บทที่ 3
การให้เหตุผลทางคณิตศาสตร์

ในสองบทแรก เราทบทวนมโนทัศน์มูลฐานของคณิตศาสตร์อันได้แก่ ตรรกศาสตร์, เซต, ฟังก์ชัน, และความสัมพันธ์ ซึ่งทำหน้าที่เป็น “อิฐบล็อก” ทางคณิตศาสตร์ที่เราใช้สร้าง**ระบบคณิตศาสตร์** (mathematical system) ที่ซับซ้อนยิ่งขึ้น เช่นระบบจำนวน, เวคเตอร์, เมทริกซ์, กราฟ ฯลฯ ในระบบคณิตศาสตร์หนึ่งๆ เราใช้*เซต*ในการนิยามกลุ่มของวัตถุที่เราสนใจในระบบนั้น ใช้*ฟังก์ชัน*และ*ความสัมพันธ์*ในการนิยามการดำเนินการและความสัมพันธ์ในลักษณะต่างๆของวัตถุในระบบ และใช้ตรรกศาสตร์เป็นภาษาที่แม่นยำในการบรรยายและเชื่อมโยงมโนทัศน์ต่างๆในระบบอย่างสมเหตุสมผล. บทนี้จะกล่าวถึงบทบาทเพิ่มเติมของตรรกศาสตร์ในฐานะเป็นเครื่องมือที่สำคัญยิ่งยวดในการค้นหาและพิสูจน์ความจริงต่างๆในระบบคณิตศาสตร์ที่เราสร้างขึ้น. เป้าหมายของบทนี้คือเพื่อเรียนรู้การอ้างเหตุผลที่ถูกต้องและศึกษาเทคนิคต่างๆที่ใช้ในการพิสูจน์ความจริงทางคณิตศาสตร์.

3.1 การสร้างระบบคณิตศาสตร์

โดยทั่วไปแล้ว มนุษย์สร้างระบบคณิตศาสตร์แต่ละระบบขึ้นมาเพื่อใช้เป็นแบบจำลองของโครงสร้างทางกายภาพและปรากฏการณ์ต่างๆ ที่อยู่รอบตัว. เมื่อเราต้องการนับจำนวนสิ่งของ เราก็สร้างระบบจำนวนนับขึ้น. เมื่อเราเริ่มมีการหยิบยืมและเป็นหนี้สิน เราก็สร้างจำนวนเต็มลบและระบบจำนวนเต็มขึ้นและพัฒนาไปสู่ระบบจำนวนจริงและจำนวนเชิงซ้อนในที่สุด. ความสนใจในเรื่องรูปทรงต่างๆในระนาบทำให้เกิดวิชาเรขาคณิต และความสนใจเรื่องอัตราการเปลี่ยนแปลงของค่าต่างๆทำให้เกิดวิชาแคลคูลัสเป็นต้น.

อย่างไรก็ตาม ระบบคณิตศาสตร์ทุกระบบที่สร้างขึ้นจะต้องเป็นนามธรรมอันบริสุทธิ์บนพื้นฐานของเหตุผลที่ถูกต้องแม่นยำ. ความจริงต่างๆเกี่ยวกับระบบจะต้องพิสูจน์ได้โดยปราศจากความกำกวมจึงจะเป็นที่ยอมรับได้ว่าเป็นความจริง. การพิสูจน์ความจริงทางคณิตศาสตร์ทำได้โดยการอ้างความจริงที่เรา “ยอมรับแล้ว” เป็นวัตถุดิบและใช้กลไกของการอ้างเหตุผลที่ถูกต้องสร้างข้อความที่เป็นความจริงเป็นลำดับจนกระทั่งได้ความจริงที่เราต้องการจะพิสูจน์ในที่สุด. หลังจากนั้นเราก็จะถือว่าความจริงที่เราพิสูจน์แล้วนี้เป็นความจริงที่เรา “ยอมรับแล้ว” ด้วยเช่นกัน.

การใช้ความจริงที่เรายอมรับแล้วมาพิสูจน์ความจริงใหม่ๆ ทำให้เกิดคำถามดุจเดียวกับคำถามที่ว่า “มนุษย์อุบัติขึ้นได้อย่างไร?” เราแต่ละคนเกิดมาจากพ่อแม่เรา, พ่อแม่เราเกิดมาจากปู่ย่าตายายเรา, ปู่ย่าตายายเกิดมาจากปู่ทวดย่าทวดตาทวดยายทวดเรา, ปู่ทวดย่าทวด.... ฯลฯ ซึ่งเป็นคำถามที่ไม่มีที่สิ้นสุด เพราะต่อให้เราพบว่ามนุษย์คู่แรกคือตาอินกับยายนา เราก็ยังอดถามต่อไม่ได้ว่าแล้วตาอินกับยายนามาจากไหนอีก. แต่ความจริงทางคณิตศาสตร์จะต้องสืบสาวในเชิงเหตุผลได้จนถึงความจริงตั้งต้นที่เราจะต้องยอมรับว่าเป็นความจริงโดยไม่ต้องพิสูจน์จากความจริงใดๆอีก. ความจริงตั้งต้นเหล่านี้เราเรียกว่าเป็น**สัจพจน์** (axiom or postulate) ของระบบคณิตศาสตร์นั้น.

การสร้างระบบคณิตศาสตร์หนึ่งๆ จะต้องเริ่มจาก**เซตเอกภพ** (universal set) ของ**สิ่งนามธรรม** (abstract entity) ที่เป็นองค์ประกอบของระบบนั้น. จากนั้นเราจะประกาศ**สัจพจน์**ของระบบเพื่อบรรยายลักษณะสมบัติที่เราต้องการเกี่ยวกับสิ่งนามธรรมในเซตเอกภพนั้น. ระบบหนึ่งๆอาจมีสัจพจน์ได้หลายสัจพจน์ และที่เราจะต้องตระหนักคือสัจพจน์เป็นข้อความที่ผู้สร้างระบบกำหนดได้*ตามอำเภอใจ (arbitrary)* โดยมีข้อแม้แต่เพียงว่า สัจพจน์ต่างๆในระบบจะต้องไม่ขัดแย้งกันเองและสัจพจน์แต่ละสัจพจน์จะต้องไม่ใช่ข้อความที่สามารถพิสูจน์ได้จากสัจพจน์อื่นๆ. ด้วยเหตุนี้ระบบคณิตศาสตร์หนึ่งๆจะมีสัจพจน์เป็นจำนวนจำกัดและมีจำนวนน้อยที่สุดเท่าที่จะเป็นไปได้ ซึ่งจะทำหน้าที่เป็นความจริงตั้งต้นของระบบในการพิสูจน์ความจริงอื่นๆในระบบต่อไป.

แม้ว่าสัจพจน์จะเป็นความจริงที่ผู้สร้างระบบประกาศขึ้นตามอำเภอใจ แต่ถ้าเป็นการประกาศขึ้นอย่างสะเปะสะปะไร้เป้าหมาย เราก็จะได้ระบบคณิตศาสตร์ที่แม้จะมีความสมเหตุสมผลในตัวมันเอง แต่ไม่สามารถนำไปใช้เป็นแบบจำลองของโครงสร้างทางกายภาพใดๆได้. ระบบคณิตศาสตร์นั้นก็จะเป็นเพียงของเล่นทางความคิดที่ไร้ประโยชน์และไม่คุ้มค่าที่จะให้ความสนใจ.

เมื่อเราเริ่มสร้างระบบคณิตศาสตร์หนึ่งขึ้นมาโดยการกำหนดเซตเอกภพของสิ่งนามธรรมในระบบและประกาศกลุ่มของสัจพจน์ของระบบนั้น เราจำเป็นจะต้องใช้คำบางคำที่ใช้แทนมโนทัศน์เชิงนามธรรมบางอย่างที่จะบรรยายสมาชิกในเซตเอกภพและใช้ในข้อความสัจพจน์. คำเหล่านี้เรียกว่า **คำอนิยาม** (undefined term) เพราะเป็นคำที่เราจะ<u>ไม่มี</u>**บทนิยาม** (definition) ให้กับมัน เนื่องจากในขณะที่เรากำลังสร้างระบบใหม่นั้น เรายังไม่มีนามธรรมอื่นใดมาใช้ในการให้นิยามคำเหล่านี้ได้. คำอนิยามของระบบจึงทำหน้าที่คล้ายคลึงกับสัจพจน์ในแง่ที่ว่า เราจะยอมรับการมีอยู่ของมันโดยไม่ตั้งคำถามว่ามันคืออะไร ได้มาจากไหน. โดยทั่วไป คำอนิยามจะใช้กล่าวถึงสิ่งนามธรรมที่เรามีภาพอยู่ในใจแล้วว่ามันแทนสิ่งอะไรทางกายภาพ.

ตัวอย่าง 1: **สัจพจน์สำหรับระบบจำนวน -- *สัจพจน์เปอาโน (Peano's Axioms)***

ในช่วงรอยต่อระหว่างศตวรรษที่ 19 กับ 20 มีความสนใจครั้งใหญ่ในวงการคณิตศาสตร์ที่จะแสดงให้เห็นว่าความรู้ทางคณิตศาสตร์ทั้งหมดที่เรามีสามารถสร้างขึ้นได้บนรากฐานของตรรกศาสตร์ล้วนๆ. นักคณิตศาสตร์อิตาเลียนชื่อ *ยูเซปเป เปอาโน (Giuseppe Peano, 1858-1932)* ได้เสนอเมื่อปี ค.ศ. 1889 ว่าความจริงเกี่ยวกับระบบจำนวนที่มนุษย์รวบรวมกันมาหลายพันปีนั้นสามารถสร้างได้จากสัจพจน์เพียง 5 ข้อและคำอนิยามเพียง 3 คำคือ ***จำนวนนับ*** *(natural number)*, ***ศูนย์*** *(zero)*, และ ***ตัวตาม*** *(successor)*. สัจพจน์ทั้ง 5 ข้อสำหรับระบบจำนวน ซึ่งมีชื่อเรียกเป็นเกียรติแก่เขาว่า **สัจพจน์เปอาโน** (Peano's Axioms) มีดังต่อไปนี้:

สัจพจน์เปอาโน

1. ศูนย์เป็นจำนวนนับ.
2. จำนวนนับทุกตัวมี *ตัวตาม* ซึ่งก็เป็นจำนวนนับ.
3. ศูนย์ไม่เป็นตัวตามของจำนวนนับตัวใด.
4. จำนวนนับที่แตกต่างกันจะมีตัวตามที่แตกต่างกัน.
5. ถ้า A เป็นเซตที่มีสมาชิกเป็นจำนวนนับและมีสมบัติที่ว่า *(1) ศูนย์เป็นสมาชิกของ A* และ *(2) ตัวตามของสมาชิกแต่ละตัวใน A ก็เป็นสมาชิกของ A เช่นกัน*, จะได้ว่า A คือเซตของจำนวนนับทั้งหมด. (นั่นคือ $A = \mathbb{N}$)

ถ้าเราใช้สัญลักษณ์ 0 แทน*ศูนย์*, S(n) แทนตัวตามของจำนวนนับ n, และ $\mathbb{N}$ แทนเซตของจำนวนนับทั้งหมด, เราอาจเขียนสัจพจน์เปอาโนในรูปสัญลักษณ์ทางเซตและตรรกศาสตร์ได้ดังนี้:

1. $0 \in \mathbb{N}$
2. $\forall n\in \mathbb{N}\ \exists m\in \mathbb{N}\ [m = S(n)]$
3. $\forall n\in \mathbb{N}\ [0 \neq S(n)]$
4. $\forall m\in \mathbb{N}\ \forall n\in \mathbb{N}\ ([m \neq n] \rightarrow [S(m) \neq S(n)])$
5. $([A \subseteq \mathbb{N}] \wedge [0 \in A] \wedge \forall n\in A\ [S(n)\in A]) \rightarrow [A = \mathbb{N}]$

❑

เมื่อเรากำหนดคำอนิยามและสัจพจน์สำหรับระบบคณิตศาสตร์ที่เราจะสร้างขึ้นแล้ว เราก็จะนิยามสัญลักษณ์หรือคำใหม่ๆที่เราอาจเรียกว่า **คำมีนิยาม** (defined term) เพื่อเป็นสื่อทางภาษาที่จะบรรยายมโนทัศน์และความจริงเกี่ยวกับโครงสร้างของระบบได้อย่างสะดวกและชัดเจน. ข้อความที่แสดงนิยามของคำเหล่านั้นเรียกว่า **บทนิยาม** (definition). โดยทั่วไปแล้ว เรานิยามสัญลักษณ์หรือคำเพื่อใช้แทนสิ่งนามธรรมหรือกลุ่มของสิ่งนามธรรมที่สร้างจากมโนทัศน์ที่มีอยู่ในขณะนั้น, เพื่อใช้เป็นชื่อเรียกสมบัติที่น่าสนใจของสิ่งนามธรรมต่างๆ, หรือเพื่อใช้แทนการดำเนินการหรือความสัมพันธ์ระหว่างสิ่งนามธรรมต่างๆในระบบ. เราถือว่าข้อความในบทนิยามเป็น "ความจริง" ที่เราใช้อ้างได้ เพราะบทนิยามเป็นเพียงการกำหนด "ชื่อ" ให้กับมโนทัศน์ที่เราต้องการใช้สื่อความหมายเท่านั้น ดังนั้นข้อความในบทนิยามจึงเป็นความจริงเพราะเรากำหนดให้มันเป็นเช่นนั้น.

มีข้อน่าสังเกตบางประการเกี่ยวกับการเขียนบทนิยามทางคณิตศาสตร์. บทนิยามส่วนใหญ่เป็นการนิยามมโนทัศน์ใหม่จากมโนทัศน์ที่มีอยู่แล้ว. ตัวอย่างเช่นในเรื่องจำนวนเต็ม หลังจากที่เรานิยาม "การหารลงตัว" แล้ว เราก็ใช้มันมานิยาม "จำนวนคู่" ดังนี้

บทนิยาม: *จำนวนเต็มใดๆ จะเรียกว่าเป็น**จำนวนคู่** ถ้าจำนวนเต็มนั้นหารด้วยสองลงตัว.*

ความหมายที่เราต้องการจากบทนิยามนี้คือ *ถ้าจำนวนเต็ม n ใดหารด้วยสองลงตัว เราจะเรียก n ว่าเป็นจำนวนคู่* และในทางกลับกัน *ถ้าจำนวนเต็ม n ใดเป็นจำนวนคู่ จะสรุปได้ว่า n หารด้วยสองลงตัว.* ดังนั้นความหมายที่แท้จริงของบทนิยามนี้คือ *"จำนวนเต็ม n ใดๆเป็นจำนวนเต็มคู่ <u>เมื่อและต่อเมื่อ</u> n หารด้วยสองลงตัว"* แต่ทว่าในการเขียนบทนิยามทางคณิตศาสตร์มักใช้คำว่า ***ถ้า*** แทนคำว่า ***เมื่อและต่อเมื่อ*** ในรูปแบบของ *"เรากล่าวว่า...มโนทัศน์ใหม่...**ถ้า**...เงื่อนไขจากมโนทัศน์ที่มีอยู่..."* เพื่อเป็นการสื่อความหมายโดยนัยว่ามโนทัศน์ใดเกิดก่อน มโนทัศน์ใดเกิดหลัง.

ตัวอย่าง 2: เรานิยามสัญลักษณ์ 1 แทนตัวตามของจำนวนนับ 0, สัญลักษณ์ 2 แทนตัวตามของจำนวนนับ 1, ... ฯลฯ และนิยามการดำเนินการทวิภาค "+" ระหว่างจำนวนนับด้วยบทนิยามต่อไปนี้:

บทนิยาม: ***การบวกจำนวนนับ***

ให้ n และ m เป็นจำนวนนับใดๆ, การบวกระหว่าง n และ m เขียนแทนด้วย n+m มีนิยามดังนี้

1. $n+0 = n$
2. สำหรับจำนวนนับ k ใดๆ, $n+S(k) = S(n+k)$

จากบทนิยามข้างบน เราสามารถหาค่าผลบวกระหว่างจำนวนนับสองตัวใดๆได้ เช่นเราหาค่า 3+2 ได้ด้วยขั้นตอนดังนี้

3+0 = 3

ดังนั้น 3+1 = 3+S(0) = S(3+0) = S(3) = 4

ดังนั้น 3+2 = 3+S(1) = S(3+1) = S(4) = 5

❑

เมื่อเรามีคำอนิยาม, สัจพจน์, และคำมีนิยามต่างๆ ที่กำหนดขึ้นเพื่อบรรยายสิ่งนามธรรมและโครงสร้างมูลฐานของระบบเป็นวัตถุดิบตั้งต้นแล้ว, เราสามารถค้นหาและพิสูจน์ความจริงใหม่ๆเกี่ยวกับสมบัติและโครงสร้างของระบบนั้นได้โดยใช้การอ้างเหตุผลเชิงตรรกที่ถูกต้อง. เราเรียกข้อความที่จะต้องมีการพิสูจน์อย่างชัดเจนว่าเป็นความจริงว่า **ทฤษฎีบท** (theorem) และเรียกบทความที่เป็นการพิสูจน์ทฤษฎีบทว่า **บทพิสูจน์** (proof). เราจะเรียกทฤษฎีบทบางบทว่า **บทประกอบ** (lemma) ถ้าทฤษฎีบทนั้นมีประโยชน์หลักเพื่อใช้พิสูจน์ทฤษฎีบทอื่นที่สำคัญกว่า, และเรียกทฤษฎีบทบางบทว่า **บทอนุนัย** (corollary) ถ้าทฤษฎีบทนั้นเป็นผลที่ได้มาโดยตรงจากทฤษฎีที่เราเพิ่งจะพิสูจน์ก่อนหน้านั้น. ทั้งบทประกอบและบทอนุนัยล้วนเป็นความจริงที่ต้องพิสูจน์เช่นเดียวกับทฤษฎีบทอื่นๆ แต่การพิสูจน์บทอนุนัยมักจะทำได้โดยง่ายโดยอาศัยบทพิสูจน์ของทฤษฎีบทก่อนหน้านั้น.

การพิสูจน์ทฤษฎีบทแรกๆของระบบมักต้องอ้างความจริงจากสัจพจน์และบทนิยามที่มีอยู่โดยตรง เพราะในขณะนั้นเราไม่มีความจริงอื่นใดในระบบอีกแล้วที่จะอ้างได้. เมื่อทฤษฎีบทใดได้รับการพิสูจน์แล้ว เราก็ถือว่าทฤษฎีบทเป็นความจริงที่เราจะใช้อ้างได้เช่นเดียวกับสัจพจน์ของระบบ. การพิสูจน์ทฤษฎีบทต่อๆไปจึงสามารถอ้างความจริงได้จากสัจพจน์ บทนิยาม และทฤษฎีบทที่พิสูจน์ไปแล้วก่อนหน้านั้นได้.

ตัวอย่าง 3: จงพิสูจน์ทฤษฎีบทสำหรับระบบจำนวนนับต่อไปนี้

ทฤษฎีบท: S(n) = n+1 สำหรับจำนวนนับ n ใดๆ

<u>*วิธีทำ*</u> ทฤษฎีบทนี้ซึ่งเป็นความจริงลำดับแรกๆสำหรับระบบจำนวน สามารถพิสูจน์ได้โดยตรงจากสัจพจน์สำหรับระบบจำนวนในตัวอย่าง 1 และบทนิยามของการบวกจำนวนนับในตัวอย่าง 2. เราจะเขียนบทพิสูจน์ได้ง่ายๆดังนี้

บทพิสูจน์: ให้ n เป็นจำนวนนับใดๆ. เราได้

n+1 = n+S(0) --*จากสัจพจน์เปอาโนข้อที่ 2 และบทนิยาม S(0) = 1*

= S(n+0) --*จากบทนิยามของการบวกจำนวนนับข้อที่ 2*

= S(n) --*จากบทนิยามของการบวกจำนวนนับข้อที่ 1*

นั่นคือเราได้แสดงแล้วว่า n+1 = S(n) สำหรับ n ใดๆ ❑

❑

ทฤษฎีบทโดยทั่วไปจะมีองค์ประกอบสองส่วนคือ กลุ่มของ**ข้อกำหนด** (premise) และ**ข้อสรุป** (conclusion) โดยที่ข้อความของทฤษฎีบทก็คือการกล่าวว่า *เมื่อข้อกำหนดทุกข้อของทฤษฎีบทเป็นจริง จะสรุปได้ว่าข้อสรุปของทฤษฎีบทเป็นจริง*. นั่นคือถ้าให้ประพจน์ p_1, p_2, ..., p_n แทนข้อกำหนด n ข้อของทฤษฎีบทและประพจน์ C คือข้อสรุปของทฤษฎีบท, เราจะเขียนทฤษฎีบทในรูปสัญลักษณ์ได้ว่า

$$(p_1 \wedge p_2 \wedge ... \wedge p_n) \longrightarrow C$$

ซึ่งอ่านเป็นภาษาธรรมดาได้ว่า “p_1, p_2, ..., และ p_n ทำให้สรุปได้ C”

พิจารณาทฤษฎีบทในตัวอย่าง 3 ข้างบนเป็นตัวอย่าง. ข้อกำหนดของทฤษฎีบทนี้มีเพียงข้อเดียวคือ “n เป็นจำนวนนับใดๆ” และข้อสรุปของทฤษฎีบทคือ “S(n) = n+1” ดังนั้นเราอาจเขียนทฤษฎีบทนี้ในรูปมาตรฐานได้ดังนี้

[n เป็นจำนวนนับใดๆ]$\longrightarrow$[S(n) = n+1]

ตัวอย่าง 4: จงหาข้อกำหนดและข้อสรุปของทฤษฎีบท 3 หัวข้อ 2.3.

<u>*วิธีทำ*</u> ข้อกำหนดของทฤษฎีบทดังกล่าวสามารถแบ่งได้เป็น 3 ข้อความได้แก่

- *A, B, และ C เป็นเซตใดๆ*
- *f เป็นฟังก์ชันใดๆจาก A ไป B*
- *g เป็นฟังก์ชันใดๆจาก B ไป C*

ข้อสรุปของทฤษฎีบทนี้คือ

$g \circ f$ เป็นฟังก์ชันจาก A ไป C โดยที่ $(g \circ f)(x) = g(f(x))$

❑

ทฤษฎีบทบางบทอาจมีแต่เพียงข้อสรุปโดยปราศจากข้อกำหนดใดๆ เช่นทฤษฎีบทเกี่ยวกับระบบจำนวนจริงบทหนึ่งมีข้อความเพียงว่า

π เป็นจำนวนอตรรกยะ

ทฤษฎีบทในลักษณะเช่นนี้เป็นการประกาศข้อความที่เป็นจริงในทุกบริบทโดยปราศจากเงื่อนไข.

การพิสูจน์ทฤษฎีบทมีเป้าหมายหลักเพียงประการเดียวคือการแสดงให้เห็นว่าข้อสรุปของทฤษฎีบทนั้นเป็นจริงบนเงื่อนไขของข้อกำหนดของทฤษฎีบทนั้น (ถ้ามี). ในระหว่างการพิสูจน์ทฤษฎีบทหนึ่งๆ ข้อความที่เราถือว่าเป็นความจริงที่อ้างได้ได้แก่ ข้อกำหนดของทฤษฎีบทนั้นเอง, สัจพจน์ของระบบ, บทนิยาม, และทฤษฎีบทที่เราพิสูจน์แล้ว. มีเทคนิคและวิธีการหลายแบบในการโยงความจริงเหล่านี้ไปสู่ข้อสรุปของทฤษฎีบท แต่ทุกแบบจะต้องอาศัย**การอ้างเหตุผลที่สมเหตุสมผล** (valid argument) ในทุกขั้นตอนของการพิสูจน์. การอ้างเหตุผลที่สมเหตุสมผลจะต้องตั้งอยู่บนหลักทางตรรกศาสตร์ที่เรียกว่า **กฎการอนุมาน** (rule of inference) ซึ่งเราจะศึกษาในหัวข้อย่อยต่อไป.

3.2 การอ้างเหตุผลและกฎการอนุมาน

กฎการอนุมาน (Rules of Inference)

ถ้าให้ p และ q เป็นประพจน์ใดๆ เราสามารถใช้ตารางค่าความจริง (ดูตาราง 1) แสดงให้เห็นว่าประพจน์ประกอบ $((p\rightarrow q)\wedge p)\rightarrow q$ เป็นสัจนิรันดร์.

ตาราง 1 : ตารางค่าความจริงของ $((p\rightarrow q)\wedge p)\rightarrow q$

p	q	$p\rightarrow q$	$(p\rightarrow q)\wedge p$	$((p\rightarrow q)\wedge p)\rightarrow q$
T	T	T	T	**T**
T	F	F	F	**T**
F	T	T	F	**T**
F	F	T	F	**T**

การที่ประพจน์ $((p\rightarrow q)\wedge p)\rightarrow q$ เป็นสัจนิรันดร์มีนัยสำคัญอย่างไร? ใจความหลักของ $((p\rightarrow q)\wedge p)\rightarrow q$ คือ "$(p\rightarrow q)\wedge p$ ทำให้สรุปได้ q". การที่ประพจน์ประกอบนี้เป็นสัจนิรันดร์แสดงว่า *ไม่ว่า p และ q จะมีค่าความจริงใดก็ตาม ถ้าทั้ง $p\rightarrow q$ และ p เป็นจริงแล้ว ไม่มีทางเป็นไปได้ว่า q เป็นเท็จ นั่นคือ q จะต้องเป็นจริงอย่างแน่นอน.* เราเรียกเหตุการณ์เช่นนี้ว่า **$(p\rightarrow q)\wedge p$ สรุปได้ q ในเชิงตรรก** และเขียนในรูปสัญลักษณ์ว่า $(p\rightarrow q)\wedge p \Rightarrow q$. บทนิยามต่อไปนี้ให้คำจำกัดความของ**การสรุปได้ในเชิงตรรก** สำหรับประพจน์ประกอบใดๆ.

บทนิยาม 1: **การสรุปได้ในเชิงตรรก** (logical implication)
ให้ P และ Q เป็นประพจน์ใดๆ (อาจเป็นประพจน์ประกอบหรือประพจน์เดี่ยวก็ได้). ถ้า $P\rightarrow Q$ เป็นสัจนิรันดร์, เราจะกล่าวว่า **P สรุปได้ Q ในเชิงตรรก** (P logically implies Q) และเขียนในรูปสัญลักษณ์ว่า $P\Rightarrow Q$.

การสรุปได้ในเชิงตรรกเป็นรากฐานของ**การอ้างเหตุผลที่สมเหตุสมผล** (valid argument). เมื่อเราทราบว่า $(p\rightarrow q)\wedge p \Rightarrow q$ เราจะได้การอ้างเหตุผลที่สมเหตุสมผลรูปแบบหนึ่งคือ

สมมติฐาน $p\rightarrow q$ และ p ทำให้ได้ข้อสรุป q

หรือเขียนในเชิงลำดับเหตุผลว่า

$$\begin{array}{rl} & p\rightarrow q \\ & p \\ \hline \therefore & q \end{array}$$

ซึ่งเขียนโดยย่อในบรรทัดเดียวได้ว่า $\{p\rightarrow q, p\}\therefore q$

การอ้างเหตุผล $\{p\rightarrow q, p\}\therefore q$ นี้ จะสมเหตุสมผลเสมอไม่ว่า p และ q จะเป็นประพจน์ใดก็ตาม. หลักการอ้างเหตุผลที่ใช้ได้ทั่วไปเช่นนี้เรียกว่า **กฎการอนุมาน** (rule of inference). กฎการอนุมาน $\{p\rightarrow q,p\}\therefore q$ เป็นที่รู้จักกันดีตั้งแต่สมัยกรีกโบราณในชื่อ **โมดัสโพเนนส์** (modus ponens).

กล่าวโดยทั่วไป เมื่อเราพบว่าประพจน์ประกอบ $(P_1 \wedge P_2 \wedge \ldots \wedge P_n) \longrightarrow Q$ ใดเป็นสัจนิรันดร์, เราจะได้กฎการอนุมานใหม่คือ $\{P_1, P_2, \ldots, P_n\} \therefore Q$ เป็นหลักการอ้างเหตุผลที่สมเหตุสมผลแบบหนึ่ง. เราเรียกข้อความ $P_1, P_2, \ldots, P_n$ แต่ละข้อความว่าเป็น**สมมติฐาน** (hypothesis) และเรียกข้อความ Q ว่าเป็น **ข้อสรุป** (conclusion) ของการอ้างเหตุผลนี้. เราอ่านกฎการอนุมาน $\{P_1, P_2, \ldots, P_n\} \therefore Q$ ว่า

สมมติฐาน $P_1, P_2, \ldots, P_n$ ทำให้ได้ข้อสรุป Q

ตาราง 2 แสดงกฎการอนุมานที่ใช้กันมากในการอ้างเหตุผล. ผู้อ่านควรเข้าใจว่า *การสรุปได้ในเชิงตรรก* $(P_1 \wedge P_2 \wedge \ldots \wedge P_n) \Longrightarrow Q$ กับ*กฎการอนุมาน* $\{P_1, P_2, \ldots, P_n\} \therefore Q$ คือการกล่าวถึงสิ่งเดียวกันในสองรูปแบบ. การสรุปได้ในเชิงตรรกเป็นการกล่าวในแง่ความจริงทางตรรกศาสตร์ ส่วนกฎการอนุมานเป็นการกล่าวในแง่ของการประยุกต์ใช้เป็นหลักของการอ้างเหตุผลที่สมเหตุสมผล.

ตาราง 2: กฎการอนุมาน

(p, q, และ r แทนประพจน์ใดๆ, $\mathcal{F}$ แทนประพจน์ใด ๆที่เป็นเท็จ)

สัจนิรันดร์	กฎการอนุมาน	ชื่อกฎ
$p \Longrightarrow p \vee q$	$\{p\} \therefore (p \vee q)$	การเพิ่มทางเลือก (disjunctive addition)
$(p) \wedge (q) \Longrightarrow p \wedge q$	$\{p, q\} \therefore (p \wedge q)$	การเชื่อม (conjunction)
$p \wedge q \Longrightarrow p$	$\{p, q\} \therefore p$	การลดรูปของการเชื่อม (conjunctive simplification)
$(p \vee q) \wedge \sim p \Longrightarrow q$	$\{p \vee q, \sim p\} \therefore q$	การลดรูปของการเลือก (disjunctive simplification) หรือตรรกบทแบบการเลือก (disjunctive syllogism)
$(p \longrightarrow q) \wedge p \Longrightarrow q$	$\{p \longrightarrow q, p\} \therefore q$	โมดัสโพเนนส์ (modus ponens)
$(p \longrightarrow q) \wedge \sim q \Longrightarrow \sim p$	$\{p \longrightarrow q, \sim q\} \therefore \sim p$	โมดัสทอลเลนส์ (modus tollens)
$(p \longrightarrow q) \wedge (q \longrightarrow r) \Longrightarrow p \longrightarrow r$	$\{p \longrightarrow q, q \longrightarrow r\} \therefore (p \longrightarrow r)$	การถ่ายทอดของ $\longrightarrow$ (transitivity of $\longrightarrow$) หรือตรรกบทแบบสมมติฐาน (hypothetical syllogism)
$(p \longleftrightarrow q) \wedge (q \longleftrightarrow r) \Longrightarrow p \longleftrightarrow r$	$\{p \longleftrightarrow q, q \longleftrightarrow r\} \therefore (p \longleftrightarrow r)$	การถ่ายทอดของ $\longleftrightarrow$ (transitivity of $\longleftrightarrow$)
$p \longrightarrow \mathcal{F} \Longrightarrow \sim p$	$\{p \longrightarrow \mathcal{F}\} \therefore \sim p$	การพิสูจน์โดยข้อขัดแย้ง (proof by contradiction)

ตัวอย่าง 1: วันเสาร์วันหนึ่งมีเพื่อนมาหากรรณิการ์ที่บ้าน. สามีของกรรณิการ์บอกกับเพื่อนคนนั้นว่ากรรณิการ์ไม่อยู่ แต่ถ้าอยากพบกรรณิการ์ ให้ไปที่สวนจตุจักรเพราะเธอไปขายของที่นั่นทุกวันเสาร์. ถ้าสามีของกรรณิการ์ไม่ได้พูดเท็จ เพื่อนของกรรณิการ์ควรเชื่อว่าวันนั้นกรรณิการ์อยู่ที่สวนจตุจักรหรือไม่? เพราะเหตุใด?

วิธีทำ ให้ p คือข้อความ “วันนี้เป็นวันเสาร์” และ q คือข้อความ “กรรณิการ์ขายของอยู่ที่สวนจตุจักร”. ถ้าตั้งสมมติฐานว่าสามีของกรรณิการ์ไม่พูดเท็จ แสดงว่าข้อความ $p \longrightarrow q$ เป็นจริง และเนื่องจากวันนั้นเป็น

วันเสาร์ ดังนั้น p เป็นจริง เราจึงสรุปได้อย่างสมเหตุสมผลด้วยกฎโมดัสโพเนนส์ว่า q เป็นจริง ดังนั้นเพื่อนของกรรณิการ์ควรเชื่อว่าเธออยู่ที่สวนจตุจักรในวันนั้น.

❑

ตัวอย่าง 2: จงแสดงว่าสมมติฐาน 4 ข้อคือ *(1) รถไม่ติดและฝนไม่ตก (2) ฉันจะเล่นหมากรุกต่อเมื่อรถติด (3) ถ้าฉันไม่เล่นหมากรุก ฉันจะเล่นฟุตบอล (4) ถ้าฉันเล่นฟุตบอล เสื้อฉันจะสกปรก* ทำให้ได้ข้อสรุปว่า *เสื้อฉันสกปรก.*

<u>*วิธีทำ*</u> ให้ p แทนข้อความ “รถติด”, q แทนข้อความ “ฝนตก”, r แทนข้อความ “ฉันเล่นหมากรุก”, s แทนข้อความ “ฉันเล่นฟุตบอล”, และ t แทนข้อความ “เสื้อฉันสกปรก” ดังนั้นสมมติฐานทั้ง 4 ข้อคือ $\sim p \wedge \sim q$, $r \longrightarrow p$, $\sim r \longrightarrow s$, และ $s \longrightarrow t$ ตามลำดับ และข้อสรุปที่ได้คือ t. เราจะแสดงว่าสมมติฐานทั้งสี่ทำให้ได้ข้อสรุป t ด้วยการอ้างเหตุผลที่สมเหตุสมผลดังต่อไปนี้:

ข้ออ้าง	เหตุผล
1. $\sim p \wedge \sim q$	สมมุติฐาน (1)
2. $\sim p$	จาก 1 โดยใช้กฎการลดรูป
3. $r \longrightarrow p$	สมมติฐาน (2)
4. $\sim r$	จาก 2 และ 3 โดยใช้กฎโมดัสทอลเลนส์
5. $\sim r \longrightarrow s$	สมมติฐาน (3)
6. s	จาก 4 และ 5 โดยใช้กฎโมดัสโพเนนส์
7. $s \longrightarrow t$	สมมติฐาน (4)
8. t	จาก 6 และ 7 โดยใช้กฎโมดัสโพเนนส์

❑

ตัวอย่าง 3: จงแสดงว่าสมมติฐาน 3 ข้อคือ *(1) ถ้าฝนตกและรถติด โจ้จะกลับบ้านดึก (2) ถ้าฝนไม่ตก โจ้จะเล่นฟุตบอล (3) รถติด* ทำให้ได้ข้อสรุปว่า *ถ้าโจ้ไม่เล่นฟุตบอล โจ้จะกลับบ้านดึก.*

<u>*วิธีทำ*</u> ให้ p แทนข้อความ “ฝนตก”, q แทนข้อความ “รถติด”, r แทนข้อความ “โจ้กลับบ้านดึก”, และ s แทนข้อความ “โจ้เล่นฟุตบอล” ดังนั้นสมมติฐานทั้งสามข้อคือ $(p \wedge q) \longrightarrow r$, $\sim p \longrightarrow s$, และ q ตามลำดับ และข้อสรุปที่ได้คือ $\sim s \longrightarrow r$. เราจะแสดงว่าสมมติฐานทั้งสามทำให้ได้ข้อสรุปดังกล่าวด้วยการอ้างเหตุผลที่สมเหตุสมผลดังต่อไปนี้:

ข้ออ้าง	เหตุผล
1. $\sim p \longrightarrow s$	สมมุติฐาน (2)
2. $\sim s \longrightarrow p$	คอนทราโพสิทิฟของข้ออ้าง 1
3. $(p \wedge q) \longrightarrow r$	สมมติฐาน (1)
4. $p \longrightarrow (q \longrightarrow r)$	จาก 3 โดยกฎตรรกศาสตร์ $(p \wedge q) \longrightarrow r \Leftrightarrow p \longrightarrow (q \longrightarrow r)$
5. $\sim s \longrightarrow (q \longrightarrow r)$	จาก 2 และ 4 โดยกฎการถ่ายทอดของ $\longrightarrow$
6. $s \vee (\sim q \vee r)$	จาก 5 โดยกฎตรรกศาสตร์ $p \longrightarrow q \Leftrightarrow \sim p \vee q$
7. $s \vee (r \vee \sim q)$	จาก 6 โดยกฎการสลับที่ของ $\vee$
8. $(s \vee r) \vee \sim q$	จาก 7 โดยกฎการเปลี่ยนหมู่ของ $\vee$
9. q	สมมติฐาน (3)
10. $s \vee r$	จาก 8 และ 9 โดยกฎการลดรูปของการเลือก

11. $\sim s \rightarrow r$ จาก 10 โดยกฎตรรกศาสตร์ $p \rightarrow q \Leftrightarrow \sim p \lor q$

❑

ตัวอย่าง 4: จงแสดงว่าสมมติฐาน “2 หาร 11 ลงตัว หรือ 5 หาร 11 ลงตัว” และ “5 หาร 11 ไม่ลงตัว” ทำให้ได้ข้อสรุปว่า “2 หาร 11 ลงตัว”.

วิธีทำ จะเห็นได้อย่างชัดเจนว่าข้อความ “2 หาร 11 ลงตัว” เป็นข้อสรุปที่สมเหตุสมผลจากสมมติฐานทั้งสองโดยใช้กฎการลดรูปของการเลือก.

ผู้อ่านควรสังเกตว่าข้อสรุป “2 หาร 11 ลงตัว” นี้เป็นเท็จ แม้ว่าจะได้จากการอ้างเหตุผลที่สมเหตุสมผลก็ตาม. (เพราะเหตุใด?)

❑

ตัวอย่าง 4 ข้างบนแสดงให้เห็นว่า แม้ว่าการอ้างเหตุผลจะสมเหตุสมผล แต่ข้อสรุปที่ได้อาจเป็นเท็จก็ได้ ถ้าหากมีสมมติฐานบางข้อเป็นเท็จ. อย่างไรก็ตาม ถ้าสมมติฐานทุกข้อเป็นความจริงและเราใช้การอ้างเหตุผลที่สมเหตุสมผลทุกขั้นตอน เราจะมั่นใจได้ว่าข้อสรุปที่ได้จะต้องเป็นความจริง. (เพราะเหตุใด?)

กฎการอนุมานสำหรับข้อความบ่งปริมาณ

(Rules of Inference for Quantified Statements)

มีกฎการอนุมานเกี่ยวกับข้อความที่มีตัวบ่งปริมาณหลายกฎที่ใช้บ่อยในการอ้างเหตุผลและการพิสูจน์ทางคณิตศาสตร์ แต่เป็นการใช้โดยละไว้ในฐานที่เข้าใจเสียมาก. หัวข้อย่อยนี้จะประกาศกฎที่ถูกใช้อย่างแฝงเร้นเหล่านี้อย่างเป็นทางการ.

กฎการอนุมานข้อแรกเรียกว่า**กฎนัยทั่วไปสู่นัยจำเพาะ** (universal instantiation) ซึ่งมีใจความว่า *“ถ้าข้อความ P(x) เป็นจริงสำหรับทุก x ∈ U และ a เป็นสมาชิกตัวหนึ่งใน U, จะสรุปได้ว่า P(a) เป็นจริง”*. เราเขียนกฎการอนุมานนี้ในรูปสัญลักษณ์ได้ดังนี้.

กฎนัยทั่วไปสู่นัยจำเพาะ (Universal Instantiation)

$$\begin{array}{l} \forall x \in U\ P(x) \\ a \in U \\ \hline \therefore\ P(a) \end{array}$$

ตัวอย่างการอ้างเหตุผลโดยใช้กฎการอนุมานนี้ได้แก่

สมมติฐาน:	*มนุษย์ทุกคนต้องตาย*
สมมติฐาน:	*กาลิเลโอเป็นมนุษย์*
ข้อสรุป:	∴ *กาลิเลโอต้องตาย*

สัจพจน์, บทนิยาม, และทฤษฎีบทส่วนใหญ่ในคณิตศาสตร์เป็นข้อความที่แสดงความจริงโดยทั่วไปเช่น “x+y = y+x สำหรับทุกจำนวนจริง x และ y”. จากความจริงในรูปทั่วไปเช่นนี้ เราสรุปได้ความจริง

เฉพาะเช่น 2+π = π+2 โดยใช้*กฎนัยทั่วไปสู่นัยจำเพาะ* เพราะเราทราบว่าทั้ง 2 และ π ล้วนเป็นจำนวนจริง.

กฎการอนุมานข้อที่สองเรียกว่า**กฎนัยจำเพาะสู่นัยทั่วไป** (universal generalization) ซึ่งมีใจความว่า *"ถ้าข้อความ P(a) เป็นจริงสำหรับ a ใดๆ ในเซต U, จะสรุปได้ว่า P(x) เป็นจริงสำหรับทุก x $\in$ U"*. เราเขียนกฎการอนุมานนี้ในรูปสัญลักษณ์ได้ดังนี้.

กฎนัยจำเพาะสู่นัยทั่วไป (Universal Generalization)

a เป็นสมาชิกใดๆ ใน U
P(a)
___
$\therefore$ $\forall x \in U\ P(x)$

ข้อความ "a เป็นสมาชิกใดๆ ใน U" หมายความว่าเรามิได้กำหนดเฉพาะเจาะจงว่า a เป็นสมาชิกตัวใดในเอกภพ U นั่นคือ a เป็น*สมาชิกตัวใดก็ได้*ใน U. ในเมื่อเราไม่ได้สนใจว่า c คือตัวไหน เราจึงยังคงอ้างถึงมันในรูปตัวแปร.

ตัวอย่างการอ้างเหตุผลโดยใช้กฎการอนุมานนี้ได้แก่

สมมติฐาน:	*a เป็นมนุษย์ (คนใดก็ได้)*
สมมติฐาน:	*a ต้องตาย*
ข้อสรุป:	$\therefore$ *มนุษย์ทุกคนต้องตาย*

เรามักใช้*กฎนัยเฉพาะสู่นัยทั่วไป*ในการพิสูจน์ทฤษฎีบทที่อยู่ในรูป $\forall x\ P(x)$. วิธีการคือเราให้ x เป็นสมาชิกใดๆในเอกภพที่ไม่เฉพาะเจาะจง (ดังนั้นเราจึงอ้างถึงมันในรูปตัวแปร x) จากนั้นก็พยายามแสดงว่า P(x) เป็นสำหรับ x นั้น. เมื่อแสดงว่า P(x) เป็นจริงได้แล้ว ก็สรุปได้ว่า P(x) เป็นจริงสำหรับทุก x ในเอกภพ. โดยทั่วไปเราจะใช้กฎนี้โดยละไว้ในฐานที่เข้าใจ นั่นคือเมื่อแสดงได้แล้วว่า P(x) เป็นจริงสำหรับ x ใดๆ ก็ถือว่าเราพิสูจน์ $\forall x\ P(x)$ แล้วโดยปริยาย.

เรามีกฎการอนุมานที่เกี่ยวกับข้อความที่มี*การบ่งปริมาณการมี*เช่นกัน. กฎการอนุมานข้อที่สามเรียกว่า**กฎการมีของสิ่งที่มีอยู่** (existential instantiation) ซึ่งมีใจความว่า *"ถ้ามี x อย่างน้อยหนึ่งตัวในเซต U ที่ทำให้ P(x) เป็นจริง, จะสรุปได้ว่ามีสมาชิก a บางตัวใน U ที่ P(a) เป็นจริง"* หรือเขียนในรูปสัญลักษณ์ได้ดังนี้:

กฎการมีของสิ่งที่มีอยู่ (Existential Instantiation)

$\exists x \in U\ P(x)$
___
$\therefore$ P(a) สำหรับ a บางตัวใน U

เมื่อเราทราบความจริงที่อยู่ในรูป $\exists x \in U\ P(x)$, โดย*กฎการมีของสิ่งที่มีอยู่* เราสามารถอ้างถึงสมาชิก a ตัวหนึ่งใน U ที่ทำให้ P(a) เป็นจริงได้. โดยทั่วไปแล้ว เรามักจะไม่สนใจว่าเป็น a ตัวไหน เพียง

แต่เรารู้ว่าจะต้องมี a ตัวนั้นอยู่ ดังนั้นเราจะตั้งชื่อมันว่า a แล้วใช้ความจริงของ P(a) เป็นประโยชน์ในการอ้างเหตุผลในบริบทนั้น.

กฎการอนุมานสุดท้ายที่เราจะกล่าวถึงในหัวข้อย่อยนี้เรียกว่า**กฎการพิสูจน์การมี** (existential generalization) ซึ่งมีใจความว่า *"ถ้า $a \in U$ และ P(a) เป็นจริง, จะสรุปได้ว่า มี x อย่างน้อยหนึ่งตัวใน U ที่ P(x) เป็นจริง"* หรือเขียนในรูปสัญลักษณ์ได้ดังนี้:

กฎการพิสูจน์การมี (Existential Generalization)

$$\begin{array}{l} a \in U \\ P(a) \\ \hline \therefore \exists x \in U\ P(x) \end{array}$$

กฎการพิสูจน์การมี ให้วิธีการที่ตรงไปตรงมาวิธีหนึ่งในการพิสูจน์ข้อความที่อยู่ในรูป $\exists x \in U$ P(x). นั่นคือถ้าเพียงเราสามารถหาสมาชิก a ใน U ได้สักตัวหนึ่งที่ทำให้ P(a) เป็นจริง, ก็เป็นอันว่าเราได้พิสูจน์ข้อความ $\exists x \in U$ P(x) แล้ว.

ตัวอย่างเช่นเราต้องการพิสูจน์ว่า "มีจำนวนคู่บางตัวที่ 3 หารลงตัว". เราค้นพบจำนวนคู่ตัวหนึ่งคือ 6 ซึ่ง 3 หารลงตัว. ด้วยกฎการพิสูจน์การมี การค้นพบนี้เพียงพอแล้วที่จะสรุปว่าข้อความที่เราต้องการพิสูจน์เป็นความจริง.

ตัวอย่าง 5: เราให้นิยามของ *จำนวนคู่ (even number)* ว่า "จำนวนเต็ม x ใดๆ เป็นจำนวนคู่ ถ้ามีจำนวนเต็ม k บางตัวซึ่ง x = 2k". จงพิสูจน์ว่า "สำหรับทุกจำนวนคู่ x, x^2 เป็นจำนวนคู่".

วิธีทำ เราพิสูจน์เป็นขั้นตอนดังนี้:

ข้ออ้าง	**เหตุผล**
1. ให้ n เป็นจำนวนคู่ใดๆ	กำหนดให้
2. มีจำนวนเต็ม k บางตัวซึ่ง n = 2k	จาก 1 โดยนิยามของจำนวนคู่
3. ให้ c เป็นจำนวนเต็มซึ่ง n = 2c	จาก 2 โดยกฎการมีของสิ่งที่มีอยู่
4. $n^2 = (2c)^2 = 2(2c^2)$	จาก3 โดยการยกกำลังสองทั้งสองข้างของสมการ
5. $2c^2$ เป็นจำนวนเต็ม	จาก 3, c เป็นจำนวนเต็ม และจำนวนเต็มมีสมบัติปิดสำหรับการคูณ
6. มีจำนวนเต็ม k บางตัวซึ่ง $n^2 = 2k$	จาก 4, 5 โดยกฎการพิสูจน์การมี
7. n^2 เป็นจำนวนคู่	จาก 6 โดยนิยามของจำนวนคู่
8. สำหรับทุกจำนวนคู่ x, x^2 เป็นจำนวนคู่	จาก 1, 7 โดยกฎนัยจำเพาะสู่นัยทั่วไป

❑

การอ้างเหตุผลที่ไม่สมเหตุสมผล (Invalid Argument)

เราทราบจากหัวข้อย่อยที่ผ่านมาว่าการอ้างเหตุผลที่สมเหตุสมผลมีรากฐานมาจากกฎการอนุมานในตรรกศาสตร์. ในหัวข้อย่อยนี้ เราจะมาทำความรู้จักกับการอ้างเหตุผลที่ไม่ถูกต้องซึ่งมักใช้ในวงการเมืองแต่ไม่มีประโยชน์ใดๆในคณิตศาสตร์.

เราทราบแล้วว่าประพจน์ประกอบในรูป $(P_1 \wedge P_2 \wedge \ldots \wedge P_n) \longrightarrow Q$ ที่เป็นสัจนิรันดร์ ทำให้เราได้กฎการอนุมานซึ่งเป็นหลักการอ้างเหตุผลที่สมเหตุสมผล. แต่ถ้าประพจน์ประกอบในรูป $(P_1 \wedge P_2 \wedge \ldots \wedge P_n) \longrightarrow Q$ <u>ไม่</u>เป็นสัจนิรันดร์ แสดงว่าเมื่อให้สมมติฐาน $P_1, P_2, \ldots, P_n$ เป็นจริง ข้อสรุป Q อาจไม่เป็นจริงก็ได้ ดังนั้นประพจน์ประกอบเหล่านี้ไม่อาจใช้เป็นกฎการอนุมานได้. เราเรียกการอ้างเหตุผล $\{P_1, P_2, \ldots, P_n\} \therefore Q$ ที่มีรากฐานมาจากประพจน์ประกอบในรูป $(P_1 \wedge P_2 \wedge \ldots \wedge P_n) \longrightarrow Q$ ที่ไม่เป็นสัจนิรันดร์ว่า **การอ้างเหตุผลที่ไม่สมเหตุสมผล** (invalid argument) หรือ**การสรุปผิดหลักเหตุผล** (fallacy).

ตัวอย่างเช่นประพจน์ประกอบ $(p \vee q) \longrightarrow p$ ไม่เป็นสัจนิรันดร์เพราะเป็นไปได้ว่า $p \vee q$ เป็นจริง แต่ p เป็นเท็จ นั่นคือกรณีที่ p เป็นเท็จและ q เป็นจริง. ดังนั้นเมื่อเราตั้งสมมติฐานว่า "วันนี้เป็นวันเสาร์หรือเป็นวันอาทิตย์" แล้วสรุปว่า "วันนี้เป็นวันเสาร์" จึงถือเป็นการสรุปผิดหลักเหตุผล ถึงแม้ว่าวันนี้จะบังเอิญเป็นวันเสาร์จริงๆก็ตาม.

$\{p \longrightarrow q, q\} \therefore p$ เป็นอีกรูปแบบหนึ่งของการอ้างเหตุผลที่ไม่สมเหตุสมผลที่เรียกว่า **การสรุปผิดหลักเหตุผลโดยการยืนยันข้อสรุป** (fallacy of affirming the conclusion) ทั้งนี้เพราะประพจน์ประกอบ $((p \longrightarrow q) \wedge q)) \longrightarrow p$ ไม่เป็นสัจนิรันดร์.

ตัวอย่าง 6: การอ้างเหตุผลต่อไปนี้สมเหตุสมผลหรือไม่:

ถ้าตี๋ใหญ่เป็นผู้บริสุทธิ์ ศาลจะยกฟ้องตี๋ใหญ่. เนื่องจากศาลยกฟ้องตี๋ใหญ่ จึงสรุปได้ว่าตี๋ใหญ่เป็นผู้บริสุทธิ์.

<u>*วิธีทำ*</u> ถ้าให้ p แทนข้อความ "ตี๋ใหญ่เป็นผู้บริสุทธิ์" และ q แทน "ศาลยกฟ้องตี๋ใหญ่", การอ้างเหตุผลดังกล่าวอยู่ในรูปของ $\{p \longrightarrow q, q\} \therefore p$ ซึ่งเป็น*การสรุปผิดหลักเหตุผลโดยการยืนยันข้อสรุป* ดังนั้นจึงเป็นการอ้างเหตุผลที่ไม่สมเหตุสมผล.

เราไม่อาจสรุปว่า "ตี๋ใหญ่เป็นผู้บริสุทธิ์" จากสมมติฐานทั้งสอง เพราะแม้ว่าศาลจะยกฟ้องตี๋ใหญ่ถ้าตี๋ใหญ่บริสุทธิ์ แต่ถ้าศาลมีหลักฐานไม่เพียงพอ ศาลก็จะยกฟ้องเขาเช่นกัน ดังนั้นการที่ศาลยกฟ้องเขาจึงไม่อาจสรุปได้ว่าเขาบริสุทธิ์.

❑

$\{p \longrightarrow q, \sim p\} \therefore \sim q$ ก็เป็นอีกรูปแบบหนึ่งของการอ้างเหตุผลที่ไม่สมเหตุสมผลที่เรียกว่า **การสรุปผิดหลักเหตุผลโดยการปฏิเสธสมมติฐาน** (fallacy of denying the hypothesis) ทั้งนี้เพราะประพจน์ประกอบ $((p \longrightarrow q) \wedge \sim p)) \longrightarrow \sim q$ ไม่เป็นสัจนิรันดร์.

ตัวอย่าง 7: การอ้างเหตุผลต่อไปนี้สมเหตุสมผลหรือไม่:

ให้ n เป็นจำนวนเต็ม. ถ้า $n > 2$, จะได้ $n^2 > 4$. แต่ $n \le 2$ ดังนั้น $n^2 \le 4$.

<u>*วิธีทำ*</u> การอ้างเหตุผลนี้คือ

$$[n > 2] \rightarrow [n^2 > 4]$$
$$n \leq 2$$
$$\therefore n^2 \leq 4$$

ซึ่งอยู่ในรูป $\{p \rightarrow q, \sim p\} \therefore \sim q$ ดังนั้นจึงเป็น*การสรุปผิดหลักเหตุผลโดยการปฏิเสธสมมติฐาน* ซึ่งเป็นการอ้างเหตุผลที่ไม่สมเหตุสมผล.

เราไม่อาจสรุปว่า $n^2 \leq 4$ จากสมมติฐานทั้งสอง เพราะอาจเป็นไปได้ว่าเมื่อ $n \leq 2$ แล้ว $n^2 > 4$ เช่นในกรณีที่ n = -3 เป็นต้น.

❑

การสรุปผิดหลักเหตุผลอีกรูปแบบหนึ่งที่มักเกิดขึ้นอย่างแฝงเร้นจนเราแทบไม่รู้ตัวคือ ขณะที่เรากำลังพิสูจน์ข้อความ P อยู่นั้น เราเผลอไปตั้งสมมติฐานว่า P (หรือข้อความที่สมมูลเชิงตรรกกับ P) เป็นจริง แล้วในที่สุดก็ได้ข้อสรุปว่า P เป็นจริง. การสรุปว่าข้อความใดจริงโดยใช้สมมติฐานว่าข้อความนั้นจริงเท่ากับว่าเราไม่ได้พิสูจน์อะไรเลย จึงถือเป็นการอ้างเหตุผลที่ไม่สมเหตุสมผลที่เรียกว่า **การให้เหตุผลวนเป็นวงกลม** (circular reasoning) หรือ**การสรุปผิดหลักเหตุผลโดยการอ้างตัวเอง** (fallacy of begging the question).

ตัวอย่าง 8: บทพิสูจน์ของทฤษฎีบทต่อไปนี้ใช้การอ้างเหตุผลที่สมเหตุสมผลหรือไม่? เพราะเหตุใด?

ทฤษฎีบท: ให้ d เป็นจำนวนเต็มบวกใดๆ และให้ A และ B เป็นจำนวนเต็มใดๆ โดยที่ d หาร A ลงตัวแต่ d หาร B ไม่ลงตัว. จะได้ว่า d หาร A+B ไม่ลงตัว.

บทพิสูจน์:

ข้ออ้าง	**เหตุผล**
1. d หาร A ลงตัว	ข้อกำหนดของทฤษฎี
2. ให้ k เป็นจำนวนเต็มซึ่ง A = kd	จาก 1 โดยนิยามของการหารลงตัว
3. d หาร B ไม่ลงตัว	ข้อกำหนดของทฤษฎี
4. ให้ q และ r เป็นจำนวนเต็มซึ่ง B = qd+r โดยที่ $0 < r < d$.	จาก 3 โดยทฤษฎีบทขั้นตอนวิธีการหาร (division algorithm theorem)
5. A+B = kd+qd+r = (k+q)d+r	จาก 2, 3
6. d หาร (k+q)d ลงตัว	d เป็นตัวประกอบของจำนวนเต็ม (k+q)d
7. d หาร r ไม่ลงตัว	จาก 4 เพราะ $0 < r < d$
8. d หาร (k+q)d+r = A+B ไม่ลงตัว	จาก 6, 7

วิธีทำ ขั้นตอนที่ไม่สมเหตุสมผลคือการสรุปข้ออ้าง 8 จากข้ออ้าง 6 และ 7 เพราะเป็นการประยุกต์ใช้ทฤษฎีบทที่เรากำลังพิสูจน์อยู่นั่นเอง. นี่คือตัวอย่างของ*การให้เหตุผลวนเป็นวงกลม* หรือที่เรียกอีกอย่างหนึ่งว่า*การสรุปผิดหลักเหตุผลโดยการอ้างตัวเอง*.

❑

การสรุปผิดหลักเหตุผลอีกแบบหนึ่งที่พบบ่อยคือ **การใช้ความจริงในบางกรณีสรุปความจริงทั่วไป** ซึ่งเกิดขึ้นเมื่อเราแสดงให้เห็นว่า P(c) เป็นจริงสำหรับ c บางตัวแล้วสรุปว่า $\forall x\, P(x)$. ตัวอย่างเช่นเราพิสูจน์ว่า “ผลบวกของจำนวนคู่กับจำนวนคี่เป็นจำนวนคี่เสมอ” โดยอ้างเหตุผลดังนี้

2 เป็นจำนวนคู่ และ 1 เป็นจำนวนคี่. เราได้ 2+1 = 3 เป็นจำนวนคี่. ดังนั้นผลบวกของจำนวนคู่กับจำนวนคี่ต้องเป็นจำนวนคี่เสมอ.

ผู้อ่านคงเห็นได้ชัดเจนว่า การอ้างเหตุผลแบบนี้ไม่สมเหตุสมผลเพราะความจริงเพียงบางกรณีไม่อาจใช้ยืนยันความจริงในทุกกรณีได้. อย่างไรก็ตาม นักเรียนมักใช้การอ้างเหตุผลแบบนี้ในข้อสอบในยามจนปัญญาเพื่อหวังได้คะแนนสงสาร แต่หารู้ไม่ว่าอาจารย์ผู้ตรวจข้อสอบส่วนใหญ่จะรู้สึกหดหู่แต่ไม่สงสาร.

การใช้ตัวแปรตัวเดียวกันแทนสิ่งสองสิ่งที่แตกต่างกัน ก็เป็นข้อผิดพลาดในการอ้างเหตุผลที่พบมาก. พิจารณาการพิสูจน์ต่อไปนี้:

ให้ m เป็นจำนวนคู่ใดๆ และ n เป็นจำนวนคี่ใดๆ. โดยนิยามของจำนวนคู่และจำนวนคี่จะได้ $m = 2k$ และ $n = 2k+1$ สำหรับจำนวนเต็ม k บางตัว. ดังนั้น $m+n = 2k+2k+1 = 2(2k)+1$ ซึ่งเป็นจำนวนคี่เพราะ $2k$ เป็นจำนวนเต็ม. เพราะฉะนั้นสรุปได้ว่า ผลบวกของจำนวนคู่และจำนวนคี่จะเป็นจำนวนคี่เสมอ.

ข้อบกพร่องในการอ้างเหตุผลข้างบนคือ การให้ $m = 2k$ และ $n = 2k+1$ สำหรับจำนวนเต็ม k ตัวเดียวกัน ซึ่งไม่จริงเสมอไป. เมื่อ m เป็นจำนวนคู่และ n เป็นจำนวนคี่, เป็นความจริงที่มีจำนวนเต็ม j ที่ $m = 2j$ และมีจำนวนเต็ม k ที่ $n = 2k+1$ แต่ j ไม่จำเป็นต้องเท่ากับ k. ดังนั้นการพิสูจน์ที่ถูกต้องควรเป็นดังนี้:

ให้ m เป็นจำนวนคู่ใดๆ และ n เป็นจำนวนคี่ใดๆ. โดยนิยามของจำนวนคู่และจำนวนคี่จะได้ $m = 2j$ และ $n = 2k+1$ สำหรับจำนวนเต็ม j และ k บางตัว. ดังนั้น $m+n = 2j+2k+1 = 2(j+k)+1$ ซึ่งเป็นจำนวนคี่เพราะ $j+k$ เป็นจำนวนเต็ม. เพราะฉะนั้นสรุปได้ว่า ผลบวกของจำนวนคู่และจำนวนคี่จะเป็นจำนวนคี่เสมอ.

3.3 วิธีการพิสูจน์ (Methods of Proof)

กลยุทธ์พื้นฐาน (Basic Strategies)

ดังที่กล่าวแล้วในหัวข้อ 3.1 ทฤษฎีบททางคณิตศาสตร์เป็นข้อความที่จะต้องพิสูจน์ว่าเป็นจริง. ข้อความในทฤษฎีบทโดยทั่วไปจะมีองค์ประกอบสองส่วนใหญ่ๆ คือ *กลุ่มข้อกำหนด* และ *ข้อสรุป* ของทฤษฎีบทนั้น. ตัวอย่างเช่นทฤษฎีบทขั้นตอนวิธีการหารในหัวข้อ 2.5 กล่าวว่า

ให้ a เป็นจำนวนเต็มใดๆ และ d เป็นจำนวนเต็มบวกใดๆ. จะมีจำนวนเต็ม q และ r โดย $0 \leq r < d$ *เพียงคู่เดียวเท่านั้นที่ทำให้* $a = qd + r$.

ข้อกำหนดของทฤษฎีบทนี้มีสองข้อคือ 1) *a เป็นจำนวนเต็มใดๆ* และ 2) *d เป็นจำนวนเต็มบวกใดๆ* และข้อสรุปของทฤษฎีบทนี้คือ *มีจำนวนเต็ม q และ r โดย* $0 \leq r < d$ *เพียงคู่เดียวเท่านั้นที่ทำให้* $a = qd+r$.

การพิสูจน์ทฤษฎีบทก็คือการแสดงให้เห็นว่า *ข้อสรุปของทฤษฎีบทนั้นเป็นจริงบนเงื่อนไขของข้อกำหนดทุกข้อของทฤษฎีบทนั้น*. นั่นคือถ้าให้ P_1, P_2, ..., P_n แทนข้อกำหนด n ข้อของทฤษฎีบทและให้ C แทนข้อสรุปของทฤษฎีบท, การพิสูจน์ทฤษฎีบทก็คือการแสดงให้เห็นว่าข้อความ $(P_1 \wedge P_2 \wedge \ldots \wedge P_n) \rightarrow C$ เป็นจริงนั่นเอง. ดังนั้นโครงร่างมาตรฐานของบทพิสูจน์คือ

1. *ตั้งสมมติฐานว่าข้อกำหนดทุกข้อของทฤษฎีบทเป็นจริง*
2. *ใช้การอ้างเหตุผลที่สมเหตุสมผลแสดงให้เห็นว่าข้อสรุปของทฤษฎีบทเป็นจริง*

การเขียนบทพิสูจน์โดยทั่วไปมักจะละการตั้งสมมติฐานในขั้นตอนที่หนึ่งข้างบนไว้ในฐานที่เข้าใจ. ส่วนในขั้นตอนที่สอง ผู้พิสูจน์สามารถอ้างความจริงต่างๆของระบบคณิตศาสตร์นั้น อันได้แก่สัจพจน์, บทนิยาม, และทฤษฎีบทอื่นที่พิสูจน์แล้ว รวมทั้งข้อกำหนดทุกข้อของทฤษฎีบทที่กำลังพิสูจน์อยู่ และใช้การอ้างเหตุผลที่สมเหตุสมผลเพื่อแสดงให้ได้ว่าข้อสรุปของทฤษฎีบทเป็นความจริงในที่สุด.

ลักษณะของข้อสรุปทฤษฎีบทก็มีส่วนกำหนดวิธีการที่ใช้ในการพิสูจน์. ข้อสรุปของทฤษฎีบทต่างๆมีได้หลายลักษณะ. ลักษณะหลักๆที่สำคัญได้แก่

1. **ข้อความเดี่ยว** เช่น *$\sqrt{2}$ เป็นจำนวนอตรรกยะ.*
2. **ข้อความในรูป $P \rightarrow Q$** เช่น *ถ้า d หาร a ลงตัว, จะได้ d หาร ak ลงตัวสำหรับทุกจำนวนเต็ม k.*
3. **ข้อความในรูป $P \leftrightarrow Q$** เช่น *$a \equiv b \pmod d$ เมื่อและต่อเมื่อ $a \bmod d = b \bmod d$.*
4. **ข้อความในรูป $P \wedge Q$** เช่น *2 หาร n ลงตัวและ 3 หาร n ลงตัว.*
5. **ข้อความในรูป $P \vee Q$** เช่น *m เป็นจำนวนคู่หรือ n เป็นจำนวนคู่.*
6. **ข้อความในรูป $\forall x \forall y \ldots P(x,y,\ldots)$** เช่น *d หาร (xa+yb) ลงตัวสำหรับทุกจำนวนเต็ม x และ y.*
7. **ข้อความในรูป $\exists x \exists y \ldots P(x,y,\ldots)$** เช่น *มีจำนวนเต็ม q และ r โดย $0 \leq r < d$ เพียงคู่เดียวเท่านั้นที่ทำให้ $a = qd+r$.*

เราจะศึกษาเทคนิคการพิสูจน์ข้อความลักษณะต่าง ๆเหล่านี้ในหัวข้อย่อยต่อ ๆไป.

การเขียนบทพิสูจน์

จริง ๆแล้ว เราไม่มีสิ่งที่เรียกว่าแบบฟอร์มมาตรฐานในการเขียนบทพิสูจน์ทางคณิตศาสตร์แต่อย่างใด. ลักษณะการเขียนบทพิสูจน์ขึ้นกับว่าผู้เขียนเป็นใครและเขียนให้ใครอ่าน. อาจารย์เขียนให้นักเรียนอ่าน หรือนักเรียนเขียนให้เพื่อนนักเรียนอ่าน หรือนักคณิตศาสตร์เขียนให้นักคณิตศาสตร์ด้วยกันอ่าน ล้วนมีมาตรฐานที่แตกต่างกันไป.

สำหรับผู้ที่เริ่มต้นเรียนรู้เทคนิคการพิสูจน์และต้องการทำความเข้าใจกลไกของการอ้างเหตุผลอย่างละเอียด เราอาจเขียนบทพิสูจน์เป็นข้อ ๆ ที่แสดงข้ออ้างและเหตุผลที่ชัดเจนดังตัวอย่าง 5 และ 8 ในหัวข้อที่แล้ว. ตัวอย่างเช่น ถ้าเราต้องการพิสูจน์ทฤษฎีบทต่อไปนี้

***ทฤษฎีบท**: ผลบวกของจำนวนคี่สองตัวเป็นจำนวนคู่เสมอ.*

เราอาจเขียนบทพิสูจน์โดยแสดงขั้นตอนและเหตุผลโดยละเอียดดังต่อไปนี้:

บทพิสูจน์:

ข้ออ้าง	**เหตุผล**
1. ให้ a และ b เป็นจำนวนคี่	สมมติฐาน
2. ให้ m เป็นจำนวนเต็มซึ่ง $a = 2m+1$.	จาก 1 และนิยามของจำนวนคี่
3. ให้ n เป็นจำนวนเต็มซึ่ง $b = 2n+1$	จาก 1 และนิยามของจำนวนคี่
4. $a+b = 2m+1+2n+1 = 2(m+n+1)$	จาก 2, 3
5. มีจำนวนเต็ม k ที่ทำให้ $a+b = 2k$	จาก 4, ให้ $k = m+n+1$
6. $a+b$ เป็นจำนวนคู่	จาก 5 และนิยามของจำนวนคู่
7. ทฤษฎีบทนี้เป็นจริง	สมมติฐาน 1 ทำให้ได้ข้อสรุป 6

การเขียนบทพิสูจน์เป็นขั้นตอนในลักษณะ *ข้ออ้าง-เหตุผล* แบบข้างบน แม้ว่าจะแสดงกลไกการอ้างข้อความและเหตุผลที่ชัดเจนแจ่มแจ้ง แต่กลับอ่านได้ไม่สะดวกนัก. เพื่อให้อ่านได้ลื่นไหลดีขึ้น เราอาจเขียนบทพิสูจน์ในลักษณะกึ่งความเรียงที่ยังคงมีหมายเลขข้อความเพื่อสะดวกแก่การอ้างอิง. เราเขียนบทพิสูจน์ข้างบนในลักษณะกึ่งความเรียงได้ดังนี้:

บทพิสูจน์:

1. สมมติให้ a และ b เป็นจำนวนคี่.
2. ดังนั้นจากนิยามของจำนวนคี่ $a = 2m+1$ และ $b = 2n+1$ สำหรับจำนวนเต็ม m และ n บางตัว.
3. จาก 2 เราได้ $a+b = 2m+1+2n+1 = 2(m+n+1)$.
4. จาก 3 เนื่องจาก $m+n+1$ เป็นจำนวนเต็ม ดังนั้น 2 หาร $a+b$ ลงตัว.
5. จาก 4 และนิยามของจำนวนคู่ เราได้ $a+b$ เป็นจำนวนคู่.
6. เนื่องจากสมมติฐาน 1 ทำให้ได้ข้อสรุป 5 ดังนั้นทฤษฎีบทนี้เป็นจริง.

อย่างไรก็ตาม นักคณิตศาสตร์ส่วนใหญ่นิยมเขียนบทพิสูจน์ในลักษณะความเรียงที่ปราศจากหมายเลขข้อความ และใช้การอ้างเหตุผลแบบค่อนข้างรวบรัดดังนี้

บทพิสูจน์: *สมมติให้ a และ b เป็นจำนวนคี่. ดังนั้น a = 2m+1 และ 2n+1 สำหรับจำนวนเต็ม m และ n บางตัว. เราได้ a+b = 2m+1+2n+1 = 2(m+n+1). นั่นคือ 2 หาร a+b ลงตัว ดังนั้น a+b เป็นจำนวนคู่. เพราะฉะนั้นเราได้แสดงแล้วว่าทฤษฎีบทนี้เป็นจริง.*

สำหรับในบทนี้ซึ่งเรากำลังจะเรียนรู้เทคนิคการพิสูจน์แบบต่างๆ เราจะใช้การเขียนแบบที่สองซึ่งเป็นทางสายกลางที่ดี เพราะยังคงแสดงโครงสร้างการอ้างเหตุผลที่ค่อนข้างชัดเจนแต่เป็นกึ่งความเรียงที่อ่านได้ลื่นไหลกว่าแบบที่หนึ่ง แต่ไม่รวบรัดเกินไปสำหรับมือใหม่หัดพิสูจน์อย่างแบบที่สาม. ให้สังเกตด้วยว่า หนังสือเล่มนี้จะใช้สัญลักษณ์ แสดงการจบบทพิสูจน์.

การพิสูจน์ข้อความในรูป P⟶Q โดยวิธีตรง (Direct Proof)

ข้อสรุปของทฤษฎีบทที่พบบ่อยที่สุดคือข้อสรุปที่อยู่ในรูป P⟶Q. เราสามารถแสดงให้เห็นว่าข้อความ P⟶Q เป็นจริงได้โดย*การตั้งสมมติฐานว่า P เป็นจริงแล้วแสดงให้ได้ว่า Q จะต้องเป็นจริงเช่นกัน.* การพิสูจน์ P⟶Q ด้วยวิธีนี้เรียกว่า **การพิสูจน์โดยวิธีตรง** (direct proof) ซึ่งมีเค้าโครงดังนี้:

สมมติข้อความ P.
พิสูจน์ข้อความ Q.
ดังนั้น P⟶Q.

ตัวอย่าง 1: จงพิสูจน์ทฤษฎีบทต่อไปนี้ด้วยการพิสูจน์โดยวิธีตรง.

ทฤษฎีบท: *ให้ d เป็นจำนวนเต็มบวกและให้ A และ B เป็นจำนวนเต็ม. ถ้า d หาร A ลงตัวแต่ d หาร B ไม่ลงตัว, จะได้ว่า d หาร A+B ไม่ลงตัว.*

<u>วิธีทำ</u> ข้อสรุปของทฤษฎีบทนี้คือ *"ถ้า d หาร A ลงตัวแต่ d หาร B ไม่ลงตัว, จะได้ว่า d หาร A+B ไม่ลงตัว."* ซึ่งอยู่ในรูป P⟶Q. การพิสูจน์โดยวิธีตรงทำได้โดยการตั้งสมมติฐานว่า "d หาร A ลงตัวและ d หาร B ไม่ลงตัว" แล้วใช้สมมติฐานเหล่านี้แสดงให้เห็นว่า "d หาร A+B ไม่ลงตัว" ดังบทพิสูจน์ต่อไปนี้.

บทพิสูจน์:

1. สมมติให้ d หาร A ลงตัวและ d หาร B ไม่ลงตัว.
2. ดังนั้น จากนิยามของการหารลงตัว, A = kd สำหรับจำนวนเต็ม k บางตัว.
3. เนื่องจาก $d \nmid B$, จากทฤษฎีบทขั้นตอนวิธีการหาร เราได้ B = qd+r สำหรับจำนวนเต็ม q และ r บางตัวโดย $0 < r < d$.
4. จาก 2 และ 3 เราได้ A+B = kd+qd+r = (k+q)d+r, $0 < r < d$.
5. จาก 4 โดยทฤษฎีบทขั้นตอนวิธีการหาร, r คือเศษเหลือของการหาร A+B ด้วย d, และเนื่องจาก $r \neq 0$ ดังนั้น d หาร A+B ไม่ลงตัว.
6. สมมติฐาน 1 ทำให้ได้ข้อสรุป 5, ดังนั้นทฤษฎีบทนี้เป็นจริง.

❑

ตัวอย่าง 2: จงพิสูจน์ทฤษฎีบทต่อไปนี้ด้วยการพิสูจน์โดยวิธีตรง.

ทฤษฎีบท: *ให้ d เป็นจำนวนเต็มบวกที่มากกว่า 1 และให้ a เป็นจำนวนเต็ม. ถ้า d หาร a ลงตัว, จะได้ว่า d หาร a+1 ไม่ลงตัว.*

วิธีทำ ข้อสรุปของทฤษฎีบทนี้คือ *"ถ้า d หาร a ลงตัว, จะได้ว่า d หาร a+1 ไม่ลงตัว."* ซึ่งอยู่ในรูป $P \longrightarrow Q$. การพิสูจน์โดยวิธีตรงทำได้โดยการตั้งสมมติฐานว่า "d หาร a ลงตัว" แล้วใช้สมมติฐานเหล่านี้แสดงให้เห็นว่า "d หาร a+1 ไม่ลงตัว" ดังบทพิสูจน์ต่อไปนี้.

บทพิสูจน์:

1. สมมติให้ d หาร a ลงตัว.
2. ดังนั้น จากนิยามของการหารลงตัว, $a = kd$ สำหรับจำนวนเต็ม k บางตัว.
3. จาก 2 เราได้ $a+1 = kd+1$.
4. จาก 3, เนื่องจาก $0 < 1 < d$ (ตามข้อกำหนดของทฤษฎีบท), ดังนั้น 1 คือเศษเหลือของการหาร a+1 ด้วย d.
5. จาก 4 สรุปได้ว่า d หาร a+1 ไม่ลงตัว.
6. สมมติฐาน 1 ทำให้ได้ข้อสรุป 5, ดังนั้นทฤษฎีบทนี้เป็นจริง.

❑

เนื่องจากเรามีกฎตรรกศาสตร์ $(p \longrightarrow q) \longrightarrow r \Leftrightarrow (p \wedge q) \longrightarrow r$, เราจึงเห็นความหมายในอีกมุมมองหนึ่งของการพิสูจน์โดยวิธีตรง. ดังที่เราทราบแล้วว่าข้อความของทฤษฎีบทจะอยู่ในรูป $(P_1 \wedge P_2 \wedge \ldots \wedge P_n) \longrightarrow C$ เมื่อ P_i, $1 \leq i \leq n$, คือข้อกำหนด n ข้อของทฤษฎีบทและ C คือข้อสรุปของทฤษฎีบท. เมื่อข้อสรุป C คือข้อความในรูป $P \longrightarrow Q$, ข้อความทั้งหมดของทฤษฎีบทก็คือ $(P_1 \wedge P_2 \wedge \ldots \wedge P_n) \longrightarrow (P \longrightarrow Q)$ ซึ่งสมมูลเชิงตรรกกับข้อความ $(P_1 \wedge P_2 \wedge \ldots \wedge P_n \wedge P) \longrightarrow Q$. ดังนั้นการพิสูจน์ข้อสรุป $P \longrightarrow Q$ โดยวิธีตรงซึ่งเริ่มต้นด้วยการตั้งสมมติฐานว่า P เป็นจริง ย่อมเทียบเท่ากับการเพิ่มข้อความ P เข้าไปเป็นข้อกำหนดอีกข้อหนึ่งของทฤษฎีบทนั่นเอง. กล่าวอีกนัยหนึ่งคือการพิสูจน์ $P \longrightarrow Q$ โดยวิธีตรงเป็นการเปลี่ยนเป้าหมายการพิสูจน์จากข้อความ $P \longrightarrow Q$ ไปเป็นข้อความ Q โดยการย้ายข้อความ P ไปเป็นส่วนหนึ่งของข้อกำหนดของทฤษฎีบทนั้น ดังแสดงในแผนผังต่อไปนี้.

กลยุทธ์การพิสูจน์ $P \longrightarrow Q$ ก่อนใช้การพิสูจน์โดยวิธีตรง:

ข้อสมมติฐาน	***เป้าหมายที่จะพิสูจน์***
P_1	$P \longrightarrow Q$
P_2	
...	
P_n	

กลยุทธ์การพิสูจน์ $P \longrightarrow Q$ เมื่อใช้การพิสูจน์โดยวิธีตรง:	
ข้อสมมติฐาน	***เป้าหมายที่จะพิสูจน์***
P_1	Q
P_2	
...	
P_n	
P	

เมื่อเราเข้าใจความหมายในลักษณะนี้ของการพิสูจน์โดยวิธีตรง เราจึงทราบว่าข้อความของทฤษฎีบทในตัวอย่าง 2 ข้างบนซึ่งอยู่ในรูป

$$([d \in \mathbb{Z}+] \wedge [d > 1] \wedge [a \in \mathbb{Z}]) \longrightarrow ([d \mid a] \longrightarrow [d \nmid a+1])$$

ให้ความหมายเช่นเดียวกับการเขียนว่า

ให้ d เป็นจำนวนเต็มบวกที่มากกว่า 1 และให้ a เป็นจำนวนเต็มซึ่งหารด้วย d ลงตัว. จะได้ว่า d หาร a+1 ไม่ลงตัว.

ซึ่งอยู่ในรูป

$$([d \in \mathbb{Z}+] \wedge [d > 1] \wedge [a \in \mathbb{Z}] \wedge [d \mid a]) \longrightarrow [d \nmid a+1])$$

ซึ่งก็มีความหมายเช่นเดียวกับการเขียนว่า

ให้ d เป็นจำนวนเต็มบวกและให้ a เป็นจำนวนเต็ม. ถ้า d > 1 และ d หาร a ลงตัว, จะได้ว่า d หาร a+1 ไม่ลงตัว.

ซึ่งอยู่ในรูป

$$([d \in \mathbb{Z}+] \wedge [a \in \mathbb{Z}]) \longrightarrow (([d > 1] \wedge [d \mid a]) \longrightarrow [d \nmid a+1]).$$

การพิสูจน์ข้อความในรูป P⟶Q โดยวิธีอ้อม (Indirect Proof)

เนื่องจากข้อความในรูป $P \longrightarrow Q$ สมมูลเชิงตรรกกับคอนทราโพสิทิฟของมันคือ $\sim Q \longrightarrow \sim P$, เราจึงพิสูจน์ข้อความ $P \longrightarrow Q$ ได้โดย*การพิสูจน์ข้อความ $\sim Q \longrightarrow \sim P$ โดยวิธีตรง*. เราเรียกวิธีการพิสูจน์ $P \longrightarrow Q$ เช่นนี้ว่า**การพิสูจน์โดยวิธีอ้อม** (indirect proof) หรือ**การพิสูจน์โดยการแย้งสลับที่** (proof by contraposition) ซึ่งมีเค้าโครงดังนี้:

สมมติข้อความ $\sim Q$.
พิสูจน์ข้อความ $\sim P$.
ดังนั้น $P \longrightarrow Q$.

ตัวอย่าง 3 ข้างล่างแสดงให้เห็นว่าในยามที่การพิสูจน์โดยวิธีตรงดูไร้ความหวัง การพิสูจน์โดยวิธีอ้อมกลับประสบความสำเร็จอย่างง่ายดาย. ส่วนตัวอย่าง 4 แสดงให้เห็นว่าแม้ว่าทฤษฎีบทบางบทจะพิสูจน์ได้ทั้งวิธีตรงและวิธีอ้อม การพิสูจน์โดยวิธีตรงจะเป็นธรรมชาติมากกว่า.

ตัวอย่าง 3: จงพิสูจน์ทฤษฎีบทต่อไปนี้ด้วยการพิสูจน์โดยวิธีอ้อม.

ทฤษฎีบท: *ให้ n เป็นจำนวนเต็มใดๆ. ถ้า n^2 เป็นจำนวนคู่, จะได้ n เป็นจำนวนคู่.*

<u>*วิธีทำ*</u> เราอาจจะลองพิสูจน์ทฤษฎีบทนี้ด้วยวิธีตรงดังต่อไปนี้:

สมมติให้ n^2 เป็นจำนวนคู่. ดังนั้น $n^2 = 2k$ สำหรับจำนวนเต็ม k บางตัว. เราได้ $n = \sqrt{2k}$ หรือ $-\sqrt{2k}$. ดังนั้น ???

เราอาจพบทางตันในลักษณะข้างบน. เมื่อเป็นเช่นนี้ เราอาจลองการพิสูจน์โดยวิธีอ้อมโดยตั้งสมมติฐานว่า n ไม่เป็นจำนวนคู่ แล้วพิสูจน์ให้ได้ว่า n^2 จะไม่เป็นจำนวนคู่เช่นกัน ดังต่อไปนี้:

บทพิสูจน์:

1. สมมติให้ n ไม่เป็นจำนวนคู่ นั่นคือ n เป็นจำนวนคี่.
2. ดังนั้น n = 2k+1 สำหรับจำนวนเต็ม k บางตัว.
3. จาก 2 เราได้ $n^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$.
4. จาก 3, เนื่องจาก $2k^2+2k$ เป็นจำนวนเต็ม, ดังนั้น n^2 เป็นจำนวนคี่.
5. สมมติฐาน 1 ทำให้ได้ข้อสรุป 4, ดังนั้นทฤษฎีบทนี้เป็นจริง.

❑

ตัวอย่าง 4: จงพิสูจน์ทฤษฎีบทในตัวอย่าง 2 ด้วยการพิสูจน์โดยวิธีอ้อม.

<u>*วิธีทำ*</u> เราเคยพิสูจน์ทฤษฎีบทนี้ในตัวอย่าง 2 โดยวิธีตรง. ตัวอย่างนี้จะแสดงการพิสูจน์โดยวิธีอ้อมซึ่งต้องใช้กลเม็ดที่ซับซ้อนกว่า.

บทพิสูจน์:

1. สมมติให้ d หาร a+1 ลงตัว.
2. ดังนั้น จากนิยามของการหารลงตัว, a+1 = kd สำหรับจำนวนเต็ม k บางตัว.
3. จาก 2 เราได้ a = kd−1.
4. ให้ j = k−1; แทนค่า k ในสมการข้อ 3 เราได้ a = kd−1 = (j+1)d−1 = jd+(d−1).
5. จากข้อกำหนด $0 < 1 < d$ เราได้ $0 < d-1 < d$. ดังนั้น เราสรุปจากข้อ 4 โดยทฤษฎีบทขั้นตอนวิธีการหารได้ว่า d−1 เป็นเศษเหลือที่ไม่เท่ากับ 0 ของการหาร a ด้วย d.
6. จาก 5, d หาร a ไม่ลงตัว
7. สมมติฐาน 1 ทำให้ได้ข้อสรุป 6, ดังนั้นทฤษฎีบทนี้เป็นจริง.

❑

การพิสูจน์ข้อความในรูป P⟶Q โดยการพิสูจน์เพียงข้างเดียว

สำหรับข้อความในรูป P⟶Q ถ้าเราสามารถแสดงว่า P เป็นเท็จได้ ก็ถือได้ว่าเราได้พิสูจน์ข้อความนั้นสำเร็จแล้ว เพราะเมื่อ P เป็นเท็จ ข้อความ P⟶Q จะเป็นจริงเสมอไม่ว่า Q จะเป็นจริงหรือเท็จ. ในลักษณะเช่นนี้ เรากล่าวว่า P⟶Q **เป็นจริงแบบสุญกรรม** (vacuously true) และเรียกการพิสูจน์ข้อความ P⟶Q โดยการแสดงให้เห็นว่า P เป็นเท็จว่า **การพิสูจน์แบบสุญกรรม** (vacuous proof).

โดยทั่วไปแล้ว เราแทบไม่เคยพบทฤษฎีบทในรูป P⟶Q ที่สามารถพิสูจน์แบบสุญกรรมได้ เพราะทฤษฎีบทในรูป P⟶Q ที่ P เป็นเท็จนั้นจะไม่ค่อยน่าสนใจมากนัก. อย่างไรก็ตาม การพิสูจน์แบบสุญกรรมมักมีประโยชน์ในการพิสูจน์*กรณีเฉพาะ*บางกรณีของทฤษฎีบทในรูป ∀n P(n) ดังตัวอย่างต่อไปนี้.

ตัวอย่าง 5: ให้ P(n) แทนข้อความ “ถ้า n เป็นจำนวนคู่, จะได้ n^2 เป็นจำนวนคู่”. จงพิสูจน์ว่า P(1) เป็นจริง.

<u>*วิธีทำ*</u> P(1) คือข้อความ “ถ้า 1 เป็นจำนวนคู่, จะได้ 1^2 เป็นจำนวนคู่”. เนื่องจากข้อความ “1 เป็นจำนวนคู่” เป็นเท็จ เราจึงสรุปได้ว่า P(1) เป็นจริงแบบสุญกรรม.

ให้สังเกตว่า ทันทีที่เราพบว่าข้อความหน้าเป็นเท็จ เราไม่จำเป็นต้องสนใจความจริงเท็จของข้อความหลังคือ “1^2 เป็นจำนวนคู่” แต่อย่างใด.

❑

ในทำนองคล้ายคลึงกัน เราทราบจากตรรกศาสตร์ว่า ถ้าข้อความ Q เป็นจริง จะสรุปได้ว่าข้อความ P⟶Q เป็นจริงเสมอไม่ว่า P จะเป็นจริงหรือเท็จ. ในลักษณะเช่นนี้ เรากล่าวว่า P⟶Q **เป็นจริงแบบตื้น** (trivially true) และเรียกการพิสูจน์ข้อความ P⟶Q โดยการแสดงให้เห็นว่า Q เป็นจริงว่า **การพิสูจน์แบบตื้น** (trivial proof).

เช่นเดียวกับการพิสูจน์แบบสุญกรรม การพิสูจน์แบบตื้นมักใช้กับการพิสูจน์กรณีเฉพาะของทฤษฎีบทในรูป $\forall$n P(n) ดังตัวอย่างต่อไปนี้.

ตัวอย่าง 6: ให้ a และ b เป็นจำนวนเต็มบวกใดๆ. จงพิสูจน์ว่าข้อความต่อไปนี้เป็นจริงในกรณี n = 0:

ถ้า $a \le b$, จะได้ $a^n \le b^n$.

<u>*วิธีทำ*</u> ในกรณีที่ n = 0, ข้อความข้างบนคือ “ถ้า $a \le b$, จะได้ $a^0 \le b^0$”. เนื่องจาก $a^0 \le b^0$ เป็นจริงเพราะ $a^0 = b^0 = 1$ สำหรับทุกจำนวนเต็มบวก a และ b, เราสรุปได้ว่าข้อความ “ถ้า $a \le b$, จะได้ $a^0 \le b^0$” เป็นจริงแบบตื้นเขิน.

ให้สังเกตว่า ในการพิสูจน์ข้างบน ทันทีเราพบว่าข้อความหลังเป็นจริงเสมอ เราไม่จำเป็นต้องสนใจความจริงเท็จของข้อความหน้าคือ “$a \le b$” แต่อย่างใด

❑

การพิสูจน์โดยข้อขัดแย้ง (Proof by Contradiction)

กฎการอนุมาน {p⟶$\mathcal{F}$}∴~p ที่เรากล่าวถึงในหัวข้อ 3.2 ทำให้เราได้วิธีการพิสูจน์ที่สำคัญยิ่งวิธีหนึ่งและใช้บ่อยเป็นอันดับต้นๆ นั่นคือ **การพิสูจน์โดยข้อขัดแย้ง** (proof by contradiction). ถ้าข้อความที่จะพิสูจน์คือ P, การพิสูจน์โดยข้อขัดแย้งจะมีเค้าโครงดังนี้:

สมมติข้อความ ~P. *แสดงให้เห็นว่าข้อสมมติดังกล่าวนำไปสู่**ข้อความที่เป็นเท็จ** ($\mathcal{F}$).* ดังนั้น P.

นั่นคือเราเริ่มด้วยการตั้งสมมติฐานว่านิเสธของข้อความที่เราจะพิสูจน์เป็นจริง (นั่นคือ ~P เป็นจริง หรืออีกนัยหนึ่ง P เป็นเท็จ) แล้วแสดงให้เห็นว่าสมมติฐานนี้นำไปสู่ข้อความที่เป็นเท็จ. เช่นนี้แสดงว่า เราได้พิสูจน์แล้วว่า ~P⟶$\mathcal{F}$ เป็นจริง ดังนั้นด้วยกฎการอนุมาน {p⟶$\mathcal{F}$}∴~p เราจึงสรุปได้ว่าข้อความ P เป็นจริง.

อนึ่ง ข้อความที่เป็นเท็จที่ได้ส่วนใหญ่มักเป็นข้อขัดแย้งที่อยู่ในรูป $q \wedge \sim q$ กล่าวคือเป็นข้อความสองข้อความที่ไม่อาจเป็นจริงพร้อมกันได้. นี่คือเหตุที่เราเรียกวิธีพิสูจน์แบบนี้ว่า*การพิสูจน์โดยข้อขัดแย้ง*.

ตัวอย่าง 7: จงพิสูจน์ทฤษฎีบทต่อไปนี้โดยใช้การพิสูจน์โดยข้อขัดแย้ง.

ทฤษฎีบท: *ไม่มีจำนวนเต็มตัวใดที่ใหญ่ที่สุด.*

วิธีทำ เราเริ่มต้นโดยการสมมติตรงข้ามกับทฤษฎีบท แล้วแสดงว่านำไปสู่ข้อความที่เป็นเท็จดังนี้:

บทพิสูจน์:

1. สมมติว่ามีจำนวนเต็มที่ใหญ่ที่สุด (นี่คือนิเสธของทฤษฎีบทนี้) และให้ N เป็นจำนวนเต็มตัวนั้น.
2. ให้ M = N+1. ดังนั้น M เป็นจำนวนเต็มเพราะจำนวนเต็มมีสมบัติปิดภายใต้การบวก.
3. จาก 2 เราได้ $M > N$.
4. จาก 3 แสดงว่ามีจำนวนเต็มที่ใหญ่กว่า N.
5. จาก 1 และ 4; แสดงว่า*มีจำนวนเต็มที่ใหญ่กว่าจำนวนเต็มที่ใหญ่ที่สุด.*
6. สมมติฐาน 1 นำมาสู่ข้อความ 5 ซึ่งเป็นเท็จ ดังนั้นสมมติฐาน 1 เป็นเท็จ แสดงว่าทฤษฎีบทนี้เป็นจริง.

❑

ตัวอย่าง 8: จงพิสูจน์ทฤษฎีบทต่อไปนี้โดยใช้การพิสูจน์โดยข้อขัดแย้ง.

ทฤษฎีบท: *$\sqrt{2}$ เป็นจำนวนอตรรกยะ.*

วิธีทำ ทฤษฎีบทนี้นับได้ว่าเป็นตัวอย่างอมตะของการพิสูจน์โดยข้อขัดแย้ง. ผู้อ่านควรทบทวนบทนิยามของจำนวนตรรกยะและจำนวนอตรรกยะก่อนที่จะทำความเข้าใจบทพิสูจน์ข้างล่าง.

บทพิสูจน์:

1. สมมติว่า $\sqrt{2}$ เป็นจำนวนตรรกยะ. (นี่คือนิเสธของทฤษฎีบทนี้)
2. ดังนั้นจากนิยามของจำนวนตรรกยะ จะต้องมีจำนวนเต็ม a และ b ซึ่ง $\sqrt{2} = a/b$ โดยที่ a และ b ไม่มีตัวประกอบร่วมกัน (ยกเว้น 1).
3. จาก 2, ยกกำลังสองทั้งสองข้าง เราได้ $2 = a^2/b^2$. นั่นคือ $a^2 = 2b^2$.
4. จาก 3, แสดงว่า a^2 เป็นจำนวนคู่.
5. จาก 4 และทฤษฎีบทที่พิสูจน์ในตัวอย่าง 3, เราได้ a เป็นจำนวนคู่ ดังนั้นเราให้ $a = 2k$ สำหรับจำนวนเต็ม k บางตัว.
6. แทนค่า $a = 2k$ ในสมการข้อ 3 เราได้ $4k^2 = 2b^2$. นั่นคือ $b^2 = 2k^2$ แสดงว่า b^2 เป็นจำนวนคู่.
7. จาก 6 และทฤษฎีบทที่พิสูจน์ในตัวอย่าง 3, เราได้ b เป็นจำนวนคู่.
8. จาก 5 และ 7, แสดงว่า a และ b มีตัวประกอบร่วมกันคือ 2.
9. ข้อสรุป 8 ขัดแย้งกับข้ออ้าง 2 ข้างบนที่ว่า a และ b ไม่มีตัวประกอบร่วมกัน ดังนั้นสมมติฐาน 1 เป็นเท็จ นั่นคือทฤษฎีบทนี้เป็นจริง □

❑

การพิสูจน์ข้อความในรูป P⟶Q โดยการพิสูจน์โดยข้อขัดแย้ง

การพิสูจน์โดยข้อขัดแย้งสามารถใช้พิสูจน์ข้อความในรูป $P \longrightarrow Q$ ได้เช่นกันโดยการตั้งสมมติฐานว่า *นิเสธของข้อความ* $P \longrightarrow Q$ นั้นเป็นจริง แล้วแสดงให้เห็นว่าสมมติฐานนี้นำไปสู่ข้อขัดแย้งหรือข้อความที่เป็นเท็จ. เนื่องจาก $\sim(p \longrightarrow q)$ สมมูลเชิงตรรกกับ $p \wedge \sim q$, ดังนั้นการพิสูจน์ $P \longrightarrow Q$ โดยข้อขัดแย้งจะมีเค้าโครงดังนี้:

สมมติข้อความ P และข้อความ ~Q.
*แสดงให้เห็นว่าข้อสมมติดังกล่าวนำไปสู่**ข้อความที่เป็นเท็จ** ($\mathcal{F}$).*
ดังนั้น $P \longrightarrow Q$.

ตัวอย่าง 9: จงพิสูจน์ทฤษฎีบทในตัวอย่าง 2 โดยการพิสูจน์โดยข้อขัดแย้ง.

วิธีทำ เราเคยพิสูจน์ทฤษฎีบทนี้ในตัวอย่าง 2 โดยวิธีตรงและในตัวอย่าง 4 โดยวิธีอ้อม. ตัวอย่างนี้จะแสดงการพิสูจน์โดยข้อขัดแย้ง. เนื่องจากข้อความที่เราจะพิสูจน์คือ "ถ้า $d \mid a$ แล้ว $d \nmid a+1$", เราจะเริ่มบทพิสูจน์ด้วยการสมมตินิเสธของข้อความนี้.

บทพิสูจน์:

1. สมมติให้ $d \mid a$ และ $d \mid a+1$.
2. จาก 1 และนิยามของการหารลงตัว, เราได้ $a = jd$ และ $a+1 = kd$ สำหรับจำนวนเต็ม j และ k บางตัว.
3. จาก 2 เราได้ $jd = kd-1$ ดังนั้น $(k-j)d = 1$.
4. จาก 3, เนื่องจาก $k-j$ เป็นจำนวนเต็ม แสดงว่า d หาร 1 ลงตัว.
5. จากข้อกำหนดของทฤษฎีบทที่ว่า $d > 1$ ดังนั้น d หาร 1 ไม่ลงตัว.
6. ข้อสรุป 4 และ 5 ขัดแย้งกันเอง, ดังนั้นสมมติฐาน 1 เป็นเท็จ นั่นคือทฤษฎีบทนี้เป็นจริง.

❑

การพิสูจน์แบบแจกแจงกรณี (Proof by Cases)

เรามีสมมูลเชิงตรรกอันหนึ่งที่น่าสนใจคือ

$$(p_1 \vee p_2 \vee \ldots \vee p_n) \longrightarrow q \iff (p_1 \longrightarrow q) \wedge (p_2 \longrightarrow r) \wedge \ldots \wedge (p_n \longrightarrow q)$$

โดย $n \geq 1$. (เราเคยพิสูจน์ในกรณี n = 2 แล้วในตัวอย่าง 5 หัวข้อ 1.2)

สมมูลเชิงตรรกดังกล่าวทำให้เราได้วิธีพิสูจน์ข้อความในรูป $P \longrightarrow Q$ เมื่อข้อความ P สามารถเขียนได้ในรูป $(p_1 \vee p_2 \vee \ldots \vee p_n)$. กล่าวคือเราจะแบ่งการพิสูจน์เป็น n กรณี โดยกรณีที่ 1 เราพิสูจน์ข้อความ $p_1 \longrightarrow Q$, กรณีที่ 2 เราพิสูจน์ข้อความ $p_2 \longrightarrow Q$, ..., และกรณีที่ n เราพิสูจน์ข้อความ $p_n \longrightarrow Q$ ตามลำดับ. เมื่อเราพิสูจน์ครบ n กรณีดังกล่าวแล้ว ก็สรุปได้ว่าข้อความ $(p_1 \vee p_2 \vee \ldots \vee p_n) \longrightarrow q$ เป็นจริง. เราเรียกวิธีการพิสูจน์ข้อความ $P \longrightarrow Q$ เช่นนี้ว่า**การพิสูจน์แบบแจกแจงกรณี** (proof by cases) ซึ่งสรุปเป็นเค้าโครงดังนี้.

แสดงให้เห็นว่าข้อความ P คือข้อความ $(p_1 \vee p_2 \vee \ldots \vee p_n)$ *กรณีที่ 1: พิสูจน์ข้อความ* $p_1 \rightarrow Q$. *กรณีที่ 2: พิสูจน์ข้อความ* $p_2 \rightarrow Q$. ... *กรณีที่ n: พิสูจน์ข้อความ* $p_n \rightarrow Q$. ดังนั้น $P \rightarrow Q$.

ตัวอย่าง 10: จงพิสูจน์ข้อความต่อไปนี้

ให้ n เป็นจำนวนเต็ม. ถ้า 3 หาร n ไม่ลงตัว, จะได้ $n^2 \equiv 1 \pmod 3$.

<u>*วิธีทำ*</u> เมื่อ 3 หาร n ไม่ลงตัว แสดงว่าได้เศษเหลือเป็น 1 หรือ 2 ทำให้เราแบ่งบทพิสูจน์ได้เป็น 2 กรณี โดยแต่ละกรณีเราจะใช้การพิสูจน์โดยวิธีตรงดังนี้:

บทพิสูจน์:

- ***กรณีที่ 1:*** *พิสูจน์ว่า ถ้า 3 หาร n แล้วเหลือเศษ 1, จะได้* $n^2 \equiv 1 \pmod 3$.
    1. สมมติให้ 3 หาร n แล้วเหลือเศษ 1.
    2. ดังนั้น จากทฤษฎีบทขั้นตอนวิธีการหาร เราได้ $n = 3q+1$ สำหรับจำนวนเต็ม q บางตัว.
    3. จาก 2 เราได้ $n^2 = 9q^2+6q+1 = 3(3q^2+2q)+1$. นั่นคือ $n^2-1 = 3(3q^2+2q)$.
    4. จาก 3, เนื่องจาก $3q^2+2q$ เป็นจำนวนเต็ม แสดงว่า 3 หาร n^2-1 ลงตัว.
    5. จาก 4 และนิยามของการสมภาค, เราได้ $n^2 \equiv 1 \pmod 3$.
    6. สมมติฐาน 1 ทำให้ได้ข้อสรุป 5, ดังนั้นทฤษฎีบทนี้เป็นจริงสำหรับกรณีที่ 1.
- ***กรณีที่ 2:*** *พิสูจน์ว่า ถ้า 3 หาร n แล้วเหลือเศษ 2, จะได้* $n^2 \equiv 1 \pmod 3$.
    1. สมมติให้ 3 หาร n แล้วเหลือเศษ 2.
    2. ดังนั้น จากทฤษฎีบทขั้นตอนวิธีการหาร เราได้ $n = 3q+2$ สำหรับจำนวนเต็ม q บางตัว.
    3. จาก 2 เราได้ $n^2 = 9q^2+12q+4 = 3(3q^2+4q+1)+1$. นั่นคือ $n^2-1 = 3(3q^2+4q+1)$.
    4. จาก 3, เนื่องจาก $3q^2+4q+1$ เป็นจำนวนเต็ม แสดงว่า 3 หาร n^2-1 ลงตัว.
    5. จาก 4 และนิยามของการสมภาค, เราได้ $n^2 \equiv 1 \pmod 3$.
    6. สมมติฐาน 1 ทำให้ได้ข้อสรุป 5, ดังนั้นทฤษฎีบทนี้เป็นจริงสำหรับกรณีที่ 2.

ดังนั้นเราได้แสดงแล้วว่าข้อความนี้เป็นจริงในทุกกรณีที่เป็นไปได้.

❑

เราสามารถใช้การพิสูจน์แบบแจกแจงกรณีพิสูจน์ข้อความในรูป $\forall x \forall y \ldots P(x,y,\ldots)$ ได้เช่นกัน ถ้าเราสามารถแจกแจงกรณีที่เป็นไปได้ทั้งหมดของค่า x และ y ในเอกภพของตัวแปรทั้งสอง. เราจะดำเนินการพิสูจน์โดยแสดงให้เห็นว่าข้อความ $P(x,y,\ldots)$ เป็นจริงในแต่ละกรณีเหล่านั้นจนครบทุกกรณี.

ตัวอย่าง 11: ให้ min(x,y) คือค่าที่น้อยที่สุดระหว่าง x และ y และ max(x,y) คือค่าที่มากที่สุดระหว่าง x และ y. จงพิสูจน์ทฤษฎีบทต่อไปนี้

ทฤษฎีบท: *สำหรับทุกจำนวนจริง x และ y,* $\min(x,y)+\max(x,y) = x+y$.

<u>*วิธีทำ*</u> เนื่องจากทฤษฎีบทนี้เกี่ยวกับค่ามากที่สุดและค่าน้อยที่สุดระหว่าง x และ y ดังนั้นการแบ่งกรณีที่เหมาะสมคือแบ่งเป็นกรณีที่ $x \geq y$ และกรณีที่ $x < y$. เราจะพิสูจน์ว่า min(x,y)+max(x,y) = x+y เป็นจริงในทั้งสองกรณี.

บทพิสูจน์: ให้ x และ y เป็นจำนวนจริงใดๆ.

- ***กรณี $x \geq y$***

  เมื่อ $x \geq y$ เราได้ min(x,y) = y และ max(x,y) = x. ดังนั้น min(x,y)+max(x,y) = x+y.

- ***กรณี $x < y$***

  เมื่อ $x < y$ เราได้ min(x,y) = x และ max(x,y) = y. ดังนั้น min(x,y)+max(x,y) = x+y.

ดังนั้นเราได้แสดงแล้วว่าทฤษฎีบทนี้เป็นจริงในทุกกรณีที่เป็นไปได้.

❑

อนึ่ง ให้สังเกตว่าปัจจัยสำคัญที่จะทำให้*การพิสูจน์แบบแจกแจงกรณี*ประสบความสำเร็จคือการหาเงื่อนไขการแบ่งกรณีที่เหมาะสมกับข้อความที่เราจะพิสูจน์. ในตัวอย่าง 11 ข้างบน ถ้าเราเปลี่ยนเป็นพิจารณา 3 กรณีคือ กรณี x+y = 0, กรณี $x+y < 0$, และกรณี $x+y > 0$, การพิสูจน์จะไม่เป็นธรรมชาติและยากลำบากโดยไม่จำเป็น (ถ้ายังโชคดีที่หาวิธีพิสูจน์ได้).

การพิสูจน์ข้อความในรูป $\forall x \forall y \ldots P(x,y,\ldots)$

ทฤษฎีบทจำนวนมากเป็นข้อความที่มี*การบ่งปริมาณทั้งหมด*ทั้งอย่างเปิดเผยและโดยนัย. ทฤษฎีบทที่เราพิสูจน์ในตัวอย่าง 11 ข้างบนคือ

สำหรับทุกจำนวนจริง x และ y, min(x,y)+max(x,y) = x+y.

เป็นข้อความที่มีการบ่งปริมาณทั้งหมดอย่างเปิดเผย. เราอาจเขียนใหม่ให้เป็นการบ่งปริมาณแบบโดยนัยได้หลายแบบ เช่น

ให้ x และ y เป็นจำนวนจริงใดๆ. จะได้ min(x,y)+max(x,y) = x+y.

โดยเราอาจละคำว่า "ใดๆ" ออกไปก็ได้ หรือเขียนว่า

ถ้า x และ y เป็นจำนวนจริง, จะได้ min(x,y)+max(x,y) = x+y.

การเขียนทั้งสามแบบข้างบนล้วนให้ความหมายเดียวกัน ซึ่งเขียนในรูปสัญลักษณ์ได้ว่า

$\forall x \in \mathbb{R} \forall y \in \mathbb{R}$ [min(x,y)+max(x,y) = x+y]

กลยุทธ์ทั่วไปของการพิสูจน์ข้อความที่มีความหมายเป็นการบ่งปริมาณทั้งหมดก็คือการประยุกต์ใช้**กฎการอนุมานนัยจำเพาะสู่นัยทั่วไป**ที่กล่าวถึงในหัวข้อ 3.2 นั่นคือ

{[x เป็นสมาชิกใดๆใน $\mathbb{U}$], P(x)} $\therefore \forall x \in \mathbb{U}$ P(x)

ดังนั้นเค้าโครงการพิสูจน์ข้อความในรูป $\forall x \forall y \ldots P(x,y,\ldots)$ เป็นดังนี้:

ให้ x, y, ... เป็นค่าใดๆ (ในเอกภพของตัวแปรแต่ละตัว)
พิสูจน์ข้อความ P(x,y,...).
ดังนั้น $\forall x \forall y \ldots P(x,y,\ldots)$.

การพิสูจน์ข้อความ P(x,y,...) ในเค้าโครงข้างบนนั้น เราจะกล่าวถึงค่า x, y, ... ในรูปตัวแปร และต้องตระหนักเสมอว่าตัวแปรเหล่านี้ถูกตรึงให้มีค่าเป็นค่าใดค่าหนึ่ง แต่เป็นค่าใดก็ได้ตามอำเภอใจ.

อนึ่ง การเขียนบทพิสูจน์ส่วนใหญ่ตามเค้าโครงข้างบนมักจะละการตั้งสมมติฐาน *"ให้ x, y, ... เป็นค่าใดๆ"* และข้อสรุป *"ดังนั้น $\forall x\forall y...P(x,y,...)$"* ไว้ในฐานที่เข้าใจ ทำให้บทพิสูจน์ย่นย่อเหลือเพียงการพิสูจน์ข้อความ P(x,y,...) เท่านั้น. ให้สังเกตว่าบทพิสูจน์ในตัวอย่าง 1, 2, 3, 4, 9, 10, และ 11 ข้างบนล้วนเป็นการพิสูจน์ข้อความในรูป $\forall x\forall y...P(x,y,...)$ ทั้งสิ้น.

การพิสูจน์ข้อความในรูป P⟷Q

ทฤษฎีบทบางบทเป็นข้อความในรูป P⟷Q ซึ่งมักเขียนว่า *"P เมื่อและต่อเมื่อ Q"* หรือ *"P สมมูลกับ Q"*. เนื่องจากเรามีกฎตรรกศาสตร์ $p\leftrightarrow q \Leftrightarrow (p\rightarrow q)\wedge(q\rightarrow p)$ ดังนั้นการพิสูจน์ข้อความ P⟷Q ทำได้โดยแบ่งบทพิสูจน์เป็น 2 ส่วนคือ บทพิสูจน์ข้อความ P⟶Q และบทพิสูจน์ข้อความ Q⟶P. เราเรียกบทพิสูจน์ส่วนแรกว่า ***ส่วนต่อเมื่อ*** (*only if* part) และเรียกบทพิสูจน์ส่วนที่สองว่า ***ส่วนเมื่อ*** (*if* part) ดังนั้นเค้าโครงการพิสูจน์จะเป็นดังนี้:

พิสูจน์ข้อความ P⟶Q. (ส่วน "ต่อเมื่อ")
พิสูจน์ข้อความ Q⟶P. (ส่วน "เมื่อ")
ดังนั้น P⟷Q.

ตัวอย่าง 12: จงพิสูจน์ทฤษฎีบทต่อไปนี้

ทฤษฎีบท: *จำนวนเต็ม n เป็นจำนวนคู่ เมื่อและต่อเมื่อ n^2 เป็นจำนวนคู่.*

<u>วิธีทำ</u> เนื่องจากทฤษฎีบทนี้เกี่ยวกับค่ามากที่สุดและค่าน้อยที่สุดระหว่าง x และ y ดังนั้นการแบ่งกรณีที่เหมาะสมคือแบ่งเป็นกรณีที่ $x \geq y$ และกรณีที่ $x < y$. เราจะพิสูจน์ว่า min(x,y)+max(x,y) = x+y เป็นจริงในทั้งสองกรณี.

บทพิสูจน์:

- ***ส่วนต่อเมื่อ***: พิสูจน์ว่า *ถ้า n เป็นจำนวนคู่, จะได้ n^2 เป็นจำนวนคู่.*

  เราจะพิสูจน์โดยวิธีตรงดังนี้:

  1. สมมติให้ n เป็นจำนวนคู่.
  2. ดังนั้น จากนิยามของจำนวนคู่ เราได้ n = 2k สำหรับจำนวนเต็ม k บางตัว.
  3. จาก 2 เราได้ $n^2 = 4k^2 = 2(2k^2)$.
  4. จาก 3, เนื่องจาก $2k^2$ เป็นจำนวนเต็ม ดังนั้น n^2 เป็นจำนวนคู่.
  5. สมมติฐาน 1 ทำให้ได้ข้อสรุป 4, ดังนั้นทฤษฎีบทนี้เป็นจริงสำหรับส่วน*ต่อเมื่อ*.

- ***ส่วนเมื่อ***: พิสูจน์ว่า *ถ้า n^2 เป็นจำนวนคู่, จะได้ n เป็นจำนวนคู่.*

  เราเคยพิสูจน์ข้อความนี้แล้วในตัวอย่าง 3 โดยใช้การพิสูจน์โดยวิธีอ้อม ดังนั้นทฤษฎีบทนี้เป็นจริงสำหรับส่วน*เมื่อ*เช่นกัน.

  เมื่อเราพิสูจน์ทั้งสองส่วนแล้ว ก็สรุปได้ว่าทฤษฎีบทนี้เป็นจริง.

❑

อนึ่ง เมื่อเราพิสูจน์ว่าข้อความในรูป “P เมื่อและต่อเมื่อ Q” เป็นจริงแล้ว เราสามารถสรุปได้ทันทีว่าข้อความ “~P เมื่อและต่อเมื่อ ~Q” เป็นจริงเช่นกันโดยไม่ต้องเสียเวลาพิสูจน์อีก ทั้งนี้เพราะ $p\leftrightarrow q$ สมมูลเชิงตรรกกับ $\sim p\leftrightarrow \sim q$. ตัวอย่างเช่น ทฤษฎีบทในตัวอย่าง 12 ทำให้เราสรุปได้เช่นกันว่า *จำนวนเต็ม n เป็นจำนวนคี่ เมื่อและต่อเมื่อ n^2 เป็นจำนวนคี่.*

การพิสูจน์การสมมูลกันของข้อความหลายข้อความ

(Proof of Equivalence of Several Statements)

ในหัวข้อย่อยที่แล้ว เรากล่าวถึงวิธีการพิสูจน์ข้อความในรูป $P\leftrightarrow Q$ ซึ่งก็คือการสมมูลกันของข้อความสองข้อความ. ทฤษฎีบทบางบทกล่าวถึงการสมมูลกันของข้อความมากกว่าสองข้อความ กล่าวคือ ทฤษฎีบทจะอยู่ในรูป

ข้อความ $P_1, P_2, \ldots, P_n$ สมมูลกันหมด

หรือเขียนในรูปสัญลักษณ์ว่า

$$\forall\, i \in \{1, 2, \ldots, n\}\ \forall j \in \{1, 2, \ldots, n\}\ (P_i \leftrightarrow P_j)$$

ข้อความบ่งปริมาณข้างบนมีการสมมูลกันทั้งหมด n^2 คู่. เราทราบว่าทุกข้อความสมมูลกับตัวเอง ดังนั้นจะเหลือการสมมูลที่ต้องพิสูจน์เพียง $n^2 - n$ คู่. เรายังทราบด้วยว่าโอเปอเรเตอร์เชิงตรรก $\leftrightarrow$ มีสมบัติการสลับที่ ดังนั้นการสมมูลที่ต้องพิสูจน์จะเหลือเพียงครึ่งหนึ่งคือ $(n^2\text{-}n)/2$ คู่. เราทราบจากหัวข้อย่อยที่แล้วว่า การพิสูจน์การสมมูลกันของข้อความคู่หนึ่งจะต้องพิสูจน์ข้อความในรูป $P\rightarrow Q$ สองครั้ง ดังนั้นการพิสูจน์การสมมูลกันของ n ข้อความจึงต้องพิสูจน์ข้อความในรูป $P\rightarrow Q$ ถึง $((n^2\text{-}n)/2)\cdot 2 = n^2\text{-}n$ ครั้ง.

ในทางปฏิบัติ เราไม่จำเป็นต้องพิสูจน์มากถึงเพียงนั้น เพราะเราโชคดีที่โอเปอเรเตอร์ $\rightarrow$ มีสมบัติการถ่ายทอด เช่นเมื่อเราพิสูจน์ได้แล้วว่า $P_1\rightarrow P_2$ และ $P_2\rightarrow P_3$ เราก็สรุปได้ทันทีว่า $P_1\rightarrow P_3$ โดยไม่ต้องพิสูจน์. ข้อสังเกตนี้ทำให้เราได้สัจนิรันดร์ที่มีประโยชน์คือ

[ข้อความ $P_1, P_2, \ldots, P_n$ สมมูลกันหมด] $\Leftrightarrow (P_1\rightarrow P_2)\wedge(P_2\rightarrow P_3)\wedge\ldots\wedge(P_n\rightarrow P_1)$

ซึ่งทำให้เราสามารถพิสูจน์การสมมูลกันของ n ข้อความ โดยพิสูจน์ข้อความในรูป $P\rightarrow Q$ เพียง n ครั้งเท่านั้น นั่นคือพิสูจน์ว่า $(P_1\rightarrow P_2)$, $(P_2\rightarrow P_3)$, ..., และ $(P_n\rightarrow P_1)$ เป็นจริงทุกข้อความ.

ตัวอย่าง 13: จงพิสูจน์ทฤษฎีบทต่อไปนี้:

ทฤษฎีบท: *ให้ a และ b เป็นจำนวนเต็มและ d เป็นจำนวนเต็มบวก. สามข้อความต่อไปนี้สมมูลกัน:*

1) $a \equiv b \pmod d$
2) *a mod d = b mod d*
3) *มีจำนวนเต็ม q ซึ่ง a = b+qd*

__วิธีทำ__ ทฤษฎีบทนี้ครอบคลุมใจความของทฤษฎีบท 6 หัวข้อ 2.5. เนื่องจากเป็นการสมมูลกันของข้อความ 3 ข้อความ เราจะแบ่งการพิสูจน์เป็นสามส่วน.

บทพิสูจน์:

- **ส่วนที่ 1**: พิสูจน์ว่า *ถ้า $a \equiv b \pmod d$, จะได้ a mod d = b mod d.*

เราจะพิสูจน์โดยวิธีตรงดังนี้:

1. สมมติให้ $a \equiv b \pmod d$ ดังนั้นจากนิยามของการสมภาค เราได้ $d \mid (a-b)$.
2. ดังนั้น $a-b = kd$ สำหรับจำนวนเต็ม k บางตัว. นั่นคือ $a = b+kd$.
3. ให้ q คือผลหารและให้ r คือเศษเหลือของการหาร b ด้วย d. ดังนั้น $b = qd+r$, $r = b \bmod d$ และ $0 \leq r < d$.
4. แทน $b = qd+r$ ในสมการข้อ 2 เราได้ $a = (qd+r)+kd = (q+k)d+r$.
5. จาก 4, เนื่องจาก q+k เป็นจำนวนเต็มและ $0 \leq r < d$, เราได้ r เป็นเศษเหลือของการหาร a ด้วย d. นั่นคือ $r = a \bmod d$.
6. จาก 3 และ 5 เราได้ $a \bmod d = b \bmod d$.
7. สมมติฐาน 1 ทำให้ได้ข้อสรุป 6, ดังนั้นทฤษฎีบทนี้เป็นจริงสำหรับส่วนที่ 1.

- **ส่วนที่ 2**: พิสูจน์ว่า *ถ้า a mod d = b mod d, จะได้ว่า มีจำนวนเต็ม q ซึ่ง a = b+qd.*

  เราจะพิสูจน์โดยวิธีตรงดังนี้:

1. สมมติให้ $a \bmod d = b \bmod d = r$.
2. จาก 1 และทฤษฎีบทขั้นตอนวิธีการหาร, เราได้ $a = md+r$ และ $b = nd+r$ สำหรับจำนวนเต็ม m และ n บางตัว.
3. จาก 2 เราได้ $a-b = (m-n)d$. นั่นคือ $a = b+(m-n)d$.
4. เนื่องจาก $(m-n)$ เป็นจำนวนเต็ม ดังนั้นมีจำนวนเต็ม q (เช่น $m-n$) ซึ่ง $a = b+qd$.
5. สมมติฐาน 1 ทำให้ได้ข้อสรุป 4, ดังนั้นทฤษฎีบทนี้เป็นจริงสำหรับส่วนที่ 2.

- **ส่วนที่ 3**: พิสูจน์ว่า *ถ้ามีจำนวนเต็ม q ซึ่ง a = b+qd, จะได้ a ≡ b (mod d).*

  เราจะพิสูจน์โดยวิธีตรงดังนี้:

1. สมมติให้ $a = b+qd$ สำหรับจำนวนเต็ม q บางตัว.
2. ดังนั้น $a-b = qd$. นั่นคือ $d \mid (a-b)$.
3. จาก 2 และนิยามของการสมภาค เราได้ $a \equiv b \pmod d$.
4. สมมติฐาน 1 ทำให้ได้ข้อสรุป 3, ดังนั้นทฤษฎีบทนี้เป็นจริงสำหรับส่วนที่ 3.

❑

อนึ่ง ให้สังเกตว่าการจัดลำดับข้อความ n ข้อความเป็นข้อความที่ 1, 2, ..., n นั้นทำได้ตามใจชอบ. ผลที่ได้ทางอ้อมคือ ในกรณี n = 4 การพิสูจน์ว่าข้อความ P_1, P_2, P_3, และ P_4 สมมูลกันโดยการพิสูจน์

$$(P_1 \rightarrow P_2),\ (P_2 \rightarrow P_3),\ (P_3 \rightarrow P_4),\ \text{และ}\ (P_4 \rightarrow P_1)$$

จะให้ผลเทียบเท่ากับการพิสูจน์

$$(P_1 \rightarrow P_3),\ (P_3 \rightarrow P_4),\ (P_4 \rightarrow P_2),\ \text{และ}\ (P_2 \rightarrow P_1)$$

ซึ่งก็เทียบเท่ากับการพิสูจน์

$$(P_1 \rightarrow P_4),\ (P_4 \rightarrow P_2),\ (P_2 \rightarrow P_3),\ \text{และ}\ (P_3 \rightarrow P_1)$$

เช่นกัน. กล่าวโดยทั่วไปคือ ในการพิสูจน์การสมมูลกันของ n ข้อความนั้น เรามีวิธีการพิสูจน์ (n-1)! แบบให้เลือก. (ผู้อ่านควรใช้ความรู้เรื่องการนับในระดับมัธยมหาที่มาของสูตรนี้ด้วยตนเอง)

การพิสูจน์ข้อความในรูป $P\wedge Q$

หลักการของการพิสูจน์ข้อความในรูป $P\wedge Q$ นั้นง่ายมากจนแทบไม่ต้องกล่าวถึง นั่นคือเราใช้กฎการอนุมาน $\{p,q\}\therefore(p\wedge q)$. ดังนั้นบทพิสูจน์สำหรับข้อความ $P\wedge Q$ จะแบ่งเป็นสองส่วน: ส่วนแรกพิสูจน์ข้อความ P และส่วนที่สองพิสูจน์ข้อความ Q.

ในทำนองเดียวกัน วิธีที่ตรงไปตรงมาที่สุดในการพิสูจน์ข้อความในรูป $Q_1\wedge Q_2\wedge\ldots\wedge Q_n$ ทำได้โดยพิสูจน์ Q_i แยกทีละข้อความจนครบทั้ง n ข้อความ. ในหัวข้อย่อยที่แล้ว การพิสูจน์ $(P_1\longrightarrow P_2)\wedge(P_2\longrightarrow P_3)\wedge\ldots\wedge(P_n\longrightarrow P_1)$ เพื่อแสดงการสมมูลกันของ P_1, P_2, ..., และ P_n นับเป็นตัวอย่างหนึ่งของการพิสูจน์ข้อความในรูป $Q_1\wedge Q_2\wedge\ldots\wedge Q_n$ ดังกล่าว. (ดูตัวอย่าง 13 ข้างบน)

การพิสูจน์ข้อความในรูป $P\vee Q$

สัจนิรันดร์ $(p\vee q)\Leftrightarrow(\sim p\longrightarrow q)$ ทำให้เราพิสูจน์ข้อความในรูป $P\vee Q$ ได้โดยการพิสูจน์ข้อความ $\sim P\longrightarrow Q$ โดยใช้เทคนิคต่างๆที่ผ่านมาสำหรับข้อความในรูป *ถ้า..แล้ว*. ดังนั้นเค้าโครงการพิสูจน์คือ:

พิสูจน์ข้อความ $\sim P\longrightarrow Q$. ดังนั้น $P\vee Q$.

บ่อยครั้งที่การพิสูจน์ข้อความในรูป $P\vee Q$ เป็นส่วนหนึ่งของการพิสูจน์ข้อความที่ใหญ่กว่าเช่น $R\longrightarrow(P\vee Q)$. การพิสูจน์ข้อความนี้โดยวิธีตรงทำได้โดยการสมมติให้ R เป็นจริงแล้วพิสูจน์ว่า $P\vee Q$ เป็นจริงด้วยวิธีการดังกล่าวข้างบน ดังแสดงในตัวอย่างต่อไปนี้.

ตัวอย่าง 14: จงพิสูจน์ทฤษฎีบทต่อไปนี้

ทฤษฎีบท: *ให้ a และ b เป็นจำนวนเต็ม. ถ้า ab เป็นจำนวนคู่ จะได้ a เป็นจำนวนคู่หรือ b เป็นจำนวนคู่.*

<u>*วิธีทำ*</u> ข้อสรุปของทฤษฎีบทนี้คือ [ab เป็นจำนวนคู่]$\longrightarrow$([a เป็นจำนวนคู่]$\vee$[b เป็นจำนวนคู่]) ซึ่งอยู่ในรูป $P\longrightarrow(Q\vee R)$. เราเริ่มการพิสูจน์โดยการสมมติ P แล้วแสดงให้เห็นว่า $Q\vee R$ เป็นจริงโดยการพิสูจน์ $\sim Q\longrightarrow R$ โดยวิธีตรง นั่นคือสมมติ $\sim Q$ แล้วพิสูจน์ R.

บทพิสูจน์:

1. สมมติให้ ab เป็นจำนวนคู่. ดังนั้น ab = 2k สำหรับจำนวนเต็ม k บางตัว.
2. สมมติว่า a ไม่เป็นจำนวนคู่ นั่นคือ a เป็นจำนวนคี่ ดังนั้น a = 2m+1 สำหรับจำนวนเต็ม m บางตัว.
3. แทนค่า a ในสมการข้อ 1 ได้ (2m+1)b = 2k. ดังนั้น b = 2(k-nb).
4. จาก 3 เนื่องจาก k-nb เป็นจำนวนเต็ม ดังนั้น b เป็นจำนวนคู่.
5. สมมติฐาน 2 ทำให้ได้ข้อสรุป 4 แสดงว่า a เป็นจำนวนคู่หรือ b เป็นจำนวนคู่.
6. สมมติฐาน 1 ทำให้ได้ข้อสรุป 5 แสดงว่าทฤษฎีบทนี้เป็นจริง.

❑

อนึ่ง ให้สังเกตว่าการพิสูจน์ $\sim P\longrightarrow Q$ โดยวิธีตรงแล้วสรุปว่า $P\vee Q$ เป็นจริง ซึ่งมีเค้าโครงคือ

> *สมมติ ~P.*
> *พิสูจน์ Q*
> ดังนั้น P∨Q.

เทียบเท่าได้กับการพิสูจน์ P∨Q โดยแยกเป็นสองกรณีคือ *กรณีที่ P เป็นจริง* และ *กรณีที่ P เป็นเท็จ*. ทว่าในกรณีที่ P เป็นจริงนั้น เราสรุปได้ทันทีว่า P∨Q จะต้องเป็นจริงโดยไม่ต้องพิสูจน์อะไร ดังนั้นส่วนที่ต้องออกแรงอย่างแท้จริงคือกรณีที่ P เป็นเท็จ ซึ่งจะต้องแสดงให้เห็นว่า Q เป็นจริงจึงจะสรุปได้ว่า P∨Q เป็นจริงได้. ดังนั้นเค้าโครงของการพิสูจน์จะเป็นดังนี้:

> กรณี P เป็นจริง:
> ดังนั้น P∨Q เป็นจริง.
> กรณี P เป็นเท็จ (นั่นคือ ~P เป็นจริง)
> *พิสูจน์ Q.*
> ดังนั้น P∨Q.

ในเค้าโครงข้างบน ถ้าเราละกรณีที่ P เป็นจริง (คือสองบรรทัดแรก) ไว้ในฐานที่เข้าใจแล้ว ก็จะเห็นได้ชัดเจนว่าเค้าโครงการพิสูจน์ทั้งสองนี้มีเนื้อใหญ่ใจความเดียวกัน หากแต่เขียนด้วยสำนวนลีลาที่แตกต่างกันเท่านั้น.

อนึ่ง เราอาจใช้การพิสูจน์โดยข้อขัดแย้งมาพิสูจน์ข้อความในรูป P∨Q ได้. นั่นคือเราเริ่มด้วยการตั้งสมมติฐานว่า ~(P∨Q) ซึ่งก็คือ ~P∧~Q จากนั้นแสดงให้เห็นว่าข้อสมมติดังกล่าวนำไปสู่ข้อขัดแย้งหรือข้อความที่เป็นเท็จ ดังแสดงเป็นเค้าโครงดังนี้:

> สมมติ ~P และ ~Q.
> *แสดงให้เห็นว่าข้อสมมติดังกล่าวนำไปสู่**ข้อความที่เป็นเท็จ** ($\mathcal{F}$).*
> ดังนั้น P∨Q.

ตัวอย่างเช่นเราอาจพิสูจน์ทฤษฎีบทในตัวอย่าง 14 โดยใช้การพิสูจน์โดยข้อขัดแย้งในขั้นตอนที่ 2 ถึง 5 ดังต่อไปนี้:

บทพิสูจน์:

1. สมมติให้ ab เป็นจำนวนคู่.
2. สมมติว่าทั้ง a และ b เป็นจำนวนคี่. ดังนั้น a = 2m+1 และ b = 2n+1 สำหรับจำนวนเต็ม m และ n บางตัว.
3. ดังนั้นเราได้ ab = (2m+1)(2n+1) = 4mn+2m+2n+1 = 2(2mn+m+n)+1.
4. จาก 3, เนื่องจาก 2mn+m+n เป็นจำนวนเต็ม ดังนั้น ab เป็นจำนวนคี่.
5. ข้อสรุป 4 ขัดแย้งกับสมมติฐาน 1 ดังนั้นสมมติฐาน 2 จึงเป็นเท็จ นั่นคือ a หรือ b (หรือทั้งสองตัว) จะต้องเป็นจำนวนคู่.
6. สมมติฐาน 1 ทำให้ได้ข้อสรุป 5 แสดงว่าทฤษฎีบทนี้เป็นจริง.

การพิสูจน์การมีอยู่จริง (Existence Proof)

การพิสูจน์การมีอยู่จริง (Existence Proof) คือการพิสูจน์ข้อความในรูป $\exists x\ P(x)$ ซึ่งอ้างการมีอยู่ของค่า x อย่างน้อยหนึ่งค่าที่ทำให้ P(x) เป็นจริง. วิธีการที่ตรงไปตรงมาที่สุดในการพิสูจน์ข้อความในรูป $\exists x\ P(x)$ คือการประยุกต์ใช้กฏการอนุมานที่เรียกว่า ***กฏการพิสูจน์การมี*** (ดูหัวข้อ 3.2) นั่นคือ

$$\{a\in U,\ P(a)\} \therefore \exists x\in U\ P(x)$$

กฏการพิสูจน์การมี ดังกล่าวชี้แนะว่า การพิสูจน์ $\exists x\in U\ P(x)$ แบ่งเป็น 2 ขั้นตอนคือ:

ขั้นตอนที่ 1: หาค่า x ใน U ให้ได้สักตัวหนึ่งที่คาดว่าจะทำให้ P(x) เป็นจริง. สมมติว่าค่าที่หาได้คือ a.
ขั้นตอนที่ 2: พิสูจน์ว่า P(a) เป็นจริง.

เราเรียกวิธีการพิสูจน์การมีอยู่จริงเป็นสองขั้นตอนเช่นนี้ว่า **การพิสูจน์การมีอยู่จริงโดยการหาตัวอย่าง** (constructive existence proof).

จุดยากของการพิสูจน์การมีอยู่จริงโดยการหาตัวอย่างไม่ใช่ขั้นตอนที่สอง หากแต่เป็นขั้นตอนแรก เพราะการหาค่า a ซึ่ง P(a) เป็นจริงอาจคล้ายกับการงมเข็มในมหาสมุทร. ถ้าเราโชคดีที่หาพบ การพิสูจน์ว่า P(a) เป็นจริงในขั้นตอนที่สองก็มักทำได้อย่างง่ายดาย แต่ถ้าเราโชคร้ายหาไม่พบ ก็เท่ากับว่าเราไม่ได้พิสูจน์อะไรเลย เพราะการหาไม่พบมิได้หมายความว่าไม่มี.

สิ่งที่ควรตระหนักประการหนึ่งในการเขียนบทพิสูจน์การมีอยู่จริงโดยการหาตัวอย่างคือ บทพิสูจน์มักจะไม่กล่าวถึงขั้นตอนแรกแต่อย่างใด แต่จะแสดงเฉพาะการพิสูจน์ P(a) ในขั้นตอนที่สองเท่านั้น. ที่เป็นเช่นนี้เพราะเป็นขนบธรรมเนียมของการเขียนบทพิสูจน์ที่จะแสดงเฉพาะความสมเหตุสมผลที่จะนำไปสู่ข้อความที่เราจะพิสูจน์เท่านั้น โดยไม่จำเป็นต้องแสดงว่าเราคิดเหตุผลเหล่านี้ขึ้นมาได้อย่างไร ดังนั้นบทพิสูจน์จึงไม่จำเป็นต้องอธิบายว่าเราหาค่า a ดังกล่าวพบได้อย่างไร เพียงแต่แสดงให้เห็นว่า P(a) เป็นจริงก็เพียงพอแล้ว. เรื่องราวของการหาค่า a ในขั้นตอนที่ 1 จึงเพียงอยู่ในกระดาษทดของผู้พิสูจน์ ในขณะที่บทพิสูจน์ที่ปรากฏต่อสายตาชาวโลกจะมีเค้าโครงดังต่อไปนี้:

ให้ x = a (ที่เราหาพบแล้วในกระดาษทด)
พิสูจน์ P(a).
ดังนั้น $\exists x\ P(x)$.

ตัวอย่าง 15: จงพิสูจน์ว่า “มีจำนวนคู่บางตัวที่ 3 หารลงตัว”

<u>วิธีทำ</u> เราหาจำนวนคู่ที่ 3 หารลงตัวได้มากมายเช่น 6, 12, 30 เป็นต้น ดังนั้นเราเขียนบทพิสูจน์ดังนี้.

บทพิสูจน์: เนื่องจาก 6 เป็นจำนวนคู่ และ 3 หาร 6 ลงตัว ดังนั้นมีจำนวนคู่ที่ 3 หารลงตัวอยู่จริง.

❑

ตัวอย่าง 16: จงพิสูจน์ทฤษฎีบทต่อไปนี้

ทฤษฎีบท: *สำหรับจำนวนจริงบวก x แต่ละตัว, จะมีจำนวนจริง y ซึ่ง y(y+1) = x.*

<u>วิธีทำ</u> เราต้องการหาค่า y ที่สอดคล้องกับสมการ y(y+1) = x เมื่อ x เป็นจำนวนเต็มบวก. การหาค่า y ดังกล่าวทำได้โดยมอง x เป็นค่าคงที่ แล้วแก้สมการ $y^2+y-x = 0$ เพื่อหาค่า y ในเทอมของ x. ดังนั้นเราได้ y

สองค่าคือ $y = \left(-1 \pm \sqrt{1+4x}\right)\big/2$ เนื่องจาก x เป็นจำนวนเต็มบวก ค่า 1+4x เป็นบวก ทำให้ค่า y ทั้งสองเป็นจำนวนจริงเสมอ. เนื่องจากค่า y เพียงค่าเดียวก็เพียงพอต่อการพิสูจน์ เราจะเลือกเพียงค่าเดียวคือ $y = \left(-1 + \sqrt{1+4x}\right)\big/2$. บทพิสูจน์ข้างล่างจะกล่าวแต่เพียงค่า y ที่เราหามาได้ แต่ไม่จำเป็นต้องบรรยายที่มาของค่านี้แต่ประการใด.

บทพิสูจน์:

1. ให้ x เป็นจำนวนจริงบวกใดๆ.
2. ให้ $y = \left(-1 + \sqrt{1+4x}\right)\big/2$. จะเห็นว่า y เป็นจำนวนจริง เพราะ x เป็นจำนวนจริงบวก ทำให้ $1+4x > 0$.
3. ดังนั้นเราได้ $y(y+1) = \left(\dfrac{-1+\sqrt{1+4x}}{2}\right)\left(\dfrac{-1+\sqrt{1+4x}}{2}+1\right) = \dfrac{-1+4x-1}{4} = x$
4. จาก 2 และ 3 แสดงว่าเราหาจำนวนจริง y ได้เสมอ (จากสูตรในข้อ 2) สำหรับทุกจำนวนจริงบวก x ที่ทำให้ y(y+1) = x. ดังนั้นทฤษฎีบทนี้เป็นจริง.

❑

เราอาจพิสูจน์ข้อความในรูป $\exists x\ P(x)$ ได้โดยไม่ต้องหาค่า a ที่ทำให้ P(a) เป็นจริง แต่แสดงให้เห็นว่าค่า a ที่ทำให้ P(a) เป็นจริงนั้น *จะต้องมีอยู่อย่างแน่นอน* หรือ *เป็นไปไม่ได้ที่จะไม่มี*. การพิสูจน์ในลักษณะนี้เรียกว่า **การพิสูจน์การมีอยู่จริงโดยปราศจากตัวอย่าง** (nonconstructive existence proof) ดังแสดงในตัวอย่างต่อไปนี้.

ตัวอย่าง 17: จงพิสูจน์ทฤษฎีบทต่อไปนี้:

ทฤษฎีบท: *สำหรับทุกจำนวนเต็มบวก n, จะมีจำนวนเฉพาะที่มากกว่า n เสมอ.*

<u>*วิธีทำ*</u> เราจะพิสูจน์โดยแสดงให้เห็นว่า จำนวนเฉพาะที่มากกว่าจำนวนเต็มบวก n ใดๆ จะต้องมีอยู่อย่างแน่นอนแม้ว่าจะไม่ทราบว่ามีค่าเท่าใด. ให้สังเกตว่าพระเอกที่นำเราไปสู่ดวงดาวได้คือจำนวนเต็ม n!+1.

บทพิสูจน์:

1. จำนวนเฉพาะทุกตัวใหญ่กว่า 1 ดังนั้นทฤษฎีบทนี้เป็นจริงเมื่อ n = 1.
2. ให้ n เป็นจำนวนเต็มบวกใดๆ ที่มากกว่า 1.
3. จำนวนเต็มบวกทุกตัวตั้งแต่ 2 ถึง n หารจำนวนเต็มบวก $(2\cdot 3\cdot\ldots\cdot n)+1 = n!+1$ ไม่ลงตัว เพราะทุกตัวหารแล้วเหลือเศษ 1.
4. จาก 3 แสดงว่าจำนวนเฉพาะทุกตัวที่น้อยกว่าหรือเท่ากับ n ล้วนหาร n!+1 ไม่ลงตัว.
5. จากทฤษฎีบทหลักมูลของเลขคณิต, n!+1 จะต้องมีตัวประกอบเฉพาะอย่างน้อยหนึ่งตัว. แต่เนื่องจาก n!+1 ไม่มีตัวประกอบเฉพาะที่เล็กกว่า n (จาก 4) ดังนั้นตัวประกอบเฉพาะของ n!+1 จะต้องมากกว่า n.
6. จาก 5 แสดงว่าจะต้องมีจำนวนเฉพาะที่มากกว่า n ดังนั้นทฤษฎีบทนี้เป็นจริง.

❑

*การพิสูจน์โดยข้อขัดแย้ง*เป็นอีกวิธีหนึ่งที่ใช้กันมากในการพิสูจน์การมีอยู่จริงโดยปราศจากตัวอย่าง. เราจะเริ่มพิสูจน์ข้อความในรูป $\exists x\ P(x)$ โดยการสมมติ<u>นิเสธ</u>ของข้อความนี้ นั่นคือสมมติว่า *ไม่มี x ตัวใดเลยที่ทำให้ P(x) เป็นจริง* แล้วแสดงให้เห็นว่าสมมติฐานนี้นำไปสู่ข้อความที่เป็นเท็จหรือข้อความที่ขัดแย้งกันเอง. เราจะใช้การพิสูจน์ทฤษฎีบทที่สำคัญต่อไปนี้เป็นตัวอย่าง.

ทฤษฎีบท 1: *จำนวนประกอบ n ทุกตัวมีตัวประกอบบางตัวที่มากกว่า 1 แต่ไม่เกิน $\sqrt{n}$.*

ตัวอย่าง 18: จงพิสูจน์ทฤษฎีบท 1 ข้างบน.

วิธีทำ ทฤษฎีบทนี้เป็นข้อความในรูป $\forall n \exists d\ P(n,d)$. เค้าโครงการพิสูจน์คือให้ n เป็นค่าใดๆ แล้วแสดงให้เห็นว่าสมมติฐาน $\sim\exists d\ P(n,d)$ นำไปสู่ข้อความที่เป็นเท็จ.

บทพิสูจน์: *(แบบที่ 1)*

1. ให้ n เป็นจำนวนประกอบใดๆ. ดังนั้น n จะต้องมีตัวประกอบที่มากกว่า 1 และน้อยกว่า n.
2. สมมติว่าตัวประกอบที่มากกว่า 1 ทุกตัวของ n มีค่ามากกว่า $\sqrt{n}$.
3. จาก 1, ให้ a เป็นตัวประกอบตัวหนึ่งของ n โดย $1 < a < n$. ดังนั้น n = ab สำหรับจำนวนเต็ม b บางตัว. ดังนั้นเราได้ b เป็นตัวประกอบอีกตัวหนึ่งของ n โดยที่ $1 < b < n$.
4. จากสมมติฐาน 2 เราได้ $a > \sqrt{n}$ และ $b > \sqrt{n}$.
5. ดังนั้นเราได้ $n = ab > \sqrt{n}\cdot\sqrt{n} = n$ นั่นคือ $n > n$ ซึ่งเป็นไปไม่ได้.
6. สมมติฐาน 2 นำไปสู่ข้อสรุป 5 ซึ่งเป็นเท็จ ดังนั้นสมมติฐาน 2 เป็นเท็จ นั่นคือจะต้องมีตัวประกอบที่มากกว่า 1 บางตัวของ n ที่มีค่าไม่เกิน $\sqrt{n}$.

เราอาจเขียนบทพิสูจน์ทฤษฎีบทนี้ได้อีกแบบหนึ่ง โดยให้ส่วนของการพิสูจน์โดยข้อขัดแย้งอยู่ "ลึก" ลงไปกว่าบทพิสูจน์ข้างบน. ผู้อ่านบางคนอาจรู้สึกว่าบทพิสูจน์แบบที่สองข้างล่างอ่านเข้าใจง่ายกว่าแบบแรก.

บทพิสูจน์: *(แบบที่ 2)*

1. ให้ n เป็นจำนวนประกอบใดๆ. ดังนั้น n จะต้องมีตัวประกอบที่มากกว่า 1 และน้อยกว่า n.
2. ให้ a เป็นตัวประกอบตัวหนึ่งของ n โดย $1 < a < n$. ดังนั้น n = ab สำหรับจำนวนเต็ม b บางตัว. ดังนั้นเราได้ b เป็นตัวประกอบอีกตัวหนึ่งของ n โดยที่ $1 < b < n$.
3. สมมติว่า $a > \sqrt{n}$ และ $b > \sqrt{n}$.
4. ดังนั้นเราได้ $n = ab > \sqrt{n}\cdot\sqrt{n} = n$ นั่นคือ $n > n$ ซึ่งเป็นไปไม่ได้.
5. สมมติฐาน 3 นำไปสู่ข้อสรุป 4 ซึ่งเป็นเท็จ แสดงว่าสมมติฐาน 3 เป็นเท็จ ดังนั้น a หรือ b จะต้องมีค่าไม่เกิน $\sqrt{n}$. ดังนั้น n มีตัวประกอบบางตัวที่มากกว่า 1 แต่ไม่เกิน $\sqrt{n}$.

❑

ทฤษฎีบท 1 ข้างบนมีประโยชน์ในการตรวจสอบว่าจำนวนเต็มบวกใดเป็นจำนวนเฉพาะหรือไม่. ประโยชน์ในการตรวจสอบดังกล่าวมาจากบทอนุนัยของทฤษฎีบทนี้ ดังต่อไปนี้:

บทอนุนัย 1a: ให้ n เป็นจำนวนเต็มที่มากกว่า 1. ถ้าจำนวนเต็มทุกตัวที่มากกว่า 1 แต่ไม่เกิน $\sqrt{n}$ หาร n ไม่ลงตัว, จะได้ n เป็นจำนวนเฉพาะ.

บทพิสูจน์: ผู้อ่านควรพิสูจน์เป็นแบบฝึกหัดโดยแสดงให้เห็นว่า บทอนุนัย 1a กับทฤษฎีบท 1 เป็นข้อความที่สมมูลกัน.

❑

เมื่อเราต้องการตรวจสอบว่าจำนวนเต็มบวก n ใดๆ เป็นจำนวนเฉพาะหรือไม่ ถ้าเราไม่ทราบบทอนุนัย 1a เราจะเอาจำนวนเต็มบวกทุกตัวที่อยู่ระหว่าง 2 ถึง n (รวม 2 แต่ไม่รวม n) มาลองหาร n ดู; ถ้าพบว่าทุกตัวหาร n ไม่ลงตัว เราจึงสรุปว่า n เป็นจำนวนเฉพาะ. แต่บทอนุนัย 1a ข้างบนชี้แนะว่า เราไม่จำเป็นต้องลองตัวหารที่ใหญ่เกิน $\sqrt{n}$ ให้เสียเวลา เพียงลองตัวหารตั้งแต่ 2 จนถึง $\sqrt{n}$ ก็พอแล้ว ดังตัวอย่างต่อไปนี้.

ตัวอย่าง 19: จงตรวจสอบว่า 53 เป็นจำนวนเฉพาะหรือไม่ โดยใช้ความรู้จากบทอนุนัย 1a.

วิธีทำ จำนวนเต็มบวกที่มากกว่า 1 แต่ไม่เกิน $\sqrt{53}$ มี 6 ตัวคือ 2, 3, 4, 5, 6, และ 7. เราพบว่าทั้ง 6 ตัวนี้หาร 53 ไม่ลงตัว ดังนั้นสรุปได้ว่า 53 เป็นจำนวนเฉพาะ.

❑

บทอนุนัย 1b ข้างล่างทำให้จำนวนตัวหารที่จะนำมาลองลดน้อยลงไปอีก ถ้าเราทราบจำนวนเฉพาะในช่วง 2 ถึง $\sqrt{n}$.

บทอนุนัย 1b: ให้ n เป็นจำนวนเต็มที่มากกว่า 1. ถ้าจำนวนเฉพาะทุกตัวที่ไม่เกิน $\sqrt{n}$ หาร n ไม่ลงตัว, จะได้ n เป็นจำนวนเฉพาะ.

บทพิสูจน์: ผู้อ่านควรพิสูจน์เป็นแบบฝึกหัดโดยใช้บทอนุนัย 1a และความรู้เกี่ยวกับการหารจำนวนเต็ม.

❑

ตัวอย่าง 20: จงตรวจสอบว่า 53 เป็นจำนวนเฉพาะหรือไม่ โดยใช้ความรู้จากบทอนุนัย 1b.

วิธีทำ เราทราบว่าจำนวนเฉพาะที่ไม่เกิน $\sqrt{53}$ มี 4 ตัวคือ 2, 3, 5, และ 7. เราพบว่าทั้ง 4 ตัวนี้หาร 53 ไม่ลงตัว ดังนั้นสรุปได้ว่า 53 เป็นจำนวนเฉพาะ.

❑

การพิสูจน์การมีอยู่เพียงหนึ่งเดียว (Existence and Uniqueness Proof)

ทฤษฎีบทจำนวนไม่น้อยเป็นข้อความที่กล่าวถึงการมีอยู่เพียงหนึ่งเดียวของสิ่งนามธรรมบางอย่าง. ตัวอย่างเช่นทฤษฎีบทขั้นตอนการหารในหัวข้อ 2.5 มีใจความว่า จะมีผลหารและเศษเหลือของการหารจำนวนเต็มตัวหนึ่งด้วยจำนวนเต็มบวกอีกตัวหนึ่งเสมอและมีเพียงคู่เดียว ซึ่งเราเขียนในรูปสัญลักษณ์ได้ว่า $\forall a\in\mathbb{Z}\ \forall d\in\mathbb{Z}^+\ \exists! q\in\mathbb{Z}\ \exists! r\in\mathbb{Z}\ ([0 \leq r < d]\wedge[a = qd+r])$. การพิสูจน์ข้อความในรูป $\exists! x\ P(x)$ เช่นนี้เรียกว่า **การพิสูจน์การมีอยู่เพียงหนึ่งเดียว** (existence and uniqueness proof).

ในหัวข้อย่อยที่แล้ว เราได้ศึกษาวิธีการพิสูจน์ข้อความในรูป $\exists x\ P(x)$ ซึ่งเป็นการแสดงแต่เพียงว่า*จะต้องมีค่า x อย่างน้อยหนึ่งค่า*ที่ทำให้ P(x) เป็นจริง. การพิสูจน์ข้อความในรูป $\exists! x\ P(x)$ จะต้องออกแรงมากกว่านั้น เพราะนอกจากจะต้องพิสูจน์ว่ามีค่า x ที่ทำให้ P(x) เป็นจริงแล้ว ยังต้องแสดงด้วยว่าค่า x เช่นนั้น *มีเพียงค่าเดียวที่เป็นไปได้*.

เทคนิคการพิสูจน์ข้อความในรูป $\exists! x\ P(x)$ มาจากความจริงที่เราทราบจากหัวข้อ 1.3 ว่า ข้อความทั้งสามรูปแบบต่อไปนี้สมมูลกัน:

1. $\exists! x\ P(x)$

2. $\exists x(P(x) \wedge \forall y(P(y) \rightarrow [x=y]))$
3. $(\exists x\ P(x)) \wedge \forall x \forall y((P(x) \wedge P(y)) \rightarrow [x=y])$

การสมมูลกันของข้อความทั้งสามทำให้เราได้วิธีการพิสูจน์ข้อความในรูป $\exists! x\ P(x)$ สองวิธี. *วิธีแรก*โดยการพิสูจน์ข้อความ $\exists x(P(x) \wedge \forall y(P(y) \rightarrow [x=y]))$ และ*วิธีที่สอง*โดยการพิสูจน์ข้อความ $(\exists x P(x)) \wedge \forall x \forall y((P(x) \wedge P(y)) \rightarrow [x=y])$.

การพิสูจน์ข้อความในรูป $\exists! x\ P(x)$ โดยการพิสูจน์ $\exists x(P(x) \wedge \forall y(P(y) \rightarrow [x=y]))$

ข้อความ $\exists x(P(x) \wedge \forall y(P(y) \rightarrow [x=y]))$ แสดงโดยนัยว่าการพิสูจน์มี 2 ขั้นตอนใหญ่ที่ต่อเนื่องกัน นั่นคือ

ขั้นตอนที่ 1: พิสูจน์ข้อความ $\exists x\ P(x)$ โดยการหาตัวอย่างด้วยวิธีการในหัวข้อย่อยที่แล้ว. สมมติว่าเราได้ค่า a ที่ทำให้ P(a) เป็นจริง.

ขั้นตอนที่ 2: พิสูจน์ว่า $\forall y(P(y) \rightarrow [y=a])$ โดยใช้ค่า a ได้จากขั้นตอนที่ 1.

จะเห็นว่าขั้นตอนแรกเป็นการพิสูจน์**การมีอยู่จริง** (existence) และขั้นตอนที่สองเป็นการพิสูจน์**ความเป็นไปได้อย่างเดียว** (uniqueness) ของการมีอยู่นั้น. เนื่องจากการพิสูจน์ความเป็นไปได้อย่างเดียวในขั้นตอนที่สองจะต้องใช้ค่า a ที่พบในขั้นตอนที่ 1 ดังนั้นการพิสูจน์ในขั้นตอนแรกจึงต้องใช้วิธีพิสูจน์โดยการหาตัวอย่าง. ส่วนการพิสูจน์ $\forall y(P(y) \rightarrow [y=a])$ ในขั้นตอนที่สองนั้น เราใช้เทคนิคและวิธีการใดก็ได้ที่บรรยายในหัวข้อย่อยที่ผ่านมา. ดังนั้นเค้าโครงการพิสูจน์โดยรวมเป็นดังนี้:

[ส่วนการมีอยู่จริง]
 ให้ x = a (ที่เราหาพบแล้วในกระดาษทด)
  พิสูจน์ P(a).
 ดังนั้น $\exists x\ P(x)$.
[ส่วนความเป็นไปได้อย่างเดียว]
 ให้ y เป็นค่าใดๆ
  พิสูจน์ $P(y) \rightarrow [y=a]$.
 ดังนั้นค่า x ที่ทำให้ P(x) เป็นจริงนั้นมีเพียงหนึ่งเดียวคือค่า a.

ดังนั้น $\exists! x\ P(x)$.

ตัวอย่าง 21: จงพิสูจน์ข้อความต่อไปนี้:

สำหรับทุกจำนวนจริง x ที่ไม่เท่ากับ 1, จะมีจำนวนจริง y เพียงค่าเดียวเท่านั้นที่ทำให้ y/(y+1) = x.

<u>*วิธีทำ*</u> ทฤษฎีบทนี้คือข้อความ $\forall x\ ([x \neq 1] \rightarrow \exists! y\ [y/(y+1) = x])$. เราจะพิสูจน์โดยให้ x เป็นจำนวนจริงใดๆ ที่ไม่เท่ากับ 1 แล้วพิสูจน์ข้อความ $\exists! y\ [y/(y+1) = x]$ เป็นสองขั้นตอนคือ

ส่วนการมีอยู่จริง: พิสูจน์ว่า มีจำนวนจริง y ซึ่ง y/(y+1) = x โดยหาค่า a ที่ทำให้ a/(a+1) = x.

ส่วนความเป็นไปได้อย่างเดียว: พิสูจน์ว่า ถ้ามีจำนวนจริง z ใดที่ทำให้ z/(z+1) = x, จะได้ z= a.

ก่อนที่เราจะเริ่มพิสูจน์ เราควรหาค่า a ที่ทำให้ a/(a+1) = x เสียก่อน โดยการแก้สมการ y/(y+1) = x. เราได้ y = x/(1-x) ซึ่งหาค่าได้เสมอเมื่อ $x \neq 1$ ดังนั้นค่า a ที่เราต้องการก็คือ x/(1-x).

บทพิสูจน์:

1. ให้ x เป็นจำนวนจริงใดๆ โดย $x \neq 1$.

(ส่วนการมีอยู่จริง)

2. ให้ y = x/(1-x).
3. ดังนั้นเราได้ y/(y+1) = (x/(1-x))/((x/(1-x))+1) = (x/(1-x))(1-x) = x.
4. ดังนั้นแสดงว่า มีจำนวนจริง y (นั่นคือค่า y ในข้อ 2) ที่ทำให้ y/(y+1) = x.

(ส่วนความเป็นไปได้อย่างเดียว)

5. ให้ z เป็นจำนวนจริงซึ่ง z/(z+1) = x.
6. แก้สมการ z/(z+1) = x ได้ z = x/(1-x) ซึ่งเท่ากับค่า y ในข้อ 2.
7. ดังนั้น มีจำนวนจริง y เพียงค่าเดียว (คือค่า y ในข้อ 2) ที่ทำให้ y/(y+1) = x.

❑

การพิสูจน์ข้อความในรูป ∃!x P(x) โดยการพิสูจน์ (∃x P(x)) ∧ ∀x∀y((P(x)∧P(y))→[x=y])

การพิสูจน์ข้อความ (∃x P(x)) ∧ ∀x∀y((P(x)∧P(y))→[x=y]) ค่อนข้างสะดวกกว่าการพิสูจน์ข้อความ ∃x(P(x) ∧ ∀y(P(y)→[x=y])) เพราะบทพิสูจน์<u>ส่วนการมีอยู่จริง</u> (คือข้อความ ∃x P(x)) แยกเป็นอิสระจากบทพิสูจน์<u>ส่วนความเป็นไปได้อย่างเดียว</u> (คือข้อความ ∀x∀y((P(x)∧P(y))→[x=y])) โดยสิ้นเชิง ดังนั้นเราจึงมีอิสระที่จะพิสูจน์ส่วนการมีอยู่จริงด้วยวิธีการใดก็ได้แล้วแต่สะดวก ไม่จำเป็นต้องพิสูจน์โดยการหาตัวอย่างเหมือนแบบที่แล้ว. เค้าโครงการพิสูจน์จึงเป็นดังนี้:

[ส่วนการมีอยู่จริง]
พิสูจน์ ∃x P(x).
ดังนั้น ∃x P(x).
[ส่วนความเป็นไปได้อย่างเดียว]
ให้ x และ y เป็นค่าใดๆ.
พิสูจน์ (P(x)∧P(y))→[x=y]).
ดังนั้น (∃x P(x))→[ค่า x ที่ทำให้ P(x) เป็นจริงนั้นมีเพียงหนึ่งเดียว]
ดังนั้น ∃!x P(x).

ให้สังเกตว่าบทพิสูจน์ทั้งสองส่วนเป็นอิสระจากกันโดยสิ้นเชิงในแง่ที่ว่า แต่ละส่วนไม่ได้ทึกทักว่าอีกส่วนหนึ่งเป็นความจริง ดังนั้นจึงไม่ได้อ้างซึ่งกันและกัน. เนื่องจากการพิสูจน์*ส่วนความเป็นไปได้อย่างเดียว*ไม่ได้สนใจแม้แต่น้อยว่าค่า x ที่ทำให้ P(x) เป็นจริงนั้นที่แท้แล้วมีหรือไม่ ดังนั้นอาจเป็นไปได้ที่เราจะมีข้อความในรูป ∃!x P(x) ที่เราสามารถพิสูจน์ได้แต่เพียง*ส่วนความเป็นไปได้อย่างเดียว* แต่ยังไม่สามารถพิสูจน์*ส่วนการมีอยู่จริง*ได้.

ตัวอย่างของเหตุการณ์เช่นนี้เช่นข้อความที่ว่า *"มีคนเพียงคนเดียวเท่านั้นในจักรวาลที่ตัวล่ำบึ๊กแต่กลับสวมเสื้อเบอร์ S, ใส่กางเกงในไว้ด้านนอก, และบินด้วยความเร็วเหนือเสียงโดยทรงผมยังคงเรียบแปร้".* เป็นที่ยอมรับกันมานานในวงการคณิตศาสตร์ว่า *ถ้ามีบุคคลประหลาดขนาดนี้จริง ก็จะมีเพียงคนเดียวเท่านั้น* เราจึงเรียกเขาอย่างยกย่องว่า **ซูเปอร์แมน** (superman) และสร้างภาพยนตร์แสดงวีรกรรมของเขามากมาย แต่น่าเสียดายที่จนบัดนี้ยังไม่มีใครพิสูจน์ได้ว่าวีรบุรุษผู้นี้มีตัวตนจริง.

ตัวอย่าง 22: จงพิสูจน์ทฤษฎีบทต่อไปนี้:

ทฤษฎีบท: มีเซต $A \subseteq \mathbb{U}$ เพียงเซตเดียวเท่านั้นที่ทำให้ $A \cup B = B$ สำหรับทุกเซต $B \subseteq \mathbb{U}$.

_วิธีทำ_ ข้อความในทฤษฎีบทนี้คือ $\exists! A \forall B (A \cup B = B)$. เราจะพิสูจน์*ส่วนการมีอยู่*จริงกับ*ส่วนความเป็นไปได้อย่างเดียว*แยกเป็นอิสระจากกันโดยสิ้นเชิง โดยใช้เค้าโครงการพิสูจน์ดังแสดงข้างบน.

การพิสูจน์ส่วนการมีอยู่จริงเป็นการพิสูจน์ว่า "มีเซต A บางเซตซึ่งสำหรับทุกเซต B, $A \cup B = B$." เราจะลองพิสูจน์โดยวิธีหาตัวอย่าง. เมื่อลองนึกดูว่าจะมีเซตใดในเซตเอกภพที่ยูเนียนกับเซต B ใดๆแล้วได้เซต B ตัวเดิม เราคงนึกถึง *เซตว่าง* ทันที ดังนั้นเซตว่างคือตัวอย่างที่เราต้องการ. เราจึงเขียนบทพิสูจน์ส่วนการมีอยู่จริงได้อย่างง่ายดายดังนี้:

บทพิสูจน์ส่วนการมีอยู่จริง:

เนื่องจาก $\varnothing \cup B = B$ สำหรับทุกเซต $B \subseteq \mathbb{U}$. ดังนั้นมีเซต $A \subseteq \mathbb{U}$ บางเซต (เช่น $A = \varnothing$) ซึ่ง $A \cup B = B$ สำหรับทุกเซต $B \subseteq \mathbb{U}$.

การพิสูจน์ส่วนความเป็นไปได้อย่างเดียวเป็นการพิสูจน์ว่า "ถ้าเซต C และ D ใดๆ มีสมบัติที่ว่า $\forall B\, [C \cup B = B]$ และ $\forall B\, [D \cup B = B]$, จะได้ $C = D$." กโลบายการพิสูจน์ของเราคือเราจะแทน B ด้วย D ในสมการ $C \cup B = B$ และแทน B ด้วย C ในสมการ $D \cup B = B$. จากนั้นทุกอย่างก็จะราบรื่น:

บทพิสูจน์ส่วนความเป็นไปได้อย่างเดียว:

1. ให้ C และ D เป็นเซตใดๆ ที่มีสมบัติคือ สำหรับทุกเซต $B \subseteq \mathbb{U}$, $C \cup B = B$ และ $D \cup B = B$.
2. ดังนั้นเราได้ $C \cup D = D$ และ $D \cup C = C$.
3. จาก 2, เนื่องจาก $C \cup D = D \cup C$, เราได้ $C = D$.
4. ข้อความ 1 นำมาสู่ข้อสรุป 3 แสดงว่า ถ้ามีเซต A ซึ่ง $\forall B\, [A \cup B = B]$ แล้ว, เซตเช่นนี้จะมีเพียงเซตเดียว.

เนื่องจากบทพิสูจน์ทั้งสองส่วนเป็นอิสระจากกัน ลำดับก่อนหลังของบทพิสูจน์ทั้งสองจึงไม่มีความสำคัญ ดังนั้นเราอาจเขียนบทพิสูจน์ส่วนความเป็นไปได้อย่างเดียวก่อนบทพิสูจน์ส่วนการมีอยู่จริงก็ได้.
❑

การพิสูจน์แย้งโดยใช้ตัวอย่างค้าน (Disproof by Counterexample)

ในตัวอย่างการพิสูจน์ที่ผ่านมา เราพยายามพิสูจน์ข้อความต่างๆ โดยตระหนักอยู่แก่ใจแล้วว่าข้อความเหล่านั้นเป็นจริง (มิฉะนั้นผู้เขียนตำราเล่มนี้คงไม่นำมาเป็นตัวอย่างแสดงวิธีพิสูจน์). ในโลกความเป็นจริง ผู้พิสูจน์อาจตกอยู่ในสถานการณ์ที่ต้องพิสูจน์ข้อความที่ไม่มีใคร (ในละแวกนั้น) ทราบว่าเป็นจริง

หรือไม่. ควรทราบว่าการพิสูจน์ข้อความที่ยังไม่รู้ว่าเป็นจริงหรือเท็จย่อมยากลำบากและสยองขวัญกว่าการพิสูจน์ข้อความที่รู้อยู่แล้วว่าเป็นจริงมากนัก และการออกแรงพิสูจน์ข้อความที่ที่แท้แล้วเป็นเท็จก็เป็นการเสียเวลาเปล่า เพราะไม่ว่าเราจะพยายามแค่ไหนก็ไม่มีวันสำเร็จ.

ข้อความที่มีเค้าว่าอาจเป็นจริงแต่ยังพิสูจน์ไม่ได้ว่าเป็นจริงหรือเท็จเรียกว่า **ข้อความคาดการณ์** (conjecture). ข้อความคาดการณ์ทางคณิตศาสตร์ที่ถูกพิสูจน์แล้วว่าเป็นจริง ก็จะเปลี่ยนสถานภาพเป็น*ทฤษฎีบท*. อันที่จริงแล้ว ถึงแม้ว่าข้อความคาดการณ์ P ใดๆ ถูกพิสูจน์แล้วว่าเป็นเท็จ ก็นับว่าเป็นข่าวดีเช่นกัน เพราะ P จะไม่ใช่ข้อความคาดการณ์อีกต่อไป และเราได้ $\sim$P เป็นทฤษฎีบทอีกบทหนึ่ง.

การพิสูจน์ว่าข้อความใดข้อความหนึ่งเป็นเท็จเรียกว่า**การพิสูจน์แย้ง** (disproof). การพิสูจน์แย้งข้อความ P ใดๆ ก็คือการพิสูจน์ข้อความ $\sim$P นั่นเอง ซึ่งเราอาจเลือกใช้เทคนิคการพิสูจน์ใดก็ได้ที่ร่ำเรียนมา. ตัวอย่างเช่น การพิสูจน์แย้งข้อความ "$\sqrt{2}$ เป็นจำนวนตรรกยะ" ก็คือการพิสูจน์นิเสธของข้อความนี้ นั่นคือพิสูจน์ว่า "$\sqrt{2}$ ไม่เป็นจำนวนตรรกยะ" ซึ่งเราเคยกระทำแล้วในตัวอย่าง 8 ข้างบน.

โดยสรุปแล้วเค้าโครงทั่วไปของการพิสูจน์แย้งข้อความ P ใดๆ จะเป็นดังนี้:

พิสูจน์ข้อความ $\sim$P.
ดังนั้น P เป็นเท็จ.

พิจารณากรณีที่ข้อความที่เราต้องการพิสูจน์แย้งอยู่ในรูป $\forall x\ P(x)$. เราทราบจากตรรกศาสตร์แล้วว่านิเสธของข้อความนี้คือ $\exists x \sim P(x)$ ซึ่งหมายความว่าจะต้องมีค่า x บางค่าที่ทำให้ P(x) เป็นเท็จ. เราเรียกค่า x ซึ่ง P(x) เป็นเท็จนี้ว่าเป็น**ตัวอย่างค้าน** (counterexample) ของข้อความ $\forall x\ P(x)$ เพราะค่า x ดังกล่าวทำให้เราสรุปได้ว่าข้อความ $\forall x\ P(x)$ เป็นเท็จ. **การพิสูจน์แย้งโดยใช้ตัวอย่างค้าน** (disproof by counterexample) จึงมีเค้าโครงดังนี้:

ให้ x = a (คือ *ตัวอย่างค้าน* ที่เราหาพบแล้วในกระดาษทด)
แสดงให้เห็นว่า P(a) เป็นเท็จ.
ดังนั้นข้อความ $\forall x\ P(x)$ เป็นเท็จ.

ตัวอย่าง 23: จงพิสูจน์หรือพิสูจน์แย้งข้อความ "n^2-n+41 เป็นจำนวนเฉพาะสำหรับทุกจำนวนนับ n."

<u>*วิธีทำ*</u> เมื่อเรายังไม่ทราบว่าข้อความนี้เป็นจริงหรือเท็จ เราก็ยังไม่ควรทุ่มเทความพยายามหาวิธีพิสูจน์ข้อความนี้ เพราะถ้าข้อความนี้ที่แท้แล้วเป็นเท็จ ความพยายามของเราก็สูญเปล่า. โดยธรรมชาติแล้ว เราจะลองแทนค่า n ในสูตรดังกล่าวดู โดยเริ่มตั้งแต่ n = 0, 1, 2, 3, ... ไปตามลำดับ. เราจะประหลาดใจ (ระคนดีใจ) ที่พบว่าเราได้ n^2-n+41 เป็นจำนวนเฉพาะโดยตลอดสำหรับค่า n น้อยๆ เหล่านี้ ดังนั้นด้วยความอุตสาหะ เราจึงลองแทนค่า n ตั้งแต่ 0 ไปจนถึง 40 และยังพบว่า $40^2-40-41 = 1601$ เป็นจำนวนเฉพาะ. ถึงตอนนี้หลายคนจะค่อนข้างเชื่อแล้วว่าข้อความนี้น่าจะเป็นจริง และเริ่มลงมือเค้นสมองหาวิธีพิสูจน์กันเป็นการใหญ่.

โชคร้ายที่ผู้ที่พยายามพิสูจน์จะไม่มีวันพบความสำเร็จ เพราะที่แท้แล้วข้อความนี้เป็นเท็จ. ผู้ที่มีปฏิภาณไหวพริบดีจะสนใจเลข 41 เป็นพิเศษ จึงลองแทนค่า n = 41 ในสูตร แล้วพบว่า $41^2-41+41 = 41^2$ เป็นจำนวนประกอบ. ดังนั้น n = 41 คือตัวอย่างค้านของข้อความนี้ เราจึงสรุปได้ว่าข้อความนี้ไม่เป็นความจริง.

❑

ตัวอย่าง 24: จงพิสูจน์หรือพิสูจน์แย้งข้อความต่อไปนี้:

ให้ n เป็นจำนวนเต็มและ d เป็นจำนวนเต็มบวก. ถ้า d หาร n^2 ลงตัว, จะได้ d หาร n ลงตัว.

วิธีทำ ผู้ที่พยายามพิสูจน์ข้อความนี้จะไม่มีทางประสบความสำเร็จเช่นกัน. ตัวอย่างค้านของข้อความนี้ เช่นเมื่อ n = 4 และ d = 8. จะเห็นว่า 8 หาร 4^2 ลงตัว แต่ 8 กลับหาร 4 ไม่ลงตัว ดังนั้นข้อความนี้ไม่เป็นความจริง.

❑

อนึ่ง ควรตระหนักว่า การหาตัวอย่างค้านเพื่อพิสูจน์แย้งข้อความคาดการณ์หนึ่งอาจไม่ใช่เรื่องง่ายเหมือนตัวอย่าง 23 และ 24 ข้างบนเสมอไป. ข้อความคาดการณ์บางข้อความทนทานต่อการพิสูจน์แย้งได้หลายร้อยปี. *เลออนฮาร์ด ออยเลอร์ (Leonhard Euler, 1707-1783)* นักคณิตศาสตร์ชาวสวิสเคยประกาศข้อความคาดการณ์หนึ่งว่า

ไม่มีจำนวนเต็มบวก a, b, c, และ d ใดที่สอดคล้องกับสมการ $a^4+b^4+c^4 = d^4$

เป็นเวลามากกว่าสองศตวรรษที่ไม่เคยมีใครพิสูจน์หรือพิสูจน์แย้งข้อความคาดการณ์ของออยเลอร์นี้ได้ จนกระทั่งเมื่อปีค.ศ. 1987 นักคณิตศาสตร์จากมหาวิทยาลัยฮาร์วาร์ดชื่อ *โนอาม เอลคีส (Noam Elkies)* สามารถพิสูจน์แย้งข้อความนี้ได้สำเร็จ และอีกไม่นานต่อมา ด้วยความช่วยเหลือจากเครื่องคอมพิวเตอร์ *โรเจอร์ ฟราย (Roger Frye)* จาก Thinking Machines Corporation สามารถหาตัวอย่างค้านตัวอย่างหนึ่งได้สำเร็จเมื่อพบว่า

$$95800^4+217519^4+414560^4 = 422481^4.$$

อย่างไรก็ตาม ยังมีข้อความคาดการณ์อื่นๆ ในคณิตศาสตร์อีกไม่น้อยที่ยังรอการพิสูจน์หรือการพิสูจน์แย้งอยู่จนกระทั่งบัดนี้. ข้อความคาดการณ์ที่มีชื่อเสียงแต่ดูเรียบง่ายมากคือ ***ข้อความคาดการณ์ของโกลด์บาค*** (Goldbach's conjecture) ซึ่งกล่าวว่า

จำนวนคู่ทุกตัวที่มากกว่า 4 เป็นผลบวกของจำนวนเฉพาะคี่สองตัว.

ข้อความคาดการณ์นี้เสนอโดยนักคณิตศาสตร์ชาวเยอรมันชื่อ *คริสเตียน โกลด์บาค (Chistian Goldbach, 1690-1764)* เมื่อปีค.ศ. 1742. จนบัดนี้ผ่านไปแล้วกว่า 250 ปีก็ยังไม่มีใครพิสูจน์หรือพิสูจน์แย้งหรือหาตัวอย่างค้านได้. แม้ว่าจะมีการใช้เครื่องคอมพิวเตอร์แสดงให้เห็นแล้วว่าข้อความคาดการณ์ของโกลด์บาคยังคงเป็นจริงจนถึง 10^{14} แต่นั่นก็ยังไม่สามารถเปลี่ยนสถานภาพของข้อความคาดการณ์นี้เป็นทฤษฎีบทได้.

สุดยอดแห่งเกม (The Ultimate Game)

การพิสูจน์คือการเข้าถึงแก่นแท้ของวิชาคณิตศาสตร์. ข้อความในทฤษฎีบทต่างๆ เป็นเพียงความจริงที่ตายตัว หยุดนิ่ง ไม่แสดงความสำคัญของตัวมันเอง ไม่แสดงความเชื่อมโยงกับทฤษฎีบทอื่น และไม่ชี้แนะไปสู่ความคิดสร้างสรรค์ใหม่ๆ แต่อย่างใด. ที่แท้แล้ว "ชีวิตชีวา" ของทฤษฎีบทล้วนอยู่ในบทพิสูจน์ของมันทั้งสิ้น. ความเรียงต่อไปนี้แสดงความสำคัญของการพิสูจน์ในคณิตศาสตร์ได้อย่างเยี่ยมยิ่ง:

การพิสูจน์ทางคณิตศาสตร์สนองจุดประสงค์หลายอย่างพร้อมกัน. เนื่องจากบทพิสูจน์จะต้องผ่านการพินิจพิจารณาจากผู้อ่านใหม่ๆ อยู่เสมอ จึงตกอยู่ในกระบวนการตรวจ

สอบและวิพากษ์วิจารณ์อยู่ตลอดเวลา ดังนั้นข้อผิดพลาด ความกำกวม หรือความเข้าใจผิดต่างๆ ในบทพิสูจน์จะค่อยๆ ปลาสนาการไป. บทพิสูจน์สร้างความยอมรับนับถือ. บทพิสูจน์คือตราประทับของ "พลังอำนาจแห่งความจริง" ของทฤษฎีบทที่มันพิสูจน์.

ในบทบาทที่ดีที่สุดของมัน บทพิสูจน์จะสร้างเสริมความเข้าใจด้วยการเปิดเผยให้เห็นหัวใจของเรื่องราว. บทพิสูจน์ชี้แนะให้เกิดความคิดสร้างสรรค์ใหม่ๆ ในคณิตศาสตร์. ผู้เริ่มต้นศึกษาคณิตศาสตร์ที่อ่านบทพิสูจน์จะได้สัมผัสอย่างใกล้ชิดถึงกระบวนการสร้างสรรค์ทางคณิตศาสตร์อันน่าตื่นตาตื่นใจ. บทพิสูจน์คือพลังขับเคลื่อนของคณิตศาสตร์ คือจิตวิญญาณที่ทำให้ข้อความอันจืดชืดตายตัวของทฤษฎีบทมีชีวิตชีวาขึ้นมา.

ท้ายที่สุด การพิสูจน์คือพิธีกรรมอันผ่าเผยของนักคณิตศาสตร์ เพื่อเฉลิมฉลองพลังสติปัญญาอันงดงามบริสุทธิ์ของมนุษยชาติ.

-- Philip J. Davis and Reuben Hersh, *The Mathematical Experience*, 1981

ในหัวข้อ 3.3 อันยาวนานนี้ เราได้เรียนรู้เทคนิคและวิธีการอันหลากหลายที่ใช้ในการพิสูจน์ข้อความทางคณิตศาสตร์. อย่างไรก็ตาม ไม่มีสิ่งที่เรียกว่า "สูตรสำเร็จ" ในการพิสูจน์ เพราะการพิสูจน์เป็นทั้งศาสตร์และศิลป์ที่ปราศจากขั้นตอนวิธีตายตัวอันใดที่จะใช้ได้ในทุกกรณีและทุกสถานการณ์. ส่วนที่เป็น "ศาสตร์" ของการพิสูจน์คือหลักการอ้างเหตุผลที่ถูกต้องบนพื้นฐานของหลักตรรกศาสตร์ซึ่งบรรยายในหัวข้อ 3.2 และเทคนิควิธีการต่างๆ ที่ใช้เป็น "แบบแผน" ของการพิสูจน์ดังบรรยายในหัวข้อ 3.3 นี้. แต่ทว่าผู้ที่เรียนรู้ศาสตร์ของการพิสูจน์เหล่านี้จนหมดสิ้นก็ไม่แน่ว่าจะพิสูจน์อะไรได้สำเร็จ ถ้าหากขาดประสบการณ์การฝึกฝน ปฏิภาณไหวพริบ และปัญญาญาณในเชิงคณิตศาสตร์. เราอาจดูคนว่ายน้ำนับร้อยนับพัน และเข้าใจแบบแผนการเคลื่อนไหวร่างกายในท่าว่ายต่างๆ เป็นอย่างดี แต่กลับว่ายน้ำเองไม่เป็น. ฉันใดก็ฉันนั้น. เราอาจอ่านบทพิสูจน์ของคนอื่นนับร้อยนับพัน สามารถไล่ตามตรรกะในบทพิสูจน์เหล่านั้นได้ แต่อาจไม่สามารถพิสูจน์อะไรด้วยตนเองได้เลย. นี่ย่อมสะท้อนว่าเรารู้แต่ "ศาสตร์" ของการพิสูจน์ แต่ยังไม่เข้าถึง "ศิลป์" ของการสร้างบทพิสูจน์ด้วยตนเอง. การเข้าถึงศิลปะการพิสูจน์ก็เช่นเดียวกับการพัฒนาทักษะอื่นๆ เช่นการว่ายน้ำหรือการเขียนโปรแกรมคอมพิวเตอร์ นั่นคือต้องอาศัยความสนใจใคร่รู้ การศึกษาเลียนแบบกระบวนท่าของยอดฝีมือ และที่สำคัญที่สุดคือการฝึกฝนตัวเองด้วยแบบฝึกหัด.

อนึ่ง แม้ว่าหัวข้อนี้จะบรรยายเทคนิควิธีการพิสูจน์เอาไว้มากมายก็ตาม แต่ยังขาดเทคนิคการพิสูจน์ที่สำคัญที่สุดอันหนึ่งไป นั่นคือ**การอุปนัยเชิงคณิตศาสตร์** (mathematical induction). เนื่องจากการอุปนัยเชิงคณิตศาสตร์เป็นเรื่องค่อนข้างใหญ่และมีเรื่องราวที่ตามมามากมาย เราจึงต้องอุทิศบทที่ 4 ทั้งบทให้กับเรื่องนี้ จึงจะเหมาะสมกับความสำคัญของมัน.

เราจะจบหัวข้อ 3.3 นี้ด้วยบทสนทนาในครอบครัวนักวิชาการครอบครัวหนึ่ง:

เด็กชายวัยสิบขวบคนหนึ่งรักการเล่นเกมคอมพิวเตอร์เป็นชีวิตจิตใจจนแทบไม่เป็นอันกินอันนอน. บ่ายวันหนึ่งขณะที่เขากำลังเล่นเกมคอมพิวเตอร์อย่างเมามัน พ่อของเด็กซึ่งเป็นนักคอมพิวเตอร์มายืนอยู่ข้างหลัง แล้วตบบ่าลูกชายเบาๆ.

"ลูกเอ๋ย ลูกเล่นเกมมาก็เยอะแล้ว น่าเสียดายที่ยังไม่รู้จัก 'สุดยอดแห่งเกม'"

เด็กชายตาเป็นประกาย หันมาถามทันที

"เกมอะไรครับพ่อ?"

พ่อยิ้มเล็กน้อย "การเขียนโปรแกรมคอมพิวเตอร์ไงลูก"
ทันใดนั้น เสียงชราภาพเสียงหนึ่งก็ดังขึ้นจากด้านหลัง
"หลานเอ๋ย ลูกเอ๋ย พวกเจ้าล้วนไม่รู้จัก 'สุดยอดแห่งเกม' ที่แท้จริง"
สองพ่อลูกหันมาถามพร้อมเพรียงกัน
"เกมอะไรครับปู่?"   "เกมอะไรครับพ่อ?"
"การพิสูจน์ทฤษฎีบท!" ปู่นักคณิตศาสตร์ตอบ.