

บทที่ 1

ความรู้เบื้องต้นของทฤษฎีจำนวน

วิชาทฤษฎีจำนวน (Number Theory) เป็นวิชาที่ศึกษาเกี่ยวกับสมบัติของจำนวนโดยเฉพาะอย่างยิ่งสมบัติของจำนวนเต็มและจำนวนนับ เนื่องจากการนับจำนวนเป็นสิ่งที่อยู่คู่กับการดำเนินชีวิตของมนุษย์มาช้านาน และเป็นจำนวนชนิดแรกที่มีมนุษย์รู้จัก สมบัติต่าง ๆ ของจำนวนนับจึงเป็นสิ่งที่สนใจตลอดเวลาอันยาวนาน มีแง่มุมต่าง ๆ ที่ให้ได้ศึกษาค้นคว้าไว้มากมายหลายแง่มุม ทฤษฎีจำนวนเป็นสาขาหนึ่งที่ถือว่าเก่าแก่ที่สุดทางคณิตศาสตร์ และปัจจุบันยังได้รับการศึกษาค้นคว้าอีกมากมายจากนักคณิตศาสตร์ ซึ่งในบทนี้จะนำเสนอเนื้อหาจาก วิวัฒนาการของวิชาทฤษฎีจำนวนนับเป็นพื้นฐานความรู้เพื่อให้รู้จักวิชานี้ซึ่งจะกล่าวถึงเป็นส่วนแรก การพิสูจน์เบื้องต้น สมบัติจำนวนเต็ม และข้อแนะนำบางประการเกี่ยวกับจำนวนเต็มเนื่องจากการศึกษาขอบข่ายการศึกษาทฤษฎีจำนวน จะจำกัดเฉพาะจำนวนเต็มเท่านั้นและการเข้าใจสมบัติที่เกี่ยวกับจำนวนเต็มจะเป็นเครื่องมือสำคัญในการพิสูจน์สมบัติต่าง ๆ ที่เกี่ยวข้องต่อไป

1.1 วิวัฒนาการของวิชาทฤษฎีจำนวน

ณรงค์ ปันนิม และนิตยา ปภาพจน์ (2553 : 1-2) ได้กล่าวถึงวิวัฒนาการของวิชาทฤษฎีจำนวนโดยมีวัตถุประสงค์เพื่อให้ทราบถึงความเป็นมาของทฤษฎีจำนวนไว้ว่า ทฤษฎีจำนวนทฤษฎีจำนวนเป็นสาขาหนึ่งที่เก่าแก่ที่สุดทางคณิตศาสตร์ เพราะถูกพัฒนามาตั้งแต่สมัยกรีกโบราณเมื่อประมาณ 2500 ปีมาแล้ว โดยพิจารณาจากหลักฐานที่ปรากฏในอดีต นักคณิตศาสตร์มีความเห็นว่าจะเริ่มจากยุคของพีทาโกรัส (Pythagoras 569 – 500 ปีก่อนคริสต์ศักราช) และปัจจุบันยังได้รับการศึกษาค้นคว้าอีกมากมายจากทั้งนักคณิตศาสตร์มืออาชีพและมือสมัครเล่น ด้วยเหตุผลที่ว่าปัญหาทางทฤษฎีจำนวนนั้นชวนคิดและท้าทายความสามารถ มีความง่ายที่จะทำความเข้าใจประกอบกับปัญหาแต่ละปัญหา ดูเหมือนว่ามีโอกาสหาคำตอบได้ นอกจากนี้ยังมีข้อคาดเดาและปัญหาที่ยังไม่สามารถหาคำตอบได้อีกมากมายน่าสนใจจะศึกษา โดยทั่วไปเป็นที่ยอมรับกันว่า พีทาโกรัส (Pythagoras) และศิษย์เป็นผู้ริเริ่มในการพัฒนาจำนวน พีทาโกรัสและศิษย์มีความเชื่อว่ากฎเกณฑ์สำคัญที่จะอธิบายสิ่งต่าง ๆ ในจักรวาลคือจำนวนแนวคิดของคนกลุ่มนี้ยึดปรัชญาว่า “ทุกสิ่งทุกอย่างคือจำนวน” การศึกษาจำนวนในสมัยของพีทาโกรัสได้นำความมหัศจรรย์ของจำนวนไปผูกพันกับความเชื่อโชคลาง โหราศาสตร์และราศี เช่น จำนวนเชิงมิตร (Amicable Numbers) คู่แรก ที่เชื่อว่าพบในสมัยของพีทาโกรัส คือ 284 และ 220 สองจำนวนนี้มีสมบัติพิเศษ คือ ตัวหารแท้ของจำนวนหนึ่งมีผลบวกเท่ากับตัวหารแท้ของอีกจำนวนหนึ่ง หรือตัวหารแท้ของ 284 ได้แก่ 1, 2, 4, 71, 142 และ $1 + 2 + 4 + 71 + 142 = 220$ ตัวหารแท้ของ 220 ได้แก่ 1, 2, 4, 5, 10, 11, 20, 22, 44, 55, 110 และ

$$1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284$$

ผู้ที่เชื่อโชคลางจะจารึกตัวเลขลงในเครื่องรางของขลัง โดยเชื่อว่าคนคูใดห้อยของขลังที่จารึกตัวเลขดังกล่าวจะเป็นมิตรแท้ต่อกัน การค้นหาจำนวนเชิงमितรข้างต้นเป็นฐานให้เกิดการค้นหาจำนวนเชิงमितรอื่น ๆ อีกมากมาย ในปี ค.ศ. 1636 ปีแยร์เดอแฟร์มาร์ (Pierre De Fermat ค.ศ.1601 – 1665) พบจำนวนเชิงमितรคู่ที่สองคือ 17,296 และ 18,416 ต่อมาในปี ค.ศ. 1638 เรอเนเดส์การ์ตส์ (Rene Descartes ค.ศ.1596 – 1650) ได้ค้นพบจำนวนเชิงमितรคู่ที่สามคือ 9,363,584 และ 9,437,056 จากนั้นในปี ค.ศ. 1747 เลออนฮาร์ด ออยเลอร์ (Leonhard Euler ค.ศ.1707 – 1783) ได้เสนอจำนวนเชิงमितรถึง 64 คู่ แต่จากการตรวจสอบโดยนักคณิตศาสตร์รุ่นหลังปรากฏว่ามี 2 คู่ในจำนวน 64 คู่ ไม่ใช่จำนวนเชิงमितร แต่ค้นพบหลังจากออยเลอร์ประกาศเกือบ 200 ปี ต่อมาในปี ค.ศ. 1830 อาเดรียงมารีเลอจองด์ (Adrien Marie Legendre ค.ศ. 1752 – 1833) ได้พบคูใหม่อีก 1 คู่ คือ 2,172,649,216 และ 8,520,191 ในปี ค.ศ. 1866 นิโคโลไปนิน (Nicolo Painini) ชาวอิตาลีอายุ 16 ปี พบจำนวนเชิงमितรที่น้อยกว่า ของแฟร์มา คือ 1,184 และ 1,210 ต่อมาในปี ค.ศ. 1981 ฮิลตันเชน (Hilton Chen) และเดลวูดส์ (Dale Woods) ได้พบจำนวนเชิงमितร อีกคู่หนึ่ง โดยแต่ละจำนวนประกอบด้วย 50 หลัก คือ 21,741,269,040,875,890,083,566,772,572,567,935,979,368,836,363,843 และ 22,261,723,990,815,556,829,012,769,686,652,975,057,942,956,477 โดยในปัจจุบันสามารถใช้คอมพิวเตอร์คำนวณจำนวนमितรภาพได้มากกว่า 1,000 ล้านคู่ ความมหัศจรรย์ของจำนวน ในยุคของพีทาโกรัส จากการค้นพบว่ามีจำนวนที่มีค่าเท่ากับผลบวกของตัวหารแท้ทั้งหมดของจำนวนนั้น โดยเรียกจำนวนนั้นว่า จำนวนสมบูรณ์ (perfect number) ซึ่ง 6 และ 28 เป็นจำนวนสมบูรณ์ เนื่องจาก

$$6 \quad \text{มี } 1, 2, 3 \quad \text{เป็นตัวหารแท้และ } 1 + 2 + 3 = 6$$

$$28 \quad \text{มี } 1, 2, 4, 7, 14 \quad \text{เป็นตัวหารแท้และ } 1 + 2 + 4 + 7 + 14 = 28$$

การศึกษาเกี่ยวกับทฤษฎีจำนวนมีหลักฐานเด่นชัดในสมัยของกรีกประมาณ 300 ปีก่อนคริสต์ศักราช ปรากฏใน หนังสืออีลีเมนต์ (Elements) ซึ่งเรียบเรียงโดย ยูคลิด แห่งอะเล็กซานเดรีย (Euclid of Alexandria ประมาณ 450 – 380 ก่อน คริสต์ศักราช) มี 13 เล่ม เล่มที่ 7, 8 และ 9 มีเรื่องราวเกี่ยวกับทฤษฎีจำนวน เนื้อหาที่รู้จักกันดีในปัจจุบัน ได้แก่ จำนวนเต็มคู่ จำนวนเต็มคี่ จำนวนเฉพาะ ทฤษฎีบทขั้นตอนวิธีแบบยูคลิด (Euclidean Algorithm) ตัวหารร่วมมาก (Greatest Common Divisor) ตัวคูณร่วมน้อย (Least Common Multiple) และทฤษฎีบทที่ว่าจำนวนเฉพาะมีจำนวนอนันต์ เป็นต้น

ความเฟื่องฟูของทฤษฎีจำนวนหลังจากยุคของยูคลิดได้หยุดชะงักไป จนกระทั่งปี ค.ศ. 250 มินักคณิตศาสตร์ ชาวกรีกชื่อ ดีโอฟานโตสแห่งอะเล็กซานเดรีย (Diophantos of Alexandria) ได้ตีพิมพ์หนังสือจำนวน 13 เล่ม โดยดีโอฟานโตสสามารถแก้สมการทางพีชคณิตที่มีตัวไม่ทราบค่าสอง

ตัวหรือสามตัวได้และปัญหาของดีโอแฟนโตสหลาย ๆ ปัญหากลายเป็นจุดเริ่มต้นของทฤษฎีจำนวน โดยเฉพาะอย่างยิ่งดีโอแฟนโตสสนใจสมการพีชคณิตที่มีคำตอบเป็นจำนวนเต็ม ปัจจุบันเรียกสมการพีชคณิตที่มีคำตอบเป็นจำนวนเต็มนี้ว่า สมการไดโอแฟนไทน์(Diophantine equation) กลายเป็นรากฐานของการศึกษาทฤษฎีจำนวนในปัจจุบัน แม้การศึกษาทฤษฎีจำนวนจะมีมาตั้งแต่สมัยกรีกหากการสิ้นสุดอารยธรรมกรีกโรมันต่อด้วยการเข้าสู่ยุคกลางของยุโรปทำให้เกิดการชะงักงันทางการศึกษาดังกล่าว เนื่องจากองค์ความรู้จากคริสต์ศาสนาได้กลายเป็นศูนย์กลางในการอธิบายสรรพสิ่งรอบตัวแทน จนกระทั่งเข้าสู่ยุคฟื้นฟูศิลปวิทยาการราวคริสต์ศตวรรษที่ 14 – 17 ได้มีการฟื้นฟูวิทยาการสมัยกรีกโรมันขึ้น มาอีกครั้ง ช่วงเวลานี้เองที่เป็นจุดเริ่มต้นของทฤษฎีจำนวนสมัยปัจจุบัน

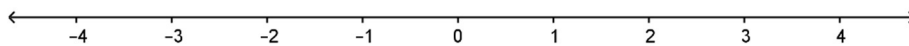
ชาวฝรั่งเศสชื่อว่า ปีแยร์ เดอ แฟร์มา (Piere de Fermat 1601 – 1665) เขาได้ทำการศึกษางานของดีโอแฟนโตสและเป็นคนที่ได้พบสมบัติของจำนวนเต็มอีกมากมาย โดยเฉพาะการคาดการณ์ว่าสมการ $x^n + y^n = z^n$ ไม่มีคำตอบเป็นจำนวนเต็มที่ไม่ใช่ศูนย์เมื่อ n เป็นจำนวนเต็มที่มากกว่า 2 แม้ขณะนั้นเขาสามารถพิสูจน์ได้เพียงกรณีที่ $n = 3$ เท่านั้น หากต่อมานักคณิตศาสตร์รุ่นหลัง ได้พยายามพิสูจน์ต่อจนสำเร็จ และตั้งชื่อว่า ทฤษฎีบทสุดท้ายของแฟร์มา(Fermat's Last Theorem) เพื่อเป็นเกียรติพร้อมยกย่องแฟร์มาว่าเป็นบิดาของทฤษฎีจำนวนสมัยใหม่ทฤษฎีจำนวนของแฟร์มาได้ส่งอิทธิพลต่อนักทฤษฎีจำนวนคนสำคัญอีกคน คือ เกาส์(Carl Friedrich Gauss) ซึ่งได้ ตีพิมพ์หนังสือ Disquisitiones Arithmeticae ในปี 1801 เนื้อหาเกี่ยวกับการพิสูจน์อย่างเป็นระบบ ก่อนพัฒนาต่อมาเป็นสมบัติของจำนวนเฉพาะอันเป็นการวางรากฐานเกี่ยวกับทฤษฎีจำนวนไว้อย่างมั่นคง จากการศึกษาวิชาทฤษฎีจำนวนหลายพันปีเห็นได้ว่า มีหัวข้อเกี่ยวกับจำนวนให้ขบคิดมากมาย หัวข้อในการศึกษาบางประการต้องใช้เวลานานกว่าจะได้รับการแก้ไข บางครั้งต้องผ่านการพิสูจน์ ซ้ำแล้วซ้ำเล่า หากพิจารณาว่าประเด็นใดเป็นสิ่งที่นักคณิตศาสตร์ให้ความสนใจอย่างยิ่งคงไม่พ้น เรื่องจำนวนเฉพาะ(Prime Number) เหตุผลประการแรก คือการตรวจสอบว่าจำนวนใดเป็นจำนวนเฉพาะไม่ใช่เรื่องที่จะตรวจสอบได้ง่ายถ้าจำนวนนั้นเป็นจำนวนขนาดใหญ่ เช่น 10,006,721 แต่ปัญหานี้ในปัจจุบันสามารถตรวจสอบโดยใช้คอมพิวเตอร์พบว่าจำนวนดังกล่าวเป็นจำนวนเฉพาะตัวที่ 664,999 เหตุผลอีกประการ หนึ่ง คือมีสูตรทั่วไปในการหาจำนวนเฉพาะตัวที่ n หรือไม่ หลายศตวรรษมาแล้วเชื่อว่า $n^2 + n + 41$ เป็นจำนวนเฉพาะสูตรนี้เป็นจริงเพียง 40 จำนวนเรียงติดกันคือ $n = 0, 1, 2, \dots, 39$ ทั้งนี้ ข้อเสนอของ แฟร์มาในการหาจำนวนเฉพาะคือ $F_n = 2^{2^n} + 1$ เป็นจำนวนเฉพาะสำหรับทุกจำนวนเต็ม $n \geq 0$ ต่อมาพบว่า $n = 5$ ไม่เป็นจำนวนเฉพาะเนื่องจาก 641 เป็นตัวประกอบของ F_5 พบโดยออยเลอร์ (Leonhard Euler ค.ศ. 1707 – 1783) เรียก F_n ว่าจำนวนแฟร์มา (Fermat number) ในกรณีที่ F_n เป็นจำนวนเฉพาะเรียกว่า จำนวนเฉพาะแฟร์มา (Fermat prime) ปัญหาเกี่ยวกับจำนวนเฉพาะที่สนใจเรื่องหนึ่งก็คือ จำนวนเฉพาะคู่แฝด (twin prime) คือ จำนวนเต็ม p และ $p + 2$ เป็นจำนวนเฉพาะทั้งคู่ เช่น 5, 7, 11, 17 เป็นต้น มีจำนวนเฉพาะคู่แฝดไม่จำกัดจำนวนใช้

หรือไม่ โดยใช้เครื่องคอมพิวเตอร์ตรวจสอบพบว่า มีจำนวนเฉพาะคู่แฝดที่น้อยกว่า 30,000,000 มีทั้งหมด 152,892 คู่

เนื้อหาที่ได้กล่าวมาในข้างต้นเป็นเพียงจุดเริ่มต้นและวิวัฒนาการบางส่วนในวิชาทฤษฎีจำนวนเท่านั้นนอกจากนี้ยังมีสิ่งที่น่าสนใจอีกมากมาย ซึ่งบางปัญหายังไม่สามารถหาคำตอบได้ แต่ในยุคปัจจุบันได้มีการใช้เทคโนโลยีต่าง ๆ ช่วยในการคิดค้นทำให้บางปัญหาสามารถหาคำตอบได้ง่าย สะดวกและรวดเร็วมากยิ่งขึ้น แต่ก็ยังมีบางปัญหาที่ถึงแม้จะใช้เทคโนโลยีต่าง ๆ เข้ามาช่วยแล้วแต่ก็ยังไม่สามารถหาคำตอบของปัญหาได้ สิ่งนี้จึงเป็นความท้าทายที่ก่อให้เกิดองค์ความรู้ใหม่ ๆ ตามมาได้

1.2 ระบบจำนวนเต็ม

ในหัวข้อนี้จะศึกษาสมบัติของจำนวนเต็ม พร้อมทั้งพิสูจน์ข้อความที่เกี่ยวข้องกับจำนวนเต็ม โดยจะมุ่งเน้นให้เห็นวิวัฒนาการและความสวยงามของระบบจำนวนดังกล่าว ระบบจำนวนเต็มเป็นระบบที่สามารถศึกษาคุณสมบัติได้มากมาย และเอกภาพสัมพันธ์ที่จะอ้างถึงคือ เซตของจำนวนเต็ม $\mathbb{Z}$ โดยที่ $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ แสดงได้ดังภาพประกอบ 1.1



ภาพประกอบ 1.1 แผนภาพแสดงจำนวนเต็มบนเส้นจำนวน

นอกจากเซตของ $\mathbb{Z}$ ที่แทนจำนวนเต็มยังมีเซตอื่น ๆ ที่ใช้แทนจำนวนในรูปแบบต่าง ๆ ดังต่อไปนี้

1. เซตของจำนวนเต็ม ($\mathbb{Z}$) โดยที่ $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$
2. เซตของจำนวนเต็มบวก ($\mathbb{Z}^+$) โดยที่ $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$
3. เซตของจำนวนเต็มลบ ($\mathbb{Z}^-$) โดยที่ $\mathbb{Z}^- = \{-1, -2, -3, \dots\}$
4. เซตของจำนวนเต็มศูนย์ ($\mathbb{Z}^0$) โดยที่ $\mathbb{Z}^0 = \{0\}$
5. เซตของจำนวนธรรมชาติ ($\mathbb{N}$) โดยที่ $\mathbb{N} = \{1, 2, 3, \dots\}$
6. เซตของจำนวนตรรกยะ ($\mathbb{Q}$) โดยที่ $\mathbb{Q} = \left\{ x \mid x = \frac{a}{b} \text{ เมื่อ } a, b \in I \text{ และ } b \neq 0 \right\}$
7. เซตของจำนวนอตรรกยะ ($\mathbb{Q}'$) โดยที่ $\mathbb{Q}' =$ เซตของเลขจำนวนที่ไม่ใช่จำนวนตรรกยะ
8. เซตของจำนวนจริง ($\mathbb{R}$) โดยที่ $\mathbb{R} = \mathbb{Q} \cup \mathbb{Q}'$
9. เซตของจำนวนเชิงซ้อน ($\mathbb{C}$) โดยที่ $\mathbb{C} = \{a + bi \mid a, b \in R \text{ และ } i = \sqrt{-1}\}$

ระบบจำนวนเต็มคือระบบที่ประกอบด้วยจำนวนเต็ม $\mathbb{Z}$ พร้อมกับการดำเนินการบวก (+) และการคูณ ($\cdot$) ที่สอดคล้องกับสัจพจน์แบ่งได้ 3 กลุ่ม ดังนี้

กลุ่มที่ 1 สมบัติทางพีชคณิต(Algebraic Properties)

กลุ่มที่ 2 สมบัติไตรวิภาค(Trichotomy Law)

กลุ่มที่ 3 หลักการจัดอันดับดี(Well ordering Principle)

1. สมบัติทางพีชคณิต

สมบัติการปิด(Closure Property)

สำหรับการบวก : ทุก ๆ $a, b \in \mathbb{Z}$ จะได้ว่า $a + b \in \mathbb{Z}$

สำหรับการคูณ : ทุก ๆ $a, b \in \mathbb{Z}$ จะได้ว่า $a \cdot b \in \mathbb{Z}$

สมบัติการสลับที่(Commutative Property)

สำหรับการบวก : ทุก ๆ $a, b \in \mathbb{Z}$ จะได้ว่า $a + b = b + a$

สำหรับการคูณ : ทุก ๆ $a, b \in \mathbb{Z}$ จะได้ว่า $a \cdot b = b \cdot a$

สมบัติการเปลี่ยนหมู่(Associative Property)

สำหรับการบวก : ทุก ๆ $a, b, c \in \mathbb{Z}$ จะได้ว่า $(a + b) + c = a + (b + c)$

สำหรับการคูณ : ทุก ๆ $a, b, c \in \mathbb{Z}$ จะได้ว่า $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

สมบัติการมีเอกลักษณ์(Identity Property)

สำหรับการบวก : มี $0 \in \mathbb{Z}$ ซึ่ง $a + 0 = a = 0 + a$ ทุก ๆ $a \in \mathbb{Z}$

เรียก 0 ว่าเอกลักษณ์การบวก

สำหรับการคูณ : มี $1 \in \mathbb{Z}$ ซึ่ง $a \cdot 1 = a = 1 \cdot a$ ทุก ๆ $a \in \mathbb{Z}$

เรียก 1 ว่าเอกลักษณ์การคูณ

สมบัติการมีตัวผกผัน(Inverse Property)

สำหรับ $a \in \mathbb{Z}$ จะมี $-a \in \mathbb{Z}$ ซึ่ง $a + (-a) = 0 = (-a) + a$

เรียก $-a$ ว่าตัวผกผันการบวกของ a

สมบัติการแจกแจง(Distributive Property)

สำหรับ $a, b, c \in \mathbb{Z}$ จะได้ว่า $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ และ

$(b + c) \cdot a = (b \cdot a) + (c \cdot a)$

จากสมบัติทางพีชคณิตทั้ง 6 ข้อที่กล่าวมาข้างต้น นำไปพิสูจน์หรือให้เหตุผลดังทฤษฎีบทต่อไปนี

ทฤษฎีบท 1.1 ข้อความต่อไปนี้เป็นจริง

1. ในระบบจำนวนเต็มจะมี 0 เพียงตัวเดียวเท่านั้นที่เป็นสมาชิกเอกลักษณ์ของการบวก
2. ในระบบจำนวนเต็มจะมี 1 เพียงตัวเดียวเท่านั้นที่เป็นสมาชิกเอกลักษณ์ของการคูณ
3. ถ้า $a, b, c \in \mathbb{Z}$ และ $a + b = a + c$ แล้ว $b = c$
4. สำหรับจำนวนเต็ม a ใด ๆ $a(0) = 0 = (0)a$

พิสูจน์

1. สมมติว่ามี $x \in \mathbb{Z}$ ซึ่ง $a + x = a$ สำหรับจำนวนเต็ม a ใด ๆ
 ดังนั้น $0 = 0 + x = x$
 นั่นคือ $x = 0$
2. สมมติว่ามี $x \in \mathbb{Z}$ ซึ่ง $ax = a$ สำหรับจำนวนเต็ม a ใด ๆ
 ดังนั้น $1 = 1x = x$
 นั่นคือ $x = 1$
3. สมมติว่า $a + b = a + c$ และให้ x แทนผกผันการบวกของ a
 จะได้ว่า $b = 0 + b = (x + a) + b = x + (a + b) = x + (a + c)$
 ดังนั้น $b = (x + a) + c = 0 + c = c$
4. ให้ $a \in \mathbb{Z}$ จะได้ $a0 = a(0 + 0) = a0 + a0$
 จะได้ $a0 = a0 + a0$ หรือ $a0 = 0$
 และในทำนองเดียวกัน $0a = (0 + 0)a = 0a + 0a$
 นั่นคือ $0a = 0$

ทฤษฎีบท 1.2 ข้อความต่อไปนี้เป็นจริง

1. สำหรับจำนวนเต็ม a ใด ๆ a จะมีสมาชิกผกผันของการบวกเพียงตัวเดียวเท่านั้น
2. สำหรับจำนวนเต็ม a ใด ๆ ผกผันการบวกของ $-a$ คือ a
3. สำหรับจำนวนเต็ม a, b ใด ๆ จะได้ $(-a)b = a(-b) = -(ab)$
 และ $(-a)(-b) = ab$

พิสูจน์

1. ให้ a เป็นจำนวนเต็ม สมมติว่ามี $b \in \mathbb{Z}$ ซึ่ง $a + b = b + a = 0$
 ดังนั้น $b = b + 0$

$$\begin{aligned}
&= b + [a + (-a)] \\
&= (b + a) + (-a) \\
&= 0 + (-a) \\
&= -a
\end{aligned}$$

นั่นคือ $b = -a$

2. ให้ $a \in \mathbb{Z}$ จะได้ว่า $(-a) + [-(-a)] = (-a) + a = 0$

ดังนั้น $-(-a) = a$

นั่นคือ ผกผันการบวกของ $-a$ คือ a

3. ให้ $a, b \in \mathbb{Z}$ จะได้ว่า

$$ab + (-a)b = [a + (-a)]b = (0)b = 0$$

เนื่องจาก $ab + (-a)b = 0$ ตามนิยามของตัวผกผันการบวก แสดงว่า $(-a)b$ คือตัวผกผันการบวกของ ab ดังนั้น $(-a)b = -(ab)$

$$ab + a(-b) = a[b + (-b)] = a0 = 0$$

เนื่องจาก $ab + a(-b) = 0$ ตามนิยามของตัวผกผันการบวก แสดงว่า $a(-b)$ คือตัวผกผันการบวกของ ab ดังนั้น $a(-b) = -(ab)$

แสดงว่า $(-a)b = a(-b) = -(ab)$

พิจารณา $(-a)b + (-a)(-b) = (-a)[b + (-b)] = (-a)(0) = 0$ แสดงว่า $(-a)(-b)$

คือตัวผกผันการบวกของ $(-a)b$ และเนื่องจาก ab ก็เป็นตัวผกผันการบวกของ $(-a)b$ ด้วย และตัวผกผันการบวกมีได้เพียงตัวเดียวเท่านั้น ดังนั้น ตัวผกผันทั้งสองตัวต้องมีค่าเท่ากัน ดังนั้น $(-a)(-b) = ab$

ทฤษฎีบท 1.3

ให้ $a, b \in \mathbb{Z}$ ถ้า $ab = 0$ แล้ว $a = 0$ หรือ $b = 0$

พิสูจน์

กำหนดให้ $a, b \in \mathbb{Z}$ โดยที่ $ab = 0$ จะพิสูจน์ว่า $a = 0$ หรือ $b = 0$

โดยสมมติให้ $a \neq 0$ แล้วจะแสดงว่า $b = 0$

เนื่องจาก $ab = 0$ และ $a(0) = 0$ (ทฤษฎีบท 1.1 ข้อ 4) จะได้ว่า $ab = a(0)$

เนื่องจาก $a \neq 0$ แสดงว่า $b = 0$

ในทำนองเดียวกัน ถ้าสมมติให้ $b \neq 0$ จะสามารถพิสูจน์ได้ว่า $a = 0$

ดังนั้น จึงสรุปได้ว่า $a = 0$ หรือ $b = 0$

บทแทรก 1.2

ให้ $a, b, c \in \mathbb{Z}$ ถ้า $ab = ac$ และ $a \neq 0$ หรือ $b = c$

พิสูจน์

สมมติว่า $ab = ac$ และ $a \neq 0$ จะได้ว่า $ab = ac = a(b - c) = 0$

ดังนั้น $b - c = 0$

นั่นคือ $b = c$

2. กฎไตรวิภาค

มีสับเซต N ของ $\mathbb{Z}$ คือ $N = \{1, 2, 3, \dots\}$ ที่มีสมบัติว่า

1. $0 \notin N$
2. ถ้า $a, b \in N$ แล้ว $a + b \in N$ และ $ab \in N$
3. ถ้า $x \in \mathbb{Z}$ แล้ว $x \in N$ หรือ $x = 0$ หรือ $-x \in N$

กฎไตรวิภาคในข้างต้นสามารถกำหนดความสัมพันธ์ มากกว่า มากกว่าหรือเท่ากับ น้อยกว่า น้อยกว่าหรือเท่ากับ เขียนแทนด้วย $>, \geq, <, \leq$ ดังบทนิยามต่อไปนี้

บทนิยาม 1.1 สำหรับ $a, b \in \mathbb{Z}$

1. $a > b$ หมายถึง $a - b \in N$
2. $a < b$ หมายถึง $b > a$
3. $a \geq b$ หมายถึง $a - b \in N$ หรือ $a = b$
4. $a \leq b$ หมายถึง $b \geq a$

จากสมบัติข้างต้นจะได้ว่าสำหรับจำนวนเต็ม a, b ใด ๆ นั้นจะมีความสัมพันธ์กันอย่างแน่นอนอย่างใดอย่างหนึ่งเท่านั้น $a > b, a < b$ หรือ $a = b$

ทฤษฎีบท 1.4 ให้ $a, b, c, x, y \in \mathbb{Z}$ จะได้ว่า

1. ถ้า $a > b$ แล้ว $a + c > b + c$
2. ถ้า $a > b$ และ $b > c$ แล้ว $a > c$
3. ถ้า $a > b$ และ $x > y$ แล้ว $a + x > b + y$
4. ถ้า $a > b$ และ $x > 0$ แล้ว $ax > bx$
5. ถ้า $a > b$ และ $x < 0$ แล้ว $ax < bx$

พิสูจน์

1. กำหนดให้ $a > b$ และ $b > c$ จะได้ $a - b \in \mathbb{N}$ และ $b - c \in \mathbb{N}$

$$(a - b) + 0 \in \mathbb{N}$$

$$(a - b) + (c - c) \in \mathbb{N}$$

$$(a + c) - (b + c) \in \mathbb{N}$$

นั่นคือ $a + c > b + c$

2. กำหนดให้ $a > b$ และ $b > c$ จะได้ $a - b \in \mathbb{N}$ และ $b - c \in \mathbb{N}$

$$(a - b) + (b - c) \in \mathbb{N}$$

$$a + (-b + b) - c \in \mathbb{N}$$

$$a - c \in \mathbb{N}$$

นั่นคือ $a > c$

สำหรับการพิสูจน์ข้อที่เหลือจะคล้ายกันกับการพิสูจน์ข้อ 1 และ ข้อ 2

ทฤษฎีบท 1.5 ให้ $a, b, c, x, b \in \mathbb{Z}$ จะได้ว่า

1. ถ้า $a < b$ แล้ว $a + b < b + c$
2. ถ้า $a < b$ และ $b < c$ แล้ว $a < c$
3. ถ้า $a < b$ และ $x < y$ แล้ว $a + x < b + y$
4. ถ้า $a < b$ และ $x > 0$ แล้ว $ax < bx$
5. ถ้า $a < b$ และ $x < 0$ แล้ว $ax > bx$

พิสูจน์

สำหรับการพิสูจน์จะคล้ายกันทฤษฎีบท 1.4

3. หลักการจัดอันดับดี

หลักการจัดอันดับดีมีบทบาทสำคัญที่ใช้ในการพิสูจน์ในบทต่อ ๆ ไป จึงขอกล่าวไว้ในหัวข้อนี้พร้อมกับตัวอย่าง ดังนี้

ให้ $S \subseteq \mathbb{N}$ และ $S \neq \emptyset$ จะได้ว่ามี $x \in S$ ซึ่ง $x \leq a$ สำหรับทุก $a \in S$

สมบัติของการจัดอันดับดีในระบบจำนวนเต็ม นำไปสู่ทฤษฎีบทที่น่าสนใจ ซึ่งสามารถนำไปประยุกต์ใช้ในการพิสูจน์ทฤษฎีบทต่าง ๆ ดังต่อไปนี้

ทฤษฎีบท 1.6

ไม่มีจำนวนเต็มใดอยู่ระหว่าง 0 และ 1

พิสูจน์

ให้ $T = \{a \in \mathbb{Z} \mid 0 < a < 1\}$ และสมมติ $T \neq \emptyset$

จากหลักการจัดอันดับดี จะได้ว่ามี $m \in T$ ซึ่ง $m \leq x$ สำหรับทุก $x \in T$

ดังนั้น $0 < m < 1$ เมื่อนำ m (ซึ่งเป็นจำนวนจริงบวก) คูณตลอดสมการจะได้

$0 < m^2 < m$ เนื่องจาก m เป็นจำนวนเต็ม ดังนั้น m^2 จึงเป็นจำนวนเต็มด้วย

ทำให้ได้ว่า m^2 เป็นสมาชิกของ T ที่มีค่าน้อยกว่า m

จึงเกิดข้อขัดแย้งในการเลือก m นั่นคือ ที่เป็นจำนวนเต็มบวกที่น้อยที่สุดใน T

ดังนั้นจึงสรุปได้ว่า $T = \emptyset$ หรือ ไม่มีจำนวนเต็มใดอยู่ระหว่าง 0 และ 1

ทฤษฎีบท 1.7 สมบัติของอาร์คิมิดีส(Archimedean Property)

สำหรับจำนวนเต็มบวก a และ b จะมีจำนวนเต็มบวก n ซึ่ง $na \geq b$

พิสูจน์

สมมติว่าข้อความในทฤษฎีบทไม่จริง

นั่นคือ มีจำนวนเต็มบวก a, b และทุก ๆ จำนวนเต็มบวก $n, na < b$

ให้ $S = \{b - na \mid n \in \mathbb{N}\}$ จากสมมติฐานจะเห็นว่า $S \subseteq \mathbb{N}$ และ $S \neq \emptyset$

จากหลักการจัดอันดับดีจะมี $k \in \mathbb{N}$ ซึ่ง $m = b - ka$ ที่ m เป็นจำนวนเต็มบวก

ที่น้อยที่สุดใน S จาก $b - (k+1)a \in S$ และ $[b - (k+1)a] - [b - ka] = -a < 0$

ดังนั้น $b - (k+1)a < b - ka$

จึงเกิดข้อขัดแย้งในการเลือก $m = b - ka$ ที่เป็นสมาชิกที่น้อยที่สุดใน S

สำหรับหลักการจัดอันดับดียังนำไปสู่ทฤษฎีบทที่สำคัญที่ใช้เพื่อพิสูจน์ข้อความต่าง ๆ ที่เกี่ยวข้องกับจำนวนเต็มบวกเรียกทฤษฎีบทนี้ว่า หลักอุปนัยเชิงคณิตศาสตร์ซึ่งจะกล่าวในหัวข้อถัดไป

1.3 การพิสูจน์เบื้องต้น

ในหัวข้อนี้จะกล่าวถึงพื้นฐานทางตรรกศาสตร์ และระเบียบวิธีการพิสูจน์เบื้องต้นเพื่อนำไปใช้เป็นเครื่องมือในการศึกษาทฤษฎีจำนวนในบทต่อ ๆ ไป เริ่มต้นด้วยประโยคหรือข้อความที่น่าสนใจทางคณิตศาสตร์เป็นข้อความที่ตัดสินใจได้ว่า ต้องเป็นจริงหรือเป็นเท็จอย่างใดอย่างหนึ่งเท่านั้นจะเป็นทั้งสองอย่างไม่ได้ กล่าวคือถ้าข้อความใดไม่เป็นจริงแล้วข้อความนั้นต้องเป็นเท็จ ในทางกลับกันถ้าข้อความใดไม่เป็นเท็จแล้วข้อความนั้น ต้องเป็นจริง การพิสูจน์ในเอกสารหรือตำราเล่มอื่นอาจใช้

จำนวน วิธีการพิสูจน์ที่แตกต่างกัน สำหรับในตำราเล่มนี้ผู้เขียนจะนำเสนอวิธีการพิสูจน์ไว้ทั้งหมด 7 วิธีดังต่อไปนี้

1. การพิสูจน์ข้อความแบบมีเงื่อนไข
2. การพิสูจน์โดยการแจกแจงกรณี
3. การพิสูจน์ข้อความแบบผันกลับได้
4. การพิสูจน์ข้อความเลือก
5. การพิสูจน์ข้อความซึ่งเป็นไปได้อย่างเดียว
6. การพิสูจน์โดยการยกตัวอย่างค้าน
7. การพิสูจน์โดยหลักอุปนัยเชิงคณิตศาสตร์

1. การพิสูจน์ข้อความแบบมีเงื่อนไข

การพิสูจน์ข้อความที่อยู่ในรูปแบบมีเงื่อนไข $p \rightarrow q$ ซึ่งการพิสูจน์ในรูปแบบนี้ต้องการแสดงว่าข้อความ $p \rightarrow q$ เป็นจริงทุก ๆ กรณีหรือเป็นสัจนิรันดร์ นั่นคือแสดงว่าถ้า p เป็นจริง แล้ว q เป็นจริงเสมอ เขียนเป็น โครงพิสูจน์ได้ดังนี้

สมมติ p เป็นจริง

⋮

ดังนั้น q เป็นจริง(ข้อสรุป)

เรียกวิธีนี้ว่าการพิสูจน์โดยวิธีตรง ในส่วนที่ว่างเว้นไว้คือส่วนที่จะเติมรายละเอียดให้สมบูรณ์อาจจะได้จากนิยาม ทฤษฎีบทที่พิสูจน์มาก่อนหน้า หรือสัจพจน์ เพื่อให้นำไปสู่ข้อสรุปอย่างเป็นเหตุเป็นผลกัน เมื่อพิสูจน์โดยวิธีตรงไม่ได้โดยจะใช้หลักการสมมูลที่ว่า $p \rightarrow q \equiv \sim q \rightarrow \sim p$ เรียกว่า การพิสูจน์โดยวิธีการแย้งสลับที่มีโครงการพิสูจน์ดังนี้

สมมติ $\sim q$ เป็นจริง

⋮

ดังนั้น $\sim p$ เป็นจริง(ข้อสรุป)

ก่อนจะให้ตัวอย่างการพิสูจน์ในรูปแบบนี้จะให้บทนิยามเพื่อนำไปใช้ในการพิสูจน์ดังนี้

บทนิยาม 1.2

a เป็นจำนวนคู่ ถ้ามีจำนวนเต็ม k ซึ่ง $a = 2k$ และจำนวนคี่ คือจำนวนเต็มที่ ไม่ใช่จำนวนคู่ หรือจะกล่าวว่า a เป็นจำนวนคี่ถ้ามีจำนวนเต็ม k ซึ่ง $a = 2k + 1$

ตัวอย่าง 1.1 จงพิสูจน์ว่า ถ้า n เป็นจำนวนคู่ แล้ว n^2 เป็นจำนวนคู่
 พิสูจน์ข้อความ ถ้า n เป็นจำนวนคู่ แล้ว n^2 เป็นจำนวนคู่
 เขียนโครงการพิสูจน์ได้ดังนี้

สมมติ n เป็นจำนวนคู่

$\vdots$

ดังนั้น n^2 เป็นจำนวนคู่

พิสูจน์ ให้ n เป็นจำนวนคู่จะได้ว่ามีจำนวนเต็ม k ซึ่ง $n = 2k$ จะได้

$$n^2 = (2k)^2 = 4k^2 = 2(2k^2)$$

ให้ $p = 2k^2$ เนื่องจาก k เป็นจำนวนเต็มดังนั้น p เป็นจำนวนเต็ม นั่นคือมีจำนวนเต็ม p
 ซึ่งทำให้ $n^2 = 2p$ จึงสรุปได้ว่า n^2 เป็นจำนวนคู่

ตัวอย่าง 1.2 จงพิสูจน์ว่า ถ้า n^2 เป็นจำนวนคู่ แล้ว n เป็นจำนวนคู่
 พิสูจน์ข้อความ ถ้า n^2 เป็นจำนวนคู่แล้ว n เป็นจำนวนคู่
 พิสูจน์โดยวิธีการแย้งกลับ
 พิสูจน์ข้อความ ถ้า n เป็นจำนวนคี่แล้ว n^2 เป็นจำนวนคี่
 เขียนโครงการพิสูจน์ได้ดังนี้

สมมติ n เป็นจำนวนคี่

$\vdots$

ดังนั้น n^2 เป็นจำนวนคี่

พิสูจน์ ให้ n เป็นจำนวนคี่จะได้ว่ามีจำนวนเต็ม k ซึ่ง $n = 2k + 1$ จะได้

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

ให้ $p = 2k^2 + 2k$ เนื่องจาก k เป็นจำนวนเต็ม ดังนั้น p เป็นจำนวนเต็ม
 นั่นคือมีจำนวนเต็ม p ซึ่งทำให้ $n^2 = 2p + 1$ จึงสรุปได้ว่า n^2 เป็นจำนวนคี่

2. การพิสูจน์โดยการแจกแจงกรณี

การพิสูจน์ข้อความในรูปแบบ $(p \vee q) \rightarrow r$ เนื่องจาก

$$(p \vee q) \rightarrow r \equiv (p \rightarrow r) \wedge (q \rightarrow r)$$

จึงต้องพิสูจน์ว่า $p \rightarrow r$ และ $q \rightarrow r$ ทั้งสองกรณีเป็นจริงทั้งคู่

ตัวอย่าง 1.3 จงพิสูจน์ว่า ถ้า a เป็นจำนวนเต็มแล้ว $a^2 + 3a$ เป็นจำนวนคู่

a เป็นจำนวนเต็มแยกได้เป็นสองกรณี คือ a เป็นจำนวนคู่ หรือ a เป็นจำนวนคี่

ดังนั้นการพิสูจน์จึงแยกเป็นสองกรณีคือ

กรณีที่ 1. a เป็นจำนวนคู่ แล้ว $a^2 + 3a$ เป็นจำนวนคู่ และ

กรณีที่ 2. a เป็นจำนวนเต็มคี่ แล้ว $a^2 + 3a$ เป็นจำนวนคู่

พิสูจน์

- 1 ถ้า a เป็นจำนวนคู่จะได้ว่ามีจำนวนเต็ม k ซึ่ง $a = 2k$ แล้ว

$$\begin{aligned} a^2 + 3a &= (2k)^2 + 3(2k) \\ &= 4k^2 + 6k \\ &= 2(2k^2 + 3k) \end{aligned}$$

ให้ $p = 2k^2 + 3k$ เนื่องจาก k เป็นจำนวนเต็ม ดังนั้น p เป็นจำนวนเต็ม

นั่นคือมีจำนวนเต็ม p ซึ่งทำให้ $a^2 + 3a = 2p$

จึงสรุปได้ว่า $a^2 + 3a$ เป็นจำนวนคู่

- 2 ถ้า a เป็นจำนวนคี่จะได้ว่ามีจำนวนเต็ม k ซึ่ง $a = 2k + 1$ แล้ว

$$\begin{aligned} a^2 + 3a &= (2k + 1)^2 + 3(2k + 1) \\ &= 4k^2 + 4k + 1 + 6k + 3 \\ &= 4k^2 + 10k + 4 \\ &= 2(2k^2 + 5k + 2) \end{aligned}$$

ให้ $p = 2k^2 + 5k + 2$ เนื่องจาก k เป็นจำนวนเต็ม

ดังนั้น p เป็นจำนวนเต็ม นั่นคือมีจำนวนเต็ม p ซึ่งทำให้ $a^2 + 3a = 2p$

จึงสรุปได้ว่า $a^2 + 3a$ เป็นจำนวนคู่

3. การพิสูจน์ข้อความแบบผันกลับได้

การพิสูจน์ข้อความในรูปแบบ $p \leftrightarrow q$ เนื่องจาก

$$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$$

จึงต้องพิสูจน์ว่า $p \rightarrow q$ และ $q \rightarrow p$ ทั้งสองกรณีเป็นจริงทั้งคู่

ตัวอย่าง 1.4 จงพิสูจน์ว่า k^2 เป็นจำนวนคู่ ก็ต่อเมื่อ $k + 1$ เป็นจำนวนเต็มคี่

การพิสูจน์จึงแยกเป็นสองกรณีคือ

กรณีที่ 1. ถ้า k^2 เป็นจำนวนคู่แล้ว $k + 1$ เป็นจำนวนเต็มคี่

กรณีที่ 2. ถ้า $k + 1$ เป็นจำนวนเต็มคี่แล้ว k^2 เป็นจำนวนคู่

- 1 พิสูจน์โดยใช้ข้อความแย้งสลับที่

ถ้า $k + 1$ ไม่เป็นจำนวนเต็มคี่แล้ว k^2 ไม่เป็นจำนวนคู่

ให้ $k + 1$ ไม่เป็นจำนวนเต็มคี่จะได้ว่า $k + 1$ เป็นจำนวนคู่

จะได้ว่ามีจำนวนเต็ม m ซึ่ง $k + 1 = 2m$ แล้ว

$$k + 1 = 2m$$

$$k = 2m - 1$$

$$\begin{aligned} k^2 &= (2m - 1)^2 \\ &= 4m^2 - 4m + 1 \\ &= 2(m^2 - 2m) + 1 \end{aligned}$$

ให้ $p = m^2 - 2m$ เนื่องจาก m เป็นจำนวนเต็มดังนั้น p เป็นจำนวนเต็ม
นั่นคือมีจำนวนเต็ม p ซึ่งทำให้ $k^2 = 2p + 1$ แสดง k^2 เป็นจำนวนเต็มคี่
ดังนั้น k^2 ไม่เป็นจำนวนคู่

2 ให้ $k + 1$ เป็นจำนวนเต็มก็จะได้ว่ามีจำนวนเต็ม m ซึ่ง $k + 1 = 2m + 1$

$$k + 1 = 2m + 1$$

$$k = 2m$$

$$\begin{aligned} k^2 &= (2m)^2 \\ &= 4m^2 \\ &= 2(2m^2) \end{aligned}$$

ให้ $p = 2m^2$ เนื่องจาก m เป็นจำนวนเต็มดังนั้น p เป็นจำนวนเต็ม
นั่นคือมีจำนวนเต็ม p ซึ่งทำให้ $k^2 = 2p$ แสดง k^2 เป็นจำนวนเต็มคู่
ดังนั้น k^2 ไม่เป็นจำนวนคี่

4. การพิสูจน์ข้อความเลือก

การพิสูจน์ข้อความในรูปแบบ $p \vee q$ เนื่องจาก

$$p \vee q \equiv \sim p \rightarrow q \text{ และ } p \vee q \equiv \sim q \rightarrow p$$

จึงต้องพิสูจน์ว่า $\sim p \rightarrow q$ หรือ $\sim q \rightarrow p$

สำหรับการพิสูจน์ประโยค $r \rightarrow (p \vee q)$ เนื่องจาก

$$r \rightarrow (p \vee q) \equiv (r \wedge \sim p) \rightarrow q \text{ หรือ } r \rightarrow (p \vee q) \equiv (r \wedge \sim q) \rightarrow p$$

จึงต้องพิสูจน์ว่า $(r \wedge \sim p) \rightarrow q$ หรือ $(r \wedge \sim q) \rightarrow p$

ตัวอย่าง 1.5 ให้ ab เป็นจำนวนคู่ จงพิสูจน์ว่า a เป็นจำนวนคู่หรือ b เป็นจำนวนคู่

การพิสูจน์ข้อความ ab เป็นจำนวนคู่ $\rightarrow (a$ เป็นจำนวนคู่ $\vee b$ เป็นจำนวนคู่)

มีโครงการพิสูจน์ดังนี้

สมมติ ab เป็นจำนวนคู่ และ a ไม่เป็นจำนวนคู่

$\vdots$

ดังนั้น b เป็นจำนวนคู่

พิสูจน์ ให้ ab เป็นจำนวนคู่จะได้ว่ามีจำนวนเต็ม l ซึ่ง

$$ab = 2l$$

และ a ไม่เป็นจำนวนคู่แสดงว่า a เป็นจำนวนเต็มคี่ จะได้ว่ามีจำนวนเต็ม k ซึ่ง

$$a = 2k + 1 \text{ และ } ab = 2kb + b \text{ จะได้}$$

$$2l = 2kb + b$$

$$b = 2l - 2kb$$

$$= 2(l - kb)$$

ให้ $p = l - kb$ เนื่องจาก k และ b เป็นจำนวนเต็ม ดังนั้น p เป็นจำนวนเต็ม

นั่นคือมีจำนวนเต็ม p ซึ่งทำให้ $b = 2p$ จึงสรุปได้ว่า b เป็นจำนวนคู่

5. การพิสูจน์ข้อความซึ่งเป็นไปได้โดยตรง

การพิสูจน์ข้อความ $\exists! x \in U, p(x)$ อ่านว่า มี x ใน U เพียงตัวเดียวเท่านั้นที่สอดคล้อง $p(x)$ ดังนั้นการพิสูจน์ $\exists! x \in U, p(x)$ แบ่งการพิสูจน์ออกเป็น 2 ขั้นตอนคือ

ขั้นที่ 1 มีอย่างน้อยหนึ่งตัว(Existence) ต้องแสดงว่ามี x อยู่จริง

$$\exists x \in U, p(x)$$

ขั้นที่ 2 มีเพียงตัวเดียว(Uniqueness) ต้องแสดงว่าถ้ามีตัวอื่นที่เป็นจริงเหมือนกัน(สมมติให้เป็น y) ตัวนั้นต้องเท่ากับ x

$$\forall y \in U, [p(y) \rightarrow y = x]$$

ตัวอย่าง 1.6 จงพิสูจน์ว่า มีจำนวนจริง x เพียงตัวเดียวเท่านั้นซึ่ง $2^x = 1$

เขียนสัญลักษณ์ได้ $\exists! x \in \mathbb{R}, 2^x = 1$

ขั้นที่ 1 มีอย่างน้อยหนึ่งตัว เลือก $x = 0$ จะได้ว่า

$$2^x = 2^0 = 1$$

ขั้นที่ 2 มีเพียงตัวเดียว ให้ $x, y \in \mathbb{R}$ สมมติ $2^x = 1$ และ $2^y = 1$ จะได้

$$2^x = 2^y$$

จากสมบัติของเลขยกกำลังจะได้ว่า $x = y$

ตัวอย่าง 1.7 จงพิสูจน์ว่า ทุก ๆ จำนวนจริง x จะมีจำนวนจริง y เพียงตัวเดียวซึ่ง $x + y = 1$

เขียนสัญลักษณ์ได้ $\forall x, \exists! y \in \mathbb{R}, x + y = 1$

ขั้นที่ 1 มีอย่างน้อยหนึ่งตัว เลือก $y = 1 - x$ ซึ่ง $y \in \mathbb{R}, x + y = 1$ จะได้ว่า

$$x + y = x + (1 - x) = 1$$

ขั้นที่ 2 มีเพียงตัวเดียว ให้ $y, z \in \mathbb{R}$ สอดคล้อง $x + y = 1$ และ $x + z = 1$ จะได้

$$x + y = 1 = x + z$$

จากสมบัติการตัดออกของการบวกบนจำนวนจริงจะได้ว่า $y = z$

6. การพิสูจน์โดยการยกตัวอย่างค้าน

การพิสูจน์ประพจน์บ่งปริมาณที่มีคำว่า “ทั้งหมด” เช่น $\forall x, p(x)$ ว่าเป็นเท็จสามารถทำได้โดยการหาสมาชิกหนึ่งตัวจากเอกภพสัมพัทธ์มาแทนตัวแปร x แล้วทำให้ $p(x)$ เป็นเท็จ ก็เป็นการเพียงพอแล้วเรียกการพิสูจน์นี้ว่า การพิสูจน์ว่าเท็จโดยการยกตัวอย่างค้าน

ตัวอย่าง 1.8 จงพิสูจน์ว่า $\forall x$, ถ้า x เป็นจำนวนเฉพาะแล้ว x เป็นจำนวนคี่ เป็นเท็จ
เนื่องจาก มี 2 ที่เป็นจำนวนเฉพาะ และ 2 เป็นไม่เป็นจำนวนคี่ นั่นคือ 2 เป็นจำนวนคู่

7. การพิสูจน์โดยหลักอุปนัยเชิงคณิตศาสตร์

พิจารณาผลรวมของจำนวนต่อไปนี้

$$1 = 1$$

$$1 + 2 = 3$$

$$1 + 2 + 3 = 6$$

$$1 + 2 + 3 + 4 = 10$$

$$1 + 2 + 3 + 4 + 5 = 15$$

จากผลรวมดังกล่าวสรุปข้อคาดเดาได้ว่า

$$1 + 2 + 3 + 4 + 5 + 6 + \cdots + n = \frac{n(n+1)}{2}$$

สำหรับจำนวนเต็มบวก ใดๆ ซึ่งจากข้อความคาดเดานี้ สามารถพิสูจน์ได้ตามวิธีการทางคณิตศาสตร์ โดยใช้หลักอุปนัยเชิงคณิตศาสตร์ด้วยการพิสูจน์ข้อความที่มีเอกภพสัมพัทธ์เป็นจำนวนนับ โดยจะแบ่งการพิสูจน์ออกเป็น 2 แบบคือ หลักอุปนัยเชิงคณิตศาสตร์แบบที่ 1 (อุปนัยเชิงคณิตศาสตร์แบบอ่อน) และหลักอุปนัยเชิงคณิตศาสตร์แบบที่ 2 (อุปนัยเชิงคณิตศาสตร์แบบเข้ม) โดยมีทฤษฎีบทดังต่อไปนี้

ทฤษฎีบท 1.8 (หลักอุปนัยเชิงคณิตศาสตร์แบบที่ 1)

ให้ $S \subseteq \mathbb{N}$ ที่มีคุณสมบัติดังนี้

$$1. 1 \in S$$

$$2. \text{ สำหรับทุก } k \in \mathbb{N} \text{ ถ้า } k \in S \text{ แล้ว } k+1 \in S$$

จะได้ว่า $S = \mathbb{N}$

พิสูจน์

กำหนดให้ $S \subseteq \mathbb{N}$ ที่มีสมบัติว่า $1 \in S$ และถ้า $k \in S$ แล้ว $k+1 \in S$

พิจารณาเซต $T = \mathbb{N} - S$

สมมติให้ T ไม่ใช่เซตว่าง เนื่องจาก $T \subseteq \mathbb{N}$

จากหลักการจัดอันดับดีจะได้ว่า T มีสมาชิกค่าน้อยที่สุด สมมติให้เป็น m

เนื่องจาก 1 เป็นจำนวนเต็มบวกที่มีค่าน้อยที่สุด

เนื่องจาก $1 \in S$ ดังนั้น $1 < m$ จะได้ว่า $0 < m - 1 < m$

เนื่องจาก m เป็นสมาชิกที่น้อยที่สุดของ T จะได้ว่า $m - 1 \notin T$

ดังนั้น $m - 1 \in S$

จะได้ว่า $(m - 1) + 1 \in S$ ดังนั้น $m \in S$ จึงเกิดข้อขัดแย้งกับที่สมมติให้ $m \in T$

ที่สมมติให้ T ไม่ใช่เซตว่างจึงเป็นไปไม่ได้ นั่นคือ $S = \mathbb{N}$

การนำหลักอุปนัยเชิงคณิตศาสตร์แบบที่ 1 ไปพิสูจน์ข้อความในรูปแบบ $\forall x, \mathbb{N}, P(n)$ โดยกำหนดให้ $S = \{n \in \mathbb{N} \mid P(n) \text{ เป็นจริง} \}$ ดังนั้น ถ้าเราสามารถแสดงได้ว่า $1 \in S$ หรือ $P(1)$ เป็นจริง และสำหรับจำนวนนับ k ใด ๆ จะต้องแสดงว่าถ้า $P(k)$ เป็นจริง แล้ว $P(k + 1)$ เป็นจริง ดังนั้นโดยหลักอุปนัยเชิงคณิตศาสตร์แบบที่ 1 จะต้องแสดง 2 ขั้นตอนดังนี้

1. ขั้นฐาน : $P(1)$ เป็นจริง
2. ขั้นอุปนัย : สำหรับจำนวนนับ k ถ้า $P(k)$ เป็นจริง แล้ว $P(k + 1)$ เป็นจริง

ตัวอย่าง 1.9 จงแสดงว่า $1 + 2 + 3 + \dots + n = \frac{n(n + 1)}{2}$ สำหรับทุกจำนวนนับ n

วิธีทำ ให้ $n \in \mathbb{N}$ และ $P(n)$ แทนข้อความ

$$1 + 2 + 3 + \dots + n = \frac{n(n + 1)}{2}$$

1. ขั้นฐาน

$$1 = \frac{1(1 + 1)}{2} = 1 \text{ ดังนั้น } P(1) \text{ เป็นจริง}$$

2. ขั้นอุปนัย

ให้ $k \in \mathbb{N}$ สมมติ $P(k)$ เป็นจริง นั่นคือ

$$1 + 2 + 3 + \dots + k = \frac{k(k + 1)}{2} \text{ เป็นจริง}$$

โดยสมมติฐาน จะได้ว่า

$$\begin{aligned} 1 + 2 + 3 + \dots + k + (k + 1) &= \frac{k(k + 1)}{2} + (k + 1) \\ &= \frac{k(k + 1) + 2(k + 1)}{2} \\ &= \frac{(k + 1)[(k + 2)]}{2} \end{aligned}$$

$$= \frac{(k+1)[(k+1)+1]}{2}$$

ทำให้สรุปได้ว่า $P(k+1)$ เป็นจริง

ดังนั้น $1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$ สำหรับทุกจำนวนนับ n

ตัวอย่าง 1.10 จงแสดงว่า $1 + 3 + 5 + \dots + (2n-1) = n^2$ สำหรับทุกจำนวนนับ n

วิธีทำ ให้ $n \in \mathbb{N}$ และ $P(n)$ แทนข้อความ

$$1 + 3 + 5 + \dots + (2n-1) = n^2$$

1. ขั้นฐาน

$$1 = (2(1)-1) = 1 \text{ ดังนั้น } P(1) \text{ เป็นจริง}$$

2. ขั้นอุปนัย

ให้ $k \in \mathbb{N}$ สมมติ $P(k)$ เป็นจริง นั่นคือ

$$1 + 3 + 5 + \dots + (2k-1) = k^2 \text{ เป็นจริง}$$

โดยสมมติฐาน จะได้ว่า

$$\begin{aligned} 1 + 3 + 5 + \dots + (2k-1) + (2(k+1)-1) &= k^2 + (2(k+1)-1) \\ &= k^2 + 2k + 2 \\ &= (k+1)^2 \end{aligned}$$

ทำให้สรุปได้ว่า $P(k+1)$ เป็นจริง

ดังนั้น $1 + 3 + 5 + \dots + (2n-1) = n^2$ สำหรับทุกจำนวนนับ n

ตัวอย่าง 1.11 จงแสดงว่า $\forall n \in \mathbb{N}, 2^n < 2^{n+1}$

วิธีทำ ให้ $n \in \mathbb{N}$ และ $P(n)$ แทนข้อความ

$$2^n < 2^{n+1}$$

1. ขั้นฐาน

เนื่องจาก $2^1 < 2^2$ ดังนั้น $P(1)$ เป็นจริง

2. ขั้นอุปนัย

ให้ $k \in \mathbb{N}$ สมมติ $P(k)$ เป็นจริง นั่นคือ $2^k < 2^{k+1}$ เป็นจริง

จะได้ว่า

$$2^{k+1} = 2 \cdot 2^k < 2 \cdot 2^{k+1} = 2^{k+2} = 2^{(k+1)+1}$$

ทำให้สรุปได้ว่า $P(k+1)$ เป็นจริง

ดังนั้น $\forall n \in \mathbb{N}, 2^n < 2^{n+1}$ เป็นจริง

อุปนัยเชิงคณิตศาสตร์แบบแบบที่ 1 ในบางครั้งไม่เพียงพอที่จะนำไปพิสูจน์บางข้อความได้ อุปนัยเชิงคณิตศาสตร์อีกแบบหนึ่งคืออุปนัยเชิงคณิตศาสตร์แบบที่ 2 หรือเรียกอีกชื่อว่าอุปนัยเชิงคณิตศาสตร์แบบเข้มโดยมีข้อแตกต่างจากทฤษฎีบท 1.18 เพียงเล็กน้อย แต่ก็สามารถนำไปใช้ในการพิสูจน์ได้กว้างขวางเช่นกัน ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 1.9 (หลักอุปนัยเชิงคณิตศาสตร์แบบที่ 2)

ให้ $S \subseteq \mathbb{N}$ ที่มีคุณสมบัติดังนี้

1. $1 \in S$

2. ถ้า k เป็นจำนวนเต็มบวกซึ่ง $2, 3, 4, \dots, k \in S$ แล้ว $k + 1 \in S$

จะได้ว่า $S = \mathbb{N}$

พิสูจน์ การพิสูจน์คล้ายทฤษฎีบท 1.8

การนำหลักอุปนัยเชิงคณิตศาสตร์แบบที่ 2 ไปพิสูจน์ข้อความ ไปพิสูจน์ข้อความในรูปแบบ $\forall x \in \mathbb{N}, P(n)$ โดยกำหนดให้ $S = \{n \in \mathbb{N} \mid P(n) \text{ เป็นจริง} \}$ กำหนดให้ $P(n)$ เป็นประพจน์ที่เกี่ยวข้องกับจำนวนเต็มบวก n ดังนั้นโดยหลักอุปนัยเชิงคณิตศาสตร์แบบที่ 2 จะต้องแสดง 2 ขั้นตอนดังนี้

1. ขั้นฐาน : $P(a)$ เป็นจริง

2. ขั้นอุปนัย : ถ้า $P(a), P(a + 1), P(a + 2), \dots, P(k)$ เป็นจริงแล้ว $P(k + 1)$

จะได้ว่า $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n ที่ $n \geq a$

ตัวอย่าง 1.12 พิจารณาลำดับ $1, 3, 4, 7, 11, 18, 29, 47, \dots$ ให้ $a_1 = 1, a_2 = 3$ และ

$a_n = a_{n-1} + a_{n-2}$ สำหรับทุกจำนวนเต็มบวก n ที่ $n \geq 3$ จงพิสูจน์ว่า $a_n < \left(\frac{7}{4}\right)^n$ เป็นจริง

สำหรับทุกจำนวนเต็มบวก n

วิธีทำ ให้ $P(n)$ แทน $a_n < \left(\frac{7}{4}\right)^n$

1. ขั้นฐาน

$$a_1 = 1 < \frac{7}{4}$$

$$a_2 = 3 < \left(\frac{7}{4}\right)^2$$

$$a_3 = a_2 + a_1 = 4 < \left(\frac{7}{4}\right)^3$$

ดังนั้น $P(1), P(2), P(3)$ เป็นจริง

2. ขั้นอุปนัย

สมมติให้ $P(4), P(5), P(6), \dots, P(k)$ เป็นจริง นั่นคือ $a_k < \left(\frac{7}{4}\right)^k$

จะแสดงว่า $P(k+1)$ เป็นจริงด้วย นั่นคือจะแสดงว่า $a_{k+1} < \left(\frac{7}{4}\right)^{k+1}$

พิจารณา

$$\begin{aligned} a_{k+1} &= a_k + a_{k-1} \\ &< \left(\frac{7}{4}\right)^k + \left(\frac{7}{4}\right)^{k-1} \\ &= \left(\frac{7}{4}\right)^{k-1} \left[\frac{7}{4} + 1 \right] \\ &= \left(\frac{7}{4}\right)^{k-1} \left[\frac{11}{4} \right] \\ &< \left(\frac{7}{4}\right)^{k-1} \left(\frac{7}{4}\right)^2 = \left(\frac{7}{4}\right)^{k+1} \end{aligned}$$

ทำให้สรุปได้ว่า $P(k+1)$ เป็นจริง

ดังนั้น $a_n < \left(\frac{7}{4}\right)^n$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n

1.4 ข้อเสนอแนะบางประการเกี่ยวกับจำนวนเต็ม

ก่อนที่จะศึกษาเนื้อหาหลักในทฤษฎีจำนวนนั้น ก่อนอื่นผู้เขียนจะความรู้เกี่ยวกับสัญลักษณ์และสมบัติที่สำคัญเกี่ยวกับจำนวนเต็มดังต่อไปนี้

1. ให้ a และ d เป็นจำนวนเต็มใด ๆ $a, a+d, a+2d, a+3d, \dots, a+(n-1)d, \dots$

เรียกลำดับจำนวนดังกล่าวนี้ว่า ลำดับเลขคณิต(Arithmetic Sequence) เรียก a ว่า พจน์แรก เรียก d ว่า ผลต่างร่วม

ตัวอย่าง 1.13

ลำดับ $3, 5, 7, 9, 11, 13, \dots$ เป็นลำดับเลขคณิต

ที่มี $a = 3$ และ $d = 2$

2. ให้ a และ r เป็นจำนวนเต็มใด ๆ และ $a, ar, ar^2, ar^3, \dots, ar^{n-1}, \dots$ เรียกลำดับจำนวนนี้ว่า ลำดับเรขาคณิต(Geometric Sequence) เรียก a ว่า พจน์แรก เรียก r ว่า อัตราส่วนร่วม

ตัวอย่าง 1.14

ลำดับ $5, -15, 45, -135, \dots$ เป็นลำดับเรขาคณิต

ที่มี $a = 5$ และ $r = -3$

3. ผลบวก n พจน์แรกของลำดับเลขคณิต

$$a + (a + d) + (a + 2d) + \dots + (a + (n - 1)d) = \frac{n}{2}[2a + (n - 1)d]$$

และผลบวก n พจน์แรกของลำดับเรขาคณิต

$$a + ar + ar^2 + ar^3 + \dots + ar^{n-1} = \frac{a(r^n - 1)}{r - 1}$$

ตัวอย่าง 1.15

$$2 + 4 + 6 + 8 + 10 + \dots + 400 = \frac{200}{2}[2(2) + (200 - 1)2] = 40,200$$

$$3 + 3 \cdot 2 + 3 \cdot 2^2 + 3 \cdot 2^3 + \dots + 3 \cdot 2^{25} = \frac{3(2^{26} - 1)}{2 - 1} = 3(2^{26} - 1)$$

4. สัญลักษณ์แทนการบวก คือสัญลักษณ์ “ $\sum$ ” อ่านว่า ซิกมา ซึ่งมีความหมายดังนี้

$$\sum_{k=1}^n a_k = a_1 + a_2 + a_3 + \dots + a_n$$

ตัวอย่าง 1.16

$$\sum_{k=1}^4 (2k + 1) = (2 \cdot 1 + 1) + (2 \cdot 2 + 1) + (2 \cdot 3 + 1) + (2 \cdot 4 + 1)$$

การใช้สัญลักษณ์ “ $\sum$ ” นี้ อาจไม่เริ่มที่ 1 ก็ได้ เช่น

$$\sum_{k=m}^n a_k = a_m + a_{m+1} + a_{m+2} + \dots + a_n, \quad m \leq n$$

$$\sum_{k=3}^5 k^2 = 3^2 + 4^2 + 5^2 = 50$$

$$\sum_{k=0}^2 3^k = 3^0 + 3^1 + 3^2 = 13$$

$$\sum_{k=-2}^1 k^3 = (-2)^3 + (-1)^3 + (0)^3 + (1)^3 = -8$$

5. สัญลักษณ์แทนการคูณ คือสัญลักษณ์ “ Π ” อ่านว่า พาย (Pi) ซึ่งมีความหมายดังนี้

$$\prod_{j=1}^n a_j = a_1 \cdot a_2 \cdot a_3 \dots a_n$$

ตัวอย่าง 1.17

$$\prod_{j=1}^5 j = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$$

$$\prod_{j=1}^5 2 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^5 = 32$$

$$\prod_{j=1}^5 2^j = 2 \cdot 2^2 \cdot 2^3 \cdot 2^4 \cdot 2^5 = 2^{15}$$

$$\prod_{k=1}^n k = 1 \cdot 2 \cdot 3 \cdot 4 \dots (n-2)(n-1)(n) = n!$$

สัญลักษณ์ $n!$ เป็นสัญลักษณ์ที่อ่านว่า n แฟกทอเรียล โดยมีความหมายว่า $n! = n(n-1)(n-2) \dots 3 \cdot 2 \cdot 1$ เมื่อ $n \geq 1$ โดยที่กำหนด $0! = 1$

6. สำหรับจำนวนเต็มบวก n และจำนวนเต็ม k ซึ่ง $0 \leq k \leq n$ นิยาม

$$\begin{aligned} \binom{n}{k} &= \frac{n!}{k!(n-k)!} \\ &= \frac{n(n-1)\dots(k-1)}{(n-k)!} \\ &= \frac{n(n-1)\dots(n-k+1)}{k!} \end{aligned}$$

เรียกสัญลักษณ์ $\binom{n}{k}$ ว่า สัมประสิทธิ์ทวินาม เช่น

$$\binom{8}{3} = \frac{8!}{3!5!} = \frac{8 \cdot 7 \cdot 6 \cdot 5 \cdot 4}{5!} = \frac{8 \cdot 7 \cdot 6}{3!} = 56$$

จากความหมายนี้จะได้ $\binom{n}{0} = \binom{n}{n} = 1$ และ $\binom{n}{k} = \binom{n}{n-k}$

ในการหาสัมประสิทธิ์ของการกระจายผลบวกของเลขยกกำลังนั้น อาจใช้รูปแบบการเขียนสามเหลี่ยมปาสคาลในการหาสัมประสิทธิ์ตัวที่ $k+1$ ซึ่งเท่ากับ $\binom{n}{k}$ ได้ ซึ่งมีรายละเอียดต่อไปนี้

					1					
					1		1			
			1		2		1			
		1	3		6		3		1	
	1	4	10		20		10		4	1
1	5	10	10		6		5		1	1
					⋮					

จากสามเหลี่ยมปาสคาล จะได้

$$(a+b)^0 = 1 \quad (\text{ดูแถวที่ 1})$$

$$(a+b)^1 = a+b \quad (\text{ดูแถวที่ 2})$$

$$(a+b)^2 = a^2 + 2ab + b^2 \quad (\text{ดูแถวที่ 3})$$

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3 \quad (\text{ดูแถวที่ 4})$$

$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4 \quad (\text{ดูแถวที่ 5})$$

ในทำนองเดียวกัน ถ้าต้องการกระจายผลบวกของยกกำลัง n ก็ดูแถวที่ $n+1$ หรืออาจใช้

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \dots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n$$

หรือ

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k$$

ตัวอย่าง 1.18

$$(x+1)^6 = \binom{6}{0}x^6 + \binom{6}{1}x^5 + \binom{6}{2}x^4 + \binom{6}{3}x^3 + \binom{6}{4}x^2 + \binom{6}{5}x + \binom{6}{6}$$

$$(x+2)^5 = \binom{5}{0}x^5 + \binom{5}{1}x^4 \cdot 2 + \binom{5}{2}x^3 \cdot 2^2 + \binom{5}{3}x^2 \cdot 2^3 + \binom{5}{4}x \cdot 2^4 + \binom{5}{5}2^5$$

$$2^n = (1+1)^n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{n-1} + \binom{n}{n}$$

7. ให้ $a \in \mathbb{Z}$ ค่าสัมบูรณ์ ของ a เขียนแทนด้วย $|a|$ นิยามโดย

$$|a| = \begin{cases} 0; & a = 0 \\ a; & a \in \mathbb{N} \\ -a; & -a \in \mathbb{N} \end{cases}$$

จากบทนิยามพบว่า

1. $|a| \geq 0$
2. $|a| = 0$ ก็ต่อเมื่อ $a = 0$
3. $-|a| \leq a \leq |a|$
4. $|a| \leq b$ ก็ต่อเมื่อ $-b \leq a \leq b$
5. $|a| \geq b$ ก็ต่อเมื่อ $a \geq b$ หรือ $a \leq -b$
6. $|ab| = |a||b|$
7. $|a + b| \leq |a| + |b|$
8. $|a| - |b| \leq |a - b|$
9. $-(|a| + |b|) \leq a + b \leq |a| + |b|$
10. $||a| - |b|| \leq |a - b|$
11. $|a| = |b|$ ก็ต่อเมื่อ $a = b$ หรือ $a = -b$

1.5 สรุปท้ายบทที่ 1

ส่วนแรกในเนื้อหาบทนี้ได้กล่าวถึงความเป็นมาและวิวัฒนาการของวิชาทฤษฎีจำนวน พบว่าทฤษฎีจำนวนเป็นสาขาทางคณิตศาสตร์ที่เก่าแก่ได้ถูกพัฒนามาตั้งแต่สมัยกรีกโบราณเมื่อประมาณ 2500 ปีมาแล้วโดยยูคลิดออกสำคัญที่จะอธิบายสิ่งต่าง ๆ ในจักรวาล คือจำนวน วิวัฒนาการของวิชาทฤษฎีจำนวน จำนวนที่มีสมบัติพิเศษ เช่น จำนวนเชิงमितร จำนวนสมบูรณ์ เป็นต้น รวมทั้งนักคณิตศาสตร์ที่มีบทบาทสำคัญที่ทำให้ทฤษฎีจำนวนพัฒนามาถึงทุกวันนี้ ปัญหาเกี่ยวกับจำนวนเฉพาะที่มีมากมายซึ่งบางปัญหายังไม่สามารถหาคำตอบได้ในปัจจุบัน และบางปัญหาทำให้เกิดแนวคิดใหม่ ๆ สำหรับการศึกษาต่อไปในระดับสูง การพิสูจน์เบื้องต้นนั้นจะอาศัยพื้นฐานทางตรรกศาสตร์ แบ่งการพิสูจน์ออกเป็น 7 วิธีดังนี้ การพิสูจน์ข้อความแบบมีเงื่อนไข การพิสูจน์โดยการแจกแจงกรณี การพิสูจน์ข้อความแบบผันกลับได้ การพิสูจน์ข้อความเลือก การพิสูจน์ข้อความซึ่งเป็นไปได้อย่างเดียว การพิสูจน์โดยการยกตัวอย่างค้าน และการพิสูจน์โดยหลักอุปนัยเชิงคณิตศาสตร์ หลังจากนั้น กล่าวถึงสมบัติของจำนวนเต็มซึ่ง จะเป็นพื้นฐานอีกประการในการศึกษาทฤษฎีจำนวนโดยแบ่งออกเป็น 3 กลุ่มดังนี้ สมบัติทางพีชคณิต สมบัติไตรวิภาค และหลักการจัดอันดับดี ในหัวข้อสุดท้ายเป็นข้อเสนอแนะบางประการเกี่ยวกับจำนวนเต็ม เช่น ลำดับเลขคณิต ลำดับเรขาคณิต สัญลักษณ์แทนการบวก สัญลักษณ์แทนการคูณสัมประสิทธิ์ทวินาม เพื่อเป็นพื้นฐานในการศึกษาทฤษฎีจำนวนในบทต่อไป

แบบฝึกหัดท้ายบทที่ 1

1. จงใช้บทนิยามและสัจพจน์เพื่อพิสูจน์ว่า
 - 1.1 ถ้า a เป็นจำนวนเต็มคี่และ b เป็นจำนวนเต็มคี่ แล้ว $a + b$ เป็นจำนวนคู่
 - 1.2 ถ้า k เป็นจำนวนคู่แล้ว k^2 เป็นจำนวนคู่
 - 1.3 ถ้า k เป็นจำนวนเต็มคี่แล้ว k^2 เป็นจำนวนเต็มคี่
 - 1.4 a^2 เป็นจำนวนเต็มคี่ ก็ต่อเมื่อ $a + 2$ เป็นจำนวนเต็มคี่
 - 1.5 a เป็นจำนวนคู่ ก็ต่อเมื่อ $a^2 + 2$ เป็นจำนวนคู่
2. กำหนดให้ a และ b เป็นจำนวนเต็มจงพิสูจน์ว่า ถ้า $ab = 0$ แล้ว $a = 0$ หรือ $b = 0$
3. ถ้า a เป็นจำนวนเต็มแล้ว $a^2 + a + 1$ เป็นจำนวนเต็มคี่
4. จงพิสูจน์ว่า มีจำนวนจริง x เพียงตัวเดียวเท่านั้นซึ่ง $5^x = 1$
5. จงพิสูจน์ว่า $\forall x \forall y, x + y \leq 10$ เป็นจริงเมื่อกำหนด $U = \{3, 4, 5\}$
6. จงพิสูจน์ว่า $\forall x \forall y, x + y = 1$ เป็นเท็จเมื่อกำหนด $U = \{-1, 0, 1\}$
7. จงพิสูจน์ข้อความต่อไปนี้โดยใช้หลักอุปนัยเชิงคณิตศาสตร์
 - 7.1 $1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$ สำหรับทุกจำนวนนับ n
 - 7.2 $1^3 + 2^3 + 3^3 + \dots + n^3 = \frac{[n(n+1)]^2}{4}$ สำหรับทุกจำนวนนับ n
 - 7.3 $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \dots + n(n+1) = \frac{n(n+1)(n+2)}{8}$ สำหรับทุกจำนวนนับ n
 - 7.4 $1 \cdot 2 + 2 \cdot 2^2 + 3 \cdot 2^3 + \dots + n \cdot 2^n = (n-1)2^{n+1} + 2$ สำหรับทุกจำนวนนับ n
 - 7.5 จงพิสูจน์ว่า $2n < 2^n$ สำหรับทุกจำนวนเต็ม n ที่ $n \geq 3$
 - 7.6 กำหนดให้ a_n เป็นลำดับซึ่งกำหนดโดย $a_1 = 1, a_2 = 8$ และ $a_n = a_{n-1} + 2a_{n-2}$
สำหรับ $n \geq 3$ จงพิสูจน์ว่า $a_n = 3 \cdot 2^{n-1} + 2(-1)^n$ สำหรับทุก $n \in \mathbb{N}$
 - 7.7 กำหนดให้ a_n เป็นลำดับซึ่งกำหนดโดย $a_1 = 1, a_2 = 3$ และ $a_n = 2a_{n-1} - a_{n-2}$
สำหรับ $n \geq 3$ จงพิสูจน์ว่า $a_n = 2n - 1$ สำหรับทุก $n \in \mathbb{N}$
 - 7.8 จงพิสูจน์ว่าทุก ๆ จำนวนเต็มบวก n จะมี t และ m เพียงคู่เดียวเท่านั้นที่ทำให้ $n = 2^t m$ โดยที่ $t \in \{0, 1, 2, \dots\}$ และ m เป็นจำนวนเต็มคี่

8. กำหนดให้ $a, b, c, d \in \mathbb{Z}$ จงพิสูจน์ว่า

8.1 ถ้า $ab = ac$ แล้ว $b = c$

8.2 สำหรับจำนวนจริง a ทุกตัว $a0 = 0$ และ $0a = 0$

8.3 $-(-a) = a$

8.4 $(a - b)(c - d) = (ac + bd) - (ad + bc)$

8.5 $a - b = c - d$ ก็ต่อเมื่อ $a + d = b + c$

8.6 $(a - b)c = ac - bc$

9. กำหนดให้ $a, b, c, x, y \in \mathbb{Z}$ จงพิสูจน์ว่า

9.1 ถ้า $a > b$ แล้ว $a + c > b + c$

9.2 $a - x < a - y$ ก็ต่อเมื่อ $x > y$

9.3 ถ้า $a < 0$ และ $ax > ay$ แล้ว $x < y$

9.4 ถ้า $a < b$ และ $c < 0$ แล้ว $ac > bc$

9.5 ถ้า $x + x + x + x = 0$ แล้ว $x = 0$

9.6 ถ้า $a < b$ แล้ว $a^3 < b^3$