}$
ดังนั้น $41 \mid (2^{20}-1)$

ตัวอย่างที่ 1.10 จงแสดงว่า $2^{23} \equiv 1 \pmod{47}$

วิธีทำ เนื่องจาก $2^5 \equiv 32 \pmod{47}$ และ $32 \equiv -15 \pmod{47}$
โดยทฤษฎีบท 1.42 (3.) จะได้ว่า $2^5 \equiv -15 \pmod{47}$
โดยทฤษฎีบท 1.42 (6.) จะได้ว่า $(2^5)^2 \equiv (-15)^2 \pmod{47}$
นั่นคือ $2^{10} \equiv 225 \pmod{47}$
แต่ $225 \equiv -10 \pmod{47}$
โดยทฤษฎีบท 1.42 (3.) จะได้ว่า $2^{10} \equiv -10 \pmod{47}$
โดยทฤษฎีบท 1.42 (6.) จะได้ว่า $(2^{10})^2 \equiv (-10)^2 \pmod{47}$
นั่นคือ $2^{20} \equiv 100 \pmod{47}$
แต่ $100 \equiv 6 \pmod{47}$
โดยทฤษฎีบท 1.42 (3.) จะได้ว่า $2^{20} \equiv 6 \pmod{47}$
โดยทฤษฎีบท 1.42 (4.) จะได้ว่า $(2^{20})(2^3) \equiv (6)(2^3) \pmod{47}$
นั่นคือ $2^{23} \equiv 48 \pmod{47}$
เนื่องจาก $48 \equiv 1 \pmod{47}$
โดยทฤษฎีบท 1.42 (3.) จะได้ว่า $2^{23} \equiv 1 \pmod{47}$

ทฤษฎีบท 1.43 กำหนดให้ $a\ b\ c\ d$ เป็นจำนวนเต็ม และ n เป็นจำนวนเต็มบวก จะได้ว่า
1. ถ้า $a \equiv b \pmod{n}$ และ $c \equiv d \pmod{n}$ แล้ว $ax + cy \equiv bx + dy \pmod{n}$ สำหรับทุก $x, y \in Z$
2. ถ้า $a \equiv b \pmod{n}$ และ $d \in N$ ซึ่ง $d \mid n$ แล้ว $a \equiv b \pmod{d}$
3. ถ้า $a \equiv b \pmod{n}$ แล้ว $ak \equiv bk \pmod{nk}$ สำหรับทุก $k \in N$

ทฤษฎีบท 1.44 กำหนดให้ $a\ b$ เป็นจำนวนเต็ม และ n เป็นจำนวนเต็มบวก จะได้ว่า $a \equiv b \pmod{n}$ ก็ต่อเมื่อ เศษที่ได้จากการหาร a ด้วย n เท่ากับเศษที่ได้จากการหาร b ด้วย n

ตัวอย่างที่ 1.11 จงหาเศษที่ได้จากการหาร 5^{110} ด้วย 6

วิธีทำ เนื่องจาก $5 \equiv -1 \pmod 6$
โดยทฤษฎีบท 1.42 (6.) จะได้ว่า $5^{110} \equiv (-1)^{110} \pmod 6$
แต่ $(-1)^{110} \equiv 1 \pmod 6$
โดยทฤษฎีบท 1.42 (3.) จะได้ว่า $5^{110} \equiv 1 \pmod 6$
โดยทฤษฎีบท 1.44 จะได้ว่า 5^{110} และ 1 ถูกหารด้วย 6 แล้วจะเหลือเศษเท่ากัน
แต่ 6 หาร 1 เหลือเศษ 1 ดังนั้น เศษที่ได้จากการหาร 5^{110} ด้วย 6 คือ 1

บทนิยาม 1.45 กำหนดให้ a เป็นจำนวนเต็ม และ n เป็นจำนวนเต็มบวก จะเขียนแทนเซตของจำนวนเต็มทั้งหมดที่คอนกรูเอนซ์กับ a มอดุโล n ด้วยสัญลักษ์ $[a]$ กล่าวคือ

$$\begin{aligned}[a] &= \{x \in \mathbb{Z} | x \equiv a \pmod n\} \\ &= \{x \in \mathbb{Z} | n \mid (x-a)\} \\ &= \{x \in \mathbb{Z} | x - a = kn \text{ สำหรับบางจำนวนเต็ม } k\} \\ &= \{x \in \mathbb{Z} | x = a + kn \text{ สำหรับบางจำนวนเต็ม } k\}\end{aligned}$$

เรียก $[a]$ ว่าเป็นชั้นสมมูล (equivalence class) ของจำนวนเต็มภายใต้คอนกรูเอนซ์มอดุโล n ที่มี a เป็นสมาชิก และเรียก a ว่าเป็นตัวแทน (representation) ของชั้นสมมูล $[a]$

ตัวอย่างที่ 1.12 จงหาชั้นสมมูลของจำนวนเต็มภายใต้คอนกรูเอนซ์มอดุโล 5

วิธีทำ

$$\begin{aligned}[0] &= \{x \in \mathbb{Z} | x = 5k \text{ สำหรับบาง } k \in \mathbb{Z}\} \\ &= \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\} \\ [1] &= \{x \in \mathbb{Z} | x = 1 + 5k \text{ สำหรับบาง } k \in \mathbb{Z}\} \\ &= \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\} \\ [2] &= \{x \in \mathbb{Z} | x = 2 + 5k \text{ สำหรับบาง } k \in \mathbb{Z}\} \\ &= \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\} \\ [3] &= \{x \in \mathbb{Z} | x = 3 + 5k \text{ สำหรับบาง } k \in \mathbb{Z}\} \\ &= \{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\} \\ [4] &= \{x \in \mathbb{Z} | x = 4 + 5k \text{ สำหรับบาง } k \in \mathbb{Z}\} \\ &= \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\}\end{aligned}$$

จากตัวอย่างที่ 1.12 หากทำต่อไปเรื่อย ๆ จะพบว่า

$$\begin{aligned}[0] &= [5] = [10] = \ldots \\ [1] &= [6] = [11] = \ldots \\ [2] &= [7] = [12] = \ldots \\ [3] &= [8] = [13] = \ldots \\ [4] &= [9] = [14] = \ldots\end{aligned}$$

นั่นคือ ชั้นสมมูลหนึ่งชั้นสมมูลใด ๆ ของจำนวนเต็มภายใต้คอนกรูเอนซ์มอดุโล 5 นั้น สามารถเขียนได้หลายรูปแบบ โดยเปลี่ยนแต่ตัวแทนซึ่งเป็นสมาชิกของชั้นสมมูลนั้น ๆ เพื่อความสะดวกเรามักจะใช้จำนวนเต็มที่ไม่เป็นลบที่น้อยที่สุดจากแต่ละชั้นสมมูลมาเป็นตัวแทน ซึ่งมีเครื่องมือที่ช่วยตรวจสอบว่าชั้นสมมูลใดเป็นชั้นสมมูลเดียวกันดังทฤษฎีบท 1.46

ทฤษฎีบท 1.46 กำหนดให้ a b เป็นจำนวนเต็ม และ n เป็นจำนวนเต็มบวก จะได้ว่า $a \equiv b \pmod{n}$ ก็ต่อเมื่อ $[a] = [b]$

ทฤษฎีบท 1.47 กำหนดให้ n เป็นจำนวนเต็มบวกใด ๆ ความสัมพันธ์คอนกรูเอนซ์มอดุโล n จะแบ่งเซตของจำนวนเต็มออกเป็น n ชั้นสมมูลของจำนวนเต็มภายใต้คอนกรูเอนซ์มอดุโล n ที่แตกต่างกัน

จากทฤษฎีบท 1.47 เราจะสร้างเซตของชั้นสมมูลทั้งหมดได้ดังบทนิยาม 1.48

บทนิยาม 1.48 กำหนดให้ n เป็นจำนวนเต็มบวก จะเรียกเซต $\mathbb{Z}_n$ ที่มีสมาชิกเป็นชั้นสมมูลทั้งหมดของจำนวนเต็มภายใต้คอนกรูเอนซ์มอดุโล n ว่าเซตของจำนวนเต็มมอดุโล n (the set of integers modulo n) กล่าวคือ $\mathbb{Z}_n = \{[0], [1], [2], ..., [n-1]\}$

จากตัวอย่างที่ 1.12 มีสิ่งที่น่าสนใจเช่นเดียวกับการเท่ากันของชั้นสมมูล คือ อินเตอร์เซกชันของสองชั้นสมมูลใด ๆ จะเป็นเซตว่าง และ $[0] \cup [1] \cup [2] \cup [3] \cup [4] = \mathbb{Z}$ ซึ่งมีการพิสูจน์แล้วว่าเป็นจริงเสมอสำหรับจำนวนเต็มบวก n ใด ๆ ดังทฤษฎีบท 1.49

ทฤษฎีบท 1.49 กำหนดให้ n เป็นจำนวนเต็มบวก จะได้ว่า

1. สำหรับแต่ละ $[a] \in \mathbb{Z}_n$ จะได้ว่า $[a] \neq \varnothing$
2. ถ้า $[a] \in \mathbb{Z}_n$ และ $b \in [a]$ แล้ว $[b] = [a]$
3. สำหรับแต่ละ $[a], [b] \in \mathbb{Z}_n$ ที่ซึ่ง $[a] \neq [b]$ จะได้ว่า $[a] \cap [b] = \varnothing$
4. $\mathbb{Z} = \bigcup_{a \in \mathbb{Z}} [a]$

จากทฤษฎีบท 1.49 สำหรับจำนวนเต็มบวก n ใด ๆ $\mathbb{Z}_n$ จะเป็นผลแบ่งส่วนของ $\mathbb{Z}$ เสมอ สิ่งที่น่าสนใจนอกเหนือไปจากเซตของชั้นสมมูลของจำนวนเต็ม คือ การดำเนินการของสมาชิกใน $\mathbb{Z}_n$ ซึ่งมีการนิยามการดำเนินการที่สำคัญดังบทนิยาม 1.50

บทนิยาม 1.50 กำหนดให้ n เป็นจำนวนเต็มบวก จะนิยามการบวก และการคูณบน $\mathbb{Z}_n$ ดังนี้ $[a] +_n [b] = [a+b]$ และ $[a] \cdot_n [b] = [ab]$ สำหรับทุก $[a], [b] \in \mathbb{Z}_n$

พิจารณาจากบทนิยาม 1.50 และคุณสมบัติของจำนวนเต็มภายใต้การบวก และการคูณปกติ จะสามารถพิสูจน์ทฤษฎีบท 1.51 ได้โดยตรง

ทฤษฎีบท 1.51 กำหนดให้ n เป็นจำนวนเต็มบวก และ $[a], [b], [c] \in \mathbb{Z}_n$ จะได้ว่า

1. $[a] +_n [b] = [b] +_n [a]$
2. $[a] \cdot_n [b] = [b] \cdot_n [a]$
3. $([a] +_n [b]) +_n [c] = [a] +_n ([b] +_n [c])$
4. $([a] \cdot_n [b]) \cdot_n [c] = [a] \cdot_n ([b] \cdot_n [c])$
5. $[a] \cdot_n ([b] +_n [c]) = ([a] \cdot_n [b]) +_n ([a] \cdot_n [c])$
6. $[0] +_n [a] = [a]$
7. $[1] \cdot_n [a] = [a]$
8. ถ้า n เป็นจำนวนเฉพาะ และ $[a] \in \mathbb{Z}_n$ โดยที่ $[a] \neq [0]$ แล้วจะมี $[b] \in \mathbb{Z}_n$ ที่ทำให้ $[a] \cdot_n [b] = [1]$

สรุปท้ายบท

พีชคณิตนามธรรมประกอบด้วยหัวใจหลัก 2 อย่าง คือ เซต และตัวดำเนินการ ผลแบ่งส่วนของ $\mathbb{Z}$ ภายใต้การดำเนินการในบทนิยาม 1.50 เป็นตัวอย่างที่สำคัญในบทต่อ ๆ ไป เนื้อหาในบทนี้มีความหลากหลาย หากจัดทำเนื้อหาอย่างละเอียดครบถ้วน อาจทำให้ผู้อ่านจับประเด็นเนื้อหาพีชคณิตนามธรรมคลาดเคลื่อน จึงกล่าวถึงเนื้อหาเพียงบางส่วนที่จำเป็นพร้อมกับไม่พิสูจน์ทฤษฎีบทต่าง ๆ ในบทนี้ แต่จะให้ความสำคัญกับการพิสูจน์ทฤษฎีบท และเพิ่มตัวอย่างตั้งแต่บทที่ 2 เป็นต้นไป