# ทฤษฎีจำนวน

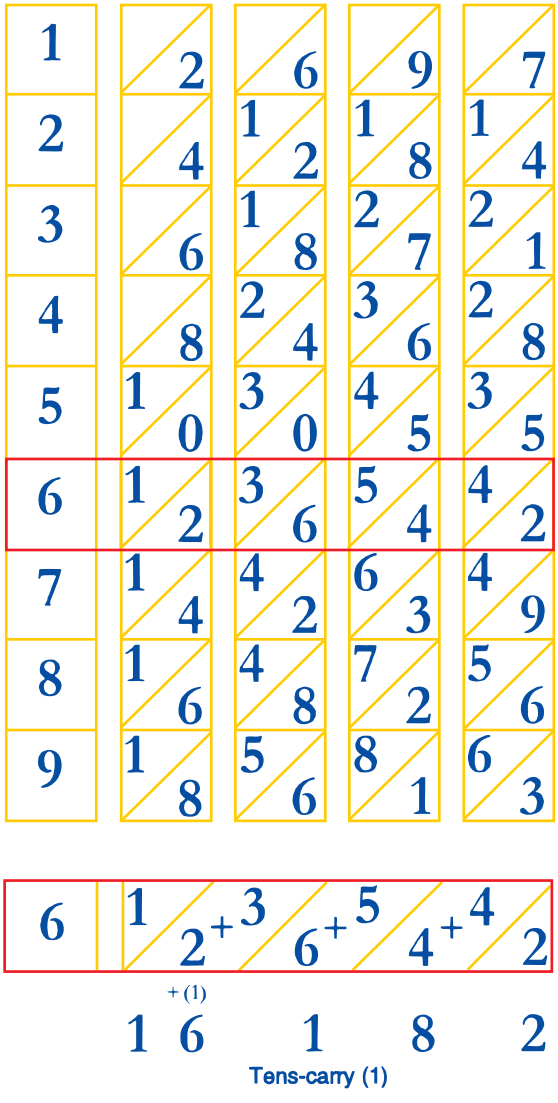
( ความรู้เบื้องต้น การหารลงตัว จำนวนเฉพาะ ข้อเท็จจริงบางประการเกี่ยวกับจำนวนเฉพาะ
ฟังก์ชันเลขคณิต คอนกรูเอนซ์ สมการไดโอแฟนไทน์ )

**โครงการตำราวิทยาศาสตร์และคณิตศาสตร์มูลนิธิ สอวน.**

# ทฤษฎีจำนวน

( ความรู้เบื้องต้น การหารลงตัว จำนวนเฉพาะ ข้อเท็จจริงบางประการเกี่ยวกับจำนวนเฉพาะ
ฟังก์ชันเลขคณิต คอนกรูเอนซ์ สมการไดโอแฟนไทน์ )

$$6 \times 2{,}697 = 16{,}182$$




*The model shows six rotating rods suitable for a six-digit multiplicand. As the rods cannot be exchanged, only four different digits can be chosen in each position.*

โครงการตำราวิทยาศาสตร์และคณิตศาสตร์มูลนิธิ สอวน.

# มูลนิธิส่งเสริมโอลิมปิกวิชาการและพัฒนามาตรฐานวิทยาศาสตร์ศึกษา ในพระอุปถัมภ์สมเด็จพระเจ้าพี่นางเธอ เจ้าฟ้ากัลยาณิวัฒนา กรมหลวงนราธิวาสราชนครินทร์ (สอวน.)

**ความเป็นมา**

ประเทศไทยส่งนักเรียนเข้าแข่งขันคณิตศาสตร์โอลิมปิกระหว่างประเทศครั้งแรกในปี พ.ศ. 2532 ที่ประเทศเยอรมนี โดยความร่วมมือระหว่างสมาคมวิทยาศาสตร์แห่งประเทศไทยในพระบรมราชูปถัมภ์ และสมาคมคณิตศาสตร์แห่งประเทศไทยในพระบรมราชูปถัมภ์ สมเด็จพระเจ้าพี่นางเธอ เจ้าฟ้ากัลยาณิวัฒนา (พระยศในขณะนั้น) ได้พระราชทานเงินส่วนพระองค์จำนวนหนึ่งเพื่อเป็นค่าใช้จ่าย

การคัดเลือกนักเรียนเพื่อไปแข่งขันคณิตศาสตร์โอลิมปิกระหว่างประเทศ ครั้งที่ 30 สมาคมคณิตศาสตร์แห่งประเทศไทยฯ ได้จัดคณาจารย์มหาวิทยาลัยจำนวนหนึ่งมาช่วยฝึกอบรมรวมเป็นเวลาประมาณสองเดือน เพื่อให้นักเรียนได้เรียนรู้เนื้อหาเพิ่มเติมครอบคลุมหลักสูตรที่จะใช้แข่งขัน ซึ่งอยู่ในระดับชั้นปีที่ 1-2 ของมหาวิทยาลัย จากผลสำเร็จในปีแรก ทำให้รัฐบาลเห็นความสำคัญจึงได้จัดสรรงบประมาณให้กับโครงการนี้ผ่านสถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) ตั้งแต่ปี พ.ศ. 2533 เป็นต้นมา สมทบกับเงินพระราชทานเป็นรายปีจากสมเด็จพระเจ้าพี่นางเธอ เจ้าฟ้ากัลยาณิวัฒนา กรมหลวงนราธิวาสราชนครินทร์ เพื่อสนับสนุนการส่งนักเรียนไทยไปแข่งขันโอลิมปิกวิชาการระหว่างประเทศ 5 สาขา จนถึงปัจจุบันรวม 14 ปี นักเรียนไทยได้ทำชื่อเสียงได้เหรียญทองรวม 17 เหรียญ เหรียญเงิน 53 เหรียญ เหรียญทองแดง 93 เหรียญ และเกียรติคุณประกาศอีก 35 ราย รวมทั้งสิ้น 198 รางวัล จากจำนวนนักเรียนที่ส่งไปเข้าแข่งขัน 276 คน (72%)

อย่างไรก็ตาม จากการที่ประเทศไทยดำเนินการจัดส่งนักเรียนเข้าร่วมการแข่งขันคณิตศาสตร์ วิทยาศาสตร์ โอลิมปิกระหว่างประเทศ ตั้งแต่ พ.ศ.2532 จนถึงปัจจุบัน ทำให้เห็นว่ามาตรฐานการศึกษาด้านคณิตศาสตร์และวิทยาศาสตร์ของไทยยังต่ำกว่ามาตรฐานสากล การเตรียมตัวของนักเรียนยังใช้เวลาน้อยเกินไป

เพื่อให้การส่งเสริมและสนับสนุนโครงการจัดส่งผู้แทนประเทศไทยไปแข่งขันโอลิมปิกวิชาการระหว่างประเทศมีประสิทธิภาพยิ่งขึ้นสมเด็จพระเจ้า พี่นางเธอ เจ้าฟ้ากัลยาณิวัฒนา กรมหลวงนราธิวาสราชนครินทร์ จึงมีพระดำริให้จัดตั้งมูลนิธิ สอวน. และได้รับอนุมัติจากกระทรวงมหาดไทยเมื่อวันที่ 12 ตุลาคม 2542 โดยมีวัตถุประสงค์หลัก 2 ประการ

**วัตถุประสงค์**

1. ส่งเสริมให้นักเรียนในระดับมัธยมศึกษาตอนปลายทั่วประเทศที่มีความสามารถทางวิทยาศาสตร์และคณิตศาสตร์ มีโอกาสได้รับการพัฒนาศักยภาพทางด้านคณิตศาสตร์ คอมพิวเตอร์ เคมี ฟิสิกส์ และชีววิทยา ตามความถนัดทั้งด้านทฤษฎีและทักษะด้านปฏิบัติ ให้สามารถคิดวิเคราะห์และแก้ปัญหาที่ซับซ้อนได้ โดยจัดให้มีศูนย์อบรมทั่วประเทศเป็นการเพิ่มเวลาฝึกอบรม เพื่อช่วยให้นักเรียนมีความพร้อมที่จะเข้ารับการคัดเลือกไปแข่งขันโอลิมปิกวิชาการระหว่างประเทศให้ได้ผลดียิ่งขึ้น ตามพระดำริของสมเด็จพระเจ้าพี่นางเธอเจ้าฟ้ากัลยาณิวัฒนา กรมหลวงนราธิวาสราชนครินทร์ องค์ประธานมูลนิธิ สอวน.
2. เพื่อนำประสบการณ์ที่ได้จากการแข่งขันโอลิมปิกวิชาการระหว่างประเทศมาพัฒนามาตรฐานคณิตศาสตร์และวิทยาศาสตร์ศึกษาของไทยให้สูงขึ้นเทียบเท่าระดับสากล

# โครงการตำราวิทยาศาสตร์และคณิตศาสตร์มูลนิธิ สอวน.

มูลนิธิส่งเสริมโอลิมปิกวิชาการและพัฒนามาตรฐานวิทยาศาสตร์ศึกษา ในพระอุปถัมภ์สมเด็จพระเจ้าพี่นางเธอ เจ้าฟ้ากัลยาณิวัฒนา กรมหลวงนราธิวาสราชนครินทร์ (สอวน.) ได้ร่วมมือกับคณาจารย์มหาวิทยาลัยของรัฐ 20 แห่ง และกระทรวงศึกษาธิการ ดำเนินการจัดตั้งศูนย์ สอวน. ในภูมิภาค 12 ศูนย์ และในกรุงเทพฯ 1 ศูนย์ (5 โรงเรียน) เพื่อพัฒนาศักยภาพทางปัญญาของนักเรียนที่มีความพร้อมในด้านวิทยาศาสตร์ คณิตศาสตร์และคอมพิวเตอร์จากทั่วประเทศ เพื่อให้นักเรียนได้มีความรู้ความสามารถเทียบเท่ามาตรฐานสากล และพร้อมที่จะสอบคัดเลือกเป็นผู้แทนประเทศไทยไปร่วมการแข่งขันโอลิมปิกวิชาการระหว่างประเทศในสาขาวิชาต่างๆ ได้ และเพื่อขยายผลจากประสบการณ์ที่ได้เข้าแข่งขันโอลิมปิกวิชาการระหว่างประเทศมาพัฒนามาตรฐานวิทยาศาสตร์และคณิตศาสตร์ของไทยให้สูงขึ้นเทียบเท่าสากล

ในการอบรมนักเรียนของศูนย์ สอวน. มูลนิธิ สอวน.ได้พิจารณาเห็นว่าตำราที่มีความสมบูรณ์ของเนื้อหาตามหลักสูตรของ สอวน. จะช่วยพัฒนาศักยภาพของนักเรียนในศูนย์สอวน.ให้สูงยิ่งขึ้นได้ นอกจากนั้นตำราเรียนในวิชาวิทยาศาสตร์และคณิตศาสตร์ในระดับมัธยมศึกษาตอนปลายที่มีความสมบูรณ์ถูกต้องยังขาดแคลน นักเรียนและครูสามารถนำตำราที่พัฒนาขึ้นมานี้ไปใช้เป็นหนังสืออ้างอิงประกอบการเรียนการสอนได้อีกด้วย มูลนิธิ สอวน. จึงได้มี “โครงการจัดทำตำราส่งเสริมพัฒนาศักยภาพของนักเรียนด้านวิทยาศาสตร์ คณิตศาสตร์และคอมพิวเตอร์” ขึ้น เพื่อผลิตตำราคณิตศาสตร์ คอมพิวเตอร์ เคมี ชีววิทยาและฟิสิกส์ที่มีเนื้อหาหลักสูตรตามมาตรฐานสากล โดยมีวัตถุประสงค์

1. เพื่อเป็นที่ระลึกในมหามงคลสมัยที่สมเด็จพระเจ้าพี่นางเธอ เจ้าฟ้ากัลยาณิวัฒนา กรมหลวงนราธิวาสราชนครินทร์ ทรงเจริญพระชนมายุ 80 พรรษา ซึ่งพระองค์ทรงมีพระมหากรุณาธิคุณต่อโครงการจัดส่งผู้แทนประเทศไทยไปแข่งขันโอลิมปิกวิชาการระหว่างประเทศและทรงสนับสนุนการดำเนินงานเพื่อพัฒนามาตรฐานการศึกษาวิทยาศาสตร์และคณิตศาสตร์ของไทยอย่างหาที่สุดมิได้

2. เพื่อผลิตหนังสือคณิตศาสตร์ คอมพิวเตอร์ เคมี ชีววิทยาและฟิสิกส์ระดับมัธยมศึกษาตอนปลายถึงระดับชั้นปีที่ 1 ของคณะวิทยาศาสตร์ในมหาวิทยาลัยให้มีคุณภาพเทียบเท่าสากล เรียบเรียงโดยคณาจารย์จากมหาวิทยาลัยของรัฐที่มีประสบการณ์สูงและที่มีส่วนรวมในการฝึกอบรมนักเรียนในค่าย สอวน. ค่าย สสวท. และควบคุมนักเรียนไปแข่งขันโอลิมปิกวิชาการระหว่างประเทศ เนื้อหาในหนังสือเน้นกระบวนการคิดแบบวิทยาศาสตร์ เพื่อฝึกฝนให้นักเรียนสามารถคิดวิเคราะห์และแก้ปัญหาที่ซับซ้อนทั้งในเชิงทฤษฎีและประยุกต์ได้โดยจัดพิมพ์บนกระดาษอาร์ตอย่างดีและมีภาพสีประกอบคำบรรยาย

โครงการตำราวิทยาศาสตร์และคณิตศาสตร์ของมูลนิธิ สอวน. มีเป้าหมายในการผลิตตำราคณิตศาสตร์ รวม 5 เล่ม คอมพิวเตอร์ 3 เล่ม เคมี 3 เล่ม ชีววิทยา 5 เล่ม และฟิสิกส์ 3 เล่ม โดยหนังสือชุดแรกจะนำขึ้นทูลเกล้าถวายในวันที่ 6 มิถุนายน 2547 ซึ่งเป็นวันประชุมสามัญประจำปี พ.ศ. 2547 ของคณะกรรมการบริหาร และสมเด็จพระเจ้าพี่นางเธอ เจ้าฟ้ากัลยาณิวัฒนา กรมหลวงนราธิวาสราชนครินทร์ เสด็จเป็นองค์ประธานที่ประชุม ส่วนที่เหลือคาดว่าจะจัดพิมพ์ให้แล้วเสร็จภายในปี พ.ศ. 2547 นี้ นอกจากนั้นคณะกรรมการโครงการผลิตตำราวิทยาศาสตร์และคณิตศาสตร์มูลนิธิ สอวน. มีเป้าหมายจะผลิตตำราที่มีคุณภาพสูงนี้ในระดับมัธยมศึกษาต้นโดยคณาจารย์จากมหาวิทยาลัย เพื่อวางรากฐานวิทยาศาสตร์และคณิตศาสตร์พื้นฐานและเพื่อสร้างแรงบันดาลใจและความสนใจทางด้านวิทยาศาสตร์ คณิตศาสตร์แก่เยาวชนอีกด้วย หากได้รับความอนุเคราะห์ช่วยเหลือด้านงบประมาณจากภาครัฐและเอกชน

คณะจัดทำหนังสือคณิตศาสตร์ วิทยาศาสตร์หวังว่าโครงการตำราคณิตศาสตร์ วิทยาศาสตร์ของมูลนิธิ สอวน. จะมีส่วนร่วมในการปฏิรูปการเรียนรู้และยกระดับมาตรฐานวิทยาศาสตร์และคณิตศาสตร์ของไทยให้เทียบเท่ากับระดับสากลเพื่อสนองพระดำริของสมเด็จพระเจ้าพี่นางเธอ เจ้าฟ้ากัลยาณิวัฒนา กรมหลวงนราธิวาสราชนครินทร์

**********

*คำขอบคุณ : คณะกรรมการดำเนินงานโครงการตำราฯ ขอขอบคุณพิพิธภัณฑ์ ARTTHMEUM, Bonn ที่อนุญาตให้ประธานคณะกรรมการฯ เข้าถ่ายภาพในพิพิธภัณฑ์ เพื่อนำมาเผยแพร่

# คณะกรรมการโครงการตำราวิทยาศาสตร์และคณิตศาสตร์มูลนิธิ สอวน.

**คณะกรรมการที่ปรึกษา**

| | |
|---|---|
| 1. ศาสตราจารย์ นายแพทย์ จรัส สุวรรณเวลา | รองประธานมูลนิธิ สอวน. |
| 2. รองศาสตราจารย์ ดร.กำจัด มงคลกุล | กรรมการมูลนิธิฯ |
| 3. ดร. คุณหญิงกษมา วรวรรณ ณ อยุธยา | กรรมการมูลนิธิฯ |
| 4. รองศาสตราจารย์ ดร. คุณหญิงสุมณฑา พรหมบุญ | กรรมการมูลนิธิฯ |
| 5. นายเชาว์ อรรถมานะ (อดีต) | กรรมการมูลนิธิฯ |
| 6. นายสมนึก พิมลเสถียร | กรรมการมูลนิธิฯ |
| 7. นายสุนทร อรุณานนท์ชัย | กรรมการมูลนิธิฯ |
| 8. รองศาสตราจารย์บุญรักษา สุนทรธรรม | กรรมการมูลนิธิฯ |

**คณะกรรมการดำเนินงานโครงการตำราฯ**

| | |
|---|---|
| 1. ศาสตราจารย์ศักดา ศิริพันธุ์ (ราชบัณฑิต) เลขาธิการมูลนิธิ สอวน. | ประธาน |
| 2. รองศาสตราจารย์เย็นใจ สมวิเชียร | รองประธาน |
| 3. รองศาสตราจารย์ ดร. ณรงค์ ปั้นนิ่ม | กรรมการ (วิชาคณิตศาสตร์) |
| 4. รองศาสตราจารย์ยืน ภู่วรวรรณ | กรรมการ (วิชาคอมพิวเตอร์) |
| 5. รองศาสตราจารย์ ดร. พินิติ รตะนานุกูล | กรรมการ (วิชาเคมี) |
| 6. ผู้ช่วยศาสตราจารย์ ดร. วุทธิพันธุ์ ปรัชญพฤทธิ์ | กรรมการ (วิชาฟิสิกส์) |
| 7. ศาสตราจารย์อักษร ศรีเปล่ง | กรรมการ (วิชาชีววิทยา ประเภทพืช) |
| 8. รองศาสตราจารย์ ดร. อุษณีย์ ยศยิ่งยวด | กรรมการ (วิชาชีววิทยา ประเภทสัตว์) |

**คณะผู้เขียนวิชาคณิตศาสตร์**

| | |
|---|---|
| 1. รองศาสตราจารย์ ดร. ณรงค์ ปั้นนิ่ม | ประธานคณะอนุกรรมการ |
| 2. ศาสตราจารย์ กิตติคุณยุพิน พิพิธกุล | อนุกรรมการ |
| 3. ผู้ช่วยศาสตราจารย์ ดร. อุษณีย์ ลีรวัฒน์ | อนุกรรมการ |
| 4. ผู้ช่วยศาสตราจารย์ ดร. นิตติยา ปภาพจน์ | อนุกรรมการ |
| 5. รองศาสตราจารย์ ดร. ฉวีวรรณ รัตนประเสริฐ | อนุกรรมการ |
| 6. รองศาสตราจารย์ ดร.วิเชียร เลาหโกศล | อนุกรรมการ |
| 7. ดร. ภัททิรา เรืองสินทรัพย์ | อนุกรรมการ |
| 8. นายวัชรพล พิมพ์เสริฐ | อนุกรรมการ |

# คำนำ

ตำราทฤษฎีจำนวนเล่มนี้ ผู้เขียนได้เขียนขึ้นมาโดยมีวัตถุประสงค์ 5 ประการ คือ

1. เพื่อรวบรวมความรู้พื้นฐานที่จำเป็นในการศึกษาทฤษฎีจำนวนเบื้องต้น
2. เพื่อให้ง่ายต่อการอ่านของนักเรียน นิสิต นักศึกษาและง่ายต่อผู้สอนที่จะนำตำราเล่มนี้ไป เพื่อใช้ในการสอน
3. เพื่อให้เหมาะสมสำหรับผู้สนใจในวงกว้าง ทั้งทางด้านคณิตศาสตร์บริสุทธิ์และคณิตศาสตร์ประยุกต์
4. เพื่อให้ผู้เรียนได้มีโอกาสพัฒนาทักษะทางด้านการพิสูจน์จากตัวแบบง่ายๆ
5. เพื่อให้ผู้เรียนได้มีโอกาสฝึกการแก้ปัญหาโจทย์ทางด้าน "การแก้ปัญหาทางทฤษฎีจำนวน" โดยมีการบรรจุแบบฝึกหัดในหลายระดับเรียงตามความยากง่าย

เพื่อให้ตำราเล่มนี้บรรลุตามวัตถุประสงค์ที่ได้ตั้งไว้ ผู้เขียนได้เริ่มต้นกล่าวถึงประวัติความเป็นมาของการศึกษาทฤษฎีจำนวนโดยเริ่มจากปีทาโกรัส (Pythagoras 569-500 ปีก่อนคริสต์ศักราช) ซึ่งนับเป็นเวลากว่า 2500 ปีแล้ว ทฤษฎีจำนวนนับว่าเป็นศาสตร์ในสาขาคณิตศาสตร์เก่าแก่ที่สุดและได้ถูกพัฒนาขึ้นมาเรื่อยๆ โดยนักคณิตศาสตร์แต่ละยุค แต่ละสมัย โดยนักคณิตศาสตร์รุ่นต่อๆ มา พยายามที่จะตอบปัญหาที่นักคณิตศาสตร์รุ่นก่อนๆ ยังไม่สามารถหาคำตอบได้ ความพยายามในการหาคำตอบของปัญหาก่อให้เกิดเทคนิคและแนวคิดใหม่ๆ อย่างไรก็ตามผู้อ่านจะได้พบว่าการพัฒนาเทคนิคและแนวคิดที่ได้รับการพัฒนาขึ้นมาก็ยังไม่เพียงพอที่จะตอบปัญหาได้ทุกๆ ปัญหาซึ่งผู้อ่านก็จะได้พบ "ข้อคาดเดา (Conjecture)" มากมายในการศึกษาทฤษฎีจำนวน

เนื้อหาทางด้านทฤษฎีจำนวนได้รับการนำไปประยุกต์ใช้ในด้านต่างๆ มากมายเช่น ทฤษฎีรหัส (Coding Theory), การพัฒนาของขั้นตอนวิธีในการสั่งงานของคอมพิวเตอร์, การกำหนดแถบรหัสสินค้า (Bar code) การกำหนดการออกชุดของเลขรหัสของบัตรเครดิตต่างๆ ตลอดจนใช้เป็นกฎเกณฑ์ในการออกบัตรประจำตัวประชาชนของบางประเทศ

ตำราทฤษฎีจำนวนเล่มนี้ได้บรรจุเนื้อหาที่เพียงพอในการใช้เป็นแนวทางในการสอนวิชาทฤษฎีจำนวนในทุกระดับ ตั้งแต่ระดับมัธยมศึกษาสำหรับนักเรียนที่มีความสามารถพิเศษ จนถึงระดับนิสิต-นักศึกษาในระดับปริญญาตรี ทั้งในส่วนเนื้อหาสาระที่กำหนดไว้เป็นขั้นตอนและวิวัฒนาการ เพื่อให้ผู้อ่านได้เห็นความพยายามของนักคณิตศาสตร์ในอดีต นอกจากนั้นเพื่อให้สอดคล้องกับยุคโลกาภิวัฒน์ ผู้เขียนยังได้รับรู้ข้อมูลข่าวสารที่ทันสมัยผ่านทาง website เช่น www.yahoo.com หรือ www.google.com โดนตระหนักถึงวิวัฒนาการที่รวดเร็วทางด้านคณิตศาสตร์และตระหนักถึงความทันสมัยของเนื้อหาวิชา ซึ่งเป็นที่ทราบดีว่าเมื่อตำราเล่มนี้ได้ถูกพิมพ์เผยแพร่และผู้อ่านทุกๆ ท่านเมื่อได้อ่านตำราเล่มนี้แล้วอาจพบว่าตำราเล่มนี้ขาดความทันสมัยในเนื้อหาสาระบางส่วน ดังนั้นเพื่อให้ตำราเล่มนี้ยังคงมีความทันสมัยในด้านเนื้อหาสาระ ผู้เขียนสนับสนุนให้ผู้อ่านได้ติดตามข้อมูลข่าวสารที่ทันสมัยได้จาก website ที่กำหนดข้างต้น

แบบฝึกหัดท้ายหัวข้อของแต่ละบทมีความสำคัญในการทำความเข้าใจในเนื้อหาที่ได้เรียนในแต่ละหัวข้อและแบบฝึกหัดท้ายบทก็มีความสำคัญในการตรวจสอบความเข้าใจในหัวข้อต่างๆ ในบทนั้นๆ แบบฝึกหัดมีความหลากหลายทั้งง่ายและยาก ผู้เขียนขอให้ผู้อ่านทุกท่านใช้ความพยายามในการทำแบบฝึกหัดเพื่อพัฒนาทางด้านความคิดและเป็นพื้นฐานที่ดีในการศึกษาคณิตศาสตร์ต่อไป

ISBN 974-92235-1-9

**สงวนลิขสิทธิ์**

จัดพิมพ์โดย มูลนิธิ สอวน.
พิมพ์ครั้งที่ 3 พ.ศ. 2552 (2009)
ออกแบบปก หน้ารองปกและหน้านำบทที่ 1 โดย ศาสตราจารย์ศักดา ศิริพันธุ์
ศิลปกรรม: นายปรีชา ฉัตระเนตร
พิมพ์ที่ บริษัทด่านสุทธาการพิมพ์ จำกัด
แยกสี / เพลท เอ็นอาร์ ฟิล์ม

**ที่ปรึกษา**
อาจารย์ไอศุริย สุดประเสริฐ
วท.ม. (คณิตศาสตร์) จุฬาลงกรณ์มหาวิทยาลัย

**ผู้เขียน**
รองศาสตราจารย์ ดร. ฉรงค์ ปิ้นนิ่ม
Ph.D. (Mathematics) University of The Philippines
ผู้ช่วยศาสตราจารย์ ดร. นิตติยา ปภาพจน์
กศ.ด. (คณิตศาสตร์ศึกษา) มหาวิทยาลัยศรีนครินทรวิโรฒ

# สารบัญ


## บทที่ 1 ความรู้เบื้องต้น

1.1 บทนำ 1
1.2 ระบบจำนวนเต็ม 6
1.3 หลักอุปนัยเชิงคณิตศาสตร์ 11
1.4 ข้อแนะนำบางประการเกี่ยวกับจำนวนเต็ม 16
โจทย์ปัญหาเสริมเรื่อง ความรู้เบื้องต้น 20
แบบฝึกหัดเรื่องความรู้เบื้องต้น 27

## บทที่ 2 การหารลงตัว

2.1 ขั้นตอนวิธีการหาร 29
2.2 นิยามการหารลงตัว 32
2.3 สมบัติเบื้องต้นของการหารลงตัว 34
2.4 ตัวหารร่วมมาก 36
2.5 ขั้นตอนวิธีแบบยุคลิด 41
2.6 ตัวคูณร่วมน้อย 44
โจทย์ปัญหาเสริมเรื่อง การหารลงตัว 48
แบบฝึกหัดเรื่องการหารลงตัว 55

## บทที่ 3 จำนวนเฉพาะ

3.1 นิยามของจำนวนเฉพาะ 57
3.2 ทฤษฎีบทหลักมูลของเลขคณิต 61
3.3 การค้นหาจำนวนเฉพาะ 65
โจทย์ปัญหาเสริมเรื่อง จำนวนเฉพาะ 68
แบบฝึกหัดเรื่องจำนวนเฉพาะ 71

## บทที่ 4 ข้อเท็จจริงบางประการเกี่ยวกับจำนวนเฉพาะ

4.1 ทฤษฎีบทสำคัญของจำนวนเฉพาะ 73
4.2 ข้อคาดเดาที่เกี่ยวข้องกับจำนวนเฉพาะ 79
4.3 จำนวนเฉพาะแฟร์มาต์ 82
4.4 จำนวนเฉพาะแมร์เซน 84
โจทย์ปัญหาเสริมเรื่อง ข้อเท็จจริงบางประการเกี่ยวกับจำนวนเฉพาะ 88
แบบฝึกหัดเรื่องข้อเท็จจริงบางประการเกี่ยวกับจำนวนเฉพาะ 91

## บทที่ 5 ฟังก์ชันเลขคณิต


5.1 ฟังก์ชันแยกคูณ 94
5.2 ฟังก์ชัน $\tau$ 98
5.3 ฟังก์ชัน $\sigma$ และ $\sigma_k$ 101
5.4 ฟังก์ชัน $\phi$ 106
5.5 ฟังก์ชัน $\mu$ 111
5.6 ฟังก์ชันจำนวนเต็มค่ามากสุด 115
โจทย์ปัญหาเสริมเรื่อง ฟังก์ชันเลขคณิต 121
แบบฝึกหัดเรื่องฟังก์ชันเลขคณิต 125


## บทที่ 6 คอนกรูเอนซ์


6.1 นิยามและสมบัติของคอนกรูเอนซ์ 128
6.2 สมการคอนกรูเอนซ์ 136
6.3 ทฤษฎีบทของแฟร์มาต์และออยเลอร์ 154
โจทย์ปัญหาเสริมเรื่อง คอนกรูเอนซ์ 161
แบบฝึกหัดเรื่องคอนกรูเอนซ์ 165


## บทที่ 7 สมการไดโอแฟนไทน์


7.1 บทนำ 169
7.2 สมการเชิงเส้นดีกรีหนึ่ง 170
7.3 สมการของปีทาโกรัส 178
7.4 สมการ $x^4 + y^4 = z^2$ และ $x^4 + y^4 = z^4$ 184
7.5 สมการไดโอแฟนไทน์กำลังสอง 186
โจทย์ปัญหาเสริมเรื่อง สมการไดโอแฟนไทน์ 193
แบบฝึกหัดเรื่องสมการไดโอแฟนไทน์ 195

**บรรณานุกรม** 197

**ดัชนี** 199

**บัญชีสัญลักษณ์** 202

ภาพหน้ารองปกจากหนังสือคำนวณเล่มแรก ของ ADAM RIESE พิมพ์ปี ค.ศ.1525

# บทที่ 1
# ความรู้เบื้องต้น

## 1.1 บทนำ

วิชาทฤษฎีจำนวน (เลขคณิตชั้นสูง) เป็นวิชาที่ศึกษาเกี่ยวกับสมบัติของจำนวนโดยเฉพาะอย่างยิ่งสมบัติของจำนวนเต็มและจำนวนนับ เนื่องจากจำนวนนับเป็นจำนวนชนิดแรกที่มนุษย์รู้จัก สมบัติต่าง ๆ ของจำนวนนับจึงเป็นสิ่งที่สนใจของมนุษย์ตลอดเวลาอันยาวนาน มีแง่มุมต่าง ๆ ที่มนุษย์ได้ศึกษาค้นคว้าไว้มากมายหลายแง่มุมและอาจกล่าวได้ว่าไม่มีวันที่จะจบสิ้นตราบที่มนุษย์ยังมีความคิด จินตนาการ และมีความยากรู้อยากเห็นในความมหัศจรรย์ของจำนวนเหล่านั้นอยู่ (สมใจ จิตพิทักษ์. 2545 : คำนำ) ซึ่งคำกล่าวนี้ได้สอดคล้องกับนักคณิตศาสตร์หลายท่านและอาจกล่าวว่าวิชาทฤษฎีจำนวนเป็นวิชาที่มีความสำคัญอย่างยิ่งวิชาหนึ่งจนได้รับการยกย่องจาก คาร์ล ฟรีดริช เกาส์ (Carl Friedrich Gauss ค.ศ. 1777 – 1855) ที่กล่าวว่า "*ทฤษฎีจำนวนเปรียบเสมือนเป็นราชินีแห่งคณิตศาสตร์ (Number Theory is the queen of mathematics)*" ธรรมชาติของวิชาทฤษฎีจำนวนนั้นง่ายต่อการเรียนรู้เพราะอาศัยความรู้เพียงน้อยนิดแต่พัฒนาความคิดได้หลากหลายและลึกซึ้ง และเป็นตัวแบบที่เปิดโอกาสให้ผู้เรียนได้ค้นพบความสำเร็จในการแก้ปัญหาด้วยตนเอง โดยเฉพาะอย่างยิ่งผู้เรียนที่มีความคิดสร้างสรรค์จะได้มีโอกาสแสดงความสามารถของตนเองออกมาในลักษณะการแก้ปัญหาต่าง ๆ ที่หลากหลายในวิชาทฤษฎีจำนวน

ทฤษฎีจำนวนเป็นสาขาหนึ่งที่เก่าแก่ที่สุดทางคณิตศาสตร์ เพราะถูกพัฒนามาตั้งแต่สมัยกรีกโบราณเมื่อประมาณ 2500 ปีมาแล้ว โดยพิจารณาจากหลักฐานที่ปรากฏในอดีต นักคณิตศาสตร์มีความเห็นว่าน่าจะเริ่มจากยุคของปีทาโกรัส (Pythagoras 569 – 500 ปีก่อนคริสต์ศักราช) และปัจจุบันยังได้รับการศึกษาค้นคว้าอีกมากมายจากทั้งนักคณิตศาสตร์มืออาชีพและมือสมัครเล่น ด้วยเหตุผลที่ว่าปัญหาทางทฤษฎีจำนวนนั้นชวนคิดและท้าทายความสามารถ มีความง่ายที่จะทำความเข้าใจประกอบกับปัญหาแต่ละปัญหาดูเหมือนว่ามีโอกาสหาคำตอบได้ นอกจากนี้ยังมีข้อคาดเดา (conjecture) และปัญหาที่ยังไม่สามารถหาคำตอบได้ (unsolved problems) อีกมากมายน่าสนใจจะศึกษา

โดยทั่วไปเป็นที่ยอมรับกันว่า ปีทาโกรัส และศิษย์เป็นผู้ริเริ่มในการพัฒนาจำนวน ปีทาโกรัสและศิษย์มีความเชื่อว่ากุญแจดอกสำคัญที่จะอธิบายสิ่งต่าง ๆ ในจักรวาลคือจำนวน แนวคิดของคนกลุ่มนี้ยึดปรัชญาว่า "ทุกสิ่งทุกอย่างคือจำนวน"

การศึกษาจำนวนในสมัยของปีทาโกรัส ได้นำความมหัศจรรย์ของจำนวนไปผูกพันกับความเชื่อโชคลางโหราศาสตร์และราศี เช่น **จำนวนมิตรภาพ** (*amicable numbers*) คู่แรก ที่เชื่อว่าพบในสมัยของปีทาโกรัส คือ 284 และ 220 สองจำนวนนี้มีสมบัติพิเศษ คือตัวหารแท้ของจำนวนหนึ่งมีผลบวกเท่ากับตัวหารแท้ของอีกจำนวนหนึ่ง กล่าวคือ ตัวหารแท้ของ 284 ได้แก่ 1, 2, 4, 71 และ 142 มีผลบวกเป็น 220 ตัวหารแท้ของ 220 ได้แก่ 1, 2, 4, 5, 10, 11, 20, 22, 44, 55 และ 110 มีผลบวกเป็น 284 ผู้ที่เชื่อโชคลางจะจารึกตัวเลขลงในเครื่องรางของขลัง โดยเชื่อว่าคนคู่ใดห้อยของขลังที่จารึกตัวเลขดังกล่าวจะเป็นมิตรแท้ต่อกัน ในปี ค.ศ. 1636 ปีแยร์ เดอ แฟร์มาต์ (Pierre De Fermat ค.ศ. 1601 – 1665) พบจำนวนมิตรภาพคู่ที่สองคือ 17,296 และ 18,416 ต่อมาในปี ค.ศ. 1638 เรอเน เดส์การ์ตส์ (René Descartes ค.ศ. 1596 – 1650) พบจำนวนมิตรภาพคู่ที่สามคือ 9,363,584 และ 9,437,056 จากนั้นในปี ค.ศ. 1747 เลออนฮาร์ด ออยเลอร์ (Leonhard Euler ค.ศ. 1707 – 1783) ได้เสนอจำนวนมิตรภาพถึง 64 คู่ แต่จากการตรวจสอบโดยนักคณิตศาสตร์รุ่นหลัง ปรากฏว่ามี 2 คู่ในจำนวน 64 คู่ ไม่ใช่จำนวนมิตรภาพ แต่ค้นพบหลังจากออยเลอร์ประกาศเกือบ 200 ปี ในปี ค.ศ. 1830 อาเดรียง มารี เลอจองด์ (Adrien Marie Legendre ค.ศ. 1752 – 1833) ได้พบคู่ใหม่อีก 1 คู่ คือ 2,172,649,216 และ 8,520,191 ในปี ค.ศ. 1866 เด็กชายนิโคโล ไปนินิ (Nicolo Painini) ชาวอิตาลีอายุ 16 ปี พบจำนวนมิตรภาพที่น้อยกว่าของแฟร์มาต์ คือ 1,184 และ 1,210 ต่อมาในปี ค.ศ. 1981 ฮิลตัน เชน (Hilton Chen) และเดล วูดส์ (Dale Woods) ได้พบจำนวนมิตรภาพที่มีขนาด อีกคู่หนึ่งโดยแต่ละจำนวนประกอบด้วย 50 หลัก คือ

21,741,269,040,875,890,083,566,772,572,567,935,979,368,836,363,843

และ 22,261,723,990,815,556,829,012,769,686,652,975,057,619,942,956,477

และในปัจจุบันโดยการใช้คอมพิวเตอร์ในการค้นหาจำนวนมิตรภาพ เราพบว่ามีทั้งหมด 6,262,871 คู่ (ข้อมูล ณ ปี ค.ศ. 2004)

อีกหนึ่งตัวอย่างที่เกี่ยวกับความเชื่อถือในความมหัศจรรย์ของจำนวน คือ **จำนวนสมบูรณ์** (*perfect number*) เป็นจำนวนที่มีสมบัติพิเศษ คือจำนวนนั้นมีค่าเท่ากับผลบวกของตัวหารแท้ทั้งหมดของจำนวนนั้น เช่น 6 เป็นจำนวนสมบูรณ์ เพราะมี 1, 2, 3 เป็นตัวหารแท้ และ $6 = 1 + 2 + 3$ ในสมัยนั้นเชื่อว่าพระเจ้าสร้างโลกและสร้างเสร็จภายใน 6 วัน ซึ่งเป็นจำนวนสมบูรณ์ จนถึงปี ค.ศ. 1952 มีการพบจำนวนสมบูรณ์รวม 12 จำนวน ทุกจำนวนเป็นจำนวนคู่ สามจำนวนแรกคือ 6, 28 และ 496 ต่อมาในปี ค.ศ. 2004 ได้มีการค้นพบจำนวนสมบูรณ์รวมทั้งสิ้น 40 จำนวน ซึ่งรายละเอียดของการค้นพบศึกษาได้ในบทที่ 4

การศึกษาเกี่ยวกับทฤษฎีจำนวนมีหลักฐานเด่นชัดในสมัยของกรีกประมาณ 300 ปีก่อน คริสต์ศักราช ปรากฏในหนังสืออิลิเมนต์ซึ่งเรียบเรียงโดย ยุคลิด แห่งอะเล็กซานเดรีย (Euclid of Alexandria ประมาณ 450 – 380 ก่อนคริสต์ศักราช) มี 13 เล่ม เล่มที่ 7, 8 และ 9 มีเรื่องราวเกี่ยวกับทฤษฎีจำนวน เนื้อหาที่รู้จักกันดีในปัจจุบันได้แก่ จำนวนเต็มคี่ จำนวนเต็มคู่ จำนวนเฉพาะ ทฤษฎีบทขั้นตอนวิธีแบบยุคลิด ตัวหารร่วมมาก ตัวคูณร่วมน้อย และทฤษฎีบทที่ว่าจำนวนเฉพาะมีจำนวนอนันต์ เป็นต้น (สมวงษ์ แปลงประสพโชค. 2537 : 3)

ความเฟื่องฟูของทฤษฎีจำนวนหลังจากยุคของยุคลิดได้หยุดชะงักไป จนกระทั่งปี ค.ศ. 250 มีนักคณิตศาสตร์ชาวกรีกชื่อ ดีโอฟานโตสแห่งอะเล็กซานเดรีย (Diophantos of Alexandria) ได้ตีพิมพ์หนังสือจำนวน 13 เล่ม โดยดีโอฟานโตสสามารถแก้สมการทางพีชคณิตที่มีตัวไม่ทราบค่าสองตัวหรือสามตัวได้และปัญหาของดีโอฟานโตสหลาย ๆ ปัญหากลายเป็นจุดเริ่มต้นของทฤษฎีจำนวน โดยเฉพาะอย่างยิ่งดีโอฟานโตสสนใจสมการพีชคณิตที่มีคำตอบเป็นจำนวนเต็ม ปัจจุบันเราเรียกสมการพีชคณิตที่มีคำตอบเป็นจำนวนเต็มนี้ว่า **สมการไดโอแฟนไทน์** (*Diophantine equation*) ตัวอย่างหนึ่งของสมการไดโอแฟนไทน์คือสมการสามจำนวนของปีทาโกรัส $x^2 + y^2 = z^2$ เป็นต้น

เมื่อสิ้นยุคของดีโอฟานโตสแล้วการพัฒนาทฤษฎีจำนวนมีเพียงเล็กน้อย มีหลักฐานแสดงถึงการพัฒนาทฤษฎีจำนวนในดินแดนแถบตะวันออกไกลในช่วงปี ค.ศ. 500 – 1200 โดยเฉพาะอย่างยิ่งในประเทศอินเดีย จนกระทั่งศตวรรษที่ 17 ทฤษฎีจำนวนได้กลับมาเจริญอีกครั้งในแถบยุโรปตะวันตกโดยมีนักคณิตศาสตร์ชาวฝรั่งเศสที่มีชื่อเสียงมาก คือ แฟร์มาต์ ซึ่งต่อมาได้รับการยกย่องให้เป็นบิดาของทฤษฎีจำนวนสมัยใหม่ แฟร์มาต์ได้ศึกษางานของดีโอฟานโตส และเป็นคนแรกที่ค้นพบสมบัติของจำนวนเต็มมากมาย

เมื่อหมดยุคของแฟร์มาต์ไม่นาน ก็มีนักคณิตศาสตร์ที่มีชื่อเสียงทางด้านทฤษฎีจำนวนเกิดขึ้นอีกหลายคน อาทิ ออยเลอร์ ชาวสวิส, โซแซฟ ลุยส์ ลากรองจ์ (Joseph Louis Lagrange ค.ศ. 1736 – 1813) ชาวฝรั่งเศส, ปีเตอร์ กุสตาฟ เลอเจิน เลอจองด์ ชาวฝรั่งเศส, เกาส์ ชาวเยอรมัน, ดีริชเลต์ (Peter Gustav Lejeune Dirichlet ค.ศ. 1805 – 1859) ชาวเยอรมัน ตำราทฤษฎีจำนวนเล่มแรกได้ตีพิมพ์ขึ้นโดยเลอจองด์ในปี ค.ศ. 1798 และอีกสามปีถัดมา เกาส์ก็ได้ตีพิมพ์หนังสือชื่อ Disquistiones Arithmeticae ซึ่งเป็นหนังสือเกี่ยวกับทฤษฎีจำนวนที่ได้ทำการพิสูจน์ทฤษฎีบทต่าง ๆ ไว้อย่างเป็นระบบ จากหนังสือเล่มนี้ของเกาส์ก่อให้เกิดประโยชน์ต่อคณิตศาสตร์ในสาขาอื่นเป็นอย่างมาก และตัวเกาส์เองก็ถือว่าหนังสือทฤษฎีจำนวนเล่มนี้เป็นผลงานอันยิ่งใหญ่ที่สุดของตน

จากประวัติของทฤษฎีจำนวนที่กล่าวมาทั้งหมดทำให้เราทราบถึงพัฒนาการตลอดจนนักคณิตศาสตร์ที่ยิ่งใหญ่และมีชื่อเสียงในด้านทฤษฎีจำนวน นักคณิตศาสตร์หลายท่านถือว่าทฤษฎีจำนวนเป็นรากฐานที่จะนำไปสู่การศึกษาคณิตศาสตร์สมัยใหม่หลายสาขาวิชา และในการศึกษาทฤษฎีจำนวนนั้น เราสามารถมองเห็นวิวัฒนาการต่าง ๆ เกี่ยวกับความพยายามของมนุษย์ที่จะตอบปัญหาต่าง ๆ ที่ยังไม่มีผู้ใดตอบได้ในอดีตดังตัวอย่างของปัญหาต่อไปนี้

ปัญหาเกี่ยวกับจำนวนเฉพาะ คือ จำนวนเฉพาะตัวที่ $n$ คือจำนวนอะไร ตัวอย่างเช่น จำนวนเฉพาะตัวที่ 10 คือ 29 จำนวนเฉพาะตัวที่ 100 คือ 541 จำนวนเฉพาะตัวที่ 664,999 คือ 10,006,721 สูตรทั่วไปในการหาจำนวนเฉพาะตัวที่ $n$ สำหรับ $n$ ทุกจำนวน ยังไม่เป็นที่ทราบกัน อีกปัญหาหนึ่งเกี่ยวกับจำนวนเฉพาะคือ มีสูตรใดบ้างที่ให้แต่จำนวนเฉพาะ เมื่อหลายศตวรรษมาแล้วมีความเชื่อกันว่า ถ้า $n$ เป็นจำนวนเต็มบวกแล้ว $n^2 + n + 41$ เป็นจำนวนเฉพาะ สูตรนี้เป็นจริงสำหรับ $n = 0, 1, 2, \ldots, 39$ ซึ่งให้จำนวนเฉพาะติดต่อกัน 40 จำนวน แต่ไม่เป็นจริงสำหรับ $n = 40$ และ $n = 41$ (ทั้งสองกรณีมี 41 เป็นตัวประกอบร่วม) สูตรอีกสูตรหนึ่งที่ให้จำนวนเฉพาะติดต่อกันถึง 80 จำนวนคือ $n^2 - 79n + 1601$

เราสามารถพิสูจน์ต่อไปได้ว่าไม่มีพหุนามใด ๆ ที่ให้แต่จำนวนเฉพาะ แฟร์มาต์ได้เสนอว่า $F_n = 2^{2^n} + 1$ เป็นจำนวนเฉพาะ สำหรับทุก ๆ จำนวนเต็ม $n \geq 0$ เขาได้ตรวจสอบข้อเสนอของเขาสำหรับ $n = 0, 1, 2, 3, 4$ และพบว่า $F_n$ คือ 3, 5, 17, 257, 65537 ตามลำดับ ซึ่งเป็นจำนวนเฉพาะ สำหรับ $n = 5$ จะได้ $F_5 = 4{,}294{,}967{,}297$ แฟร์มาต์ไม่ได้ตรวจสอบข้อเสนอของเขา จนกระทั่งในปี ค.ศ. 1732 ออยเลอร์ได้พิสูจน์ว่า $641 \mid F_5$ ดังนั้น $F_5$ ไม่เป็นจำนวนเฉพาะ ยังไม่เป็นที่ทราบกับว่าเมื่อ $n > 4$ มี $F_n$ ตัวใดเป็นจำนวนเฉพาะอีกบ้าง จำนวนที่อยู่ในรูป $2^{2^n} + 1$ มีชื่อเรียกว่า **จำนวนแฟร์มาต์** (*Fermat number*) ในกรณีที่เป็นจำนวนเฉพาะเรียกว่า **จำนวนเฉพาะแฟร์มาต์** (*Fermat prime*)

ปัญหาเกี่ยวกับจำนวนเฉพาะอีกปัญหาหนึ่งคือ มีจำนวนเฉพาะกี่จำนวนที่น้อยกว่าหรือเท่ากับจำนวนเต็มบวก $n$ ที่กำหนดให้ ต่อมาเกาส์ได้เสนอว่าคำตอบที่ใกล้เคียงคือ

$$\frac{n}{1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}}$$

อัตราส่วนของจำนวนนี้กับจำนวนของจำนวนเฉพาะที่น้อยกว่าหรือเท่ากับ $n$ จะเข้าใกล้ 1 เมื่อ $n$ มีค่ามาก ๆ ทฤษฎีบทนี้มีชื่อรู้จักกันโดยทั่วไปว่า "*ทฤษฎีบทของจำนวนเฉพาะ* (*Prime number theorem*)" ทฤษฎีบทนี้ อาดามาด์ (J. S. Hadamard ค.ศ. $1865-1963$) และ ปูแซง (C. V. Poussin ค.ศ. $1866-1962$) พิสูจน์ได้ในปี ค.ศ. 1896 โดยใช้สมบัติของฟังก์ชันซีตา (zeta function) ในวิชา**ทฤษฎีฟังก์ชันเชิงซ้อน** (*Complex Function Theory*) ต่อมาในปี ค.ศ. 1949 อาเทิล เซลเบิร์ก (Atle Selberg) และ พอล เออดอส (Paul Erdös ค.ศ. $1913-1996$) พิสูจน์ได้อีกทางหนึ่งโดยใช้ทฤษฎีบททางเลขคณิตซึ่งก็ยากและซับซ้อนมาก

ถ้าให้จำนวนใด ๆ มา เราจะบอกได้อย่างไรว่าจำนวนนั้นเป็นจำนวนเฉพาะหรือไม่ ในปัจจุบันยังไม่มีสูตรทั่วไปที่จะตอบคำถามนี้ บางครั้งเราอาจลองผิดลองถูก หาตัวประกอบของจำนวนดังกล่าว แล้วสรุปว่าเป็นจำนวนประกอบ แต่ถ้ามีเลข 20 หลัก ตัวอย่างเช่น

$$32{,}598{,}158{,}477{,}190{,}044{,}731$$

ถ้าถามว่า ตัวเลข 20 หลักดังกล่าวนี้เป็นจำนวนเฉพาะหรือไม่ จะทดสอบได้อย่างไร มีวิธีการทางทฤษฎีบทบางวิธีที่จะตอบคำถามนี้ แต่ใช้ได้ไม่สะดวกอย่างยิ่งในทางปฏิบัติ ตัวอย่างเช่น มีทฤษฎีบทที่ว่าจำนวนเต็มบวก $n$ เป็นจำนวนเฉพาะก็ต่อเมื่อ $n \mid [(n-1)!+1]$

ตัวอย่างเช่น $5 \mid [4!+1]$ ดังนั้น 5 เป็นจำนวนเฉพาะ

$6 \nmid [5!+1]$ ดังนั้น 6 ไม่เป็นจำนวนเฉพาะ

ทฤษฎีบทเหล่านี้น่าสนใจแต่ก็ใช้ประโยชน์อะไรได้ไม่มากนัก เช่น ในการตรวจสอบเลข 20 หลักข้างต้นว่าเป็นจำนวนเฉพาะหรือไม่

มีปัญหาหลายปัญหาที่อยู่ในแวดวงของจำนวนเฉพาะ เช่น **จำนวนเฉพาะคู่แฝด** (*twin prime*) มีได้ไม่จำกัดจำนวนหรือไม่ จำนวนเฉพาะคู่แฝดคือคู่ของจำนวนเต็มบวก $p$ และ $p+2$ ซึ่งต่างเป็นจำนวนเฉพาะ ตัวอย่างเช่น 5 และ 7, 11 และ 13, 17 และ 19, 29 และ 31, 10,006,427 และ 10,006,429 เป็นต้น (สมใจ จิตพิทักษ์. 2545 : $3-4$) จากการใช้เครื่องคอมพิวเตอร์พบว่า มีจำนวนเฉพาะคู่แฝดที่น้อยกว่า 30,000,000 อยู่ทั้งหมด 152,892 คู่ และจำนวนเฉพาะคู่แฝดที่อยู่ระหว่าง 999,999,990,000 และ 1,000,000,000,000 มี 15 คู่ และระหว่าง 1,000,000,000,000 และ 1,000,000,010,000 มี 20 คู่ คู่หนึ่งในจำนวนนี้คือ 1,000,000,000,061 และ 1,000,000,000,063 ในปี ค.ศ. 1989 มีผู้ค้นพบจำนวนเฉพาะคู่หนึ่งคือ $1706595 \cdot 2^{11235} \pm 1$ โดยที่แต่ละจำนวนประกอบด้วยเลขโดด 3,389 หลัก

จำนวนเฉพาะที่อยู่ในรูป $2^p-1$ โดยที่ $p$ เป็นจำนวนเฉพาะมีได้ไม่จำกัดจำนวนหรือไม่ ตั้งแต่ก่อนคริสตกาลจนถึง ค.ศ. 2004 จำนวนเฉพาะในรูปดังกล่าวเพิ่งทราบเพียง 40 จำนวนเท่านั้น จำนวนเฉพาะในรูป $2^p-1$ มีชื่อเรียกว่า **จำนวนเฉพาะแมร์เซน** (*Mersenne prime*) ที่กล่าวมานี้เป็นเพียงแง่มุมหนึ่งของจุดสนใจในวิชาทฤษฎีจำนวนเท่านั้น

ตัวอย่างต่อไปเป็นตัวอย่างของปัญหาการบวกซึ่งเกี่ยวข้องกับจำนวนเฉพาะ คือ **ข้อคาดเดาของโกลด์บาค** (*Goldbach's conjectures*) ซึ่งคริสเตียน โกลด์บาค (Cristian Goldbach ค.ศ. $1690-1764$) ได้เสนอในปี ค.ศ. 1742 ว่า จำนวนคู่ทุก ๆ จำนวนที่มากกว่า 4 สามารถเขียนเป็นผลบวกของจำนวนเฉพาะคี่ 2 จำนวนได้ และจำนวนคี่ทุกจำนวนที่มากกว่า 7 สามารถเขียนเป็นผลบวกของจำนวนเฉพาะคี่ทุกจำนวนได้ ตัวอย่างเช่น

$$6 = 3+3,\ 8 = 5+3,\ 12 = 7+5,\ 20 = 13+7 = 17+3$$

ปิพปิง (N. Pipping) ได้ตรวจสอบข้อเสนอนี้สำหรับจำนวนเต็มคู่จนถึง 100,000 ต่อมามีการตรวจสอบว่าเป็นจริง สำหรับจำนวนเต็มคู่ทุกจำนวนที่น้อยกว่า $10^{10}$ แต่การพิสูจน์ว่าข้อเสนอนี้เป็นจริงสำหรับจำนวนเต็มคู่ทุก ๆ

จำนวนที่มากกว่า 4 ยังไม่มีผู้ใดทราบ ในปี ค.ศ. 1922 ฮาร์ดี (G. H. Hardy ค.ศ. 1877 – 1947) ได้กล่าวถึงข้อคาดเดาของโกลด์บาคว่า บางทีมันอาจยากจนไม่สามารถหาคำตอบได้ แต่ถ้าข้อคาดเดานี้เป็นจริงแล้วจะกล่าวได้ว่าทุก ๆ จำนวนเต็มคี่ที่มากกว่า 7 สามารถเขียนได้ในรูปผลบวกของจำนวนเฉพาะคี่ 3 จำนวนได้ ต่อมาในปี ค.ศ. 1937 นักคณิตศาสตร์ชาวรัสเซียชื่อ วิโนกราดอฟ (I. M. Vinogradov) ได้พิสูจน์ว่าจะมีจำนวนเต็มบวก $K$ ที่ทำให้ทุก ๆ จำนวนเต็มคี่ $N$ ซึ่ง $N > K$ แล้ว $N$ สามารถเขียนได้ในรูปผลบวกของจำนวนเฉพาะคี่ 3 จำนวนได้ แต่เขาก็ไม่สามารถบอกได้ว่า $K$ ควรมีขนาดเท่าใด แต่ในปี ค.ศ. 1956 บอรอซคิน (Borozdkin) พิสูจน์ว่า $K < 3^{3^{15}}$ จนมาถึง ค.ศ. 1988 มีการตรวจสอบโดยใช้คอมพิวเตอร์พบว่า $K < 10^{400,000}$

หัวข้อสำคัญที่อยู่ในจุดสนใจอีกเรื่องหนึ่งนอกเหนือจากปัญหาเกี่ยวกับจำนวนเฉพาะหรือปัญหาเกี่ยวกับการบวก ซึ่งเป็นปัญหาที่ยอมรับว่าเป็นปัญหาที่ยากที่สุดปัญหาหนึ่งคือ *"ทฤษฎีบทสุดท้ายของแฟร์มาต์ (Fermat's last theorem)"* ในปี ค.ศ. 1637 แฟร์มาต์ได้เขียนเป็นบทสรุปในบันทึกส่วนตัวของเขาว่า เขาได้ค้นพบบทพิสูจน์ของทฤษฎีบทที่ว่า "สมการ $x^n + y^n = z^n$ ไม่มีคำตอบ $x, y, z$ ที่เป็นจำนวนเต็มบวก สำหรับทุก ๆ ค่าของจำนวนเต็มบวก $n$ ที่ $n \geq 3$" แต่เขาไม่ได้แสดงบทพิสูจน์ไว้โดยอ้างว่าเนื้อที่ที่เหลือในบันทึกนั้นไม่พอที่จะเขียนบทพิสูจน์ แต่แฟร์มาต์ได้พิสูจน์เพียงว่าทฤษฎีบทของเขาเป็นจริงกรณี $n = 4$ ในปี ค.ศ. 1770 ออยเลอร์พิสูจน์ว่าทฤษฎีบทนี้เป็นจริงสำหรับ $n = 3$ ซึ่งการพิสูจน์ของเขายังมีส่วนบกพร่องอยู่แต่นักคณิตศาสตร์รุ่นต่อมาได้แก้ไขให้ถูกต้องสมบูรณ์ สำหรับ $n = 5$ ดีริชเลต์และเลอจองด์ พิสูจน์ได้ในปี ค.ศ. 1825 กรณี $n = 6$ ใช้ผลจากกรณี $n = 3$ สำหรับกรณี $n = 7$ กาเบรียล เลม (Gabriel Lamé ค.ศ. 1795 – 1870) พิสูจน์ได้ในปี ค.ศ. 1839 ต่อมาในปี ค.ศ. 1857 คุมเมอร์ (E. E. Kummer ค.ศ. 1810 – 1893) นักคณิตศาสตร์ชาวเยอรมัน พิสูจน์ได้ว่าทฤษฎีบทนี้เป็นจริงสำหรับ $n$ ที่น้อยกว่า 100 เป็นเวลากว่า 300 ปีที่แฟร์มาต์ได้เสนอทฤษฎีบทของเขา จนกระทั่งได้มีการตรวจสอบสำหรับ $n$ ที่มีค่ามาก ๆ แต่การพิสูจน์ "ทฤษฎีบท" นี้ว่าเป็นจริงสำหรับทุก ๆ $n \geq 3$ ยังไม่เป็นที่ทราบกัน จนกระทั่งในปี ค.ศ. 1993 เมื่อแอนดรู ไวลส์ (Andrew Wiles ค.ศ. 1953 - ) นักคณิตศาสตร์ชาวอังกฤษได้ประกาศต่อสาธารณชนว่าเขาสามารถพิสูจน์ทฤษฎีบทสุดท้ายของแฟร์มาต์ได้ โดยการจัดบรรยายอย่างต่อเนื่องในวันที่ 21 – 23 ของเดือนมิถุนายน ค.ศ. 1993 ที่ Newton Institute ในเมืองเคมบริดจ์ ประเทศอังกฤษ ไวลส์ได้ตรวจสอบบทพิสูจน์พร้อมกับคณะทำงานจนกระทั่งเดือนธันวาคมในปีเดียวกัน เขาพบข้อบกพร่องของบทพิสูจน์บางประการ เขาและเทย์เลอร์ (R. Taylor) จึงต้องเติมในส่วนที่บกพร่องให้ชัดเจนและถูกต้อง และที่สุดงานของเขาก็สำเร็จลุล่วงได้ในช่วงเดือนกันยายนปี ค.ศ. 1994 (ณรงค์ ปั้นนิ่ม. 2545 : 1 – 2)

ถึงตอนนี้อาจมีคำถามว่า เราจะศึกษาวิชานี้ไปเพื่ออะไรและมีประโยชน์ด้านใดบ้าง ก่อนจะตอบคำถามนี้ได้จะต้องศึกษารายละเอียดของวิชานี้เสียก่อน เพราะว่าทฤษฎีจำนวนไม่ใช่เพียงแต่ศึกษาเฉพาะสมบัติและการพิสูจน์ข้อความที่เกี่ยวข้องกับจำนวนนับและจำนวนเต็มเท่านั้น ส่วนหนึ่งของวิชาทฤษฎีจำนวนที่ไม่ค่อยได้ปรากฏในหนังสือก็คือการแก้ปัญหาฉงน (Puzzles) ต่าง ๆ เกี่ยวกับตัวเลข เช่น Games with digits, Magic square, Number puzzles เป็นต้น ซึ่งปัญหาส่วนนี้จะสามารถพัฒนาความคิดความสามารถในการแก้ปัญหาอย่างสร้างสรรค์ได้เป็นอย่างดี

## 1.2 ระบบจำนวนเต็ม

ในการศึกษาทฤษฎีจำนวนเบื้องต้นนั้น เราจะมุ่งเน้นการศึกษาสมบัติของจำนวนนับและจำนวนเต็ม ตลอดจนการพิสูจน์ข้อความที่เกี่ยวข้องกับจำนวนนับและจำนวนเต็ม นอกจากนั้นเรายังมุ่งเน้นให้ผู้เรียนได้เห็นวิวัฒนาการและความสวยงามของระบบจำนวนดังกล่าว และยังให้ผู้เรียนได้นำความรู้ที่ได้รับจากการศึกษาทฤษฎีจำนวนเพื่อเป็นพื้นฐานในการเรียนคณิตศาสตร์ชั้นสูงต่อไป

เพื่อให้บรรลุถึงวัตถุประสงค์ดังกล่าวข้างต้น เนื้อหาในบทนี้จะประกอบด้วยสมบัติพื้นฐานของจำนวนเต็มบางส่วนที่เพียงพอในการนำไปอ้างอิงเมื่อมีการพิสูจน์ทฤษฎีบท และเพื่อทำให้การพิสูจน์ทฤษฎีบทต่าง ๆ เป็นไปตามวิธีการทางคณิตศาสตร์

ในหัวข้อนี้จะกล่าวถึง ระบบจำนวนเต็ม ซึ่งเป็นระบบที่เราสามารถศึกษาสมบัติได้มากมาย และเอกภพสัมพัทธ์ที่เราจะอ้างถึงคือ เซตของจำนวนเต็ม $\mathbb{Z}$ โดยที่

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

**ระบบจำนวนเต็ม**คือระบบที่ประกอบด้วยเซตของจำนวนเต็ม $\mathbb{Z}$ พร้อมด้วยการดำเนินการ "$+$" และ "$\cdot$" ที่สอดคล้องกับสัจพจน์ที่แบ่งได้ 3 กลุ่ม ดังนี้

กลุ่มที่ 1 สมบัติทางพีชคณิต (algebraic property)
กลุ่มที่ 2 สมบัติไตรวิภาค (trichotomy law)
กลุ่มที่ 3 หลักการจัดอันดับดี (well ordering principle)

นั่นคือ ระบบจำนวนเต็มเป็นระบบเชิงสัจพจน์ระบบหนึ่งซึ่งประกอบด้วย เซตของจำนวนเต็ม $\mathbb{Z}$ และการดำเนินการ $+$ และ $\cdot$ ที่สอดคล้องสมบัติ $\mathbf{P}_1$ ถึง $\mathbf{P}_8$ ที่จะได้กล่าวต่อไป เราสามารถนำสัจพจน์ $\mathbf{P}_1$ ถึง $\mathbf{P}_8$ ข้อใดหรือหลายข้อใดไปอ้างในการพิสูจน์ข้อเท็จจริงต่าง ๆ ที่เกี่ยวข้องกับระบบจำนวนเต็ม ข้อเท็จจริงที่ได้จากการนำสัจพจน์เหล่านี้ไปอ้าง เราเรียกว่า **ทฤษฎีบท** ทฤษฎีบทบางทฤษฎีบทอาจเป็นผลสืบเนื่องโดยตรงจากสัจพจน์หรืออาจเป็นผลสืบเนื่องมาจากสัจพจน์กับทฤษฎีบทที่ได้ผ่านการพิสูจน์มาแล้วก็ได้ และทฤษฎีบทบางทฤษฎีบทอาจเป็นผลสืบเนื่องมาจากสัจพจน์ ทฤษฎีบทที่ได้ผ่านการพิสูจน์มาแล้วและบทนิยามที่ตั้งขึ้นมาใหม่นั้น จะต้องไม่มีความขัดแย้งกันในระบบ

### สมบัติทางพีชคณิต (Algebraic properties)

$\mathbf{P}_1$ : *สมบัติการปิด* (*closure laws*)

สำหรับการบวก : ทุก ๆ $a, b \in \mathbb{Z}$ จะมี $c \in \mathbb{Z}$ เพียงตัวเดียวเท่านั้น ที่ทำให้ $a + b = c$

สำหรับการคูณ : ทุก ๆ $a, b \in \mathbb{Z}$ จะมี $c \in \mathbb{Z}$ เพียงตัวเดียวเท่านั้น ที่ทำให้ $a \cdot b = c$

$\mathbf{P}_2$ : *สมบัติการเปลี่ยนกลุ่ม* (*associative laws*)

สำหรับการบวก : ถ้า $a, b, c \in \mathbb{Z}$ แล้ว $(a + b) + c = a + (b + c)$

สำหรับการคูณ : ถ้า $a, b, c \in \mathbb{Z}$ แล้ว $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

$\mathbf{P_3}$ : *สมบัติการมีเอกลักษณ์* $(existence\ \ of\ \ identities)$

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

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

$\mathbf{P_4}$ : *สมบัติการมีอินเวอร์สการบวก* $(existence\ \ of\ \ additive\ \ inverse)$

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

$\mathbf{P_5}$ : *สมบัติการสลับที่* $(commutative\ \ laws)$

สำหรับการบวก : ถ้า $a, b \in \mathbb{Z}$ แล้ว $a + b = b + a$

สำหรับการคูณ : ถ้า $a, b \in \mathbb{Z}$ แล้ว $a \cdot b = b \cdot a$

$\mathbf{P_6}$ : *สมบัติการกระจาย* $(distributive\ \ law)$

ถ้า $a, b, c \in \mathbb{Z}$ แล้ว

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{และ} \quad (a + b) \cdot c = a \cdot c + b \cdot c$$

**ข้อตกลง** เราจะใช้สัญลักษณ์ $\langle \mathbb{Z}, +, \cdot \rangle$ แทนระบบจำนวนเต็ม และเราจะเขียน $ab$ แทน $a \cdot b$ และ $a - b$ แทน $a + (-b)$

จากระบบจำนวนเต็มพร้อมด้วยสมบัติ 6 ข้อที่กล่าวข้างต้น เราอาจนำไปพิสูจน์หรือให้เหตุผลต่อความจริงดังทฤษฎีบทต่อไปนี้

**ทฤษฎีบท 1.2.1** ข้อความต่อไปนี้เป็นจริง

1. ในระบบจำนวนเต็มจะมี 0 เพียงตัวเดียวเท่านั้นที่เป็นสมาชิกเอกลักษณ์ของการบวก
2. ในระบบจำนวนเต็มจะมี 1 เพียงตัวเดียวเท่านั้นที่เป็นสมาชิกเอกลักษณ์ของการคูณ
3. สำหรับจำนวนเต็ม $a$ ใด ๆ $a0 = 0a = 0$
4. ถ้า $a, b, c \in \mathbb{Z}$ และ $a + b = a + c$ แล้ว $b = c$

**บทพิสูจน์**

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

**ทฤษฎีบท 1.2.2** ข้อความต่อไปนี้เป็นจริง

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

**บทพิสูจน์** 1. สมมติว่ามี $b \in \mathbb{Z}$ ซึ่ง $a + b = b + a = 0$ สำหรับจำนวนเต็ม $a$ ใด ๆ

ดังนั้น $b = b + 0 = b + [a + (-a)]$

$= (b + a) + (-a) = 0 + (-a) = -a$

นั่นคือ $b = -a$

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

ดังนั้น $-(-a) = a$

นั่นคือ อินเวอร์สการบวกของ $-a$ คือ $a$

3. ให้ $a, b \in \mathbb{Z}$ จะได้ว่า

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

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

นั่นคือ $(-a)b = a(-b)$

พิสูจน์ในทำนองเดียวกันจะได้ว่า $(-a)b = -(ab)$

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

เนื่องจาก $-(-a)(-b) = (-a)b$

ดังนั้น $(-a)(-b) = ab$ ■

## สมบัติไตรวิภาค (Trichotomy law)

**$P_7$ : สมบัติไตรวิภาค**

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

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

สมบัติไตรวิภาคนี้มีประโยชน์ในการกำหนดนิยามเพื่อเปรียบเทียบสมาชิก 2 ตัวใด ๆ ใน $\mathbb{Z}$ ในแง่ "มากกว่า" หรือ "น้อยกว่า" กล่าวคือ

**บทนิยาม 1.2.3** ให้ $a, b \in \mathbb{Z}$ เรากล่าวว่า

$a$ **มากกว่า** $b$ เขียนแทนด้วย $a > b$ ก็ต่อเมื่อ $a - b \in \mathbb{N}$ และ

$a$ **น้อยกว่า** $b$ เขียนแทนด้วย $a < b$ ก็ต่อเมื่อ $b > a$

**ทฤษฎีบท 1.2.4** ให้ $a, b, c, x, b \in \mathbb{Z}$ 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 $ax < bx$

**บทพิสูจน์** 1. เพราะว่า $(a + c) - (b + c) = a - b \in \mathbb{N}$ ดังนั้น $a + c > b + c$

สำหรับการพิสูจน์ในข้ออื่น ๆ สามารถกระทำได้โดยการใช้สมบัติไตรวิภาคของระบบจำนวนเต็ม จึงขอละไว้เพื่อเป็นแบบฝึกหัด ■

**ทฤษฎีบท 1.2.5** ให้ $a, b, c, x, b \in \mathbb{Z}$ 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 $ax > bx$

**บทพิสูจน์** ขอให้ผู้เรียนพิสูจน์เป็นแบบฝึกหัด ■

ทฤษฎีบทต่อไปจะแสดงว่าระบบจำนวนเต็มจะมีเซตที่สอดคล้องกับสัจพจน์ $\mathbf{P}_7$ เพียงเซตเดียวเท่านั้น คือ $\mathbb{N} = \{1, 2, 3, \ldots\}$ นั่นคือ จากบทนิยามการเปรียบเทียบสมาชิกใน $\mathbb{Z}$ ในแง่ "มากกว่า" หรือ "น้อยกว่า" ซึ่งเราสามารถเปรียบเทียบได้เพียงแบบเดียวเท่านั้น

**ทฤษฎีบท 1.2.6** $\mathbb{Z}$ มีเพียงสับเซตเดียวเท่านั้นคือ $\mathbb{N}$ ที่สอดคล้องกับสมบัติไตรวิภาค

**บทพิสูจน์** สมมติว่า $S \subseteq \mathbb{Z}$ ที่สอดคล้องกับสมบัติไตรวิภาค จะได้ว่า $1 \in S$ หรือ $-1 \in S$

ถ้า $-1 \in S$ จะได้ว่า $(-1)(-1) = 1 \in S$ และ $1 + (-1) = 0 \in S$ ซึ่งเป็นไปไม่ได้ขัดแย้งกับ $0 \notin S$ ดังนั้น $1 \in S$

ให้ $n \in \mathbb{N}$ จะได้ว่า $n = 1 + 1 + 1 + \cdots + 1$ ($n$ ตัว)

ดังนั้น $n \in S$ แสดงว่า $\mathbb{N} \subseteq S$ นั่นคือ $S = \mathbb{N}$ หรือ $S \setminus \mathbb{N} \neq \varnothing$

สมมติว่า $S \setminus \mathbb{N} \neq \varnothing$ จะได้ว่ามี $x \in S$ แต่ $x \notin \mathbb{N}$

ดังนั้น $x \neq 0$ นั่นคือ $-x \in \mathbb{N}$ จาก $x \in S$ และ $-x \in \mathbb{N} \subseteq S$

แสดงว่า $x + (-x) = 0 \in S$ ซึ่งเป็นไปไม่ได้จึงเกิดข้อขัดแย้ง ดังนั้น $S = \mathbb{N}$ ■

**ทฤษฎีบท 1.2.7** ให้ $a, b \in \mathbb{Z}$
ถ้า $ab = 0$ แล้ว $a = 0$ หรือ $b = 0$

**บทพิสูจน์** ถ้า $a \neq 0$ และ $b \neq 0$ จากสมบัติไตรวิภาคจะได้ว่า $a \in \mathbb{N}$ หรือ $-a \in \mathbb{N}$
และ $b \in \mathbb{N}$ หรือ $-b \in \mathbb{N}$ ดังนั้น $ab \in \mathbb{N}$ หรือ $-(ab) \in \mathbb{N}$
นั่นคือ $ab \neq 0$ ■

**บทแทรก 1.2.8** ให้ $a, b, c \in \mathbb{Z}$
ถ้า $ab = ac$ และ $a \neq 0$ แล้ว $b = c$

**บทพิสูจน์** สมมติว่า $ab = ac$ และ $a \neq 0$ จะได้ว่า $ab - ac = a(b - c) = 0$
ดังนั้น $b - c = 0$ นั่นคือ $b = c$ ■

จากทฤษฎีบท 1.2.7 และบทแทรก 1.2.8 ข้างต้น เราพบว่า สมบัติการตัดออกสำหรับการคูณ หรือ สมบัติการ**ไม่มีตัวหารศูนย์แท้** (no proper zero divisor) ในระบบจำนวนเต็ม เป็นผลสืบเนื่องมาจากสัจพจน์ $\mathbf{P}_1$ ถึง $\mathbf{P}_6$

## หลักการจัดอันดับดี

เพื่อให้การศึกษาสมบัติของจำนวนเต็มมีประสิทธิภาพมากขึ้นและเพื่อการพิสูจน์ข้อความต่าง ๆ ที่เกี่ยวข้องกับจำนวนเต็มมีความสมเหตุสมผลมากขึ้น เราจึงขอกำหนดว่าเซตของจำนวนเต็มบวกมีสมบัติหลักการจัดอันดับดี กล่าวคือ

## หลักการจัดอันดับดี (Well ordering principle)

$\mathbf{P}_8$ : ให้ $S \subseteq \mathbb{N}$ และ $S \neq \varnothing$ จะได้ว่า
มี $x \in S$ ซึ่ง $x \leq a$ สำหรับทุก $a \in S$

สมบัติของการจัดอันดับดีในระบบจำนวนเต็ม นำไปสู่ทฤษฎีบทที่น่าสนใจ ซึ่งสามารถนำไปประยุกต์ใช้ในการพิสูจน์ทฤษฎีบทต่าง ๆ ที่จะได้กล่าวถึงในบทต่อ ๆ ไป

**ทฤษฎีบท 1.2.9** ไม่มีจำนวนเต็มใดอยู่ระหว่าง 0 และ 1

**บทพิสูจน์** ให้ $T = \{a \in \mathbb{Z} \mid 0 < a < 1\}$ และสมมติว่า $T \neq \varnothing$
จากหลักการจัดอันดับดี จะได้ว่ามี $m \in T$ ซึ่ง $m \leq x$ สำหรับทุก $x \in T$
ดังนั้น $0 < m < 1$ นั่นคือ $0 < m^2 < m$ แสดงว่า $m^2 \in T$
จึงเกิดข้อขัดแย้งในการเลือก $m$ ที่เป็นจำนวนเต็มบวกที่น้อยที่สุดใน $T$
นั่นคือ $T = \varnothing$ ■

**ทฤษฎีบท 1.2.10** *สมบัติของอาร์คีมิดีส* (*Archimedean property*)
สำหรับจำนวนเต็มบวก $a$ และ $b$ จะมีจำนวนเต็มบวก $n$ ซึ่ง $na \geq b$

**บทพิสูจน์** 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 $S \neq \varnothing$
จากหลักการจัดอันดับดี จะมี $k \in \mathbb{N}$ ซึ่ง $m = b - ka$ ที่ $m$ เป็นจำนวนเต็มบวกที่น้อยที่สุดใน $S$
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 $S$ ■

หลักการจัดลำดับดียังนำไปสู่ทฤษฎีบทที่สำคัญที่ใช้เพื่อพิสูจน์ข้อความต่าง ๆ ที่เกี่ยวข้องกับจำนวนเต็มบวก เรียกทฤษฎีบทนี้ว่า "*หลักอุปนัยเชิงคณิตศาสตร์*" (*Principle of Mathematical Induction*)

**ทฤษฎีบท 1.2.11** ให้ $S \subseteq \mathbb{N}$ จะได้ว่า $\mathbb{N} = S$ ก็ต่อเมื่อ
(1) $1 \in S$ และ
(2) ถ้า $n \in S$ แล้ว $n + 1 \in S$

**บทพิสูจน์** ให้ $S = \mathbb{N}$ เห็นได้ชัดว่า (1) และ (2) เป็นจริง
สมมติว่า (1) และ (2) เป็นจริง และ $\mathbb{N} \setminus S \neq \varnothing$ โดยหลักการจัดอันดับดี จะมี $m \in \mathbb{N} \setminus S$ ซึ่ง $m$ เป็นจำนวนเต็มบวกที่น้อยที่สุดใน $\mathbb{N} \setminus S$ เพราะว่า $m - 1 < m$
ดังนั้น $m - 1 \notin \mathbb{N} \setminus S$
จาก $1 \in S$ แสดงว่า $m > 1$ ดังนั้น $m - 1 \in \mathbb{N}$
จากการเลือก $m$ เราพบว่า $m - 1 \in S$ และจาก (2) จะได้ว่า
$m = (m-1) + 1 \in S$ ซึ่งเป็นไปไม่ได้เกิดข้อขัดแย้งที่ว่า $m \notin S$
ดังนั้น $\mathbb{N} = S$ ■

## 1.3 หลักอุปนัยเชิงคณิตศาสตร์

ในการพิสูจน์หรือการให้เหตุผลทางทฤษฎีจำนวนนั้น หลักการพื้นฐานที่สำคัญมีอยู่ 2 ประการ คือ

1. ทุกสับเซตของ $\mathbb{N}$ จะมีสมาชิกตัวน้อยที่สุด ซึ่งหลักการนี้ได้กล่าวไว้แล้วในหลักการจัดอันดับดีข้างต้น
2. หลักอุปนัยเชิงคณิตศาสตร์ เป็นหลักการที่ใช้สำหรับพิสูจน์ประพจน์ต่าง ๆ ที่เป็นจริงสำหรับทุก ๆ ค่าของ $n$ ที่เป็นจำนวนเต็มบวกซึ่งมีรายละเอียดดังนี้

**ทฤษฎีบท 1.3.1** *หลักอุปนัยเชิงคณิตศาสตร์ที่* 1 ($1^{st}$ *Principle of Mathematical Induction*)
ให้ $P(n)$ แทนข้อความที่เกี่ยวข้องกับจำนวนเต็มบวก $n$ ถ้า
(1) $P(1)$ เป็นจริง
และ (2) ถ้า $P(k)$ เป็นจริงแล้ว $P(k+1)$ เป็นจริง
สำหรับจำนวนเต็มบวก $k$ ใด ๆ
จะได้ว่า $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก $n$

**บทพิสูจน์** ให้ $P(n)$ แทนข้อความที่สอดคล้องกับเงื่อนไข (1) และ (2)
ให้ $S = \{n \in \mathbb{N} \mid P(n) \text{ เป็นจริง}\}$
จาก (1) จะได้ว่า $1 \in S$ และจาก (2) จะได้ว่า ถ้า $k \in S$ แล้ว $k+1 \in S$
ดังนั้นโดยทฤษฎีบท 1.2.11 จะได้ว่า $S$ เป็นเซตของจำนวนเต็มบวก
นั่นคือ $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก $n$ ■

**ตัวอย่าง 1** จงพิสูจน์ว่า $1+2+3+\cdots+n = \dfrac{n(n+1)}{2}$ เป็นจริงสำหรับทุก $n \in \mathbb{N}$

**บทพิสูจน์** ให้ $P(n)$ แทน $1+2+3+\cdots+n = \dfrac{n(n+1)}{2}$
เราจะต้องพิสูจน์ว่า $P(n)$ เป็นจริงสำหรับทุก $n \in \mathbb{N}$
(1) $P(1)$ เป็นจริง เพราะว่า $1 = \dfrac{1(1+1)}{2}$
(2) ถ้ายอมรับ $P(k)$ เป็นจริง แล้วจะต้องแสดงว่า $P(k+1)$ เป็นจริง
สมมติว่า $P(k)$ เป็นจริง นั่นคือ $1+2+3+\cdots+k = \dfrac{k(k+1)}{2}$
ดังนั้น จากสมบัติการเท่ากันของการบวก นำ $k+1$ บวกเข้าทั้งสองข้าง
จะได้ว่า
$$\begin{aligned} 1+2+3+\cdots+k+(k+1) &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{(k+1)[(k+1)+1]}{2} \end{aligned}$$
นั่นคือ $P(k+1)$ เป็นจริง
ดังนั้น $1+2+3+\cdots+n = \dfrac{n(n+1)}{2}$ สำหรับทุก $n \in \mathbb{N}$ ❑

**ตัวอย่าง 2** พิจารณา
$$\begin{aligned} 1+3 &= 4 &&= 2^2 \\ 1+3+5 &= 9 &&= 3^2 \\ 1+3+5+7 &= 16 &&= 4^2 \\ 1+3+5+7+9 &= 25 &&= 5^2 \\ &\vdots \end{aligned}$$
จงพิสูจน์ว่า $1+3+5+\cdots+(2n-1) = n^2$ เป็นจริงสำหรับทุก $n \in \mathbb{N}$

**บทพิสูจน์** ให้ $P(n)$ แทนข้อความ $1+3+5+7+\cdots+(2n-1) = n^2$
เราจะต้องพิสูจน์ว่า $P(n)$ เป็นจริงสำหรับทุก $n \in \mathbb{N}$

(1) $P(1)$ เป็นจริง เพราะว่า $1 = 1^2$

(2) ถ้ายอมรับ $P(k)$ เป็นจริงแล้วจะต้องแสดงว่า $P(k+1)$ เป็นจริง
สมมติว่า $P(k)$ เป็นจริง นั่นคือ $1+3+5+\cdots+(2k-1) = k^2$
ดังนั้นจากสมบัติการเท่ากันของการบวก นำ $2k+1$ บวกเข้าทั้งสองข้าง
จะได้ว่า

$$\begin{aligned} 1+3+5+7+\cdots+(2k-1)+(2k+1) &= k^2+(2k+1) \\ &= (k+1)^2 \end{aligned}$$

นั่นคือ $P(k+1)$ เป็นจริง

ดังนั้น $1+3+5+7+\cdots+(2n-1) = n^2$ สำหรับทุก $n \in \mathbb{N}$ ❑

การพิสูจน์โดยใช้หลักอุปนัยเชิงคณิตศาสตร์ อาจนำไปใช้พิสูจน์ข้อความที่เกี่ยวกับจำนวนเต็ม $n$ ใด ๆ ที่ $n \geq a$ เมื่อ $a \in \mathbb{Z}$ ซึ่งมีรายละเอียดดังทฤษฎีบทต่อไปนี้

**ทฤษฎีบท 1.3.2** ให้ $P(n)$ แทนข้อความที่เกี่ยวข้องกับจำนวนเต็ม $n$ และ $a \in \mathbb{Z}$

(1) $P(a)$ เป็นจริง

และ (2) สำหรับจำนวนเต็ม $k$ ซึ่ง $k \geq a$
ถ้า $P(k)$ เป็นจริง แล้ว $P(k+1)$ เป็นจริง

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

**บทพิสูจน์** เนื่องจาก $n \geq a$ ดังนั้น $n = a, a+1, a+2, a+3, \ldots$
ถ้าให้ $m = n-a+1$ จะได้ $m = 1, 2, 3, 4, \ldots$
และจะได้ $P(n)$ คือประโยคเดียวกับ $P(m+a-1)$
ในการพิสูจน์ว่าข้อความ $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็ม $n$ ที่ $n \geq a$
เป็นการเพียงพอที่เราจะพิสูจน์ว่าข้อความ $P(m+a-1)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก $m$
ให้ $Q(m)$ แทน $P(m+a-1)$
จะได้ว่า $Q(1)$ แทน $P(1+a-1)$ ซึ่งก็คือ $P(a)$
$Q(k)$ แทน $P(k+a-1)$
และ $Q(k+1)$ แทน $P(k+1+a-1)$

(1) $Q(1)$ เป็นจริงเพราะ $P(a)$ เป็นจริงตามที่กำหนดให้ข้อ (1)

(2) ถ้า $Q(k)$ เป็นจริงจะได้ $P(k+a-1)$ เป็นจริงโดยที่ $k \geq 1$
จะได้ $k+a-1 \geq a$ เมื่อ $P(k+a-1)$ เป็นจริง
จากที่กำหนดให้ ข้อ (2) จะได้ $P(k+1+a-1)$ เป็นจริง
นั่นคือ $Q(k+1)$ เป็นจริง

จาก (1) และ (2) สรุปว่า $Q(m)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก $m$
ดังนั้น $P(m+a-1)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก $m$ ที่ $m \geq 1$
แต่ $n = m+a-1$ เมื่อ $m \geq 1$ จะได้ว่า $n \geq a$
จึงได้ว่า $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็ม $n$ ที่ $n \geq a$ ■

**ตัวอย่าง 3** จงพิสูจน์ว่า $3^n > n^3$ เป็นจริงสำหรับทุกจำนวนเต็มบวก $n$ ที่ $n \geq 4$

**บทพิสูจน์** ให้ $P(n)$ แทนข้อความ $3^n > n^3$

(1) $P(4)$ เป็นจริง เพราะว่า $3^4 > 4^3$

(2) ถ้ายอมรับ $P(k)$ เป็นจริงเมื่อ $k \geq 4$ แล้วจะต้องแสดงว่า $P(k+1)$ เป็นจริง
สมมติว่า $P(k)$ เป็นจริง นั่นคือ $3^k > k^3$ เป็นจริง
จากสมบัติของจำนวนเต็ม นำ 3 คูณทั้งสองข้าง จะได้ว่า

$$3^{k+1} > k^3 + k^3 + k^3 > k^3 + 3k^2 + 3k + 1$$

ดังนั้น $3^{k+1} > (k+1)^3$

นั่นคือ $P(k+1)$ เป็นจริง
ดังนั้น $3^n > n^3$ เป็นจริงสำหรับทุกจำนวนเต็มบวก $n$ ที่ $n \geq 4$ ❑

**ปัญหา 4** ให้ $n! = n(n-1)(n-2)\cdots(3)(2)(1)$
จงพิสูจน์ว่า $n! > 2^n$ เป็นจริงสำหรับทุกจำนวนเต็มบวก $n$ ที่ $n \geq 4$

**ทฤษฎีบท 1.3.3** *หลักอุปนัยเชิงคณิตศาสตร์ที่ 2 ($2^{nd}$ Principle of Mathematical Induction)*
ให้ $P(n)$ แทนข้อความที่เกี่ยวข้องกับจำนวนเต็มบวก $n$ ถ้า
(1) $P(1)$ เป็นจริง
และ (2) ถ้า $P(k)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก $k$ ที่ $k < m$ แล้ว $P(m)$ เป็นจริง
จะได้ว่า $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก $n$

**บทพิสูจน์** ให้ $S = \{n \in \mathbb{N} \mid P(n) \text{ เป็นเท็จ}\}$
สมมติว่า $S \neq \varnothing$ โดยหลักการจัดอันดับดี จะมี $m \in S$ ซึ่ง $m$ เป็นจำนวนเต็มบวกที่น้อยที่สุดใน $S$
ดังนั้น $P(m)$ เป็นเท็จ
เนื่องจาก $P(1)$ เป็นจริง ดังนั้น $m > 1$
แสดงว่า $P(k)$ เป็นจริงสำหรับทุกจำนวนจริงบวก $k$ ที่ $k < m$
โดยสมมติฐานข้อ (2) จะได้ว่า $P(m)$ เป็นจริงซึ่งผลที่ได้ ขัดแย้งกับ $m \in S$
ดังนั้นที่สมมติว่า $S \neq \varnothing$ เป็นเท็จ แสดงว่า $S = \varnothing$
นั่นคือ $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก $n$ ■

**หมายเหตุ** (1) โดยทั่วไปนิยมเรียกการพิสูจน์หลักอุปนัยเชิงคณิตศาสตร์ที่ 2 นี้ว่า**หลักอุปนัยอย่างเข้ม** (*Strong Induction*)

(2) เราสามารถแสดงได้ว่าการพิสูจน์โดยใช้ทฤษฎีบท 1.3.3 อาจนำไปใช้พิสูจน์ข้อความที่เกี่ยวกับจำนวนเต็ม $n$ ใด ๆ ที่ $n \geq a$ เมื่อ $a \in \mathbb{Z}$ ซึ่งมีรายละเอียดดังนี้

**หลักอุปนัยอย่างเข้ม (Strong Induction)**

ให้ $P(n)$ เป็นข้อความที่เกี่ยวข้องกับจำนวนเต็ม $n$ และ $a \in \mathbb{Z}$ ซึ่ง

(1) $P(a)$ เป็นจริง

(2) ถ้า $P(a),\ P(a+1),\ P(a+2),\ \ldots,\ P(m-1)$ เป็นจริง แล้ว $P(m)$ เป็นจริง

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

**ตัวอย่าง 4** พิจารณาลำดับ $1, 3, 4, 7, 11, 18, 29, 47, 76, \ldots$

ลำดับนี้เรียกว่า **ลำดับลูคัส** (*Lucus sequence*)

โดยที่ $a_1 = 1, \quad a_2 = 3$ และ

$a_n = a_{n-1} + a_{n-2}$ สำหรับทุกจำนวนเต็มบวก $n$ ที่ $n \geq 3$

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

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

(1) $n = 1$ จะได้ $a_1 = 1 < \left(\frac{7}{4}\right)^1$ ดังนั้น $P(1)$ เป็นจริง

$n = 2$ จะได้ $a_2 = 3 < \left(\frac{7}{4}\right)^2$ ดังนั้น $P(2)$ เป็นจริง

(2) สมมติว่า $P(k)$ เป็นจริงสำหรับทุก $k < m$ เมื่อ $m \geq 3$

ดังนั้น $a_{m-1} < \left(\frac{7}{4}\right)^{m-1}$ และ $a_{m-2} < \left(\frac{7}{4}\right)^{m-2}$

แต่ $a_m = a_{m-1} + a_{m-2} < \left(\frac{7}{4}\right)^{m-1} + \left(\frac{7}{4}\right)^{m-2} = \left(\frac{7}{4}\right)^{m-2}\left(\frac{7}{4} + 1\right)$

ดังนั้น $a_m < \left(\frac{7}{4}\right)^{m-2}\left(\frac{11}{4}\right) < \left(\frac{7}{4}\right)^{m-2}\left(\frac{7}{4}\right)^{n} < \left(\frac{7}{4}\right)^{m}$ เป็นจริง

นั่นคือ $P(m)$ เป็นจริง

โดยหลักอุปนัยเชิงคณิตศาสตร์ที่ 2 สรุปได้ว่า

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